GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

GUIDE D'ADMINISTRATION

Version 2.6.3

Dernière mise à jour du document : 19 septembre 2024

Référence : ses-fr-guide_d_administration-v2.6.3

Table des matières

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.

1. Avant de commencer

Bienvenue dans le guide d'administration de Stormshield Endpoint Security Evolution version 2.6.3.

Ce document contient toutes les informations techniques nécessaires au fonctionnement et à la supervision du produit dans votre environnement.

La solution de sécurité globale SES Evolution offre aux organisations de toutes tailles une protection complète des postes de travail des collaborateurs. L'agent SES Evolution est installé sur les postes et les protège des attaques connues et inconnues, ainsi que des intrusions, de façon transparente pour les collaborateurs. L'agent est paramétré à partir d'une console d'administration et est en contact permanent avec les gestionnaires d'agents SES Evolution qui diffusent les politiques de sécurité.

La console d'administration permet également de configurer les politiques de sécurité et de consulter les logs des événements remontés par les postes de travail afin d'en surveiller le fonctionnement.

SES Evolution dispose également d'une API REST publique. Par défaut, elle n'est pas activée. Pour plus d'informations sur l'API publique, reportez-vous à la section Activer et gérer l'API publique de SES Evolution.

2. Se connecter à la console d'administration SES Evolution

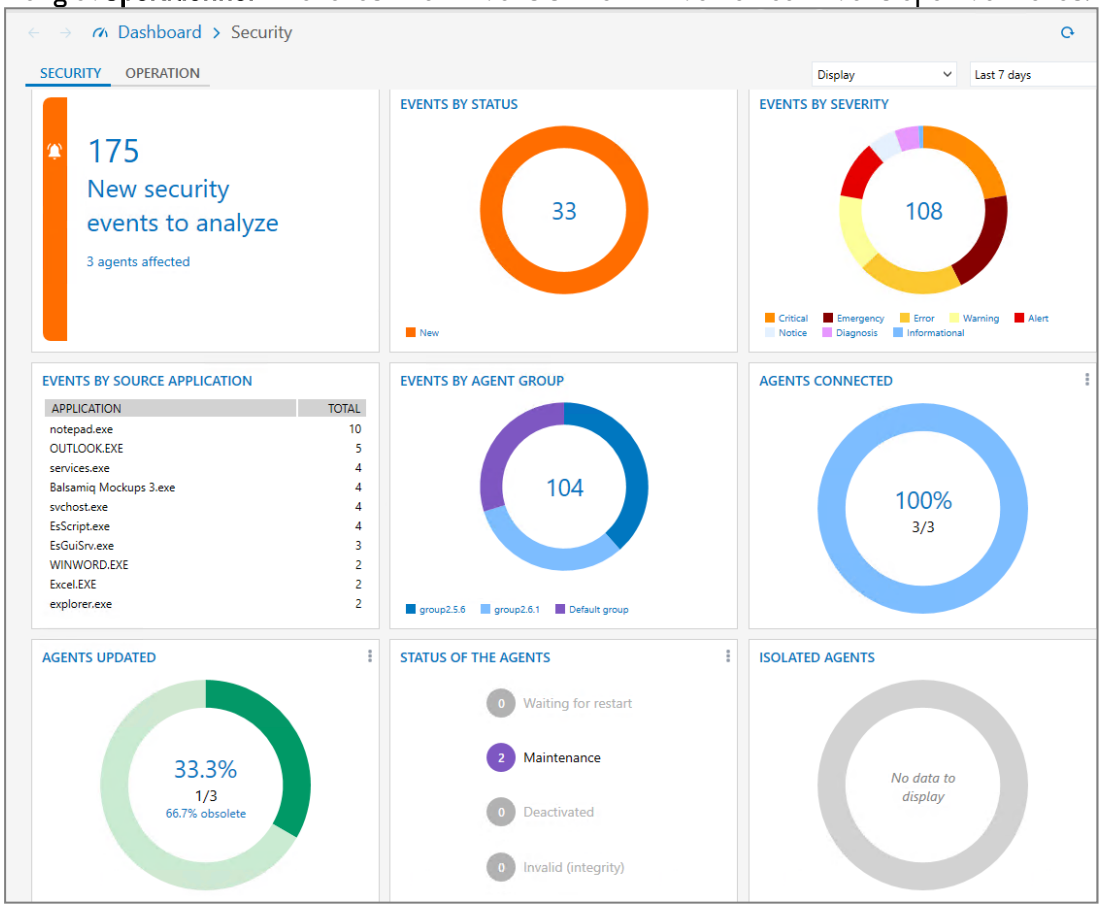
1. Connectez-vous au poste de travail avec votre compte de domaine Microsoft Windows.
2. Lancez la console d'administration Stormshield Endpoint Security Evolution  .
   Vous êtes maintenant connecté à la console avec votre compte Windows.
   Si le compte Windows n'est pas reconnu ou si le composant backend est injoignable, une fenêtre de connexion s'affiche mais la console d'administration ne s'ouvre pas.
3. Pour consulter les préférences de votre compte, cliquez sur l'icône  dans le bandeau supérieur de la console, à côté de votre nom d'utilisateur. La console d'administration s'affiche par défaut dans la langue de votre système d'exploitation, vous pouvez modifier la langue de la console.

Pour se connecter avec un autre compte que celui avec lequel la session Windows a été ouverte, il est également possible de lancer le fichier exécutable de la console en utilisant l'option **Exécuter en tant qu'autre utilisateur**.

3. Comprendre le tableau de bord

Le tableau de bord SES Evolution présente une vue synthétique de l'administration et de la sécurité de votre parc. Il permet de repérer rapidement quels éléments posent problème et fournit des raccourcis vers les différents panneaux de configuration ou de surveillance. Il est composé de deux onglets :

- L'onglet **Sécurité** affiche les indicateurs sur les événements qui se produisent sur les agents.
- L'onglet **Opérationnel** affiche les informations sur le maintien en conditions opérationnelles.



3.1 Surveiller les agents SES Evolution

L'onglet **Sécurité** du tableau de bord fournit un aperçu rapide des événements les plus critiques qui surviennent sur votre parc, et de l'état des agents SES Evolution.

3.1.1 Surveiller les événements survenant sur les agents

Un événement est un groupement de plusieurs logs identiques générés sur plusieurs agents.

- La tuile **Nouveaux événements de sécurité à analyser** affiche les informations suivantes sans limite de temps :
  - Nombre d'événements de niveau *Urgence* et *Alerte* ayant l'état *Nouveau*,
  - Nombre d'agents concernés,
  - Nombre d'événements apparus dans les dernières 24 heures,
  - Pourcentage de progression des derniers événements apparus dans les dernières 24 heures, par rapport au total.

  Cliquez sur le nombre pour consulter la liste des logs agents de niveau *Urgence* et *Alerte* ayant l'état *Nouveau*.
- Les autres tuiles **Événements...**affichent par défaut des indicateurs sur les dernières 24 heures. Vous pouvez modifier cette période via la liste déroulante en haut à droite. Cliquez sur le titre des tuiles **Événements...** ou sur les différentes parties des diagrammes ou listes pour accéder directement au panneau **Environnement > Logs agents** et voir la liste filtrée selon la période sélectionnée et le type d'indicateur.

3.1.2 Vérifier l'état des agents

- Le diagramme **Agents** permet de connaître le nombre d'agents et leur état.

État	Description
À jour	Agent qui dispose d'une version logicielle, de politique et de configuration en accord avec celle définie par son groupe d'agents. Il peut éventuellement avoir une version logicielle supérieure si le retour à une version antérieure est interdit et que cet agent a fait l'objet d'une mise à jour forcée.
Connecté	Agent qui s'est bien reconnecté à son gestionnaire d'agents dans le temps normal défini dans son groupe.
Désactivé	Agent ayant été désactivé par challenge.
En attente de redémarrage	Agent devant être redémarré pour terminer une installation, une mise à jour, ou un changement de fonctionnalités.
Maintenance	Agent ayant le mode Maintenance activé.
Invalide	Agent ayant remonté des problèmes après une vérification d'intégrité.

Cliquez sur les cercles, textes et nombres d'agents pour accéder directement au panneau **Agents** et voir la liste filtrée.
Cliquez sur **Agents** en haut à gauche de la tuile pour accéder directement au panneau général sur les agents. Pour plus d'informations, reportez-vous à la section Visualiser les agents dans la console.

- Le diagramme **Agents isolés** permet de connaître le nombre d'agents isolés du réseau et leur état d'isolation :

État d'isolation	Description
Isolé	Agent ayant été isolé du réseau
En attente d'isolation	Une isolation a été demandée pour l'agent, mais l'agent ne l'a pas encore exécutée.
En attente d'arrêt d'isolation	Un arrêt d'isolation a été demandé pour l'agent, mais l'agent ne l'a pas encore exécuté.

Cliquez sur chaque partie du graphique pour accéder directement au panneau **Isolation** et voir la liste filtrée.
Cliquez sur **Agents isolés** en haut à gauche de la tuile pour accéder directement au panneau général sur l'isolation. Pour plus d'informations, reportez-vous à la section Isoler des ordinateurs du réseau.

3.2 Surveiller les ressources opérationnelles

L'onglet **Opérationnel** du tableau de bord fournit un aperçu rapide de l'état des ressources du backoffice et le maintien en conditions opérationnelles.

3.2.1 Connaître la version des agents SES Evolution

La tuile **Agents SES Evolution versions** affiche la répartition des versions logicielles sur votre parc. Passez la souris sur la portion du cercle correspondant à une version pour afficher le nombre d'agents concernés.

Cliquez sur ••• pour exporter au format csv la liste de tous les agents du parc, ou une liste d'agents selon leur état.

Dans l'image ci-dessus, on voit que le parc est composé de 21 agents dont 11 sont en mode maintenance et un seul est à jour. La totalité des agents sont connectés.

Cliquez sur le cercle, texte et nombres d'agents pour accéder directement au panneau **Agents** et voir la liste filtrée.

Cliquez sur **Agents** en haut à gauche de la tuile pour accéder directement au panneau général sur les agents. Pour plus d'informations, reportez-vous à la section Visualiser les agents dans la console.

3.2.2 Contrôler les licences

La tuile **Licences** contient des informations sur les licences sous la forme d'un diagramme.

Le diagramme affiche le nombre d'agents actifs et la proportion par rapport au nombre d'agents autorisés par la licence. Un agent actif est un agent qui s'est connecté au gestionnaire d'agents depuis moins de 10 jours. Le diagramme change de couleur selon la proportion de licences utilisées.

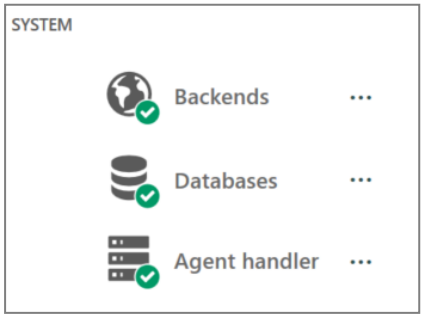
Vert	Le nombre d'agents actifs est inférieur à 90% de la capacité totale des licences.
Orange	Le nombre d'agents actifs est entre 90% et 110% de la capacité totale des licences.
Rouge	La marge de tolérance de 110% est dépassée.
Gris	La licence est expirée.

Les informations de licence sont actualisées à chaque accès au tableau de bord et toutes les heures.

Cliquez sur **Licences** en haut à gauche de la tuile pour accéder directement au panneau des licences. Pour plus d'informations, reportez-vous à la section Gérer les licences SES Evolution.

3.2.3 Vérifier l'état des serveurs

La tuile **Système** permet de connaître sous forme de couleurs l'état des différents serveurs : backends, bases de données, et gestionnaires d'agents. Pour plus d'informations, reportez-vous au *Guide d'installation SES Evolution*.



Si un problème est détecté sur un serveur, SES Evolution émet un log système et l'icône du serveur change de couleur.

Cliquez sur les icônes et noms des serveurs pour accéder directement au panneau des **Logs système** et voir la liste filtrée.

Backends

Le backend est le serveur applicatif qui centralise les opérations effectuées sur l'environnement SES Evolution. L'icône des backends  change de couleur selon la consommation de ressources :

Vert	Tous les backends sont fonctionnels.
Orange	Un ou plusieurs backends ont une consommation moyenne de RAM ou CPU supérieure à 90% (moyenne glissante sur 1h), ou l'espace disque occupé est supérieur à 75%.
Rouge	Un ou plusieurs backends n'ont pas mis à jour leur état depuis plus de 5 minutes, la tâche de suppression des logs ne s'est pas déroulée correctement, ou l'espace disque occupé est supérieur à 85% .

Cliquez sur  pour obtenir des informations plus précises sur la consommation des ressources et la date de dernière connexion de chaque backend. Ces informations sont également accessibles depuis le bandeau supérieur de la console.

Le résultat de la tâche de suppression des logs est également indiqué. Si la tâche a échoué, déplacez votre souris sur la croix rouge de la colonne **Tâche** pour afficher le message d'erreur exact. Pour plus d'informations sur cette tâche, reportez-vous à la section Superviser les bases de données

Bases de données

SES Evolution fonctionne avec plusieurs bases de données, dont une base de données d'administration et une base de données de logs.

L'icône des bases de données  change de couleur selon si elles sont joignables ou non et selon l'occupation de l'espace disque :

Vert	Toutes les bases de données sont joignables, et l'espace disque occupé est inférieur à 70%, et la saturation des bases de données est estimée à plus de trois mois.
Orange	Sur au moins une base de données, entre 70% et 80% de l'espace disque est occupé, ou la saturation est estimée entre un mois et trois mois.
Rouge	Au moins une base de données est injoignable, ou l'espace disque occupé est supérieur à 80%, ou la saturation d'une des bases de données est estimée à moins d'un mois.

Cliquez sur  pour connaître le pourcentage d'utilisation de l'espace disque et la date de dernière connexion de chaque base de données. Ces informations sont également accessibles depuis le bandeau supérieur de la console et via le menu **Backoffice > Système**. Pour plus d'informations, reportez-vous à la section Superviser les bases de données

Gestionnaires d'agents

Le gestionnaire d'agents reçoit directement les informations des agents et leurs logs et met à jour la base de données d'administration par l'intermédiaire du backend. L'icône des gestionnaires d'agents  change de couleur selon la consommation de ressources :

Vert	Tous les gestionnaires d'agents sont fonctionnels.
Orange	Un ou plusieurs gestionnaires d'agents ont une consommation moyenne de RAM ou CPU supérieure à 90% (moyenne glissante sur 1h) ou l'espace disque occupé est supérieur à 75%.
Rouge	Un ou plusieurs gestionnaires d'agents n'ont pas mis à jour leur état depuis plus de 5 minutes ou l'espace disque occupé est supérieur à 85%.

Cliquez sur [...] pour obtenir des informations plus précises sur la consommation des ressources et la date de dernière connexion de chaque gestionnaire d'agents. Ces informations sont également accessibles depuis le bandeau supérieur de la console.

3.3 Envoyer les indicateurs du tableau de bord par e-mail

Vous pouvez configurer SES Evolution afin d'envoyer un rapport d'activité par e-mail aux personnes de votre choix. Ce rapport d'activité reprend tous les indicateurs du tableau de bord.

Au préalable vous devez configurer un serveur SMTP. Pour plus d'informations, reportez-vous à la section Configurer un serveur SMTP.

Vous devez disposer du droit **Notifications par e-mails-Modifier** pour configurer l'envoi de rapports d'activité.

Pour envoyer les indicateurs du tableau de bord par e-mail :

1. Dans le menu **Backoffice > Système** de la console d'administration, rendez vous dans l'onglet **Notifications par e-mail**.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
3. Dans la zone **Rapports d'activité**, cliquez sur **Ajouter une règle**.
   L'assistant de création d'une règle s'ouvre.
4. Saisissez le **Nom de la règle** et la **Fréquence** à laquelle vous souhaitez envoyer le rapport d'activité, puis cliquez sur **Suivant**.
5. Dans le champ en bas de l'écran, saisissez l'adresse e-mail de l'utilisateur destinataire du rapport d'activité, choisissez sa langue, puis cliquez sur **Ajouter**.
6. Ajoutez d'autres adresses e-mail si vous souhaitez envoyer le rapport à plusieurs destinataires.
7. Cliquez sur **Créer**.
   La règle est ajoutée dans le tableau de la zone **Rapports d'activité**.
8. Ajoutez d'autres règles si besoin.

Le rapport est envoyé par e-mail à 00:00 chaque jour, chaque dimanche, ou chaque dernier jour du mois, selon la fréquence choisie. Le titre de l'e-mail est de la forme : *SES Evolution - Rapport d'activité du 11/12/2023 au 11/12/2023*.

Vous pouvez désactiver ou réactiver une règle d'envoi en cliquant sur la case à cocher de la colonne **Activé**. Les boutons d'actions à droite d'une règle permettent de la dupliquer ou de la supprimer.

Vous pouvez arrêter temporairement l'envoi des rapports d'activité en désactivant l'option **Activer les notifications**.

SES Evolution permet également d'envoyer par e-mail des alertes en fonction des types de logs générés. Pour plus d'informations, reportez-vous aux sections Envoyer des alertes de logs agents par e-mail et Envoyer des alertes de logs système par e-mail.

4. Gérer les licences SES Evolution

Vous avez enregistré une licence au cours de l'installation de votre environnement SES Evolution.

Les licences définissent le nombre d'agents SES Evolution actifs que vous pouvez gérer avec la solution, ainsi qu'une date de fin de validité.

Vous pouvez importer plusieurs licences, auquel cas le nombre d'agents autorisés correspond à la somme des agents de chaque licence.

4.1 Importer une licence dans SES Evolution

Vous devez disposer du droit **Licences-Modifier** pour importer une licence.

1. Dans le Tableau de bord de la console d'administration, onglet **Opérationnel**, cliquez sur **Licences**.
2. Cliquez sur **Ajouter une licence** et choisissez le fichier de licence (par exemple *SES-JCCA-WE9T-Q5RA.lic*). Le champ **Capacité** représente le nombre d'agents SES Evolution actifs ainsi que le nombre total d'agents autorisés par la licence.

4.2 Consulter les informations de licence

Vous devez disposer du droit **Licences-Afficher** pour consulter les informations de licence.

La zone **Licences** du tableau de bord de la console d'administration, onglet **Opérationnel**, affiche le nombre d'agents actifs et la proportion par rapport au nombre d'agents autorisés. Un agent actif est un agent qui s'est connecté au gestionnaire d'agents depuis moins de 10 jours. Le graphique est vert quand le nombre d'agents actifs est inférieur à 90% de la capacité totale de la licence, orange entre 90% et 110%, et rouge quand la marge de tolérance de 110% est dépassée.

Les informations de licence sont actualisées à chaque accès au tableau de bord et toutes les heures.

5. Gérer les utilisateurs de la console d'administration SES Evolution

Les utilisateurs accèdent à la console avec leur compte Microsoft Windows qui doit appartenir au même domaine Active Directory que le composant backend. Sinon une relation de confiance doit exister entre les domaines.

Par défaut, seul le super administrateur spécifié lors de l'installation peut se connecter à la console d'administration. Il peut ensuite ajouter d'autres utilisateurs ou groupes d'utilisateurs qui pourront s'y connecter à leur tour.

NOTE
Si vous renommez le compte Windows de ce super administrateur, assurez-vous d'avoir créé au préalable un utilisateur portant le nouveau nom dans la console d'administration SES Evolution. Sinon vous ne pourrez plus vous connecter à la console. Pour plus d'informations, reportez-vous à la section Ajouter un utilisateur de la console d'administration.

Chaque utilisateur ou groupe se voit attribuer un rôle qui définit son profil et restreint les fonctionnalités disponibles dans la console d'administration. Trois rôles sont disponibles par défaut : Audit, Assistance et Administration. Vous pouvez également en créer de nouveaux et les personnaliser.

EXEMPLE
Vous pouvez créer un groupe *Administrateurs SES Evolution* dans Active Directory, l'ajouter dans SES Evolution, et lui attribuer le rôle *Administration*. Dans ce cas, tous les utilisateurs du groupe disposeront automatiquement des droits d'administration dans la console SES Evolution. Vous n'aurez pas besoin de les ajouter individuellement.

Plusieurs utilisateurs peuvent se connecter simultanément à des consoles administrant le même parc.

5.1 Créer des rôles personnalisés

Seul un utilisateur disposant du rôle *Administration* est autorisé à ajouter d'autres utilisateurs.

1. Choisissez le menu **Backoffice > Utilisateurs**, puis l'onglet **Rôles**.
2. Cliquez sur **Modifier** dans le bandeau supérieur puis cliquez sur **Créer un rôle**.
3. Attribuez un nom au rôle et entrez sa description si besoin.
4. Cliquez sur **Valider**. Le nouveau rôle s'affiche dans la liste. Par défaut, les droits les plus restrictifs sont appliqués.
5. Pour chaque droit, choisissez le type d'accès que vous souhaitez attribuer. Chaque droit correspond à un panneau de la console d'administration. Par défaut, seuls les panneaux **Déploiement**, **Tableau de bord** et **Licences** sont accessibles.
   Le droit **Verrous** permet de débloquer un verrou positionné par un autre utilisateur sur un panneau de la console. Pour plus d'informations sur les verrous, reportez-vous à la section suivante.

5.2 Ajouter un utilisateur ou un groupe d'utilisateurs de la console d'administration

Seul un utilisateur disposant du rôle *Administration* est autorisé à ajouter d'autres utilisateurs ou groupes.

1. Choisissez le menu **Backoffice > Utilisateurs**, puis l'onglet **Utilisateurs et groupes**.
2. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter** dans la zone **Utilisateurs** ou **Groupes**.
   Une ligne vide s'affiche.
3. Vous pouvez :
   - Cliquer sur l'icône  à droite de la ligne pour sélectionner un utilisateur/groupe dans l'annuaire Active Directory.
   - Saisir manuellement un nom d'utilisateur/groupe Active Directory en respectant la syntaxe *DomainName\samAccountName* pour un utilisateur, et *samAccountName* pour un groupe.
   - Saisir manuellement un nom d'utilisateur local.

   SES Evolution vérifie la validité de l'utilisateur/groupe et affiche son état à droite. Passez votre souris sur l'icône dans la colonne **État** pour en savoir plus.
4. Sélectionnez le rôle à attribuer à l'utilisateur/groupe :
   - **Audit** : Ce rôle permet de visualiser l'ensemble des panneaux de la console et de modifier les paramètres de son compte personnel, mais aucune autre action de modification ou de déploiement n'est possible. Il est dédié à la visualisation des logs et à la surveillance des agents.
   - **Assistance** : Ce rôle possède les mêmes droits que l'Audit. Il permet en plus de répondre à des challenges et de débloquer les verrous. Il est dédié à la maintenance du parc SES Evolution.
   - **Administration** : Ce rôle permet d'effectuer sans restriction toutes les opérations accessibles depuis la console d'administration.
   - **Rôle personnalisé**
5. Dans la zone **Groupe**, classez les groupes par ordre de priorité à l'aide des flèches de la colonne **Ordre**. Si un utilisateur appartient à plusieurs groupes, c'est le rôle du groupe le plus prioritaire qui lui est attribué.

Si un utilisateur est déclaré de manière individuelle ET via un groupe, c'est le rôle de l'utilisateur individuel qui lui est attribué.

5.3 Gérer la connexion simultanée d'utilisateurs à des consoles administrant le même parc

Plusieurs utilisateurs peuvent administrer simultanément le même parc depuis des machines différentes.

Lorsqu'un utilisateur est en train de modifier une des ressources suivantes, elles sont automatiquement verrouillées et aucun autre utilisateur ne peut les modifier :

- Les groupes d'agents,
- Les politiques,
- Les groupes de gestionnaires d'agents.

Le panneau entier est alors verrouillé, c'est-à-dire tous les groupes d'agents, tous les groupes de gestionnaires d'agents, toutes les politiques ou tous les utilisateurs. Par exemple, l'utilisateur 1 ne peut pas modifier la politique A pendant que l'utilisateur 2 modifie la politique B.

Il n'est pas non plus possible d'ajouter de nouveaux groupes ou de nouvelles politiques lorsqu'un panneau est verrouillé.

Lorsqu'un utilisateur enregistre ou annule ses modifications, le verrou sur le panneau est automatiquement libéré si aucun objet n'est plus en cours d'édition dans ce panneau.

Si un utilisateur essaie de modifier un panneau verrouillé, un message dans le bandeau supérieur indique qui a verrouillé le panneau et depuis combien de temps. Il ne peut alors rien modifier.

Cependant, si un utilisateur possède le droit **Verrous - Débloquer** dans son rôle, il peut alors casser le verrouillage du panneau grâce au bouton **Casser le verrou** qui s'affiche dans le bandeau supérieur. Cela peut être utile si une ressource est restée par erreur en cours de modification par exemple.

Cette opération libère le panneau et annule les modifications en cours de l'autre utilisateur. Elle est donc à manier avec précaution. Dans ce cas, l'utilisateur qui détenait le verrou le premier est prévenu au moment où il tente d'enregistrer ses modifications.

Pour casser le verrou sur un panneau si vous possédez le droit :

1. Cliquez sur **Casser le verrou** dans le bandeau supérieur.
2. Confirmez l'opération dans la fenêtre qui s'affiche.

6. Paramétrer les gestionnaires d'agents SES Evolution

Les gestionnaires d'agents sont des serveurs SES Evolution qui permettent de distribuer les politiques de sécurité aux agents ainsi que les mises à jour logicielles. Ils permettent également de réceptionner :

- les logs d'événements des agents, de les enregistrer, et éventuellement de les transmettre à des serveurs Syslog.
- le statut et les données de surveillance des agents et de les afficher dans l'onglet **Agents** du groupe d'agents.

Chaque gestionnaire d'agents appartient à un groupe de gestionnaires d'agents.

Vous devez définir les paramètres propres à chaque gestionnaire d'agents et à chaque groupe. Pour cela, vous devez disposer du droit **Gestionnaires d'agents-Modifier**.

Nous vous recommandons d'installer au moins deux gestionnaires d'agents par groupe de gestionnaires, installés sur deux serveurs distincts, afin d'assurer une continuité de service. Pour plus d'informations, reportez-vous à la section Assurer la continuité de service du *Guide d'installation*.

Afin d'éviter la saturation du disque d'un gestionnaire d'agents, les limites suivantes s'appliquent :

- une limite de 500 Mo sur les dossiers nommés "InvalidPackages" situés dans les dossiers "Normal" et "Urgent" à l'emplacement "%programdata%\Stormshield\SES Evolution\Server\AgentLogs". Ces dossiers stockent des packages de logs envoyés par les agents et que les gestionnaires d'agents ne parviennent pas à traiter correctement.
- une limite de 100 Mo sur le dossier nommé "InvalidCertificates" situé à l'emplacement "%programdata%\Stormshield\SES Evolution\Server". Ce dossier stocke les certificats des agents considérés comme invalides (révoqués ou expirés).

Lorsque ces limites sont atteintes, les fichiers les plus anciens sont supprimés pour libérer la moitié de la capacité de stockage des dossiers.

6.1 Créer des groupes de gestionnaires d'agents

Un groupe de gestionnaires d'agents est composé d'un ou plusieurs gestionnaires d'agents. Lorsqu'un agent doit se connecter à un gestionnaire, il contacte de préférence le dernier gestionnaire ayant accepté sa demande. Si la connexion échoue, il choisit de manière aléatoire un autre gestionnaire du groupe jusqu'à ce que sa demande soit acceptée.

Après installation d'un gestionnaire d'agents, ce dernier s'affiche automatiquement dans le menu **Backoffice > Gestionnaires d'agents** de la console d'administration. Il appartient par défaut à un groupe nommé *Nouveau Groupe (nom_gestionnaire d'agents)*. Vous pouvez modifier ce groupe par défaut, en créer de nouveaux ou déplacer un gestionnaire d'agents dans un autre groupe.

Vous pouvez envoyer les logs des agents vers différents serveurs Syslog, paramétrés pour chaque groupe de gestionnaires d'agents. Paramétrez par exemple plusieurs serveurs Syslog pour recevoir des logs, de différents niveaux de gravité ou avec des formats de contenu différents.

Vous pouvez utiliser la solution de gestion des logs Stormshield Log Supervisor (SLS) avec SES Evolution. Pour plus d'informations, reportez-vous à la section Paramétrer la communication

avec un serveur Stormshield Log Supervisor (SLS) et à la documentation SLS disponible sur le site Stormshield Technical Documentation.

> **NOTE**
> Si un serveur Syslog ou SLS est injoignable, les gestionnaires d'agents stockent temporairement les logs pendant 24h maximum, à condition que l'espace disque soit suffisant.

6.1.1 Créer un nouveau groupe de gestionnaires d'agents

1. Choisissez le menu **Backoffice > Gestionnaires d'agents**.
2. Dans le panneau de gauche, cliquez sur l'icône **+**. La ligne *Nouveau groupe* s'affiche.
3. Dans les **Paramètres du groupe de gestionnaires d'agents**, entrez le **Nom** de votre groupe de gestionnaires d'agents.

4. Si vous souhaitez envoyer les logs des agents de ce groupe de gestionnaires d'agents vers des serveurs Syslog, cliquez sur **Ajouter un serveur** et définissez les paramètres suivants :
   - **Adresse** : Saisissez l'adresse IP ou nom DNS du serveur Syslog.
   - **Protocole** : Choisissez le protocole de communication avec le serveur Syslog. Si vous souhaitez que les données échangées soient chiffrées, sélectionnez TCP/TLS. Dans ce cas, l'autorité de certification racine et les autorités intermédiaires du serveur Syslog doivent être importées dans le magasin de certificats de chaque machine hébergeant un gestionnaire d'agents.
   - **Port** : Entrez le numéro de port utilisé pour Syslog (par défaut *TCP 1468*). Les numéros de port TCP ou UDP indiqués ici doivent être autorisés sur le pare-feu de la machine hébergeant le gestionnaire d'agents, et également sur tous les équipements réseau situés entre le gestionnaire d'agents et le serveur Syslog.
   - **Type de transfert** : Choisissez le paramètre défini à l'installation du serveur Syslog.
   - **Structured data** : Utilisez ce champ pour spécifier des données additionnelles à intégrer dans l'en-tête des messages Syslog. Pour connaître le format attendu des données, consultez la RFC 5424. Vous pouvez ajouter plusieurs données dans le champ. Par exemple : [ABC param1="value1"][KEY@12345 param2="value2"].
   - **Format des messages** : Choisissez le format des messages :
     - le mode textuel simple (comme les messages affichés dans le menu **Logs agents**),
     - le JSON brut contenant toutes les données techniques,
     - le format CEF,
     - le format IDMEF.
   - **Langue du message** : Choisissez la langue le cas échéant.
   - Vous pouvez indiquer une taille maximum des messages en octets.
   - Choisissez la gravité minimum des logs à envoyer vers ce serveur.
   - **Détail de contexte** : Choisissez le niveau de contexte que vous souhaitez envoyer au serveur Syslog :
     - **Aucun** : Aucun détail de contexte n'est envoyé au serveur Syslog qui ne reçoit que les signaux forts d'une attaque (i.e, alertes).
     - **Détail de contexte simple** : Sont envoyés au serveur Syslog les signaux forts et les logs de création et arrêt des processus qui se sont exécutés sur l'agent au moment de l'attaque et peu après le premier log de l'attaque.
     - **Détail de contexte complet** : Sont envoyés au serveur Syslog tous les logs liés à l'attaque quel que soit le niveau de sévérité sélectionné au dessus.
       La réception du détail de contexte complet par le gestionnaire d'agents dépend de la configuration du groupe d'agents. Par défaut, cet envoi est différé, et le détail de contexte simple est envoyé bien avant le détail de contexte complet.

     Pour plus d'informations sur les détails de contextes, reportez-vous à la section Comprendre la composition d'un contexte.

   Si vous avez paramétré au moins un serveur Syslog, un indicateur de fonctionnement des serveurs Syslog s'affiche dans le bandeau supérieur de la console, après déploiement de l'environnement. Il indique, le cas échéant, la présence d'avertissements ou d'alertes. Cliquez sur l'indicateur pour afficher le détail pour chaque serveur.
5. Si vous souhaitez déplacer un gestionnaire d'agents d'un autre groupe vers votre nouveau groupe, sélectionnez le gestionnaire et faites un glisser-déposer vers le nouveau groupe.
6. Cliquez sur **Enregistrer** dans le bandeau supérieur.

NOTE
L'utilisation du protocole UDP n'est pas recommandée pour communiquer avec le serveur Syslog. Nous recommandons l'utilisation du protocole TLS.

6.1.2 Paramétrer la communication avec un serveur Stormshield Log Supervisor (SLS)

Si vous utilisez SLS, la solution de gestion des logs Stormshield, complétez les paramètres de la façon suivante dans la partie **Serveurs Syslog** du panneau de paramétrage d'un groupe de gestionnaires d'agents.

Transmission des logs via le protocole TCP

1. Indiquez l'adresse IP du serveur SLS.
2. Sélectionnez le protocole TCP.
3. Indiquez le port 601.
4. Sélectionnez **JSON brut** pour le **Format des messages**.
5. Sélectionnez **Non-Transparent-Framing** pour le **Type de transfert**.

Transmission des logs via le protocole TCP/TLS

Le serveur SLS doit posséder un certificat X.509 au format PEM.

1. Renseignez le certificat *.crt* et la clé privée *.key* dans la console d'administration de SLS.
2. Importez le certificat racine du serveur SLS dans le magasin de certificats de chaque machine hébergeant un gestionnaire d'agents.
3. Dans la partie **Serveurs Syslog** de la console d'administration SES Evolution, complétez les paramètres de la façon suivante :
   - Indiquez le nom d'hôte ou l'adresse IP du serveur SLS. Elle doit correspondre à l'adresse renseignée dans le certificat. Si vous avez utilisé le nom d'hôte du serveur dans le certificat, vous pouvez indiquer l'adresse IP correspondante dans le fichier HOST des machines hébergeant les gestionnaires d'agents.
   - Sélectionnez le protocole TCP/TLS,
   - Indiquez le port 6514,
   - Sélectionnez **JSON brut** pour le **Format des messages**,
   - Sélectionnez **Non-Transparent-Framing** pour le **Type de transfert**.

Dans les deux cas, si vous avez des problème de réception des logs dans SLS, consultez les logs Système dans la console d'administration SES Evolution. Filtrez sur le gestionnaire d'agents concerné. Pour plus d'informations, reportez-vous à la section Surveiller l'activité des composants backoffice SES Evolution.

NOTE
Le numéro de port TCP indiqué doit être autorisé sur le pare-feu des machines hébergeant les gestionnaires d'agents, et également sur tous les équipements réseau situés entre les gestionnaires d'agents et le serveur SLS.

6.1.3 Résoudre les problèmes

Un serveur Syslog ne reçoit pas les logs émis par les agents :

- *Situation* : Un des serveurs Syslog paramétrés dans un groupe de gestionnaires d'agents ne reçoit aucun log des agents.
- *Cause* : Il peut y avoir une erreur dans la configuration TCP/TLS du serveur Syslog.
- *Solution* : Commencez par vérifier que le serveur Syslog fonctionne bien en TCP.
  Si c'est le cas, consultez alors les logs émis par le gestionnaire d'agents. En cas de problème de configuration TCP/TLS, le gestionnaire d'agents émet un log désignant le serveur Syslog défectueux et décrivant les causes possibles.
  Si vous ne voyez pas ce log, tentez de redémarrer le gestionnaire d'agents pour forcer l'émission de logs. Attendez au moins une minute après le redémarrage.
  Selon les indications données par le log, revoyez alors la configuration TCP/TLS du serveur Syslog.
  Vous pouvez également vérifier le niveau de gravité minimum des logs que vous avez paramétré, pour qu'ils soient envoyés au serveur Syslog.

6.2 Configurer les paramètres d'un gestionnaire d'agents

Après installation d'un gestionnaire d'agents, ce dernier s'affiche automatiquement dans le panneau **Gestionnaires d'agents** de la console d'administration. Il appartient par défaut à un groupe de gestionnaire d'agents nommé *New Group (nom_gestionnaire d'agents)*.

1. Choisissez le menu **Backoffice > Gestionnaires d'agents**.
2. Sélectionnez le gestionnaire d'agents dans le panneau de gauche.
3. Cliquez sur **Modifier** dans le bandeau supérieur.
4. Modifiez le **Nom** par défaut pour ce gestionnaire d'agents si nécessaire.
5. Cliquez sur **Enregistrer** dans le bandeau supérieur.

7. Gérer les agents SES Evolution

L'agent SES Evolution est installé sur tous les postes de travail afin de détecter ou protéger des attaques malveillantes. Le gestionnaire d'agents SES Evolution lui fournit la politique de sécurité et il applique les protections correspondantes. Chaque agent envoie au gestionnaire d'agents les logs des événements qui se sont produits, ainsi que son état. Vous pouvez ainsi suivre l'état de votre parc depuis la console d'administration.

L'agent se connecte de manière périodique aux gestionnaires d'agents du groupe de gestionnaires qui lui est attribué. Il se connecte de préférence au dernier gestionnaire ayant accepté sa demande. Si la connexion échoue, il choisit de manière aléatoire un autre gestionnaire du groupe jusqu'à ce que sa demande soit acceptée.

Lorsque l'agent n'est pas connecté à un réseau ou qu'aucun des gestionnaires d'agents par défaut ou de secours n'est accessible, il fonctionne de manière autonome en appliquant les dernières politiques de sécurité connues.

L'agent conserve ses logs en local pendant toute la durée où il est déconnecté du réseau. À la reconnexion, il envoie ses logs au gestionnaire d'agents. Il est également possible d'exporter ses logs dans un fichier *.cab* et de les importer pour les visualiser dans la console d'administration. Pour plus d'informations, reportez-vous à la section Consulter les logs des agents déconnectés.

7.1 Créer et configurer les groupes d'agents

Un groupe d'agents est un modèle d'agent SES Evolution que vous déployez sur tous les postes de travail qui doivent partager la même configuration, en particulier la même politique de sécurité. Toute modification ultérieure de la configuration du groupe d'agent est appliquée à tous les agents du groupe.

EXEMPLE

Vous pouvez créer des groupes d'agents distincts pour les cas suivants :

- Les serveurs et les postes de travail des utilisateurs qui ne bénéficieront pas du même niveau de sécurité,
- Les différents services de la société qui peuvent nécessiter des règles de sécurité personnalisées,
- Les ordinateurs portables des salariés en mobilité et les ordinateurs fixes, etc.

Après l'installation d'un agent SES Evolution sur un poste de travail, celui-ci s'affiche dans le panneau **Agents** de la console d'administration. Il est placé automatiquement dans le groupe d'agents auquel il appartient.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour créer et configurer les groupes d'agents.

Pour créer un groupe d'agents :

Un groupe d'agents nommé *Groupe par défaut* est créé automatiquement dans la console, mais vous pouvez créer des groupes d'agents personnalisés.

1. Choisissez le menu **Environnement > Agents**.
2. Dans le panneau de gauche, cliquez sur **Créer un groupe**. La ligne *Nouveau groupe* s'affiche.
3. Dans l'onglet **Agents** du panneau de droite, entrez un **Nom** pour le groupe.

4. Configurez le groupe d'agents à votre convenance dans les onglets **Politiques**, **Tâches planifiées**, **Paramètres** et **État et logs**. Vous devez au minimum choisir une politique.
5. Cliquez sur **Enregistrer** dans le bandeau supérieur pour enregistrer vos modifications.

Pour créer un nouveau groupe, vous pouvez également dupliquer un groupe existant. Un groupe dupliqué conserve tous les paramètres du groupe d'origine mais ne contient pas d'agent.

1. Sélectionnez le groupe à dupliquer.
2. Cliquez sur **Dupliquer** depuis le menu ≡.

7.1.1 Appliquer des politiques de sécurité aux agents

Vous devez obligatoirement appliquer au moins une politique de sécurité à chaque groupe d'agents. Il est possible d'ajouter aussi plusieurs politiques secondaires qui s'appliquent lorsque certaines conditions sont remplies.

EXEMPLE
Vous pouvez ajouter une politique conditionnelle de mobilité qui s'applique lorsque le poste de travail ne se trouve plus sur le réseau interne de la société. Ou bien une politique de quarantaine qui s'applique si les indicateurs de santé d'un agent ne sont pas satisfaisants.

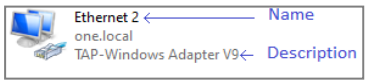
Pour appliquer une ou plusieurs politiques de sécurité à un groupe d'agents :

1. Rendez-vous dans l'onglet **Politiques** d'un groupe d'agents.
2. Dans la liste déroulante **Politique**, choisissez la politique de sécurité principale que vous souhaitez appliquer à tous les agents du groupe.

ASTUCE
Une "politique vide" est proposée dans la liste déroulante. Elle permet de désactiver ponctuellement la protection d'un groupe d'agents (excepté l'autoprotection), par exemple en phase de test ou de dépannage.

3. Si nécessaire, cliquez sur **Ajouter une politique conditionnelle** et attribuez-lui un nom.
4. Dans la liste déroulante **Politique**, choisissez la politique qui s'appliquera sous certaines conditions.
5. Cliquez sur **Ajouter une condition** et attribuez un nom à la condition.

6. Cliquez sur **Ajouter un test** et choisissez l'un des tests suivants :
   Adresse IP
   Indiquez une adresse IP, une plage d'adresses ou un sous-réseau et choisissez s'ils doivent se trouver dans l'intervalle ou hors de l'intervalle pour valider le test.
   Vous pouvez indiquer plusieurs intervalles séparés par des virgules. Par exemple *172.16.16.0/0.0.0.24,10.10.0.0/16*.
   Gestionnaire d'agents joignable
   Activez l'option pour indiquer que l'agent doit pouvoir joindre le gestionnaire d'agents pour valider le test.
   Ping
   Indiquez l'adresse IP ou le nom réseau de la machine que vous souhaitez atteindre par un ping, si l'agent doit pouvoir la joindre ou non pour valider le test, le nombre de tentatives, et la fréquence des tentatives.
   Résultat d'un script personnalisé
   Cliquez sur [***] pour ajouter un script en précisant son chemin, les arguments, et le contexte d'exécution. Indiquez obligatoirement quel doit être son **Résultat** pour valider le test. Ce résultat doit correspondre à un code de sortie du script.
   Utilisez de préférence **Service local** car c'est un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.
   Notez que même si vous avez bloqué l'exécution de scripts dans les politiques de sécurité, SES Evolution considère que vos scripts personnalisés internes sont fiables et autorise leur exécution.
   Connexion à un domaine
   Indiquez le nom du domaine et si l'agent doit ou ne doit pas y être connecté pour valider le test. La valeur *Non connecté* indique :
   - Que l'agent n'est pas lié au domaine en question,
   - Si l'agent est lié au domaine, qu'il n'est pas connecté au réseau de domaine.

   Statut d'une interface réseau
   Cliquez sur [***] pour ajouter une interface réseau en précisant son nom, son identifiant unique (GUID) ou sa description. Indiquez aussi quel doit être son statut pour valider le test : **Connectée** ou **Déconnectée ou inactive**.
   Le Nom et la Description d'une interface sont visibles dans le panneau des connexions réseau de Windows.
   

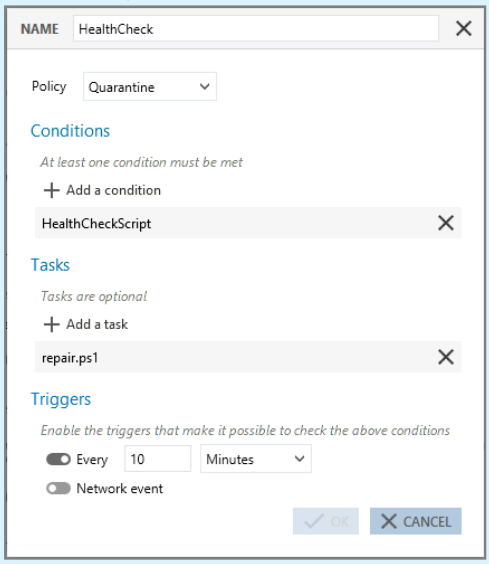
   Sous Windows 10, pour obtenir toutes les informations sur une interface, dont son GUID, exécutez la commande Powershell suivante :
   ```
   Get-NetAdapter | Select Name, InterfaceName, InterfaceGUID, InterfaceDescription, Status
   ```
7. Si nécessaire, ajoutez d'autres tests puis cliquez sur **OK**. L'ordre des tests est indifférent puisque TOUS les tests doivent être validés pour que la condition soit remplie.
8. Si nécessaire, ajoutez d'autres conditions. Il suffit que l'une des conditions soit remplie pour que la politique correspondante s'applique.
   Les conditions s'appliquent dans l'ordre où elles sont affichées.
9. Si vous souhaitez exécuter un script personnalisé à chaque application de la politique conditionnée, cliquez sur **Ajouter une tâche**. À l'ajout du script, vous précisez son chemin, les arguments, et le contexte d'exécution.
   Utilisez de préférence **Service local** car c'est un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

10. Dans la zone **Déclencheurs**, choisissez un ou plusieurs événements qui déclencheront la vérification des conditions :
    - Activez l'option **Toutes les** pour vérifier les conditions à un intervalle régulier que vous spécifiez.
    - Activez l'option **Événement réseau** pour vérifier les conditions quand le poste de travail change d'interface réseau, par exemple s'il se connecte à un réseau wi-fi, si un portable est branché sur une station d'accueil, etc.
11. Cliquez sur **Valider**. Le résumé des conditions s'affiche dans l'onglet **Politiques** des groupes d'agents.
12. Ordonnez les conditions à votre convenance à l'aide des flèches situées à gauche. L'ordre des politiques conditionnelles est important.

EXEMPLE 1

Mise en quarantaine d'un poste de travail si ses indicateurs de santé ne sont pas satisfaisants.

Ici, toutes les 10 minutes, un script s'exécute sur les agents qui vérifie leur état de santé. Si le résultat n'est pas satisfaisant sur un agent, la politique *Quarantine* lui est appliquée et un deuxième script de réparation s'exécute. Une politique de quarantaine isole un agent en bloquant par exemple ses communications sur le réseau ainsi que tous les périphériques amovibles, sauf ceux des administrateurs.



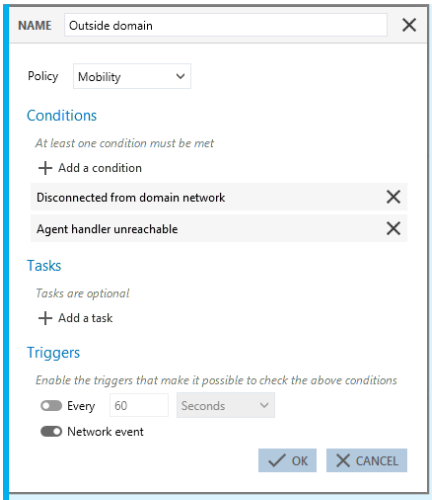
EXEMPLE 2

Application d'une politique spécifique pour les ordinateurs portables en mobilité.

Ici, à chaque événement réseau se produisant sur un poste de travail, SES Evolution lance tous les tests prévus par la condition :

- Le poste de travail n'est pas connecté à son réseau de domaine,
- Le gestionnaire d'agents n'est pas joignable.

Si les tests sont positifs, alors la politique *Mobility* est appliquée.



7.1.2 Activer les clichés instantanés Windows

La protection anti-ransomware de SES Evolution surveille les modifications et chiffrements de fichiers et bloque le processus responsable si elle détecte que ces opérations sont malveillantes. Quelques fichiers peuvent être néanmoins chiffrés avant que le blocage ne soit effectif.

Si vous activez la protection anti-ransomware, il est fortement recommandé d'activer la création quotidienne de clichés instantanés par SES Evolution. Cette fonctionnalité, basée sur le service VSS de Windows, vous permettra de restaurer rapidement les quelques fichiers perdus.

ATTENTION :
L'activation des clichés instantanés ne remplace pas les sauvegardes régulières. Il est primordial de disposer d'une solution de sauvegarde dédiée en parallèle.

Prérequis

Vous devez vous conformer aux prérequis Windows suivants pour pouvoir activer les clichés instantanés dans SES Evolution :

- Autoriser la création de clichés instantanés pour tous les volumes NTFS sur tous les postes de travail protégés par un agent SES Evolution.
- Réserver de l'espace pour les clichés instantanés sur tous les volumes locaux NTFS des postes de travail protégés par un agent SES Evolution.
  Utilisez la commande Windows `vssadmin resize shadowstorage` pour définir cet espace.

Pour plus d'informations, consultez la documentation Microsoft.

EXEMPLE
Exécutez la commande :
`vssadmin resize shadowstorage /For=C: /On=C: /MaxSize=15%`
pour réserver 15% de l'espace du volume C:\ au stockage des clichés instantanés du volume C:\.

Activer les clichés instantanés

1. Dans l'onglet **Politiques** d'un groupe d'agents, rendez-vous dans la section **Clichés instantanés quotidiens**.
2. Activer l'option **Activer les clichés instantanés quotidiens**.
   SES Evolution effectuera un cliché par 24 heures des lecteurs locaux du poste de travail dont le système de fichiers est NTFS. Seuls les cinq derniers clichés seront conservés.

Pour plus d'informations sur la protection anti-ransomware et la procédure de restauration de fichiers chiffrés, reportez-vous aux sections :

- Configurer la protection contre les menaces
- Gérer une attaque par ransomware

7.1.3 Détecter et configurer le niveau de confiance des périphériques

SES Evolution contrôle les clés USB et autres périphériques de stockage USB. Tout périphérique de stockage USB branché sur un agent SES Evolution peut être détecté et s'afficher dans le panneau **Sécurité > Périphériques** de la console d'administration en fonction des options activées. Ce panneau permet d'attribuer manuellement un niveau de confiance à ces périphériques. Pour plus d'informations, reportez-vous à la section Modifier le niveau de confiance d'un périphérique USB.

Vous pouvez aussi automatiser certaines actions pour tous les périphériques USB branchés sur les agents d'un groupe.

1. Dans l'onglet **Politiques** d'un groupe d'agents, rendez-vous dans la section **Confiance des périphériques**.
2. Activez l'option **Autoriser l'identification d'un périphérique** si vous souhaitez que SES Evolution détecte chaque périphérique USB branché sur un agent du groupe et lui attribue automatiquement le niveau de confiance 1.
3. Activez l'option **Accorder la confiance aux périphériques vides** si vous souhaitez que SES Evolution détecte chaque périphérique USB branché sur un agent du groupe et attribue automatiquement le niveau de confiance 2 à chaque périphérique USB vide.
4. Activez l'option **Analyser automatiquement le périphérique** pour attribuer automatiquement le niveau de confiance 2 à chaque périphérique USB branché sur un agent du groupe. Lorsque cette option est activée, le ou les antivirus installés sur le poste analysent la clé lors de son branchement, et neutralisent d'éventuels fichiers malveillants. Si tous les fichiers sont analysables par l'antivirus, alors le périphérique est considéré comme fiable. En revanche, si certains fichiers sont inaccessibles, le périphérique n'obtient pas le niveau 2 de confiance. Il conserve son niveau courant.

Pour plus d'informations, reportez-vous à la section Gérer les périphériques de stockage USB.

7.1.4 Créer des tâches planifiées

Les tâches planifiées permettent d'exécuter automatiquement des scripts sur les agents à intervalles réguliers et/ou lorsqu'un événement réseau se produit.

1. Dans l'onglet **Tâches planifiées** d'un groupe d'agents, rendez-vous dans la section **Tâches planifiées** et cliquez sur **Ajouter une tâche planifiée**.
2. Dans la fenêtre **Exécuter un script personnalisé**, saisissez un nom pour la tâche.

a. À droite du champ **Script**, cliquez sur + pour ajouter le script à exécuter.

b. Dans le champ **Arguments**, spécifiez les arguments à ajouter lors de l'exécution du script.

c. Dans la liste **Contexte d'exécution**, privilégiez **Service local** car il s'agit d'un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

4. Dans la zone **Déclencheurs**, choisissez un ou plusieurs événements qui déclencheront l'exécution du script :
   - Activez l'option **Récurrent toutes les** pour lancer le script à un intervalle régulier que vous spécifiez.
   - Activez l'option **Événement réseau** pour lancer le script quand le poste de travail change d'interface réseau, par exemple s'il se connecte à un réseau wi-fi, si un portable est branché sur une station d'accueil, etc.
5. Cliquez sur **Valider**.

Tous les scripts déclarés dans SES Evolution s'affichent dans la liste **Script**. Sélectionnez un script existant, et cliquez sur le bouton  pour le visualiser, ou sur  pour importer une nouvelle version du script.

7.1.5 Créer des analyses Yara planifiées

Les analyses planifiées permettent d'exécuter automatiquement des analyses Yara sur les postes des utilisateurs à intervalles réguliers. Pour plus d'informations, reportez-vous à la section Réaliser des analyses Yara.

Pour planifier des analyses, vous devez avoir créé au préalable des unités d'analyse. Pour plus d'informations, reportez-vous à la section Créer des unités d'analyse Yara .

1. Dans l'onglet **Tâches planifiées** d'un groupe d'agents, rendez-vous dans la section **Analyses planifiées** et cliquez sur **Programmer une analyse planifiée > Programmer une analyse planifiée Yara**.
2. Dans la fenêtre **Programmer une analyse**, saisissez un nom pour l'analyse.
3. Cliquez sur **Ajouter des unités d'analyse** et sélectionnez les unités d'analyse que vous souhaitez inclure dans votre analyse Yara. Cliquez sur **Suivant**.
4. Cliquez sur Paramètres des logs pour déterminer le niveau de gravité et la destination des logs SES Evolution émis lors de l'analyse Yara.
5. Dans la zone **Paramètres de l'analyse de fichiers**, choisissez **Analyse par défaut** pour exécuter une analyse récursive du dossier *\\.\EsaRoots\SystemDrive* et exclure les dossiers *\\.\EsaRoots\SystemRoot*, *\\.\EsaRoots\ProgramFiles* et *\\.\EsaRoots\ProgramFilesX86*, sinon choisissez **Analyse personnalisée** :
   - **Analyser le fichier image des processus en cours d'exécution** : Vérifie si le fichier *.exe* des processus contient le schéma Yara recherché. Permet également d'arrêter sur les agents les processus malveillants identifiés lors de l'analyse Yara et/ou d'exclure de l'analyse les processus exécutés par les comptes Windows Administrateur et/ou Système.
   - **Extensions de fichiers** : Limite l'analyse aux types d'extensions indiqués.
   - **Fichiers et dossiers inclus** : Exécute l'analyse sur les fichiers et dossiers indiqués avec ou sans récursivité.
   - **Fichiers et dossiers exclus** : Exclut de l'analyse les fichiers et dossiers indiqués avec ou sans récursivité. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.

6. Dans la zone **Paramètres de l'analyse de processus**, choisissez **Analyse par défaut** pour exécuter une analyse de la mémoire de tous les processus en cours d'exécution sur le poste de travail, sinon choisissez **Analyse personnalisée** :
   - **Interrompre le processus détecté** : Arrête les processus malveillants identifiés lors de l'analyse Yara.
   - **Exclure les processus exécutés par** : Exclut de l'analyse les processus exécutés avec les niveaux d'intégrité indiqués (Administrateur et/ou Système).
   - **Répertoire des processus exclus** : Exclut de l'analyse les processus dont les exécutables se trouvent dans les répertoires indiqués. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
     Vous pouvez également exporter les paramètres d'analyse au format JSON et les réimporter pour d'autres tâches.
7. Remplissez ensuite les informations de planification :
   - Période pendant laquelle l'analyse planifiée sera active,
   - Fréquence à laquelle l'analyse planifiée sera exécutée,
   - Heure de démarrage de l'analyse. Si l'agent est arrêté à l'heure indiquée, l'analyse s'effectuera dès que possible à son redémarrage
8. Vous pouvez également importer tous les paramètres d'une analyse planifiée qui a été préalablement exportée au format JSON.
9. Cliquez sur **OK**.
10. Pour déployer l'analyse planifiée sur tous les agents du groupe afin qu'ils l'appliquent, choisissez le menu **Sécurité** > **Déploiement** et cliquez sur le bouton **Déployer**.
11. Consultez les logs de l'agent pour vérifier que les analyses se sont bien effectuées. Vous pouvez aussi Consulter l'utilisation des analyses Yara.

7.1.6 Créer des analyses IoC planifiées

Les analyses planifiées permettent d'exécuter automatiquement des analyses IoC sur les postes des utilisateurs à intervalles réguliers. Pour plus d'informations, reportez-vous à la section Rechercher des indicateurs de compromission .

Pour planifier des analyses, vous devez avoir créé au préalable des unités d'analyse. Pour plus d'informations, reportez-vous à la section Créer des unités d'analyse IoC.

1. Dans l'onglet **Tâches planifiées** d'un groupe d'agents, rendez-vous dans la section **Analyses planifiées** et cliquez sur **Programmer une analyse planifiée** > **Programmer une analyse planifiée IoC**.
2. Dans la fenêtre **Programmer une analyse**, saisissez un nom pour l'analyse.
3. Cliquez sur **Ajouter des unités d'analyse** et sélectionnez les unités d'analyse que vous souhaitez inclure dans votre analyse IoC. Cliquez sur **Suivant**.
4. Cliquez sur Paramètres des logs pour déterminer le niveau de gravité et la destination des logs SES Evolution émis lors de l'analyse IoC.
   L'affichage des zones suivantes dépend du type des indicateurs dans les unités d'analyse sélectionnées à l'étape précédente.
5. Pour les indicateurs de type Texte, vous pouvez désactiver l'analyse IoC dans les fichiers, dans les processus ou bien dans les journaux d'événements en décochant les cases **Recherche textuelle**.

6. Dans la zone **Paramètres de l'analyse de fichiers**, choisissez **Analyse par défaut** pour exécuter une analyse récursive du dossier *\\.\EsaRoots\SystemDrive* et exclure les dossiers *\\.\EsaRoots\SystemRoot*, *\\.\EsaRoots\ProgramFiles* et *\\.\EsaRoots\ProgramFilesX86*, sinon choisissez **Analyse personnalisée** :
   - **Analyser le fichier image des processus en cours d'exécution** : Vérifie si le fichier *.exe* des processus contient les indicateurs recherchés. Permet également d'arrêter sur les agents les processus malveillants identifiés lors de l'analyse IoC et/ou d'exclure de l'analyse les processus exécutés par les comptes Windows Administrateur et/ou Système.
   - **Extensions de fichiers** : Limite l'analyse aux types d'extensions indiqués.
   - **Fichiers et dossiers inclus** : Exécute l'analyse sur les fichiers et dossiers indiqués avec ou sans récursivité.
   - **Fichiers et dossiers exclus** : Exclut de l'analyse les fichiers et dossiers indiqués avec ou sans récursivité. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
7. Dans la zone **Paramètres de l'analyse de processus**, choisissez **Analyse par défaut** pour exécuter une analyse de la mémoire de tous les processus en cours d'exécution sur le poste de travail, sinon choisissez **Analyse personnalisée** :
   - **Interrompre le processus détecté** : Arrête les processus malveillants identifiés lors de l'analyse IoC.
   - **Exclure les processus exécutés par** : Exclut de l'analyse les processus exécutés avec les niveaux d'intégrité indiqués (Administrateur et/ou Système).
   - **Répertoire des processus exclus** : Exclut de l'analyse les processus dont les exécutables se trouvent dans les répertoires indiqués. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
8. Dans la zone **Journaux d'événements**, sélectionnez les types de journaux à analyser et leur ancienneté.
9. Dans la zone **Paramètre de requête DNS**, indiquez l'ancienneté des requêtes DNS à analyser.
10. Remplissez ensuite les informations de planification :
    - Période pendant laquelle l'analyse planifiée sera active,
    - Fréquence à laquelle l'analyse planifiée sera exécutée,
    - Heure de démarrage de l'analyse. Si l'agent est arrêté à l'heure indiquée, l'analyse s'effectuera dès que possible à son redémarrage
11. Vous pouvez également importer tous les paramètres d'une analyse planifiée qui a été préalablement exportée au format JSON.
12. Cliquez sur **OK**.
13. Pour déployer l'analyse planifiée sur tous les agents du groupe afin qu'ils l'appliquent, choisissez le menu **Sécurité** > **Déploiement** et cliquez sur le bouton **Déployer**.
14. Consultez les logs de l'agent pour vérifier que les analyses se sont bien effectuées. Vous pouvez aussi Consulter l'utilisation des analyses IoC.

7.1.7 Comprendre l'autoprotection des agents et réaliser des opérations de maintenance

Les agents SES Evolution possèdent un mécanisme d'autoprotection, mis en œuvre par un ensemble de règles transparentes pour les administrateurs et utilisateurs. Ces règles permettent :

- de garantir que les politiques de sécurité appliquées par les administrateurs n'entravent pas le bon fonctionnement des agents (sans pour autant empêcher que les politiques n'entravent le fonctionnement des postes de travail en cas de règles erronées),
- de protéger les agents des attaques externes ou des utilisateurs malveillants qui pourraient tenter de désactiver ou désinstaller les agents.

Or, pour effectuer des opérations de maintenance sur les agents d'un groupe, vous devez auparavant les basculer en mode Maintenance pour désactiver le système d'autoprotection. Pour cela, vous devez autoriser l'utilisation du mode Maintenance dans la configuration du groupe.

Les droits d'administration sont nécessaires pour activer le mode Maintenance.

Toutes les opérations de maintenance réalisées pendant que le mode Maintenance est actif sont journalisées.

Pendant l'activation du mode Maintenance, les mises à jour automatiques de l'agent sont suspendues. Elles seront appliquées automatiquement lorsque le mode Maintenance prendra fin. Vous pouvez également leur appliquer une mise à jour forcée. Pour plus d'informations, reportez-vous à la section Effectuer une mise à jour forcée d'un agent.

ATTENTION
Lorsque le mode Maintenance est activé, le poste de travail reste protégé par l'agent car la politique de sécurité reste active. Cependant, ce mode doit être utilisé avec précaution et par des personnes de confiance.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Maintenance**.
2. Activez le paramètre **Autoriser le mode Maintenance**.
3. Déployez la configuration sur l'environnement pour appliquer le changement de configuration.

De son côté, l'utilisateur doit activer le mode Maintenance dans l'interface de l'agent, dans l'onglet **Assistance** du panneau **Aide et Support**  . Pour plus d'informations, reportez-vous à la section Configurer les préférences de l'agent.

Lorsque les opérations de maintenance sont terminées, il est important de bien mettre fin au mode Maintenance en cliquant sur le bouton **Désactiver** de l'interface de l'agent afin de rétablir l'autoprotection et la sécurité. Une vérification de l'intégrité des ressources de l'agent est alors opérée. Si une anomalie est détectée, l'agent lance une réparation. Un redémarrage du poste de travail peut alors être demandé à l'utilisateur.

Vous avez également la possibilité d'activer et de désactiver le mode Maintenance via un script, en lançant le programme EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) avec les options de ligne de commande `/EnterMaintenanceMode` et `/LeaveMaintenanceMode`.

La désactivation du mode Maintenance ne requiert pas les droits d'administration.

Vous pouvez également activer le mode Maintenance de façon unitaire sur le poste de travail concerné, grâce aux challenges. Les droits d'administration ne sont alors pas nécessaires. Pour plus d'informations, reportez-vous à la section Résoudre les problèmes avec les challenges.

7.1.8 Autoriser les administrateurs à désinstaller les agents

Par défaut, la seule solution pour désinstaller un agent SES Evolution d'un poste utilisateur est via un challenge. Pour plus d'informations, reportez-vous à la section Désinstaller un agent.

Néanmoins, vous pouvez configurer un groupe d'agents de façon à ce qu'un administrateur du poste de travail soit autorisé à désinstaller l'agent SES Evolution sans challenge.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Désinstallation**.
2. Activez le paramètre **Autoriser la désinstallation** et cliquez sur **Enregistrer**.
3. Déployez la configuration sur l'environnement pour appliquer le changement de configuration.

7.1.9 Collecter les données de diagnostic

Par défaut, la seule solution pour collecter des données de diagnostic sur un poste utilisateur qui présente un problème est le challenge. Pour plus d'informations, reportez-vous à la section Lancer un diagnostic.

Néanmoins, vous pouvez configurer un groupe d'agents de façon à ce qu'un administrateur du poste de travail soit autorisé à démarrer un diagnostic sans challenge.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Collecte des données de diagnostic**.
2. Activez le paramètre **Autoriser la collecte de données de diagnostic** et cliquez sur **Enregistrer**.
3. Déployez la configuration sur l'environnement pour appliquer le changement de configuration.

Pour en savoir plus sur les diagnostics, reportez-vous à la section Établir un diagnostic.

7.1.10 Choisir les paramètres de mise à jour des agents

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Version**.
2. Dans **Version**, choisissez la version de l'agent à appliquer à ce groupe d'agents.
3. Activez l'option **Autoriser le retour à une version antérieure** pour permettre des mises à jour vers des versions antérieures de l'agent.
   Cette option est particulièrement utile si vous constatez un problème de fonctionnement avec une version de l'agent. Elle vous permet de revenir à une version antérieure sur laquelle le problème n'apparaît pas.
4. Désactivez l'option **Appliquer automatiquement les mises à jour logicielles** pour que les gestionnaires d'agents n'appliquent pas les mises à jour lors d'un nouveau déploiement sur le parc d'agents. Dans ce cas, seules les modifications de configuration ou de politiques de sécurité sont déployées, si elles sont compatibles avec la version des agents en cours.

