STORMSHIELD ENDPOINT SECURITY EVOLUTION

NOTES DE VERSION

Version 2

Dernière mise à jour du document : 20 décembre 2021

Référence : ses-fr-notes_de_version-v2.1.2

Table des matières

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

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Vulnérabilités résolues de SES Evolution 2.1.2

Backend

Une vulnérabilité de sévérité élevée a été corrigée. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-070/.

Console d'administration

Une vulnérabilité de sévérité moyenne a été corrigée. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-071/.

Logs

Une vulnérabilité de sévérité faible a été corrigée. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-072/.

Versions de Microsoft Windows compatibles

SES Evolution version 2 est compatible avec les versions de Microsoft Windows suivantes. Pour plus d'informations, reportez-vous à la section Prérequis système pour SES Evolution du *Guide d'installation*.

Console d'administration
Windows 7 - 32 et 64 bits
Windows 8.1 update - Août 2014 - 32 et 64 bits
Windows 10 Enterprise 2015 LTSB – 32 et 64 bits Windows 10 Enterprise 2016 LTSB – 32 et 64 bits Windows 10 1809 – 32 et 64 bits Windows 10 1909 – 32 et 64 bits Windows 10 20H2 – 32 et 64 bits Windows 10 21H1 – 32 et 64 bits Windows 10 21H2 – 32 et 64 bits
Windows Server 2008 R2
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Backend
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Gestionnaire d'agents
Windows 10 Enterprise 2015 LTSB – 64 bits Windows 10 Enterprise 2016 LTSB – 64 bits Windows 10 1809 – 64 bits Windows 10 1909 – 64 bits Windows 10 20H2 – 64 bits Windows 10 21H1 – 64 bits Windows 10 21H2 – 64 bits
Windows Server 2008 R2*
Windows Server 2012 R2*
Windows Server 2016
Windows Server 2019

* Sur ces systèmes d'exploitation fraîchement installés, l'installation préalable du framework .NET 4.6.2 est nécessaire pour que le Centre d'installation SES Evolution fonctionne.

Agent
Windows 7 - 32 et 64 bits
Windows 8.1 mise à jour 3 (août 2014) - 32 bits ou 64 bits
Windows 10 Enterprise 2015 LTSB – 32 et 64 bits Windows 10 Enterprise 2016 LTSB – 32 et 64 bits Windows 10 1809 – 32 et 64 bits Windows 10 1909 – 32 et 64 bits Windows 10 20H2 – 32 et 64 bits Windows 10 21H1 – 32 et 64 bits Windows 10 21H2 – 32 et 64 bits
Windows Server 2008 R2
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Préconisations

Avant de mettre à jour un environnement existant vers la version 2.1 de SES Evolution, vous devez :

- Lire attentivement la section **Problèmes connus** de la Base de connaissance Stormshield (anglais uniquement - identifiants identiques à ceux de votre espace client MyStormshield),
- Lire attentivement la section Précisions sur les cas d'utilisation.

Mise à jour des politiques de sécurité intégrées

Lors de la mise à jour de SES Evolution 2.0.x à 2.1, les politiques de sécurité intégrées et les jeux de règles intégrés sont mis à jour également.

Les politiques mises à jour n'écrasent pas vos politiques intégrées existantes. Ces dernières sont renommées avec le suffixe *(Before update)*. Si vous utilisez des politiques intégrées et que voulez leur faire bénéficier des améliorations de la mise à jour, deux options s'offrent à vous :

Si vous avez conservé les politiques initiales sans les modifier :

1. Changez la politique dans la configuration des groupes d'agents concernés afin de choisir la nouvelle politique mise à jour, i.e., celle qui ne contient pas le suffixe *(Before update)*.
2. Supprimez vos anciennes politiques *(Before update)*.

Si vous avez personnalisé les politiques intégrées :

1. Reportez vos modifications dans les nouvelles politiques.
2. Changez la politique dans la configuration des groupes d'agents concernés afin de choisir la nouvelle politique mise à jour, i.e., celle qui ne contient pas le suffixe *(Before update)*.
3. Supprimez vos anciennes politiques *(Before update)*.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SES Evolution est consultable sur la Base de connaissance Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissance, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Précisions sur les cas d'utilisation

Installation de la solution SES Evolution

Si une mise à jour Windows est en cours lors d'une installation complète du serveur SES Evolution ou du composant backend, l'installation échoue. Il est recommandé de désactiver les mises à jour Windows avant d'installer SES Evolution et de les réactiver ensuite.

Périphériques Bluetooth Low Energy

Les périphériques Bluetooth Low Energy ne sont pas filtrés par l'agent SES Evolution : seuls les périphériques Bluetooth standard sont reconnus.

Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de Documentation Technique Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Guide d'installation
- Guide d'administration

Merci de consulter la Base de connaissances (anglais uniquement) pour des informations techniques spécifiques.

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 2.1.2 de Stormshield Endpoint Security Evolution :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Endpoint Security Evolution :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur votre espace personnel l'espace client MyStormshield, rubrique **Téléchargements**.

Versions précédentes de SES Evolution v2

Retrouvez dans cette section les nouvelles fonctionnalités et correctifs des versions précédentes de SES Evolution v2.

2.1.1			Correctifs
2.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
2.0.2			Correctifs
2.0.1		Vulnérabilités résolues	Correctifs
2.0.0	Nouvelles fonctionnalités		

Correctifs de SES Evolution 2.1.1

Installation

Références support : SESNG-7486

Vous pouvez désormais relancer une mise à jour via le Centre d'installation si celle-ci a été précédemment annulée.

Références support : SESNG-7842

Le Centre d'installation vérifie désormais correctement le mot de passe du backend.

Politique par défaut Stormshield

Références support : SESNG-7714

La protection keylogging ne bloque plus la saisie du coffre-fort de mots de passe Keepass.

Références support : SESNG-7865

Les règles Wi-Fi initialement présentes dans le jeu de règles *Socle de protection* ont été externalisées dans un jeu de règles indépendant non inclus par défaut dans les politiques. Cela permet de séparer politique de sécurité logicielle et politique d'utilisation de composants matériels. De plus, les règles Wi-Fi et de périphériques généraux ne génèrent plus systématiquement un incident.

Références support : SESNG-8105

L'ajout d'un nouveau certificat racine utilisé par Google Chrome permet de nouveau de démarrer ce navigateur lorsqu'un utilisateur clique sur un lien hypertexte d'e-mail depuis Microsoft Outlook.

Références support : SESNG-8399

Le mode d'identification de SQL Server VSS Writer a changé. Celui-ci n'est désormais plus bloqué lorsqu'il écrit des informations dans le registre concernant les Shadow Copies.

Références support : SESNG-8444

Les applications Microsoft Office qui écrivent des fichiers d'extension *.js* ne provoquent plus d'alertes.

Afin de limiter les faux positifs, certaines règles d'heuristique de détection des malware voleurs de mots de passe ont été retirées de la politique, et deux programmes Microsoft connus pour faire des accès aux volume en raw ont été ajoutés à la politique.

Jeux de règles

Références support : SESNG-8335