Pour plus d'informations, reportez-vous à la section Mettre à jour les agents, notamment pour connaître les autres modes de mise à jour des agents si vous avez désactivé la deuxième option.

7.1.11 Choisir les fonctionnalités à activer sur les agents

Pour des questions d'incompatibilité ou de doublon avec d'autres logiciels installés, vous pouvez avoir besoin de désactiver une ou plusieurs fonctionnalités de la solution SES Evolution.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Fonctionnalités actives**.

2. Décochez les fonctionnalités que vous souhaitez désactiver.
   Après l'application de la nouvelle configuration, un message sur le tableau de bord des agents du groupe indique que ces derniers doivent être redémarrés.

L'interface des agents affiche la liste des fonctionnalités, et leur état, dans l'onglet **Protections** du panneau **Aide et support**. Pour plus d'informations, reportez-vous à la section Obtenir de l'aide sur l'agent.

7.1.12 Choisir les groupes de gestionnaires d'agents attribués aux agents

Vous pouvez choisir les gestionnaires d'agents auxquels les agents d'un groupe doivent se connecter pour envoyer leurs informations et récupérer les différentes mises à jour. Si votre infrastructure s'étend sur plusieurs sites géographiques, il peut être intéressant de répartir les groupes d'agents sur les gestionnaires d'agents les plus proches.

Les agents qui ne sont associés à aucun gestionnaire d'agents sont appelés agents autonomes. Vous devez effectuer toutes leurs mises à jour manuellement en générant un installeur et en l'exécutant sur les agents, comme lors de leur déploiement initial. Pour plus d'informations, reportez-vous à la section Installer les agents sur les postes de travail.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Gestionnaires d'agents**.
2. Dans **Groupe de gestionnaires d'agents par défaut**, ajoutez le ou les groupes de gestionnaires d'agents auxquels doivent se connecter les agents de ce groupe d'agents.
3. Dans **Groupe de gestionnaires d'agents de secours**, ajoutez le ou les groupes de gestionnaires d'agents auxquels peuvent se connecter les agents en cas de défaillance des groupes par défaut.

7.1.13 Afficher des informations de Support technique sur les agents

Vous pouvez personnaliser les informations affichées dans l'onglet **Aide et Support** > **Contact** de l'interface de l'agent.

1. Dans l'onglet **Paramètres** d'un groupe d'agents, rendez-vous dans la section **Aide et Support**.
2. Choisissez la description que vous souhaitez voir apparaître dans l'en-tête de l'onglet **Contact** du panneau **Aide et Support** de l'interface de l'agent, par exemple "*En cas de problème avec SES Evolution, n'hésitez pas à solliciter le service IT*".
3. Entrez l'**Adresse e-mail**, le numéro de **Téléphone** et le **Site Web** du service en charge du support technique pour SES Evolution.

7.1.14 Surveiller les agents en temps réel

Dans le tableau de l'onglet **Agents** des agents, vous pouvez différencier les agents connectés, des agents déconnectés. Les agents déconnectés sont grisés.

Tout agent est considéré comme déconnecté s'il ne s'est pas connecté à un gestionnaire d'agents depuis une durée définie dans la configuration des groupes d'agents.

Vous pouvez choisir la fréquence de connexion des agents au gestionnaire d'agents pour que leur état se mette à jour. Vous pouvez également personnaliser la durée avant la déconnexion de l'agent ainsi que la durée de déconnexion après laquelle un agent sera automatiquement supprimé de la base de données. Pour plus d'informations, reportez-vous à la section Supprimer automatiquement les agents déconnectés

Pour définir la fréquence de connexion et ces différentes durées :

1. Dans l'onglet **État et logs** d'un groupe d'agents, rendez-vous dans la section **Surveillance des agents en temps réel**.
2. Choisissez la fréquence en secondes de **Mise à jour de l'état de l'agent**. Par défaut, l'agent se connecte automatiquement au gestionnaire d'agents toutes les 60 secondes pour :
   - Envoyer les informations sur son état afin d'actualiser le panneau des groupes d'agents,
   - Récupérer les nouvelles configurations, politiques ou mises à jour si elles sont disponibles.

   Vous pouvez aussi manuellement forcer une connexion au gestionnaire d'agents et l'envoi des logs en cliquant sur le bouton **Vérifier la présence de mises à jour** dans le panneau **État** des protections de l'interface de l'agent.
3. Définissez une valeur pour le paramètre **Déconnexion après**. Par défaut, un agent est considéré comme déconnecté s'il ne s'est pas connecté pendant sept jours consécutifs à son gestionnaire d'agents.
4. Définissez une valeur pour le paramètre **Suppression automatique après**. Par défaut, un agent est supprimé après 30 jours consécutifs de déconnexion.

7.1.15 Configurer la transmission des logs émis par les agents

1. Dans l'onglet **État et logs** d'un groupe d'agents, rendez-vous dans la section **Logs**.
2. Choisissez à partir de quel niveau de gravité les logs seront transmis vers les destinations suivantes :
   - **Afficher sur l'agent** dans le panneau **Aide et Support**, onglet **Événements** de l'interface de l'agent,
   - **Afficher sur la console** dans le panneau **Environnement > Logs agents** de la console d'administration, c'est-à-dire stockés dans la base de données de logs.

   Par exemple, si vous choisissez le niveau *Information* pour l'agent, alors tous les logs seront visibles dans l'interface de l'agent, sauf les logs de niveau *Diagnostic*.
   Les logs de niveau *Urgence* et *Alerte* sont systématiquement transmis vers toutes les destinations. Les logs non transmis ne seront jamais consultables.
   Attention, seuls les logs de niveau *Alerte* et *Urgence* ayant entraîné un blocage sont visibles dans l'interface de l'agent pour un utilisateur non administrateur de sa machine.
   Si vous validez un nouveau logiciel, un nouveau poste de travail etc., transmettez temporairement les logs de niveau *Information*. En cas de maintenance ou dépannage, les logs de niveau *Diagnostic* vous seront aussi utiles.
   Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
   Vous pouvez affiner ce comportement global et définir pour chaque règle de sécurité les logs à transmettre. Pour plus d'informations, reportez-vous à la section Configurer la gestion des logs.
   Pour configurer l'envoi des logs vers des serveurs Syslog, reportez-vous à la section Créer des groupes de gestionnaires d'agents.
3. Dans la section **Fréquence de transmission des logs**, choisissez la fréquence maximale en secondes à laquelle les logs de l'agent sont envoyés au gestionnaire d'agents :
   - Les **Logs urgents** correspondent aux logs de niveau *Urgence* et *Alerte*.
   - Les **Logs standard** regroupent tous les autres niveaux.

   Ce paramètre vous permet de gérer l'utilisation de la bande passante. Par défaut, les logs urgents sont envoyés toutes les 30 secondes et les logs standard toutes les heures (3600 secondes).

4. Par défaut, les logs affichés sur un agent sont supprimés de son disque selon les critères suivants :
   - La taille des fichiers de logs dépasse 500 Mo. Dans ce cas, les logs les plus anciens sont supprimés pour revenir en dessous de 500 Mo.
   - Les logs ont dépassé 30 jours d'existence.
     Vous pouvez modifier ce délai dans le champ **Conserver les logs de moins de**. Si vous désactivez complètement l'option, seul le critère de taille des fichiers de logs s'applique.
5. Choisissez si vous souhaitez **Envoyer les logs d'autoprotection** des agents au gestionnaire d'agent. Il s'agit des logs des mécanismes qui protègent les composants indispensables à l'intégrité de l'agent. Si ce paramètre est désactivé, les logs d'autoprotection restent disponibles sur les agents.

7.1.16 Configurer les détails de contextes émis par les agents

Les détails de contextes sont tous les logs produits par l'agent dans le périmètre d'une attaque, y compris ceux qui n'apparaissent pas sur la console d'administration habituellement. Par exemple même les logs restés en local sur l'agent ou envoyés vers un serveur Syslog sont affichés dans les détails de contextes. Pour plus d'informations, reportez-vous à la section Analyser les contextes pour comprendre une attaque.

Vous pouvez configurer la taille de ces contextes, l'ancienneté maximale de leurs logs, ainsi que la manière dont ils sont envoyés au gestionnaire d'agents.

1. Dans l'onglet **État et logs** d'un groupe d'agents, rendez-vous dans la section **Contextes**.
2. Définissez la **Taille maximale** d'un contexte qui est de 500 Ko par défaut. Il s'agit de la taille estimée des données qui transitent sur le réseau. Si les connexions réseau entre les agents et le gestionnaire d'agents sont limitées, réduisez cette taille. À l'inverse, si vous avez ajouté des jeux de règles d'audit très verbeuses, augmentez cette taille pour être sûr de récupérer suffisamment de logs utiles.
3. Définissez l'**Ancienneté maximale des logs**. La valeur par défaut est de 10 minutes car la plupart des attaques se déroulent rapidement, mais vous pouvez l'ajuster à votre convenance.
4. Choisissez la manière dont s'effectue la **Remontée des détails de contexte** de l'agent au gestionnaire d'agents. La remontée peut être :
   - **Immédiate** : Les logs de contexte sont envoyés au gestionnaire d'agents en même temps que l'alerte. Ils sont visibles immédiatement dans la console d'administration.
   - **Différée** : Les logs de contexte sont envoyés au gestionnaire d'agents à une **Fréquence** que vous pouvez définir, la valeur par défaut étant toutes les heures. Si vous n'analysez les attaques qu'une fois par jour, augmentez cette fréquence à deux ou trois heures pour éviter d'encombrer le réseau.
   - **Sur demande** : Les logs de contexte ne seront pas transmis au gestionnaire d'agents de manière automatique. Vous pourrez télécharger ces données manuellement au moment d'étudier une attaque. Pour plus d'informations, reportez-vous à la section Analyser les contextes pour comprendre une attaque.
5. Enregistrez vos modifications.

7.2 Installer les agents sur les postes de travail

Une fois les groupes d'agents configurés à votre convenance, vous devez installer les agents sur les postes de travail à protéger.

Un agent SES Evolution peut être installé sur tous les types de machines dont le système d'exploitation est compatible : serveurs ou postes de travail, y compris sur un contrôleur de domaine ou sur une machine hébergeant un ou plusieurs composants SES Evolution (e.g., gestionnaire d'agents, backend, etc.)

Cette installation s'effectue en deux étapes. Générez d'abord un installeur contenant toute la configuration propre au groupe d'agents. Déployez ensuite l'agent sur chaque poste de travail devant appartenir à ce groupe. Une fois installé, l'agent récupère une identité unique lors de sa première connexion au gestionnaire d'agents. Il s'affiche ensuite dans le panneau du groupe d'agents correspondant dans la console d'administration. Toute la configuration du groupe d'agents lui est appliquée, en particulier les politiques de sécurité.

Si vous avez installé SES Evolution sur un master, vous devez en plus modifier l'identifiant des agents sur lequel vous le déployez. Pour plus d'informations, reportez-vous à la sectionInstaller l'agent sur des postes de travail issus d'un master

NOTE
Le répertoire pointé par %TEMP% et %TMP% doit exister et être accessible en écriture pendant la phase d'installation de l'agent et lors de la mise à jour de l'agent.

7.2.1 Prérequis système pour les agents

Pour installer et utiliser Stormshield Endpoint Security Evolution version 2.6.3 sous Microsoft Windows, les agents doivent disposer au minimum des prérequis ci-dessous :

Systèmes d'exploitation	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.
Processeurs pour machines physiques	Processeurs 64 bits avec au minimum 2 GHz Intel Pentium 4 ou équivalent. Les processeurs Itanium ne sont pas supportés.
Processeurs pour machines virtuelles	Au minimum une socket virtuelle et un cœur de 1 GHz par socket. Stormshield recommande une socket virtuelle et deux cœurs de 2 GHz par socket.
Mémoire physique	Au minimum 1 Go. Davantage si le système d'exploitation le nécessite. Stormshield recommande 2 Go.
Espace disque	• Au minimum 100 Mo pour l'installation, • Au minimum 200 Mo pour le stockage des données. Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS. De l'espace supplémentaire est aussi nécessaire pour les mises à jour et les logs.
Configuration réseau	• Communications sortantes : ◦ TCP 17000 (RPC)
Bande passante réseau	Au minimum 12 Kbit/s. Une bande passante plus faible peut empêcher les échanges entre l'agent et le gestionnaire d'agents.
Logiciel	Framework .NET 4.6.2 ou supérieur.
Affichage	Au minimum 1024X768.

Certificat	Présence du certificat *VeriSign Universal Root Certification Authority* pour vérifier l'authenticité des mises à jour SES Evolution. Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie. Vous pouvez le télécharger directement sur votre espace client MyStormshield, dans la section **Téléchargements** > **Stormshield Endpoint Security** > **Evolution** > **Resources**. Dans l'archive, le fichier *.bat* permet d'installer automatiquement le certificat dans le magasin de certificats avec un compte administrateur.

Activer les points de restauration Windows

L'installeur de l'agent SES Evolution crée un point de restauration Windows juste avant de copier les fichiers sur le disque. En cas de problème ou d'incompatibilité avec un autre logiciel, cela permet de revenir à l'état du système tel qu'il était avant l'installation de SES Evolution. La mise à jour de l'agent crée également un point de restauration.

Pour que le point de restauration soit créé, la fonctionnalité doit être activée dans le panneau **Système > Protection du système** de Windows. Pour plus d'informations sur la restauration, reportez-vous à la documentation Windows.

Désactiver le mode sans échecs pour les utilisateurs standard

Le mode sans échec permet de diagnostiquer des problèmes qui empêchent d'utiliser un poste de travail lorsqu'il est démarré normalement. Par défaut la configuration Windows permet à tous les utilisateurs de démarrer leur poste avec ce mode.

Or, en mode sans échec, l'auto-protection de l'agent SES Evolution est désactivée. Vous devez donc autoriser l'utilisation de ce mode aux seuls administrateurs.

Pour désactiver l'accès au mode sans échec aux utilisateurs non administrateurs, dans la base de registre Windows, positionnez la valeur *SafeModeBlockNonAdmins* de la clé *HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System* à « 1 ».

7.2.2 Générer un installeur pour les agents

Vous devez disposer du droit **Groupes d'agents-Modifier** pour générer un installeur pour les agents.

1. Choisissez le menu **Environnement > Agents**.
2. Assurez-vous d'avoir configuré le groupe d'agents à votre convenance et déployé l'environnement. Pour plus d'informations, reportez-vous à la section Créer et configurer les groupes d'agents.
3. Dans le panneau de gauche, sélectionnez le groupe d'agents que vous souhaitez appliquer aux postes de travail.
4. Dans l'onglet **Agents**, cliquez sur **Installeur > Générer un installeur**.
5. Enregistrez le fichier d'installation *AgentSetup_x64.exe* à l'emplacement de votre choix.

7.2.3 Déployer l'agent sur chaque poste de travail standard via GPO

Une fois l'installeur généré, vous pouvez déployer ce fichier sur les postes de travail via GPO. La procédure par GPO décrite ci-dessous utilise le script powershell *SesAgentDeploymentScript.ps1* fourni par Stormshield et effectue une installation par défaut en mode silencieux.

1. Sur votre espace client Mystormshield, choisissez le menu **Téléchargements > Stormshield Endpoint Security > Evolution > Ressources** et cliquez sur le lien *SES Agent deployment script*. Le script nécessite PowerShell version 5 ou supérieure.
2. Sur le contrôleur de domaine, ouvrez la Console de gestion des stratégies de groupe (*gpmc.msc*).
3. Faites un clic-droit sur l'unité d'organisation où vous souhaitez déployer l'agent SES Evolution, puis choisissez **Créer un objet GPO dans ce domaine, et le lier ici**.
4. Dans la fenêtre **Nouvel objet GPO**, saisissez un nom pour la GPO, par exemple *SES EVOLUTION Deployment*.
5. Faites un clic-droit sur la nouvelle GPO, puis choisissez **Modifier**.
   L'Éditeur de gestion des stratégies de groupe s'ouvre.
6. Choisissez le menu **Configuration ordinateur > Stratégies > Paramètres Windows > Scripts (Démarrage/Arrêt)**, et double cliquez sur **Démarrage**.
7. Dans la fenêtre **Propriétés de démarrage**, cliquez sur l'onglet **Scripts Powershell**, puis sur **Afficher les fichiers** et collez les fichiers suivants :
   - Les fichiers *AgentSetup_x64.exe*,
   - Le script *SesAgentDeploymentScript.ps1*.
8. Cliquez sur **Ajouter**, puis sur **Parcourir**
9. Sélectionnez le script, cliquez sur **Ouvrir**, puis sur **OK**.
10. Dans la fenêtre **Propriétés de démarrage**, cliquez sur **Appliquer** puis **OK**.
11. Dans la Console de gestion des stratégies de groupe, sélectionnez la GPO créée.
12. Dans l'onglet **Étendue**, vérifiez les éléments suivants :
    - L'unité d'organisation dans la section **Liaisons**,
    - Les groupes d'utilisateurs cibles dans la section **Filtrage de sécurité**.
13. Faites un clic droit sur l'OU, puis sélectionnez **Mise à jour de la stratégie de groupe**.
    L'agent SES Evolution s'installe automatiquement en mode silencieux au prochain démarrage des postes de travail.
    Vous pouvez consulter les traces de l'installation par GPO dans le dossier *C:\Windows\Temp\InstallSESLogGPO*.
14. Une fois l'agent installé, l'icône  s'affiche dans la barre d'état de Windows, indiquant que l'installation n'est pas complète.
15. Redémarrez le poste de travail. L'icône  indique que l'agent est désormais complètement fonctionnel.

7.2.4 Déployer l'agent sur chaque poste de travail standard via MECM (ex SCCM)

Une fois l'installeur généré, vous pouvez déployer le fichier sur les postes de travail via l'outil Microsoft Endpoint Configuration Manager, remplaçant de l'outil SCCM.

NOTE
La version 2.3 minimum de SES Evolution et la version 2210a minimum des politiques de sécurité intégrées sont requises pour le déploiement de l'agent via MECM.
Consultez votre espace client MyStormshield pour télécharger les versions les plus à jour de SES Evolution et des politiques. Vous pouvez également télécharger les dernières politiques depuis le serveur de mises à jour. Pour plus d'informations, reportez-vous à la section Télécharger les mises à jour Stormshield.

Dans votre environnement MECM, nous vous recommandons :

- De disposer au minimum d'un dossier partagé, utilisable par les machines du parc connectées à MECM,
- De répartir la liste des machines du parc dans des **Regroupements de périphériques**. Vous pouvez répartir les agents SES Evolution par groupes d'agents par exemple.

La procédure suivante a été testée sur la version 2207 de MECM.

Pour déployer l'agent via l'outil MECM, suivez les quatre étapes ci-dessous :

1	Créer un package d'installation	1. Déposez les fichiers d'installation *AgentSetup_x64.exe* dans le dossier partagé utilisable par les machines du parc connectées à MECM. 2. Ouvrez la console **Configuration Manager**. 3. Dans le menu **Bibliothèque de logiciels** > **Vue d'ensemble** > **Gestion des applications**, cliquez sur **Packages**. 4. Créez un package et un programme. Nommez le package, par exemple : *Install SES Evolution agent*. 5. Sélectionnez le type de programme standard. 6. Nommez le programme, par exemple : *SES Evolution agent on Windows x64*. 7. Entrez la ligne de commande `AgentSetup_x64.exe /s`. D'autres options sont disponibles, consultez la liste des options sous le tableau. 8. Sélectionnez le dossier partagé contenant le fichier d'installation comme dossier de démarrage. 9. Sélectionnez le mode d'exécution **Exécuter avec les droits d'administration**. 10. Sélectionnez le système d'exploitation sur lequel l'agent va être déployé dans **Exigences de plates-formes**.
2	Créer des programmes à installer via le package	Dans le package créé, créez autant de programmes que nécessaire, pour chaque groupe d'agents par exemple. Pour créer un nouveau programme : 1. Faites un clic droit sur le package et sélectionnez **Créer un programme**. 2. Sélectionnez les paramètres comme indiqué à l'étape 1.
3	Déployer les programmes sur les postes de travail	1. Sur chaque programme créé dans le package, faites un clic droit et sélectionnez **Déployer**. 2. Sélectionnez le **Regroupement** sur lequel déployer l'agent. 3. Spécifiez une **Planification** de déploiement. 4. Dans les **Paramètres de notification**, sélectionnez **Autoriser les utilisateurs à exécuter le programme indépendamment des attributions**. 5. Dans les **Options de déploiement**, sélectionnez **Exécuter le programme à partir du point de distribution**.

4	Surveiller et finaliser le déploiement	1. Dans le menu **Surveillance** > **Vue d'ensemble**, cliquez sur **Déploiements**. 2. Sélectionnez un déploiement en cours pour voir son état d'avancement. 3. Vous pouvez sélectionner **Exécuter le résumé** pour forcer la synchronisation entre les postes de travail et MECM. 4. Une fois l'agent installé sur les postes de travail, l'icône  s'affiche dans la barre d'état de Windows, indiquant que l'installation n'est pas complète. 5. Redémarrez les postes de travail. L'icône  indique que l'agent est désormais complètement fonctionnel.

Vous pouvez également ajouter les options suivantes à la commande `AgentSetup_x64.exe` :

`/silent ou /s`	Pour que l'installation soit transparente pour l'utilisateur du poste de travail.
`/installdir`	Pour copier les fichiers d'installation de l'agent (binaires et ressources) dans un répertoire différent de *%SYSTEMDRIVE%\Program Files*. Ce chemin doit être différent de celui des fichiers de données de l'agent.
`/datadir`	Pour copier les fichiers de données de l'agent (logs, politiques, scripts…) dans un répertoire différent de *%SYSTEMDRIVE%\ProgramData*. Ce chemin doit être différent de celui des fichiers d'installation de l'agent.
`/log <chemin>`	Pour spécifier le chemin du fichier de log d'installation de l'agent.
`/newagentid`	Pour supprimer les données de communication de l'agent avec le gestionnaire d'agents : identifiant unique, certificats utilisés en interne, identifiant et données privées pour les challenges. L'agent récupère de nouvelles données à sa prochaine connexion au gestionnaire d'agents. Attribuer de nouvelles données de communication est utile si l'agent se trouve sur une machine virtuelle dupliquée, ou si vous installez l'agent sur un poste de travail issu d'un master.

7.2.5 Installer l'agent sur des postes de travail issus d'un master

1. Installez un agent SES Evolution sur un master via la procédure d'installation d'un agent standard.

2. Sur le master, supprimez l'identifiant de l'agent en utilisant d'une des méthodes ci-dessous. Les gestionnaires d'agents ne doivent pas pouvoir être contactés par l'agent pendant cette opération, sans quoi l'agent obtiendra immédiatement de nouvelles données de communication.
   - Supprimez la valeur registre de l'identifiant de l'agent (valeur : *AgentGuid*) située dans : *HKEY_LOCAL_MACHINE\SOFTWARE\Stormshield\SES Evolution*. Un nouvel identifiant sera généré à la prochaine connexion de l'agent au gestionnaire d'agents.
     - ou -
   - Exécutez l'installeur de l'agent *AgentSetup_x64.exe* ou le composant de l'agent *Agent\bin\Gui\EsSetup.exe* en mode commande avec l'option */newagentid*. Cette commande attribue un nouvel identifiant à l'agent sans effectuer de nouveau l'installation.

   Après déploiement du master sur un poste de travail, l'agent SES Evolution contactera le gestionnaire d'agents, et un nouvel identifiant lui sera attribué.

7.2.6 Utiliser l'agent sur les systèmes d'exploitation Microsoft Windows Server Core

Vous pouvez installer l'agent SES Evolution sur les systèmes d'exploitation Windows Server Core 2012 R2, 2016, 2019 et 2022.

Ces systèmes d'exploitation possèdent une interface graphique réduite. L'interface de l'agent n'est donc pas démarrée automatiquement lors de l'ouverture de session d'un utilisateur (icône  dans la barre des tâches sur un système d'exploitation "classique"). Pour afficher l'interface graphique de l'agent :

- Utilisez la commande `EsGui.exe`.

De même, si une demande de confirmation par l'utilisateur est paramétrée dans une règle de sécurité, l'agent n'affiche pas de fenêtre et considère automatiquement que la réponse à la confirmation est "non". L'utilisateur n'a pas la possibilité de répondre "oui".

7.2.7 Résoudre les problèmes

Failed to extract files from patch (0xa0050005)

Situation : Lors de l'installation d'un agent, cette erreur s'affiche :
Failed to extract files from patch (0xa0050005).

Cause : Le certificat nécessaire à la vérification de l'authenticité de la mise à jour SES Evolution n'est pas présent sur la machine.

Solution : Ajoutez le certificat **VeriSign Universal Root Certification Authority** au magasin de certificats *Autorités de certification racines de confiance* ou *Autorités de certification racines tierce-partie*.

- ou -
Connectez la machine à Internet afin que le certificat soit téléchargé automatiquement.

7.3 Visualiser les agents dans la console

La console d'administration vous permet de suivre en temps réel l'état des agents sur tous les postes de travail. Vous pouvez les classer selon différents critères : système d'exploitation, domaine, version SES Evolution etc.

Vous pouvez aussi filtrer les agents, les déplacer d'un groupe à l'autre et exporter une sélection d'agents au format CSV.

Votre utilisateur doit disposer du droit **Groupes d'agents - Afficher** pour visualiser ce panneau.

7.3.1 Afficher la liste des agents

1. Dans le menu **Environnement > Agents**, sélectionnez **Tous les agents** pour visualiser tous les agents indépendamment de leur groupe.
   - ou -
   Sélectionnez un groupe d'agents dans le panneau de gauche, puis cliquez sur l'onglet **Agents**. Chaque agent déployé via l'installeur du groupe d'agents se connecte au gestionnaire d'agents et s'affiche ensuite dans le tableau avec les informations suivantes :
   - **Ordinateur** : Nom du poste de travail sur lequel est installé l'agent SES Evolution,
   - **Adresse IP** : Adresse IP principale si l'ordinateur a plusieurs cartes réseau,
   - **Version** : Numéro de la version de l'agent SES Evolution,
   - **Système d'exploitation** : Version du système d'exploitation du poste de travail,
   - **Type de machine** : PC fixe, PC portable, Serveur, Machine virtuelle, ou Inconnu,
   - **Politique** : Nom de la politique de sécurité SES Evolution appliquée sur le poste de travail,
   - **Dernière connexion** : Date de la dernière connexion de l'agent SES Evolution au gestionnaire d'agents,
   - **Domaine** : Nom du domaine Windows auquel appartient le poste de travail,
   - **Utilisateur** : Nom du compte Windows qui a effectué la dernière connexion au serveur SES Evolution depuis ce poste de travail.
   - **Groupe** : Nom du groupe d'agents auquel appartient l'agent.
   - **Mode** : Mode de fonctionnement de l'agent SES Evolution, Normal, Arrêté ou Maintenance. Le mode Arrêté signifie que le poste de travail n'est plus protégé par SES Evolution. Pour plus d'informations sur le mode Maintenance, reportez-vous à la section Activer le mode Maintenance.
   - **Épinglé** : L'icône  signifie que l'agent restera dans son groupe d'agents quelles que soient les règles d'affectation Active Directory. Si la colonne est vide, alors l'agent se conforme aux règles Active Directory et il peut être déplacé automatiquement d'un groupe à un autre s'il change de critères Active Directory. Pour plus d'informations, reportez-vous à la section Affecter automatiquement des agents à des groupes d'agents.
2. Cliquez sur un titre de colonne pour classer la liste des agents selon ce critère. Par exemple cliquez sur **Groupe** pour classer les agents selon leur groupe d'agents.

7.3.2 Filtrer la liste des agents

1. Dans la section **Filtres** de l'onglet **Agents**, activez des filtres pour personnaliser votre liste d'agents. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant.
   La liste des agents s'actualise en fonction des filtres activés.
2. À tout moment, vous pouvez retrouver la liste totale des agents en cliquant sur **Effacer les filtres**.

Pour filtrer selon le nom de l'ordinateur, son GUID, la date de dernière connexion ou l'utilisateur, saisissez une chaîne de caractères dans le champ de recherche en haut à droite.

7.3.3 Déplacer des agents d'un groupe à un autre

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez déplacer.
2. Cliquez sur **Déplacer les agents vers > Nom du groupe souhaité**. Le nom de l'agent s'affiche en bleu et en italique dans le groupe de départ et dans le groupe d'arrivée pour indiquer que l'agent est en cours de déplacement.
3. Choisissez le menu **Sécurité** > **Déploiement** et cliquez sur **Déployer** pour appliquer à l'agent la configuration et les politiques de sécurité du nouveau groupe.
   Le nom de l'agent s'affiche de nouveau en noir. Il est supprimé du groupe et appartient désormais au groupe vers lequel il a été déplacé.

Si l'agent a été placé dans son groupe par une règle d'affectation Active Directory et que vous le déplacez manuellement, il sera épinglé dans son nouveau groupe. La règle d'affectation Active Directory ne sera plus appliquée.
Si l'agent était épinglé dans son groupe de départ, il sera épinglé dans son groupe de destination. Pour plus d'informations sur les règles d'affectation Active Directory et l'épinglage, reportez-vous à la section Affecter automatiquement des agents à des groupes d'agents.

7.3.4 Exporter une liste d'agents

Vous pouvez exporter les informations sur les agents au format CSV pour les consulter et les traiter dans un tableur.

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez exporter.
2. Faites un clic droit et choisissez **Exporter les agents sélectionnés**, puis sélectionnez le séparateur souhaité (i.e., virgule, point-virgule ou tabulation). Par défaut un fichier *ExportedAgents.csv* est créé sur le Bureau. Modifiez son nom et sa destination si besoin.
3. Ouvrez le fichier *.csv* avec l'outil de votre choix.

Pour surveiller l'activité sur les agents, vous pouvez visualiser leurs logs. Pour plus d'informations, reportez-vous à la section Visualiser et gérer les logs des agents dans la console d'administration.

7.4 Affecter automatiquement des agents à des groupes d'agents

Vous pouvez affecter automatiquement un agent à un groupe d'agents selon les groupes Active Directory ou unités d'organisation auxquels il appartient.

Si vous utilisez cette fonctionnalité, un agent est automatiquement affecté à un groupe d'agents selon les critères Active Directory dont il dispose au démarrage du poste de travail :

- Si par la suite, l'agent change de groupe Active Directory ou d'unité d'organisation, alors il sera déplacé dans le groupe d'agents correspondant après un redémarrage du poste de travail,
- Si seules les règles d'affectation sont modifiées et déployées depuis la console d'administration, il sera déplacé automatiquement dans le groupe correspondant sans redémarrer.

Pour affecter automatiquement les agents, vous devez créer des règles d'affectation basées soit sur les groupes Active Directory, soit sur les unités d'organisation (OU). La vérification se fait sur les critères Active Directory de la machine et non pas celles de l'utilisateur connecté.

Si vous souhaitez que des agents conservent leur appartenance à un groupe d'agents quels que soient leurs critères Active Directory, vous pouvez les épingler manuellement à ce groupe.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour créer des règles d'affectation.

7.4.1 Créer une règle d'affectation à un groupe d'agents

1. Dans le menu **Environnement > Agents**, sélectionnez **Tous les agents** puis l'onglet **Règles d'affectation**.
2. Cliquez sur **Modifier** en haut à droite.
3. Cliquez sur **Ajouter une règle par groupe AD** ou **Ajouter une règle par OU** au choix.
   Une nouvelle ligne s'affiche.
4. Entrez une **Description** permettant de reconnaître facilement la règle.
5. Cliquez sur  et sélectionnez le groupe ou l'OU souhaité dans la fenêtre qui s'affiche.
   Vous pouvez aussi entrer manuellement le groupe ou l'unité d'organisation en utilisant la syntaxe LDAP, e.g. *OU=Paris,DC=Grey,DC=local*.
6. Dans la liste **Affecter au groupe d'agents**, choisissez le groupe d'agents auquel les postes de travail de ce groupe ou OU appartiendront.
7. Créez d'autres règles si nécessaire.
8. Modifiez l'ordre des règles en les survolant avec la souris pour afficher les flèches à gauche.
   S'il existe plusieurs règles correspondant aux critères AD d'un agent, celui-ci sera affecté au groupe d'agents de la première règle rencontrée.
9. Cliquez sur **Enregistrer**.

   L'icône du groupe d'agent dans le panneau de gauche change  , montrant qu'au moins un règle d'affectation Active Directory concerne le groupe.
   Dans l'onglet **Agents** des groupes d'agents concernés, le nom des règles d'affectation s'affiche sous forme de liens qui permettent de consulter directement les règles.
10. Choisissez le menu **Sécurité** > **Déploiement** et cliquez sur **Déployer**.
    Un agent sera affecté à son groupe selon ses critères AD lorsque l'agent aura récupéré la nouvelle configuration puis renvoyé au gestionnaire d'agents ses critères AD. Un redémarrage peut être nécessaire si les modifications ont été réalisées sur le contrôleur Active Directory durant la session de l'utilisateur.

7.4.2 Épingler un agent à un groupe d'agents pour ignorer ses critères Active Directory

Épinglez manuellement un agent à un groupe d'agents si vous souhaitez qu'il conserve son groupe quels que soient ses critères Active Directory.

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez épingler.
2. Cliquez sur **Épingler ou détacher les agents > Épingler à un groupe**.

   L'icône  apparaît dans la colonne **Épinglé**. L'agent restera toujours dans ce groupe d'agents quoi qu'il en soit, même si ses critères Active Directory changent. Il ne pourra changer de groupe que si vous le déplacez manuellement ou si vous le détachez du groupe.
3. Choisissez le menu **Sécurité** > **Déploiement** et cliquez sur **Déployer**.

7.4.3 Détacher un agent d'un groupe d'agents

Détachez un agent d'un groupe d'agents si vous souhaitez qu'il soit de nouveau affecté à un groupe d'agents automatiquement selon ses critères Active Directory.

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez détacher du groupe.
2. Cliquez sur **Épingler ou détacher les agents** > **Détacher d'un groupe**.

   L'icône  disparaît de la colonne **Épinglé**. L'agent pourra désormais changer de groupe automatiquement s'il est concerné par une règle d'affectation Active Directory.
3. Choisissez le menu **Sécurité** > **Déploiement** et cliquez sur **Déployer**.

7.5 Comprendre l'interface de l'agent sur les postes de travail

Les agents disposent d'une interface affichant des informations sur l'état de santé de l'agent et permettant d'établir un diagnostic en cas de problème, grâce à la lecture des journaux d'événements.

Des outils d'assistance et de diagnostic, ainsi qu'un suivi des fichiers en quarantaine sont également disponibles.

- Pour ouvrir l'interface de l'agent SES Evolution, double-cliquez sur l'icône  dans la barre des tâches des postes de travail.

7.5.1 Consulter l'état de santé de l'agent

Le tableau de bord **État des protections** de l'agent affiche le fonctionnement des quatre principaux modules de protection de l'agent selon le code couleur suivant :

- Vert : Tous les modules sont fonctionnels,
- Orange : Une protection dans un module est arrêtée ou en attente de redémarrage,
- Rouge : Un module ne fonctionne pas,
- Gris : Une protection dans un module a été désactivée dans la configuration du groupe d'agents.

Cliquez sur les noms des modules ou sur le bouclier pour accéder au détail de l'état des protections. L'onglet **Protections** dans le panneau **Aide et Support** s'affiche. Il présente l'état des modules et de leurs protections. Cette liste de protections correspond aux fonctionnalités que vous pouvez activer ou désactiver dans la configuration de l'agent dans la console d'administration. Pour plus d'informations, reportez-vous à la section Choisir les fonctionnalités à activer sur les agents.

La zone du milieu affiche les trois derniers événements de niveau *Alerte* ou *Urgence*, ayant entraîné un blocage, qui ont été émis sur l'agent. Les événements identiques sont regroupés.

La zone inférieure du tableau de bord fournit des informations sur la configuration SES Evolution :

- **Groupe d'agents** : Nom du groupe d'agents auquel appartient cet agent,
- **Politique de sécurité** : Nom de la politique de sécurité appliquée sur cet agent,
- **Dernière mise à jour de la politique** : Date à laquelle cet agent a mis à jour sa politique de sécurité pour la dernière fois,
- **Dernière connexion** : Date à laquelle cet agent s'est connecté au gestionnaire d'agents pour la dernière fois.

Par défaut, l'agent se connecte automatiquement au gestionnaire d'agents à une fréquence que vous pouvez paramétrer. Cliquez sur le bouton **Vérifier la présence de mises à jour** pour forcer la connexion au gestionnaire d'agents et ainsi effectuer les opérations suivantes :

- Envoyer au gestionnaire d'agents les informations sur l'état de l'agent, y compris les logs,
- Récupérer les nouvelles configurations, politiques ou mises à jour si elles sont disponibles.

Vous avez également la possibilité de forcer la connexion au gestionnaire d'agents via un script, en lançant le programme EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) avec l'option de ligne de commande `/ForceConnection`.

7.5.2 Configurer les préférences de l'agent

1. Dans l'interface de l'agent, cliquez sur l'onglet  pour ouvrir le panneau **Préférences**.
2. Positionnez les options à votre convenance. Vous pouvez :
   - Choisir la langue de l'interface de l'agent,
   - Sauvegarder la position et la taille de la fenêtre de l'interface de l'agent,
   - Afficher les notifications par info-bulles.

7.5.3 Obtenir de l'aide sur l'agent

- Dans l'interface de l'agent, cliquez sur l'onglet  pour ouvrir le panneau **Aide et Support**.

Visualiser les informations de l'agent

Dans l'onglet **Contact**, retrouvez les informations suivantes :

- **Contact du support** : Coordonnées du service à contacter en cas de problèmes avec l'agent SES Evolution. Ces informations ne sont affichées que si vous les avez paramétrées dans la configuration du groupe d'agents. Pour plus d'informations, reportez-vous à la section Afficher des informations de Support technique sur les agents.
- **Informations** : Détails liés à l'agent installé sur ce poste de travail.

Demander une assistance

Dans l'onglet **Assistance**, vous pouvez effectuer les trois actions suivantes :

- Demander un challenge à votre administrateur. Pour plus d'informations, reportez-vous à la section Résoudre les problèmes avec les challenges.
- Activer le mode maintenance si vous avez besoin de désactiver l'autoprotection de l'agent pour effectuer des opérations de maintenance. Vous devez disposer des droits d'administration. Pour plus d'informations, reportez-vous à la section Comprendre l'autoprotection des agents et réaliser des opérations de maintenance.

ATTENTION
Si vous activez le mode Maintenance, il est important de bien y mettre un terme lorsque les opérations de maintenance sont terminées en cliquant sur le bouton **Désactiver** de l'interface de l'agent. Ceci permet de rétablir l'autoprotection et la sécurité du poste. De plus, lorsque le mode Maintenance est activé, les mises à jour automatiques de l'agent sont suspendues.

- Exporter les logs qui n'ont pas encore été transmis au gestionnaire d'agents parce que l'agent est déconnecté du réseau par exemple.

Établir un diagnostic

Pour établir un diagnostic, reportez-vous à la section Diagnostiquer les problèmes sur les agents.

Consulter les journaux d'événements

Consultez les logs d'un agent dans l'onglet **Événements** de l'interface de l'agent. Pour plus d'informations, reportez-vous à la section Visualiser les logs sur l'interface des agents.

Seuls les logs de niveau *Alerte* et *Urgence* ayant entraîné un blocage s'affichent sur l'agent d'un utilisateur non administrateur.

Un utilisateur administrateur peut voir tous les niveaux de logs, bloquants ou non, selon les niveaux configurés dans les règles de sécurité pour être envoyés vers l'agent. Pour plus d'informations, reportez-vous à la section Configurer la gestion des logs.

Les logs similaires sont regroupés dans l'interface de l'agent d'un utilisateur non administrateur.

Les logs des agents sont aussi consultables sur la console d'administration et sur le serveur Syslog si vous l'avez configuré.

Suivre les fichiers en quarantaine

Le tableau de bord de l'agent indique le nombre de fichiers en quarantaine dans la zone du milieu. Cliquez sur l'indication pour afficher l'onglet **Quarantaine** du panneau **Aide et Support**.

L'onglet affiche en temps réel la liste des fichiers qui ont été placés en quarantaine avec leur nom, leur emplacement, la date de mise en quarantaine ainsi que la date à laquelle les fichiers seront supprimés.

Consulter l'état des protections

Dans l'onglet **Protections**, vous pouvez consulter la liste et l'état des modules de protection de l'agent SES Evolution. Elle correspond aux fonctionnalités que vous pouvez activer ou désactiver dans la configuration de l'agent dans la console d'administration. Pour plus d'informations, reportez-vous à la section Choisir les fonctionnalités à activer sur les agents.

Les modules ou protections désactivés s'affichent en gris ou avec une icône en forme de rond barré.

7.5.4 Utiliser la commande EsGui

La commande EsGui permet d'interagir avec l'interface de l'agent SES Evolution. Elle peut être utilisée dans des scripts ou dans le raccourci de l'interface sur le Bureau Windows. Les options de cette commande sont les suivantes :

`/silent ou /s`	Permet de ne pas afficher l'interface de l'agent mais seulement son icône dans la zone de notifications de Windows.

/ShowPanel <panel>	Affiche un onglet spécifique de l'interface de l'agent. Les valeurs possibles sont : • `ProtectionStatus` : affiche le tableau de bord **État des protections**, • `Settings` : affiche la panneau **Préférences**, • `Contact` : affiche l'onglet **Contacts** du panneau Aide et Support, ◦ `Assistance` : affiche l'onglet **Assistance** du panneau Aide et Support, • `Diagnostics` : affiche l'onglet **Diagnostic** du panneau Aide et Support, • `Logs` : affiche l'onglet **Événements** du panneau Aide et Support.
/EnterMaintenanceMode	Démarre le mode maintenance. L'interface de l'agent doit être lancée avec les droits d'administration, et le mode maintenance doit être autorisé par les paramètres de groupe d'agents. Pour plus d'informations, reportez-vous à la section Comprendre l'autoprotection des agents et réaliser des opérations de maintenance
/LeaveMaintenanceMode	Quitte le mode maintenance. L'interface de l'agent doit être lancée avec les droits d'administration.
/GenerateDiagnostic <path.zip> /AcknowledgePersonalDataCollection /DiagnosticComment <comment>	Génère un package de diagnostic sans prise de traces. Spécifiez le répertoire de destination du package. Le paramètre `/AcknowledgePersonalDataCollection` est obligatoire pour accepter que des données personnelles soient collectées. Le paramètre `/DiagnosticComment` est optionnel, il permet d'ajouter un commentaire. Pour plus d'informations, reportez-vous à la section Établir un diagnostic.
/StartDiagnosticWithTraces /AcknowledgePersonalDataCollection	Démarre un diagnostic et la prise de traces.
/StopDiagnosticWithTraces <path.zip> /DiagnosticComment <comment>	Arrête la prise de traces et termine la génération du package de diagnostic. Spécifiez l'emplacement pour enregistrer le package.
/CancelDiagnostic	Annule le diagnostic en cours.
/GrantWebAccess	Démarre une période d'accès temporaire au web, si cela est permis par la politique. Pour plus d'informations, reportez-vous à la section Accéder temporairement au web depuis l'agent.

`/ExportLogs`	Exporte les logs de l'agent. Vous pouvez spécifier en option le dossier de destination. L'interface de l'agent doit être lancée avec les droits d'administration. Pour plus d'informations, reportez-vous à la section Consulter les logs des agents déconnectés.
`/ForceConnection`	Force la connexion de l'agent au gestionnaire d'agents pour envoyer les informations sur l'état de l'agent et les logs, et récupérer les nouvelles configurations, politiques ou mises à jour. Cette option est l'équivalent d'un clic sur le bouton **Vérifier la présence de mises à jour** de l'interface de l'agent. Pour plus d'informations, reportez-vous à la section Consulter l'état de santé de l'agent.

7.6 Mettre à jour les agents

Lorsque vous avez mis à jour SES Evolution avec le Centre d'installation, vous pouvez alors appliquer cette version à un ou plusieurs groupes d'agents via la console d'administration. Si certains agents ne sont pas connectés au gestionnaire d'agents ou si vous ne souhaitez pas que la mise à jour soit automatique, appliquez-leur la nouvelle version manuellement.

Il est recommandé d'appliquer une mise à jour d'abord sur un groupe d'agents de test afin de l'éprouver. Vous l'appliquerez ensuite à vos groupes de production.

Pour faire revenir les agents à une version logicielle antérieure de SES Evolution, assurez-vous que l'option **Autoriser le retour à une version antérieure** est activée dans la section Choisir les paramètres de mise à jour des agents.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour mettre à jour les agents.

7.6.1 Appliquer la mise à jour à un agent connecté au gestionnaire d'agents

Cette procédure s'applique si vous souhaitez que les gestionnaires d'agents mettent automatiquement les agents à jour lors d'un nouveau déploiement. Dans le cas contraire, désactivez l'option **Appliquer automatiquement les mises à jour logicielles** dans le menu indiqué ci-dessous. Pour une mise à jour manuelle, consultez les deux sections suivantes.

1. Choisissez le menu **Environnement > Agents**, puis sélectionnez le groupe d'agents à mettre à jour.
2. Dans l'onglet **Paramètres**, section **Version**, un message vous indique qu'une nouvelle version est disponible. Choisissez la nouvelle version à appliquer aux agents de ce groupe.
3. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.
4. Dans le menu **Sécurité** > **Déploiement**, cliquez sur **Déployer**.
   La nouvelle configuration sera appliquée aux agents du groupe à leur prochaine connexion au gestionnaire d'agents.
   Vous pouvez accélérer l'application de la mise à jour sur l'agent en cliquant sur **Vérifier la présence de mises à jour** dans l'interface de l'agent. Pour plus d'informations, reportez-vous à la section Comprendre l'interface de l'agent sur les postes de travail.

7.6.2 Appliquer la mise à jour manuellement à un agent

Si votre agent n'est pas connecté au gestionnaire d'agents ou si vous souhaitez maîtriser les mises à jour de vos agents, vous devez générer un installeur et l'exécuter manuellement sur les agents comme lors d'un déploiement initial. Pour plus d'informations, reportez-vous à la section Installer les agents sur les postes de travail

Lors de la mise à jour, non seulement la nouvelle version logicielle est appliquée à un agent, mais également la nouvelle version de configuration, dont les politiques de sécurité et la configuration des groupes d'agents.

Pour que la mise à jour fonctionne, il faut que :

- L'agent mis à jour appartienne au groupe d'agent pour lequel l'installeur a été généré,
- La version de configuration (e.g., politiques, configuration des groupes d'agents) incluse dans la mise à jour soit plus récente que la version de configuration de l'agent.

Si ces conditions ne sont pas réunies, effectuez une mise à jour forcée de l'agent.

7.6.3 Effectuer une mise à jour forcée d'un agent

Un installeur standard ne vous permet pas d'appliquer à un agent la configuration d'un groupe d'agents auquel il n'appartient pas, ou de le faire revenir à une version de configuration antérieure. Pour cela, vous devez effectuer une mise à jour forcée de l'agent. Il est préférable que l'agent soit déconnecté du gestionnaire d'agents lorsque vous procédez à sa mise à jour forcée. En effet, à la prochaine connexion de l'agent au gestionnaire d'agents, il retournera dans le groupe qui lui a été initialement attribué.

1. Choisissez le menu **Environnement > Agents**, puis sélectionnez le groupe d'agents que vous souhaitez appliquer à l'agent.
2. Dans l'onglet **Agents**, cliquez sur **Installeur > Mise à jour forcée > Générer un installeur 64 bits**.
3. Enregistrez le fichier d'installation *AgentSetup_x64.exe* à l'emplacement de votre choix et exécutez-le sur l'agent comme lors d'un déploiement initial. Pour plus d'informations, reportez-vous à la section Installer les agents sur les postes de travail.
4. Si vous souhaitez éviter que l'agent retourne dans son groupe d'agents d'origine à la prochaine connexion au gestionnaire d'agents, déplacez l'agent dans le groupe souhaité avant sa reconnexion. Pour plus d'informations, reportez-vous à la section Déplacer des agents d'un groupe à l'autre.

Vous devrez également effectuer une mise à jour forcée si un agent en mode Maintenance a besoin d'être mis à jour. Pour plus d'informations sur le mode Maintenance, reportez-vous à la section Comprendre l'autoprotection des agents et réaliser des opérations de maintenance.

7.7 Gérer un parc avec des agents de différentes versions

Si vous mettez à jour SES Evolution vers une nouvelle version, mais que certains groupes d'agents ou agents conservent l'ancienne version, votre parc sera hétérogène.

Pour plus d'informations sur la mise à jour des agents, reportez-vous à la section Mettre à jour les agents.

Vous pouvez facilement visualiser le nombre d'agents pour chaque version sur le tableau de bord dans le diagramme Agents. Cette information se trouve aussi dans l'onglet Agents du panneau Agents.

Dans un parc hétérogène, les agents ayant conservé l'ancienne version ne bénéficient pas de toutes les nouvelles fonctionnalités. Les informations d'incompatibilité sont affichées sous la

forme d'icônes et d'info-bulles descriptives dans le menu **Environnement > Agents** de la console d'administration.

L'icône...	Signifie ...
[2.3+]	La version logicielle sélectionnée dans le groupe d'agents ne supporte pas cette fonctionnalité. C'est le cas par exemple du paramètre **Autoriser la désinstallation** dans la configuration d'un groupe d'agents. Vous pouvez cependant enregistrer la configuration du groupe d'agents et déployer la politique sur le groupe.
[2.2+]	La version logicielle sélectionnée dans le groupe d'agents ne supporte pas une fonctionnalité. C'est le cas par exemple du filtrage d'applications par les arguments de la ligne de commande de la version 2.2. Si l'icône est rouge, vous ne pouvez pas enregistrer la configuration du groupe et déployer la politique.
	Certains agents dans le groupe n'ont pas encore la version nécessaire pour utiliser une fonctionnalité. C'est le cas par exemple de la fonctionnalité d'affectation automatique des agents à un groupe.

7.8 Supprimer les agents obsolètes de la console

Lorsque des agents ne sont plus utilisés sur des postes de travail de l'entreprise, ils continuent de s'afficher dans le tableau de surveillance du panneau **Environnement > Agents** de la console et de compter dans le nombre d'agents autorisés par la licence.

Nous vous recommandons de nettoyer la liste d'agents afin d'éviter le dépassement d'agents autorisés par la licence et la présence dans la base de données d'agents n'existant plus.

Selon les cas, vous avez la possibilité de nettoyer cette liste par le biais de deux mécanismes : la suppression automatique périodique d'agents ou la fusion de doublons.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour supprimer les agents obsolètes.

7.8.1 Supprimer automatiquement les agents déconnectés

La suppression automatique des agents déconnectés se configure indépendamment pour chaque groupe d'agents et a lieu à intervalles réguliers. Elle répond aux cas de figures suivants :

- remasterisation d'un poste de travail parce que le collaborateur a quitté l'entreprise, parce qu'il change de machine ou parce que le poste de travail nécessite une mise à jour de système d'exploitation par exemple.
- machine qui n'est plus utilisée dans l'entreprise.
- agent désinstallé d'un poste de travail alors qu'il était déconnecté du gestionnaire d'agents au moment de la désinstallation.

Pour programmer la suppression automatique périodique des agents qui ne se sont pas connectés aux gestionnaires d'agents depuis une durée définie :

1. Dans le menu **Environnement > Agents**, sélectionnez un groupe d'agents et cliquez sur **Modifier** en haut à droite.
2. Dans l'onglet **État et logs** du groupe, rendez-vous dans la section **Surveillance des agents en temps réel**.
3. Définissez le nombre de jours pour le paramètre **Suppression automatique après**. La valeur par défaut est de 30 jours.

La suppression automatique se déclenche à deux heures du matin. Il n'est pas possible de modifier l'horaire.

Si un agent supprimé de la console venait à se reconnecter à son gestionnaire d'agents, une nouvelle identité lui serait attribuée.

7.8.2 Fusionner les agents en double

La fusion de doublons s'opère de façon globale sur tous les agents. C'est une opération manuelle et instantanée. Elle répond aux cas de figures suivants :

- remasterisation d'un poste de travail en gardant le même nom d'ordinateur.
- vous ne souhaitez pas attendre la suppression automatique des agents déconnectés.

Pour fusionner des agents en double :

1. Dans le menu **Environnement > Agents**, sélectionnez **Tous les agents**.
2. Rendez-vous dans l'onglet **Maintenance**.
3. Sélectionnez un **Critère d'affichage des doublons** :
   - **Nom Active Directory** : dans le cas où tous les postes de travail se trouvent dans l'annuaire Active Directory, le Nom Active Directory est le meilleur critère car il garantit l'unicité des agents et les doublons détectés seront bien à supprimer.
   - **Nom d'ordinateur, Nom NetBIOS** : vous pouvez choisir ces critères si tous les postes de travail ne se trouvent pas dans l'annuaire Active Directory car ce sont en général des noms uniques.
   - **Adresse IP** : vous pouvez choisir ce critère dans le cas où plusieurs machines du parc d'une entreprise porteraient les mêmes noms. Attention cependant au cas où plusieurs machines partageraient la même adresse IP.
4. Sélectionnez une ou plusieurs lignes. Chaque ligne affiche les deux agents, celui qui s'est connecté le plus récemment s'affiche en premier.
5. Cliquez sur **Fusionner**. Tous les agents "grisés" sont supprimés de la base de données.

7.9 Désinstaller les agents

Il existe plusieurs méthodes pour désinstaller un agent. Vous devez disposer des droits d'administration et l'action doit aussi être autorisée dans la configuration du groupe d'agents, sauf pour la méthode via challenge. Pour plus d'informations, reportez-vous à la section Autoriser les administrateurs à désinstaller les agents.

- Pour désinstaller plusieurs agents via GPO, MECM (ex SCCM), etc., lancez l'exécutable EsSetupWorker.exe situé dans le répertoire d'installation\SES Evolution\Agent\Bin. Par défaut, le répertoire d'installation est C:\Program Files.
- Pour désinstaller un agent d'un poste de travail individuel, utilisez le menu **Désinstaller** dans les **Programmes et fonctionnalités** du Panneau de configuration de Windows. C'est le programme *EsSetup.exe* qui sera lancé. Pour connaître les options de ce programme si vous souhaitez l'utiliser dans un script, reportez-vous à la section Utiliser la commande EsSetup.
- Pour désinstaller un agent sans les droits d'administration grâce aux challenges, reportez-vous à la section Résoudre les problèmes avec les challenges.
- Si aucune des méthodes ci-dessus ne fonctionne, vous pouvez forcer la désinstallation avec l'outil *AgentRemovalTool.exe*. Reportez-vous à la section ci-dessous pour utiliser l'outil.

Dans tous les cas, la désinstallation n'est effective qu'après redémarrage du poste de travail. Tous les fichiers liés à l'agent sont supprimés sauf la clé de registre *HKEY_LOCAL_MACHINE\Software\Stormshield\SES Evolution* qui contient l'identifiant unique de l'agent pouvant être réutilisé lors d'une installation future.

Le fichier de log de la désinstallation est aussi conservé dans le dossier temporaire de l'utilisateur ayant effectué la désinstallation de l'agent.

7.9.1 Utiliser les commandes EsSetup ou EsSetupWorker

La commande EsSetup permet de désinstaller ou réparer l'agent SES Evolution. Les options de cette commande sont les suivantes :

`/silent ou /s`	Permet de ne pas afficher la barre de progression lors de la désinstallation ou réparation de l'agent.
`/Repair`	Provoque une vérification de l'intégrité, et une réparation de l'agent.
`/Log <chemin>`	Spécifie le chemin du fichier de log de l'agent.
`/NewAgentId`	Supprime les données de communication de l'agent avec le gestionnaire d'agents : identifiant unique, certificats utilisés en interne, identifiant et données privées pour les challenges. L'agent récupère de nouvelles données à sa prochaine connexion au gestionnaire d'agents.

Utilisée sans les options `/Repair` ou `/NewAgentId`, cette commande désinstalle l'agent SES Evolution.

La commande EsSetupWorker exécute les mêmes options que EsSetup sans interface graphique. Elle est à privilégier pour les opérations via GPO, SCCM, etc. Elle dispose des mêmes options que EsSetup à l'exception de `-Silent`.

7.9.2 Forcer la désinstallation de l'agent

Si les méthodes de désinstallation standard ne fonctionnent pas, téléchargez l'outil *AgentRemovalTool.exe* sur votre espace client MyStormshield (versions 32 et 64 bits disponibles dans la rubrique **Téléchargements** > **Stormshield Endpoint Security** > **Evolution** > **Tools**). L'outil, en ligne de commande, vous permet de forcer la désinstallation de l'agent sur un poste via le mode sans échec de Windows.

Pour forcer la désinstallation d'un agent, suivez la procédure ci-dessous. Vous devez répéter l'opération deux fois :

- La première fois en mode sans échec de Windows,
- La deuxième fois en mode démarrage normal de Windows.

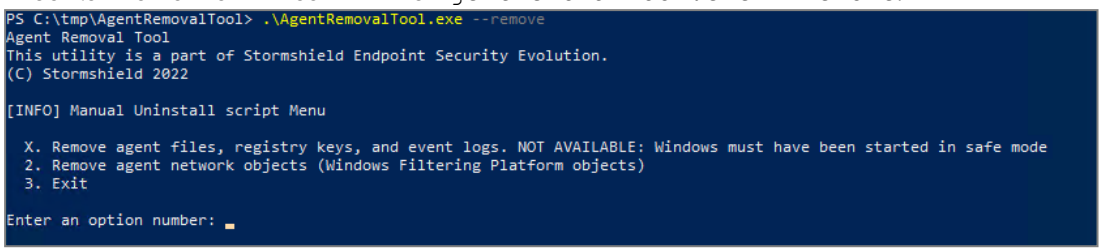
Les droits d'administration sont nécessaires pour exécuter l'outil.

1. Démarrez le poste de travail en mode sans échec.
2. Si besoin, affichez l'aide avec la commande `AgentRemovalTool.exe --help`.
3. Assurez-vous que l'outil détecte la bonne version de l'agent installée sur le poste avec la commande `AgentRemovalTool.exe --supported-versions`.
4. Exécutez la commande `AgentRemovalTool.exe --remove` pour lancer la désinstallation.

```
PS C:\tmp\AgentRemovalTool> .\AgentRemovalTool.exe --remove
Agent Removal Tool
This utility is a part of Stormshield Endpoint Security Evolution.
(C) Stormshield 2022

[INFO] Manual Uninstall script Menu

  1. Remove agent files, registry keys, and event logs
  X. Remove agent network objects (Windows Filtering Platform objects). NOT AVAILABLE: This cannot be run in safe mode
  3. Exit

Enter an option number:
```

5. Choisissez le menu numéro 1. Le menu numéro 2 n'est pas disponible en mode sans échec.
6. Démarrez ensuite le poste de travail en "mode standard".

7. Exécutez de nouveau la commande `AgentRemovalTool.exe --remove`.



8. Choisissez le menu numéro 2. Le menu numéro 1 n'est pas disponible en "mode standard". À l'issue de ces étapes, l'agent est correctement désinstallé.
9. Choisissez le menu 3 pour quitter l'outil.

Les commandes suivantes sont également disponibles, en mode sans échec et en "mode standard" :

- Si l'outil ne peut pas détecter la version de l'agent installée, la commande `AgentRemovalTool.exe --remove --agent-version "2.3.2.0"` permet d'indiquer la version à supprimer.
- La commande `AgentRemovalTool.exe --remove --force` permet de forcer la relance de la désinstallation si celle-ci a échoué une première fois avec l'outil.

7.10 Comprendre les interactions entre SES Evolution et Windows Defender

L'agent SES Evolution ajoute automatiquement des exceptions dans les paramètres du système de sécurité de Windows afin d'éviter que le programme antivirus Windows Defender ne se déclenche lorsque SES Evolution réalise des opérations légitimes et qu'il ne les bloque.

Ces exceptions sont ajoutées dans le menu **Protection contre les virus et menaces** de la fenêtre **Sécurité Windows** :

- dans la liste des accès contrôlés aux dossiers,
- dans la liste des exclusions.

Grâce à ces exceptions, Windows Defender ne bloque pas les actions suivantes de SES Evolution :

- des analyses Yara ou des recherches d'indicateurs de compromission (IoC),
- la création de clichés instantanés Windows dans le cadre de la protection contre une attaque par ransomware. Cette création est bloquée si la protection Ransomware de Windows Defender est activée.

Ces exceptions sont supprimées en cas de désinstallation de l'agent.

> **NOTE**
> Nous vous recommandons de fermer la fenêtre **Sécurité Windows** lors de l'installation, de la mise à jour ou de la réparation d'un agent SES Evolution.

8. Gérer les politiques de sécurité

Une politique de sécurité est appliquée sur les agents SES Evolution et permet de contrôler l'accès aux ressources et de protéger les postes de travail contre les comportements malveillants.

Avant de mettre en œuvre des politiques de sécurité sur votre parc de machines, vous avez la possibilité de les tester de façon transparente pour les utilisateurs. Vous pouvez ainsi évaluer leurs impacts et les ajuster si besoin. Pour plus d'informations, reportez-vous à la section Tester une politique de sécurité.

8.1 Comprendre une politique de sécurité

Une politique de sécurité se compose de jeux de règles d'audit et de protection. Un jeu de règles est en ensemble de règles de sécurité, portant sur les applications, les ressources ACL, les ressources réseau, les périphériques et la protection contre les menaces. Il peut être privé, c'est-à-dire propre à une politique ou bien partagé entre plusieurs politiques.

Ce fonctionnement par jeux de règles permet de mutualiser des règles communes à plusieurs politiques et de gérer différentes versions de ces jeux afin de créer des politiques de pré-production et des politiques de production. L'agrégation de ces jeux au sein d'une politique permet également de surcharger les règles communes avec des règles spécifiques à l'environnement de votre entreprise.

EXEMPLE
Vous pouvez utiliser deux politiques qui s'appliquent en alternance selon la situation géographique d'un collaborateur : une politique pour gérer l'accès aux ressources en interne et une politique pour gérer l'accès aux ressources lorsque le collaborateur est en déplacement. Ces deux politiques peuvent partager les mêmes jeux de règles et n'avoir qu'un jeu qui diffère, afin de bloquer les connexions réseau des postes nomades lorsqu'ils ne sont pas connectés à leur réseau de domaine et qui autorise uniquement l'établissement d'un tunnel VPN pour se connecter à leur domaine.

Une fois créées, les politiques de sécurité sont liées à des groupes d'agents qui vont les appliquer sur votre parc. Seules les politiques de sécurité peuvent être liées aux groupes d'agents. Les jeux de règles ne peuvent pas être directement liés aux agents.

Avant de les mettre en œuvre, vous pouvez tester le fonctionnement de vos politiques. Pour plus d'informations, reportez-vous à la section Tester une politique de sécurité.

À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.

8.1.1 Comprendre les politiques de sécurité intégrées et personnalisées

SES Evolution permet l'utilisation de deux types de politiques de sécurité : intégrées ou personnalisées.

Politiques de sécurité intégrées

SES Evolution est équipé de plusieurs politiques de sécurité intégrées qui permettent de bloquer les comportements et les techniques employées par la majorité des logiciels malveillants, quelle que soit leur finalité. Par exemple cheval de Troie, outil de prise de contrôle à distance, ransomware, voleur de mots de passe, etc. Les politiques intégrées sont les

suivantes :

- **La politique par défaut simplifiée** - Elle permet de déployer rapidement et simplement SES Evolution dans un parc en y dédiant peu de ressources humaines et sans avoir à maîtriser finement son administration. Elle est utilisable sans configuration spécifique. Vous devez tout de même savoir manipuler la console d'administration pour créer des exceptions ou mettre à jour des politiques.
- **La politique par défaut** - Elle constitue un compromis équilibré entre le besoin d'administration et le niveau de sécurité correspondant au besoin de la plupart des sociétés. Elle cible les sociétés dont les équipes Sécurité sont modérément dimensionnées et qui maîtrisent les bases de l'administration de SES Evolution.
  Cette politique de sécurité est appliquée par défaut au groupe d'agents par défaut.
- **La politique par défaut renforcée** - Elle renforce au maximum le niveau de sécurité d'un parc au prix de la simplicité d'administration. Il est important de tester avec un groupe pilote avant de déployer cette politique pour profiter de ses possibilités tout en minimisant les faux positifs. Elle est utilisée par les sociétés ayant un haut niveau de maturité en matière de sécurité et une politique de sécurité définie (par exemple, un catalogue de logiciels approuvés). Elle nécessite une maintenance suivie de la part des administrateurs.
- **La politique de protection des composants backoffice** - Elle assure la protection des composants backoffice de SES Evolution : le backend, les gestionnaires d'agents et la console d'administration. Elle contient des protections de la politique par défaut, auxquelles s'ajoutent plusieurs règles de protection qui viennent renforcer la sécurité des processus protégés et bloquer les tentatives de lecture ou modification de leurs données de paramétrage.
  Vous pouvez appliquer cette politique telle quelle aux groupes d'agents contenant les composants backoffice.

Les politiques intégrées sont constituées de jeux de règles intégrés. Pour plus d'informations, reportez-vous à la section Comprendre les jeux de règles intégrés.

Politiques de sécurité personnalisées

Si les politiques intégrées ne sont pas suffisantes, vous pouvez créer des politiques de sécurité personnalisées qui s'adaptent précisément à votre infrastructure. Pour cela, utilisez les jeux de règles qui composent les politiques intégrées, ou créez vos propres jeux de règles. Pour plus d'informations, reportez-vous à la section Construire une politique de sécurité.

> **EXEMPLE**
> Créez des règles pour gérer les accès au réseau de l'entreprise de vos collaborateurs en déplacement ou bien pour gérer l'utilisation de périphériques de confiance sur votre parc.

8.1.2 Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit

Il existe deux types de jeux de règles : audit et protection.

Selon le jeu de règles auquel appartiennent les règles de sécurité, elles remplissent des objectifs différents. Dans un jeu de règles de protection, les règles permettent de bloquer les attaques sur les postes de travail, de détecter des élévations de privilèges et de gérer les accès aux différentes applications, réseaux, périphériques, etc. Dans un jeu de règles d'audit, elles permettent de générer des logs uniquement à des fins de surveillance de l'activité de votre parc et éventuellement pour reconstituer le contexte d'une attaque.

L'onglet **Menaces** des jeux de règles ne liste pas exactement les mêmes protections selon qu'il s'agit d'un jeu de protection ou d'un jeu d'audit. Pour plus d'informations, reportez-vous à la section Gérer l'exploitation des vulnérabilités.

De même, la gestion de l'accès temporaire au web et le contrôle de l'activation de la carte Wi-Fi ne sont possibles que dans un jeu de règles de protection.

Comprendre les jeux de règles de protection

Dans un jeu de règles de protection, l'agent évalue les règles une par une et dans l'ordre :

- Si une action est interdite pour une ressource donnée, l'agent émet un log, bloque l'action, et ne parcourt pas les autres règles concernant cette ressource.
- Si une action est autorisée explicitement pour une ressource donnée, l'agent l'autorise et ne parcourt pas les autres règles concernant cette ressource.
- Si une ressource n'est pas concernée par une règle, alors l'agent parcourt les règles suivantes.

Utilisez ce mode pour protéger vos postes contre des comportements malveillants, et restreindre les accès pour protéger votre parc contre des comportements dangereux.

Dans les jeux de protection, toutes les règles de contrôle d'accès à des ressources ou des périphériques possèdent un mode **Règle passive**. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.

Vous pouvez également tester un jeu de règles complet ou une politique complète avant de les mettre en œuvre sur votre parc de machines. Pour plus d'informations, reportez-vous à la section Tester une politique de sécurité.

Comprendre les jeux de règles d'audit

Dans un jeu de règles d'audit, si le comportement **Audit** est sélectionné pour une action dans une règle, l'agent émet des logs pour indiquer les actions effectuées par des applications. Dans tous les cas, l'agent parcourt toutes les règles suivantes.
Utilisez ce mode pour surveiller l'accès à certaines ressources et envoyer les informations correspondantes à l'administrateur sans bloquer les accès, afin de détecter les comportements anormaux.

Les règles d'audit peuvent également permettre de surveiller l'activité des collaborateurs : les applications qu'ils utilisent le plus ou les versions des applications qu'ils utilisent par exemple.

Pour éviter de multiplier l'émission de logs, créez des règles précises ne couvrant pas un trop large spectre de ressources ou d'applications.

Les règles d'audit peuvent être totalement transparentes dans l'utilisation de la solution SES Evolution si vous choisissez de n'afficher les logs ni sur l'agent, ni sur la console, ou de ne pas les envoyer vers un serveur Syslog. Mais en cas d'attaque, les logs produits et stockés sur l'agent peuvent servir à la reconstitution du contexte. Le contexte d'attaque est visible sous forme de graphique. Pour plus d'informations, reportez-vous à la section Analyser les contextes pour comprendre une attaque.

Dans les règles d'audit, deux comportements sont possibles pour chaque action disponible : **Autoriser** ou **Audit**. Le comportement **Autoriser** signifie que la règle ne déclenche pas d'action. Il peut être utile lorsque vous souhaitez paramétrer un comportement par défaut et un ou des comportements spécifiques dans une règle. Vous sélectionnerez peut-être **Audit** pour les comportements spécifiques et **Autoriser** pour le comportement par défaut. Il est également utile

lorsque plusieurs actions sont disponibles pour une ressource et que vous ne souhaitez surveiller qu'un type d'action par exemple.

8.1.3 Ordonner les jeux de règles et les règles dans une politique

Les règles de protection et d'audit sont évaluées par l'agent dans l'ordre des jeux de règles dans la politique et dans l'ordre des règles elles-mêmes à l'intérieur d'un jeu. Si des jeux de règles différents concernent les mêmes ressources, il faut bien veiller à l'ordre des jeux car l'évaluation des règles s'arrête dès lors qu'une règle a été appliquée par l'agent. Ce sont donc les règles du jeu le plus haut placé qui s'appliquent.

Toutes les règles d'une politique, qu'elles fassent partie de jeux privés ou partagés, sont agrégées comme si elles avaient été créées dans une même politique. Si une politique contient deux jeux de règles, l'ensemble des règles du premier jeu sont parcourues, puis l'ensemble des règles du second jeu.

De façon générale, si vous utilisez des jeux d'audit et des jeux de protection au sein d'une même politique, nous vous conseillons de placer les jeux d'audit avant les jeux de protection. Ceci permet de garantir la génération des logs sur les actions que vous souhaitez surveiller. Si vous placez les jeux de protection avant les jeux d'audit et que ceux-ci concernent les mêmes ressources, les règles d'audit ne seront pas évaluées dès lors qu'une règle de protection s'appliquera et aucun log d'audit ne sera produit.

À l'inverse, lorsqu'une règle d'audit s'applique, l'agent poursuit l'évaluation des règles, donc les règles de protection sont bien évaluées.

Dans le cas où vous souhaitez créer une politique comprenant des jeux de règles d'audit et des jeux de règles de protection fournis par Stormshield dans les jeux de règles partagés, et des jeux de règles personnalisés adaptés à votre environnement, nous vous conseillons de vous inspirer de l'ordre des jeux recommandé dans la section **Préconisations** des *Notes de version* SES Evolution.

Pour plus d'informations sur les jeux de règles fournis par Stormshield, reportez-vous à la section **Comprendre les jeux de règles intégrés**.

- Survolez un jeu de règles avec votre souris pour afficher l'icône de glisser-déposer à gauche du jeu et modifier l'ordre.

Au sein d'un même jeu de règles de protection, l'ordre des règles importe également, selon les mêmes principes d'évaluation que dans les jeux de règles. Les règles sont évaluées dans l'ordre et l'évaluation s'arrête dès lors qu'une règle s'applique. Les règles portant sur des ressources spécifiques doivent ainsi être placées avant les règles plus générales. Il en est de même pour les comportements spécifiques au sein d'une règle. Reportez-vous à la section suivante pour plus d'informations sur les comportements spécifiques.

8.1.4 Utiliser le comportement par défaut et les comportements spécifiques des règles

Dans les règles de **contrôle d'accès**, vous pouvez appliquer un comportement par défaut et un ou plusieurs comportements spécifiques.

Quand ajouter des comportements spécifiques ?

Définissez des comportements spécifiques si l'accès à la ressource visée par la règle doit être autorisé ou bloqué uniquement pour un certain nombre d'applications identifiées.

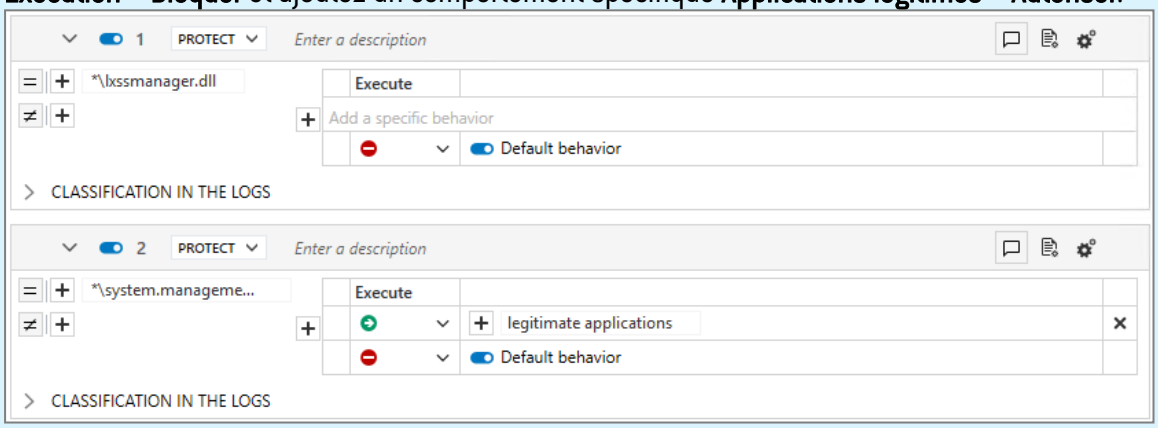
Vous pouvez ajouter plusieurs comportements spécifiques dans une même règle. Un premier par exemple pour autoriser certaines applications, et un deuxième pour en bloquer d'autres. Dans ce cas, l'ordre des comportements spécifiques est important : si une application dans le

premier comportement spécifique accède à la ressource, la règle s'applique et le deuxième comportement spécifique n'est pas lu.

Quand activer le comportement par défaut ?

Dans un jeu de règles de protection, activez un comportement par défaut lorsque vous voulez être certain que l'accès à la ressource sera bien bloqué ou autorisé, quelles que soient les règles qui suivent.

EXEMPLE 1
Dans les règles d'exécution de code :
- Pour bloquer l'exécution de la DLL *\lxssmanager.dll pour toutes les applications, activez le comportement par défaut avec **Exécution = Bloquer**.
- Pour bloquer l'exécution de la DLL *\system.management.automation.dll pour toutes les applications sauf celles qui sont reconnues légitimes, activez le comportement par défaut avec **Exécution = Bloquer** et ajoutez un comportement spécifique **Applications légitimes = Autoriser**.



EXEMPLE 2
Dans les règles d'accès aux fichiers :
Pour autoriser systématiquement l'exécution de scripts powershell (*.ps) au compte *NT SERVICE\TrustedInstaller*, activez le comportement par défaut avec **Lecture = Autoriser**.

Dans les exemples ci-dessus, le blocage ou l'autorisation sera TOUJOURS effectif. En effet, l'activation du comportement par défaut arrête la lecture des règles pour la ressource concernée. Les règles suivantes ne s'appliquent donc pas.

Dans les règles d'audit, le comportement par défaut est ignoré ; toutes les règles sont systématiquement lues.

Quand désactiver le comportement par défaut ?

Dans un jeu de règles de protection, désactivez le comportement par défaut lorsque vous voulez que la règle suivante qui concerne la même ressource soit évaluée.

EXEMPLES

- Dans les règles d'accès aux fichiers, pour que l'accès à une même ressource génère des niveaux de logs différents selon qu'elle est exécutée par une application ou une autre, désactivez le comportement par défaut d'une première règle, ajoutez un comportement spécifique pour bloquer certaines applications, et appliquez un niveau de log particulier.
  Créez ensuite une deuxième règle avec un comportement spécifique différent et un niveau de log différent.
- Dans les règles d'accès aux processus, créez une première règle pour donner toutes les autorisations au gestionnaire de tâches Windows sur tous les processus et désactivez le comportement par défaut. Ainsi le gestionnaire de tâches ne sera jamais bloqué par les règles suivantes qui pourraient interdire certaines applications d'accéder à certains processus et qui pourrait inclure le gestionnaire.

8.2 Construire une politique de sécurité

Une politique de sécurité se compose de jeux de règles d'audit et de protection. Un jeu de règles est en ensemble de règles de sécurité. Il peut être privé, c'est-à-dire propre à une politique ou bien partagé entre plusieurs politiques.

Pour plus d'informations sur les politiques de sécurité, reportez-vous à la section Comprendre une politique de sécurité.

Plusieurs versions des politiques ou des jeux de règles peuvent cohabiter et vous pouvez choisir la version à utiliser à tout moment. Pour plus d'informations, reportez-vous à la section Gérer les versions d'une politique ou d'un jeu de règles .

Avant de créer des règles de sécurité pour votre politique, vous devez avoir créé des identifiants d'applications, de pilotes et de réseaux. Pour plus d'informations, reportez-vous à la section Créer des identifiants.

Pour composer votre politique à partir des jeux de règles intégrés par défaut fournis par Stormshield (i.e., Default Policy) ou à partir de vos propres jeux, suivez les étapes suivantes.

Vous devez disposer du droit **Politiques-Modifier** pour créer et modifier des politiques de sécurité et des identifiants.

8.2.1 Comprendre les jeux de règles intégrés

Stormshield fournit une série de jeu de règles intégrés à la console. Certains sont déjà contenus dans les politiques de sécurité intégrées. Vous pouvez également les utiliser dans vos propres politiques personnalisées. Pour plus d'informations, reportez-vous à la section Créer une politique de sécurité.

Pour visualiser les jeux de règles SES Evolution intégrés, choisissez le menu **Sécurité > Politiques** et cliquez sur le lien **Voir les jeux de règles partagés**. Les jeux intégrés sont ceux qui sont précédés du préfixe Stormshield - .

D'autres jeux de règles fournis par Stormshield ne sont pas intégrés à la console et sont disponibles pour téléchargement sur votre espace personnel MyStormshield ou sur le serveur de téléchargement Stormshield.

Les jeux de règles sont régulièrement mis à jour. Vous trouverez les Notes de version de ces jeux qui contiennent leur description sur votre espace client Mystormshield ainsi que sur le panneau de téléchargement des mises à jour.

De plus, de nouveaux jeux de règles sont régulièrement mis à disposition sur le serveur de mise à jour Stormshield et également publiés sur l'espace Téléchargements de Mystormshield.

L'ordre des jeux de règles dans une politique est important. Pour plus d'informations, reportez-vous à la section Ordonner les jeux de règles et les règles dans une politique.

Les jeux de règles intégrés ne peuvent être ni modifiés, ni supprimés.

8.2.2 Personnaliser les jeux de règles intégrés

Certains jeux de règles intégrés doivent être adaptés à votre environnement pour être fonctionnels.

Cela est notamment le cas des cinq jeux de règles II 901. Ces jeux s'inspirent de la directive française de l'ANSSI, élaborée pour protéger les systèmes d'informations sensibles. Ce sont des modèles à personnaliser, pour vous aider à créer des politiques de sécurité mettant en pratique les recommandations de l'Instruction Interministérielle n° 901.

Les jeux de règles intégrés étant en lecture seule, vous devez les dupliquer pour les personnaliser, puis les ajouter à vos politiques.

Pour dupliquer un jeu de règle intégré :

1. Choisissez le menu **Sécurité > Politiques**.
2. Cliquez sur le lien **Voir les jeux de règles partagés** en haut à droite du panneau.
3. Sur la ligne du jeu de règles à dupliquer, cliquez sur l'icône ⋮, puis **Dupliquer**. Le jeu de règles dupliqué s'affiche en bas de la liste des jeux avec un numéro entre parenthèses.
4. Double-cliquez sur le jeu dupliqué puis cliquez sur **Modifier**.
5. Renommez le jeu puis adaptez les règles et identifiants à votre environnement.
6. Ajoutez le jeu à vos politiques en suivant la procédure de la section Créer une politique de sécurité.

8.2.3 Créer des jeux de règles partagés

Les jeux de règles partagés offrent la possibilité de mutualiser des règles communes à plusieurs politiques.

Si vous souhaitez utiliser des jeux de règles partagés dans vos politiques de sécurité, vous avez la possibilité de les créer en amont, indépendamment d'une politique, ou bien directement dans une politique.

Si vous fonctionnez avec des environnements de pré-production et des environnements de production, vous pouvez par exemple tester un jeu de règles privé dans une politique de pré-production et le transformer en jeu partagé lorsque son fonctionnement est validé, afin de l'utiliser dans une politique de production.

Pour créer un jeu de règles partagé indépendamment d'une politique :

1. Choisissez le menu **Sécurité > Politiques**.
2. Cliquez sur le lien **Voir les jeux de règles partagés** en haut à droite du panneau.
3. Cliquez sur **Créer**. La fenêtre **Créer un jeu de règles** s'affiche.
4. Choisissez le type du jeu et donnez un nom au jeu.
5. Cliquez sur **Créer**.

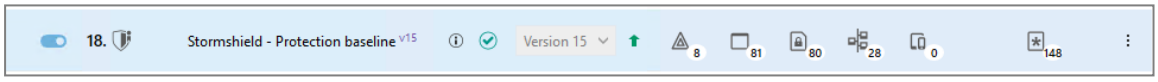
6. Vous allez maintenant créer les règles de votre jeu de règles. Cliquez sur le nouveau jeu de règles et cliquez sur **Modifier**.
7. Utilisez les onglets **Menaces**, **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** pour ajouter des règles de sécurité à votre jeu. Pour plus d'informations sur la création des règles, reportez-vous aux sections Gérer l'exploitation des vulnérabilités et Définir les règles de contrôle d'accès.
8. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour utiliser le jeu de règles dans une politique, reportez-vous à la section suivante Créer une politique de sécurité.

8.2.4 Créer une politique de sécurité

Dans une même politique de sécurité, vous pouvez assembler jeux de règles d'audit et jeux de règles de protection. Ce peut être le cas si vous composez des politiques de pré-production et des politiques de production par exemple.

Vous pouvez assembler autant de jeux de règles que nécessaire. Vous avez la possibilité de créer des règles de différentes catégories dans un même jeu, ou bien de créer un jeu par catégorie de règles. Le panneau général de chaque politique détaille la composition des jeux de règles :



Pour créer votre propre politique de sécurité :

1. Choisissez le menu **Sécurité** > **Politiques**.
2. Cliquez sur **Créer**. Une ligne s'affiche intitulée *Nouvelle politique*.
3. Faites un double-clic sur cette ligne. Le panneau général de la nouvelle politique s'affiche.
4. Dans le bandeau supérieur, cliquez sur le bouton **Modifier**.
5. Saisissez un nom et une description pour la politique. La description est importante pour qualifier les différentes versions d'une même politique.
6. Dans la section **Jeu de règles**, cliquez sur **Ajouter un jeu de règles partagé** pour ajouter un jeu de règles partagé existant, ou sur **Créer un jeu de règles** pour ajouter un nouveau jeu de règles.
7. Dans le cas d'un ajout de jeux de règles existants, sélectionnez-les dans l'ordre où vous souhaitez les voir apparaître dans la politique. Leur rang dans la politique s'affiche à gauche de leur case à cocher. Pour plus d'informations sur l'ordre des jeux de règles, reportez-vous à la section Ordonner les jeux de règles et les règles dans une politique.
8. Dans le cas d'un nouveau jeu de règles, dans la fenêtre **Créer un jeu de règles** :
   a. Choisissez le type du jeu : Protection ou Audit.
   b. Choisissez la visibilité : Privé ou Partagé. Un jeu privé n'est utilisé que dans la politique courante. Un jeu partagé peut être utilisé dans plusieurs politiques.
   c. Donnez un nom au jeu de règles.
   d. Cliquez sur **Créer**.
9. Vous allez maintenant créer les règles de votre jeu de règles. Cliquez sur le nouveau jeu de règles et cliquez sur **Modifier**.
10. Entrez éventuellement une description du jeu. La description est importante pour qualifier les différentes versions d'un même jeu.

11. Utilisez les onglets **Menaces**, **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** pour ajouter des règles de sécurité à votre jeu. Pour plus d'informations sur la création des règles, reportez-vous aux sections Gérer l'exploitation des vulnérabilités et Définir les règles de contrôle d'accès.

> **NOTE**
> Vous pouvez copier et coller des règles de même type entre jeux de règles de même type également (audit ou protection) et entre politiques.

12. Dans le panneau général de la politique, vous pouvez modifier l'ordre des jeux de règles en survolant les jeux avec la souris pour afficher l'icône glisser-déposer à gauche. L'ordre des jeux de règles est important. Pour plus d'informations, reportez-vous à la section Ordonner les jeux de règles et les règles dans une politique.
13. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour plus d'informations sur les versions des politiques et des jeux de règles ou si l'icône s'affiche sur la ligne), reportez-vous à la section Gérer les versions d'une politique ou d'un jeu de règles .

Vous devez ensuite assigner la politique de sécurité au groupe d'agents auquel vous voulez qu'elle s'applique, puis la déployer sur votre environnement. Pour plus d'informations, reportez-vous aux sections Assigner une politique de sécurité aux agents et Déployer l'environnement SES Evolution.

8.2.5 Gérer les versions d'une politique ou d'un jeu de règles

Plusieurs versions des politiques ou des jeux de règles peuvent cohabiter et vous pouvez choisir la version à utiliser à tout moment.

Gérer plusieurs versions d'une politique ou d'un jeu de règles en parallèle permet de mettre en place des politiques de pré-production et des politiques de production et ainsi de tester les conséquences de mises à jour de règles sur votre parc. Par exemple votre politique de production peut utiliser une version stable des jeux de règles, c'est-à-dire testée et validée, et votre politique de pré-production peut utiliser une version en cours de test, c'est-à-dire la version la plus récente.

Cette fonctionnalité offre également la possibilité d'opérer un retour en arrière en déployant de nouveau une version antérieure qui fonctionnait correctement. Par exemple si vous rencontrez un problème de déploiement sur l'environnement ou si les conséquences du déploiement d'une politique ou d'un jeu ne sont pas celles attendues sur votre parc.

Vous pouvez donner des descriptions précises à vos politiques et jeux pour mieux vous repérer dans les différentes versions.

Lorsque vous exportez une politique ou un jeu, vous exportez la version sélectionnée sur la droite du panneau. Pour plus d'informations sur l'import et l'export de politiques ou de jeux, reportez-vous à la section Exporter et importer les politiques et jeux de règles.

Gérer les versions d'une politique

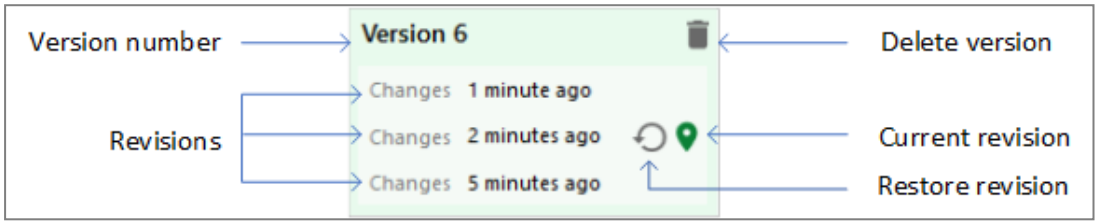
Sur le panneau général d'une politique, les numéros de version sont visibles dans le chemin de la politique en haut de page, ainsi que dans la colonne de droite. La dernière version qui a été déployée sur votre environnement s'affiche en bleu. La version sur laquelle vous êtes en train de travailler s'affiche en vert, ou en jaune si vous êtes en cours de modification.

Après chaque déploiement de politique sur votre environnement, le numéro de version s'incrémente automatiquement lorsque vous la modifiez de nouveau. Vous travaillez donc sur

une nouvelle version. La version d'une politique déployée est forcément la dernière que vous avez modifiée et enregistrée.

Pour la dernière version d'une politique, les modifications successives constituent les révisions de cette même version de politique. Cliquez sur une révision pour revenir dessus à tout moment.

L'icône indique la révision sur laquelle vous êtes en train de travailler.



Seule la dernière version d'une politique est modifiable. Pour modifier une version précédente, vous devez la restaurer au préalable.

Restaurer une version de politique :

1. Cliquez sur la version voulue de la politique. Le fond devient vert.
2. Cliquez sur le bouton pour restaurer cette version. Une nouvelle version est automatiquement créée avec le contenu de cette version restaurée, qui devient donc la plus récente. Si la politique a plusieurs révisions, vous pouvez restaurer une révision en particulier.
3. Faites vos modifications et sauvegardez. Si vous déployez la politique sur l'environnement, c'est cette version-là qui sera déployée.

Pour plus d'informations sur le déploiement d'une politique sur votre environnement, reportez-vous à la section Déployer l'environnement SES Evolution.

Gérer les versions d'un jeu de règles

Sur le panneau général d'un jeu de règles, les numéros de version sont visibles dans le chemin du jeu de règles en haut de page, ainsi que dans la colonne de droite. La dernière version qui a été déployée sur votre environnement s'affiche en bleu. La version sur laquelle vous êtes en train de travailler s'affiche en vert, ou en jaune si vous êtes en mode Modification.

Après chaque déploiement de politique sur votre environnement, le numéro de version d'un jeu s'incrémente automatiquement lorsque vous le modifiez de nouveau. Vous travaillez donc sur une nouvelle version.

Pour la dernière version d'un jeu de règles, les modifications successives constituent les révisions de cette même version de politique. Cliquez sur une révision pour revenir dessus à tout moment.

L'icône indique la version sur laquelle vous êtes en train de travailler.

Seule la dernière version d'un jeu de règles est modifiable. Pour modifier une version précédente, vous devez la restaurer au préalable.

Restaurer une version d'un jeu de règles :

1. Cliquez sur la version voulue du jeu de règles. Le fond devient vert.
2. Cliquez sur le bouton pour restaurer cette version. Une nouvelle version est automatiquement créée avec le contenu de cette version restaurée, qui devient donc la plus récente. Si le jeu a plusieurs révisions, vous pouvez restaurer une révision en particulier.
3. Faites vos modifications et sauvegardez.

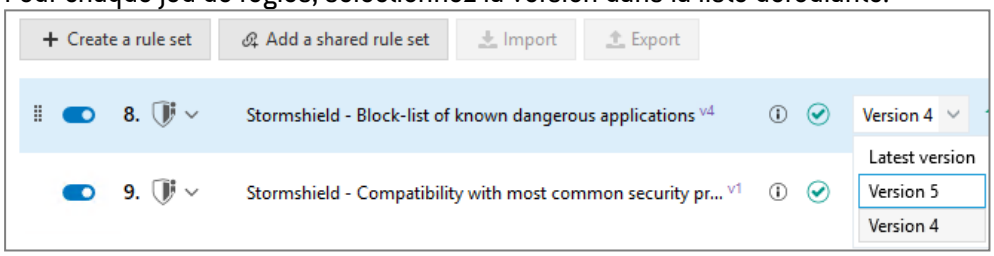
Créer manuellement une nouvelle version d'un jeu :

- Cliquez sur **Créer une nouvelle version** en haut à droite.

L'onglet **Général** d'un jeu de règles affiche les politiques dans lesquelles le jeu est utilisé et le numéro de version du jeu pour chaque politique.

Sélectionner la version d'un jeu à utiliser dans une politique :

1. Rendez-vous dans le panneau principal d'une politique.
2. Cliquez sur **Modifier** dans le bandeau supérieur.
3. Pour chaque jeu de règles, sélectionnez la version dans la liste déroulante.



Plusieurs politiques peuvent donc utiliser des versions différentes du même jeu de règles.

Dans votre environnement de production, nous vous recommandons d'utiliser une version stable d'un jeu de règles.

Si vous avez sélectionné **Toujours utiliser la dernière version** pour un jeu de règles, après un déploiement de politique, le numéro de la version du jeu déployée s'affiche dans la liste déroulante. Lorsque vous cliquez sur **Modifier**, le paramètre **Toujours utiliser la dernière version** est bien conservé.

Mettre à jour les politiques avec la dernière version d'un jeu :

Effectuez cette action seulement lorsque le jeu de règles est testé et validé.

- Dans l'onglet **Général** d'un jeu, cliquez sur pour mettre à jour toutes les politiques qui utilisent une même version d'un jeu avec la dernière version du jeu.

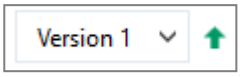
Supprimer une version d'une politique ou d'un jeu de règles

Vous pouvez supprimer des versions de politiques et de jeux de règles, y compris pour les politiques et jeux fournis par Stormshield. En revanche, il n'est pas possible de supprimer une version actuellement déployée et identifiée par l'icône .

1. Rendez-vous dans le panneau principal d'une politique ou d'un jeu de règles.
2. Cliquez sur l'icône de la version que vous souhaitez supprimer et confirmez.
   Lors de la suppression d'une version de politique, toutes les versions des jeux de règles privés utilisées dans cette version sont également supprimées. Aucune version de jeu de règles partagé n'est supprimée.

Mettre automatiquement à jour un jeu de règles

L'indicateur peut s'afficher dans le panneau général d'une politique :

- à côté de la version d'un jeu de règles 

, lorsque la version sélectionnée n'est pas la plus récente,
- à côté de l'icône des règles sur les menaces 

, lorsqu'au moins une protection avancée activée dans un jeu n'utilise pas sa dernière version.

Si vous souhaitez mettre à jour le jeu de règles concerné :

1. Cliquez sur **Modifier** dans le bandeau supérieur.
2. Cliquez sur le menu d'actions à droite de la ligne du jeu de règles, puis sur  pour mettre à jour la protection avancée ou le jeu selon le cas.

8.3 Créer des identifiants

Les identifiants permettent de définir les différentes applications, réseaux, et pilotes sur lesquels portent les règles de sécurité. Ils sont nécessaires lors de la création des règles de sécurité et vous devez donc les créer au préalable.

Chaque identifiant est constitué d'un nombre illimité d'entrées unies par un "OU" logique, c'est-à-dire qu'une règle de sécurité s'applique dès lors qu'au moins une des entrées d'un identifiant est reconnue.

Les entrées d'identifiant permettent de regrouper sous un même identifiant diverses ressources afin de mutualiser les règles les concernant.

Il n'y a pas de différence entre créer deux identifiants avec une entrée chacun ou un seul identifiant contenant deux entrées, si tous les identifiants sont liés à la même règle.

8.3.1 Créer des identifiants d'applications

Les identifiants d'applications permettent de définir les applications sur lesquelles portent les règles d'audit ou de protection, c'est-à-dire :

- Les applications à protéger ou à exclure d'une protection,
- Les applications susceptibles d'agir sur une application protégée, de manière légitime ou illégitime.

Les identifiants sont propres aux jeux de règles et vous devez donc créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section Exporter et importer des identifiants

EXEMPLE
Vous souhaitez interdire l'enregistrement des frappes clavier de votre navigateur web à toutes les applications, sauf à votre outil de virtualisation qui a légitimement besoin d'enregistrer les frappes clavier. Dans ce cas, vous devez créer un identifiant d'applications pour votre application à protéger (navigateur web), et un identifiant pour votre application qui pratique légitimement l'enregistrement de frappes (outil de virtualisation).

Les identifiants d'applications sont nécessaires lors de la création des jeux de règles et vous devez donc les créer au préalable.

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**.
3. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter un identifiant**.
   Un identifiant vide s'affiche en dessous des identifiants existants.
4. Cliquez sur **Modifier** en bas à droite.
5. Dans le champ **Nouvel identifiant d'application**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Cliquez sur  et sélectionnez tous les critères d'identifiants que vous souhaitez utiliser.
   Par exemple **Chemin** et **Certificat**.

7. Cliquez à l'extérieur de la fenêtre des critères et définissez chaque critère d'identification sélectionné :
   Chemins
   a. Cliquez sur **Modifier** puis dans le champ bleu en bas saisissez le chemin partiel ou complet du fichier exécutable de l'application. Il peut s'agir du chemin dans le système de fichiers ou d'un lien.
   Les caractères * et ? sont autorisés. Par exemple, entrez *\Apache.exe* pour désigner l'application Apache quel que soit son emplacement sur le poste de travail.
   Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.
   Stormshield recommande fortement l'utilisation des racines de chemins EsaRoots fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...)*. En effet, ces lettres peuvent différer d'un poste de travail à l'autre.
   b. Vous pouvez aussi préciser un flux de données alternatif (Alternate Data Stream). Les ADS d'un fichier exécutable lui permettent d'être constitué de plusieurs flux de données. Reportez-vous à la documentation Microsoft Windows pour en savoir plus.
   c. Cliquez sur **Ajouter**.
   d. Saisissez d'autres chemin dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
   e. Cliquez sur **Valider** pour confirmer la liste de chemins.

   Hashes
   Un hash permet d'identifier très précisément un binaire de confiance : toute modification changera le hash qui ne sera donc plus reconnu. Vous pouvez utiliser l'identification par hash dans les cas suivants :
   - Pour s'assurer qu'un binaire légitime n'est ni remplacé ni modifié. Cependant, cela nécessite une maintenance assez lourde car vous devrez modifier les identifiants à chaque mise à jour logicielle. Elle est donc à réserver pour les systèmes qui subissent très peu de changements.
   - Pour identifier les malware qui changent souvent de nom mais peuvent conserver leur hash. Importez la liste des hashes des malware les plus courants et bloquez ainsi leur exécution.

   Pour ajouter des hashes :
   a. Cliquez sur **Modifier** puis sur l'icône crayon.
   b. Dans le champ bleu en bas, saisissez le hash MD5, SHA1, ou SHA256 du binaire de l'application ainsi qu'une description, puis cliquez sur **Ajouter**
   Pour obtenir le hash d'un binaire, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le hash SHA256 de tous les fichiers *.exe* :
   ```
   Get-ChildItem -Recurse -Filter '*.exe' | get-filehash -Algorithm SHA256 | select path, Hash
   ```
   c. Saisissez d'autres hashes dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
   d. Cliquez sur **Valider**.
   e. Vous pouvez aussi importer une liste de hashes à partir d'un fichier CSV ou txt. Le fichier doit contenir une ligne par hash avec deux informations par ligne, séparées par une virgule, une tabulation ou un point-virgule :
   - Le hash (MD5, SHA1 ou SHA2),
   - La description.

   En cas d'erreur ou de doublon de hash, SES Evolution le signale et seuls les hashes valides et uniques sont importés.

Une fois les hashes saisis ou importés, la fenêtre affiche le nombre de hashes pour chaque algorithme.

f. Cliquez sur **Valider** pour confirmer la liste des hashes.

Processus parent

Sélectionnez le processus qui lance l'exécution de l'application. L'identifiant d'applications de ce processus doit avoir été créé au préalable.

a. Cliquez sur **Modifier**.

b. Recherchez l'identifiant du ou des processus parent grâce au champ de recherche et sélectionnez-les dans la liste.

c. Cliquez sur **Valider** pour confirmer la liste des processus parents.

Certificat

Importez le certificat de signature numérique fourni par l'éditeur de logiciel de l'application. Vous pouvez utiliser l'identification par certificats dans les cas suivants :

- Pour renforcer l'identification d'un binaire de confiance de manière moins restrictive qu'un hash car le certificat ne change pas à chaque nouvelle version du binaire. Elle est plus fiable que l'utilisation du chemin seul car un attaquant pourrait renommer un malware en *winword.exe* par exemple.
- Pour faire confiance à un éditeur et donc à tous les logiciels qu'il signe avec son certificat. Par exemple vous pouvez autoriser l'exécution de tous les binaires signés par Microsoft, ou même de tous les binaires signés par une autorité de certification de confiance.

Pour obtenir un certificat, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le certificat d'Acrobat Reader que l'on nomme *Adobe.cer* :

```
(Get-AuthenticodeSignature -FilePath "C:\Program Files
(x86)\Adobe\Acrobat Reader
DC\Reader\AcroRd32.exe").SignerCertificate | Export-Certificate -
FilePath Adobe.cer
```

Pour ajouter des certificats :

a. Cliquez sur **Modifier** à droite de la case à cocher, puis sur **Importer le certificat**.

b. Choisissez les certificats à importer.

c. Si nécessaire, recherchez le ou les certificats grâce au champ de recherche et sélectionnez-les dans la liste.

d. Cliquez sur **Valider** pour confirmer la liste des certificats.

e. L'option **Limiter la recherche à la liste (0)** permet de rechercher les applications identifiées par les certificats listés dans l'identifiant. Conservez la case décochée (par défaut) si vous souhaitez qu'une règle recherche parmi tous les certificats ayant signé des applications. Dans ce cas, il n'est pas nécessaire d'importer des certificats dans l'identifiant.
Vous pouvez affiner la recherche avec les options **Valide** et **Non valide** pour qu'une règle s'applique lorsqu'elle trouve des certificats valides ou non valides (listés dans l'identifiant ou non). Le statut invalide couvre les cas suivants : certificat non signé, révoqué, non vérifié, expiré, corrompu ou absence de certificat. Ces options sont compatibles avec les agents à partir de la version 2.3.

f. Si nécessaire, cochez **Ignorer les erreurs de validation de la signature du certificat** afin que les règles utilisant cet identifiant s'appliquent quand même lorsque la vérification du certificat est impossible et qu'une application est identifiée par d'autres critères définis dans l'identifiant.

La vérification du certificat peut être impossible dans les cas suivants :

- lorsqu'un fichier binaire est démarré avant l'installation de l'agent, avant le démarrage des services de l'agent, lors du premier redémarrage suivant l'installation de l'agent ou bien suivant une mise à jour majeure du système d'exploitation,
- dans le cas du fichier binaire *WerFault.exe*, qui est traité différemment des autres pour des raisons techniques,
- lorsque la lecture du fichier binaire est bloquée par un logiciel tiers.

Contexte d'exécution

a. Cliquez sur **Modifier**.

b. Dans la liste déroulante en bas, choisissez le type de compte qui lance l'application identifiée (e.g., *NT AUTHORITY\System*), puis cliquez sur **Ajouter**.
Vous pouvez choisir un niveau d'intégrité *strict* ou *supérieur ou égal*. Par exemple, si vous définissez un identifiant Powershell avec contexte d'exécution en *Niveau d'intégrité Administrateur (strict)*, la règle se déclenche uniquement pour un Powershell exécuté par un Administrateur. En revanche, avec un contexte d'exécution en *Niveau d'intégrité Administrateur (ou supérieur)*, la règle se déclenche si Powershell est exécuté par un Administrateur ou le Système d'exploitation.

Pour définir un compte bien spécifique, saisissez le SID (security identifier) du compte dans le champ.

Pour obtenir un SID, lancez une fenêtre de commandes avec les droits d'administration et exécutez la commande suivante :

```
WMIC useraccount get name,sid
```

c. Choisissez d'autres comptes si nécessaire et cliquez sur **Ajouter**.

d. Cliquez sur **Valider** pour confirmer la liste des comptes.

Type du volume
Activez le ou les types de volume sur lesquels s'exécute l'application : disque local du poste de travail, partage réseau (e.g., Samba/CIFS, DFS, etc.) ou périphérique amovible (e.g., clé USB, disque dur externe, téléphones mobiles selon leur configuration, etc.).

Ligne de commande
Filtrez les applications en fonction des arguments de leur ligne de commande. Cela permet d'appliquer des règles différentes à une même application selon l'usage qui en est fait. Pour utiliser le critère Ligne de commande, reportez-vous à la section suivante.

Plus vous spécifiez de critères, plus l'identification de l'application est précise car tous les critères doivent correspondre.

> **EXEMPLE**
> Dans l'identification de l'application *PowerShell.exe* signée par *Microsoft*, lancée par la tâche planifiée *schtasks.exe*, s'exécutant depuis le disque local via le compte *NT AUTHORITY\System*, les quatre critères doivent être présents pour que l'application soit identifiée.

8. Cliquez sur **Ajouter une entrée** si vous souhaitez ajouter une autre liste de critères pour le même identifiant. Avoir plusieurs entrées permet de regrouper sous un même identifiant diverses ressources qui sont utilisées par les mêmes règles de sécurité. Par exemple vous pouvez regrouper les différents navigateurs, ou alors regrouper diverses applications dangereuses afin d'établir une liste noire.

9. Activez l'option **Inclure les enfants des applications identifiées ci-dessous** pour qu'une règle appliquée à un identifiant soit propagée à tous ses identifiants enfants. Cette option permet par exemple d'identifier les programmes d'installation qui sont extraits dans un répertoire temporaire et lancent des exécutables ayant des noms aléatoires. Si vous déclarez le programme d'installation comme légitime, la légitimité se propagera à tous les fichiers temporaires qu'il aura créés et lancés.
10. Cliquez sur **Valider**.
11. Si vous avez terminé la création des identifiants d'applications, cliquez sur **Enregistrer** dans le bandeau supérieur.
12. Pour afficher le contenu d'un identifiant d'applications sans l'éditer, cliquez sur le bouton **Voir**.

ASTUCE
Vous pouvez également créer un identifiant d'applications directement depuis une règle. Dans une règle, cliquez sur le bouton [+], puis sur **Créer un nouvel identifiant**.
De même, depuis une règle, vous pouvez cliquer sur un identifiant déjà sélectionné afin de le modifier. Les modifications s'appliqueront aussi à l'identifiant dans l'onglet **Identifiants**.

Filtrer des applications par arguments de ligne de commande

Dans les identifiants d'applications, vous pouvez indiquer des arguments de ligne de commande en tant que critère d'identifiant.

Ce critère permet d'appliquer des règles différentes à une même application, selon l'usage qui en est fait, et ainsi de mieux maîtriser l'utilisation de certaines applications.

EXEMPLE
Ce type de filtrage permet de bloquer l'exécution de PowerShell uniquement lorsqu'il est exécuté de manière invisible ou lorsque ses arguments de ligne de commande tentent de contourner des politiques d'exécution Windows par exemple. Ces comportements peuvent en effet être l'action d'acteurs malveillants.

Gérer la compatibilité avec les versions des agents

L'utilisation de cette fonctionnalité est possible avec des agents en version 2.2.2 minimum. Si un groupe d'agents de version inférieure à la 2.2.2 applique une politique comprenant des identifiants d'applications utilisant le critère **Ligne de commande**, des indicateurs sont visibles à différents endroits de la console pour indiquer l'incompatibilité. Pour plus d'informations, reportez-vous à la section Gérer un parc avec des agents de différentes versions .

Pour faire en sorte que votre parc d'agents supporte cette fonctionnalité, les Notes de version SES Evolution indiquent une procédure de mise à jour des politiques de sécurité intégrées et du parc d'agents dans la section Préconisations.

Utiliser le critère Ligne de commande dans un identifiant

Pour créer un identifiant d'applications se basant sur des arguments de ligne de commande :

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**.
3. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter un identifiant**.
   Un identifiant vide s'affiche en dessous des identifiants existants.
4. Cliquez sur **Modifier** en bas à droite.

5. Dans le champ **Nouvel identifiant d'application**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Cliquez sur + et sélectionnez **Ligne de commande**.
7. Cliquez à l'extérieur de la fenêtre des critères.
8. Cliquez sur **Modifier**.
9. Entrez un nom et choisissez un mode :
   - **Paramètres personnalisés** (mode par défaut) : personnalisez les paramètres que la règle doit chercher dans une ligne de commande.
   - **Contient au moins un paramètre** : la règle s'applique à chaque fois qu'elle trouve des lignes de commande contenant au moins un paramètre.
   - **Sans aucun paramètre** : la règle s'applique à chaque fois qu'elle trouve des lignes de commande ne contenant pas de paramètre.

10. Si vous avez choisi le mode **Paramètres personnalisés**, vous allez créer une ou plusieurs spécifications en sélectionnant des options à gauche et en indiquant des paramètres de ligne de commande dans le champ de droite. Si vous créez plusieurs spécifications, elles sont liées par des "ET" logiques. Cela signifie que la règle utilisant cet identifiant s'applique si toutes les conditions spécifiées sont remplies.

a. Choisissez parmi les options suivantes :

Général	
Exclure	La règle s'applique sur toutes les lignes de commande qui ne contiennent pas le ou les paramètres indiqués dans le champ de droite.
Sensible à la casse	La règle s'applique uniquement lorsqu'elle trouve le ou les paramètres avec la casse indiquée dans le champ de droite.
Commande	Après le paramètre indiqué, le reste de la ligne de commande est interprété comme une ligne de commande imbriquée. Une ligne de commande imbriquée est introduite par exemple par le paramètre "`-Command`" pour PowerShell ou le paramètre "`/c`" pour cmd.
Type de paramètre	
String	Le paramètre est une chaîne de caractères.
Flag	Le paramètre se trouve dans une option de ligne de commande, commençant par exemple par "`/`" ou "`-`". Par exemple, pour créer un identifiant correspondant à l'éditeur du Registre exécutant silencieusement un fichier *.reg*, c'est-à-dire `regedit /s` en ligne de commande : 1. Créez un critère **Chemin** et indiquez `*\regedit.exe`. 2. Créez un critère **Ligne de commande**, sélectionnez les options **Flag** et **Égal à**, puis entrez le caractère "`s`" dans le champ de droite. Il n'est pas utile d'entrer les caractères "`/`" ou "`-`". Notez que le double tiret "`--`" n'est pas supporté. Par exemple, pour rechercher l'argument "`--arg`", vous devez cocher le type de paramètre **String**.
Vérification	
Égal à	Le paramètre doit être identique à la chaîne de caractères indiquée dans le champ de droite.
Commence par	Le paramètre doit commencer par la chaîne de caractères indiquée dans le champ de droite.
Se termine par	Le paramètre doit se terminer par la chaîne de caractères indiquée dans le champ de droite.
Contient	Le paramètre doit contenir la chaîne de caractères indiquée dans le champ de droite.
Est préfixé par	La valeur reconnue par la règle peut être un préfixe de la chaîne de caractères indiquée dans le champ de droite. Par exemple si vous entrez la chaîne de caractères "version", une correspondance avec les valeurs "v", "ve", "ver", etc. jusqu'à "version" sera reconnue.
Positionnement (visible à partir de la deuxième spécification)	
Aucun	Il n'y a pas de critère de positionnement.
Suivi par	Le paramètre recherché suit le paramètre précédent.

Suivi immédiatement par	Le paramètre recherché suit immédiatement le paramètre précédent.

b. Entrez un ou plusieurs paramètres dans le champ de droite. Dans une même spécification, les paramètres sont liés par des "OU" logiques. Cela signifie que la règle utilisant cet identifiant s'applique si au moins une des conditions spécifiées est remplie.

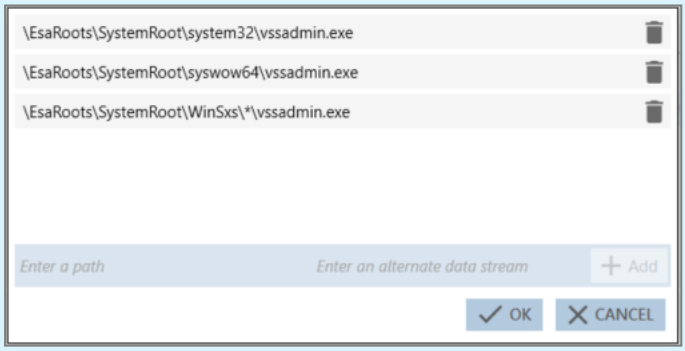
11. Lorsque vous avez créé toutes les spécifications, validez la création du critère "Ligne de commande".
12. Validez la création de l'identifiant.

Cas d'usage

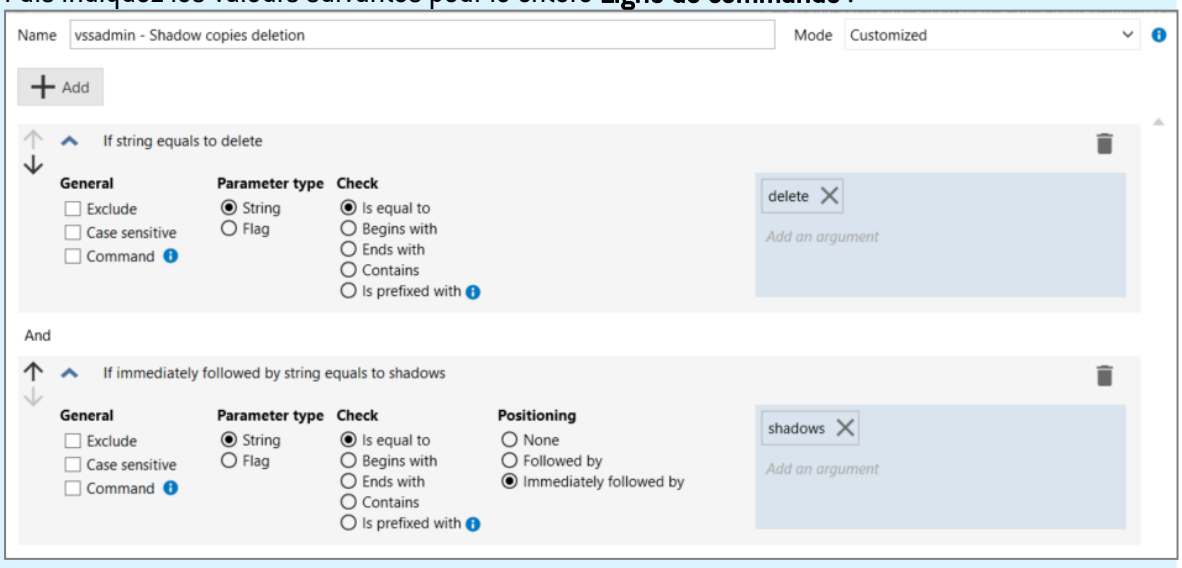
Dans le cadre de la protection anti-ransomware offerte par SES Evolution, ce type de critère permet notamment de définir des règles de type **Création de processus** sur des applications qui tenteraient entre autre de supprimer les clichés instantanés Windows. Or ces clichés instantanés doivent être protégés afin de récupérer les fichiers qui seraient chiffrés par un ransomware. Pour plus d'informations, reportez-vous à la section Gérer une attaque par ransomware. Ces règles sont incluses dans le jeu de règles intégré Protection anti-ransomware.

EXEMPLE

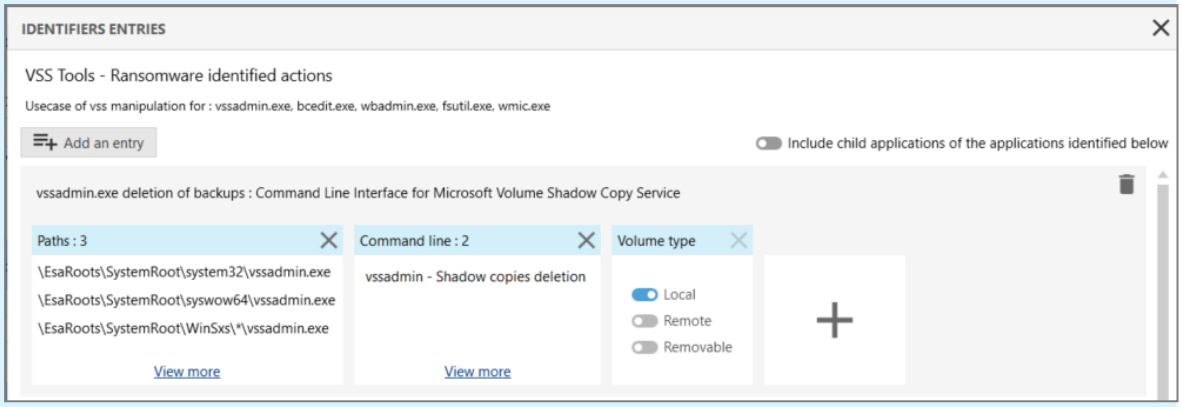
L'utilisation de l'outil VSSAdmin permettant de gérer les clichés instantanés Windows peut être autorisée sur votre parc sauf lorsqu'il tente par exemple de supprimer un cliché instantané. En effet, cette action pourrait être l'œuvre d'un ransomware.
Dans ce cas, créez un identifiant d'applications en indiquant les valeurs suivantes pour le critère **Chemins** :



Puis indiquez les valeurs suivantes pour le critère **Ligne de commande** :



L'identifiant comprend alors l'entrée suivante :



L'identifiant peut être ensuite utilisé dans une règle de type **Création de processus** bloquant et interrompant l'application VSSAdmin lorsqu'une tentative de suppression d'un cliché instantané Windows est détectée.

8.3.2 Créer des identifiants de pilotes

Les identifiants de pilotes permettent de définir les pilotes légitimes que vous souhaitez exclure de la détection de rootkit.

Les identifiants de pilote sont nécessaires lors de la création des règles d'audit de détection de rootkit et vous devez donc les créer au préalable.

Pour plus d'informations, reportez-vous à la section Détection de rootkit.

Les identifiants sont propres aux jeux de règles. Vous devez créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section Exporter et importer des identifiants

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants de pilotes**.
3. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter un identifiant**.
   Un identifiant vide s'affiche en dessous des identifiants existants.
4. Cliquez sur **Modifier** en bas à droite de l'entrée.
5. Dans le champ **Nouvel identifiant de pilotes**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Cliquez sur + et sélectionnez tous les critères d'identifiants que vous souhaitez utiliser. Par exemple **Chemin** et **Hashes**.

7. Cliquez à l'extérieur de la fenêtre des critères et définissez chaque critère d'identification sélectionné :
Chemins
   a. Cliquez sur **Modifier** puis dans le champ bleu en bas saisissez le chemin partiel ou complet du fichier du pilote. Il peut s'agir du chemin dans le système de fichiers ou d'un lien.
   Les caractères * et ? sont autorisés. Par exemple, entrez *\drivers\Stormshield Endpoint Security Agent\es*.sys* pour désigner les pilotes Stormshield.
   Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.
   Stormshield recommande fortement l'utilisation des racines de chemins EsaRoots fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...)*. En effet, ces lettres peuvent différer d'un poste de travail à l'autre.
   b. Vous pouvez aussi préciser un flux de données alternatif (Alternate Data Stream). L'ADS d'un fichier contient des métadonnées et peut permettre entre autres de connaître la provenance du fichier. Reportez-vous à la documentation Microsoft Windows pour en savoir plus.
   c. Cliquez sur **Ajouter**.
   d. Saisissez d'autres chemin dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
   e. Cliquez sur **Valider** pour confirmer la liste de chemins.

   Hashes
   Un hash permet d'identifier très précisément un pilote de confiance : toute modification changera le hash qui ne sera donc plus reconnu. Vous pouvez utiliser l'identification par hash dans les cas suivants :

   - Pour s'assurer qu'un pilote légitime n'est ni remplacé ni modifié. Cependant, cela nécessite une maintenance assez lourde car vous devrez modifier les identifiants à chaque mise à jour logicielle. Elle est donc à réserver pour les systèmes qui subissent très peu changements.
   - Pour identifier les malwares qui changent souvent de nom mais peuvent conserver leur hash. Importez la liste des hashes des malwares les plus courants et bloquez ainsi leur exécution.

   Pour ajouter des hashes :

   a. Cliquez sur **Modifier** puis sur l'icône crayon.
   b. Dans le champ bleu en bas, saisissez le hash MD5, SHA1, ou SHA256 du pilote ainsi qu'une description, puis cliquez sur **Ajouter**.
   Pour obtenir le hash d'un binaire, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le hash SHA256 de tous les fichiers *.sys* :
   ```
   Get-ChildItem -Recurse -Filter '*.sys' | get-filehash -
   Algorithm SHA256 | select path, Hash
   ```
   c. Saisissez d'autres hashes dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
   d. Cliquez sur **Valider**.
   e. Vous pouvez aussi importer une liste de hashes à partir d'un fichier CSV ou txt. Le fichier doit contenir une ligne par hash avec deux informations par ligne, séparées par une virgule, une tabulation ou un point-virgule :
      - Le hash (MD5, SHA1 ou SHA2),
      - La description

En cas d'erreur ou de doublon de hash, SES Evolution le signale et seuls les hashes valides et uniques sont importés.

Une fois les hashes saisis ou importés, la fenêtre affiche le nombre de hashes pour chaque algorithme.

f. Cliquez sur **Valider** pour confirmer la liste des hashes.

Propriétaire

a. Cliquez sur **Modifier**.

b. Dans la liste déroulante en bas, choisissez le type de compte qui lance le pilote identifié (e.g., *NT AUTHORITY\System*), puis cliquez sur **Ajouter**.
Pour obtenir un SID, lancez une fenêtre de commandes avec les droits d'administration et exécutez la commande suivante :

```
WMIC useraccount get name,sid
```

c. Choisissez d'autres comptes si nécessaire et cliquez sur **Ajouter**.

d. Cliquez sur **Valider** pour confirmer la liste des comptes.

Plus vous spécifiez de critères, plus l'identification du pilote est précise car tous les critères doivent correspondre.

8. Cliquez sur **Ajouter une entrée** si vous souhaitez ajouter une autre liste de critères pour le même identifiant. Avoir plusieurs entrées permet de regrouper sous un même identifiant diverses ressources qui sont utilisées par les mêmes règles de sécurité. Par exemple, vous pouvez regrouper tous les pilotes légitimes afin d'établir une liste blanche.
9. Cliquez sur **Valider**.
10. Si vous avez terminé la création des identifiants de pilotes, cliquez sur **Enregistrer** dans le bandeau supérieur.
11. Pour afficher le contenu d'un identifiant de pilotes sans l'éditer, cliquez sur le bouton **Voir**.

8.3.3 Créer des identifiants de réseaux

Les identifiants de réseaux permettent de définir les ressources réseau que vous souhaitez protéger : une adresse IP, un port, une plage d'adresses IP, une plage de ports.

Les identifiants de réseaux sont nécessaires lors de la création des règles Réseau et vous devez donc les créer au préalable.

Les identifiants sont propres aux jeux de règles. Vous devez créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section Exporter et importer des identifiants

Pour plus d'informations, reportez-vous à la section Contrôler l'accès au réseau.

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants de réseaux**.
3. Cliquez sur **Ajouter un identifiant**.
Un identifiant vide s'affiche.
4. Cliquez sur **Modifier** en bas à droite de l'entrée.
5. Dans le champ **Nouvel identifiant de réseaux**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Si vous souhaitez que l'identifiant réseau comprenne toutes les adresses IP SAUF les adresses spécifiées, alors activez l'option **Inverser la portée de l'identifiant**.

7. Par défaut, l'identifiant inclut toutes les adresses IPv4 et IPv6. Pour spécifier des adresses particulières, cliquez sur le texte **Aucune adresse n'a été ajoutée** et entrez manuellement les valeurs dans le champ libre qui s'affiche. Vous pouvez aussi saisir une description si nécessaire.
   - Pour ajouter plusieurs adresses à la fois, séparez-les d'une virgule dans le champ libre et tapez Entrée. Exemple : 192.168.128.254,192.168.95.15.
   - Pour ajouter une plage d'adresses, séparez la première valeur et la dernière valeur par un tiret et tapez Entrée. Exemple : 192.168.131.0-192.168.131.100.
8. Cliquez sur le bouton **Terminer la modification**.
9. Si vous avez terminé la création des identifiants d'applications, cliquez sur **Enregistrer** dans le bandeau supérieur.

8.3.4 Utiliser les racines de chemins dans les identifiants

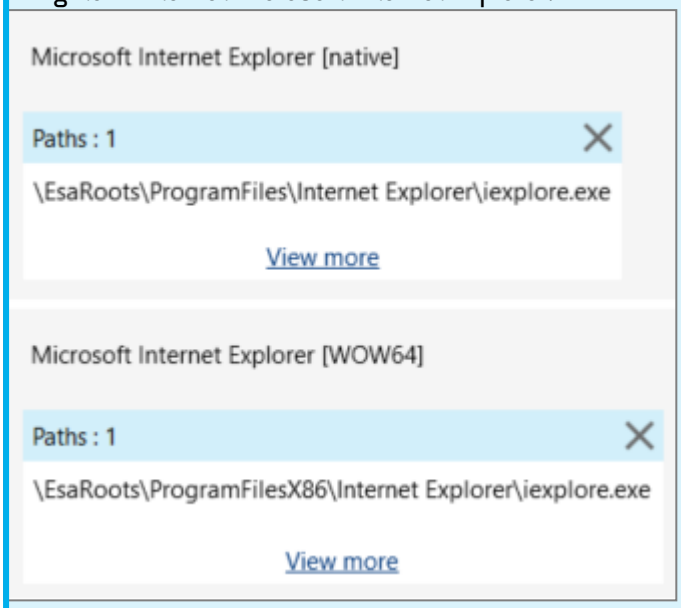
Les postes de travail de votre environnement SES Evolution ne disposent pas tous de la même installation Windows. Par exemple, d'un poste à l'autre, le profil utilisateur ou les applications peuvent se trouver sur des lecteurs différents. SES Evolution fournit des variables sous la forme de racines de chemins qui permettent aux règles de s'adapter à chaque utilisateur, quels que soient ses noms de lecteurs et ses arborescences.

Stormshield recommande fortement l'utilisation de ces racines dans le champ **Chemin** lors de la création d'identifications d'application et de règles fichiers, en particulier pour identifier les applications qui se trouvent dans le dossier *Programmes* ou *System32*.

Utilisez la racine ...	Pour désigner ...
\EsaRoots\SystemDrive	Le volume sur lequel est installé Windows, typiquement C:
\EsaRoots\SystemRoot	Le répertoire Windows, typiquement C:\Windows
\EsaRoots\UserProfiles	Le répertoire Utilisateurs
\EsaRoots\ProgramData	Le répertoire dans lequel les applications stockent des données indépendamment de l'utilisateur
\EsaRoots\ProgramFiles \EsaRoots\ProgramFilesX86	Les répertoires dans lesquels sont installées les applications 64 bits et 32 bits respectivement. Sur un système d'exploitation 32 bits, les deux liens symboliques pointent vers le même emplacement.

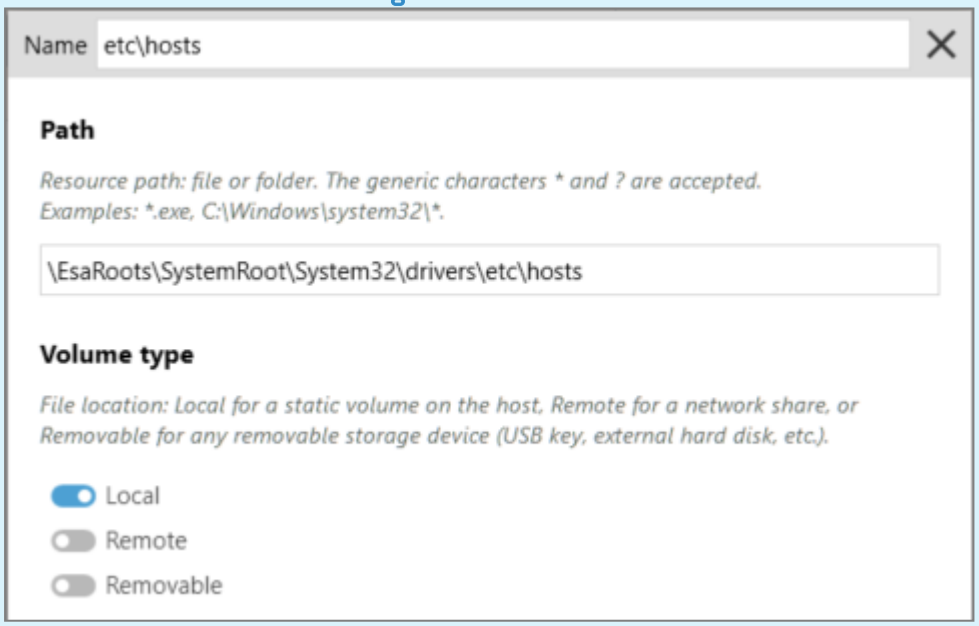
EXEMPLE 1
Utilisez les chemins *\EsaRoots\ProgramFiles\Internet Explorer\iexplore.exe* et *\EsaRoots\ProgramFilesX86\Internet Explorer\iexplore.exe* pour créer l'identifiant d'application du

navigateur internet Microsoft Internet Explorer.



EXEMPLE 2

Utilisez le chemin *\EsaRoots\SystemRoot\System32\drivers\etc\hosts* pour identifier le fichier *hosts* lors de la création d'une règle d'accès aux fichiers.



8.3.5 Exporter et importer des identifiants

Vous pouvez exporter les identifiants d'applications, de pilotes et de réseaux vers un fichier au format *.json* qui pourra ensuite être réimporté. Cela permet par exemple de :

- Utiliser les identifiants créés pour un jeu de règles dans un jeu de règles différent sans avoir à les recréer,
- Transférer la liste des identifiants au Support technique SES Evolution pour faciliter le diagnostic d'un problème.

Vous pouvez exporter/importer séparément les listes d'identifiants d'applications, de pilotes et de réseaux. En revanche, vous ne pouvez pas sélectionner seulement quelques identifiants d'une même liste. Ils sont systématiquement tous exportés/importés.

Exporter une liste d'identifiants

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**, **Identifiants de pilotes** ou **Identifiants de réseaux**.
   La liste des identifiants d'affiche.
3. Cliquez sur **Exporter les identifiants** et choisissez le nom du fichier *.json* et le dossier vers lequel vous souhaitez faire l'export. Tous les identifiants de la liste sont exportés.

Importer une liste d'identifiants

1. Dans le menu **Sécurité > Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**, **Identifiants de pilotes** ou **Identifiants de réseaux**.
   La liste des identifiants s'affiche.
3. Cliquez sur **Importer des identifiants** et choisissez le fichier *.json* que vous souhaitez importer.

8.4 Gérer l'exploitation des vulnérabilités

De nombreuses techniques malveillantes comme par exemple le Heap Spray et la dissimulation de processus sont utilisées par les attaquants pour exploiter les vulnérabilités des postes de travail. Les règles de protection contre les menaces de Stormshield Endpoint Security Evolution permettent de détecter ces techniques d'attaque et/ou de les bloquer efficacement.

Selon la gravité des menaces, certaines protections sont disponibles uniquement dans les jeux de règles d'audit ou uniquement dans les jeux de règles de protection. D'autres sont pertinentes dans les deux cas.

Dans un jeu de règles de protection, la génération d'un contexte est systématique pour la majorité des règles. Dans un jeu de règles d'audit, c'est une option que vous choisissez d'activer ou non.

La politique par défaut de Stormshield (i.e., Default Policy) met en œuvre un certain nombre de règles de protection et d'audit, mais vous pouvez créer vos propres règles personnalisées. Pour chaque type de règle, vous pouvez définir :

- Un comportement par défaut,
- Des comportements spécifiques propres à certaines applications.

Pour plus d'informations sur les jeux de règles d'audit et de protection ainsi que sur les comportements par défaut et spécifiques, reportez-vous à la section Comprendre une politique de sécurité.

À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.

8.4.1 Connaître les différentes menaces et leur protection

SES Evolution fournit des règles pour détecter les principales menaces et s'en protéger. Cette section décrit rapidement les particularités de chaque type de menace. Pour mettre en œuvre

les protections, reportez-vous à la section Configurer la protection contre les menaces.

Dissimulation de processus (Process hollowing)

La protection contre la dissimulation de processus, ou *Process Hollowing*, détecte et bloque les exécutables malveillants qui tentent de se dissimuler sous l'identité d'un processus légitime du système (e.g., explorer.exe), leur permettant d'agir sans être détectés par Windows. Elle agit contre les attaques de type RunPE ou Döppelganging.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Détecter seulement** et ne la désactiver que pour des applications internes bien identifiées qui utilisent légitimement la technique de dissimulation de processus.

Stack Pivot

Une attaque Stack Pivot exploite un débordement de mémoire afin de détourner le flux d'exécution d'une application pour faire exécuter du code malveillant à une application légitime.

La protection contre le Stack Pivot surveille régulièrement la mémoire. Si SES Evolution détecte un comportement anormal sur un agent, notamment un changement d'adresse de pile, il arrête le processus pour empêcher l'exécution du code.

Type de jeu de règles	Protection
Niveau de log	Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Détecter seulement** pour toutes les applications.

Détournement de flux d'exécution (Execution flow hijacking)

La protection contre le détournement de flux d'exécution détecte et neutralise les shellcodes malveillants qui exploitent les débordements de mémoire pour utiliser les adresses des fonctions systèmes dans la librairie dynamique kernel32.dll.

Type de jeu de règles	Protection
Niveau de log	Erreur
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Bloquer et interrompre** pour toutes les applications.

Heap Spray

Le Heap Spray est une technique consistant à allouer de grandes quantités de mémoire afin de permettre l'exécution de code malveillant suite à l'exploitation d'une vulnérabilité. La technique Heap Spray n'étant utilisable que sur les applications 32 bits, la protection de SES Evolution n'est pas activée pour les applications 64 bits.

Type de jeu de règles	Protection
Niveau de log	Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Bloquer et interrompre** pour toutes les applications.

Manipulation des jetons d'accès

Le système d'exploitation attribue à chaque processus un jeton de sécurité, qui contient entre autres le compte avec lequel le processus est exécuté et les privilèges associés à ce processus.

Certaines techniques d'attaque parviennent à dérober ou dupliquer le jeton de sécurité d'un processus plus privilégié, et ainsi à accéder à des ressources ou à des privilèges qui leur sont normalement interdits.

La protection contre la manipulation des jetons fournie par SES Evolution permet de bloquer ce type d'attaque en arrêtant le processus ayant dérobé le jeton.

Type de jeu de règles	Protection
Niveau de log	Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Bloquer et interrompre** pour tous les processus.

Pose de hooks par des applications (Windows Hooks)

L'API SetWindowsHookEx fournie par Windows permet à un programme d'être notifié lorsque certains événements se produisent sur le système ou des applications, par exemple des mouvements de souris, frappes de clavier etc. Pour cela, une DLL est injectée dans les processus cibles.

Ce mécanisme est légitime, mais un attaquant peut l'utiliser pour injecter du code malveillant afin d'observer les opérations de l'utilisateur. Par exemple il peut récupérer des mots de passe via les frappes clavier.

Type de jeu de règles	Protection et Audit
Niveau de log	Protection : Erreur Audit : Information
Génération d'un contexte	Au choix (Oui par défaut)
Recommandations	Désactiver la protection par défaut.

Lorsqu'elle est activée, cette règle contrôle toutes les applications utilisant SetWindowsHookEx. Si vous ne souhaitez pas bloquer toute utilisation de cette API, n'activez pas cette règle mais faites les ajustements au moyen de la règle applicative Enregistreur de frappes.

Élévation de privilèges

Cette protection permet de contrôler les tentatives d'élévation de privilèges effectuées par des applications via l'utilisation du privilège de Debug. Si la protection est activée, SES Evolution compare les droits accordés habituellement à l'application à ceux qu'elle demande. Si elle en

demande davantage, SES Evolution va considérer que c'est une élévation de privilèges et peut bloquer l'action.

Type de jeu de règles	Protection et Audit
Niveau de log	Protection : Erreur Audit : Information
Génération d'un contexte	Au choix (Oui par défaut)
Recommandations	Au choix

Contournement des détections EDR

Cette protection protège contre les attaques de logiciels malveillants qui cherchent à désactiver les modules de détection des EDR (Endpoint Detection and Response), basés sur les technologies AMSI et ETW.

Type de jeu de règles	Protection
Niveau de log	Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Détecter seulement** pour tous les processus.

Fileless attack

Les Fileless attacks ("attaques sans fichier") agissent sans écriture de fichiers malveillants sur les disques des postes de travail. L'attaque a lieu en mémoire.

Cette protection protège contre les processus qui tentent ce type d'attaque.

Type de jeu de règles	Protection
Niveau de log	Alerte
Génération d'un contexte	Systématique
Recommandations	Activer cette protection par défaut en mode **Détecter seulement** pour tous les processus.

Détection de rootkit

Un rootkit est un logiciel qui modifie le comportement du système d'exploitation afin de dissimuler sa propre exécution. Son objectif est d'obtenir et de conserver un accès à un ordinateur, souvent dans un but malveillant.

La détection de rootkit de SES Evolution permet de surveiller le chargement des pilotes et de vérifier leur intégrité.

Type de jeu de règles	Audit
Niveau de log	Urgence
Génération d'un contexte	Au choix (Oui par défaut)
Recommandations	Activer ces règles par défaut et les désactiver uniquement pour les pilotes qui s'avèrent légitimes.

Chargement des pilotes

La protection Chargement des pilotes détecte les pilotes chargés par le système d'exploitation et génère un log pour chacun.

Intégrité des pilotes

La protection Intégrité des pilotes vérifie régulièrement pour chaque pilote si son intégrité n'a pas été potentiellement compromise, i.e., si sa table de fonctions majeures n'a pas été modifiée. Si une modification est détectée, SES Evolution identifie quel pilote est l'auteur de l'attaque et génère un log. Par exemple, un pilote malveillant pourrait modifier un pilote d'antivirus afin de l'empêcher d'analyser les fichiers.

En revanche, certains pilotes effectuent des modifications légitimes, comme certains outils de virtualisation par exemple. Ceux-ci doivent être exclus de la règle d'audit.

Protections avancées

Stormshield fournit également un ensemble de protections avancées contre certains types de menaces, nativement intégrées à la console d'administration.

Les protections avancées permettent de détecter et bloquer des comportements malveillants sur les agents SES Evolution. Elles sont basées sur une analyse heuristique qui peut être mise à jour sans nécessiter la mise à jour logicielle de SES Evolution.

Pour voir les protections avancées dans la console :

1. Choisissez le menu **Sécurité > Politiques**.
2. Cliquez sur **Voir les protections avancées** en haut à droite du panneau d'accueil des politiques.

Pour mettre en œuvre les protections avancées, reportez-vous à la section Configurer la protection contre les menaces.

Les protections avancées possèdent des numéros de version et peuvent être mises à jour par Stormshield lorsque cela est nécessaire. En cas de mise à jour, vous pourrez alors les réimporter dans le panneau **Protections avancées**. Toutes les versions précédentes d'une protection restent disponibles dans la console d'administration.

Ticket Kerberos

Cette protection empêche de récupérer en mémoire les tickets Kerberos qui pourraient être utilisés ultérieurement pour mener une attaque Pass-the-Ticket.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique

ARP Spoofing

Cette protection permet de surveiller l'interception, la modification ou l'arrêt du trafic réseau par des attaques ARP spoofing. L'évaluation de la table ARP est effectuée toutes les 5 minutes.

Type de jeu de règles	Audit
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Au choix (Oui par défaut)

Persistance via WMI

Cette protection empêche des programmes malveillants de persister sur la machine en utilisant WMI (Windows Management Instrumentation).
Elle s'appuie sur les données du journal d'événements *Microsoft-Windows-WMI-Activity/Operational*. Sous Windows 7 et Server 2008, vous devez disposer de la mise à jour Windows KB3191566 pour que ce journal soit présent.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique

Utilisations malveillantes de Certutil

Cette protection protège contre les utilisations malveillantes du programme Windows Certutil, permettant de gérer les certificats. Elle peut générer quelques faux-positifs car elle a besoin d'ouvrir en lecture des fichiers manipulés par Certutil. Si ces fichiers ne sont pas accessibles par manque de droits, l'action sur les certificats est considérée comme malveillante, même si elle est légitime.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique

Découverte de l'environnement

Cette protection empêche l'utilisation d'outils Windows pour collecter des informations sur la machine et le système afin de conduire des opérations malveillantes.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique

Ransomware

Cette protection surveille les modifications et chiffrements de fichiers. Si un certain nombre d'événements de ce type se produit dans un intervalle de trois secondes, elle stoppe le processus responsable. La protection facilite aussi la récupération des données chiffrées par le ransomware en permettant :

- d'identifier les fichiers modifiés par le ransomware,
- de restaurer les fichiers identifiés en s'appuyant sur les clichés instantanés Windows.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Alerte
Génération d'un contexte	Systématique

Usurpation de processus parent (Parent PID Spoofing)

Cette protection empêche le démarrage de programmes qu'un attaquant déclarerait comme enfants de processus existants arbitrairement choisis afin de dissimuler les processus malveillants aux analystes de la sécurité.

Type de jeu de règles	Protection
Niveau de log	Par défaut, Critique
Génération d'un contexte	Au choix (Oui par défaut)

8.4.2 Configurer la protection contre les menaces

Parmi les règles de sécurité fournies par Stormshield, vous pouvez configurer des règles d'audit ou de protection contre les grands types d'attaque qui menacent les postes de travail.

Pour plus d'informations sur les menaces contrées par SES Evolution, reportez-vous à la section Connaître les différentes menaces et leur protection.

Toutes les règles de protection contre les menaces sont désactivées par défaut. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne les activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer la protection contre les menaces et veillez à l'ordre de vos jeux de règles dans la politique. Si vous paramétrez la protection contre les menaces dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage des protections qui serait défini dans les jeux de règles placés après.

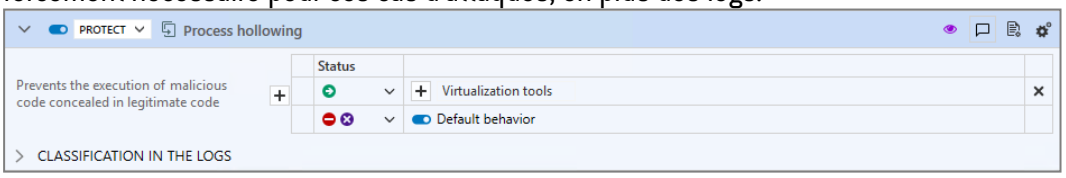
Prérequis

- Pour les règles d'audit Chargement des pilotes et Intégrité des pilotes, vous devez avoir créé au préalable un identifiant de pilote pour chaque pilote légitime à ne pas surveiller. Pour plus d'informations, reportez-vous à la section Créer des identifiants de pilotes.
- Pour tous les autres types de protections, vous devez avoir créé au préalable un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à se soustraire à la protection.
  Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

Créer une règle contre les menaces

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez le jeu de règles de protection ou d'audit dans lequel vous souhaitez ajouter votre règle.
   La page d'accueil du jeu de règles s'affiche.
3. Cliquez sur l'onglet **Menaces**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Activez la règle souhaitée en cliquant sur le bouton  à gauche.

6. Dans le champ **État** de la zone **Comportement par défaut**, trois ou quatre états sont disponibles pour chaque protection. Choisissez :
   - **Autoriser** : SES Evolution ne bloque pas l'action malveillante et ne génère aucun log,
   - **Détecter seulement** : Tout comme avec le mode Audit, SES Evolution détecte l'action malveillante sans la bloquer, et génère des logs pour l'administrateur. Mais contrairement au mode Audit, cette option arrête l'évaluation des règles suivantes qui ne sont pas parcourues.
   - **Bloquer** : SES Evolution bloque l'action malveillante et génère des logs pour l'administrateur,
   - **Bloquer et interrompre** : SES Evolution bloque l'action malveillante et arrête le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** : SES Evolution bloque l'action malveillante, arrête le processus à l'origine de l'action, et met en quarantaine les fichiers suspects. Voir Gérer la mise en quarantaine de fichiers.
     Pour les règles d'audit, les comportements disponibles sont toujours **Autoriser** qui n'entraîne aucune action, et **Audit** qui permet de générer un log puis d'évaluer la règle suivante.
7. Cliquez sur l'icône **+ Ajouter un comportement spécifique** pour ajouter les identifiants des applications pour lesquelles le comportement doit être différent. Par exemple, pour la *dissimulation de processus*, vous pouvez par défaut activer la protection, et la désactiver spécifiquement pour vos applications internes qui utilisent ce mode de fonctionnement, comme les outils de virtualisation.
8. Dans le bandeau supérieur de la règle, vous pouvez :
   - Saisir un commentaire.
   - Indiquer si la règle doit générer un contexte lorsque cela s'applique. Pour certains types de protection, la génération de contextes est automatique car le détail de contexte est forcément nécessaire pour ces cas d'attaques, en plus des logs.



   - Sélectionner les paramètres des logs qui seront émis par cette règle.
   - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.

> **NOTE**
> Si vous souhaitez que les logs soient gérés différemment en fonction des applications, vous devez répartir vos règles dans des jeux de règles différents. En effet, un jeu de règles ne peut pas contenir plusieurs règles pour une même menace.

9. Une fois la première protection configurée, répétez les étapes 5 à 8 pour configurer les autres types de protection.
10. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Configurer les protections avancées

Les protections avancées sont disponibles sur le même panneau que les règles contre les menaces décrites précédemment. Pour plus d'informations, reportez-vous à la section Protections avancées.

Pour activer et configurer les protections avancées :

1. Dans la politique voulue, sélectionnez le jeu de règles de protection ou d'audit dans lequel vous souhaitez ajouter votre règle.
2. Cliquez sur l'onglet **Menaces**.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
4. Activez la règle souhaitée en cliquant sur le bouton  à gauche.
5. Dans la liste déroulante **Version**, indiquez quelle version de la protection vous souhaitez exécuter, soit une version en particulier, soit **Toujours utiliser la dernière version**. Si vous n'utilisez pas la dernière version disponible, l'indicateur  s'affiche à droite de la liste déroulante. Il s'affiche également sur le panneau général d'une politique lorsqu'au moins une protection avancée activée n'utilise pas sa dernière version.
6. Dans le champ **État**, plusieurs états sont disponibles pour chaque protection. Choisissez :
   - **Autoriser** : SES Evolution ne bloque pas l'action malveillante et ne génère aucun log,
   - **Détecter seulement** : Tout comme avec le mode Audit, SES Evolution détecte l'action malveillante sans la bloquer, et génère des logs pour l'administrateur. Mais contrairement au mode Audit, cette option arrête l'évaluation des règles suivantes qui ne sont pas parcourues.
   - **Bloquer** : SES Evolution bloque l'action malveillante et génère des logs pour l'administrateur,
   - **Bloquer et interrompre** : SES Evolution bloque l'action malveillante et arrête le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** : SES Evolution bloque l'action malveillante, arrête le processus à l'origine de l'action, et met en quarantaine les fichiers suspects. Voir Gérer la mise en quarantaine de fichiers.
7. Dans le bandeau supérieur de la règle, vous pouvez :
   - Sélectionner la version de la protection. Toutes les versions sont conservées en base de données et restent disponibles dans la console d'administration.
   - Saisir un commentaire.
   - Sélectionner les paramètres des logs qui seront émis par cette règle.
   - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.

8. Les règles contre les menaces **Persistance via WMI**, **Utilisations malveillantes de Certutil**, **Découverte de l'environnement**, **Ransomware** et **Usurpation de processus parent** possèdent des paramètres spécifiques à chacune :

Persistance via WMI	Liste de compatibilités : listez ici les consommateurs représentant des événements WMI légitimes et qui ne doivent pas être bloqués par la protection.
Utilisations malveillantes de Certutil	Liste de compatibilités : ajoutez ici des identifiants d'applications qui pourraient utiliser *certutil.exe* dans des cas légitimes et qui ne doivent pas être bloquées par la protection.
Découverte de l'environnement	• Intervalle de temps : indiquez l'intervalle de temps en secondes (minimum cinq secondes) entre la première commande et la dernière commande et après lequel les actions de découverte doivent être ignorées. • Liste de compatibilités : ajoutez ici des identifiants d'applications autorisées à lancer des commandes s'apparentant à des actions de découverte et qui ne doivent pas être bloquées par la protection. • Seuil de sensibilité : sélectionnez le seuil à partir duquel se déclenche la protection.
Ransomware	• Liste de compatibilités : ajoutez ici des identifiants d'applications de chiffrement légitimes qui ne doivent pas être bloquées par la protection, comme par exemple *Stormshield Data Security*. • Seuil de sensibilité : sélectionnez le seuil à partir duquel se déclenche la protection. Avec le niveau **Très bas**, la protection se déclenche si au moins 20 fichiers ont été chiffrés par un ransomware en moins de 3 secondes. Avec le niveau **Bas**, c'est à partir de 15 fichiers, et avec le niveau **Moyen** 10 fichiers. Si vous activez cette protection anti ransomware, assurez-vous aussi d'Activer les clichés instantanés Windows pour pouvoir restaurer d'éventuels fichiers perdus. Pour plus d'informations sur la procédure de restauration, reportez-vous à la section Gérer une attaque par ransomware.
Usurpation de processus parent (Parent PID Spoofing)	Liste de compatibilités : ajoutez ici des identifiants d'applications qui auront le droit de réaliser de l'usurpation de processus parent sans être bloquées par la protection.

9. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

NOTE
Si vous souhaitez modifier plus tard la version utilisée d'une protection avancée, un déploiement est nécessaire après la modification.

8.5 Définir les règles de contrôle d'accès

Afin de protéger les ressources et les machines, SES Evolution permet de contrôler les accès à la base de registre, aux fichiers, aux processus, aux réseaux, aux volumes, aux périphériques et aux points d'accès Wi-Fi. Pour cela, vous devez créer des jeux de règles de sécurité permettant de contrôler ces accès et constituant une politique de sécurité.

Pour chaque règle, vous pouvez définir :

- Un comportement par défaut pour toutes les applications par rapport à la ressource visée par la règle,
- Des comportements spécifiques propres à certaines applications.

Pour plus d'informations sur les comportements, reportez-vous à la section Utiliser le comportement par défaut et les comportements spécifiques des règles.

L'ordre des règles dans une politique est important, car dès lors qu'une règle s'applique, les règles suivantes peuvent ne pas être parcourues. Les règles les plus spécifiques doivent donc être placées avant les règles plus générales. Pour plus d'informations sur l'ordre des règles, reportez-vous à la section Ordonner les jeux de règles et les règles dans une politique.

Les règles de contrôle d'accès sont créées dans le menu **Sécurité > Politiques** de la console, dans les onglets **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** des jeux de règles.

La plupart des règles de contrôle d'accès fonctionnent sur le même principe :

- Dans la partie gauche de la règle, vous définissez les ressources visées par la règle,
- Dans la partie droite de la règle, vous définissez les acteurs de la règle (comportement spécifique) et vous leur octroyez ou non des droits d'accès aux ressources visées. Les actions possibles sur les ressources diffèrent pour chaque type de règle et selon que vous êtes dans un jeu de règles de protection ou un jeu de règles d'audit. Dans les jeux de règles d'audit, les comportements disponibles pour chaque action sont systématiquement **Autoriser** et **Audit**.

Dans les deux cas, les ressources et les acteurs sont représentés par des identifiants que vous devez avoir créés au préalable ou que vous créez directement dans la règle pour certains types de règle. Pour plus d'informations, reportez-vous à la section Créer des identifiants.

À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.

8.5.1 Contrôler la création de processus

Un programme malveillant peut agir en créant des processus lui-même, ou par l'intermédiaire d'une application tierce.

SES Evolution permet de se protéger contre ce type d'attaque.

Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les processus à protéger et pour les processus légitimes autorisé à créer d'autres processus. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

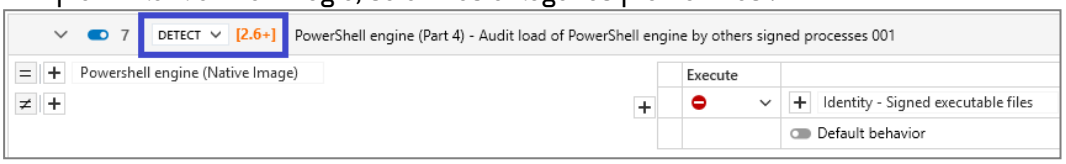
Créer une règle sur la création de processus

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Création de processus**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter > Règle (Création de processus)**.
   Une nouvelle ligne s'affiche.
6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez le ou les processus à protéger.
7. Cliquez sur l'icône  pour choisir le ou les processus à exclure de la protection.

8. Dans le champ **Création** de la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles :
   - **Autoriser** pour autoriser par défaut l'action,
   - **Bloquer** pour bloquer par défaut l'action,
   - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
   - **Demander** pour que l'utilisateur soit consulté.
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
   - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
9. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez le ou les processus à exclure du comportement par défaut. Dans le champ **Création** associé, choisissez le comportement souhaité.

10. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

11. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

EXEMPLE
Vous pouvez restreindre la création du processus *rundll32* aux seules applications Microsoft. Dans ce cas, choisissez *rundll32* dans les processus à protéger, sélectionnez **Bloquer** dans le comportement par défaut, puis autorisez les applications Microsoft dans les comportements spécifiques.

8.5.2 Contrôler l'exécution de code

Cette protection permet d'autoriser ou d'interdire le chargement de code exécutable provenant de fichiers exécutables ou de librairies (DLL).

Les fichiers ou librairies en question sont identifiés dans les règles par un chemin, un flux de données alternatif, un propriétaire et/ou un type de volume.

EXEMPLE
Ces règles permettent par exemple d'autoriser seulement l'exécution de binaires installés par le système d'exploitation ou par les administrateurs du parc, ou bien d'empêcher des applications dangereuses d'exécuter certaines DLL.

Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées ou non à exécuter un fichier ou une librairie. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

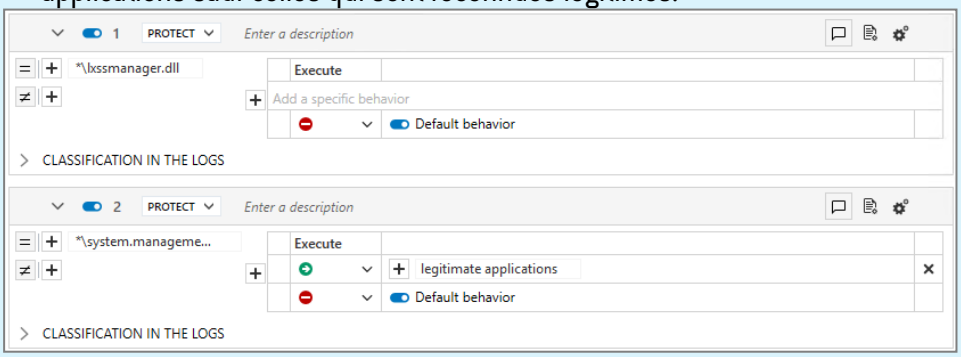
Créer une règle sur l'exécution de code

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Exécution de code**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter > Règle (Exécution de code)**. Une nouvelle ligne s'affiche.

6. Dans la zone de gauche, cliquez sur l'icône [=] [+] pour afficher la fenêtre de création de l'identifiant du ou des fichiers exécutables ou DLL pour lesquels vous souhaitez contrôler l'accès.
   - Et/ou -
   Cliquez sur l'icône [≠] [+] pour afficher la fenêtre de création de l'identifiant du ou des fichiers exécutables ou DLL que vous souhaitez exclure du contrôle d'accès.
7. Saisissez le nom de l'identifiant.
8. Saisissez un chemin, une extension ou bien un nom de fichier exécutable ou DLL. Ce champ peut contenir les caractères génériques "?" et "*".
9. Choisissez le type de volume sur lequel se trouve le fichier ou la DLL.
10. Dans les paramètres avancés, vous avez la possibilité de préciser le compte Windows propriétaire des fichiers, à condition que ceux-ci soient situés sur un volume local. Vous pouvez également entrer directement un identifiant de sécurité (SID) pour indiquer un compte Windows personnel. Cette option permet d'autoriser ou de bloquer l'exécution de fichiers ou DLL détenus par certains comptes.
11. Vous avez également la possibilité de spécifier un flux de données alternatif. Le flux de données alternatif (Alternate Data Stream) d'un fichier contient des métadonnées et permet entre autres de connaître la provenance du fichier. Par exemple, spécifier le flux de données alternatif "zone.identifier" permet d'établir des règles pour les fichiers provenant d'Internet. Le flux de données alternatif pourrait également être un vecteur d'attaque en abritant du code malveillant. Ce champ peut contenir les caractères génériques "?" et "*".
12. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.

EXEMPLES

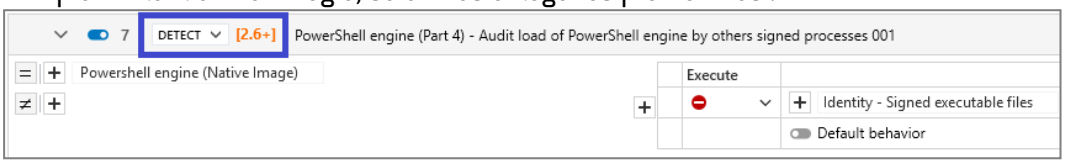
- Bloquez l'exécution de la DLL *\lxssmanager.dll* pour toutes les applications.
- Bloquez l'exécution de la DLL *\system.management.automation.dll* pour toutes les applications sauf celles qui sont reconnues légitimes.



13. Dans le champ **Exécution** de la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles : :
    - **Autoriser** pour autoriser par défaut l'action,
    - **Bloquer** pour bloquer par défaut l'action,
    - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
    - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
    - **Demander** pour que l'utilisateur soit consulté.
    - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
    - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
    - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
    - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
14. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Dans le champ **Exécution** associé, choisissez le comportement souhaité.

15. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

16. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
17. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.3 Contrôler l'accès aux processus

Un programme malveillant peut agir en accédant à des processus légitimes pour récupérer des informations sensibles ou y injecter du code malveillant.

Les règles d'accès aux processus de SES Evolution permettent de se protéger contre ce type d'attaque sans bloquer totalement les accès inter-processus dont certains sont légitimes.

Il n'est pas possible de bloquer totalement l'accès à un processus ou à un thread d'un processus mais vous pouvez restreindre les droits accordés lors de cette opération.

Ces règles ne s'appliquent qu'aux applications. Elles ne s'appliquent pas aux pilotes.

EXEMPLE
Bloquer l'accès à la mémoire d'un processus permet d'empêcher de voler les mots de passe dans la mémoire d'un navigateur lorsqu'il est ouvert.
Retrouvez d'autres exemples à la fin de cette section.

Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les processus à protéger et pour les processus légitimes autorisés à accéder à d'autres processus. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

Créer une règle d'accès aux processus

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif** > **Accès aux processus**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Accès aux processus)**.
   Une nouvelle ligne s'affiche.
6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez le ou les processus à protéger.
7. Cliquez sur l'icône  et choisissez le ou les processus à exclure de la protection.

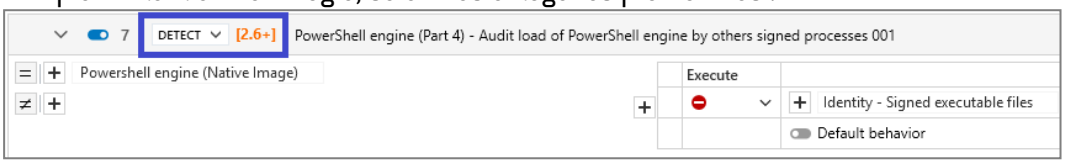
8. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque action (dans un jeu de règles d'audit, seule l'action **Lecture** est paramétrable) :
   - **Lecture** : choisissez l'action de la règle en cas de lecture de la mémoire du processus.
   - **Modification** : choisissez l'action de la règle en cas de modification de la mémoire du processus.
   - **Altération du flux d'exécution** : un programme qui prend le contrôle d'un processus peut modifier son pointeur d'exécution. Choisissez l'action de la règle en cas d'altération du flux d'exécution du processus.
   - **Duplication de handle** : choisissez l'action de la règle lorsqu'un processus tente de dupliquer une ressource appartenant à un autre processus.

   La liste de tous les comportements est décrite ci-dessous :
   - **Autoriser** pour autoriser par défaut l'action,
   - **Bloquer** pour bloquer par défaut l'action,
   - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
   - **Demander** pour que l'utilisateur soit consulté.
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
   - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.

9. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez le ou les processus à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.

10. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

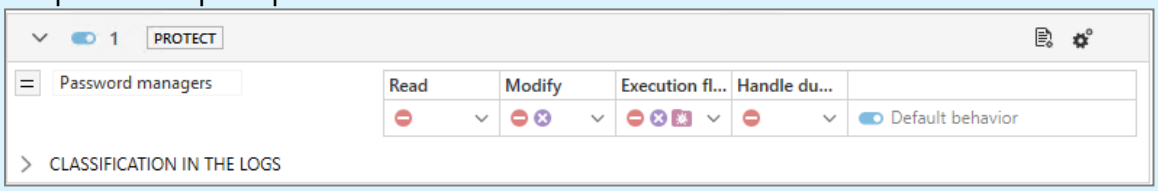
  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

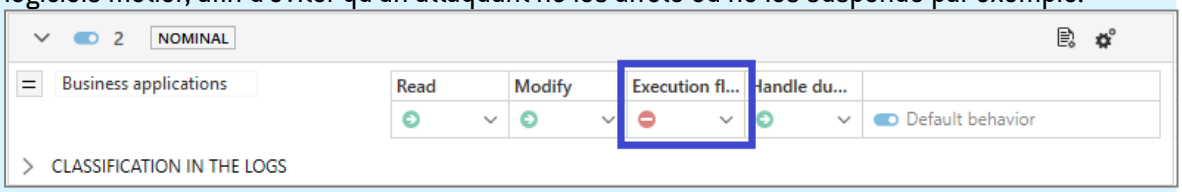
11. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

EXEMPLES

Vous pouvez interdire à toute application l'accès au gestionnaire de mots de passe, afin d'éviter qu'un attaquant n'accède aux mots de passe ou n'injecte du code dans son processus. Dans ce cas, choisissez le gestionnaire de mots de passe dans les processus à protéger et sélectionnez **Bloquer** pour toutes les actions dans le comportement par défaut. Ne définissez aucun comportement spécifique.



Vous pouvez aussi bloquer l'altération du flux d'exécution d'applications importantes comme des logiciels métier, afin d'éviter qu'un attaquant ne les arrête ou ne les suspende par exemple.



8.5.4 Se protéger contre l'injection de code

L'injection de code permet à une application de faire exécuter du code par une autre. SES Evolution permet de protéger vos applications contre l'injection de code malveillant.

EXEMPLE

Deux approches sont possibles, illustrées par les cas d'usage suivants :

- Cas d'usage 1 : Aucune application n'est autorisée à injecter du code, sauf certaines applications légitimes bien identifiées (e.g., antivirus, gestionnaire d'erreurs Windows). Il s'agit du cas le plus courant.
- Cas d'usage 2 : Aucune application n'est autorisée à injecter du code dans le gestionnaire de mots de passe.

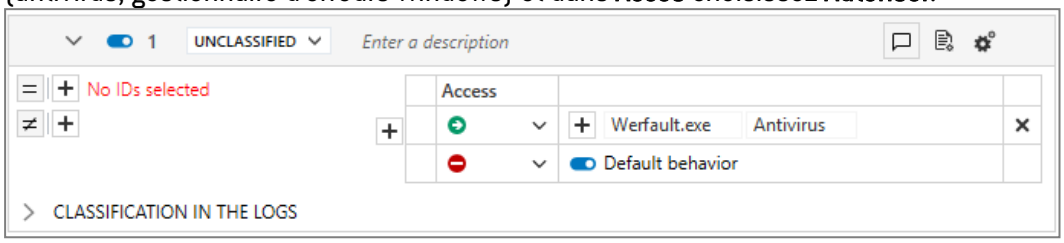
Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à faire de l'injection de code légitime. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

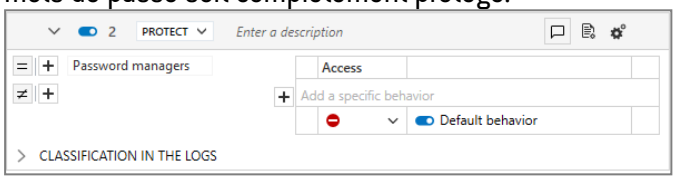
Créer une règle de protection contre l'injection de code

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif** > **Injection de code**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Injection de code)**.
   Une nouvelle ligne s'affiche.
6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez la ou les applications concernées par le comportement par défaut.
   Pour le cas d'usage 1, n'ajoutez pas d'application car vous souhaitez toutes les protéger.
   Pour le cas d'usage 2, ajoutez le gestionnaire de mots de passe.
7. Cliquez sur l'icône  pour choisir le ou les processus à exclure de la protection.
8. Dans le champ **Accès** de la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles : :
   - **Autoriser** pour autoriser par défaut l'action,
   - **Bloquer** pour bloquer par défaut l'action,
   - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
   - **Demander** pour que l'utilisateur soit consulté.
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
   - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.

9. Cliquez sur l'icône + **Ajouter un comportement spécifique** et choisissez la ou les applications que vous souhaitez exclure du comportement par défaut.
Pour le cas d'usage 1, ajoutez ici les applications qui font de l'injection de code légitime (antivirus, gestionnaire d'erreurs Windows) et dans **Accès** choisissez **Autoriser**.

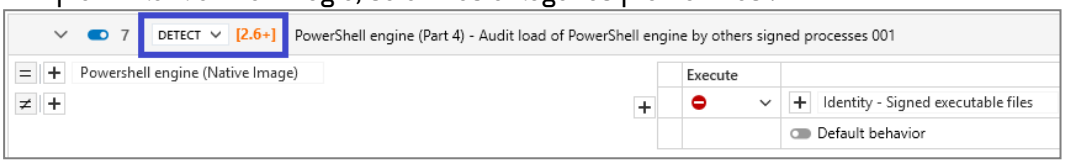


Pour le cas d'usage 2, n'ajoutez pas d'application car vous souhaitez que le gestionnaire de mots de passe soit complètement protégé.



10. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

11. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.5 Se protéger contre les enregistreurs de frappes

Un enregistreur de frappes, ou programme de keylogging, permet à un attaquant de récupérer toutes les frappes clavier afin de subtiliser des mots de passe, des informations confidentielles, etc. Il agit sur des applications ciblées.

SES Evolution empêche l'application qui est au premier plan de transmettre ses frappes clavier aux autres applications. En revanche, elle peut recevoir ses propres frappes clavier.

Afin de vous protéger de manière plus globale contre toute utilisation de l'API SetWindowsHookEx, activez plutôt la protection contre la Pose de hooks par des applications. Pour plus d'informations, reportez-vous aux sections Pose de hooks par des applications (Windows Hooks) et Configurer la protection contre les menaces.

EXEMPLE
Vous pouvez utiliser cette protection pour interdire l'enregistrement des frappes des navigateurs web, gestionnaires de mots de passe, et de l'explorateur de fichiers Windows. Autorisez-les seulement pour les applications légitimes de type outils de virtualisation et outils de prise en main à distance.

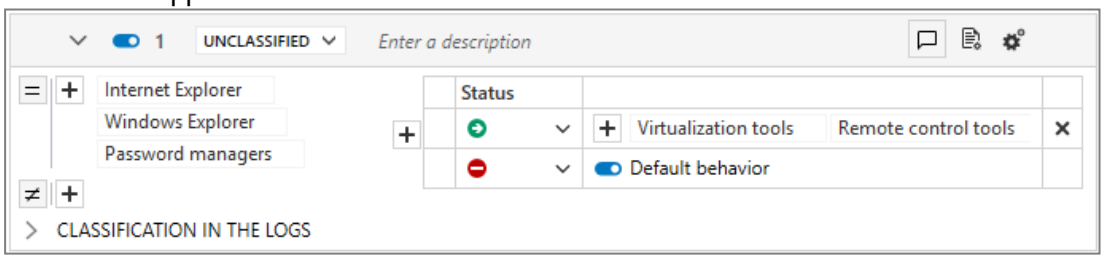
Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à faire du keylogging. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

Créer une règle de protection contre les enregistreurs de frappes

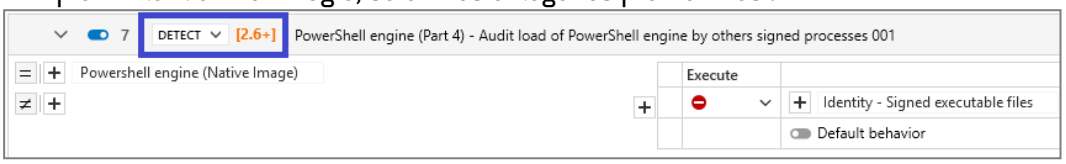
1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Enregistreur de frappes**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter > Règle (Enregistreur de frappes)**.
   Une nouvelle ligne s'affiche.
6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez la ou les applications à protéger.
   Par exemple, ajoutez *Internet Explorer*, *Windows Explorer* et le *gestionnaire de mots de passe*.

7. Cliquez sur l'icône ≠ + pour choisir la ou les applications à exclure de la protection.
8. Dans le champ **État** de la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles : :
   - **Autoriser** pour autoriser par défaut l'action,
   - **Bloquer** pour bloquer par défaut l'action,
   - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
   - **Demander** pour que l'utilisateur soit consulté.
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
   - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
9. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les applications à autoriser.
   Par exemple, ajoutez ici les applications qui font du keylogging légitime, par exemple les *outils de prise en main à distance*, et dans **État** choisissez **Autoriser** pour que la protection autorise ces applications.



10. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

11. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.6 Contrôler l'accès aux fichiers

Cette protection permet de contrôler les accès aux fichiers réalisés par des applications données. Les fichiers sont identifiés dans les règles par un chemin, un flux de données alternatif, un propriétaire et/ou un type de volume.

EXEMPLE
Vous pouvez protéger tous vos fichiers Microsoft Office et autres fichiers sensibles afin qu'ils puissent être modifiés uniquement par des applications légitimes comme l'explorateur Windows, la suite Office, les outils Windows, etc. Les autres applications n'auront accès à ces fichiers qu'en lecture seule.

Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées à accéder aux fichiers et pour celles que vous souhaitez bloquer. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

Créer une règle d'accès aux fichiers

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL** > **Fichier**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Fichiers)**.
   Une nouvelle ligne s'affiche.
6. Dans la zone de gauche, cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant du ou des fichiers pour lesquels vous souhaitez contrôler l'accès.
   - Et/ou -
   Cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant du ou des fichiers que vous souhaitez exclure du contrôle d'accès.
7. Saisissez le nom de l'identifiant.

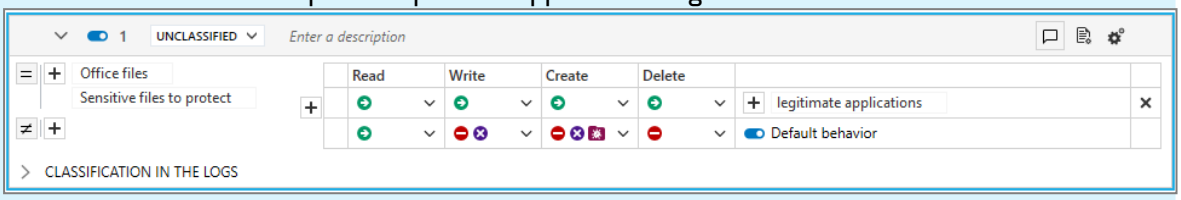
8. Saisissez un chemin de fichier, une extension de fichier ou bien un fichier. Ce champ peut contenir les caractères génériques "?" et "*".
   Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.
   Stormshield recommande fortement l'utilisation des racines de chemins EsaRoots fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...)*. En effet, ces lettres peuvent différer d'un poste de travail à l'autre.

   > **NOTE**
   > Vous pouvez saisir un chemin comprenant une lettre de lecteur local (disque dur, SSD) dans ce champ. Cependant, si un utilisateur modifie la lettre d'un lecteur ou en ajoute un, vous devez redémarrer le poste ou modifier la politique appliquée par l'agent pour que le lecteur soit détecté.

9. Choisissez le type de volume sur lequel se trouve le fichier ou le type de fichier.
10. Dans les paramètres avancés, vous avez la possibilité de préciser le compte Windows propriétaire des fichiers, à condition que ceux-ci soient situés sur un volume local. Vous pouvez également entrer directement un identifiant de sécurité (SID) pour indiquer un compte Windows personnel. Cette option permet d'autoriser ou de bloquer l'accès à des fichiers détenus par certains comptes.
11. Vous avez également la possibilité de spécifier un flux de données alternatif. Le flux de données alternatif (Alternate Data Stream) d'un fichier contient des métadonnées et permet entre autres de connaître la provenance du fichier. Par exemple, spécifier le flux de données alternatif "zone.identifier" permet d'établir des règles pour les fichiers provenant d'Internet. Le flux de données alternatif pourrait également être un vecteur d'attaque en abritant du code malveillant. Ce champ peut contenir les caractères génériques "?" et "*".
12. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.
13. Dans la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles : :
    - **Autoriser** pour autoriser par défaut l'action,
    - **Bloquer** pour bloquer par défaut l'action,
    - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
    - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
    - **Demander** pour que l'utilisateur soit consulté.
    - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
    - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
    - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
    - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
14. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.

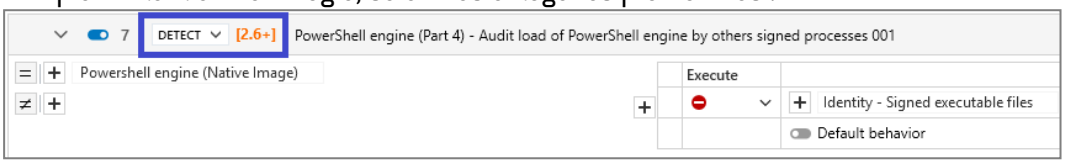
EXEMPLE

Bloquez par défaut la modification ou suppression de fichiers Office et autres fichiers sensibles. Autorisez ces actions uniquement pour les applications légitimes.



15. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

16. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
17. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.7 Contrôler l'accès à la base de registre

Cette protection permet de contrôler l'accès aux clés et valeurs en base de registre réalisé par des applications données. Elle permet ainsi de protéger l'accès à certaines clés particulièrement sensibles, qui pourraient être ciblées par des programmes malveillants.

EXEMPLE
Pour éviter qu'un malware ne désactive les outils de sécurité Windows via la base de registre, vous pouvez protéger leurs clés de registre afin qu'elles ne puissent être modifiées que par des applications légitimes de Windows.

Chaque chemin de registre peut être un chemin complet ou bien contenir les caractères génériques "?" et "*".

Prérequis

Vous devez au préalable avoir créé les identifiants d'applications pour les applications autorisées à accéder au registre et pour celles que vous souhaitez bloquer. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

Créer une règle d'accès au registre

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL** > **Registre**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Registre)**.
   Une nouvelle ligne s'affiche.
6. Dans la zone de gauche, cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant des clés de registre dont vous souhaitez contrôler l'accès.
   - Et/ou -
   Cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant des clés de registre que vous souhaitez exclure du contrôle d'accès.
7. Saisissez le nom de l'identifiant.

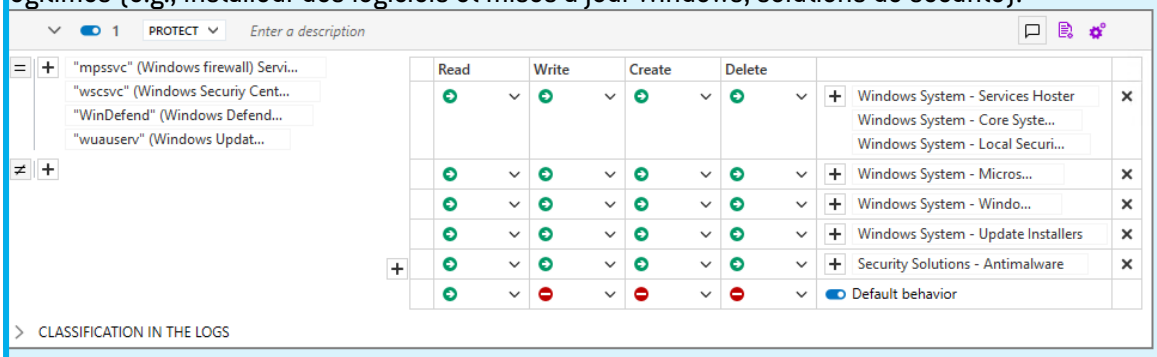
8. Indiquez le chemin vers la clé.

> **ASTUCE**
> Vous pouvez copier le chemin de la clé depuis la base de registre et le coller dans le champ **Clé**.

9. Choisissez le champ d'application :
   - **Clé et Valeurs**. Ces règles répondent au besoin de protection les plus courants. Si vous n'indiquez pas de valeur, toutes les valeurs de la clé sont protégées, ainsi que la clé elle-même. Si vous n'indiquez qu'une seule valeur, les autres valeurs de la clé ne sont pas protégées.
   - **Clé** : Ces règles relèvent d'une protection plus avancée. Seule la clé est protégée. Ses valeurs ne le sont pas.
   - **Valeurs** : Ces règles relèvent également d'une protection plus avancée. Seules les valeurs sont protégées. La clé elle-même n'est pas protégée par la règle. Par exemple, même si les valeurs d'une clé sont protégées contre la suppression, si la suppression de la clé elle-même est autorisée, les valeurs pourraient être supprimées avec la clé.
10. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.
11. Dans la zone **Comportement par défaut**, choisissez un comportement parmi ceux disponibles pour ce type de règles : :
    - **Autoriser** pour autoriser par défaut l'action,
    - **Bloquer** pour bloquer par défaut l'action,
    - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
    - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
    - **Demander** pour que l'utilisateur soit consulté.
    - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
    - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
    - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
    - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
12. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.

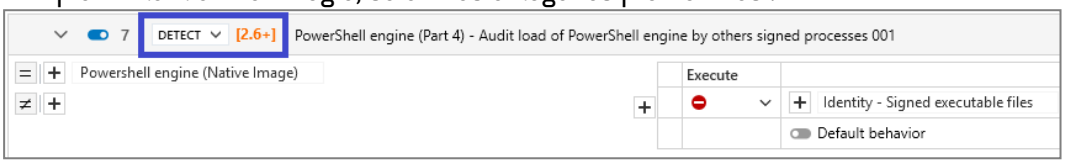
> **EXEMPLE**
> Bloquez par défaut l'accès aux clés de registre des outils de sécurité de Windows, tels que Windows Defender, Windows Firewall, etc. Autorisez ces actions seulement pour les processus

égitimes (e.g., Installeur des logiciels et mises à jour Windows, solutions de sécurité).



13. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

14. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
15. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

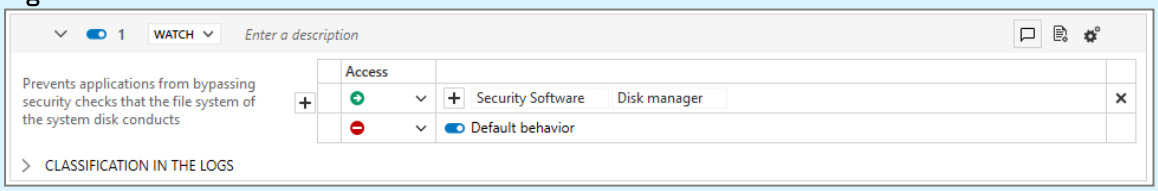
8.5.8 Contrôler l'accès au volume

Cette protection permet d'empêcher une application de contourner les vérifications de sécurité du système de fichiers du disque système et d'accéder directement au volume en raw.

Dans les règles, vous avez la possibilité d'autoriser ou d'empêcher les applications de votre choix à accéder au volume en raw.

En mode liste blanche, une seule règle peut suffire pour autoriser l'accès pour certaines applications et le bloquer pour toutes les autres. Si vous souhaitez sélectionner des paramètres de logs différents, vous devez alors créer plusieurs règles. Dans ce cas, activez le comportement par défaut "Bloquer" dans la dernière règle seulement.

EXEMPLE
Exemple de règle interdisant l'accès au volume à toutes les applications sauf aux applications légitimes :



Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées ou non à accéder au volume en raw. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

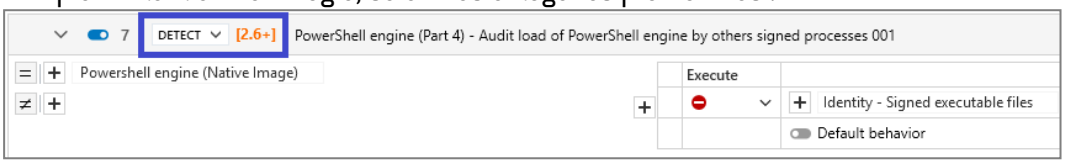
Créer une règle d'accès au volume

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL > Volume**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter >Règle (Volume)**. Une nouvelle ligne s'affiche.

6. Dans le champ **Accès** de la zone **Comportement par défaut**, choisissez le comportement qui s'applique à toutes les applications susceptibles d'accéder au volume en raw, pour une règle de protection :
   - **Autoriser** pour autoriser par défaut l'action,
   - **Bloquer** pour bloquer par défaut l'action,
   - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
   - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
   - **Demander** pour que l'utilisateur soit consulté.
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
   - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
7. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Dans le champ **Accès** associé, choisissez le comportement souhaité.

8. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

9. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
10. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.9 Contrôler l'accès au réseau

Cette protection permet de contrôler les accès aux réseaux entrants ou sortants réalisés par des applications données.

Elle permet de filtrer sur :

- Les événements réseau "bind", "accept" (règle Serveur) et "connect" (règle Client),
- Les protocoles TCP et UDP,
- Des ports donnés,
- Des adresses IPv4 ou IPv6 données.

Il n'est pas nécessaire d'ouvrir explicitement les communications entre le serveur SES Evolution et les agents. En effet, le mécanisme d'autoprotection de l'agent garantit qu'aucune règle de sécurité, quelle qu'elle soit, ne puisse bloquer ces communications.

EXEMPLE
Les règles réseau permettent par exemple de :

- Protéger un serveur en contrôlant les accès à la machine,
- Forcer les utilisateurs d'un service de l'entreprise à utiliser une application spécifique pour accéder à une ressource réseau donnée.

Prérequis

Vous devez au préalable avoir créé :

- Les identifiants d'applications pour les applications autorisées ou ne pouvant pas accéder au réseau. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.
- Les identifiants de réseaux pour les adresses IP que vous souhaitez protéger. Pour plus d'informations, reportez-vous à la section Créer des identifiants de réseaux.

Créer une règle d'accès au réseau

Il existe deux types de règles : des règles Client et des règles Serveur.

- Dans le cadre d'un jeu de règles s'appliquant à des postes de travail, les règles Client permettent d'autoriser ou non les applications à se connecter sur des ressources distantes (champ **Distant**), en contrôlant l'événement réseau "connect". Elles permettent aussi de s'adresser à des sous-réseaux spécifiques par exemple (champ **Local**).
- Dans le cadre d'un jeu de règles s'appliquant à des serveurs, les règles Serveur permettent d'autoriser ou non les applications à ouvrir des ports et à accepter les connexions entrantes (champ **Local**), en contrôlant les événements réseau "bind" et "accept". Elles permettent aussi de spécifier la provenance des connexions (champ **Distant**).

Pour créer une règle d'accès au réseau :

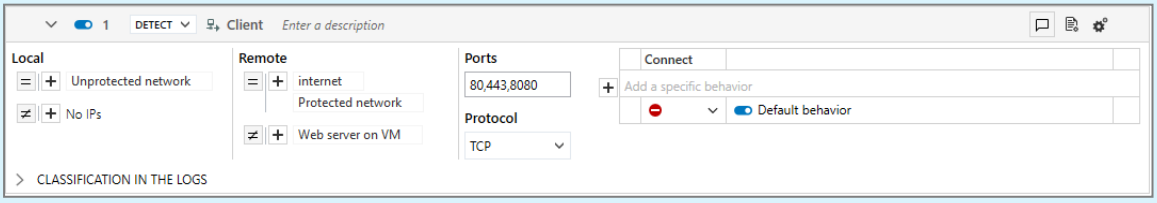
1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Réseaux > Firewall**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Choisissez d'ajouter une règle réseau Client ou une règle réseau Serveur en cliquant sur un des boutons **Ajouter**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, choisissez le ou les identifiants de réseaux des ressources à protéger :
   - **Local**  : Ressource locale concernée par la règle. Par exemple, si le poste de travail dispose de plusieurs cartes réseau, vous pouvez préciser laquelle est concernée.
   - **Local**  Ressource locale exclue de la règle.
   - **Distant**  : Ressource distante concernée par la règle. Par exemple, vous pouvez spécifier la Zone internet.
   - **Distant**  : Ressource distante exclue de la règle.
7. Dans le champ **Ports**, indiquez les ports concernés par la règle réseau. Il s'agit des ports de destination pour les règles Client et des ports locaux pour les règles Serveur.
   - Pour ajouter plusieurs ports à la fois, séparez-les d'une virgule. Exemple : 8080,8081.
   - Pour ajouter une plage de ports, séparez la première valeur et la dernière valeur par un tiret. Exemple : 80-90.
   - Pour spécifier que tous les ports sont concernés, laissez le champ vide.
8. Choisissez le protocole de transport TCP ou UDP, ou bien les deux.

9. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque événement réseau Connect, Accept ou Bind :
   - **Accept** (pour une règle Serveur): interdit ou autorise les applications spécifiées à recevoir des connexions entrantes sur la ou les ressources réseau indiquées,
   - **Bind** (pour une règle Serveur) : interdit ou autorise les applications spécifiées à ouvrir des connexions sur la ou les ressources réseau indiquées,
   - **Connect** (pour une règle Client) : interdit ou autorise les applications spécifiées à se connecter sur la ou les ressources réseau indiquées.

     Les comportements possibles dans une règle de protection sont les suivants :
     - **Autoriser** pour autoriser par défaut l'action,
     - **Bloquer** pour bloquer par défaut l'action,
     - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
     - **Bloquer, interrompre et mettre en quarantaine** pour bloquer par défaut l'action, arrêter le processus à l'origine de l'action, et mettre en quarantaine les fichiers suspects. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.
     - **Demander** pour que l'utilisateur soit consulté.
     - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
     - **Ne pas évaluer la règle** pour ignorer la règle contenue dans ce jeu de règles et évaluer la règle suivante.
     - **Ne pas évaluer le groupe de règles** pour ignorer les règles contenues dans le groupe de règles et évaluer le groupe de règles ou la règle suivants.
     - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
10. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les identifiants d'application correspondant aux ressources à exclure du comportement par défaut.

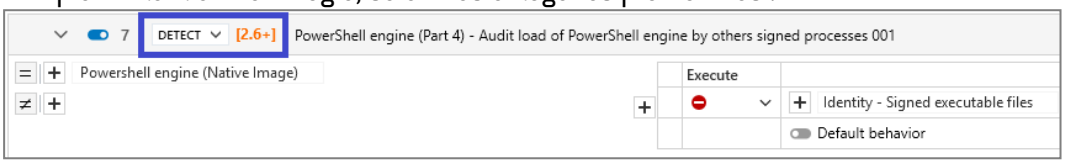
EXEMPLE

Voici la règle Client que vous pouvez créer pour **bloquer** les connexions depuis la carte réseau du réseau non protégé vers la zone internet et le réseau protégé via les ports 80, 443 et 8080 et le protocole TCP. Seul le serveur web spécifié, se trouvant dans le réseau de protégé, sera accessible.



11. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur  au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

12. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
13. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.10 Contrôler l'accès au Wi-Fi

Cette protection contrôle l'accès des postes de travail nomades aux réseaux Wi-Fi. Elle permet de :

- Autoriser ou refuser l'utilisation des connexions Wi-Fi et définir une liste blanche des points d'accès Wi-Fi sous forme de règles, en se basant sur l'identifiant SSID du réseau Wi-Fi et/ou l'adresse MAC du point d'accès,
- Autoriser ou refuser l'utilisation d'une connexion Wi-Fi Ad Hoc,
- Forcer l'utilisation de protocoles d'authentification sécurisés.

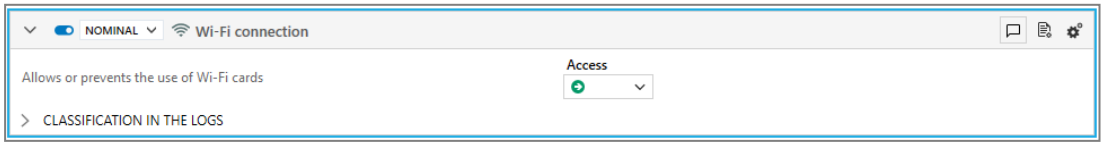
Par défaut, la connexion Wi-Fi est désactivée dans un jeu de règles de protection. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne l'activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer l'accès au Wi-Fi et veillez à l'ordre de vos jeux de règles dans la politique. Si vous activez et autorisez l'accès au Wi-Fi dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage de l'accès au Wi-Fi qui serait défini dans les jeux de règles placés après.

En fonction de certains événements, la politique de blocage des connexions Wi-Fi à l'intérieur ou à l'extérieur d'un périmètre peut s'activer grâce aux politiques conditionnelles. Pour plus d'informations, reportez-vous à la section Assigner une politique de sécurité aux agents.

Autoriser ou bloquer la connexion Wi-Fi

Pour autoriser ou bloquer la fonctionnalité de connexion Wi-Fi des postes de travail :

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Réseaux > Wi-Fi**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. La première règle **Connexion Wi-Fi** ne peut être supprimée. Elle est désactivée par défaut. Elle permet d'autoriser ou de bloquer le fonctionnement des cartes réseau Wi-Fi sur les postes de travail. Elle n'est présente quand dans un jeu de règles de protection. Dépliez la règle, puis activez-la en cliquant sur le bouton  à gauche puis autorisez ou bloquez l'accès.



Si vous désactivez la fonctionnalité Wi-Fi ou si vous bloquez l'accès, et que votre politique comprend des règles d'accès aux réseaux Wi-Fi, celles-ci ne seront pas parcourues.

Pour gérer de manière fine l'accès aux réseaux Wi-Fi, vous devez autoriser la connexion Wi-Fi et créer des règles **Réseau Wi-Fi**.

Contrôler l'accès aux réseaux Wi-Fi

Après avoir autorisé la connexion Wi-Fi dans la première règle du panneau (dans un jeu de règles de protection), créez des règles pour bloquer ou autoriser les postes de travail à accéder à certains réseaux Wi-Fi, ou bien créez des règles pour auditer les accès au Wi-Fi dans un jeu de règles d'audit. Par défaut, sans règle, l'accès à tous les réseaux Wi-Fi est autorisé et les règles peuvent donc être utilisées pour bloquer l'accès à des réseaux (mode liste noire). Si vous souhaitez fonctionner en mode liste blanche, c'est-à-dire autoriser explicitement l'accès à certains réseaux, vous devez créer en dernière position une règle qui bloque l'accès à tous les réseaux autres que ceux autorisés.

Pour créer des règles Réseaux Wi-Fi :

1. Dans l'onglet **Wi-Fi**, cliquez sur **Ajouter > Règle (Réseaux Wi-Fi)**. Une nouvelle ligne s'affiche.
2. Dans la partie gauche de la règle, cliquez sur l'icône  pour ajouter un réseau Wi-Fi.
3. Entrez les informations suivantes :
   - Le nom du réseau,
   - L'identifiant SSID (Service Set IDentifier). L'utilisation de caractères génériques est autorisée (par exemple : *stormshield**) et la casse n'importe pas,
   - L'adresse MAC du ou des points d'accès au format hexadécimal. Pour en indiquer plusieurs, cliquez sur l'icône +,
   - Sélectionnez le mode de connexion Wi-Fi,
   - Sélectionnez le type d'authentification pour la sécurisation de la communication avec le point d'accès Wi-Fi.

   > **NOTE**
   > Le mode d'authentification WPA3 n'est pas compatible avec les agents SES Evolution en version inférieure à la 2.4.
4. Dans le champ **Connexion**, sélectionnez l'action **Autoriser** ou **Bloquer**.
5. Dans le bandeau supérieur de la règle, vous pouvez :
   - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
     Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
   - Sélectionner les paramètres des logs qui seront émis par cette règle.
   - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.
   - Saisir un commentaire.
   - Saisir une description pour expliquer l'objectif de la règle.
6. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
7. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

8.5.11 Autoriser l'accès temporaire au web

Le mécanisme d'accès temporaire au web permet d'autoriser un utilisateur à contourner les règles de protection Réseaux de la politique de sécurité, avec des applications données et pour une durée que vous définissez.

Au terme de cette durée, les nouvelles connexions seront de nouveaux bloquées selon la politique de sécurité. En revanche, les applications dont les connexions ont été ouvertes durant un accès web temporaire ne seront pas fermées et les connexions existantes ne seront pas interrompues.

EXEMPLE

L'accès temporaire au web permet par exemple de gérer le cas des collaborateurs nomades souhaitant se connecter à leur réseau d'entreprise via un tunnel VPN depuis des réseaux non sécurisés. Lorsque ces postes sont en dehors du réseau de l'entreprise, la politique de sécurité qui s'applique peut empêcher toute communication réseau. La fonctionnalité d'accès temporaire au web permet alors par exemple de débloquer temporairement le client VPN et le navigateur sur demande de l'utilisateur, afin qu'il puisse se connecter au réseau d'entreprise et basculer sur la politique de sécurité interne. Il peut ainsi utiliser son poste normalement.

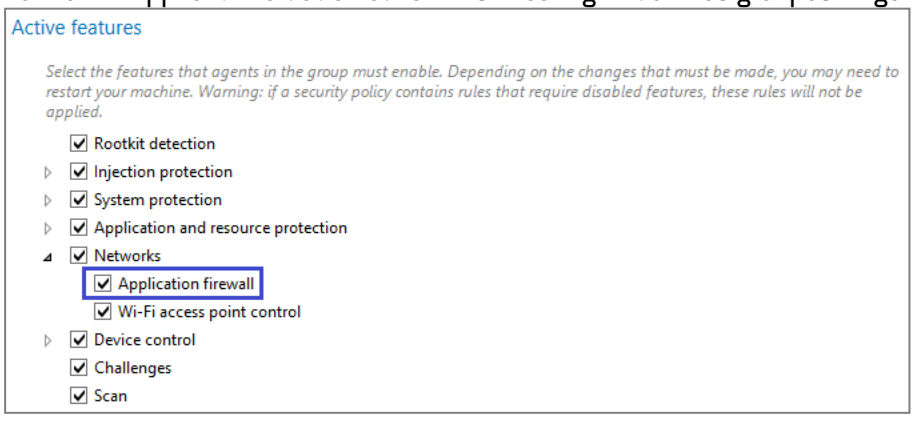
Il suffit que l'accès temporaire au web soit autorisé dans au moins une des politiques assignées à un groupe d'agents pour que la fonctionnalité soit disponible côté agent.

La fonctionnalité d'accès temporaire au web n'est disponible que dans les jeux de règles de protection.

Par défaut, cette fonctionnalité est désactivée. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne l'activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer l'accès temporaire au web et faites attention à l'ordre de vos jeux de règles dans la politique. Si vous activez et autorisez l'accès temporaire au web dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage de l'accès temporaire au web qui serait défini dans les jeux de règles placés après.

Prérequis

- Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées à effectuer des accès réseaux non restreints lorsque l'accès temporaire au web est actif. Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.
- Le firewall applicatif doit être activé dans la configuration des groupes d'agents :



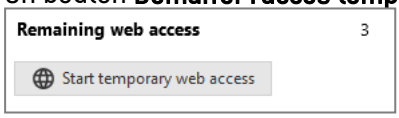
Autoriser l'accès temporaire au web

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur une politique.
2. Sélectionnez un jeu de règles de protection.
3. Cliquez sur l'onglet **Réseaux > Accès temporaire au web**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Activez la fonctionnalité.
6. Autorisez l'accès temporaire au web.
7. Sélectionnez un ou plusieurs identifiants d'applications autorisées à accéder au web. Ces applications seront autorisées à se connecter à toutes les adresses IP sur tous les ports.
8. Choisissez le temps d'accès maximum au web.
9. Choisissez le nombre d'accès autorisés. Le compteur est réinitialisé si l'utilisateur redémarre son poste de travail.
10. Si nécessaire, sélectionnez la création d'un raccourci sur le bureau de l'utilisateur. L'utilisateur dispose de plusieurs façons d'activer l'accès temporaire au web sur son poste de travail. Pour plus d'informations, reportez-vous à la section suivante.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Accéder temporairement au web depuis l'agent

L'agent SES Evolution met à la disposition de l'utilisateur plusieurs moyens pour activer l'accès temporaire au web :

- Un bouton **Démarrer l'accès temporaire au web** dans l'onglet de l'interface de l'agent,



- Un menu disponible en effectuant un clic droit sur l'icône de l'agent dans la barre des tâches,
- Une icône sur le bureau, si la fonctionnalité est activée dans le paramétrage de l'accès temporaire au web,
- La commande `EsGui /GrantWebAccess` à insérer dans un script par exemple.

Lorsque l'accès temporaire au web est en cours, un bandeau en bas de l'interface de l'agent indique le temps restant.

L'utilisateur a la possibilité d'arrêter l'accès temporaire en cours :

- via l'interface de l'agent,
- via le menu contextuel de l'icône de l'agent dans la barre des tâches.

8.5.12 Contrôler l'accès aux périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs.

Contrôler l'accès aux périphériques généraux

Contrôler l'accès aux périphériques Bluetooth

Contrôler l'accès aux périphériques USB

Contrôler le stockage sur périphériques USB

Contrôler l'exécution sur périphériques amovibles

8.6 Regrouper des règles de sécurité

Si vos jeux de règles contiennent un grand nombre de règles, la lecture et la maintenance peuvent s'avérer difficiles. Dans ce cas, vous pouvez créer des groupes contenant toutes les règles de même thématique. Par exemple, regroupez toutes les règles concernant les applications Microsoft Office.

8.6.1 Créer un groupe de règles

1. Dans le panneau des règles, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
2. Sélectionnez une ou plusieurs règles, puis cliquez sur **Ajouter > Groupe à partir de la sélection** ou utilisez le raccourci **CTRL + G**.
   Les règles sont rassemblées au sein d'un même groupe.
3. Dans l'entête du groupe de règles, saisissez un nom ou une description pour identifier le groupe, par exemple *Applications Office*.
4. A droite de l'entête du groupe, cliquez sur la palette de couleurs pour choisir la couleur du groupe.
5. Pour ajouter ou retirer des règles du groupe ou pour ordonner les règles au sein du groupe, utilisez le glisser-déposer à l'aide de l'icône.

8.6.2 Désactiver un groupe de règles

1. Dans le panneau des règles, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
2. Dans l'entête du groupe de règles, désactivez l'interrupteur  . Le groupe est grisé.
   Lorsqu'un groupe est désactivé, toutes les règles qu'il contient sont inactives.

8.6.3 Supprimer un groupe de règles

1. Dans le panneau des règles, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
2. Dans l'entête du groupe de règles à droite, cliquez sur l'icône **Supprimer**.
   La fenêtre **Supprimer le groupe** s'affiche.
3. Choisissez le degré de suppression :
   - **Supprimer le groupe uniquement** : les règles sont retirées du groupe et conservées.
   - **Supprimer le groupe et les règles** : les règles sont supprimées avec le groupe.

8.7 Classifier les attaques selon le référentiel de MITRE

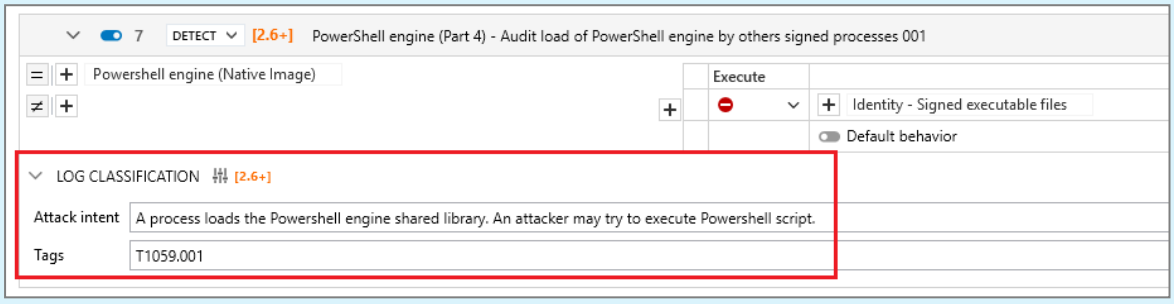
SES Evolution permet de référencer dans ses logs les techniques et sous-techniques des attaquants telles qu'elles sont listées et décrites dans les matrices MITRE Att&ck et dans les vulnérabilités et expositions communes (CVE) publiées par l'organisme américain MITRE. Ainsi en cas d'attaque, les administrateurs du parc pourront rapidement l'identifier et prendre les mesures adéquates.

La fonctionnalité a pour principe d'associer une règle de sécurité à une intention d'attaque et à des tags.

Vous pouvez ainsi indiquer pour chaque règle le type d'attaque qui pourrait être en cours lorsque la règle s'applique. Vous pouvez également indiquer une liste de tags qui permettent d'associer automatiquement vos règles SES Evolution au référentiel de MITRE.

L'objectif de la fonctionnalité est de fournir rapidement des informations aux administrateurs via les logs remontés dans la console lorsque les règles de sécurité s'appliquent. Ils peuvent ainsi identifier l'attaque possiblement en cours sur le parc en consultant sa classification, et se rendre directement sur l'URL de la technique MITRE ou de la CVE. Les tags peuvent également référencer les vulnérabilités identifiées par Stormshield sur son site https://advisories.stormshield.eu/.

EXEMPLE



8.7.1 Ajouter une intention et des tags à une règle de sécurité

Dans chaque règle de sécurité, vous pouvez ajouter une intention de l'attaque et des tags correspondants aux techniques, sous-techniques ou vulnérabilités référencées par MITRE. Ces informations permettent d'associer les règles à des types d'attaques connues. Elles s'affichent dans les logs lorsqu'une règle s'applique, permettant de classifier les logs générés par les agents et d'identifier rapidement le type d'attaque possiblement en cours.

Dans une règle de sécurité :

1. Dépliez la partie **Classification dans les logs** .
2. Indiquez l'intention de l'attaque, c'est-à-dire précisez le type d'attaque qui peut être en cours si la règle se déclenche. Par exemple, pour une règle protégeant une clé USB en lecture, vous pouvez indiquer "Extraire des données sensibles via un support amovible".
3. Indiquez jusqu'à 10 tags, faisant référence aux matrices MITRE Att&ck, aux vulnérabilités CVE ou bien Stormshield. Pour connaître le format des tags, consultez les matrices MITRE Att&ck, les vulnérabilités et expositions communes (CVE) ou le site https://advisories.stormshield.eu/. Par exemple T1546.001, CVE-2021-40444 ou STORM-2023-022.

Vous pouvez utiliser le champ de recherche pour filtrer les règles d'après l'intention de l'attaque ou les tags.

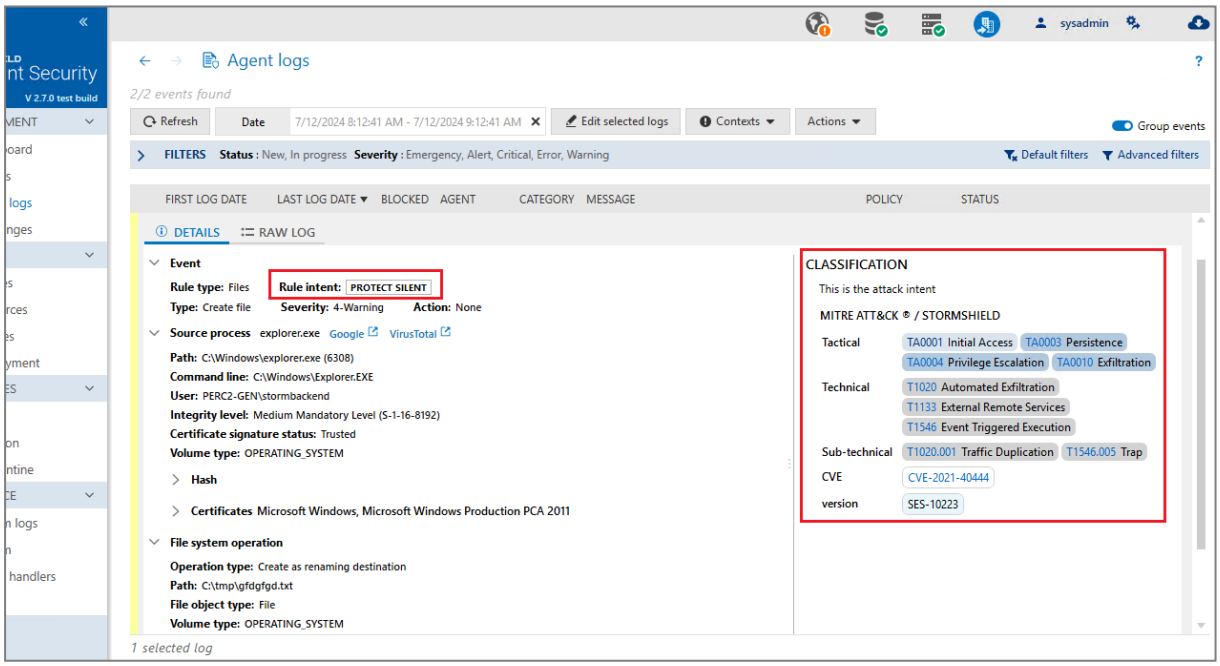
8.7.2 Consulter les intentions et les tags dans les logs

Les informations de classification s'affichent différemment sur l'agent SES Evolution et dans la console d'administration.

L'onglet **Événements** de l'interface de l'agent permet de consulter les tags associés à la règle ayant généré un log dans l'affichage **Log brut** :

Dans les logs des agents dans la console d'administration, le panneau **Classification** dans les détails d'un log affiche l'intention de l'attaque et les tags associés à la règle ayant généré le log :

- Cliquez sur les tags MITRE et CVE pour accéder directement aux détails.



8.8 Définir des règles d'événements externes

Les règles d'audit de type Événements externes vous permettent de collecter certains événements se produisant sur les postes de travail mais qui ne sont pas issus des composants SES Evolution standard :

- Événements Windows,
- Événements remontés par le moteur d'analyse OSSEC.

Lorsque la règle est activée, les événements externes collectés sont affichés sous forme de logs dans le panneau **Logs agents** de la console d'administration et sur l'interface des agents SES Evolution.

8.8.1 Transférer des événements Windows dans SES Evolution

Le transfert d'événements Windows consiste à indiquer via une règle quels journaux et quels événements Windows doivent être collectés et affichés par SES Evolution.

EXEMPLE
Vous pouvez choisir de transférer les événements relatifs aux connexions des utilisateurs sur les postes de travail, afin de surveiller qui s'est connecté et à quel moment.

Créer une règle de transfert d'événements :

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles d'audit.
3. Cliquez sur **Événements externes > Transfert d'événements**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter > Règle (Transfert d'événements)**.
   Une nouvelle ligne s'affiche.

6. Cliquez sur **+ Événements surveillés** et fournissez les informations suivantes :
   Nom du journal
   Saisissez le nom du journal Windows (e.g., *Security*, *Microsoft-Windows-Windows Defender/Operational*). Pour connaître le nom d'un journal, consultez ses propriétés dans l'Observateur d'événements Windows.
   Vous pouvez surveiller un journal qui n'est pas activé dans Windows. Dans ce cas, SES Evolution l'activera automatiquement. Néanmoins, soyez conscient que si les événements de ce journal sont nombreux, cela peut entraîner une baisse des performances de Windows.
   Si vous saisissez une requête de filtrage au format XML dans le champ suivant, le **Nom du journal** n'est pas indispensable.

   Requête de filtrage
   Si besoin, saisissez une requête de filtrage afin de ne collecter que certains événements du journal. Pour obtenir une requête :
   1. Ouvrez l'Observateur d'événements Windows.
   2. Sur le journal de votre choix, faites un clic droit > **Filtrer le journal actuel**.
   3. Dans l'onglet **Filtrer**, choisissez vos options de filtrage.
   4. Copiez le contenu de l'onglet **XML** et collez-le dans le champ **Requête de filtrage** de la fenêtre de la règle de transfert d'événements.

   Vous pouvez aussi saisir manuellement une requête au format XPath. Par exemple saisissez le nom de journal `Security` et la requête de filtrage `*[System [(EventID=4625)]]` pour récupérer tous les événements avec l'ID 4625 dans le journal Security.

   Description
   Si besoin, saisissez une description.

   Vous pouvez aussi importer une vue personnalisée d'événements Windows, ce qui permet de remplir automatiquement tous les champs avec les valeurs souhaitées. Pour cela, dans l'Observateur d'événements Windows, exportez la vue personnalisée souhaitée au format XML et importez-la en cliquant sur la flèche à droite  .

EXEMPLE

Ici, les événements d'ID 350 à 381 du journal System seront transférés, à l'exception de l'ID 376.

7. Dans le bandeau supérieur de la règle, vous pouvez :
   - Sélectionner les paramètres des logs qui seront émis par cette règle. La gravité d'un log est basée sur sa gravité dans Windows. Les correspondances sont les suivantes :

Type d'événement Windows	Log SES Evolution
Audit	Information
Critique	Critique
Erreur	Erreur
Avertissement	Avertissement
Information	Information
Verbose	Diagnostic

   - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.
   - Saisir une description pour expliquer l'objectif de la règle.
   - Saisir un commentaire.
8. Si besoin, ajoutez d'autres règles de transfert d'événements.
9. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

SES Evolution rattrape les événements Windows qui ont été émis alors qu'il n'était pas actif, par exemple lors du redémarrage de la machine.

8.8.2 Importer des règles de sécurité OSSEC

OSSEC est un détecteur d'intrusion sur machine hôte ou HIDS (Host-based Intrusion Detection System). Il comprend un module de surveillance et analyse de logs. Pour plus d'informations, reportez-vous au site web OSSEC.

SES Evolution est doté d'un moteur d'analyse de principe similaire, qui permet de surveiller en temps réel :

- Des fichiers de logs d'applications tierces,
- Des événements Windows (dans les journaux d'événements).

Cette surveillance a pour but d'extraire des informations dans les événements et les lignes de log sur les agents SES Evolution, de les classifier pour repérer des activités anormales ou suspectes et générer des alertes.

EXEMPLE
Vous pouvez surveiller les authentifications par mot de passe sur un serveur FileZilla qui proviennent de la même adresse IP, et lever des alertes en cas d'échecs multiples suivis d'un succès.

NOTE
Les options de l'analyse OSSEC ne seront pas détaillées dans ce document. Veuillez vous référer à la documentation OSSEC.

Il existe des différences entre le moteur d'analyse Stormshield et OSSEC :

- OSSEC collecte les logs sur les agents et les analyse sur le serveur alors que SES Evolution fait l'analyse sur chaque agent. Il n'est donc pas possible de corréler des événements de même nature se produisant sur des agents distincts.
- Contrairement à OSSEC, SES Evolution ne permet pas de compiler des décodeurs et des règles personnalisées. En revanche la règle *is_simple_http_request*, fournie à titre d'exemple par OSSEC mais utilisée en standard, est supportée par SES Evolution.

Pour plus d'informations sur toutes les fonctions OSSEC supportées par SES Evolution, reportez-vous à la section Connaître les fonctions OSSEC supportées

Configurer des règles OSSEC

Configurer une règle OSSEC consiste à indiquer quels fichiers de logs et/ou événements Windows doivent être surveillés et quel fichier de décodeurs et règle OSSEC leur appliquer.

1. Dans un jeu de règles d'audit, cliquez sur **Événements externes > Règles OSSEC**.
2. Cliquez sur **Ajouter une règle (OSSEC)**.
3. Si vous souhaitez surveiller un fichier de logs d'une application tierce, cliquez sur **+ Fichier surveillé** et fournissez les informations suivantes :

   Chemin
   Saisissez le chemin du fichier. Vous pouvez utiliser :
   - Des variables d'environnement, uniquement dans le chemin du dossier (jusqu'au dernier \ du chemin,
   - Des spécifications de noms de fichiers au format *strftime* en **fin** de chemin uniquement (après le dernier \ du chemin).

   > **EXEMPLE**
   > Si vous entrez le chemin *%PROGRAMFILES%\Filezilla Server\Logs\fzs-%Y-%m-%d.log*, toute ligne de log ajoutée dans tout fichier dont le nom aura la forme *fzs-YYYY-MM-DD.log* sera analysée par SES Evolution.

   Encodage
   Choisissez l'encodage attendu du fichier. Il dépend de l'application qui émet les logs. Les encodages supportés sont :
   - Page de codes ANSI (dépend de la locale système),
   - UTF8,
   - UTF-16LE.

   Description
   Saisissez une description optionnelle. Elle sera sans effet sur le fonctionnement de l'analyse.

4. Si vous souhaitez surveiller un journal ou certains événements Windows, cliquez sur **+ Événement surveillé** et fournissez les informations suivantes :
Nom du journal
Saisissez le nom du journal Windows (e.g., *System*, *Microsoft-Windows-Windows Defender/Operational*). Pour connaître le nom d'un journal, consultez ses propriétés dans l'Observateur d'événements Windows.

> **NOTE**
> Il est possible de surveiller un journal qui n'est pas activé dans Windows. SES Evolution l'activera automatiquement. Cette opération peut entraîner une baisse des performances de la machine.

Requête de filtrage
Si besoin, saisissez une requête de filtrage afin de ne surveiller que certains événements du journal. Pour obtenir une requête :

a. Ouvrez l'Observateur d'événements Windows.
b. Sur le journal de votre choix, faites un clic droit > **Filtrer le journal actuel**.
c. Dans l'onglet **Filtrer**, choisissez vos options de filtrage.
d. Copiez le contenu de l'onglet **XML** et collez-le dans le champ **Requête de filtrage** de la fenêtre de la règle OSSEC.

Description
Si besoin, saisissez une description. Elle sera sans effet sur le fonctionnement de l'analyse.

5. Cliquez sur **+ Décodeur OSSEC** et choisissez le fichier *etc/decoder.xml* de votre choix. Un fichier de décodeurs OSSEC permet d'indiquer quels types de logs doivent être analysés, et quelles valeurs extraire. Pour plus d'informations, reportez-vous à la documentation OSSEC.
Si vous importez plusieurs fichiers décodeurs, assurez-vous de les ordonner correctement à l'aide des flèches situées à gauche.
6. Cliquez sur **+ Jeux de règles OSSEC** et choisissez les fichiers *etc/rules/*.xml* de votre choix. Assurez-vous de les ordonner correctement. Le fichier *rules_config.xml* est obligatoire et doit être le premier : il contient les règles OSSEC 1 à 7 qui doivent impérativement être les premières règles déclarées.
Vous pouvez également choisir un fichier *.conf* d'OSSEC, auquel cas vous devez aussi spécifier le dossier contenant les fichiers de règles. Les règles seront automatiquement importées dans l'ordre.

7. Cliquez sur **Vérifier la règle** pour contrôler la cohérence de votre configuration d'analyse OSSEC. Les vérifications suivantes sont notamment effectuées :
   - Validation des expressions régulières présentes dans les fichiers de décodeurs et de règles,
   - Présence de décodeurs,
   - Présence des règles 1 à 7,
   - Validité des fichiers de décodeurs et de règles,
   - Utilisation d'options OSSEC non supportées et donc ignorées.

   Le résultat de la vérification affiche les erreurs, avertissements et messages d'information :
   - Les erreurs sont bloquantes et empêchent de valider la configuration OSSEC,
   - Les avertissements ne bloquent pas l'application de la configuration mais peuvent avoir des incidences sur l'évaluation des règles,
   - Les messages d'information indiquent des problèmes potentiels dans la configuration, et la manière dont ils sont résolus.

Par défaut, le moteur d'analyse OSSEC de SES Evolution récupère les événements Windows émis lorsqu'il n'est pas activé, par exemple lors du redémarrage de la machine. En revanche il ne récupère pas les fichiers de logs.

Visualiser les logs émis par OSSEC

Les logs d'événements externes produits par le moteur d'analyse SES Evolution sont visibles comme les autres logs SES Evolution dans la console d'administration et sur l'agent. Sur l'agent, ils ne sont visibles que pour les administrateurs de la machine. Pour plus d'informations, reportez-vous aux sections Visualiser et gérer les logs des agents dans la console d'administration et Visualiser les logs sur l'interface des agents.

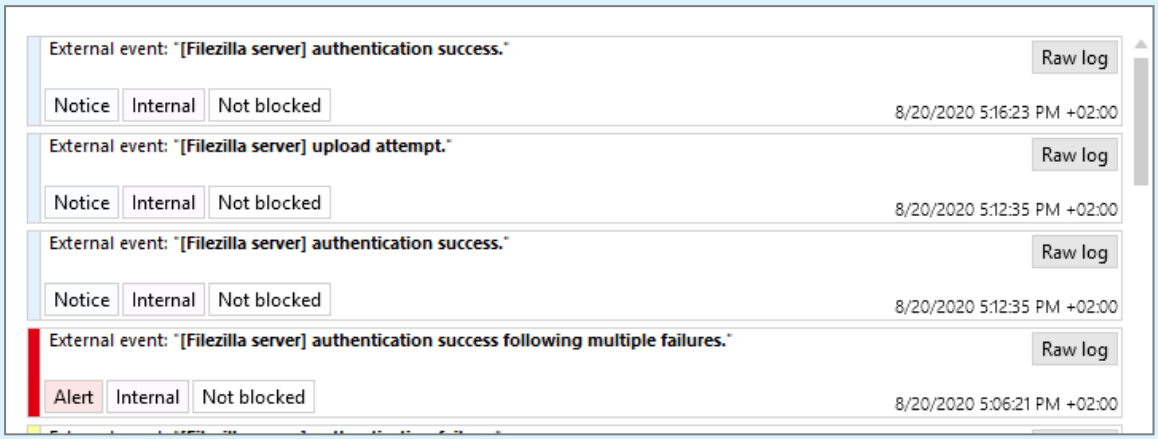
Les logs contiennent tous les champs collectés durant le décodage OSSEC.

Le niveau de gravité du log dépend du niveau de la règle OSSEC ayant spécifié le log :

Niveau de log de la règle OSSEC	Gravité du log SES Evolution
0	Pas de log
1	Diagnostic
2	Information
3, 4, 5	Remarque
6, 7, 8, 9	Avertissement
10	Erreur
11, 12	Critique
13, 14	Alerte
15	Urgence

EXEMPLE
L'image ci-dessous affiche les logs Filezilla extraits par le moteur d'analyse et remontés dans l'interface de l'agent. Il s'agit de détecter les authentifications par mot de passe sur un serveur

FileZilla qui proviennent de la même adresse IP, et de lever des alertes en cas d'échecs multiples suivis d'un succès.



8.9 Tester une politique de sécurité

Nous vous recommandons de tester vos politiques de sécurité avant de les déployer et de les mettre en œuvre sur votre parc.

Tester une politique permet de vérifier les impacts des restrictions d'utilisation imposées par la politique et de procéder à des ajustements des règles de protection avant de les mettre en production.

Les fonctionnalités mode "Détection" et "règle passive" permettent de tester une politique sur un parc sans bloquer l'utilisation des postes de travail et de façon totalement transparente pour les utilisateurs. Lorsque ces fonctionnalités sont activées, les agents SES Evolution ne bloquent pas les opérations mais émettent des logs indiquant quelles opérations auraient été bloquées par une règle.

Tester une politique est utile dans les cas suivants :

- Lorsque vous installez SES Evolution pour la première fois sur un ensemble de machines. Dans ce cas, tester une politique permet par exemple de savoir si des applications nécessaires à vos utilisateurs seraient bloquées et donc de créer les exceptions adéquates. Le test est transparent pour les utilisateurs et ils peuvent toujours utiliser leurs applications habituelles.
- Lorsque vous agrandissez votre parc de machines à protéger. Vous créez alors un nouveau groupe d'agents par exemple, et testez la politique déjà en vigueur sur les autres groupes. Vous pouvez ainsi vérifier que la politique est adaptée au nouveau groupe avant de la mettre en œuvre, et l'ajuster si nécessaire.
- Vous avez besoin d'ajouter un nouveau jeu de règles de protection à l'une de vos politiques de sécurité. Testez d'abord le jeu pour vérifier qu'il ne bloque pas d'applications légitimes avant de le mettre en production.

Vous pouvez tester une politique de sécurité sur un parc à différents niveaux :

- la politique complète, avec le mode "Détection", dans la configuration des groupes d'agents,
- un jeu de règles de protection complet, avec le mode "Détection", dans la configuration d'une politique,
- une règle en particulier avec le mode "règle passive", dans la configuration de la règle elle-même.

8.9.1 Tester une politique de sécurité entière affectée à un groupe d'agents

Vous pouvez activer le mode "Détection" dans la configuration d'un groupe d'agents. Le paramétrage s'applique sur toutes les politiques affectées au groupe (politique principale et éventuelles politiques conditionnelles).

Activer le mode "Détection" sur une politique entière signifie que toutes les règles de tous les jeux de règles de protection passeront en mode "règle passive" et les règles contre les menaces passeront en état "Détecter seulement".

Pour tester les politiques affectées à un groupe d'agents :

1. Dans le menu **Environnement > Agents**, sélectionnez un groupe d'agents.
2. Dans l'onglet **Politiques**, activez l'option **Passer les politiques en mode Détection**.
3. Déployez l'environnement.

Ce paramétrage dans la configuration du groupe d'agents est prioritaire sur le paramétrage sur les jeux de règles. Par conséquent si le mode "Détection" est activé pour un groupe d'agents, les actions seront détectées mais pas bloquées même si le jeu de règles est en mode actif dans la politique.

Pour plus d'informations sur la configuration des groupes d'agents, reportez-vous à la section Créer et configurer les groupes d'agents.

8.9.2 Tester un jeu de règles de protection

Vous pouvez tester un jeu de règles de protection avant de le mettre en production, qu'il soit privé ou partagé. Pour tester un jeu, vous devez activer le mode "Détection" du jeu dans la politique concernée. Dans le cas d'un jeu de règles partagé, l'activation du mode "Détection" n'est pas répercutée sur les autres politiques qui utiliseraient le même jeu.

Pour activer le mode "Détection" d'un jeu :

1. Dans le menu **Sécurité > Politiques**, sélectionnez la politique concernée.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
3. Sur la ligne du jeu de règles à tester, cliquez sur la flèche à droite de l'icône bouclier  .
4. Sélectionnez l'icône  pour passer le jeu en mode "Détection".

Ce paramétrage s'applique à tous les groupes d'agents qui utilisent cette politique.

Vous pouvez aussi complètement désactiver un jeu de règles avec l'interrupteur  à gauche de la règle. Dans ce cas, le jeu n'est pas déployé sur l'agent.

Pour plus d'informations sur les jeux de règles, reportez-vous à la section Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit.

8.9.3 Tester une règle

Pour connaître les impacts d'une règle de sécurité sans appliquer de blocage, activez le mode "Règle passive" dans les options du bandeau supérieur de la règle.

De la même façon, pour connaître les impacts d'une règle contre les menaces sans appliquer de blocage, sélectionnez l'état "Détecter seulement" dans la configuration de la règle.

Pour obtenir des détails sur ces options et état, consultez les sections sur les différents types de règles sous Configurer la protection contre les menaces et Définir les règles de contrôle d'accès.

8.10 Désactiver une règle de sécurité

Toutes les règles de sécurité peuvent être désactivées de façon individuelle. Une règle désactivée n'est plus prise en compte par l'agent SES Evolution, elle ne fait plus partie de la politique de sécurité.

Désactivez une règle si vous ne souhaitez pas la supprimer mais que vous ne voulez plus l'utiliser temporairement ou que vous voulez tester le comportement de l'agent sans cette règle.

Certains types de règles sont désactivés par défaut lorsqu'on créé un nouveau jeu de règles. En effet, si ces règles étaient activées dans plusieurs jeux de règles, elles pourraient surcharger et annuler l'effet du paramétrage selon l'ordre des jeux. C'est le cas des menaces, de la connexion Wi-Fi, de l'accès temporaire au web et des périphériques généraux.

Pour désactiver une règle :

1. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
2. Dans le bandeau supérieur de la règle, désactivez l'interrupteur  . La règle est grisée.

La désactivation d'une règle est différente du mode **Règle passive**. Pour plus d'informations sur les règles passives, reportez-vous à la section Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit.

8.11 Configurer la gestion des logs

Les logs émis par l'agent en cas de blocage ou d'audit peuvent être transmis vers trois destinations distinctes selon leur niveau de gravité. Ces paramètres sont définis globalement dans la page de configuration des groupes d'agents. Pour plus d'informations, reportez-vous à la section Configurer la transmission des logs émis par les agents

De plus, pour chaque règle de sécurité que vous créez, vous pouvez spécifier :

- Le niveau de gravité du log émis en cas de blocage ou d'audit,
- La destination vers laquelle est transmis le log émis en cas de blocage ou d'audit.

NOTE
Dans tous les cas, même si aucune destination n'est configurée pour des logs donnés, ils seront présents dans le détail de contexte en cas d'attaque. Pour plus d'informations sur l'analyse des contextes, reportez-vous à la section Comprendre la composition d'un contexte.

8.11.1 Recommandations

Vous pouvez ajuster le niveau de gravité des logs émis par une règle dans des cas tels que :

- Pour vos applications particulièrement sensibles, augmentez le niveau de gravité des logs. En effet, les logs de niveau *Urgence* et *Alerte* sont envoyés au gestionnaire d'agents en priorité, plus fréquemment que les autres (toutes les 30 secondes par défaut contre une heure pour les autres),
- Si une règle de sécurité génère de nombreux logs non pertinents, baissez son niveau de gravité.

8.11.2 Configurer les logs d'une règle de sécurité

1. Dans le menu **Sécurité > Politiques** de la console d'administration, sélectionnez votre politique de sécurité, puis votre jeu de règles. La page d'accueil du jeu de règles s'affiche.
2. Cliquez sur l'onglet correspondant à la règle que vous souhaitez modifier.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
4. Dans le bandeau en haut de la règle, cliquez sur l'icône  . La fenêtre **Paramètres du log** s'affiche.
5. Dans le champ **Gravité du log**, choisissez le niveau de criticité à attribuer aux logs générés par cette règle.
6. Dans le champ **Afficher sur l'agent**, choisissez si vous souhaitez que les logs de cette règle soient visibles sur l'agent :
   - **Hériter** : Le comportement global défini au niveau du groupe d'agents s'applique. Dans l'exemple ci-dessus, les logs sont visibles sur l'agent car tous les logs à partir du niveau *Remarque* le sont.
   - **Jamais** : Les logs ne sont jamais visibles sur l'agent quel que soit le comportement global.
   - **Toujours** : Les logs sont toujours visibles sur l'agent quel que soit le comportement global.
     Attention, seuls les logs de niveau *Alerte* et *Urgence* ayant entraîné un blocage sont visibles dans l'interface de l'agent pour un utilisateur non administrateur de sa machine.
7. Dans le champ **Afficher sur la console**, choisissez si vous souhaitez que les logs de cette règle soient visibles sur la console d'administration.
8. Dans le champ **Envoyer vers Syslog**, choisissez si vous souhaitez que les logs de cette règle soient envoyés vers le serveur Syslog si celui-ci est configuré. Pour plus d'informations, reportez-vous à la section Créer des groupes de gestionnaires d'agents.
9. Cliquez sur **Valider**.
10. Enregistrez les modifications apportées à la règle.

8.12 Configurer des actions déclenchées par les règles

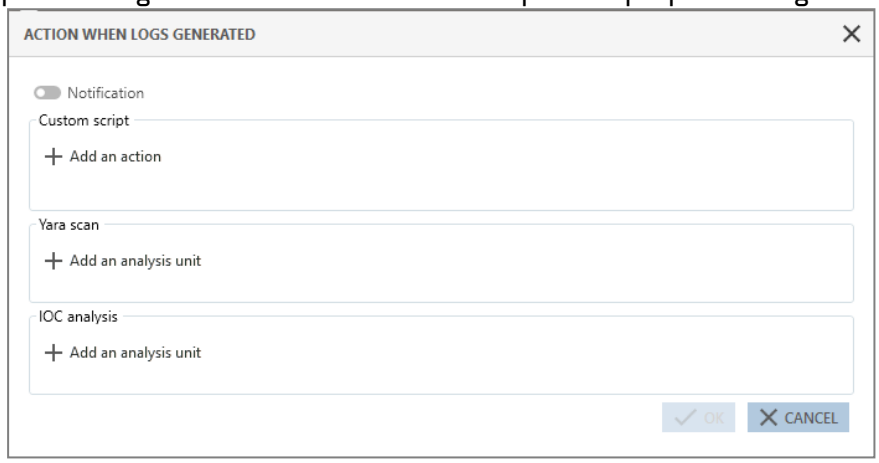
Lorsqu'une opération effectuée sur un agent SES Evolution est bloquée par une règle de protection, un log est émis, dont vous pouvez déterminer la gravité et la destination.

Si vous le souhaitez, l'émission de ce log peut déclencher des actions sur les agents concernés. Il existe différents types d'actions :

- Afficher une notification sur l'agent. Celle-ci s'affichera en bas à droite de l'écran, indiquant qu'une opération interdite a été bloquée par une règle de protection.
- Exécuter des scripts personnalisés.
- Exécuter une analyse YARA ou IoC. Pour plus d'informations, reportez-vous aux sections Réaliser des analyses Yara et Rechercher des indicateurs de compromission
  Cette action est disponible uniquement pour les règles dont les logs contiennent des processus ou des fichiers. Par exemple, les règles Périphériques et ARP Spoofing ne sont pas concernées.

EXEMPLE
Cette fonctionnalité peut être utile pour déclencher une analyse antivirale à l'émission du log, ou encore le déplacement d'un fichier malveillant dans un dossier particulier. Le déclenchement d'une analyse YARA ou IoC permet par exemple d'identifier un malware.

1. Dans le menu **Sécurité > Politiques**, sélectionnez votre politique de sécurité, puis le jeu de règles. La page générale du jeu de règles s'affiche.
2. Cliquez sur l'onglet correspondant à la règle que vous souhaitez modifier.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
4. Dans le bandeau en haut de la règle, cliquez sur l'icône  . La fenêtre **Action sur émission de logs** s'affiche.
5. Si vous le souhaitez, activez l'envoi d'une notification sur l'agent à chaque émission d'un log par cette règle. Cette fonctionnalité n'est disponible que pour les règles en mode Protection.



6. Si vous souhaitez exécuter un script à chaque émission d'un log par cette règle, cliquez sur **Ajouter une action**.
   a. Dans la fenêtre **Exécuter un script personnalisé**, saisissez un nom pour l'action.
      a. À droite du champ **Script**, cliquez sur + pour ajouter le script à exécuter.
      b. Dans le champ **Arguments**, spécifiez les arguments à ajouter lors de l'exécution du script.
      c. Dans la liste **Contexte d'exécution**, privilégiez **Service local** car il s'agit d'un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

      Notamment, il n'est pas possible de lancer un script en session interactive sur un serveur avec plusieurs utilisateurs connectés à distance.
      Tous les scripts déclarés dans SES Evolution s'affichent dans la liste **Script**.

      Sélectionnez un script existant, et cliquez sur le bouton  pour le visualiser, ou sur  pour importer une nouvelle version du script.

7. Si vous souhaitez exécuter une analyse YARA ou IoC à chaque émission d'un log par cette règle, cliquez sur **Ajouter une unité d'analyse** dans la section voulue.
   a. Cliquez sur une ou plusieurs unités d'analyse pour les sélectionner, puis fermez cette fenêtre. Pour une analyse IoC, seuls les indicateurs de type texte ou nom de fichier sont utilisables ici.
   b. Dans la fenêtre **Action sur émission de logs**, cliquez sur Paramètres des logs pour déterminer le niveau de gravité et la destination des logs émis par les règles YARA ou IoC.
   c. Si besoin, sélectionnez **Interrompre les processus détectés**, pour supprimer des agents les processus malveillants identifiés lors de l'analyse YARA ou IoC.
   Si la règle appartient à un jeu de règles d'audit ou si la règle est en mode passif, les processus ne seront pas interrompus même si ce paramètre est activé.
8. Cliquez sur **Valider**.

Dans le cas d'une analyse IoC sur émission d'un log, elle ne peut porter que sur l'élément qui a déclenché la règle. Les analyses IoC planifiées ou à la demande sont plus précises car leur paramétrage permet d'inclure ou d'exclure des répertoires à analyser. Pour plus d'informations, reportez-vous aux sections Planifier une analyse IoC et Exécuter une analyse IoC à la demande.

EXEMPLE
Dans une règle Fichier protégeant les fichiers situés sous *C:\temp* de la suppression, vous paramétrez une analyse IoC sur émission de logs afin de rechercher le texte "*suspect_text*" dans les fichiers. Si l'utilisateur tente de supprimer un fichier sous *C:\temp* avec PowerShell, la règle s'applique et l'analyse IoC se déclenche, mais seulement sur le fichier *powershell.exe* et sur la mémoire du processus *powershell.exe*.

8.13 Assigner une politique de sécurité aux agents

C'est la politique Stormshield Default Policy qui est appliquée par défaut aux groupes d'agents, mais si vous avez créé une politique de sécurité personnalisée, vous pouvez l'assigner aux groupes d'agents.

1. Choisissez le menu **Environnement > Agents**.
2. Dans le panneau de gauche, sélectionnez un groupe d'agents.
3. Dans le bandeau supérieur, cliquez sur le bouton **Modifier**.
4. Rendez-vous dans l'onglet **Politiques** d'un groupe d'agents.
5. Dans la liste déroulante **Politique**, choisissez la politique de sécurité que vous souhaitez appliquer à tous les agents du groupe.
   Pour plus d'informations, reportez-vous à la section Créer et configurer les groupes d'agents.
6. Dans le bandeau supérieur, cliquez sur le bouton **Enregistrer**.
7. Pour déployer la politique sur tous les agents du groupe afin qu'ils l'appliquent, choisissez le menu **Sécurité > Déploiement** et cliquez sur le bouton **Déployer**.

8.14 Exporter et importer les politiques et jeux de règles

Vous pouvez exporter les politiques complètes ou uniquement des jeux de règles vers un fichier au format *.cab* contenant lui-même des fichiers *.json*. Ce fichier pourra ensuite être réimporté. Cela permet par exemple de :

- Transférer une politique de sécurité d'un environnement de pré-production vers un environnement de production,
- Transférer une politique ou un jeu de règles au Support technique SES Evolution pour faciliter le diagnostic d'un problème.

Lorsque vous exportez une politique ou un jeu de règles, vous exportez la version sélectionnée sur la droite du panneau, représentée par l'icône  . Lorsque vous importez une politique ou un jeu de règles personnalisé qui existe déjà, son numéro de version s'incrémente systématiquement.

Pour plus d'informations sur la gestion des versions des politiques et des jeux de règles, reportez-vous à la section Gérer les versions d'une politique ou d'un jeu de règles .

8.14.1 Exporter toutes les politiques de sécurité de la liste

1. Dans le menu **Sécurité** > **Politique**, cliquez sur le bouton **Exporter-Tout exporter** en haut du panneau.
2. Sélectionnez le dossier vers lequel vous souhaitez faire l'export.
   La dernière version de chaque politique est exportée sous la forme d'un fichier individuel nommé *nom_politique.cab*.

8.14.2 Exporter une ou plusieurs politiques de sécurité

1. Dans le menu **Sécurité** > **Politiques**, sélectionnez la ou les politiques à exporter.
2. Par défaut, c'est la dernière version d'une politique qui est exportée. Si vous souhaitez exporter une autre version, sélectionnez-la dans la colonne de droite du panneau général de la politique.
3. Cliquez sur **Exporter-Exporter la sélection** et sélectionnez le dossier vers lequel vous souhaitez faire l'export.
   Chaque politique est exportée sous la forme d'un fichier individuel nommé *nom_politique.cab*.

8.14.3 Importer une ou plusieurs politiques de sécurité

- Pour importer une seule politique ou plusieurs politiques à la fois, dans le menu **Sécurité** > **Politiques**, cliquez sur **Importer** en haut du panneau.
  L'import d'une politique déjà existante crée automatiquement une nouvelle version de cette politique, sauf s'il s'agit d'une politique intégrée.

8.14.4 Exporter un jeu de règles

1. Dans le menu **Sécurité** > **Politiques**, double-cliquez sur la politique, puis le jeu de règles de votre choix.
2. Par défaut, c'est la dernière version du jeu de règles qui est exportée. Si vous souhaitez exporter une autre version, sélectionnez-la dans la colonne de droite.
3. Cliquez sur **Exporter** et choisissez le nom du fichier et le dossier vers lequel vous souhaitez faire l'export.

8.14.5 Exporter une sélection de jeux de règles partagés

1. Dans le menu **Sécurité > Politiques**, cliquez sur **Voir les jeux de règles partagés** en haut à droite.
2. Sélectionnez les jeux de règles que vous souhaitez exporter, et/ou filtrez la liste des jeux de règles en utilisant le champ de recherche en haut à droite.
3. Cliquez sur **Exporter-Tout exporter** pour exporter tous les jeux de règles visibles dans la liste, ou **Exporter-Exporter la sélection** si vous avez sélectionné seulement quelques jeux de règles.
4. Sélectionnez le dossier vers lequel vous souhaitez faire l'export.
   Chaque jeu de règles est exporté sous la forme d'un fichier individuel nommé *nom jeu.cab*.

Il n'est pas possible d'exporter plusieurs jeux de règles privés à la fois.

8.14.6 Importer des jeux de règles

1. Dans le menu **Sécurité > Politiques**, double-cliquez sur la politique de votre choix.
2. Dans le panneau général de la politique, cliquez sur **Importer** et choisissez le fichier *.cab* du ou des jeux de règles que vous souhaitez importer.
   L'import d'un jeu de règles déjà existant crée automatiquement une nouvelle version de ce jeu.
   S'il s'agit d'un jeu de règles intégré, il crée une nouvelle version seulement si elle n'existe pas.

9. Déployer l'environnement SES Evolution

Pour appliquer la configuration des groupes d'agents, les politiques de sécurité ainsi que des nouvelles versions logicielles de l'agent sur votre parc d'agents, vous devez déployer l'environnement.

L'action de déployer a pour effet de générer pour chaque groupe d'agents les informations à envoyer aux agents. Des packages de configuration et de politiques sont générés et stockés en base de données. Les agents se reconnectent régulièrement à leur gestionnaire d'agents pour transmettre leur statut. Le gestionnaire d'agents détecte alors la présence de mises à jour à appliquer aux agents.

Par défaut, un agent se reconnecte à son gestionnaire toutes les 60 secondes. Il faut donc moins d'une minute pour qu'un nouveau déploiement soit appliqué. Vous pouvez paramétrer cette durée dans la configuration des groupes d'agents, avec le paramètre **Mise à jour de l'état de l'agent**. Pour plus d'informations, reportez-vous à la section Surveiller les agents en temps réel

Vous devez redéployer l'environnement chaque fois que vous faites des modifications dans la console d'administration sur les éléments suivants et que vous souhaitez les appliquer sur le parc :

- Les politiques et jeux de règles,
- La configuration des groupes d'agents,
- La configuration des gestionnaires d'agents,
- La configuration du niveau de confiance d'une clé USB.

Assurez-vous de disposer du droit **Environnement-Déployer** pour pouvoir effectuer cette action.

Pour déployer l'environnement sur les agents du parc :

1. Modifiez un ou plusieurs des élément de configuration mentionnés plus haut.
   Un point orange s'affiche à droite du menu **Sécurité > Déploiement** et l'icône **Déploiement** dans le bandeau supérieur de la console devient orange  . Cela signifie que de nouveaux éléments nécessitent d'être déployés pour être fonctionnels.
2. Cliquez sur l'icône **Déploiement** ou choisissez le menu **Sécurité** > **Déploiement** et cliquez sur **Déployer**.
   Le point orange disparaît et le bouton **Déployer** se grise jusqu'à la prochaine modification de configuration.

NOTE
Plus la machine hébergeant le composant backend possède de cœurs, plus le temps de déploiement est rapide, notamment lorsque vous avez configuré un grand nombre de groupes d'agents. La recommandation minimum est de deux cœurs. Pour plus d'informations sur les prérequis système, reportez-vous à la section *Backend* du *Guide d'installation*.

Concernant les versions des jeux de règles déployées avec une politique, vous pouvez sélectionner **Toujours utiliser la dernière version** dans le panneau général de la politique. Dans ce cas, après le déploiement de la politique, le numéro de la version des jeux déployée s'affiche dans la liste déroulante des versions. Lorsque vous cliquez sur **Modifier** dans ce panneau, le paramètre **Toujours utiliser la dernière version** est bien conservé pour chaque jeu. Pour plus d'informations, reportez-vous à la section Gérer les versions d'une politique ou d'un jeu de règles .

Si le déploiement n'est pas possible, l'interface affiche un message indiquant la raison ou les actions à réaliser avant de pouvoir déployer.

Le déploiement depuis la console ne fonctionne que sur les agents connectés aux gestionnaires d'agents. Pour appliquer des mises à jour de configuration ou des mises à jour logicielles à des agents non connectés aux gestionnaires, reportez-vous à la section Mettre à jour les agents.

10. Gérer les périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs, selon leur type, leur niveau de confiance, leur contenu, etc.

Le tableau suivant dresse la liste des protections applicables pour chaque type de périphérique, et les règles de sécurité permettant de les configurer.

Périphérique	Je veux ...	J'utilise ...
USB	Contrôler l'utilisation de certains types de périphériques USB en fonction de leurs caractéristiques (e.g., classe, vendeur, numéro de série). **Exemple** : Autoriser seulement les souris USB sans fil fournies par la société ou interdire tout branchement de clé USB.	Les règles de contrôle d'accès aux périphériques USB dans le menu **Sécurité > Politiques**, règles Périphériques > USB.
	Bloquer l'accès à tout périphérique inconnu n'ayant pas été contrôlé par une station blanche (sas de décontamination).	• La configuration des groupes d'agents dans le menu **Environnement > Agents > Politiques** > Confiance des périphériques. • Les règles de contrôle du stockage sur périphériques USB dans le menu **Sécurité > Politiques**, règles Périphériques > Stockage USB. • Le panneau de gestion de la confiance des périphériques USB dans le menu Sécurité > Périphériques.
	Contrôler l'accès aux données sur un périphérique de stockage de masse USB. **Exemple** : Autoriser seulement l'accès aux fichiers de type bureautique.	• Les règles de contrôle d'accès aux fichiers dans le menu **Sécurité > Politiques**, règles Ressources ACL > Fichier. Cocher l'option type de volume **Amovible** dans l'identifiant. - ou - • Les règles de contrôle du stockage sur périphériques USB dans le menu **Sécurité > Politiques**, règles Périphériques > Stockage USB.
	Contrôler l'exécution d'une application depuis un périphérique amovible de stockage de masse. **Exemple** : Autoriser seulement un logiciel spécifique du service informatique à s'exécuter.	• Les identifiants d'applications dans le menu **Sécurité > Politiques**, règles Identifiants > Identifiants d'applications. Cocher l'option type de volume **Amovible**. - ou - • Les règles de contrôle du stockage sur périphériques USB dans le menu **Sécurité > Politiques**, règles Périphériques > Stockage USB.

Périphérique	Je veux ...	J'utilise ...
Bluetooth	Contrôler l'utilisation de certains types de périphériques Bluetooth en fonction de leurs classes. **Exemple** : Autoriser seulement les casques Bluetooth fournis par la société.	Les règles de contrôle d'accès aux périphériques Bluetooth dans le menu **Sécurité > Politiques**, règles Périphériques > Bluetooth.
CD/DVD	Contrôler l'utilisation des CD et DVD.	Les règles de contrôle d'accès aux périphériques généraux dans le menu **Sécurité > Politiques**, règles Périphériques > Généraux.
Disquette	Contrôler l'utilisation des disquettes.	
Port série	Contrôler l'utilisation des périphériques sur ports série.	

10.1 Contrôler l'accès aux périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs, selon leur type, leur niveau de confiance, leur contenu, etc.

10.1.1 Contrôler l'accès aux périphériques généraux

Cette protection permet de contrôler l'usage des lecteurs de disquette, lecteurs de CD/DVD et ports série sur les postes de travail physiques ou virtuels des utilisateurs. Les lecteurs de disquettes et les ports séries se retrouvent surtout dans des environnements industriels.

Pour chaque type de périphérique, vous avez la possibilité d'autoriser, de bloquer (dans un jeu de règles de protection) ou simplement de surveiller leur utilisation (dans un jeu de règles d'audit).

1. Choisissez le menu **Sécurité > Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques > Généraux**. Par défaut, l'accès à tout est autorisé et les règles sont désactivées. Activez-les en cliquant sur le bouton  à gauche si vous souhaitez bloquer un accès (mode Protection) ou surveiller un accès (mode Audit). Veillez à l'ordre de vos jeux de règles si ces règles sont activées dans plusieurs jeux. Elles pourraient en effet surcharger et annuler l'effet du paramétrage de l'accès aux périphériques généraux qui serait défini dans des jeux de règles placés après.
4. Pour chaque type de périphérique, sélectionnez l'action à effectuer lors de l'utilisation ou du branchement du périphérique. Si vous sélectionnez l'action **Bloquer** ou **Audit**, un log sera généré uniquement lors de la première utilisation du périphérique.
5. Dans le bandeau en haut de la règle :
   - Sélectionnez les paramètres des logs qui seront émis par cette règle.
   - Spécifiez si une action doit être effectuée lors de l'émission d'un log pour cette règle.

Les disquettes ou CD/DVD insérés dans des lecteurs USB externes, ainsi que les ports série reliés par câble USB sont considérés à la fois comme périphériques USB et comme lecteurs de disquette ou de CD/DVD, ou des ports série internes. Leur utilisation peut donc être bloquée soit depuis l'onglet **Généraux**, soit depuis l'onglet **USB**.

10.1.2 Contrôler l'accès aux périphériques Bluetooth

Cette protection permet de contrôler l'usage des périphériques Bluetooth sur les postes de travail des utilisateurs.

SES Evolution permet de surveiller les connexions et déconnexions Bluetooth via la génération de logs grâce au mode Audit dans un jeu de règles d'audit ou bien de bloquer l'accès aux périphériques Bluetooth dans un jeu de règles de protection.

Les règles permettent de filtrer les périphériques Bluetooth selon leur classe. Pour comprendre les classes Bluetooth, référez-vous à la norme internationale Bluetooth.

NOTE
Si un périphérique Bluetooth multifonction est bloqué par une règle, le blocage porte sur toutes les fonctions. Par exemple, si une règle bloque l'usage de la classe micro, l'utilisation d'un micro-casque est bloquée dans son ensemble.

Pour créer des règles sur les périphériques Bluetooth :

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques** > **Bluetooth**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Périphériques Bluetooth)**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, cliquez sur l'icône  pour ajouter un ou plusieurs identifiants de périphérique Bluetooth.
7. Entrez un nom pour l'identifiant.
8. Sélectionnez la classe de service et la classe majeure du périphérique.
9. Cliquez sur **Valider**.
10. Dans le champ **Accès**, sélectionnez l'action **Autoriser** ou **Bloquer** si vous êtes dans un jeu de règles de protection ou **Autoriser** ou **Audit** si vous êtes dans un jeu de règles d'audit. **Ne pas évaluer le jeu de règles** permet d'ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.
11. Dans le bandeau supérieur de la règle, vous pouvez :
    - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
      Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
    - Sélectionner les paramètres des logs qui seront émis par cette règle.
    - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.
    - Saisir un commentaire.
    - Saisir une description pour expliquer l'objectif de la règle.
12. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
13. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Si vous souhaitez simplement surveiller l'usage des périphériques Bluetooth sur le parc :

1. Dans un jeu de règles d'audit, créez une règle Périphériques Bluetooth.
2. Créez un identifiant qui inclue toutes les classes de périphérique Bluetooth.
3. Sélectionnez l'action **Audit** dans le champ **Accès.**
4. Surveillez les logs remontés à chaque connexion et déconnexion d'un périphérique.

10.1.3 Contrôler l'accès aux périphériques USB

Cette protection permet de contrôler l'usage des périphériques USB sur les postes de travail des utilisateurs.

Les règles peuvent porter sur des classes de périphériques USB (imprimante, vidéo, audio, stockage) et/ou sur des vendeurs, des modèles ou des numéros de série de périphériques.

Pour chaque catégorie de périphérique USB, vous avez la possibilité de :

- Autoriser leur utilisation,
- Bloquer leur utilisation,
- Afficher un message à l'utilisateur pour qu'il confirme ou non l'utilisation du périphérique lorsqu'il le branche. La demande de confirmation est affichée à l'utilisateur actuellement connecté localement sur le poste. Dans les autres cas de branchement du périphérique (connexion à distance, session locale verrouillée, démarrage de la machine, session fermée), le message de confirmation ne s'affiche pas et le périphérique est systématiquement bloqué.
- Surveiller l'utilisation des périphériques USB dans un jeu de règles d'audit.

EXEMPLE 1
SES Evolution permet notamment de détecter les clés USB de type *Rubber Ducky*. Cette clé qui joue le rôle d'un clavier, exécute des scripts malveillants et sauvegarde des informations sur une carte micro SD. Si vous créez une règle qui demande confirmation à l'utilisateur à chaque branchement d'un périphérique de type HID (claviers, souris par exemple), un message l'informera qu'un clavier vient d'être branché. L'utilisateur pourra alors refuser l'accès à ce périphérique malveillant ayant l'aspect d'une clé USB.

EXEMPLE 2
Vous pouvez choisir de n'autoriser que les casques, enceintes et téléphones mobiles fournis par le service informatique de votre entreprise.

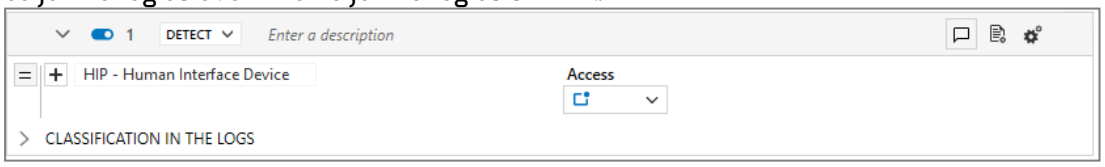
ATTENTION
Un clavier ou une souris (périphérique de type HID) branché avant le démarrage du poste de travail est automatiquement autorisé afin de ne pas rendre le poste inutilisable.
Cependant sur les systèmes d'exploitation Microsoft Windows 10 et 11, si l'option **Activer le démarrage rapide** est sélectionnée sur un ordinateur, lorsqu'on l'éteint, il passe en mode Veille prolongée. Cela signifie que si vous avez défini une règle sur un périphérique HID avec une action de blocage ou de confirmation par l'utilisateur, le périphérique est bloqué à la sortie de la mise en veille prolongée. Vous devez alors opérer un redémarrage complet de l'ordinateur via les menus classiques ou bien en effectuant un appui long sur le bouton d'allumage.

Si vous choisissez d'adopter un mode de fonctionnement "liste blanche", vous allez créer des règles pour autoriser l'usage de certains périphériques sur votre parc. Vous devez alors créer une règle en dernière position bloquant tous les autres périphériques. Nous vous

recommandons de choisir le mode Règle passive pour cette dernière règle afin de ne pas bloquer des périphériques nécessaires au bon fonctionnement des postes de travail. Ainsi vous pouvez tester en production vos règles sur les périphériques USB et les affiner par la suite en consultant les logs.

Pour créer des règles sur les périphériques USB :

1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques** > **USB**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Périphérique USB)**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, cliquez sur l'icône pour indiquer un ou plusieurs identifiants de périphériques sur lesquels la règle porte. Selon que vous souhaitez filtrer un périphérique précis ou une catégorie de périphériques, remplissez tout ou partie des propriétés suivantes :
   - Indiquez un nom pour le périphérique.
   - Sélectionnez la classe USB du périphérique dans la liste déroulante. Si nécessaire, cliquez sur l'icône pour entrer une valeur manuellement.
   - Entrez la sous-classe USB, composée de deux caractères hexadécimaux.
   - Entrez les premières lettres du nom du vendeur pour afficher la liste et sélectionner le vendeur souhaité. Vous pouvez aussi saisir les quatre caractères hexadécimaux normalisés correspondant au vendeur.
   - Sélectionnez le produit dans la liste des produits de ce vendeur ou saisissez les quatre caractères hexadécimaux.
   - Entrez le numéro de série du produit.
7. Dans le champ **Accès**, sélectionnez l'action **Autoriser**, **Bloquer** ou **Demander** si vous êtes dans un jeu de règles de protection ou **Autoriser** ou **Audit** si vous êtes dans un jeu de règles d'audit. **Ne pas évaluer le jeu de règles** permet d'ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.



8. Dans le bandeau supérieur de la règle, vous pouvez :
   - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
     Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
   - Sélectionner les paramètres des logs qui seront émis par cette règle.
   - Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle.
   - Saisir un commentaire.
   - Saisir une description pour expliquer l'objectif de la règle.
9. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos

règles en cliquant sur les flèches en dessous et au-dessus du numéro.

10. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour connaître les identifiants de vendeur ou de produit, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.

Pour connaître les identifiants de sous-classe des périphériques USB, consultez la norme internationale USB.

10.1.4 Contrôler le stockage sur périphériques USB

Cette protection permet de contrôler l'accès à des fichiers stockés sur des périphériques USB dits de stockage (disques durs externes, clés USB).

Les règles peuvent porter sur des périphériques filtrés par identifiants de vendeur ou de produit, ou sur des périphériques connus de SES Evolution et disposant d'un niveau de confiance.

Si l'accès général aux périphériques USB est bloqué, il n'est pas possible d'accéder aux fichiers sur les stockages de masse USB, même si une règle propre à ces périphériques l'autorise. Pour contrôler l'accès général, reportez-vous à la section Contrôler l'accès aux périphériques USB.

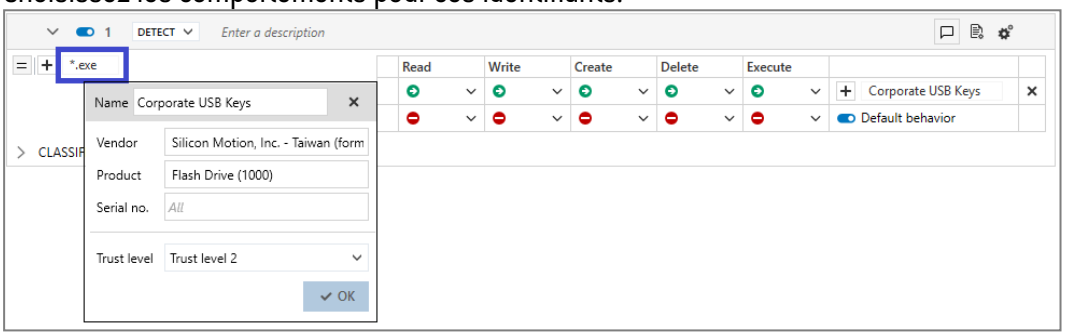
Pour plus d'informations sur les niveaux de confiance, reportez-vous à la section Gérer les périphériques de stockage USB.

La partie gauche d'une règle porte sur les fichiers qui peuvent être présents sur les périphériques USB, et la partie droite sur les périphériques eux-mêmes.

Pour créer des règles d'accès aux fichiers sur des périphériques de stockage USB :

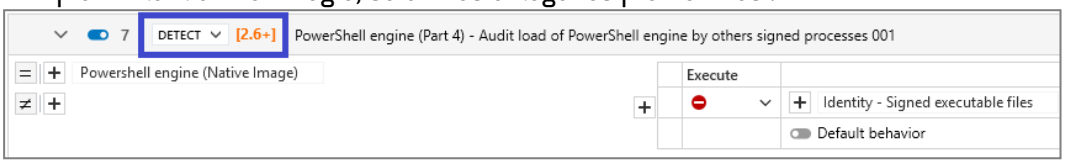
1. Choisissez le menu **Sécurité** > **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques** > **Stockage USB**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter** > **Règle (Périphérique de stockage USB)**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, cliquez sur l'icône  pour ajouter un ou plusieurs identifiants de fichiers. Un fichier peut être identifié par un chemin ou par un flux de données alternatif. Ce champ peut contenir des caractères génériques.
7. Cliquez sur **Valider** pour ajouter l'identifiant.
8. Sélectionnez le comportement par défaut qui s'applique aux périphériques pour les fichiers concernés par la règle, pour les différents types d'opération : autoriser ou bloquer (règle de protection).
   Vous pouvez aussi :
   - **Ne pas évaluer le comportement** pour ignorer la sous-règle si le comportement est détecté et passer au comportement suivant.
   - **Ne pas évaluer le jeu de règles** pour ignorer toutes les règles contenues dans ce jeu de règles et évaluer le jeu de règles suivant.

9. Pour exclure des périphériques spécifiques du comportement par défaut, cliquez sur **+ Ajouter un comportement spécifique** :
   a. Ajoutez un ou des identifiants de périphériques. Vous pouvez identifier les périphériques soit par les identifiants de vendeur ou de produit, soit par le niveau de confiance accordé par SES Evolution au périphérique.
      - Pour connaître les identifiants de vendeur ou de produit, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.
      - Pour en savoir plus sur les niveaux de confiance, reportez-vous à la section Gérer les périphériques de stockage USB.
   b. Choisissez les comportements pour ces identifiants.



10. Dans le bandeau supérieur de la règle, vous pouvez :

- Si besoin, réagencer l'ordre des règles en cliquant sur au survol de la règle. Chaque règle affiche dans le bandeau son numéro de rang.
- Désactiver la règle. Pour plus d'informations, reportez-vous à la section Désactiver une règle de sécurité.
- Indiquer l'intention de la règle, selon des catégories pré-définies :



  - Unclassified : règle non classifiée.
  - Nominal : règle passante se conformant au comportement nominal des applications.
  - Protect : règle bloquante avec un niveau de gravité élevé du log.
  - Protect silent : règle bloquante avec un niveau de gravité en dessous des seuils de logs affichés par défaut sur l'agent et sur la console. Permet de protéger des accès à des ressources estimées sensibles, même s'ils sont effectués par des programmes sans intention malveillante. Ces programmes pouvant être nombreux, une règle avec une gravité de logs trop élevée pourrait déclencher une génération massive de logs.
  - Detect : règle d'audit ou règle passive, sans blocage.
  - Context : règle participant à la construction d'un graphe d'attaque.
  - Syslog : règle déclenchant des logs exclusivement envoyés à un serveur Syslog.
  - Watch : règle permettant de surveiller des comportements afin d'affiner la politique de sécurité ou de mieux connaître les événements techniques se produisant sur le parc.

  La sélection d'une de ces catégories n'a pas d'influence sur le paramétrage de la règle. Elles permettent simplement à l'administrateur de classifier ses règles de sécurité selon leur objectif et de les trier en utilisant le filtre dédié **Intention de la règle**. L'intention de la règle est également affichée dans les détails des logs.
- Saisir une description pour expliquer l'objectif de la règle.
- Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.
  Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**. Pour plus d'informations sur les tests de règles et de politiques, reportez-vous à la section Tester une politique de sécurité.
- Indiquer si la règle doit générer un contexte lorsqu'elle s'applique. Par défaut, si la règle émet des logs de niveau *Urgence* ou *Alerte*, elle génère un contexte, mais vous pouvez désactiver cette fonctionnalité. En cas de génération massive de logs similaires, le contexte n'est pas généré. Pour plus d'informations sur la génération massive de logs, reportez-vous à la section Surveiller l'activité des agents SES Evolution .
- Ajouter un commentaire.
- Sélectionner les paramètres des logs qui seront émis par cette règle.

- Spécifier si une action doit être effectuée lors de l'émission d'un log pour cette règle. Vous pouvez demander qu'un script soit exécuté et/ou qu'une analyse Yara ou IoC soit déclenchée. Vous pouvez également demander qu'une notification soit affichée sur l'agent, à condition qu'elle soit associée à un log bloquant et de niveau *Alerte* ou *Urgence*.
- Supprimer la règle.

11. Dépliez la partie **Classification dans les logs** pour indiquer l'intention de l'attaque soupçonnée lorsque la règle s'applique et les tags permettant d'associer la règle au référentiel de MITRE. Ces informations sont ensuite visibles dans les logs générés par la règle. Pour plus d'informations, reportez-vous à la section Classifier les attaques selon le référentiel de MITRE.
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

10.1.5 Contrôler l'exécution sur périphériques amovibles

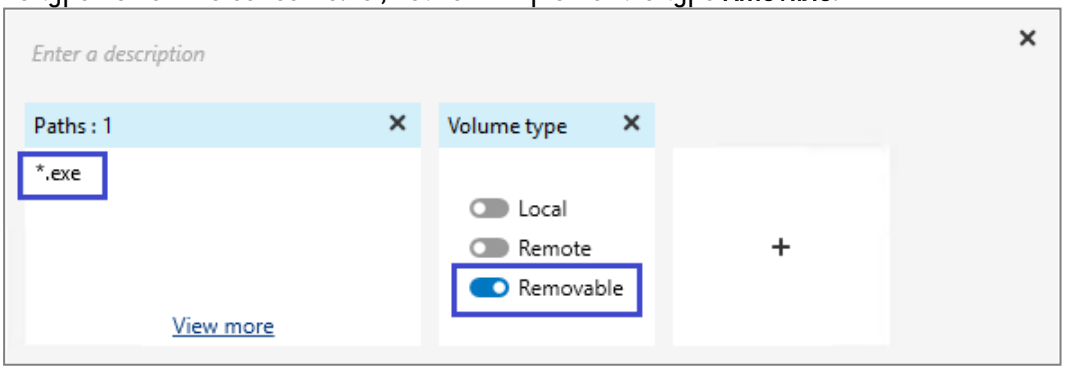
SES Evolution permet de contrôler l'exécution d'applications se trouvant sur des périphériques de stockage USB. Deux méthodes différentes sont disponibles selon le cas d'usage :

- Cas d'usage 1 : Je souhaite qu'une confirmation soit demandée à l'utilisateur dès qu'il tente d'exécuter une application sur un périphérique de stockage USB.
- Cas d'usage 2 : Je souhaite autoriser l'exécution uniquement sur un certain type de clés USB fourni aux collaborateurs par la société. Ces clés sont identifiées par leur ID vendeur et ID produit et/ou par leur niveau de confiance.

Vous pouvez aussi combiner ces deux cas d'usage.

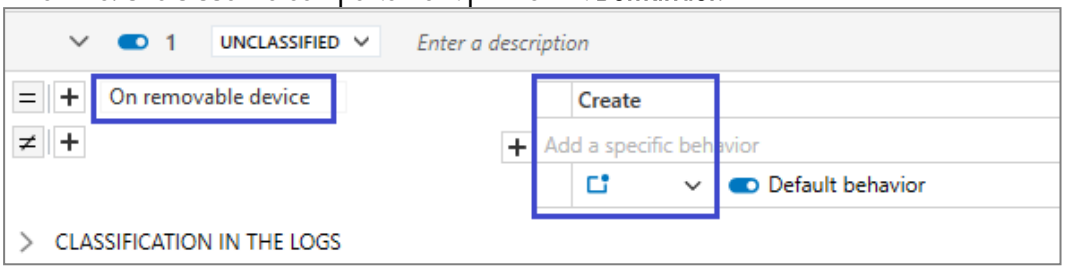
Demander la confirmation de l'utilisateur

1. Créez un identifiant d'applications indiquant :
   - Les applications pour lesquelles vous souhaitez demander une confirmation. Par exemple, entrez le **Chemin** **.exe* pour indiquer que toutes les applications sont concernées.
   - Le type de volume concerné. Ici, activez uniquement le type **Amovible**.



Pour plus d'informations, reportez-vous à la section Créer des identifiants d'applications.

2. Créez une règle de création de processus indiquant :
   - L'identifiant d'applications créé ci-dessus,
   - Que l'utilisateur doit confirmer toute exécution d'applications sur un périphérique amovible. Choisissez le comportement par défaut **Demander**.



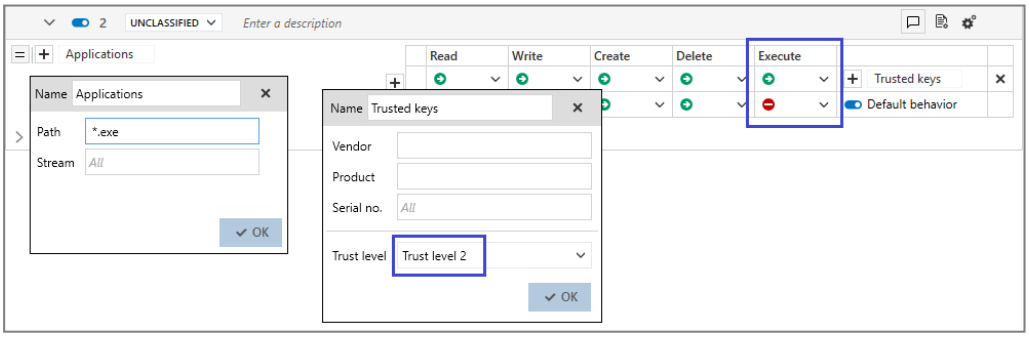
Pour plus d'informations, reportez-vous à la section Contrôler la création de processus.

Une fois cette règle créée, l'utilisateur ne pourra exécuter une application sur un périphérique amovible qu'après avoir confirmé que l'action est bien volontaire. La demande de confirmation et la réponse de l'utilisateur font l'objet d'une entrée dans les logs de l'agent.

Autoriser l'exécution uniquement pour un certain type de clés

Créez une règle Stockage USB indiquant :

- La ou les applications dont vous souhaitez interdire l'exécution si elles se trouvent sur un périphérique de stockage USB. Dans la partie gauche de la règle, entrez par exemple le **Chemin** **.exe* pour indiquer que toutes les applications sont concernées.
- Le comportement par défaut souhaité. Choisissez **Bloquer** dans la liste déroulante **Exécution** pour interdire l'exécution d'applications.
- Le type de clés sur lesquelles l'exécution est autorisée. Dans la partie droite de la règle, saisissez les informations matérielles propres à ce type de clés et/ou le niveau de confiance souhaité.



Pour plus d'informations, reportez-vous à la section Contrôler le stockage sur périphériques USB.

Une fois cette règle créée, l'exécution d'applications sur périphériques de stockage USB sera interdite, sauf pour les périphériques de Niveau de confiance 2.

10.2 Gérer les périphériques de stockage USB

SES Evolution permet de contrôler les périphériques USB dits de stockage (disques durs externes, clés USB). Dans cette section, le terme *périphérique USB* est employé pour faire référence à ce type de périphériques.

Tout périphérique de stockage USB branché sur un agent SES Evolution génère un log et s'affiche dans le panneau **Périphériques** de la console d'administration si les options de

détection sont activées dans le groupe de l'agent. Ce panneau vous permet de visualiser tous les périphériques USB qui ont été branchés sur votre parc et de connaître leur niveau de confiance. Vous pouvez aussi modifier le niveau de confiance des différents périphériques et pré-déclarer manuellement des périphériques.

Les périphériques USB contenant plusieurs partitions ne sont pas supportés par SES Evolution. La liste des périphériques les affiche mais les informations les concernant sont erronées.

Certaines opérations sur les périphériques peuvent être automatisées pour un groupe d'agents. Pour plus d'informations, reportez-vous à la section Détecter et configurer le niveau de confiance des périphériques.

Selon que vous souhaitez effectuer des modifications ou uniquement visualiser le panneau **Périphériques**, vous devez disposer du droit **Périphériques amovibles-Modifier** ou **Périphériques amovibles-Afficher**.

10.2.1 Visualiser les périphériques USB

Pour que les périphériques USB branchés sur les agents s'affichent dans la console, vous devez avoir activé au préalable les options de détection dans les groupes d'agent. Pour plus d'informations, reportez-vous à la section Détecter et configurer le niveau de confiance des périphériques.

1. Choisissez le menu **Sécurité** > **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Consultez les informations propres aux périphériques. En plus du nom, de la taille et des informations matérielles, les détails suivants sont disponibles :
   - **État** : Nouveau ou Modifié,
   - **Poste** : Poste de travail sur lequel le périphérique a été branché pour la dernière fois,
   - **Session** : Session utilisateur ouverte lors du dernier branchement du périphérique,
   - Niveau de confiance,
   - **Vu la dernière fois** : Date du dernier branchement du périphérique sur un agent SES Evolution,
   - **Identifiant unique**,
   - **Vu la première fois** : Date du premier branchement du périphérique sur un agent SES Evolution.
   - **Description** : Commentaire personnalisé que vous avez ajouté lors de la modification du périphérique dans SES Evolution,
3. Toutes les colonnes ne sont pas affichées par défaut. Pour afficher des colonnes supplémentaires, faites un clic droit sur la ligne des en-têtes de colonnes et cochez celles qui vous intéressent.
4. Dans la zone **Filtres**, choisissez les périphériques USB que vous souhaitez afficher dans la liste en filtrant selon leur niveau de confiance **actuel** et/ou **souhaité**. Cliquez sur **Effacer les filtres** en haut à droite pour afficher de nouveau la totalité des périphériques USB.

10.2.2 Ajouter une description à un périphérique USB

1. Choisissez le menu **Sécurité** > **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.

3. Dans **Description**, cliquez sur l'icône pour ajouter le commentaire de votre choix.
4. Dans la zone **Niveau de confiance**, choisissez l'action **Conserver le niveau de confiance**.
5. Cliquez sur **Valider**. Le commentaire ajouté s'affiche dans la colonne **Description** du périphérique USB.

10.2.3 Modifier le niveau de confiance d'un périphérique USB

Dans SES Evolution il existe trois niveaux de confiance pour les périphériques USB :

- **Niveau 0** : Pour l'agent SES Evolution, le périphérique n'est ni enrôlé, ni de confiance. Le périphérique a été branché sur un agent SES Evolution mais le backoffice ne lui a pas encore attribué d'identifiant unique.
- **Niveau 1** : Pour l'agent SES Evolution, le périphérique est enrôlé, mais pas de confiance. Le périphérique est connu et le backoffice lui a attribué un identifiant unique. Soit son contenu n'a pas encore été vérifié, soit il a changé depuis la dernière vérification (dans le cas d'une altération sur une machine en dehors du parc SES Evolution par exemple). Pour passer au niveau 2, le périphérique doit être analysé par une station blanche.
- **Niveau 2** : Pour l'agent SES Evolution, le périphérique est enrôlé et de confiance. Le périphérique est connu du backoffice par un identifiant unique et son contenu est considéré comme étant de confiance. Ce niveau indique que le périphérique a été vérifié par un antivirus sur une station blanche SES Evolution et qu'il ne contient pas de fichier malveillant. Ce niveau de confiance est conservé tant que le contenu du périphérique est modifié au sein du parc SES Evolution.

Le niveau de confiance d'un périphérique est reconnu au sein de tout votre parc SES Evolution. Il ne dépend pas des groupes d'agents.

Une fois les niveaux de confiance attribués, utilisez-les pour filtrer les périphériques USB autorisés dans votre parc. Par exemple, protégez votre parc en créant une règle qui n'autorise que les périphériques USB de niveau 2. Pour plus d'informations, reportez-vous à la section Contrôler le stockage sur périphériques USB.

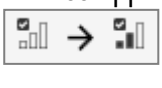
Pour des raisons de sécurité, la modification du niveau de confiance d'un périphérique USB n'est pas possible dans les cas suivants :

- Si la session utilisateur sur l'agent est verrouillée ou fermée,
- Si l'agent est contrôlé à distance via une connexion bureau à distance,
- Si le périphérique était déjà branché lors du démarrage de l'agent.

Le périphérique doit être inséré après l'ouverture de la session utilisateur sur le poste de travail physique pour que son niveau de confiance puisse être modifié.

Accorder le niveau de confiance 1 à un périphériques USB

1. Choisissez le menu **Sécurité** > **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.
3. Dans la zone **Niveau de confiance**, choisissez l'action **Augmenter le niveau de confiance des périphériques de niveau 0**.
4. Cliquez sur **Valider**.

   Le changement de niveau de confiance apparaît dans la colonne correspondante du panneau **Périphériques**. L'icône  signifie que le périphérique de niveau 0

passera au niveau 1 à son prochain branchement sur un agent SES Evolution.

5. Pour appliquer ce changement sur les agents, choisissez le menu **Sécurité** > **Déploiement** et cliquez sur le bouton **Déployer**.
6. Branchez le périphérique que vous avez modifié sur un agent SES Evolution (ou rebranchez-le s'il était resté branché). Il s'affiche dans le panneau des périphériques avec son nouveau niveau de confiance 1  .

Le niveau 1 peut aussi être accordé automatiquement à tout périphérique branché sur un agent SES Evolution si l'option **Autoriser l'identification d'un périphérique** est activée dans la configuration d'un groupe d'agents. Pour plus d'informations, reportez-vous à la section Détecter et configurer le niveau de confiance des périphériques

Accorder le niveau de confiance 2 à un périphérique USB

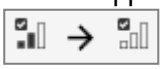
Le niveau de confiance 2 ne peut être accordé qu'après le branchement du périphérique USB sur une station blanche. Une station blanche est un agent SES Evolution chargé d'analyser les périphériques USB du parc et de leur accorder le niveau de confiance maximum s'ils sont considérés comme fiables. Elle dispose en général d'un ou plusieurs antivirus plus puissants que les autres agents du parc, et d'une politique de sécurité SES Evolution spécifique.

1. Configurez votre agent SES Evolution en tant que station blanche :
   - Ajoutez-le dans un groupe d'agents où il sera l'unique agent.
   - Paramétrez le groupe d'agents en activant les options **Accorder la confiance aux périphériques vides** et **Analyse automatique du périphérique**.
   - Déployez la politique sur l'agent depuis le menu **Sécurité** > **Déploiement**.
2. Branchez le périphérique USB sur la station blanche.
   S'il est considéré comme fiable, alors il s'affiche directement dans le panneau **Périphériques** avec le niveau de confiance maximum. Il perd ce niveau de confiance dès que son contenu est modifié en dehors du parc SES Evolution. Branchez-le de nouveau sur la station blanche pour rétablir le niveau de confiance maximum.

Retirer la confiance d'un périphérique USB

Retirer la confiance d'un périphérique USB signifie le faire passer au niveau 0 de confiance.

1. Choisissez le menu **Sécurité** > **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.
3. Dans la zone **Niveau de confiance**, choisissez l'action **Retirer la confiance des périphériques de niveau 1 ou 2**.
4. Cliquez sur **Valider**.

   Le changement de niveau de confiance apparaît dans la colonne correspondante du panneau **Périphériques**. L'icône  signifie que le périphérique de niveau 1 passera au niveau 0 à son prochain branchement sur un agent SES Evolution.

5. Pour appliquer ce changement sur les agents, choisissez le menu **Sécurité** > **Déploiement** et cliquez sur le bouton **Déployer**.
6. Branchez le périphérique que vous avez modifié sur un agent SES Evolution (ou rebranchez-le s'il était resté branché). Il s'affiche dans le panneau des périphériques avec son nouveau niveau de confiance 0  .

10.2.4 Pré-déclarer des périphériques USB

Pré-déclarer des périphériques USB permet de préparer leur identification. Lorsqu'ils seront branchés sur un agent SES Evolution, ils seront enrôlés : l'agent les reconnaîtra et leur appliquera automatiquement le niveau de confiance prédéfini. Par exemple, vous pouvez pré-déclarer les périphériques que vous avez distribués aux collaborateurs afin de leur attribuer automatiquement un niveau de confiance 1 dès leur premier branchement sur un agent SES Evolution.

Pour des raisons de sécurité, SES Evolution n'enrôle pas les périphériques USB branchés dans les cas suivants :

- Si la session utilisateur sur l'agent est verrouillée ou fermée,
- Si l'agent est contrôlé à distance via une connexion bureau à distance,
- Si le périphérique était déjà branché lors du démarrage de l'agent.

Le périphérique doit être inséré après l'ouverture de la session utilisateur sur le poste de travail physique pour que son enrôlement soit possible.

Pour pré-déclarer des périphériques USB :

1. Choisissez le menu **Sécurité** > **Périphériques**.
2. Cliquez sur le bouton **Ajouter**.
3. Spécifiez les identifiants **Vendeur** et **Produit** du périphérique.
4. Optionnellement, indiquez son **N° de série** et une **Description**.

   Pour connaître ces identifiants, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.
5. Choisissez quel **Niveau de confiance** lui sera attribué automatiquement lorsqu'il sera branché sur un agent SES Evolution : Niveau de confiance 0 ou 1.
6. Cliquez sur **Valider**.
   Une ligne correspondant à ce nouveau périphérique s'affiche dans le panneau **Périphériques**. Seules les informations que vous avez spécifiées sont visibles.
7. Pour envoyer les informations des périphériques pré-déclarés aux agents, choisissez le menu **Sécurité** > **Déploiement** et cliquez sur le bouton **Déployer**.
   Au branchement du périphérique sur un agent SES Evolution, il est identifié et les informations présentes dans le panneau **Périphériques** sont complétées.

10.2.5 Supprimer un périphérique USB

1. Choisissez le menu **Sécurité** > **Périphériques**.
2. Faites un clic droit sur le périphérique USB à supprimer, et choisissez le menu **Supprimer**.
   Le périphérique n'est plus affiché dans la liste.

   Lors de son prochain branchement sur un agent SES Evolution, le périphérique s'affichera à nouveau dans le panneau **Périphériques** avec le niveau de confiance dont il disposait à sa suppression.

10.2.6 Importer et exporter une liste de périphériques USB

Dans le panneau **Sécurité** > **Périphériques**, vous pouvez importer ou exporter une liste de périphériques USB au format CSV.

Importer une liste de périphériques USB

1. Choisissez le menu **Sécurité** > **Périphériques**.
2. Cliquez sur le bouton **Importer** et choisissez le fichier d'import.
   Le fichier doit être au format CSV et composé d'une ligne par périphérique. La syntaxe est la suivante :
   `ID produit, N° de série, ID vendeur, Niveau de confiance, Description`

   Les ID produit, ID vendeur (au format hexadécimal sur quatre caractères) et le niveau de confiance sont obligatoires.

EXEMPLE
La ligne `5834,,0A5C,2,Clé Stormshield` importe une clé dont les caractéristiques sont :

ID produit	5834
N° de série	non renseigné
ID vendeur	0A5C
Niveau de confiance	1
Description	Clé Stormshield

Exporter une liste de périphériques USB

1. Choisissez le menu **Sécurité** > **Périphériques**.
2. Pour exporter tous les périphériques de la liste, cliquez sur le bouton **Exporter**.
   - ou-
   Pour exporter uniquement certains périphériques, sélectionnez-les dans la liste, puis cliquez sur la flèche du bouton **Exporter > Exporter la sélection**.
3. Choisissez le nom du fichier et le dossier vers lequel vous souhaitez faire l'export.

10.3 Cas d'usage : Gérer l'accès à un fichier sur une clé USB

L'accès à un fichier sur une clé USB peut être bloqué à plusieurs niveaux. SES Evolution vérifie dans l'ordre :

Les règles Périphériques USB

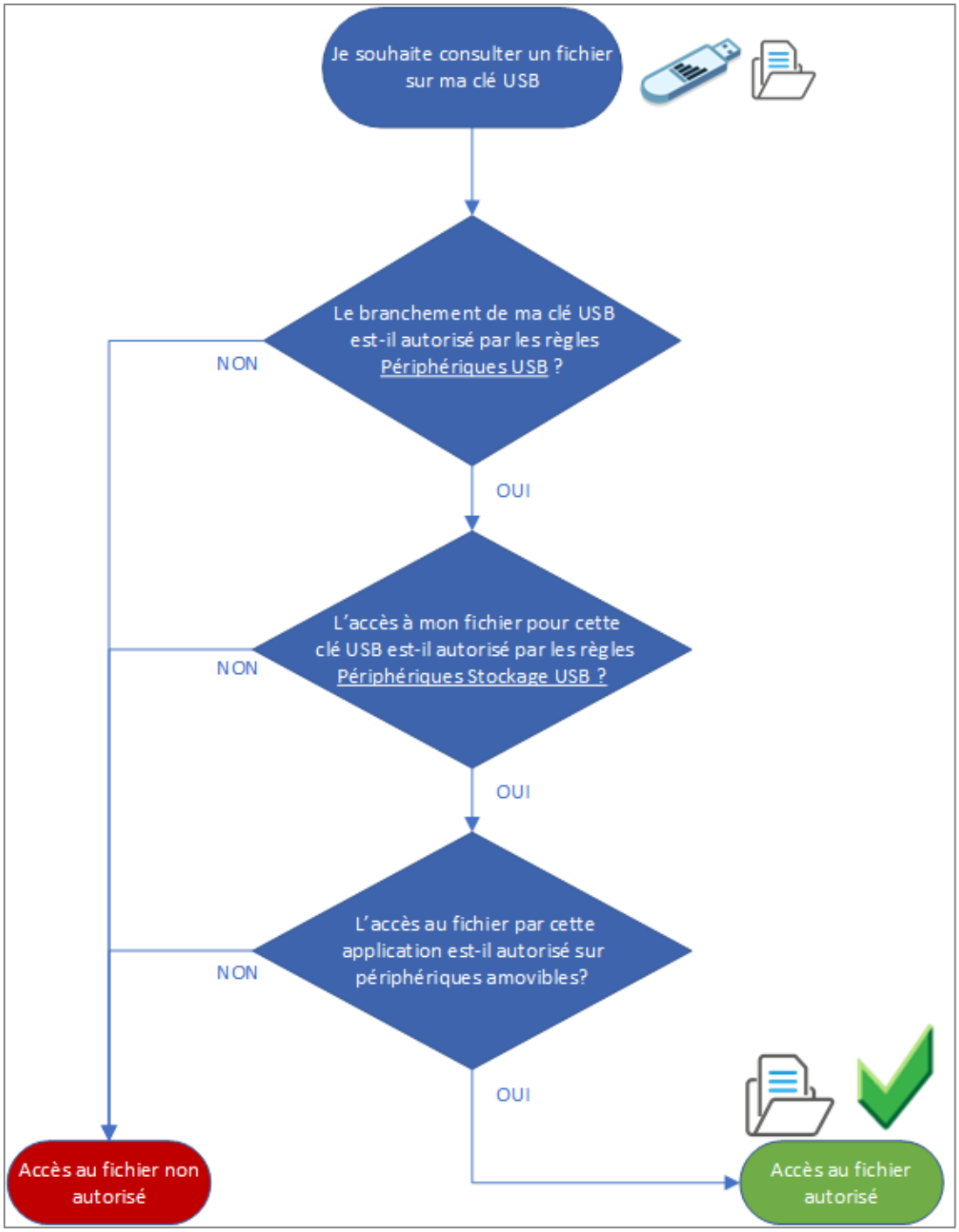
- Vérification de la clé USB : classe et sous-classe USB, ID du vendeur, produit et numéro de série.

Les règles Périphériques Stockage USB

- Vérification du chemin et nom du fichier,
- Vérification du vendeur, produit et numéro de série de la clé USB,
- Vérification du niveau de confiance de la clé USB.

Les règles Ressources ACL Fichier/ ID d'application

- Vérification que le fichier/l'application est accessible lorsqu'il se trouve sur un support amovible.



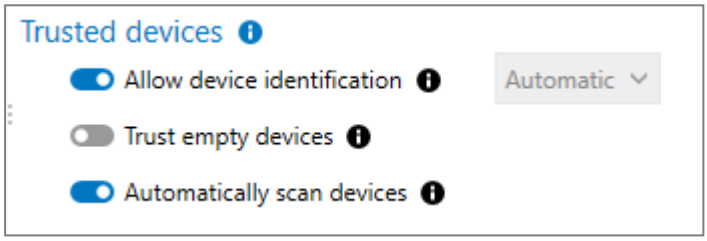
10.4 Cas d'usage : Bloquer l'accès aux clés USB non décontaminées

De nombreux malwares peuvent se propager via des clés USB. Pour contrôler de façon sûre les clés USB branchées sur votre parc, vous pouvez rendre obligatoire la décontamination de toute clé dont le contenu a été modifié à l'extérieur de la société. Pour ce faire, mettez en place des stations blanches équipées de solutions antivirus qui analysent les périphériques branchés. Ensuite, configurez SES Evolution pour qu'il automatise cette analyse et garantisse que seules les clés USB ayant le niveau de confiance approprié soient autorisées sur les agents SES Evolution.

Les clés USB modifiées sur un poste de travail protégé par SES Evolution conservent leur niveau de confiance et ne nécessitent pas de décontamination.

10.4.1 Créer un groupe d'agents pour les stations blanches

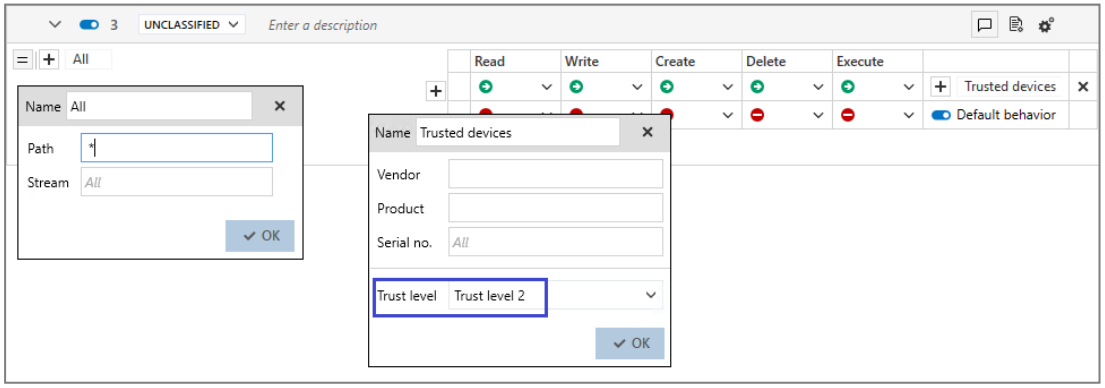
1. Créez un groupe d'agents *Décontamination* regroupant tous les postes de travail utilisés comme sas de décontamination de clés USB. Pour plus d'informations, reportez-vous à la section Créer et configurer les groupes d'agents
2. Dans la section **Confiance des périphériques**, activer les options suivantes :
   - **Autoriser l'identification d'un périphérique - Automatique**,
   - **Analyser automatiquement le périphérique**.



Pour plus d'informations, reportez-vous à la section Détecter et configurer le niveau de confiance des périphériques

10.4.2 Bloquer les clés USB selon leur niveau de confiance

1. Créez une règle de sécurité de type **Stockage USB**.
2. Dans la partie gauche de la règle, ajoutez un identifiant de fichier *All* correspondant à tous les fichiers.
3. Dans le comportement par défaut, bloquez tous les accès.
4. Ajoutez un comportement spécifique qui autorise tous les accès pour toutes les clés ayant le niveau de confiance 2.



Cette règle permet d'autoriser tout accès aux périphériques de confiance niveau 2 et de bloquer tout ceux ayant un niveau inférieur.

5. Appliquez cette règle à tous les groupes agents pour lesquels vous souhaitez contrôler le niveau de confiance des clés USB.

Pour plus d'informations, reportez-vous à la section Contrôler le stockage sur périphériques USB.

11. Surveiller l'activité des agents SES Evolution

La solution SES Evolution fournit une vue précise de l'activité des agents SES Evolution via différents types de logs classés par niveaux de gravité.

Les logs contiennent notamment l'heure d'un événement, l'agent sur lequel il s'est produit, l'identité du processus qui a fait l'action, et en cas de blocage, des informations sur le blocage.

11.1 Prérequis

Aucun nom de fichier court au format MS-DOS 8.3 ne doit apparaître dans les logs SES Evolution. La génération par Windows de noms courts doit être désactivée sur tous les agents SES Evolution.

- Pour désactiver les noms courts, attribuez la valeur 1 à la clé de registre *NtfsDisable8dot3NameCreation* dans *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem*.

11.2 Différents types de logs

Les agents SES Evolution génèrent plusieurs types de logs :

- Les **logs d'événements** sont des logs simples auxquels aucun contexte n'est attaché. Ils fournissent par exemple des informations sur le blocage d'actions utilisateurs interdites par les politiques de sécurité, permettent d'auditer certaines opérations, etc. Les événements peuvent être de plusieurs types :

Événements de protection	Émis en cas de blocage ou d'audit d'une opération par une règle de sécurité. Par exemple, le processus *illegimate_process.exe* a tenté de lancer le processus *abused_process.exe*.
Événements d'autoprotection	Émis en cas d'événements suspects sur le système Windows non liés à une règle de sécurité. Par exemple, l'utilisateur a tenté de supprimer un fichier protégé.
Événements de fonctionnement	Émis en cas d'événements liés au fonctionnement global de SES Evolution. Par exemple, l'agent a appliqué une nouvelle politique.
Événements externes	Émis en cas d'événements liés aux règles d'audit de type *Transfert d'événements externes* et *OSSEC*.
Événements Windows Defender	Émis en cas de remontée d'événements Windows liés à la fonctionnalité *Protection contre les virus et les menaces*. Ces logs ne sont affichés que si la politique de sécurité contient le jeu de règles *Stormshield - Transfert des événements de Windows Defender*.

- Les **logs d'alerte** indiquent qu'une attaque s'est produite. Ils sont accompagnés d'un contexte permettant d'analyser ce qui a conduit à l'action malveillante.
- Les **logs de contexte** sont enregistrés en continu sur les agents et représentent un audit global des actions effectuées sur un poste de travail. Ils ne sont pas conservés et sont transmis uniquement lorsqu'une alerte est détectée. Ils fournissent des informations sur les activités sur le poste juste avant et après l'attaque.

Consultez les logs des agents sur la console d'administration et sur l'interface de l'agent. Ils seront aussi visibles sur le serveur Syslog si vous l'avez configuré.

Selon que vous souhaitez effectuer des modifications ou uniquement visualiser le panneau **Logs agents**, vous devez disposer du droit **Logs agents-Modifier** ou **Logs agents-Afficher**.

Vous pouvez configurer quels niveaux de logs sont envoyés vers la console, l'agent et le serveur Syslog. Pour plus d'informations, reportez-vous aux sections Configurer la transmission des logs émis par les agents et Configurer la gestion des logs.

L'agent dispose d'un mécanisme de protection contre la génération massive de logs.

Lorsqu'il détecte un certain nombre de logs strictement identiques ou similaires sur une courte période, il arrête de générer les logs similaires suivants et les comptabilise. De plus, il ne génère pas de contexte même si la règle de sécurité associée au log est configurée pour. Les protections restent cependant actives et les autres logs sont toujours générés.

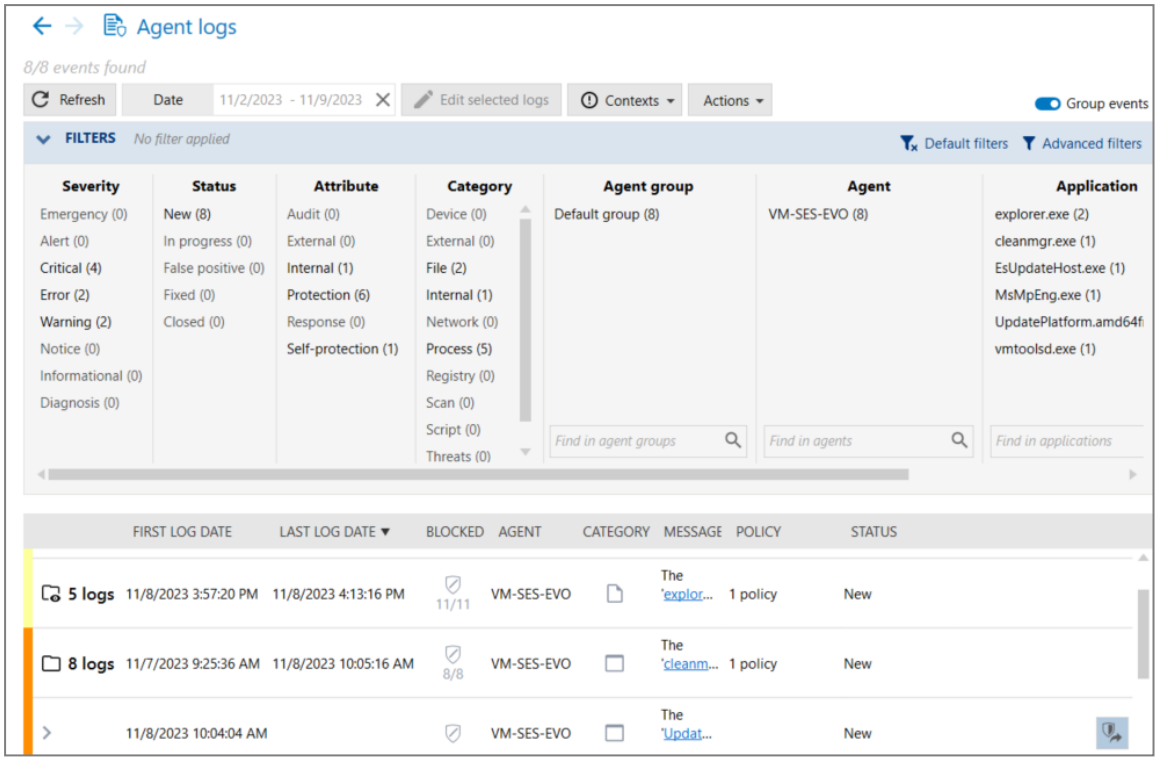
Il émet alors un log spécifique signalant la détection de la génération massive d'un log. Lorsque la génération de logs repasse en dessous d'un certain seuil, il émet un autre log pour signaler la fin de la génération des logs similaires. Selon le paramétrage d'affichage des logs, ces deux logs peuvent s'afficher sur l'interface de l'agent et dans la console d'administration.

Dans la console d'administration, depuis les logs signalant le début et la fin de la génération massive d'un log, vous pouvez accéder au log à l'origine du déclenchement de la protection. Si nécessaire, créez une exception sur ce log ou bien adaptez vos politiques de sécurité afin d'éviter la répétition du phénomène. Pour créer une exception, consultez la section Ajouter des exceptions sur les logs.

11.3 Visualiser et gérer les logs des agents dans la console d'administration

Tous les logs que vous avez configurés afin qu'ils s'affichent sur la console sont visibles dans le menu **Environnement > Logs agents**. Celui-ci vous permet d'analyser les logs, de les filtrer, de les gérer, d'ajouter des exceptions pour que certains logs ne soient plus générés et d'exécuter des analyses Yara ou IoC à partir de logs. Vous pouvez aussi Analyser les contextes pour comprendre une attaque et Gérer les tâches de remédiation à partir de logs.

La date des logs agents affichée sur la console est basée sur le fuseau horaire paramétré sur la machine hébergeant la console.

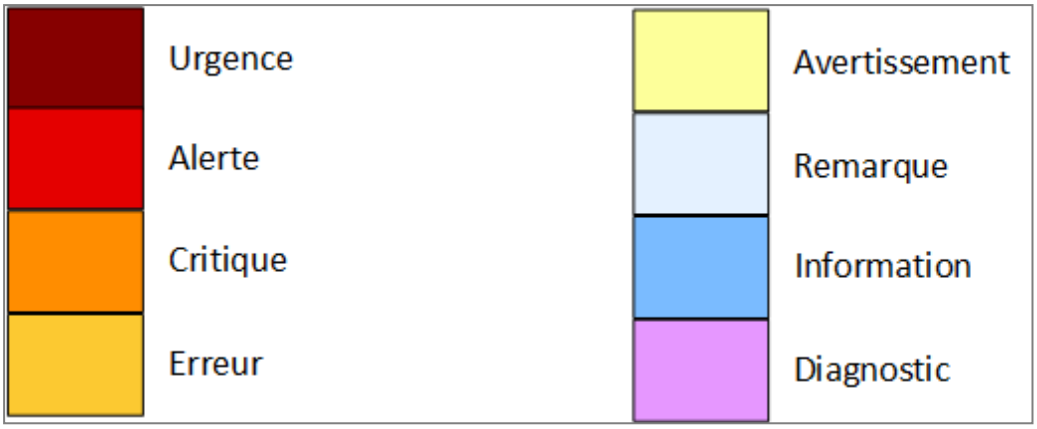


Si un agent est déconnecté et que ses logs ne sont pas transmis au gestionnaire d'agents, vous pouvez exporter ses logs pour pouvoir les importer et les visualiser ensuite dans le panneau des **Logs agents**.

Pour gérer les logs et créer des exceptions, vous devez disposer du droit **Logs agents - Modifier**.

11.3.1 Consulter les logs

1. Choisissez le menu **Environnement > Logs agents**.
   La liste des logs de tous les composants s'affichent en fonction des filtres actifs.
   À la première ouverture du panneau des logs, ce sont les logs *Nouveaux* et *En cours*, de niveau *Urgence* et *Alerte*, émis dans les dernières 24 heures qui sont visibles.
   Les logs identiques générés par plusieurs agents composent un *Événement*. Par défaut ils sont regroupés sur une même ligne et signalés par l'icône .
2. Si vous souhaitez afficher la vue non groupée des logs, désactivez l'option **Grouper les événements** en haut à droite.
3. Pour visualiser les détails des logs d'un groupe, cliquez sur l'icône de logs groupés, puis dépliez le groupe en cliquant sur le + à gauche du groupe.
4. Dans la vue principale des logs ou dans la vue d'un groupe de logs, cliquez sur le bouton **Date** pour choisir la période à visualiser, puis cliquez sur **Appliquer**. La flèche double dans le menu déroulant permet de sélectionner la période à l'aide d'un calendrier. La croix à droite du champ **Date** réinitialise la période aux dernières 24 heures.
   La liste des logs émis lors de la période sélectionnée s'affiche.
   La couleur à gauche d'une ligne de log indique le niveau de gravité : il existe 8 niveaux de gravité qui correspondent aux niveaux du protocole Syslog. Une couleur est attribuée à chacun :

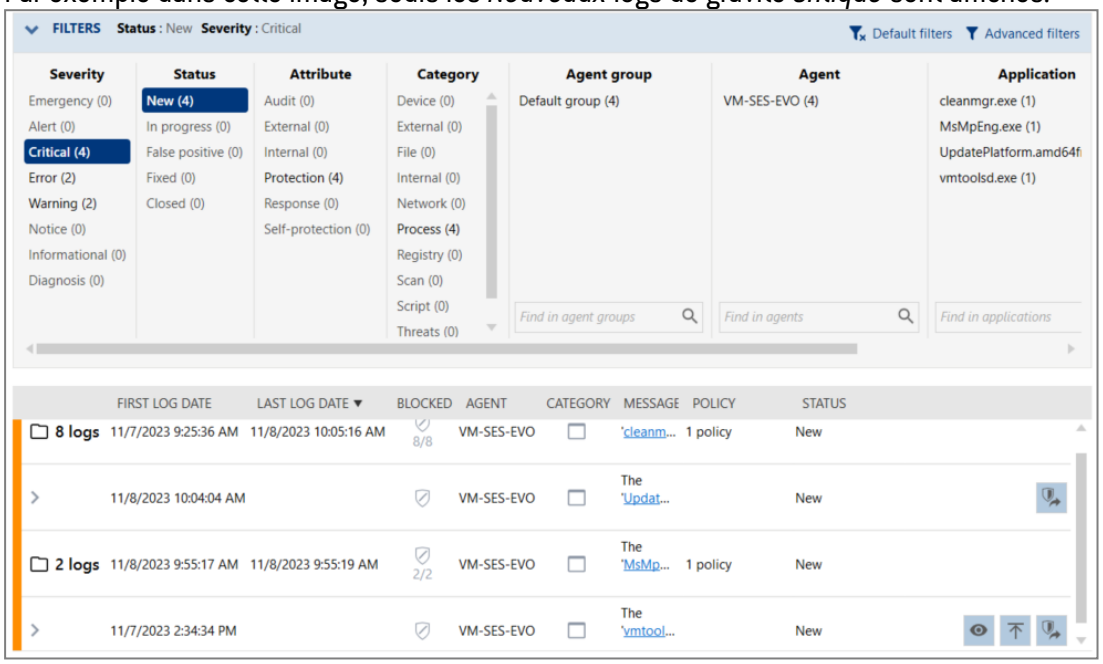


5. Dans la colonne **Agent** en vue "non groupée", cliquez sur les trois points pour choisir quelles informations afficher concernant l'agent : Nom d'hôte, d'utilisateur et/ou adresse IP.
6. Sur la droite des logs, cliquez sur l'icône  si vous souhaitez consulter ou modifier la règle responsable du log. Dans le panneau des règles, celle-ci se distingue des autres règles car elle est grisée et affiche une barre bleue sur la gauche.
7. Dans la vue principale des logs ou dans la vue d'un groupe de logs, cliquez sur la petite flèche à gauche du log pour l'ouvrir et afficher des informations complémentaires :
   - Onglet **Détails** : Description complète des processus, actions, etc. ayant causé le log. Deux liens permettent de vérifier directement le caractère malveillant de chaque processus impliqué sur le moteur de recherche Google ou sur le site VirusTotal. Cette fonctionnalité nécessite que le poste exécutant la console d'administration ait accès à internet.
   - Onglet **Log brut** : Code du log au format JSON.

   Si vous suspectez un problème et que vous avez besoin d'afficher plus de logs, modifiez les paramètres des logs dans le groupe d'agents ou dans la règle de sécurité.

11.3.2 Filtrer les logs

1. Dans le tableau **Filtres** du panneau **Logs agents**, activez des filtres pour personnaliser votre liste de logs. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant puis cliquez sur **Appliquer**.
Par exemple dans cette image, seuls les *Nouveaux* logs de gravité *Critique* sont affichés.



- Le nombre indiqué entre parenthèses est le nombre de logs distincts et non pas le nombre total de logs. Les logs identiques composent un seul événement et ne sont comptabilisés qu'une seule fois. Dans l'image ci-dessus, il y a 12 logs de niveau critique, mais seuls quatre logs sont comptabilisés : deux événements (i.e., groupements de logs) et deux logs individuels.
- La colonne **État** permet de filtrer les logs selon l'état que vous leur avez attribué. Voir la section Gérer les logs.
- Dans les colonnes **Groupe d'agents** et **Agent**, vous pouvez rechercher les groupes et agents souhaités en entrant tout ou partie de leur nom dans le champ de recherche.
- Les colonnes **Application** et **Application cible** permettent de filtrer les logs selon les applications qui ont effectué l'action et celles sur lesquelles l'action a été appliquée.

2. Cliquez sur **Filtres avancés** pour ajouter d'autres filtres plus précis et affiner ainsi votre liste de logs. Dans la fenêtre des filtres avancés :
   a. Cliquez sur **Ajouter un filtre**.
   b. Choisissez le type de filtre souhaité. Une ligne apparaît dans la fenêtre des filtres avancés.
   c. Entrez la valeur du filtre en choisissant dans une liste ou en la saisissant manuellement.
   d. Spécifiez si le filtre doit inclure la valeur ou l'exclure. Par défaut c'est un filtre d'inclusion : il affiche tous les logs correspondant à la valeur choisie. Cliquez sur l'icône  pour en faire un filtre d'exclusion.
   e. Ajoutez d'autres filtres si besoin. Plus il y a de filtres avancés, plus la liste des logs affichés se réduit.
   f. Cliquez sur **Valider**.

   À tout moment, vous pouvez retrouver le filtrage initial en cliquant sur **Filtres par défaut** : seuls les logs dont la gravité est *Urgence* ou *Alerte* et l'état est *Nouveau* ou *En cours* seront affichés.

11.3.3 Gérer les logs

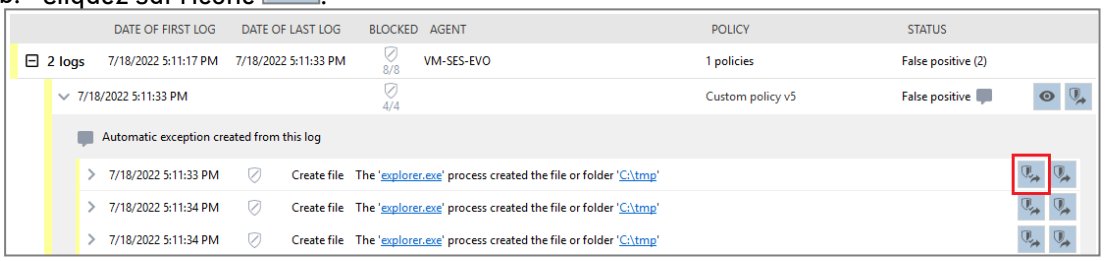
Lorsque vous travaillez sur l'analyse des logs, vous pouvez attribuer un état à chaque log et indiquer le nom de l'utilisateur qui l'a analysé. L'état des logs est une information importante visible sur le tableau de bord de la console d'administration dans la zone **Événements par état**.

1. Dans le panneau **Environnement > Logs agents**, sélectionnez un ou plusieurs logs, puis cliquez sur **Modifier les logs sélectionnés**. La fenêtre **Modifier les logs** s'affiche.
2. Dans la liste **État**, choisissez quel état vous souhaitez attribuer aux logs :
   - **Nouveau** : État par défaut d'un log. Personne n'a encore analysé le log.
   - **En cours** : Le log est en cours d'analyse.
   - **Faux positif** : Le log a été identifié comme faux-positif : il a été déclenché par une règle de sécurité mais ne représente pas une action malveillante. Cet état est attribué automatiquement à un log si vous avez ajouté une exception pour ce log. Pour plus d'informations, reportez-vous à la section Ajouter des exceptions sur les logs.
   - **Corrigé** : Le problème décrit par le log a été réglé.
   - **Clos** : L'analyse du log est terminée. Plus aucune action n'est requise.
3. Dans la liste **Assigné à**, choisissez un nom d'utilisateur à qui assigner le log. Cette liste affiche tous les utilisateurs déclarés dans SES Evolution. Pour plus d'informations, reportez-vous à la section Gérer les utilisateurs de la console d'administration SES Evolution.
4. Dans le champ **Commentaire**, entrez si besoin des informations supplémentaires sur le log ou sur votre action. Si ce champ est rempli, une bulle s'affiche dans la colonne **État** de la liste des logs.
5. Cliquez sur **Valider**.

11.3.4 Ajouter des exceptions sur les logs

Si après avoir analysé un log, vous considérez que l'action qui l'a déclenché n'était pas malveillante et qu'elle n'aurait pas dû être bloquée, vous pouvez ajouter une exception sur ce log. Cela évitera que cette action soit à nouveau bloquée et/ou ne génère un log. De même, si vous considérez qu'un fichier a été mis en quarantaine à tort, ajoutez une exception sur le log de quarantaine.

1. Dans le panneau **Environnement > Logs agents**, sélectionnez un ou plusieurs logs de contexte que vous ne souhaitez plus générer à l'avenir, puis cliquez sur **Ajouter des exceptions**. Les opérations suivantes sont automatiquement effectuées :
   - Ajout d'une ou plusieurs règles dans le *Jeu de règles d'exceptions* de la politique de sécurité concernée. Ces règles permettent d'éviter qu'un blocage se produise dans des circonstances identiques. Les identifiants d'applications nécessaires aux règles sont également créés.
   - Attribution de l'état **Faux positif** au log concerné, et mention de l'utilisateur qui a ajouté l'exception.
   - Ajout du commentaire *"Exception automatique créée à partir de ce log"* dans le log.
   - Dans le cas d'une exception sur un fichier mis en quarantaine, le fichier sera automatiquement restauré à son emplacement d'origine au prochain déploiement de l'environnement.
2. Si besoin, vous pouvez consulter ou modifier la règle d'exception créée à partir du log :
   a. Affichez votre log en activant le filtre **Faux positif**.
   b. Cliquez sur l'icône  .



La règle d'exception correspondant à ce log s'affiche. Elle se distingue des autres règles car elle a une barre bleue sur la gauche.
Si la règle est introuvable, c'est qu'elle a été supprimée entre temps.

11.3.5 Procéder à une remédiation à partir d'un log

Si votre parc a fait l'objet d'une attaque visible dans les logs agents, vous pouvez procéder à une remédiation pour limiter l'impact de l'attaque et réparer les éventuels dommages.

1. Dans le panneau **Environnement > Logs agents**, sélectionnez un log et cliquez sur **Tâches > Créer une tâche de remédiation**.
2. Suivez la procédure Gérer les tâches de remédiation.

11.3.6 Exécuter une analyse Yara ou IoC à partir d'un log

Si un log indique qu'un processus ou un fichier est potentiellement malveillant, vous pouvez configurer une analyse Yara ou IoC pour rechercher ce dernier sur l'agent.

1. Dans le panneau **Environnement > Logs agents**, sélectionnez un log et cliquez sur **Tâches**.
2. Sélectionnez le type d'analyse.
   Le panneau des tâches s'affiche et l'agent concerné par le log est directement sélectionné.
3. Suivez la procédure Exécuter une analyse Yara à la demande ou Exécuter une analyse IoC à la demande pour terminer la configuration et lancer l'analyse.

11.3.7 Consulter les logs des agents déconnectés

Lorsqu'un agent n'a pas accès au gestionnaire d'agents, ses logs ne peuvent pas être transmis à la console d'administration et ils ne sont donc pas visibles dans le panneau **Logs agents**. Vous pouvez exporter ces logs pour ensuite les importer dans la console et les consulter comme les autres logs.

Les logs exportés restent présents sur l'agent.

1. Connectez-vous au poste de travail agent en tant qu'administrateur.
2. Double-cliquez sur l'icône dans la barre d'état.
   L'interface de l'agent SES Evolution s'affiche.
3. Dans l'onglet **Aide et Support**, cliquez sur **Événements**.
   La liste des logs de ce poste de travail s'affiche.
4. Cliquez sur le bouton **Exporter les événements...**, et choisissez le dossier de destination.
   Un fichier au format *cab* est généré.
5. Copiez-le sur une clé USB ou envoyez-le par e-mail.
6. Copiez ce fichier *cab* dans le dossier d'import du gestionnaire d'agents, par exemple *C:\ProgramData\Stormshield\SES Evolution\Server\AgentLogs\Import*. Au bout d'une dizaine de secondes, le fichier disparaît du dossier *Import* et les logs qu'il contient sont affichés dans le panneau **Logs agents**.

ASTUCE
Vous avez également la possibilité d'exporter les logs via un script, en lançant le programme EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) avec la commande `/ExportLogs`. En option, vous pouvez spécifier le dossier de destination de l'export dans la ligne de commande.
Par exemple : `EsGui /ExportLogs "C:\Users\Administrator\Desktop\Logs.cab"`

11.4 Visualiser les logs sur l'interface des agents

1. Sur le poste de travail, cliquez sur l'icône dans la barre d'état.
   L'interface de l'agent s'affiche.
2. Dans l'onglet **Aide et Support**, cliquez sur **Événements**.
   La liste des logs de ce poste de travail s'affiche. Un utilisateur administrateur peut voir tous les niveaux de gravité de logs, tandis que seuls les logs de niveau *Alerte* et *Urgence* ayant entraîné un blocage s'affichent pour un utilisateur non administrateur.
   La couleur à gauche d'une ligne de log indique le niveau de gravité.
   Différentes étiquettes de couleurs différentes indiquent :
   - Le niveau de gravité, (e.g., Alerte, Remarque, etc.),
   - Le type de log, par exemple (e.g., Interne, Autoprotection, etc.),
   - La protection mise en œuvre, (e.g., Registre, etc.),
   - L'action effectuée par SES Evolution, (e.g., Bloquer, etc.).
3. Par défaut, vous ne voyez que les logs accessibles à l'utilisateur ayant ouvert la session. Cliquez sur **Afficher tous les logs** pour voir aussi les logs accessibles aux administrateurs. Par exemple, si plusieurs utilisateurs se connectent sur le même poste de travail, vous pouvez ainsi visualiser les logs de toutes les sessions.

4. Filtrez la liste de logs afin d'afficher uniquement ceux qui vous intéressent :
   - Cliquez sur une des étiquettes d'un log pour afficher uniquement la liste des logs ayant cette étiquette. Par exemple, cliquez sur l'étiquette *Registre* pour afficher tous les logs liés à la base de registre.
     Les filtres actifs s'affichent en haut de la fenêtre. Supprimez les filtres pour afficher à nouveau tous les logs.
   - Dans le champ **Rechercher**, entrez une ou plusieurs chaînes de caractères et tapez Entrée pour afficher uniquement les logs contenant ces chaînes.

Si vous suspectez un problème et que vous avez besoin d'afficher encore plus de logs, modifiez les paramètres des logs dans le groupe d'agents ou dans la règle de sécurité.

SES Evolution conserve un historique de logs de 500 Mo. Une fois cette taille atteinte, les logs les plus anciens sont supprimés, en commençant par les logs les moins prioritaires.

11.5 Envoyer des alertes de logs agents par e-mail

Vous pouvez configurer SES Evolution afin d'envoyer des alertes par e-mail aux personnes de votre choix. Les alertes sont déclenchées par certains logs générés sur les agents SES Evolution.

Au préalable vous devez configurer un serveur SMTP. Pour plus d'informations, reportez-vous à la section Configurer un serveur SMTP.

Vous devez disposer du droit **Notifications par e-mails-Modifier** pour configurer l'envoi d'alertes.

Pour envoyer des alertes par e-mail :

1. Dans le menu **Backoffice > Système** de la console d'administration, rendez-vous dans l'onglet **Notifications par e-mail**.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
3. Dans la zone **Alertes des logs agents**, cliquez sur **Ajouter une règle**.
   L'assistant de création d'une règle s'ouvre.
4. Saisissez les paramètres de la règle :
   - **Nom de la règle**.
   - **Préfixe de l'objet de l'e-mail** reçu par le destinataire. Par défaut, l'objet de l'e-mail commence par *SES EVOLUTION*. Le préfixe vous permet d'appliquer un traitement spécifique aux e-mails d'alerte SES Evolution dans votre messagerie.
   - **Fréquence** à laquelle vous souhaitez envoyer un e-mail contenant les alertes, de une minute à 24 heures. L'envoi se fera à la reconnexion de l'agent au gestionnaire d'agents.
   - **Attributs des logs** pour lesquels vous souhaitez déclencher des alertes.
   - Niveaux de **Gravité des logs** pour lesquels vous souhaitez déclencher des alertes.
5. Cliquez sur **Suivant**.
6. Dans le champ en bas de l'écran, saisissez l'adresse e-mail de l'utilisateur destinataire des alertes, choisissez sa langue, puis cliquez sur **Ajouter**.
7. Ajoutez d'autres adresses e-mail si vous souhaitez envoyer les alertes à plusieurs destinataires.
8. Cliquez sur **Créer**.
   La règle est ajoutée dans le tableau de la zone **Alertes des logs agents**.
9. Ajoutez d'autres règles si besoin.

Si dans l'intervalle de temps spécifié, les agents génèrent des logs correspondant aux règles, alors un e-mail d'alerte est envoyé.

Vous pouvez désactiver ou réactiver une règle d'envoi en cliquant sur la case à cocher de la colonne **Activé**. Les boutons d'actions à droite d'une règle permettent de la dupliquer ou de la supprimer.

Vous pouvez arrêter temporairement l'envoi des e-mails en désactivant l'option **Activer les notifications**.

SES Evolution permet également d'envoyer par e-mail des alertes sur les logs système ou tout le contenu du tableau de bord. Pour plus d'informations, reportez-vous aux sections Envoyer des alertes de logs système par e-mail et Envoyer les indicateurs du tableau de bord par e-mail.

11.6 Analyser les contextes pour comprendre une attaque

Les contextes de SES Evolution vous permettent d'analyser finement l'environnement des attaques qui se produisent sur les agents et de déterminer la nature, la provenance et le déroulement de celles-ci. Pour bénéficier de cette fonctionnalité, votre politique de sécurité doit contenir le jeu de règles intégré *Stormshield- Audits pour contextes d'attaque*. Pour plus d'informations, reportez-vous à la section Comprendre les jeux de règles intégrés.

EXEMPLE
Si la protection Détournement de flux d'exécution bloque un malware, l'analyse du contexte permet de retrouver le fichier responsable de l'exécution du malware, et d'où provient ce fichier.

11.6.1 Comprendre la composition d'un contexte

Les contextes sont composés de deux types d'éléments :

- Le **détail simple** affiche uniquement les logs de création et mort de tous les processus qui se sont exécutés sur l'agent dans le périmètre de l'attaque, ainsi que les alertes. Le détail simple est affiché par défaut dans le contexte.
- Le **détail complet** affiche tous les logs émis par l'agent dans le périmètre de l'attaque, y compris ceux qui n'apparaissent pas sur la console d'administration habituellement. Par exemple même les logs restés en local sur l'agent ou envoyés vers un serveur Syslog sont visibles dans le détail complet. Ils sont produits par le jeu de règle d'audit *Stormshield - Audits pour contextes d'attaque* de la politique par défaut.
  Selon la configuration du groupe d'agents, l'affichage du détail complet peut nécessiter une action manuelle.

11.6.2 Configurer les contextes

- Tous les logs agents de niveau Urgence et Alerte sont automatiquement des contextes. De plus, certaines protections contre les menaces génèrent systématiquement des contextes lors d'une attaque. C'est le cas notamment de la dissimulation de processus, Détournement de flux d'exécution, Heap Spray etc. Certaines règles de protection sont aussi paramétrées pour générer un contexte en cas de blocage ou même en cas de suspicion d'attaque ne justifiant pas un blocage. Pour plus d'informations, reportez-vous aux sections Gérer l'exploitation des vulnérabilités et Définir les règles de contrôle d'accès.
- Pour le détail de contextes, la taille et le périmètre, ainsi que le type et la fréquence de la remontée au gestionnaire d'agents sont configurables pour un groupe d'agents. Pour plus d'informations, reportez-vous à la section Configurer les détails de contextes émis par les agents.

- Vous pouvez aussi définir le niveau de détail de contextes à envoyer au serveur Syslog. Pour plus d'informations, reportez-vous à la section Créer des groupes de gestionnaires d'agents.

11.6.3 Analyser les contextes pour comprendre une attaque

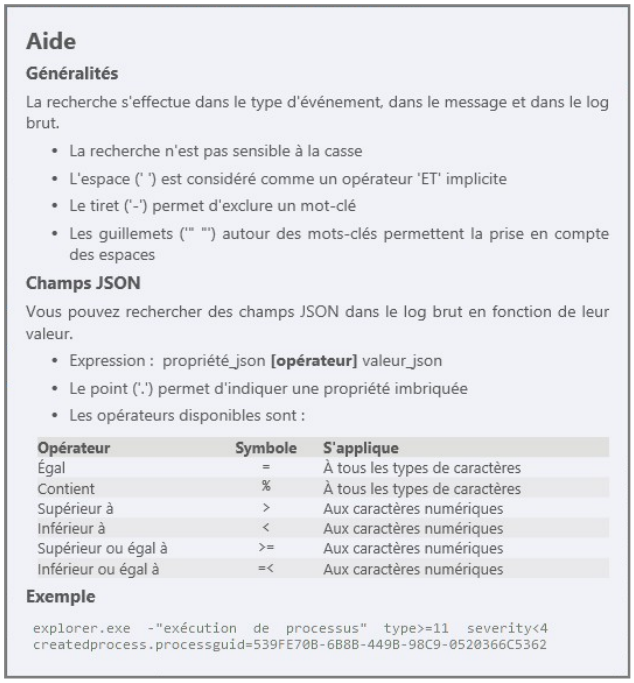
1. Choisissez le menu **Environnement > Logs agents**.
   La liste des logs de tous les agents s'affiche.
2. Cliquez sur la petite flèche à gauche d'un contexte pour l'ouvrir. Il est accompagné de l'icône œil,  ou  . Même s'il s'agit d'un groupement de logs, il contient uniquement la ligne du log ayant la gravité la plus haute. Pour plus d'informations sur la lecture des logs, reportez-vous à la section Visualiser et gérer les logs des agents dans la console d'administration.

   > **NOTE :**
   > Vous pouvez également ouvrir un contexte externe ayant été précédemment exporté. Voir Exporter des contextes et visualiser des contextes externes.

3. Cliquez sur l'icône œil  à droite du contexte pour afficher la vue détaillée et la totalité des logs qui composent le contexte. Cette vue est composée de plusieurs parties :
   - **Graphique de contexte** : représentation graphique du déroulement de l'attaque subie par l'agent. Il contient tous les processus impliqués dans le contexte et les liens entre les processus.
   - **Logs de détails de contextes** : liste de tous les logs environnant l'attaque. Par défaut, un filtre est activé et seules les alertes sont visibles. Modifiez les filtres à votre convenance.
   - Volet **Détails** ou **Log brut** : informations supplémentaires sur l'élément sélectionné dans le graphique. Le log brut est au format JSON.
   - Volet **Remédiation** : permet de sélectionner et lancer des actions de remédiation souhaitées.
4. À l'ouverture de la vue, le graphique de contexte met en évidence l'élément ayant subi l'attaque par un petit bouclier bleu. Cliquez sur les processus qui le précèdent (i.e., processus parents) et consultez les informations liées dans le volet de droite. Le **Hash** notamment permet de vérifier si ce processus est déjà identifié comme malveillant dans des bases de données de malware connus.
   Un sceau rouge barré sur le processus signifie qu'il n'a pas été signé par un certificat de signature numérique lors de sa compilation.

   > **EXEMPLE**
   > Dans notre exemple, plusieurs indicateurs montrent que le premier processus est suspect :
   > - Il affiche un sceau rouge : il n'est pas signé,
   > - Son **Nom** a été généré de manière aléatoire,
   > - Il est exécuté par WinWord, un programme qui n'exécute habituellement pas ce type de processus,
   > - Il est exécuté dans un répertoire temporaire, comme l'indique son **Chemin** *C:\Users\abott\AppData\Local\Temp*.

5. Selon la configuration du groupe d'agents, il est possible que le détail de contexte ne s'affiche pas automatiquement. Si vous avez besoin d'informations complémentaires, cliquez sur le bouton **Demander plus de détails** afin que l'agent remonte toutes les informations au gestionnaire d'agents. Pour plus d'informations sur la configuration, reportez-vous à la section Configurer les détails de contextes émis par les agents.
6. Pour faire une recherche dans les logs de contexte, entrez votre chaîne de caractères dans le champ **Rechercher**. La syntaxe de recherche est la suivante :

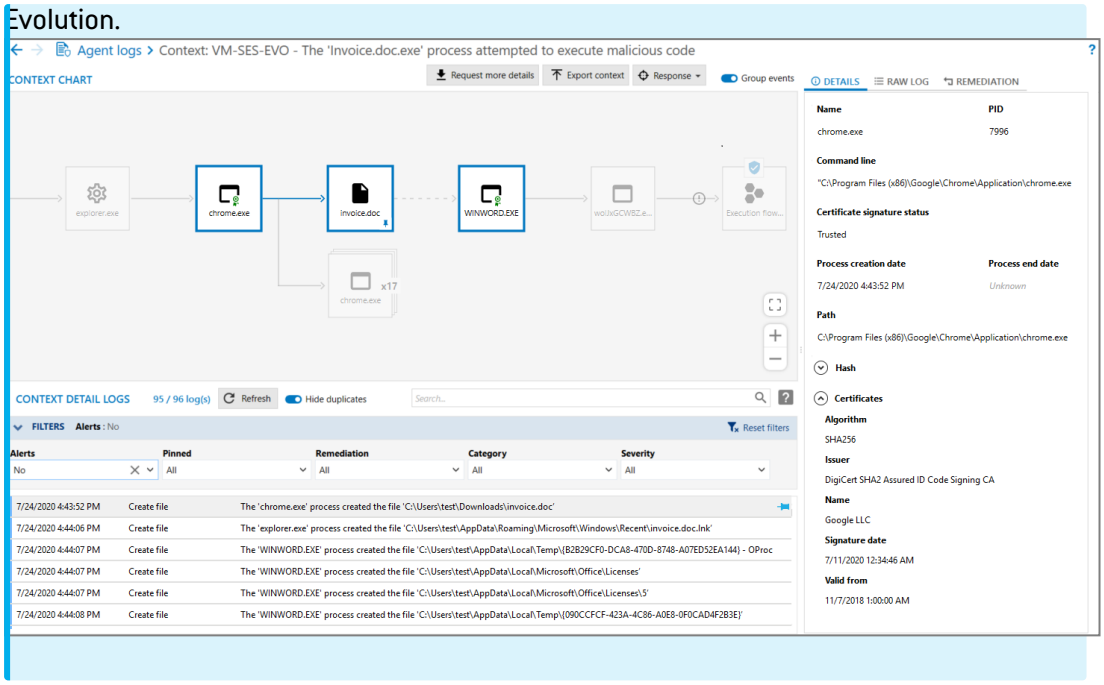


La recherche est effectuée dans les logs de détails de contexte.
Seuls les logs correspondant à la recherche restent affichés dans la liste. Le graphique de contexte n'est pas impacté par la recherche.

EXEMPLE
Dans notre exemple, la ligne de commande de l'élément *WINWORD.exe* indique qu'un fichier *invoice.doc* a été créé. La recherche de la chaîne *invoice.doc "création de fichier"* permet d'afficher tous les logs incluant ces termes et de constater que *chrome.exe* a créé ce fichier.

7. Si vous avez identifié un log pertinent pour comprendre votre attaque, épinglez-le au graphique en cliquant sur l'icône  . Ce log s'ajoute au graphique en tant que nouvel événement et le modifie.
Pour n'afficher dans la liste que les logs correspondant aux éléments du graphique, cliquez sur le bouton **Épinglés uniquement**.

EXEMPLE
Dans notre exemple, l'épinglage du log mentionnant la création du fichier *invoice.doc* permet de visualiser le déroulé de l'attaque : le malware s'est exécuté sur le poste à partir d'un document Word infecté (*invoice.doc*) que l'utilisateur à téléchargé via Chrome, puis ouvert. Il s'agit d'une tentative de Phishing qui a été bloquée par SES



8. Pour faciliter l'étude d'une partie du graphique, déplacez-vous et zoomez grâce aux boutons en bas à droite du graphique. Vous pouvez aussi utiliser le clic gauche et la molette de la souris.
9. Les processus identiques étant groupés par défaut, désactivez l'option **Grouper les événements** en haut à droite pour déployer les éléments et les analyser un par un.
10. Une fois votre analyse terminée :
    - Dans l'onglet **Remédiation** en haut à droite, créez une tâche de remédiation en cochant les actions que vous souhaitez effectuer sur le ou les agents concernés. Cliquez sur le bouton **Voir la tâche de remédiation** pour exécuter la tâche. Pour plus d'informations, reportez-vous à la section Gérer les tâches de remédiation.
    - Cliquez sur la flèche de retour en haut à gauche pour revenir au panneau des logs standard. Toutes vos modifications sont enregistrées et s'afficheront à nouveau à la prochaine ouverture de la vue des contextes.

11.6.4 Exporter des contextes et visualiser des contextes externes

Vous pouvez exporter des contextes, ce qui permet notamment de :

- Les diffuser à un service externe pour analyse,
- Les archiver sur un espace de stockage afin de pouvoir ensuite les supprimer de la base de données de logs.

Une fois exportés, ces contextes peuvent être visualisés dans une console d'administration SES Evolution.

Exporter un contexte

1. Choisissez le menu **Environnement > Logs agents**.
2. La liste des logs de tous les agents s'affiche.
3. Sélectionnez un log de type Contexte. Ils sont accompagnés de l'icône œil,  ou  .
4. Dans la barre de boutons en haut, cliquez sur **Contextes > Exporter les contextes**.

5. Par défaut le fichier est exporté sur le Bureau du poste de travail local et le nom du fichier est composé de la date et de l'heure suivis du nom du contexte. Modifiez l'emplacement et le nom à votre convenance.
6. Si besoin, ajoutez un descriptif dans le champ **Commentaire**, puis cliquez sur **Exporter**. Une notification s'affiche lorsque l'export est terminé, vous permettant d'ouvrir le fichier *.cab* exporté. L'archive peut contenir jusqu'à quatre fichiers : *contents.json*, *package.json*, *minicontext.txt* et *fullcontext.json*, ce dernier étant optionnel.

Vous pouvez sélectionner plusieurs contextes à exporter simultanément. Dans ce cas, il n'est pas possible de modifier leur nom ni de saisir un commentaire.

L'export de contextes est également possible depuis le graphique de contexte.

Visualiser un contexte exporté

1. Choisissez le menu **Environnement > Logs agents**.
2. Dans la barre de boutons en haut, cliquez sur **Contextes > Ouvrir un contexte externe**.
3. Sélectionnez le fichier *.cab* correspondant au contexte à visualiser.

> **ASTUCE**
> Vous pouvez aussi glisser-déposer le fichier *.cab* dans la zone bleue sous le menu de gauche de la console d'administration.

Le graphique de contexte s'ouvre et vous pouvez l'utiliser de la même manière qu'un contexte généré sur votre parc. Pour plus d'informations, reportez-vous à la section Analyser les contextes pour comprendre une attaque.
Si vous quittez le graphique, les données sont conservées pendant deux minutes, et vous pouvez revenir dessus en cliquant de nouveau sur le menu **Environnement > Logs agents**. Lorsque le graphique expire, vous pouvez l'ouvrir pour le visualiser de nouveau.

12. Analyser les comportements sur les postes des utilisateurs

SES Evolution permet d'effectuer des opérations d'analyse sur les postes des utilisateurs, en particulier des recherches de schémas binaires ou textuels avec l'outil Yara ainsi que des recherches d'indicateurs de compromission (IoC). Ces analyses, qui peuvent tourner en tâche de fond ou se déclencher sur un événement particulier, permettent de détecter des comportements malveillants ou suspects. Vous pouvez ainsi agir rapidement en cas d'attaque avérée.

Les fichiers mis en quarantaine sont exclus des opérations d'analyse.

12.1 Réaliser des analyses Yara

Yara est un outil qui aide notamment à l'identification et la classification de malwares via des règles. Grâce aux règles Yara, vous pouvez détecter des schémas binaires ou textuels dans les fichiers ou les processus en cours d'exécution sur les agents SES Evolution. Concrètement, l'intégration d'analyses Yara dans SES Evolution permet de nommer un malware bloqué par SES Evolution, de l'identifier sur d'autres postes de travail et éventuellement de mettre fin au processus identifié.

ATTENTION
Bien que SES Evolution soit conçu pour limiter l'impact sur les postes de travail, une analyse Yara peut affecter les performances des agents analysés. L'impact dépend du nombre de règles et de leur nature. Pour plus d'informations, reportez-vous à la section Choisir la priorité des analyses Yara et IoC.

Afin de réaliser des analyses Yara dans SES Evolution vous devez d'abord importer ces règles au sein d'unités d'analyse. L'analyse peut ensuite être exécutée sur les agents de trois façons différentes comme décrit dans l'exemple de scénario ci-dessous.

EXEMPLE
Un fichier malveillant *Facture.doc* est envoyé par e-mail à tous les collaborateurs de votre entreprise. Certains le téléchargent et l'ouvrent. A son ouverture, le fichier exécute un processus sur le poste de travail, qui effectue des actions malveillantes. Par l'exécution d'analyses Yara, l'administrateur de la sécurité peut :

- Identifier si le processus bloqué par la règle *Protect-Office apps-Part 7* du jeu *Socle de protection* est malveillant. Pour cela, il configure la règle pour que son application déclenche une analyse Yara. Voir Déclencher une analyse Yara sur l'émission d'un log dans une règle.
- Détecter et interrompre le processus malveillant sur les groupes d'agents ne bénéficiant pas de la protection de cette politique. Pour cela, il exécute une analyse à la demande sur les groupes d'agents concernés. Voir Exécuter une analyse Yara à la demande.
- Vérifier quotidiennement la présence du fichier *Facture.doc* sur les postes de travail pour pouvoir être alerté. Pour cela il configure une analyse planifiée. Voir Planifier une analyse Yara.

12.1.1 Obtenir des règles Yara

Pour effectuer des analyses Yara sur les agents SES Evolution, vous devez disposer de règles Yara. Il existe plusieurs moyens de les obtenir :

- Récupérer des règles Yara partagées publiquement par des organismes tels que CERT-FR.
- Télécharger les unités d'analyse Yara disponibles sur le serveur Stormshield. Celle-ci contiennent des règles Yara. Pour plus d'informations, reportez-vous à la section Télécharger les mises à jour Stormshield.
- Créer vos propres règles Yara. Pour plus d'informations, reportez-vous à la Documentation Yara.

12.1.2 Créer des unités d'analyse Yara

Les unités d'analyse Yara sont composées d'une ou plusieurs règles Yara.

Vous devez disposer du droit **Ressources-Modifier** pour créer des unités d'analyse.

Connaître la compatibilité Yara/SES Evolution

Version des agents SES Evolution	Versions de Yara compatibles
2.3	4.2.2 et 4.2.3
2.4	4.2.3

Créer des unités d'analyse

1. Choisissez le menu **Sécurité** > **Ressources**.
2. Dans le panneau de gauche, cliquez sur **+ Ajouter une ressource**.
3. Sélectionnez **Analyse Yara**, puis le mode d'analyse :
   - **Analyse de fichiers** pour analyser les fichiers contenus sur les agents,
   - **Analyse de processus** pour analyser la mémoire des processus qui sont exécutés sur les agents. Notez que ce mode d'analyse peut détecter le même schéma dans plusieurs processus car la mémoire d'un processus peut être copiée temporairement dans d'autres processus.
     La nouvelle unité est ajoutée sous la catégorie **YARA** dans le panneau de gauche. Sous la catégorie **Stormshield YARA**, retrouvez les ressources fournies par Stormshield.
4. Dans le champ **Nouvelle unité d'analyse**, entrez le nom de votre analyse, puis une description en dessous si besoin.

5. Cliquez sur **Importer des fichiers** et sélectionnez les fichiers **.yar*, et **.rule* que vous souhaitez utiliser dans cette unité d'analyse. Vous pouvez aussi importer des fichiers Index Yara référençant d'autres fichiers Yara.

   Si les fichiers Yara importés contiennent des incohérences ou sont susceptibles d'impacter les performances, des messages de type Erreur, Avertissement ou Performance s'affichent dans la zone **Compilation des ressources** avec une description. En cas d'erreur, vous devez corriger le problème ou retirer le fichier concerné car l'unité d'analyse ne pourra pas être enregistrée.
   Si besoin, vous pouvez filtrer ces messages selon leur gravité, la version de Yara, ou la version des agents SES Evolution.

   Vous ne pouvez pas supprimer une unité d'analyse Yara si elle est utilisée dans une tâche Yara, dans une analyse planifiée, ou en tant qu'action sur émission de logs dans une règle SES Evolution.
   Pour obtenir une copie locale des fichiers Yara, s'ils ont été importés par un autre administrateur par exemple, cliquez sur  et sélectionnez un répertoire de destination. Vous pouvez ensuite consulter ces fichiers, les modifier et les importer dans la même unité d'analyse ou dans une autre unité.

Vous pouvez également importer directement un fichier *.cab* depuis le menu  dans le panneau de gauche. Un fichier *.cab* contient le ou les fichiers à utiliser dans une unité d'analyse Yara ou IoC ainsi que d'autres données comme le titre et la description de l'unité. Dans ce même menu, le sous-menu **Exporter** permet d'exporter une unité d'analyse avec toutes ces informations, dans un fichier *.cab* également.

Vous pouvez également importer directement un fichier *.cab* depuis le menu  dans le panneau de gauche. Un fichier *.cab* contient le ou les fichiers à utiliser dans une unité d'analyse Yara ou IoC ainsi que d'autres données comme le titre et la description de l'unité. Dans ce même menu, le sous-menu **Exporter** permet d'exporter une unité d'analyse avec toutes ces informations, dans un fichier *.cab* également.

12.1.3 Déclencher une analyse Yara sur l'émission d'un log dans une règle

Vous pouvez configurer une règle SES Evolution afin de lancer automatiquement une analyse Yara sur un agent à chaque application de la règle, c'est-à-dire chaque fois qu'un log est émis pour cette règle. Les types de règles concernées sont Menaces, Applicatif, Ressources ACL et Réseaux.

ATTENTION
Une analyse Yara déclenchée sur émission de logs a un plus fort impact sur les performances des agents que les analyses panifiées ou les analyses à la demande.

Pour plus d'informations sur les actions sur émission de logs, reportez-vous à la section Configurer des actions déclenchées par les règles.

12.1.4 Exécuter une analyse Yara à la demande

Vous pouvez exécuter une analyse Yara de façon ponctuelle selon vos besoins. Pour cela, vous devez créer une tâche d'analyse Yara.

1. Choisissez le menu **Réponses** > **Tâches manuelles** et cliquez sur **Créer une tâche**.
2. Sélectionnez **Analyse Yara**.
   Vous pouvez aussi ouvrir le panneau des tâches via les **Logs agents** en sélectionnant un log et en cliquant sur **Tâches > Créer une tâche d'analyse Yara**.
3. Donnez un nom à votre tâche.
4. Cliquez sur **Ajouter des unités d'analyse** et sélectionnez les unités d'analyse que vous souhaitez inclure dans votre analyse Yara. Cliquez sur **Suivant**.
5. Cliquez sur Paramètres des logs pour déterminer le niveau de gravité et la destination des logs SES Evolution émis lors de l'analyse Yara.
6. Dans la zone **Paramètres de l'analyse de fichiers**, choisissez **Analyse par défaut** pour exécuter une analyse récursive du dossier \\.*EsaRoots\SystemDrive* et exclure les dossiers \\.*EsaRoots\SystemRoot*, \\.*EsaRoots\ProgramFiles* et \\.*EsaRoots\ProgramFilesX86*, sinon choisissez **Analyse personnalisée** :
   - **Analyser le fichier image des processus en cours d'exécution** : Vérifie si le fichier *.exe* des processus contient le schéma Yara recherché. Permet également d'arrêter sur les agents les processus malveillants identifiés lors de l'analyse Yara et/ou d'exclure de l'analyse les processus exécutés par les comptes Windows Administrateur et/ou Système.
   - **Extensions de fichiers** : Limite l'analyse aux types d'extensions indiqués.
   - **Fichiers et dossiers inclus** : Exécute l'analyse sur les fichiers et dossiers indiqués avec ou sans récursivité.
   - **Fichiers et dossiers exclus** : Exclut de l'analyse les fichiers et dossiers indiqués avec ou sans récursivité. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
7. Dans la zone **Paramètres de l'analyse de processus**, choisissez **Analyse par défaut** pour exécuter une analyse de la mémoire de tous les processus en cours d'exécution sur le poste de travail, sinon choisissez **Analyse personnalisée** :
   - **Interrompre le processus détecté** : Arrête les processus malveillants identifiés lors de l'analyse Yara.
   - **Exclure les processus exécutés par** : Exclut de l'analyse les processus exécutés avec les niveaux d'intégrité indiqués (Administrateur et/ou Système).
   - **Répertoire des processus exclus** : Exclut de l'analyse les processus dont les exécutables se trouvent dans les répertoires indiqués. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
     Vous pouvez également exporter les paramètres d'analyse au format JSON et les réimporter pour d'autres tâches.
8. Cliquez sur **Suivant** et cochez tous les agents sur lesquels vous souhaitez exécuter l'analyse Yara. Si besoin, utilisez les filtres pour afficher seulement les agents répondant à certains critères.
9. Cliquez sur **Exécuter la tâche**.
   La tâche s'affiche dans le panneau principal des tâches.
10. Sur chaque tâche, faites un clic droit pour effectuer les actions suivantes :
    - Naviguer vers les logs agents correspondant à cette tâche,
    - Retirer la tâche de la liste,
    - Annuler la tâche en cours d'exécution sur les agents,
    - Relancer la tâche en modifiant certains paramètres.
      Vous pouvez également **Supprimer les tâches terminées** du panneau des tâches.

11. Cliquez sur la flèche à gauche de la tâche pour afficher le détail des unités d'analyse qui la composent.
    Cliquez sur **Annuler la sélection** pour annuler une unité d'analyse en cours d'exécution.

12.1.5 Planifier une analyse Yara

Vous pouvez planifier une analyse Yara afin qu'elle soit exécutée régulièrement par un groupe d'agents.

Pour plus d'informations, reportez-vous à la section Créer des analyses Yara planifiées.

12.1.6 Consulter l'utilisation des analyses Yara

1. Choisissez le menu **Sécurité > Ressources**.
2. Dans le panneau de gauche, cliquez sur la ressource dont vous voulez consulter l'utilisation.
3. Déployez la zone **Utilisation de la ressource** qui fournit les informations suivantes :
   - **Groupes d'agents - Analyse planifiée** : Groupes d'agent ayant fait l'objet d'une analyse Yara planifiée pour cette ressource.
   - **Jeux de règles - Action sur émission de logs** : Jeux de règles ayant déclenché l'analyse Yara. Cliquez sur le nom du jeu pour ouvrir le panneau correspondant.
   - **Tâches** : Tâches liées aux analyses Yara exécutées à la demande. Cliquez sur le nom de la tâche pour ouvrir le panneau correspondant.

12.2 Rechercher des indicateurs de compromission

Les analyses IoC (*Indicators of Compromise*) permettent de mesurer l'ampleur d'un incident ou d'une attaque sur un poste de travail en recherchant des indicateurs de compromission. Ces indicateurs peuvent être par exemple des signatures de malware, des adresses IP particulières, des hashes de fichiers malveillants, des adresses URL ou des textes suspects. Ils peuvent être notamment recherchés dans des requêtes DNS, des objets nommés Windows ou des journaux d'événements par exemple.

Les indicateurs peuvent éventuellement révéler les outils utilisés et les auteurs de l'attaque.

Afin de rechercher des indicateurs sur les postes des utilisateurs, vous devez d'abord importer des listes d'indicateurs au sein d'unités d'analyse dans SES Evolution. L'analyse peut ensuite être déclenchée automatiquement lorsqu'une règle de sécurité détecte ou bloque un comportement inhabituel et émet un log. Afin de protéger les postes de potentielles attaques, vous pouvez également la planifier pour qu'elle s'exécute régulièrement et pendant une durée définie ou bien l'exécuter à la demande.

Les logs remontés par les analyses IoC permettent ensuite d'effectuer des actions de remédiation afin de supprimer les outils malveillants détectés. Pour plus d'informations, reportez-vous à la section Gérer les tâches de remédiation.

ATTENTION
Bien que SES Evolution soit conçu pour limiter l'impact sur les postes de travail, une analyse IoC peut affecter les performances des agents analysés. L'impact dépend du nombre d'indicateurs IoC et de leur type. Pour plus d'informations, reportez-vous à la section Choisir la priorité des analyses Yara et IoC.

12.2.1 Créer des unités d'analyse IoC

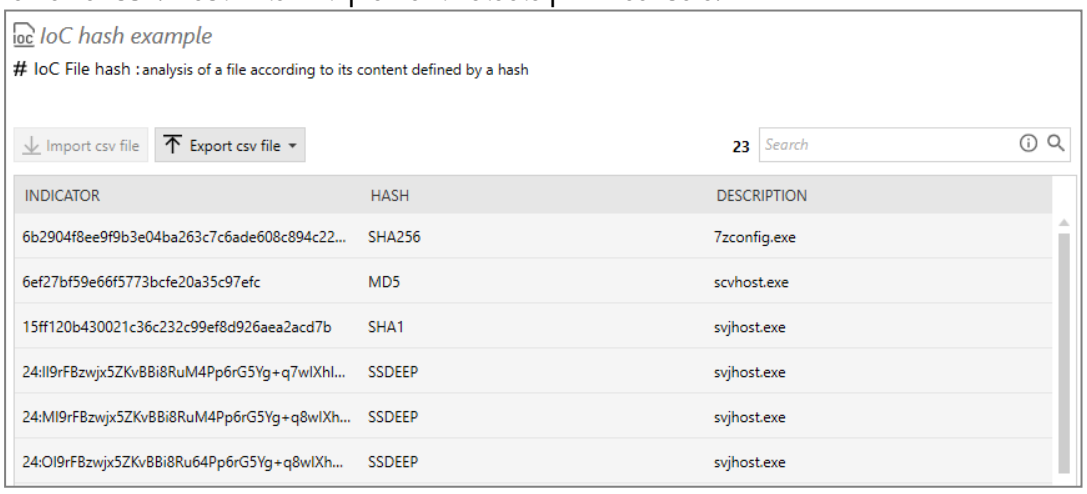
Dans les unités d'analyse IoC, vous importez des listes d'indicateurs de compromission de différents types. Vous utilisez ensuite ces unités d'analyse dans des règles de vos politiques de sécurité, dans des tâches manuelles à la demande ou bien dans des tâches planifiées.

Consultez les sections suivantes pour utiliser les unités d'analyse selon votre besoin :

- Déclencher une analyse IoC sur l'émission d'un log dans une règle
- Exécuter une analyse IoC à la demande
- Planifier une analyse IoC

Connaître les prérequis

- Vous devez disposer du droit **Ressources-Modifier** pour créer des unités d'analyse.
- Les indicateurs de compromission que vous allez utiliser dans les unités d'analyse doivent être compilés dans des fichiers au format CSV. Vous pouvez trouver des exemples d'indicateurs sur des sites Internet, par exemple sur celui de l'ANSSI. Les indicateurs peuvent également provenir de votre propre parc si vous avez détecté une compromission avec SES Evolution ou par un autre moyen, ou bien des ressources Stormshield téléchargées depuis le serveur de mise à jour. Pour plus d'informations, reportez-vous à la section Télécharger les mises à jour Stormshield.
  Le format du fichier CSV peut être le suivant : l'indicateur dans la première colonne suivi d'un séparateur (virgule, point virgule ou tabulation) et une description dans la deuxième colonne. La description n'est pas obligatoire et dans ce cas le séparateur n'est donc pas nécessaire. Si le fichier CSV contient plus de deux colonnes, il peut être importé quand même dans l'unité mais seules les deux premières sont prises en compte et affichées dans la console. Les titres de colonne ne sont pas nécessaires.
  Pour le type d'indicateur hash, il n'est pas nécessaire d'indiquer l'algorithme de hash dans le fichier CSV. Il est automatiquement détecté par la console.

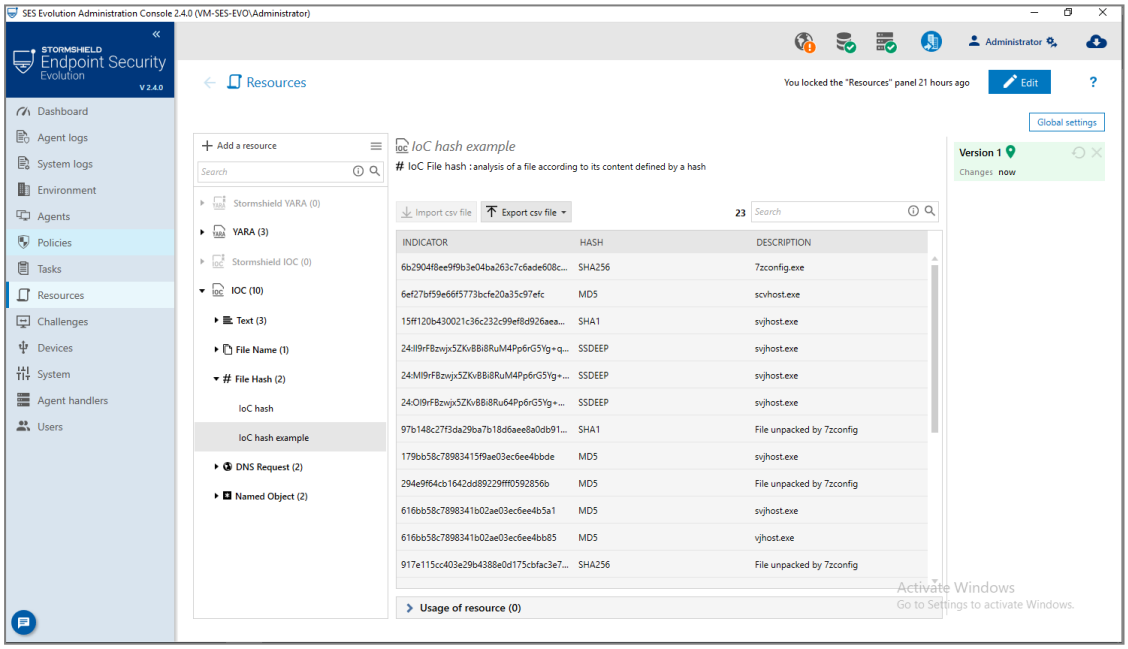


Créer une unité d'analyse IoC

1. Choisissez le menu **Sécurité** > **Ressources**.
2. Dans le panneau de gauche, cliquez sur **+ Ajouter une ressource**.

3. Sélectionnez **Analyse IoC**, puis le type d'indicateurs à rechercher dans l'analyse :
   - Texte : recherche de chaînes de caractères suspectes (nom de fichier, nom de domaine, nom d'hôte, adresse IP, nom d'objet, adresse e-mail),
   - Nom de fichier : recherche de fichiers suspects,
   - Hash de fichier : recherche de hashes de fichiers suspects. Si vous importez des hashes de fichiers de type SSDEEP, vous pouvez modifier le taux de similarité par défaut de 80% en cliquant sur le bouton **Paramètres généraux** en haut à droite du panneau **Ressources**. Une correspondance de 100% entre deux fichiers indique qu'ils sont identiques.
   - Requête DNS : recherche de requêtes effectuées vers des noms de domaine suspects,
   - Objet nommé : recherche de noms d'objets suspects parmi les objets nommés Windows (ALPC port, Event, Job, Mutant, Section, Semaphore, Timer, Mailslot, NamedPipe, etc.).

   La nouvelle unité est ajoutée sous la catégorie **IOC** dans le panneau de gauche. Sous la catégorie **Stormshield IOC**, retrouvez les ressources fournies par Stormshield.
4. Dans le champ **Nouvelle unité d'analyse**, entrez le nom de votre analyse, puis une description en dessous si besoin.
5. Cliquez sur **Importer le fichier CSV** et sélectionnez un fichier CSV listant des indicateurs correspondant au type choisi. Le nombre total d'indicateurs s'affiche à gauche du champ **Rechercher**. Vous ne pouvez importer qu'un seul fichier CSV par unité.
6. Cliquez sur **Enregistrer**.



Vous ne pouvez pas supprimer une unité d'analyse IoC si elle est utilisée dans une tâche IoC, dans une analyse planifiée, ou en tant qu'action sur émission de logs dans une règle SES Evolution.

Pour obtenir une copie locale du fichier CSV, s'il a été importé par un autre administrateur par exemple, cliquez sur ⤒ et sélectionnez un répertoire de destination. Vous pouvez ensuite consulter le fichier, le modifier et l'importer dans la même unité d'analyse ou dans une autre unité.

Vous pouvez également importer directement un fichier *.cab* depuis le menu ☰ dans le panneau de gauche. Un fichier *.cab* contient le ou les fichiers à utiliser dans une unité d'analyse Yara ou IoC ainsi que d'autres données comme le titre et la description de l'unité.

Dans ce même menu, le sous-menu **Exporter** permet d'exporter une unité d'analyse avec toutes ces informations, dans un fichier *.cab* également.

12.2.2 Déclencher une analyse IoC sur l'émission d'un log dans une règle

Vous pouvez configurer une règle SES Evolution afin de lancer automatiquement une analyse IoC sur un agent à chaque application de la règle, c'est-à-dire chaque fois qu'un log est émis pour cette règle. Les types de règles concernées sont Menaces, Applicatif, Ressources ACL et Réseaux.

ATTENTION
Une analyse IoC déclenchée sur émission de logs a un plus fort impact sur les performances des agents que les analyses panifiées ou les analyses à la demande.

Pour plus d'informations sur les actions sur émission de logs, reportez-vous à la section Configurer des actions déclenchées par les règles.

12.2.3 Exécuter une analyse IoC à la demande

Vous pouvez exécuter une analyse IoC de façon ponctuelle selon vos besoins. Pour cela, vous devez créer une tâche d'analyse IoC.

1. Choisissez le menu **Réponses** > **Tâches manuelles** et cliquez sur **Créer une tâche**.
2. Sélectionnez **Analyse IoC**.
   Vous pouvez aussi ouvrir le panneau des tâches via les **Logs agents** en sélectionnant un log et en cliquant sur **Tâches > Créer une tâche d'analyse IoC**.
3. Donnez un nom à votre tâche.
4. Cliquez sur **Ajouter des unités d'analyse** et sélectionnez les unités d'analyse que vous souhaitez inclure dans votre analyse IoC. Cliquez sur **Suivant**.
5. Cliquez sur Paramètres des logs pour déterminer le niveau de gravité et la destination des logs SES Evolution émis lors de l'analyse IoC.
6. Pour les indicateurs de type Texte, vous pouvez désactiver l'analyse IoC dans les fichiers, dans les processus ou bien dans les journaux d'événements en décochant les cases **Recherche textuelle**.
7. Dans la zone **Paramètres de l'analyse de fichiers**, choisissez **Analyse par défaut** pour exécuter une analyse récursive du dossier \\.*EsaRoots**SystemDrive* et exclure les dossiers \\.*EsaRoots**SystemRoot*, \\.*EsaRoots**ProgramFiles* et \\.*EsaRoots**ProgramFilesX86*, sinon choisissez **Analyse personnalisée** :
   - **Analyser le fichier image des processus en cours d'exécution** : Vérifie si le fichier *.exe* des processus contient les indicateurs recherchés. Permet également d'arrêter sur les agents les processus malveillants identifiés lors de l'analyse IoC et/ou d'exclure de l'analyse les processus exécutés par les comptes Windows Administrateur et/ou Système.
   - **Extensions de fichiers** : Limite l'analyse aux types d'extensions indiqués.
   - **Fichiers et dossiers inclus** : Exécute l'analyse sur les fichiers et dossiers indiqués avec ou sans récursivité.
   - **Fichiers et dossiers exclus** : Exclut de l'analyse les fichiers et dossiers indiqués avec ou sans récursivité. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.

8. Dans la zone **Paramètres de l'analyse de processus**, choisissez **Analyse par défaut** pour exécuter une analyse de la mémoire de tous les processus en cours d'exécution sur le poste de travail, sinon choisissez **Analyse personnalisée** :
   - **Interrompre le processus détecté** : Arrête les processus malveillants identifiés lors de l'analyse IoC.
   - **Exclure les processus exécutés par** : Exclut de l'analyse les processus exécutés avec les niveaux d'intégrité indiqués (Administrateur et/ou Système).
   - **Répertoire des processus exclus** : Exclut de l'analyse les processus dont les exécutables se trouvent dans les répertoires indiqués. Cliquez sur l'icône + pour ajouter un chemin supplémentaire.
9. Dans la zone **Journaux d'événements**, sélectionnez les types de journaux à analyser et leur ancienneté.
10. Dans la zone **Paramètre de requête DNS**, indiquez l'ancienneté des requêtes DNS à analyser.
11. Cliquez sur **Suivant** et cochez tous les agents sur lesquels vous souhaitez exécuter l'analyse IoC. Si besoin, utilisez les filtres pour afficher seulement les agents répondant à certains critères.
12. Cliquez sur **Exécuter la tâche**.
    La tâche s'affiche dans le panneau principal des tâches.
13. Sur chaque tâche, cliquez sur les icônes suivantes pour effectuer des actions :

	Affiche dans le panneau des logs agents les logs correspondant à cette tâche.
	Retire de la liste les tâches.
	Annule la tâche en cours d'exécution sur les agents.
	Relance la tâche en modifiant certains paramètres.

    Vous pouvez également **Supprimer les tâches terminées** du panneau des tâches.
14. Cliquez sur la flèche à gauche de la tâche pour afficher le détail des unités d'analyse qui la composent.
    Cliquez sur **Annuler la sélection** pour annuler une unité d'analyse en cours d'exécution.

12.2.4 Planifier une analyse IoC

Vous pouvez planifier une analyse IoC afin qu'elle soit exécutée régulièrement par un groupe d'agents.

Pour plus d'informations, reportez-vous à la section Créer des analyses IoC planifiées.

12.2.5 Consulter l'utilisation des analyses IoC

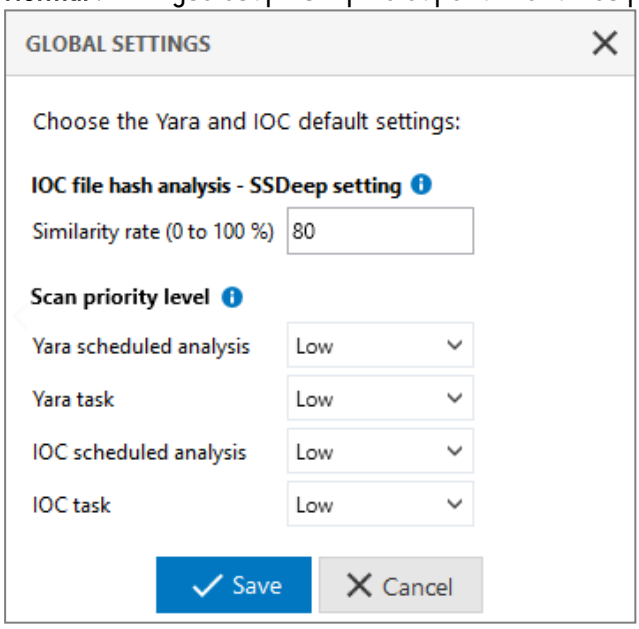
1. Choisissez le menu **Sécurité > Ressources**.
2. Dans le panneau de gauche, cliquez sur la ressource dont vous voulez consulter l'utilisation.

3. Déployez la zone **Utilisation de la ressource** qui fournit les informations suivantes :
   - **Groupes d'agents - Analyse planifiée** : Groupes d'agent ayant fait l'objet d'une analyse IoC planifiée pour cette ressource.
   - **Jeux de règles - Action sur émission de logs** : Jeux de règles ayant déclenché l'analyse IoC. Cliquez sur le nom du jeu pour ouvrir le panneau correspondant.
   - **Tâches** : Tâches liées aux analyses IoC exécutées à la demande. Cliquez sur le nom de la tâche pour ouvrir le panneau correspondant.

12.3 Choisir la priorité des analyses Yara et IoC

Pour les types d'analyse planifiée et à la demande Yara et IoC , SES Evolution permet de définir le niveau de priorité du processus par rapport aux autres processus qui s'exécutent sur le poste de l'utilisateur. Vous pouvez choisir entre une priorité basse et une priorité normale.

1. Dans le menu **Sécurité > Ressources**, cliquez sur le bouton **Paramètres généraux** à droite du panneau.
2. Dans la section **Niveau de priorité de l'analyse**, pour chaque type sélectionnez une valeur :
   - **Bas** : l'analyse s'exécute en tâche de fond et impacte peu les performances du poste,
   - **Normal** : l'analyse est plus rapide et peut ralentir les performances du poste.



13. Répondre aux événements de sécurité

Lorsqu'une action malveillante survient sur votre parc ou est suspectée, SES Evolution permet de la détecter et/ou de la bloquer tout en générant un événement de sécurité. Il permet également de répondre à cet événement en effectuant une remédiation sur les postes de travail concernés. La remédiation est un ensemble d'actions permettant de limiter l'impact des attaques et de réparer les éventuels dommages.

EXEMPLES

- Une règle d'audit SES Evolution surveille certaines arborescences de la base de registre pour détecter l'ajout ou modification de clés ou valeurs. En effet, certains programmes malveillants utilisent cette méthode pour persister après le redémarrage du poste de travail. Si une telle action est détectée, un log d'audit est émis, et vous pouvez lancer une remédiation permettant de supprimer ou modifier automatiquement les clés de registre suspectes sur les postes de travail concernés.
- Un ransomware a eu le temps de chiffrer quelques fichiers avant d'être bloqué par SES Evolution. La remédiation permet de récupérer automatiquement la version non chiffrée de ces fichiers à partir d'un cliché instantané Windows.
- Un programme malveillant a été involontairement exécuté par un utilisateur. Il est bloqué et son exécution est interrompue par SES Evolution, mais il peut en plus être mis en quarantaine. Il est ainsi hors d'atteinte de l'utilisateur, et cela vous permet à l'administrateur de l'analyser avant de le supprimer ou le restaurer.
- Les logs agents signalent un événement suspect sur le poste d'un utilisateur. Vous détectez un danger. Vous pouvez isoler le poste concerné du réseau le temps de mener votre analyse et ainsi vous évitez la propagation d'une éventuelle attaque à tout le parc.
- Après une attaque par ransomware bloquée par SES Evolution, certains programmes peuvent subsister sur le poste de travail et faciliter une nouvelle attaque, par exemple un cheval de Troie d'accès à distance (RAT). Vous pouvez détecter ces programmes grâce à une analyse IoC, puis les supprimer automatiquement grâce à la remédiation.

13.1 Gérer les tâches de remédiation

À partir des logs agents, vous pouvez lancer des tâches de remédiation sur les postes de travail. En fonction du type de logs, SES Evolution propose différentes actions de remédiation, telles que la mise en quarantaine de fichiers, la suppression de clés de registre, l'interruption de processus, etc. Ces actions permettent de limiter fortement l'impact des attaques.

Les actions de remédiation demandées peuvent outrepasser la politique de sécurité en vigueur sur le poste de travail concerné.

13.1.1 Accorder les permissions de remédiation

Deux permissions distinctes permettent de gérer les accès à la fonctionnalité de remédiation. La permission **Remédiation (avancée) - Modifier** permet d'effectuer toutes les actions de remédiation, dont l'exécution de scripts Powershell.

Sachant que l'exécution de scripts Powershell est une action très sensible, n'accordez cette permission qu'à un très petit nombre de personnes de confiance.

Pour les autres personnes susceptibles d'effectuer des actions de remédiation sans exécution de scripts, accordez-leur la permission **Remédiation - Modifier**.

Voir Gérer les utilisateurs de la console d'administration SES Evolution.

13.1.2 Créer une tâche de remédiation

1. Choisissez le menu **Environnement > Logs agents** et identifiez le log correspondant à l'action malveillante sur laquelle vous souhaitez faire une remédiation. Par exemple, une attaque par ransomware génère le log "Le processus `nom_processus` a tenté d'effectuer une attaque par ransomware". Tous les logs agents peuvent faire l'objet d'une remédiation, sauf ceux dont l'attribut est *Interne*, *Auto-protection*, ou *Remédiation*. Pour plus d'informations, reportez-vous à la section Visualiser et gérer les logs des agents dans la console d'administration.
2. Sélectionnez le log ou le groupe de logs concerné et cliquez sur **Tâches > Créer une tâche de remédiation**. La fenêtre des tâches s'affiche. Elle liste les actions de remédiation possibles pour le type de logs sélectionné, ainsi que la ressource concernée. Les actions sont regroupées par agent.
3. Saisissez un **Nom** pour votre tâche de remédiation.
4. Utilisez les filtres pour visualiser uniquement un certain **Type d'actions**, ou les actions concernant un certain **Groupe d'agents**.
5. Cochez les actions que vous souhaitez effectuer. Selon le type de log sélectionné, les actions peuvent être :
   - Interrompre un processus, en incluant ou non ses processus enfants,
   - Retirer un fichier (mise en quarantaine ou suppression),
   - Supprimer une clé de registre,
   - Supprimer ou modifier une valeur de registre,
   - Récupérer les fichiers chiffrés par un ransomware, avec visualisation des 10 premiers fichiers chiffrés,
   - Exécuter un script Powershell.

   Certaines actions peuvent comporter une pastille orange. Cela signifie qu'elles concernent un des répertoires système critiques suivants et qu'elles peuvent donc avoir un impact sur le poste de travail :
   - C:\Windows\System32
   - C:\Windows\SysWOW64
   - C:\Windows\Microsoft.NET
   - C:\Windows\WinSxS
   - C:\Program Files
   - C:\Program Files (x86)
   - C:\ProgramData\Stormshield

6. Si les actions proposées ne sont pas suffisantes et que vous disposez de la permission **Remédiation (avancée) - Modifier**, vous pouvez exécuter un script Powershell personnalisé pendant la tâche de remédiation.

> **EXEMPLE**
> Si un programme malveillant a ajouté des clés de registre pour persister après le redémarrage du poste de travail, vous pouvez vouloir les supprimer. Or, la sélection de toutes les clés à supprimer peut être assez rébarbative si elles sont très nombreuses et qu'elles concernent plusieurs agents. Il peut être intéressant de créer un script qui supprimera automatiquement toutes les clés sans que vous ayez à les sélectionner.

Pour ajouter un script Powershell :

a. Cliquez sur **Actions script Powershell > Ajouter à tous les agents**.
La fenêtre **Ajouter une action script Powershell** s'affiche.

b. À droite du champ **Script**, cliquez sur **+** pour ajouter le script à exécuter.

c. Dans le champ **Arguments**, spécifiez si besoin les arguments à ajouter lors de l'exécution du script.

d. Si vous souhaitez que le script soit exécuté sur tous les agents concernés lors de la tâche de remédiation, sélectionnez la case **Cocher l'action sur tous les agents**. Dans le cas contraire, la ligne est ajoutée dans la liste des actions mais n'est pas cochée.

e. Sélectionnez un script existant, et cliquez sur le bouton  pour le visualiser, ou sur  pour importer une nouvelle version du script.

7. Cliquez sur **Démarrer la remédiation**.
Le panneau des **Tâches** s'affiche et vous pouvez surveiller la progression de la tâche de remédiation.

8. Cliquez sur la flèche à gauche de la tâche pour afficher sa progression sur chaque agent concerné.
Les différents états possibles pour une tâche de remédiation sont les suivants :

État	Description
Non démarrée	La tâche a été lancée mais elle n'a pas encore démarré.
En cours	La tâche est en cours d'exécution.
Terminé	L'action de remédiation a été effectuée avec succès.
Erreur	Une erreur s'est produite lors de la tâche de remédiation. Un message indique la raison. Par exemple, la ressource est verrouillée, les droits sont insuffisants pour supprimer un fichier, l'agent n'est pas connecté, etc.
Partiel	• Dans le cas d'une remédiation suite à une attaque par ransomware, la totalité des fichiers n'a pas pu être récupérée. • Dans le cas d'une suppression de processus, au moins un processus n'a pas pu être supprimé.
Annulé	La tâche à été annulée par l'utilisateur lors de son exécution.

9. Si vous avez choisi de mettre des fichiers en quarantaine, ceux-ci s'affichent dans le panneau **Réponses > Quarantaine**. Pour plus d'informations, reportez-vous à la section Gérer la mise en quarantaine de fichiers.

13.1.3 Gérer les tâches de remédiation

Utilisez les filtres **Statut**, **Type**, **Créateur**, ou **Groupe** d'agents pour n'afficher que les tâches qui vous intéressent.

Cliquez sur **Détails** pour plus d'informations sur les actions de remédiation réalisées et le résultat.

Vous pouvez également effectuer les actions suivantes sur les tâches ou sous-tâches de remédiation :

- Annuler une tâche en cours,
- Naviguer vers les logs agents correspondant à cette tâche,
- Relancer une tâche,
- Retirer une tâche du panneau des tâches,
- Exporter le fichier de résultat au format CSV.

13.2 Gérer une attaque par ransomware

SES Evolution protège les postes de travail de votre entreprise contre les attaques par ransomware. Il est capable de détecter les actions exécutées habituellement par les ransomware sur un système, telles que la modification ou le chiffrement de fichiers, et de les arrêter aussitôt. Si certains fichiers ont été chiffrés par le ransomware avant le blocage par SES Evolution, vous pouvez récupérer les données perdues en procédant à une remédiation.

ATTENTION
La création de clichés instantanés par SES Evolution ne remplace pas les sauvegardes régulières. Il est primordial de disposer d'une solution de sauvegarde dédiée en parallèle.

13.2.1 Prérequis

Pour pouvoir bloquer les attaques par ransomware, vous devez configurer SES Evolution comme suit :

- Activez la protection Ransomware. Si vous utilisez les politiques *Politique par défaut* ou *Protection des composants Backoffice*, elle est activée par défaut dans le jeu de règles Protection anti-ransomware.
- Activez les clichés instantanés Windows.
- Optionnel : Interdisez l'exécution de commandes malveillantes visant notamment à supprimer les clichés instantanés. Utilisez pour cela le filtrage d'applications par arguments de ligne de commande. Si vous utilisez les politiques *Politique par défaut* ou *Protection des composants Backoffice*, elle est activée par défaut dans le jeu de règles Protection anti-ransomware.

13.2.2 Détecter une attaque par ransomware

Si vous avez activé la protection ransomware SES Evolution et choisi l'option **Bloquer et interrompre**ou **Bloquer, interrompre et mettre en quarantaine**, chaque attaque par ransomware génère un log de niveau Alerte et un contexte:

"Le processus `nom_processus` a tenté d'effectuer une attaque par ransomware. Consultez la liste des fichiers chiffrés dans le fichier `chemin_fichier`."

Le log contient :

- Le nom du processus responsable de l'attaque,
- Le chemin du fichier de remédiation qui identifie tous les fichiers chiffrés par le ransomware avant son blocage. Ce dernier est conservé pendant 30 jours dans le dossier *%PROGRAMDATA%\Stormshield\SES Evolution\Agent\Diagnostics\Ransomware Protection* sur le poste de travail où est installé l'agent SES Evolution.
- La liste des dix premiers fichiers chiffrés (dans le log détaillé).

13.2.3 Récupérer les données perdues

Si vous avez mis en place les prérequis, vous pouvez récupérer les données perdues à l'aide d'une tâche de remédiation. Elle permet de récupérer une version antérieure des fichiers perdus.

Stormshield recommande de récupérer les données dans les 5 jours car SES Evolution va continuer de créer des clichés instantanés quotidiennement après une attaque. Sachant que seuls les cinq derniers clichés sont conservés, les nouveaux clichés contenant des fichiers chiffrés vont écraser les clichés plus anciens.

Pour récupérer les données perdues :

1. Effectuez la procédure décrite dans la section Gérer les tâches de remédiation.
2. Lors de la création de la tâche, cochez les actions de type **Récupérer les fichiers chiffrés par un ransomware**.
3. Cliquez sur **Démarrer la remédiation**.
   Le panneau **Tâches manuelles** s'affiche et SES Evolution procède à la récupération des fichiers chiffrés à partir des clichés instantanés Windows.
4. Une fois la tâche terminée, cliquez sur **Détails** pour visualiser les fichiers restaurés.
5. Dans l'explorateur Windows, vérifiez dans le dossier d'origine que les fichiers restaurés sont bien présents, sous leur nom initial. Les fichiers chiffrés sont également conservés avec une extension *.bak*.

13.3 Gérer la mise en quarantaine de fichiers

Lorsqu'une action malveillante survient dans votre parc, SES Evolution permet de détecter les fichiers suspects et de les placer dans une zone de quarantaine le temps de les analyser. Les fichiers mis en quarantaine ne peuvent plus être exécutés, ni causer aucun dommage au poste de travail. Si après analyse, les fichiers s'avèrent inoffensifs, vous pouvez les restaurer à leur emplacement d'origine.

Vous pouvez établir une liste de dossiers à exclure. Les fichiers qu'ils contiennent seront protégés contre la quarantaine.

Les mises en quarantaine et les restaurations sont journalisées dans les logs Agents.

Vous devez disposer du droit **Remédiation-Modifier** pour mettre en quarantaine et restaurer des fichiers.

13.3.1 Protéger des fichiers contre la mise en quarantaine

1. Choisissez le menu **Réponses > Quarantaine**, et cliquez sur l'onglet **Paramètres**.
   Dans la section **Exclusions prédéfinies**, certains dossiers système sont exclus par défaut car il ne serait pas judicieux que leur contenu soit mis en quarantaine. Les dossiers sont affichés sous forme de variables EsaRoots.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
3. Dans la section **Exclusions personnalisées**, saisissez le chemin du dossier dont vous souhaitez protéger le contenu. Les caractères génériques ne sont pas autorisés.
4. Activez l'option **Récursif** si la protection doit s'étendre au contenu des sous-dossiers.
5. Dans le champ **Propriétaire**, sélectionnez si besoin l'un des groupes Windows propriétaire des fichiers, ou saisissez un SID spécifique.
6. Cliquez sur le bouton  pour valider la ligne.
7. Ajoutez autant de chemins que nécessaire et cliquez sur **Enregistrer**.

Vous pouvez désactiver temporairement les exclusions en décochant les cases à gauche des lignes.

13.3.2 Mettre des fichiers en quarantaine

La mise en quarantaine de fichiers peut s'effectuer :

- Automatiquement au déclenchement d'une règle de protection si vous l'avez configuré. Pour plus d'informations sur la configuration des règles, reportez-vous à la section Définir les règles de contrôle d'accès.
- Manuellement lors d'une remédiation. Pour plus d'informations, reportez-vous à la section Gérer les tâches de remédiation.

Les fichiers situés sur un partage réseau ne seront pas mis en quarantaine.

Lors d'une mise en quarantaine, les fichiers sont déplacés dans le dossier local de l'agent : *C:\ProgramData\Stormshield\SES Evolution\Agent\Quarantine*. L'accès à ce dossier n'est pas autorisé, même pour les administrateurs, et les fichiers qu'il contient sont chiffrés.

13.3.3 Suivre les fichiers en quarantaine

1. Choisissez le menu **Réponses > Quarantaine** et l'onglet **Général** pour afficher la liste des fichiers en quarantaine.
2. Si besoin, utilisez les filtres **État de la quarantaine** et **Groupe** d'agents pour réduire la liste. Les états possibles sont *En quarantaine* et *En attente de restauration*.
3. Sélectionnez un fichier dans la liste pour afficher dans le panneau de droite des informations sur ce fichier et l'agent concerné.

13.3.4 Restaurer des fichiers en quarantaine

Si après analyse, vous considérez que le fichier est inoffensif et que c'est un faux-positif, vous devez :

- Ajouter une exception sur le log et déployer les changements sur tous les agents, afin que le fichier ne soit plus détecté comme malveillant,
- Le restaurer à son emplacement d'origine. Il sera restauré à l'identique, avec les mêmes ACL et les mêmes flux de données alternatifs.

Pour restaurer le fichier :

1. Choisissez le menu **Réponses > Quarantaine** et l'onglet **Général**.
2. Faites un clic droit sur le fichier à restaurer et choisissez **Restaurer la sélection**.
   La fenêtre **Restaurer les fichiers en quarantaine** s'affiche. Tous les fichiers en quarantaine ayant le même hash sont listés et sélectionnés pour la restauration.
3. Activez l'option **Écraser le fichier existant** si le même fichier est déjà présent dans l'emplacement d'origine et que vous souhaitez le remplacer.
4. Si besoin, utilisez le champ de recherche ou les filtres **État de la quarantaine** et **Groupe** d'agents pour réduire la liste. Les états possibles sont *En quarantaine* et *En attente de restauration*.
5. Si besoin, décochez les fichiers que vous souhaitez garder en quarantaine. Tous les fichiers ayant le même hash seront systématiquement restaurés en même temps à leur emplacement respectif.
6. Cliquez sur **Restaurer**.
   Une tâche de restauration est créée et les fichiers passent dans l'état *En attente de restauration*. Ensuite, les fichiers sont déplacés de l'espace de quarantaine vers leur emplacement d'origine. Ils disparaissent alors du panneau **Quarantaine**.

13.3.5 Supprimer les fichiers en quarantaine

Les fichiers sont conservés dans l'espace de quarantaine pendant 40 jours, puis ils sont supprimés automatiquement. De plus, si l'espace de quarantaine dépasse un volume de 1 Go, les fichiers les plus anciens sont supprimés automatiquement pour laisser la place aux nouveaux.

Vous pouvez aussi choisir de retirer manuellement des fichiers du panneau **Quarantaine**. Dans ce cas, les fichiers ne sont plus affichés, mais ils sont conservés sur le disque dans l'espace de quarantaine. Ils feront ensuite l'objet d'une suppression automatique après 40 jours ou si la taille de 1 Go est dépassée.

1. Choisissez le menu **Réponses > Quarantaine** et l'onglet **Général**.
2. Faites un clic droit sur le fichier à supprimer et choisissez **Supprimer la sélection**.
3. Confirmez la suppression.
   Le fichier ne s'affiche plus dans la liste.

Les fichiers mis en quarantaine sont supprimés automatiquement lors de la désinstallation de l'Agent SES Evolution.

13.4 Isoler des ordinateurs du réseau

En cas d'attaque ou de soupçon d'attaque sur le parc, il est possible d'isoler du réseau les ordinateurs concernés. L'isolation permet de couper les connexions entrantes et sortantes immédiatement et d'éviter la propagation d'une éventuelle attaque au reste du parc ou l'exfiltration de données vers les serveurs de l'attaquant.

Pendant la mise en isolation des ordinateurs, la communication entre les agents et les gestionnaires d'agents est maintenue afin que vous puissiez procéder par exemple à des opérations d'analyse et de remédiation si nécessaire. Lorsque l'intervention est terminée, vous pouvez arrêter l'isolation des ordinateurs et rétablir ainsi les connexions.

Depuis la console d'administration SES Evolution, vous pouvez :

- Isoler des ordinateurs,
- Suivre les ordinateurs isolés,

- Exécuter des tâches d'analyse Yara ou IoC et des tâches de remédiation sur les postes isolés,
- Arrêter l'isolation des ordinateurs.

Les demandes d'isolation et d'arrêt d'isolation sont journalisées dans les logs Système et les logs Agents.

13.4.1 Prérequis

La fonctionnalité d'isolation est utilisable si les conditions suivantes sont toutes réunies :

- L'isolation des ordinateurs est possible à partir de la version 2.5.3 des agents SES Evolution.

> **NOTE**
> Si vous demandez l'isolation d'un ensemble d'agents comportant des versions logicielles différentes, seuls les agents éligibles sont isolés, c'est-à-dire en version 2.5.3 minimum.

- L'agent SES Evolution doit pouvoir communiquer avec son gestionnaire d'agents pour prendre en compte les demandes d'isolation et d'arrêt d'isolation. Un agent déconnecté du gestionnaire d'agents ne peut pas appliquer la demande.
- La fonctionnalité **Réseaux** doit être activée dans les paramètres des groupes d'agents.
- Vous devez disposer du droit **Remédiation-Modifier** pour isoler des ordinateurs, arrêter leur isolation et pour modifier la liste des connexions autorisées pendant l'isolation.
  Avec le droit **Groupes d'agents - Afficher**, vous pouvez consulter l'état d'isolation des ordinateurs dans le panneau des groupes d'agents.

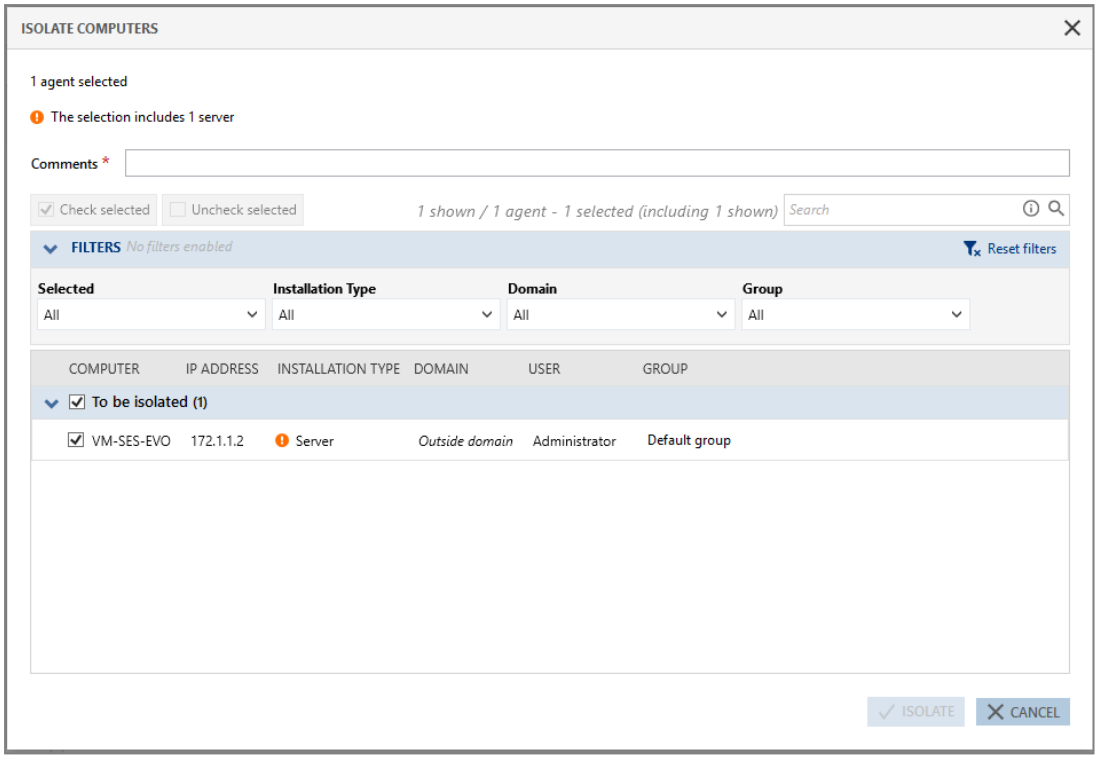
13.4.2 Isoler des ordinateurs

L'isolation des ordinateurs est possible quelle que soit la politique de sécurité appliquée aux agents.

La fonctionnalité est accessible depuis deux panneaux de la console :

- Dans le panneau **Agents**, depuis la vue **Tous les agents** ou depuis la vue d'un groupe d'agents, sélectionnez un ou plusieurs agents dans la liste et cliquez sur le bouton **Isoler les ordinateurs** en haut du panneau.
- Dans le panneau **Logs agents**, vous pouvez isoler un ou plusieurs ordinateurs directement depuis un log ou un groupe de logs si vous détectez un événement suspect. Sélectionnez un ou plusieurs logs puis cliquez sur le bouton **Actions** > **Réponse** > **Isoler l'ordinateur** en haut du panneau.

La fenêtre suivante s'affiche alors afin de créer la tâche d'isolation :



Les agents sélectionnés lors de la demande d'isolation s'affichent dans la liste. Vous pouvez filtrer l'affichage.

1. Entrez un commentaire.
2. Vérifiez la sélection d'agents à isoler. Si votre sélection d'agents comprend des agents installés sur des postes de type serveurs, assurez-vous que vous souhaitez bien isoler ces postes. Les services applicatifs installés sur ces postes ne seront plus accessibles (serveur web ou de messagerie, serveur de fichiers, etc.).
3. Cliquez sur **Isoler**.
   Le panneau de suivi de l'isolation s'affiche (menu **Réponses** > **Isolation**). Pour plus d'informations, reportez-vous à la section Suivre et analyser les ordinateurs isolés.

Dès que l'agent réceptionne une demande d'isolation :

- Les connexions TCP et UDP déjà ouvertes vers l'extérieur de l'ordinateur sont coupées. Vous pouvez cependant autoriser le maintien de certaines connexions. Pour plus d'informations, reportez-vous à la section Autoriser des connexions réseau pendant l'isolation.
- Les nouvelles connexions entrantes et sortantes ne sont plus possibles, exceptées les connexions nécessaires à la communication avec les gestionnaires d'agents (port TCP 17000) et les connexions autorisées. Pour plus d'informations, reportez-vous à la section Autoriser des connexions réseau pendant l'isolation.

Vous pouvez éteindre un ordinateur isolé, son état d'isolation est maintenu au redémarrage.

NOTE
Vous pouvez déplacer un agent isolé d'un groupe d'agents à un autre. Il conserve son état d'isolation.
A l'inverse, un agent isolé perd automatiquement son état d'isolation dans les cas suivants :
- Si vous demandez un retour de l'agent à une version antérieure à la version 2.5.3,
- Si vous désactivez la fonctionnalité **Réseaux** dans les paramètres du groupe d'agents.

13.4.3 Suivre les ordinateurs isolés

Le tableau de bord et le panneau **Isolation** permettent de suivre les agents isolés.

Sur le tableau de bord, le diagramme **Agents isolés** permet de connaître le nombre d'agents isolés du réseau et leur état d'isolation : Isolé, En attente d'isolation, En attente d'arrêt d'isolation. Pour plus d'informations, reportez-vous à la section Vérifier l'état des agents.

Depuis le panneau **Réponses** > **Isolation**, les actions suivantes sont disponibles :

- Consulter la liste des agents concernés par l'isolation,
- Arrêter l'isolation des agents. Pour plus d'informations, reportez-vous à la section Arrêter l'isolation.
- Créer des tâches d'analyse Yara et IoC directement sur les agents concernés (bouton **Recherche de menaces**). Pour plus d'informations, reportez-vous à la section Analyser les comportements sur les postes des utilisateurs.
- Définir des connexions réseau autorisées pendant l'isolation (onglet **Paramètres**). Pour plus d'informations, reportez-vous à la section Autoriser des connexions réseau pendant l'isolation.

13.4.4 Autoriser des connexions réseau pendant l'isolation

Par défaut, l'isolation bloque l'ensemble des connexions réseau de l'ordinateur sur les protocoles TCP et UDP, exceptées les requêtes DNS et DHCP sur le port 17000 afin de permettre la communication avec les gestionnaires d'agents SES Evolution.

L'onglet **Paramètres** du panneau **Isolation** vous permet d'autoriser d'autres connexions pendant l'isolation, en définissant des règles d'exception.

Pour ajouter des règles :

1. Cliquez sur **Modifier** dans le bandeau supérieur.
2. Cliquez sur **Ajouter une connexion réseau autorisée**.
3. Dans la fenêtre qui s'affiche, entrez une description.
4. Indiquez le chemin ou SID de l'application à autoriser.
5. Complétez les paramètres suivants et cliquez sur **OK**.
   La règle est créée. Elle s'applique à tous les agents, quel que soit le groupe d'agents auquel ils appartiennent.
6. Cliquez sur **Enregistrer** dans le bandeau supérieur.
7. Déployez l'environnement depuis le menu **Sécurité** > **Déploiement**.

Toutes les modifications effectuées dans cet onglet sont journalisées dans les logs Système.

Cette liste d'exceptions est prioritaire sur les règles réseau de la politique de sécurité. Elle n'est pas prioritaire sur les règles réseau d'autoprotection de l'agent.

13.4.5 Arrêter l'isolation

N'importe quel administrateur possédant les droits nécessaires peut mettre un terme à l'isolation d'un ordinateur même si un autre administrateur était à l'initiative de l'isolation.

Dès que l'agent réceptionne la demande d'arrêt d'isolation, les connexions TCP et UDP sont rétablies.

Pour arrêter l'isolation d'un ordinateur, rendez-vous dans le panneau **Isolation**, onglet **Général** :

1. Sur la ligne d'un agent ou sur une sélection d'agents, faites un clic droit > **Arrêter l'isolation pour la sélection**,
2. Entrez un commentaire,
3. Vérifiez la sélection d'agents,
4. Cliquez sur **Arrêter l'isolation**.

13.4.6 Précisions sur le fonctionnement de l'isolation et des challenges

Mode Maintenance

- Un agent en mode Maintenance peut réceptionner des demandes d'isolation ou d'arrêt d'isolation.
- Vous pouvez activer le mode Maintenance de l'agent sur un ordinateur en cours d'isolation. L'ordinateur conserve son état d'isolation.

Pour plus d'informations sur le mode Maintenance, reportez-vous à la section Activer le mode Maintenance.

Arrêt de l'agent

Lorsqu'un ordinateur est isolé et que vous demandez un arrêt de l'agent via un challenge :

- Les connexions réseau sont de nouveau autorisées,
- L'agent est toujours vu comme isolé dans la console d'administration, et les connexions réseau seront de nouveau coupées à la fin du challenge.

Lorsqu'un arrêt de l'agent via challenge est en cours et que vous réalisez une demande d'isolation de l'agent :

- La demande d'isolation est prise en compte, mais elle ne sera effective que lorsque le challenge aura pris fin.

Pour plus d'informations sur l'arrêt de l'agent, reportez-vous à la section Arrêter un agent.

13.4.7 Précisions sur la maintenance des agents isolés

Suppression automatique des agents

Le paramétrage de suppression automatique des agents déconnectés s'applique également aux agents isolés. Par défaut, un agent est supprimé après 30 jours consécutifs de déconnexion.

Pour plus d'informations, reportez-vous à la section Surveiller les agents en temps réel.

Désinstallation des agents

Vous pouvez désinstaller un agent isolé. Dans ce cas, s'il est connecté à son gestionnaire d'agents, la console d'administration ne le considère plus comme isolé du réseau.

S'il est déconnecté de son gestionnaire d'agents au moment de la désinstallation, la console d'administration le considère toujours comme isolé. Il sera supprimé automatiquement par le mécanisme de suppression automatique des agents déconnectés.

13.4.8 Limitations de la fonctionnalité d'isolation

Démarrage en mode sans échec

Les connexions réseau ne sont pas coupées lorsqu'un ordinateur isolé est redémarré en mode sans échec avec réseau.

Ordinateur déconnecté du réseau de la société

Lorsqu'un ordinateur ne se trouve plus sur le réseau interne de la société, dans le cas d'un utilisateur nomade par exemple, il ne peut pas recevoir une demande d'isolation ou d'arrêt d'isolation. La demande est prise en compte lors de sa reconnexion au réseau.

Accès temporaire au web

L'accès temporaire au web est moins prioritaire que l'isolation du réseau.

Lorsque vous réalisez une demande d'isolation d'un ordinateur bénéficiant d'un accès temporaire au web :

- L'accès temporaire est coupé et l'ordinateur est isolé,
- L'accès temporaire reprend à l'arrêt de l'isolation, avec le temps restant avant l'isolation si vous ne redémarrez pas l'ordinateur pendant son isolation,
- L'accès temporaire ne reprend pas à l'arrêt de l'isolation si vous redémarrez l'ordinateur pendant son isolation.

Pour plus d'informations sur l'accès temporaire au web, reportez-vous à la section Autoriser l'accès temporaire au web.

14. Télécharger les mises à jour Stormshield

Stormshield met régulièrement à votre disposition :

- Des nouvelles politiques de sécurité intégrées,
- Des mises à jour des jeux de règles intégrés ou de nouveaux jeux,
- Des ressources Yara,
- Des ressources IoC.

Ces ressources peuvent se trouver sur le serveur public Stormshield ou sur un serveur local de votre choix si vous travaillez dans un environnement déconnecté du réseau Internet. Pour plus d'informations sur la configuration d'un serveur personnalisé, reportez-vous à la section Configurer le serveur de mises à jour Stormshield

Vous pouvez les télécharger à tout moment dans votre console d'administration, indépendamment des mises à jour de SES Evolution.

Lorsque de nouvelles politiques, jeux de règles ou ressources Yara et IoC sont disponibles, un indicateur s'affiche sur l'icône  dans le bandeau supérieur de la console. Cliquez sur l'icône pour accéder au panneau de téléchargement des mises à jour.

Si vous souhaitez télécharger des ressources que vous ne possédez pas déjà, utilisez les boutons **Tout installer** depuis le menu ≡ ou **Installer** depuis le panneau de droite de chaque catégorie. Dans ce cas, les nouvelles versions de ressources que vous possédez déjà ne sont pas installées.

Si vous souhaitez télécharger des nouvelles versions de ressources que vous possédez, utilisez les boutons **Tout mettre à jour** depuis le menu ≡ ou **Mettre à jour** depuis le panneau de droite de chaque catégorie.

Vous devez disposer au minimum du droit **Afficher** sur les **Politiques** ou **Ressources** pour visualiser les mises à jour disponibles dans ce panneau.

Des notes de version décrivent les nouveautés pour chaque ressource. Vous pouvez les consulter au format PDF en cliquant sur l'icône  sur la ligne de la ressource, si le fichier PDF est présent sur le serveur de mise à jour.

Après le téléchargement d'une mise à jour de jeux de règles déjà déployés, une nouvelle version des politiques concernées est automatiquement créée si vous avez sélectionné **Toujours utiliser la dernière version** des jeux et vous n'avez rien à faire.

Après le téléchargement de ressources Yara ou IoC déjà utilisées et déployées dans des règles, une nouvelle version des jeux de règles utilisant ces ressources est automatiquement créée.

Retrouvez les nouvelles ressources Yara ou IoC dans le menu **Sécurité** > **Ressources**, sous les catégories **Stormshield YARA** et **Stormshield IOC**.

Vous devez disposer du droit **Modifier** sur les **Politiques** pour effectuer ces opérations.

Selon les rôles des utilisateurs, vous pouvez rendre ce panneau inaccessible ou l'afficher en lecture seule seulement, grâce à la permission **Mise à jour** dans le panneau des utilisateurs. Si vous sélectionnez le droit **Aucun**, le panneau de téléchargement des mises à jour n'est pas visible.

Pour plus d'informations, reportez-vous à la section Gérer les utilisateurs de la console d'administration SES Evolution.

Pour désactiver les notifications lorsqu'une nouvelle mise à jour est disponible, décochez **Activer les notifications** en haut à droite du panneau.

Pour plus d'informations sur les ressources disponibles dans ce panneau, reportez-vous aux sections Comprendre les politiques de sécurité intégrées et personnalisées, Comprendre les jeux de règles intégrés et Analyser les comportements sur les postes des utilisateurs.

15. Administrer les composants backoffice

Le serveur SES Evolution est constitué de plusieurs composants backoffice :

- Un ou plusieurs **gestionnaires d'agents**,
- Un ou plusieurs **backend**,
- Deux bases de données SQL Server : une pour les données d'administration et une pour les logs,
- Une ou plusieurs **consoles d'administration**,

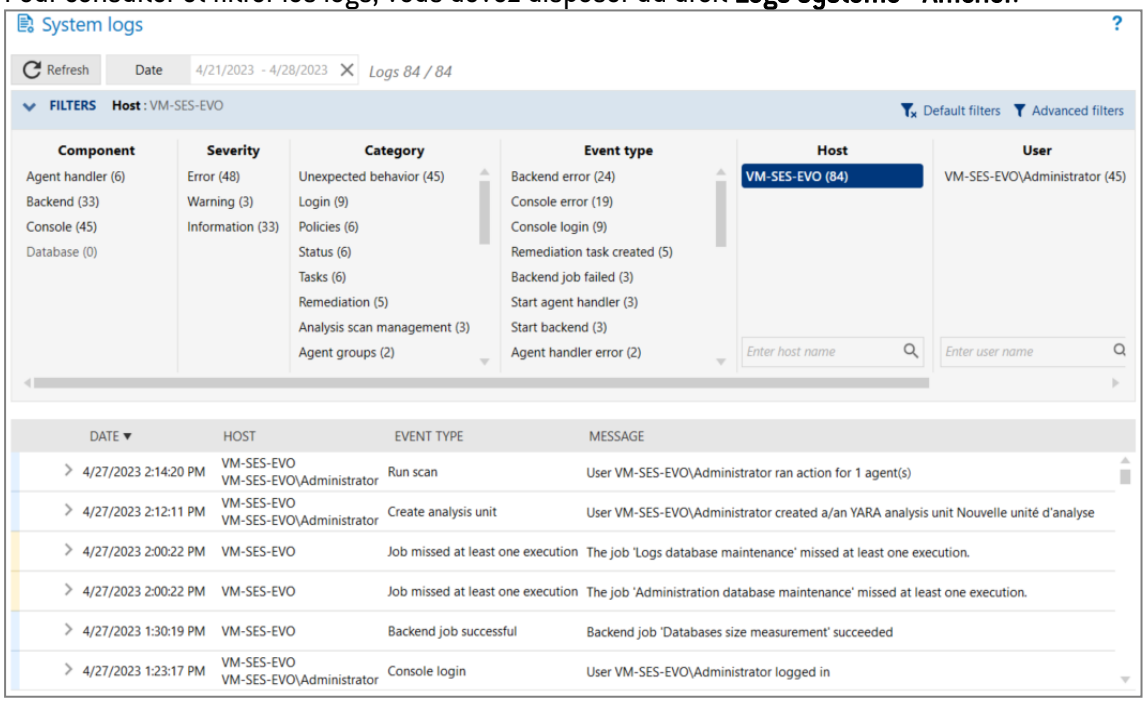
Vous pouvez consulter les logs générés par SES Evolution lorsqu'un événement se produit sur l'un de ces composants.

Vous pouvez aussi contrôler la taille de la base de données de logs, configurer un serveur SMTP pour l'envoi d'e-mails d'alertes ou d'indicateurs, configurer le serveur de mises à jour Stormshield, etc.

15.1 Surveiller l'activité des composants backoffice SES Evolution

L'activité des composants backoffice installés par la solution SES Evolution génère des logs qui sont consultables dans la console d'administration.

Pour consulter et filtrer les logs, vous devez disposer du droit **Logs système - Afficher**.



Pour consulter les logs système :

1. Choisissez le menu **Backoffice > Logs système**.
   La liste des logs de tous les composants s'affiche en fonction des filtres actifs. À la première ouverture du panneau des logs, ce sont tous les logs émis dans les dernières 24 heures qui sont visibles.

2. Cliquez sur le bouton **Date** pour choisir la période à visualiser, puis cliquez sur **Appliquer**. La flèche double permet de sélectionner la période à l'aide d'un calendrier. La croix à droite du champ **Date** réinitialise la période aux dernières 24 heures.
   La liste des logs émis lors de la période sélectionnée s'affiche.
3. Dans le tableau **Filtres**, activez des filtres pour personnaliser votre liste de logs. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant.
   Dans les colonnes **Machine** et **Utilisateur**, vous pouvez rechercher les machines et utilisateurs souhaités en entrant tout ou partie de leur nom dans le champ de recherche.
   À tout moment, vous pouvez retrouver le filtrage initial en cliquant sur **Filtres par défaut** : tous les logs seront à nouveau affichés.
   La couleur à gauche d'une ligne de log indique le niveau de gravité :
   - Bleu : Information,
   - Jaune : Avertissement,
   - Orange : Erreur.
4. Cliquez sur la petite flèche à gauche du log pour l'ouvrir et afficher des informations complémentaires :
   - Onglet **Détails** : Description complète de l'événement ayant causé le log.
   - Onglet **Log brut** : Code du log au format JSON.

15.2 Superviser les bases de données

SES Evolution utilise une base de données d'administration et une base de données de logs. Selon la configuration de vos politiques de sécurité et la quantité de logs souhaitée, le volume de ces bases de données peut augmenter rapidement et atteindre un seuil critique.

SES Evolution vous permet de suivre le remplissage des bases de données et d'anticiper leur saturation grâce à un calcul prévisionnel et des alertes. Vous pouvez également planifier des sessions de maintenance ou de suppression des logs.

15.2.1 Consulter les informations générales sur les bases de données

1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet de la base de données souhaitée, Administration ou Logs.
2. Dans la section **SQL Server**, consultez les informations suivantes :

Instance	Nom de l'instance SQL Server.
Version	Version de SQL Server utilisée.
Dernière connexion	Nombre de secondes depuis la dernière connexion du backend à la base de données.
Statut	• Vert: Toutes les bases de données sont joignables, et l'espace disque occupé est inférieur à 71%, et la saturation des bases de données est estimée à plus de trois mois. • Orange: Sur au moins une base de données, entre 71% et 80% de l'espace disque est occupé, ou la saturation est estimée entre un mois et trois mois. • Rouge: Au moins une base de données est injoignable, ou l'espace disque occupé est supérieur à 80%, ou la saturation d'une des bases de données est estimée à moins d'un mois.

Fichiers de la base de données	• **Utilisation** : Pourcentage de l'espace disponible actuellement utilisé par le fichier. • **Espace utilisé** : Espace actuellement alloué par SQL Server pour le fichier. • **Capacité** : Espace disponible sur le disque pour le fichier.

15.2.2 Surveiller la taille des bases de données

SES Evolution permet de surveiller la taille des bases de données de plusieurs façons : au moyen d'un graphique, et pour la base de données de logs via le mode automatique dégradé.

Estimer et surveiller la taille des bases de données via un graphique

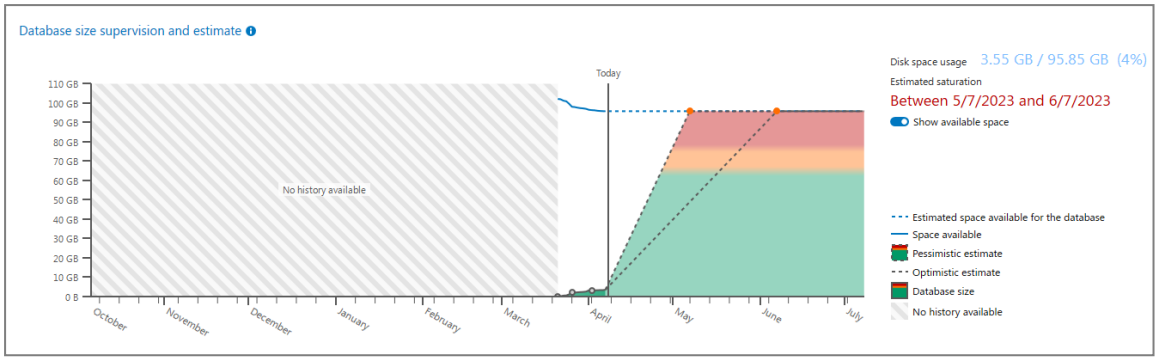
1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet de la base de données souhaitée, Administration ou Logs.
2. Dans la section **Suivi et estimation de la taille de la base de données**, consultez le graphique. Il affiche des informations sur le remplissage de la base de données sur 9 mois. Pour plus d'informations, reportez-vous à la section Comprendre le graphique de suivi des bases de données
3. Par défaut un log de sévérité *Avertissement* s'affiche dans les logs système trois mois avant la date estimée de saturation de la base de données, et un log de sévérité *Erreur* un mois avant. Pour la base de données de logs uniquement, si les valeurs par défaut ne vous conviennent pas, cliquez sur **Modifier** dans le bandeau supérieur, et choisissez le nombre de mois souhaités en modifiant les paramètres suivants :
   - **Générer un avertissement *n* mois avant la date estimée de saturation**
   - **Générer une erreur *n* mois avant la date estimée de saturation**

   Un bandeau de couleur s'affiche également lorsque la date de saturation se rapproche : orange entre trois mois et un mois de la date, ou rouge à partir d'un mois.
4. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Comprendre le graphique de suivi des bases de données

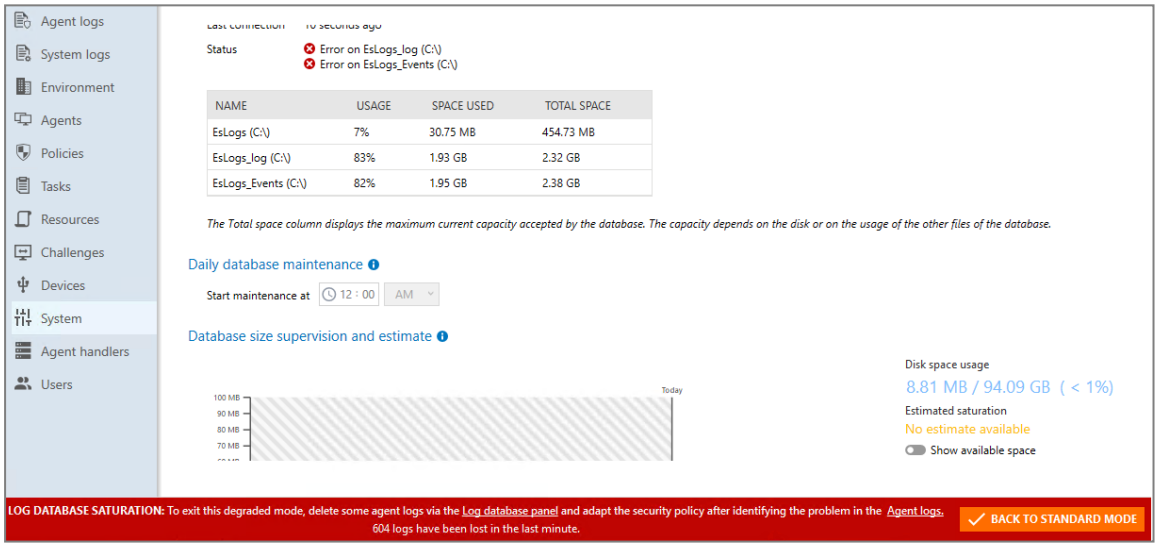
Le graphique **Suivi et estimation de la taille de la base de données** est divisé en deux parties :

- La partie gauche affiche six mois d'historique de remplissage de la base de données jusqu'à la date du jour. La taille de la base de données est mesurée quotidiennement à *00:00* UTC. Les points sur le graphique correspondent à la mesure prise le premier jour de chaque semaine.
- La partie droite affiche trois mois d'augmentation prévisionnelle de la taille de la base de données à partir de la date du jour. Pour plus de fiabilité, elle n'est visible qu'après 14 jours d'utilisation de la base de données.
  Le premier point orange indique la date à laquelle la base de données sera saturée dans un scénario de prévisions pessimiste. Le deuxième point orange représente la même date dans un scénario optimiste.
- **Utilisation de l'espace disque** : Espace disque utilisé par rapport à l'espace disponible, et pourcentage d'occupation.
- **Saturation estimée** : Période à laquelle il est estimé que la base de données arrivera à saturation.
- **Afficher l'espace disponible** : Permet d'afficher ou de masquer l'espace disponible sur le graphique et donc d'en changer l'échelle. Activez cette option lorsque le volume de la base de données par rapport à l'espace disponible devient significatif.



Gérer le volume des logs via le mode automatique dégradé

Pour éviter la saturation de la base de données de logs en cas de génération très rapide et importante de logs, un mode dégradé s'active lorsque cette base de données atteint le seuil de remplissage critique de 81%. Un bandeau d'alerte rouge s'affiche dans la partie inférieure de la console d'administration.



Tant que ce mode est actif, les nouveaux logs agents et système transmis au Backoffice ne sont plus stockés dans la base de données de logs, mais sont définitivement supprimés.

Toutefois, si vous avez configuré des serveurs Syslog pour les gestionnaires d'agents, ils continuent de recevoir les logs agents.

Pour pouvoir désactiver ce mode dégradé et stocker de nouveau les logs, vous devez réduire le volume de la base de données de logs au dessous du seuil de 81%. Pour ce faire, suivez les instructions ci-dessous :

1. Analysez les logs pour comprendre d'où provient l'afflux de logs,
2. Ajustez votre politique de sécurité pour produire moins de logs, par exemple en diminuant les faux-positifs,
3. Supprimez manuellement des logs agents,
4. Une fois le volume des logs réduit, cliquez sur le bouton **Retour au mode standard** dans le bandeau rouge de la console d'administration.
   Le bandeau disparaît et les logs sont de nouveau stockés dans la base de données de logs.

15.2.3 Configurer la tâche de maintenance quotidienne

SES Evolution réalise automatiquement une maintenance quotidienne de la base de données pour :

- Défragmenter les index et optimiser les performances de la base de données,
- Supprimer les logs les plus anciens de la base de données de logs. Pour définir les critères de suppression des logs, référez-vous à Gérer la suppression des logs .

Par défaut cette tâche de maintenance est planifiée tous les jours à 00:00 à l'heure locale du backend, mais vous pouvez en modifier l'horaire. Il est recommandé de planifier cette maintenance avant les autres opérations de maintenance SQL Server. Cela permet par exemple d'effectuer ensuite des sauvegardes moins volumineuses.

Pour configurer la tâche de maintenance quotidienne :

1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet de la base de données souhaitée, Administration ou Logs.
2. Dans le bandeau du haut, cliquez sur le bouton **Modifier**.
3. Dans la section **Maintenance quotidienne de la base de données**, saisissez l'heure à laquelle vous souhaitez démarrer cette maintenance.
4. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

15.2.4 Gérer la suppression des logs

Selon la configuration de vos politiques de sécurité et la quantité de logs souhaitée, la base de données de logs peut devenir rapidement volumineuse. Différents outils sont à votre disposition pour supprimer les logs et éviter la saturation de la base de données :

- Suppression mensuelle des logs système et agent ayant dépassé la durée de rétention spécifiée.
- Suppression quotidienne des logs agent selon les critères spécifiés, effectuée par la tâche de maintenance. Pour plus d'informations, reportez-vous à la section Configurer la tâche de maintenance quotidienne.
- Suppression manuelle des logs agent.

Supprimer mensuellement des logs système et agent

Par défaut, les logs système et agent sont conservés pendant 12 mois, ou deux mois si vous utilisez SQL Server Express. Les logs plus anciens sont supprimés. Vous pouvez modifier ces valeurs.

1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet **Base de données de logs**.
2. Dans le bandeau du haut, cliquez sur le bouton **Modifier**.
3. Dans la section **Suppression mensuelle de logs**, choisissez le nombre de mois pendant lequel vous souhaitez conserver les événements des agents et les logs système. Passée cette durée, ils sont supprimés par une tâche automatique une fois par mois.

Pour conserver les logs indéfiniment, désactivez la suppression mensuelle en grisant le bouton  . Il n'est pas possible de désactiver la suppression des logs si vous utilisez SQL Server Express.

Supprimer quotidiennement des logs agent

Vous pouvez configurer des règles de suppression quotidienne de logs. La tâche de maintenance vérifiera quotidiennement les critères spécifiés dans les règles et supprimera les

logs répondant à tous ces critères.

Pour configurer une règle de suppression de logs :

1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet **Base de données de logs**.
2. Dans le bandeau du haut, cliquez sur le bouton **Modifier**.
3. Dans la section **Suppression quotidienne de logs agent**, cliquez sur **Ajouter une règle**.
   La fenêtre **Ajouter une règle quotidienne** s'affiche.
4. Spécifiez les critères de suppression des logs :

Date	Choisissez de supprimer les logs antérieurs à une certaines période, ou de supprimer tous les logs, quelle que soit leur ancienneté.
Gravité	Choisissez les niveaux de logs à supprimer. Voir la section Gérer les logs.
État	Choisissez les états de logs à supprimer. Voir la section Gérer les logs.
Groupes d'agents (Optionnel)	Sélectionnez les groupes d'agents pour lesquels vous souhaitez supprimer des logs. Par défaut tous les groupes d'agents sont concernés.

5. Cliquez sur **OK**. La règle de suppression des logs s'affiche dans le tableau.
6. Si besoin, désactivez une ou plusieurs règles en décochant la case **État** à gauche du tableau. Cliquez sur **Masquer les règles désactivées** pour les retirer du tableau. Les règles sont exécutées chaque jour pendant la tâche de maintenance. Le résultat de la dernière exécution s'affiche dans la colonne **Dernier résultat**.

Supprimer manuellement des logs agent

Si besoin, vous pouvez ponctuellement effectuer une suppression manuelle des logs agent selon certains critères.

1. Choisissez le menu **Backoffice > Système** et cliquez sur l'onglet **Base de données de logs**.
2. Dans le bandeau du haut, cliquez sur le bouton **Modifier**.
3. Dans la section **Suppression manuelle de logs agent**, cliquez sur **Paramétrer et démarrer une suppression manuelle**.
   La fenêtre **Ajouter une règle manuelle** s'affiche.
4. Spécifiez les critères de suppression des logs :

Date	Choisissez l'ancienneté des logs que vous souhaitez supprimer en nombre de jours/mois ou en dates absolues.
Gravité	Choisissez les niveaux de logs à supprimer. Voir la section Gérer les logs.
État	Choisissez les états de logs à supprimer. Voir la section Gérer les logs.
Groupes d'agents (Optionnel)	Sélectionnez les groupes d'agents pour lesquels vous souhaitez supprimer des logs. Par défaut tous les groupes d'agents sont concernés.
Agents (Optionnel)	Saisissez le nom des agents pour lesquels vous souhaitez supprimer des logs, puis sélectionnez-les. Par défaut tous les agents du parc sont concernés.

5. Cliquez sur **Estimer le volume** en bas à droite pour afficher le volume de logs qui sera supprimé.

6. Cliquez sur **Démarrer**.
   Tous les logs correspondant aux critères spécifiés sont supprimés. Le résultat de la dernière exécution s'affiche dans la colonne **Dernier résultat**.

> **NOTE**
> L'espace libéré par la suppression manuelle sera visible dans le graphique Suivi et estimation de la taille de la base de données uniquement après la prochaine tâche de maintenance.

7. Cliquez sur **Relancer la suppression manuelle** pour supprimer les logs selon les mêmes critères que lors de la suppression précédente.

15.3 Configurer le serveur de mises à jour Stormshield

Stormshield met régulièrement à votre disposition un certains nombre de ressources telles que des nouvelles politiques de sécurité ou jeux de règles, des ressources Yara ou IoC.

Par défaut, les mises à jour sont disponibles sur un serveur public Stormshield, mais vous pouvez utiliser le serveur de votre choix.

Pour personnaliser le serveur de mise à jour :

1. Choisissez le menu **Backoffice > Système**, onglet **Général**.
2. Cliquez sur **Modifier** dans le bandeau supérieur.
3. Par défaut, la fonctionnalité est activée. Si vous la désactivez, le panneau de téléchargement des mises à jour n'est plus visible et les notifications de nouvelles mises à jour disponibles sont également automatiquement désactivées.
4. Dans la section **Serveur de mises à jour**, choisissez la fréquence de connexion au serveur. Choisissez **Jamais** pour désactiver la connexion automatique au serveur. Dans ce cas, cliquez sur le bouton **Vérifier les mises à jour** dans le panneau de téléchargement des mises à jour pour vous connecter manuellement au serveur.
5. Conservez l'adresse du serveur Stormshield par défaut ou bien entrez l'adresse d'un serveur local de votre choix.
6. Vérifiez que la connexion au serveur fonctionne en cliquant sur **Vérifier l'adresse**.

> **NOTE**
> Le composant backend établit une connexion au serveur de mises à jour en HTTPS sur le port TCP 443. S'il existe plusieurs composants backend, l'un d'entre eux est choisi au hasard pour effectuer la connexion au serveur de mises à jour.

Une fois le serveur configuré, vous pouvez Télécharger les mises à jour Stormshield.

15.4 Envoyer des alertes de logs système par e-mail

Vous pouvez configurer SES Evolution afin d'envoyer des alertes par e-mail aux personnes de votre choix. Les alertes sont déclenchées par certains logs générés sur les composants backoffice SES Evolution.

Au préalable vous devez configurer un serveur SMTP. Pour plus d'informations, reportez-vous à la section Configurer un serveur SMTP.

Vous devez disposer du droit **Notifications par e-mails-Modifier** pour configurer l'envoi d'alertes.

Pour envoyer des alertes par e-mail :

1. Dans le menu **Backoffice > Système** de la console d'administration, rendez-vous dans l'onglet **Notifications par e-mail**.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.
3. Dans la zone **Alertes des logs système**, cliquez sur **Ajouter une règle**.
   L'assistant de création d'une règle s'ouvre.
4. Saisissez les paramètres de la règle :
   - **Nom de la règle**.
   - **Préfixe de l'objet de l'e-mail** reçu par le destinataire. Par défaut, l'objet de l'e-mail commence par *SES EVOLUTION*. Le préfixe vous permet d'appliquer un traitement spécifique aux e-mails d'alerte SES Evolution dans votre messagerie.
   - **Types de logs** pour lesquels vous souhaitez déclencher des alertes parmi les catégories **Services SES**, **Bases de données**, et **Services externes**.
5. Cliquez sur **Suivant**.
6. Dans le champ en bas de l'écran, saisissez l'adresse e-mail de l'utilisateur destinataire des alertes, choisissez sa langue, puis cliquez sur **Ajouter**.
7. Ajoutez d'autres adresses e-mail si vous souhaitez envoyer les alertes à plusieurs destinataires.
8. Cliquez sur **Créer**.
   La règle est ajoutée dans le tableau de la zone **Alertes des logs système**.
9. Ajoutez d'autres règles si besoin.

Quand les composants système génèrent des logs correspondant aux règles, alors un e-mail d'alerte est envoyé.

Vous pouvez désactiver ou réactiver une règle d'envoi en cliquant sur la case à cocher de la colonne **Activé**. Les boutons d'actions à droite d'une règle permettent de la dupliquer ou de la supprimer.

Vous pouvez arrêter temporairement l'envoi des e-mails en désactivant l'option **Activer les notifications**.

SES Evolution permet également d'envoyer par e-mail des alertes sur les logs agents ou tout le contenu du tableau de bord. Pour plus d'informations, reportez-vous aux sections Envoyer des alertes de logs agents par e-mail et Envoyer les indicateurs du tableau de bord par e-mail.

15.5 Configurer un serveur SMTP

Vous devez configurer un serveur SMTP pour permettre à SES Evolution d'envoyer :

- Des e-mails d'alerte en fonction des types de logs agents générés,
- Des e-mails d'alerte en fonction des types de logs système générés,
- Des e-mails contenant les indicateurs du tableau de bord.

Vous devez disposer du droit **Système-Modifier** pour configurer un serveur SMTP.

1. Dans le menu **Backoffice > Système** de la console d'administration, rendez-vous dans l'onglet **Général**.
2. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.

3. Dans la zone **Serveur SMTP**, définissez les paramètres suivants :
   - **Adresse du serveur** : Saisissez le nom DNS ou l'adresse IP du serveur SMTP.
   - **Sécurité de la connexion** : Choisissez si la connexion doit être chiffrée, et par quel protocole.
   - **Port** : Saisissez le numéro de port de communication, par défaut 587 pour STARTTLS.
   - **Nom de l'expéditeur** : Nom de l'émetteur des notifications. Il est visible pour les destinataires des e-mails.
   - **Adresse e-mail de l'expéditeur** : Adresse e-mail de l'émetteur des notifications. Elle est visible pour les destinataires des e-mails. Veillez à vérifier régulièrement la messagerie de l'expéditeur afin de vérifier si des e-mails sont retournés en raison d'erreurs dans l'adresse du destinataire.
   - **Authentification requise** : Activez cette option si votre service SMTP nécessite une authentification. Saisissez alors l'identifiant et le mot de passe du service.
4. Cliquez sur **Vérifier les paramètres** pour tester la connexion au serveur SMTP. Aucun envoi d'e-mail n'est effectué lors de ce test.

16. Activer et gérer l'API publique de SES Evolution

SES Evolution dispose d'une API REST permettant d'utiliser la solution via vos propres outils d'orchestration.

Toutes les fonctionnalités de SES Evolution ne sont pas encore disponibles dans l'API publique. Celle-ci est enrichie au fur et à mesure des versions.

Par défaut, l'API publique n'est pas activée.

L'authentification sur l'API publique est sécurisée par des clés API, générées par les administrateurs. Ces clés possèdent une utilisation ainsi qu'une durée de validité paramétrables.

Les actions de type POST effectuées via l'API publique sont consignées dans les logs système.

Pour faciliter l'utilisation de l'API, une documentation OpenAPI est accessible via un lien affiché dans la console d'administration. Elle est également disponible sur le site de la Documentation technique Stormshield.

16.1 Prérequis

Vous devez disposer du droit **API publique-Modifier** pour activer l'API publique et générer des clés, à partir du menu **Clés API** de la console d'administration. Voir Gérer les utilisateurs de la console d'administration SES Evolution.

Ce droit est prioritaire sur le droit **Système**. Si un administrateur n'a aucun droit **Système**, mais possède le droit **API publique-Afficher** ou **API publique-Modifier**, le menu **Système** s'affiche avec uniquement l'onglet **Clés API**.

16.2 Activer l'API publique

L'API publique de SES Evolution est désactivée par défaut.

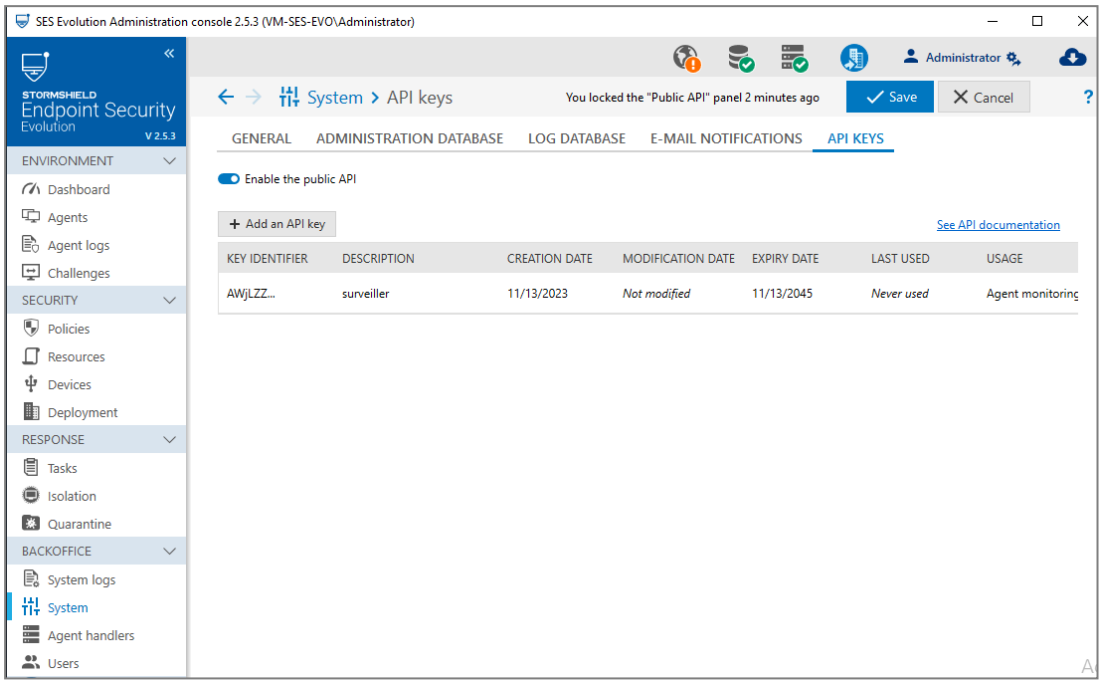
Lorsque l'API publique est activée :

- l'accès aux routes de l'API est autorisé,
- les administrateurs autorisés peuvent créer, modifier et révoquer des clés API.

Pour activer l'API publique :

1. Dans le menu **Backoffice** > **Système**, affichez l'onglet **Clés API**,
2. Cliquez sur **Modifier** dans le bandeau supérieur,

3. Cochez **Activer l'API publique**.



16.3 Ajouter une clé API

L'onglet **Clés API** permet d'ajouter, modifier et révoquer les clés donnant accès aux routes de l'API publique de SES Evolution.

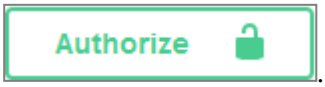
Ces clés possèdent un identifiant, une description, une date de création, une date d'expiration et une utilisation. Elles sont nécessaires pour chaque requête de l'API publique.

Pour ajouter une clé :

1. Cliquez sur **Modifier** dans le bandeau supérieur.
2. Cliquez sur **Ajouter une clé API**.
3. Entrez une description.
4. Choisissez une durée de validité. Après la création de la clé, vous ne pourrez plus modifier cette durée.
5. Cochez les utilisations de la clé, qui ouvrent l'accès aux différentes routes proposées par l'API.
6. Lorsque vous cliquez sur **OK**, la clé n'est pas enregistrée en base de données. Vous devez la copier et la stocker en sécurité car elle ne sera plus disponible par la suite.
7. Cliquez sur **Fermer**, puis sur **Enregistrer** dans le bandeau supérieur.

Tous les administrateurs de SES Evolution qui ont le droit d'afficher l'onglet **Clés API** ont accès à la liste des clés créées.

Une clé API peut être utilisée dans la documentation de l'API pour tester les requêtes :

1. Cliquez sur le lien **Voir la documentation API**.
2. Cliquez sur le bouton 

.

3. Entrez la clé API dans le champ **Value**.
4. Cliquez sur **Authorize** puis sur **Close**.

16.4 Révoquer une clé API

Vous pouvez révoquer les clés API. Lorsqu'elles sont révoquées, vous ne pouvez plus les utiliser pour faire des requêtes sur l'API.

Pour révoquer une clé :

1. Cliquez sur **Modifier** dans le bandeau supérieur,
2. Sur la ligne de la clé à révoquer, cliquez sur l'icône  dans la colonne **Actions**,
3. Validez.

Si vous souhaitez afficher dans le tableau seulement les clés non révoquées, activez le bouton **Cacher les clés révoquées**.

16.5 Résoudre les problèmes

16.5.1 La documentation de l'API publique ne s'affiche pas

Situation : Le lien **Voir la documentation API** dans la console d'administration ouvre un navigateur Internet et la documentation ne s'affiche pas.

Cause : Si vous avez mis à jour SES Evolution vers la version 2.6.3 et si votre serveur backend est installé sur le système d'exploitation Windows Server 2022, l'option TLS 1.3 est activée par défaut dans les paramètres IIS du backend. Cette option rend la documentation API incompatible avec ce système d'exploitation.

Solution : Dans votre Gestionnaire de services IIS, vous devez désactiver l'option **TLS 1.3 over TCP** dans les paramètres du nom d'hôte du backend. Le nom d'hôte à modifier est visible dans l'URL de la documentation API. Il correspond au nom d'hôte du cluster du backend, utilisé lors de l'installation de SES Evolution.

17. Résoudre les problèmes

Si vous rencontrez des problèmes avec les composants backoffice ou avec les agents sur les postes des utilisateurs, SES Evolution permet d'établir des diagnostics en mettant à votre disposition un outil dédié.

Si vous rencontrez des problèmes exclusivement avec des agents, SES Evolution propose également un mécanisme de challenge permettant de désactiver ou désinstaller un agent.

17.1 Résoudre les problèmes avec les challenges

Lorsqu'un utilisateur rencontre un problème sur son poste ou a besoin d'effectuer des actions qui ne sont pas possibles lorsque l'ensemble de l'agent SES Evolution est fonctionnel, il a la possibilité de demander à l'administrateur de la sécurité la désactivation temporaire de l'agent ou sa désinstallation, ainsi que l'autorisation de lancer un diagnostic.

La fonctionnalité **Challenges** doit être activée dans l'onglet **Paramètres** des groupes d'agents.

EXEMPLES

- Il peut être nécessaire de désactiver l'autoprotection de l'agent pour diagnostiquer des éventuels problèmes de compatibilité avec d'autres logiciels.
- Il peut être nécessaire d'arrêter temporairement l'agent sur un poste hors connexion le temps de faire des opérations de maintenance comme une installation ou une mise à jour de logiciel métier.

En tant qu'administrateur de la sécurité, vous avez la responsabilité du choix de l'action à exécuter sur le poste de travail de l'utilisateur et vous devez disposer d'un rôle comportant le droit **Challenges-Répondre**.

Le mécanisme de challenge se base sur un système de question/réponse entre l'agent et la console.

L'utilisateur du poste de travail génère depuis l'agent une chaîne de caractères (la question) qu'il vous transmet par téléphone ou par messagerie. Vous saisissez cette chaîne dans la console, qui génère alors une autre chaîne de caractères (la réponse) contenant la définition de l'action à autoriser. Vous transmettez cette réponse à l'utilisateur pour qu'il la rentre dans l'interface de l'agent. L'action est alors autorisée pour une durée que vous avez définie.

Le mécanisme fonctionne même lorsque l'agent n'est pas connecté au réseau.

Les actions possibles grâce aux challenges sont :

- l'activation du mode Maintenance,
- l'arrêt de l'agent,
- le lancement d'un diagnostic avec ou sans prise de traces,
- la désinstallation de l'agent.

L'activation de ces actions via le mécanisme des challenges ne requiert pas les droits d'administration du côté du poste de travail de l'utilisateur.

Pour des informations sur le mode Maintenance, reportez-vous à la section Comprendre l'autoprotection des agents et réaliser des opérations de maintenance.

Pour des informations sur le diagnostic et la prise de traces, reportez-vous à la section Diagnostiquer les problèmes sur les agents.

17.1.1 Activer le mode Maintenance

Le mode Maintenance désactive l'autoprotection de l'agent et permet de réaliser des opérations de maintenance ou de test.

EXEMPLE
Vous pouvez y recourir pour modifier les autorisations sur certaines clés de registre.

Pour activer ce mode via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône dans la barre des tâches.
2. Se rendre dans l'onglet pour ouvrir le panneau **Aide et Support**.
3. Dans l'onglet **Assistance**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Environnement > Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Mode Maintenance**.
4. Sélectionnez une durée.
5. Cliquez sur **Générer**.
6. Transmettez le code de réponse à l'utilisateur.
7. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.

L'utilisateur peut terminer le challenge en cours à tout moment dans le bandeau inférieur de l'interface de l'agent.

L'activation du mode Maintenance est également possible depuis l'onglet **Assistance** du panneau **Aide et Support** de l'interface de l'agent. Il doit avoir été autorisé au préalable dans la configuration des groupes d'agents et l'utilisateur du poste de travail doit posséder les droits d'administration pour activer ce mode. Pour plus d'informations sur la désactivation de l'autoprotection et le mode Maintenance, reportez-vous à la section Comprendre l'autoprotection des agents et réaliser des opérations de maintenance.

17.1.2 Arrêter un agent

Si l'activation du mode Maintenance d'un agent n'est pas suffisante pour résoudre certains problèmes, l'arrêt temporaire de l'agent peut être nécessaire. L'arrêt de l'agent permet de désactiver la protection appliquée par les règles de la politique de sécurité en plus de l'autoprotection.

Pour arrêter un agent via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône dans la barre des tâches.
2. Se rendre dans l'onglet pour ouvrir le panneau **Aide et Support**.
3. Dans l'onglet **Assistance**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Environnement > Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Arrêt de l'agent**.
4. Sélectionnez une durée.
5. Cliquez sur **Générer**.
6. Transmettez le code de réponse à l'utilisateur.
7. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.

L'utilisateur peut terminer le challenge en cours à tout moment dans le bandeau inférieur de l'interface de l'agent.

17.1.3 Lancer un diagnostic

SES Evolution fournit un outil de diagnostic qui permet de collecter des données sur les postes des utilisateurs en cas de problème. Les données collectées peuvent être analysées par le Support technique de Stormshield.

Pour lancer un diagnostic depuis un agent via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône  dans la barre des tâches.
2. Se rendre dans l'onglet  pour ouvrir le panneau **Aide et Support**.
3. Dans l'onglet **Assistance**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Environnement > Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Lancement d'un diagnostic**.
4. Si nécessaire, activez la prise de traces. Elle permet d'enregistrer une suite d'opérations exécutées par l'utilisateur et qui ont mené à un comportement inattendu de SES Evolution
5. Cliquez sur **Générer**.
6. Transmettez le code de réponse à l'utilisateur.
7. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.
8. Reportez-vous ensuite à la section Diagnostiquer les problèmes sur les agents pour utiliser l'outil de diagnostic.

17.1.4 Désinstaller un agent

En cas d'incompatibilité entre un autre logiciel et l'agent SES Evolution bloquant le travail de l'utilisateur par exemple, la seule solution est de désinstaller l'agent.

Pour désinstaller l'agent via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône  dans la barre des tâches.
2. Se rendre dans l'onglet  pour ouvrir le panneau **Aide et Support**.

3. Dans l'onglet **Assistance**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Environnement > Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Désinstallation de l'agent**.
4. Cliquez sur **Générer**.
5. Transmettez le code de réponse à l'utilisateur.
6. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.

Une fois démarré, ce challenge ne peut être arrêté et il n'y a pas de retour arrière possible. L'utilisateur doit redémarrer son poste de travail pour terminer correctement la procédure.

La désinstallation de l'agent est également possible via la procédure classique de désinstallation d'un programme, à condition que la configuration du groupe d'agents l'autorise. L'utilisateur doit posséder les droits d'administration. Pour plus d'informations, reportez-vous aux sections Autoriser les administrateurs à désinstaller les agents et Désinstaller les agents.

17.2 Établir un diagnostic

En cas de fonctionnement anormal des composants backoffice (serveur backend, gestionnaire d'agents, console d'administration) ou des agents SES Evolution, le Support technique de Stormshield peut vous proposer d'utiliser l'outil de diagnostic fourni avec la solution. Celui-ci collecte des données concernant le composant qui pose problème et le système de la machine. Le Support technique possède un outil d'analyse de ces données, qui sont compilées sous la forme d'un package de diagnostic, et peut ainsi rechercher la cause du problème.

17.2.1 Diagnostiquer les problèmes sur les composants backoffice

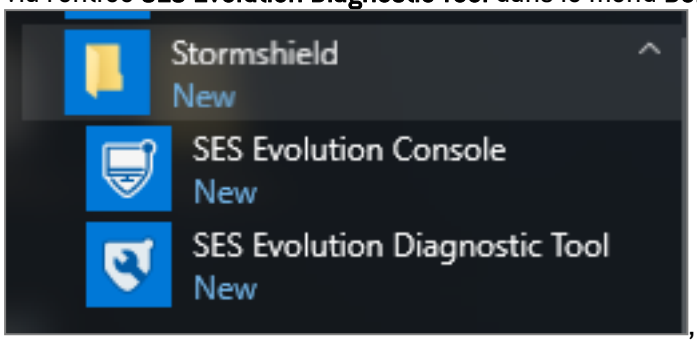
L'outil de diagnostic *EsDiag.exe* est installé avec tous les composants backoffice de SES Evolution. Il permet de collecter différentes données sur un poste sur lequel se présente un problème et de les rassembler dans un package de diagnostic (*.zip*) à fournir au Support technique de Stormshield pour l'analyse.

> **NOTE**
> Les droits d'administration sont nécessaires pour utiliser l'outil de diagnostic.

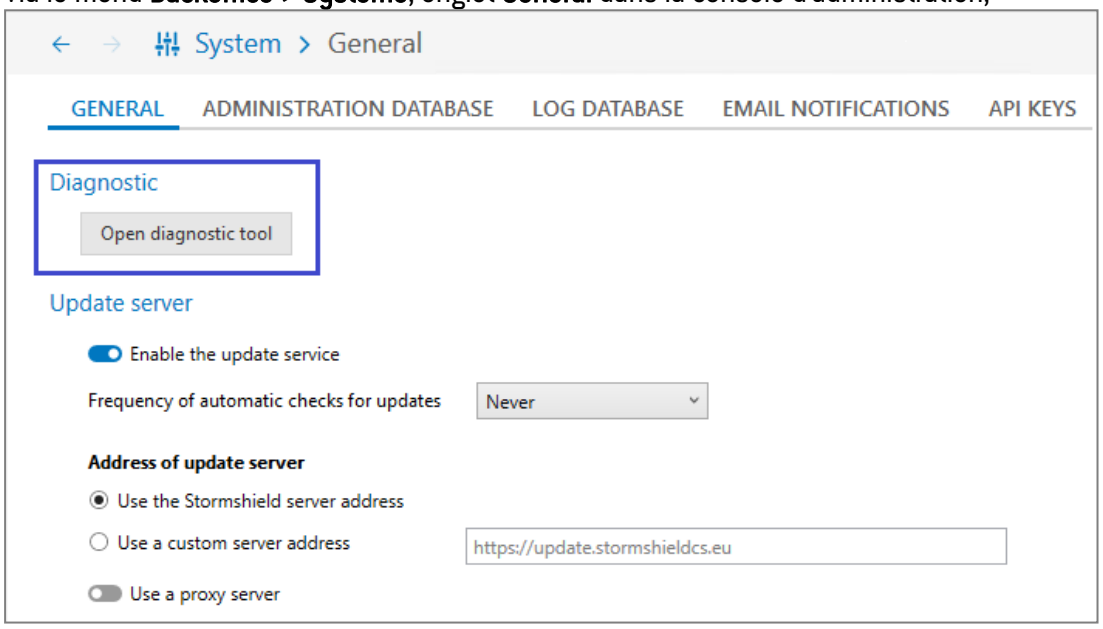
Ouvrir l'outil de diagnostic

En fonction des composants de SES Evolution installés sur le poste à analyser, vous pouvez ouvrir l'outil de diagnostic de quatre façons différentes :

- Via l'entrée **SES Evolution Diagnostic Tool** dans le menu **Démarrer** de Windows,



- Via le fichier exécutable *EsDiag.exe* dans le répertoire d'installation d'un composant,
- Via le menu **Backoffice > Système**, onglet **Général** dans la console d'administration,



- Via des options en ligne de commande.

Vous ne pouvez démarrer qu'une collecte de données à la fois par machine.

Utiliser l'outil de diagnostic via l'interface graphique

Vous avez ouvert l'outil de diagnostic selon l'une des trois premières façons proposées ci-dessus. Pour l'utiliser :

1. Sur l'écran d'accueil, cochez la case pour accepter que des données personnelles soient collectées.
2. Si un agent en version 2.4 ou supérieure est installé sur le poste, l'écran suivant propose de diagnostiquer l'agent et le backoffice, ou le backoffice seulement. La première option offre un périmètre de collecte plus complet. Dans ce cas, cliquez sur **Diagnostiquer depuis l'agent** pour ouvrir l'interface de l'agent. Vous devez avoir activé la collecte des données de diagnostic dans le groupe de l'agent auparavant, sinon vous devrez utiliser le mécanisme des challenges pour lancer le diagnostic depuis l'agent. Pour continuer la procédure, reportez-vous à la section Diagnostiquer les problèmes sur les agents
3. Si vous avez choisi de collecter les données du backoffice seulement, sur l'écran suivant, indiquez le dossier de destination et le nom du package de diagnostic. Ajoutez une description si nécessaire.

4. Cliquez sur **Démarrer**. L'outil collecte des données sur les composants backoffice et sur le système de la machine.
5. Pendant la collecte des données ou leur compression, si vous annulez, si vous fermez l'outil de diagnostic ou bien si vous fermez la session Windows, les données déjà collectées sont supprimées.
6. À la fin de la collecte, vous pouvez cocher **Ouvrir l'emplacement du fichier à la fermeture de l'outil** et fermer.

Utiliser l'outil de diagnostic via l'interface de ligne de commande

Vous avez également la possibilité d'utiliser les commandes suivantes pour utiliser l'outil de diagnostic :

`EsDiag /GenerateDiagnostic <path.zip> /AcknowledgePersonalDataCollection /DiagnosticComment <comment>`	Génère un package de diagnostic. Spécifiez le répertoire de destination du package. Le paramètre `/AcknowledgePersonalDataCollection` est obligatoire pour accepter que des données personnelles soient collectées. Le paramètre `/DiagnosticComment` est optionnel, il permet d'ajouter un commentaire.
`EsDiag /CancelDiagnostic`	Annule le diagnostic en cours.

17.2.2 Diagnostiquer les problèmes sur les agents

L'outil de diagnostic peut être démarré depuis l'interface des agents sur les postes des utilisateurs.

Il permet de collecter différentes données sur un poste sur lequel se présente un problème et de les rassembler dans un package de diagnostic (*.zip*) à fournir au Support technique de Stormshield pour l'analyse.

En complément des données de diagnostic, vous pouvez demander une prise de traces afin d'enregistrer une suite d'opérations exécutées par l'utilisateur et qui ont mené à un comportement inattendu de SES Evolution.

La prise de traces collecte les traces de debug émises par chaque module de l'agent.

Vous ne pouvez démarrer qu'une collecte de données à la fois par poste de travail.

Utiliser l'outil de diagnostic via l'interface graphique

Pour utiliser l'outil de diagnostic sur un poste utilisateur, demandez à l'utilisateur de réaliser les actions suivantes :

1. Double-cliquer sur l'icône  dans la barre des tâches pour ouvrir l'interface de l'agent.
2. Cliquer sur l'onglet  pour ouvrir le panneau **Aide et Support**.
3. Cliquer sur l'onglet **Diagnostic**.

4. Par défaut, vous devez utiliser le mécanisme des challenges pour autoriser l'utilisateur à lancer l'outil de diagnostic. Demandez-lui de générer un code de challenge dans l'onglet **Assistance** du panneau **Aide et Support**. Pour plus d'informations sur les challenges, reportez-vous à la section Résoudre les problèmes avec les challenges. La fonctionnalité **Challenges** doit être activée dans l'onglet **Paramètres** des groupes d'agents.
   Le contenu de l'onglet **Diagnostic** peut différer en fonction du paramétrage du groupe de l'agent et du statut Administrateur ou non de l'utilisateur. Pour en savoir plus, consultez les informations à la fin de cette procédure.

   > **NOTE**
   > Les droits d'administration ne sont pas nécessaires pour lancer un diagnostic via un challenge.

5. Si vous avez autorisé la prise de traces dans le challenge, demandez à l'utilisateur de commencer par cliquer sur **Démarrer la prise de traces**.
6. Demandez à l'utilisateur de reproduire le scénario ayant engendré le comportement anormal puis de cliquer sur **Suivant**.
7. L'utilisateur doit ensuite indiquer le dossier de destination et le nom du package de diagnostic. Il peut saisir une description si nécessaire.
8. L'utilisateur clique sur **Suivant**. L'outil collecte des données sur l'agent SES Evolution et sur le système de la machine. Pendant la collecte des données ou leur compression, si l'utilisateur annule, ferme l'outil de diagnostic ou bien ferme sa session Windows, les données déjà collectées sont supprimées.
9. À la fin de la collecte, l'utilisateur peut cocher **Ouvrir l'emplacement du fichier à la fermeture de l'outil** et fermer.
10. Demandez-lui de vous fournir le package de diagnostic *.zip* généré afin de le faire analyser par le Support technique Stormshield.

Pour les utilisateurs qui ont les droits d'administration sur leur poste de travail, l'option **Autoriser la collecte de données de diagnostic** dans l'onglet **Paramètres** des groupes d'agents leur permet de démarrer directement un diagnostic depuis l'agent, sans passer par un challenge. Pour plus d'informations, reportez-vous à la section Collecter les données de diagnostic.

Dans le cas où la fonctionnalité des challenges serait désactivée dans l'onglet **Paramètres** des groupes d'agents et où la collecte des données serait autorisée dans les groupes d'agents également, les utilisateurs non administrateurs de leur poste peuvent demander une élévation de privilèges pour démarrer un diagnostic depuis l'agent.

Utiliser l'outil de diagnostic via l'interface de ligne de commande

Vous avez également la possibilité d'établir un diagnostic sur un poste utilisateur via un script, en lançant le programme EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) avec les options de ligne de commande suivantes. Les droits d'administration sont nécessaires et la collecte des données de diagnostic doit être activée dans le groupe de l'agent.

`EsGui /GenerateDiagnostic <path.zip> /AcknowledgePersonalDataCollection /DiagnosticComment <comment>`	Génère un package de diagnostic sans prise de traces. Spécifiez le répertoire de destination du package. Le paramètre `/AcknowledgePersonalDataCollection` est obligatoire pour accepter que des données personnelles soient collectées. Le paramètre `/DiagnosticComment` est optionnel, il permet d'ajouter un commentaire.
`EsGui /StartDiagnosticWithTraces /AcknowledgePersonalDataCollection`	Démarre un diagnostic et la prise de traces.
`EsGui /StopDiagnosticWithTraces <path.zip> /DiagnosticComment <comment>`	Arrête la prise de traces et termine la génération du package de diagnostic. Spécifiez l'emplacement pour enregistrer le package.
`EsGui /CancelDiagnostic`	Annule le diagnostic en cours.

Pour des informations sur EsGui, reportez-vous à la section Utiliser la commande EsGui.

18. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur SES Evolution sont disponibles sur le site web Documentation et dans la base de connaissances Stormshield (authentification nécessaire).

Annexe A. Connaître les fonctions OSSEC supportées

Il existe quelques différences entre le moteur d'analyse SES Evolution et OSSEC, notamment concernant les éléments de configuration supportés. Cette annexe indique pour chaque élément OSSEC de décodeur et de règle s'il est supporté ou non par SES Evolution.

Pour plus d'informations sur l'utilisation du moteur d'analyse, reportez-vous à la section Importer des règles de sécurité OSSEC

A.1 Éléments des fichiers de décodeurs

Éléments de décodeur supportés

Élément de configuration	Remarques
`<decoder name="...">`	Le nom du décodeur est obligatoire.
`<decoder name="..."><parent>...</parent></decoder>`	Permet de relier le décodeur à un décodeur de niveau supérieur. **NOTE** SES Evolution permet plus de deux étages de décodeurs.
`<decoder name="..."><prematch>...</prematch></decoder>`	Expression régulière OSSEC avancée permettant de vérifier rapidement si le décodeur convient au message de log.
`<decoder name="..."><prematch_pcre2>...</prematch_pcre2></decoder>`	Expression régulière PCRE2 permettant de vérifier rapidement si le décodeur convient au message de log.
`<decoder name="..."><program_name>...</program_name></decoder>`	Expression régulière OSSEC simple portant sur le champ *program_name* extrait en phase de prédécodage, permettant de vérifier rapidement si le décodeur convient au message de log.
`<decoder name="..."><program_name_pcre2>...</program_name_pcre2></decoder>`	Expression régulière PCRE2 portant sur le champ *program_name* extrait en phase de prédécodage, permettant de vérifier rapidement si le décodeur convient au message de log.
`<decoder name="..."><regex>...</regex><order>...</order></decoder>`	Extraction de champs depuis le log à l'aide d'une expression régulière OSSEC avancé avec groupes de capture. SES Evolution permet d'extraire vers tout nom de champ.
`<decoder name="..."><pcre2>...</pcre2><order>...</order></decoder>`	Extraction de champs depuis le log à l'aide d'une expression régulière PCRE2 avec groupes de capture. SES Evolution permet d'extraire vers tout nom de champ.

<decoder name="..."> <use_own_name>...</use_own_name> </decoder>	Permet d'écrire par la suite des règles portant sur le nom de ce décodeur lorsqu'il n'est pas au 1er étage. SES Evolution ignore cette option mais supporte les décodeurs de tous niveaux dans l'option *decoded_as* des règles.
<decoder name="..."> <type>...</type> </decoder>	Permet de classifier le décodeur. Les valeurs supportées sont : *firewall, ids, web-log, syslog, squid, windows, host-information* et *OSSEC*. Les sept premières règles obligatoires (dans *rules_config.xml*) correspondent à tous ces types sauf *host-information*.
<decoder name="..."> <fts>...</fts> </decoder>	Permet de stocker des *n-uplets* de champs dans un cache afin de voir si leurs valeurs ont déjà été observées ensemble.

Éléments de décodeur non supportés

Élément de configuration	Remarques
<decoder status="...">	OSSEC contient du code pour lire ce champ mais toute configuration le contenant est invalide.
<decoder id="...">	OSSEC contient du code pour lire ce champ mais n'utilise pas sa valeur.
<decoder type="...">	OSSEC contient du code pour lire ce champ mais n'utilise pas sa valeur.
<decoder name="..."> <plugin_decoder>...</plugin_decoder> </decoder>	Permet de compiler ses propres décodeurs pour des besoins spécifiques.
<decoder name="..."> <accumulate/> </decoder>	Support des logs sur plusieurs lignes avec des champs communs.

A.2 Éléments des fichiers de règles

Éléments de règles supportés

Élément de configuration	Remarques
<var name="FREQ">8</var> ... <group name="..."> <rule ... frequency="$FREQ"> ...	Déclaration de constantes en haut de fichier.
<group name="..."> <rule ...> ... </rule> </group>	Les éléments <rule> doivent être sous un élément <group>. L'attribut *name* est obligatoire et se termine par une virgule. Sert à classifier les règles se trouvant dans le groupe.
<rule id="123456">	L'attribut *id* d'une règle est obligatoire, compris entre 1 et 999999.

<rule **overwrite**="yes|no">	Permet de s'affranchir de l'unicité de l'attribut *id* ; remplace une règle précédemment définie.
<rule **level**="0..15">	Obligatoire. Associe un niveau de gravité à la règle ; les règles de niveau 0 sont évaluées en priorité sur les autres.
<rule **accuracy="0"**>	Permet de rendre toutes les règles dotées de cet attribut moins prioritaires que les autres.
<rule **maxsize**="0..9999">	Permet à la règle de ne s'appliquer qu'à des logs dont le message a une longueur au moins égale à la valeur de cet attribut.
<rule **timeframe**="..." **frequency**="...">	Déclare une règle composite, se déclenchant si un événement survient plusieurs fois dans un laps de temps donné.
<rule **noalert**="...">	Considère qu'une règle n'est pas applicable si aucune règle enfant ne l'est.
<rule **ignore**="...">	Inhibe la règle pendant un certain nombre de secondes après un déclenchement.
<rule id="..." level="..."> <**decoded_as**>...</**decoded_as**> </rule>	Indique le décodeur de 1er niveau (ou de 2d niveau utilisant l'option *use_own_name*) qui doit avoir été utilisé pour le message. SES Evolution supporte les noms de décodeurs de tous les niveaux et ignore l'option *use_own_name*.
<rule id="..." level="..."> <**if_sid**>...</**if_sid**> </rule>	Relie une règle à une règle parente par ID de règle.
<rule id="..." level="..."> <**if_group**>...</**if_group**> </rule>	Relie une règle à des règles parentes par nom de groupe.
<rule id="..." level="..."> <**if_level**>...</**if_level**> </rule>	Relie une règle à des règles parentes par niveau de gravité minimal.
<rule id="..." level="..."> <**regex**>...</**regex**> </rule> <rule id="..." level="..."> <**match**>...</**match**> </rule> <rule id="..." level="..."> <**pcre2**>...</**pcre2**> </rule> <rule id="..." level="..."> <**match_pcre2**>...</**match_pcre2**> </rule>	Expression régulière OSSEC simple/avancée/PCRE2/PCRE2 portant sur le message de log, afin de déterminer si la règle correspond. **NOTE** Les deux dernières variantes sont synonymes.

<rule id="..." level="..."> <user>...</user> </rule> <rule id="..." level="..."> <user_pcre2>...</user_pcre2> </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *srcuser*, ou, à défaut, sur le champ décodé *dstuser*, afin de déterminer si la règle correspond.
<rule id="..." level="..."> <srcip>...</srcip> </rule> <rule id="..." level="..."> <dstip>...</dstip> </rule>	Spécification d'adresses IPv4 ou IPv6 (adresses individuelles, plages, réseau avec longueur de masque) comparées aux champs *srcip* ou *dstip* afin de déterminer si la règle correspond. Il est possible de mettre une spécification en négatif en la préfixant par un point d'exclamation.
<rule id="..." level="..."> <srcport>...</srcport> </rule> <rule id="..." level="..."> <srcport_pcre2>...</srcport_pcre2> </rule> <rule id="..." level="..."> <dstport>...</dstport> </rule> <rule id="..." level="..."> <dstport_pcre2>...</dstport_pcre2> </rule>	Expressions régulières OSSEC simple/PCRE2 portant sur les champs décodés *srcport* et *dstport* afin de déterminer si la règle correspond.
<rule id="..." level="..."> <id>...</id> </rule> <rule id="..." level="..."> <id_pcre2>...</id_pcre2> </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *id* afin de déterminer si la règle correspond.
<rule id="..." level="..."> <status>...</status> </rule> <rule id="..." level="..."> <status_pcre2>...</status_pcre2> </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *status* afin de déterminer si la règle correspond.
<rule id="..." level="..."> <hostname>...</hostname> </rule> <rule id="..." level="..."> <hostname_pcre2>...</hostname_pcre2> </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ (pré)décodé *hostname* afin de déterminer si la règle correspond.
<rule id="..." level="..."> <extra_data>...</extra_data> </rule> <rule id="..." level="..."> <extra_data_pcre2>...</extra_data_pcre2> </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *data* afin de déterminer si la règle correspond.

<rule id="..." level="..."> **<program_name>**...**</program_name>** </rule> <rule id="..." level="..."> **<program_name_pcre2>**...**</program_name_pcre2>** </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ (pré)décodé *program_name* afin de déterminer si la règle correspond.
<rule id="..." level="..."> **<url>**...**</url>** </rule> <rule id="..." level="..."> **<url_pcre2>**...**</url_pcre2>** </rule>	Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *url* afin de déterminer si la règle correspond.
<rule id="..." level="..."> **<action>**...**</action>** </rule>	Valeur exacte comparée avec le champ décodé *action* afin de déterminer si la règle correspond.
<rule id="..." level="..."> **<field name="...">**...**</field>** </rule>	Expression régulière OSSEC avancée portant sur le champ décodé nommé, afin de déterminer si la règle correspond.
<rule id="..." level="..."> **<time>**...**</time>** </rule>	Spécifie une plage horaire d'applicabilité de la règle. Les formats supportés par OSSEC sont supportés. **EXEMPLE** <time>1:30-17:45</time> ; <time>1 am - 12:30 PM</time> ; <time>!08:00-17:30</time> SES Evolution utilise le fuseau horaire du système pour évaluer l'heure locale.
<rule id="..." level="..."> **<weekday>**...**</weekday>** </rule>	Spécifie des jours de la semaine d'activation de la règle. Les formats supportés par OSSEC sont supportés. **EXEMPLE** <weekday>wed fri sun</weekday> ; <weekday>weekdays sunday</weekday> ; <weekday>! tue wed</weekday> SES Evolution utilise le fuseau horaire du système pour évaluer l'heure locale (et donc le jour).
<rule id="..." level="..."> **<cve>**...**</cve>** </rule> <rule id="..." level="..."> **<info type="cve">**...**</info>** </rule>	Décrit la règle en l'associant à une vulnérabilité connue.

<rule id="..." level="..."> <info type="text">...</info> </rule> <rule id="..." level="..."> <info type="link">...</info> </rule> <rule id="..." level="..."> <info type="osvdb">...</info> </rule>	Décrit la règle à l'aide d'un texte, un lien ou un item Open Source Vulnerability Database. SES Evolution ne supporte qu'un seul item de chaque type pour une même règle.
<rule id="..." level="..."> <group>...</group> </rule>	Ajoute des groupes d'appartenance à la règle en plus de ceux spécifiés dans le nœud <group> parent de la règle.
<rule id="..." level="..."> <description>...</description> </rule>	Description obligatoire de l'événement caractérisé par la règle. SES Evolution utilise cette description dans le résumé de log affiché sur l'agent et la console.
<rule id="..." level="..."> <category>...</category> </rule>	Relie la règle à un des types de décodeurs. Option utilisée pour les règles 1 à 7 dans le fichier *rules_config.xml*.
<rule id="..." level="..."> <if_fts/> </rule>	Rend la règle opérante uniquement si un décodeur a détecté (avec option fts) qu'un ensemble de champs portait des valeurs vues ensemble pour la première fois.
<rule id="..." level="..."> <ignore>...</ignore> </rule> <rule id="..." level="..."> <check_if_ignored>...</check_if_ignored> </rule>	Permet de mettre des ensembles de valeurs de champs dans un cache, puis qu'une autre règle, par la suite, soit désactivée pour les mêmes ensembles de valeurs.
<rule id="..." level="..."> <check_diff/> </rule>	Permet d'ignorer deux logs identiques successifs.
<rule id="..." level="..." frequency="..." timeframe="..."> <if_matched_regex>...</if_matched_regex> </rule>	Permet à une règle composite de se déclencher si plusieurs logs émis récemment peuvent être caractérisés par une expression régulière OSSEC avancée.
<rule id="..." level="..." frequency="..." timeframe="..."> <if_matched_group>...</if_matched_group> </rule>	Permet à une règle composite de se déclencher si plusieurs logs émis récemment ont été caractérisés par une règle dans un groupe donné.
<rule id="..." level="..." frequency="..." timeframe="..."> <if_matched_sid>...</if_matched_sid> </rule>	Permet à une règle composite de se déclencher si plusieurs logs émis récemment ont été caractérisés par une règle ayant un identifiant donné.

<rule id="..." level="..." frequency="..." timeframe="..."> same_source_ip </rule> <rule id="..." level="..." frequency="..." timeframe="..."> same_src_port </rule> <rule id="..." level="..." frequency="..." timeframe="..."> same_dst_port </rule> <rule id="..." level="..." frequency="..." timeframe="..."> same_id </rule> <rule id="..." level="..." frequency="..." timeframe="..."> same_user </rule>	Permet à une règle composite de se déclencher si l'on trouve plusieurs logs partageant le même champ *srcip*, *srcport*, *dstport*, *id* ou *user*.
<rule id="..." level="..." frequency="..." timeframe="..."> different_srcip </rule> <rule id="..." level="..." frequency="..." timeframe="..."> different_url </rule>	Permet à une règle composite de se déclencher si l'on trouve plusieurs logs ayant des valeurs distinctes pour le même champ *srcip*, *url*.

Éléments de règles non supportés

Élément de configuration	Supporté	Remarques
<rule id="..." level="..."> srcgeoip...</srcgeoip> </rule> <rule id="..." level="..."> srcgeoip_pcre2...</srcgeoip_pcre2> </rule> <rule id="..." level="..."> dstgeoip...</dstgeoip> </rule> <rule id="..." level="..."> dstgeoip_pcre2...</dstgeoip_pcre2> </rule>	Non	SES Evolution n'utilise pas la bibliothèque *libgeoip*.
<rule id="..." level="..."> list lookup="..." field="...">...</list> </rule>	Non	Recherche rapide d'un champ dans une base de données au format CDB. SES Evolution n'utilise pas la bibliothèque CDB.

<rule id="..." level="..."> <**compiled_rule**>...</**compiled_rule**> </rule>	Partiel	Permet de compiler ses propres règles pour des besoins spécifiques. SES Evolution supporte la fonction *is_simple_http_request* qui sert d'exemple mais est utilisée dans les jeux de règles standard.
<rule id="..." level="..."> <**options**>...</**options**> </rule>	Partiel	SES Evolution supporte uniquement l'option *no_log* ; les alertes par e-mail ou réponses actives ne sont pas supportées
<rule id="..." level="..." frequency="..." timeframe="..."> <**not_same_source_ip**/> </rule> <rule id="..." level="..." frequency="..." timeframe="..."> <**not_same_id**/> </rule> <rule id="..." level="..." frequency="..." timeframe="..."> <**not_same_user**/> </rule>	Non	Options OSSEC inutiles dans le cadre d'une configuration ayant pour seul effet d'annuler une option <*same_...*> précédemment écrite dans la même règle : il est conseillé d'enlever l'option précédente.
<rule id="..." level="..." frequency="..." timeframe="..."> <**same_location**/> </rule> <rule id="..." level="..." frequency="..." timeframe="..."> <**not_same_agent**/> </rule>	Non	SES Evolution effectue l'analyse et la corrélation de logs au niveau de l'agent et non au niveau du serveur. En conséquence il n'est pas possible de corréler des logs d'agents multiples ; ces options sont donc ignorées.
<rule id="..." level="..." frequency="..." timeframe="..."> <**different_srcgeoip**/> </rule>	Non	SES Evolution n'utilise pas la bibliothèque *libgeoip*.

documentation@stormshield.eu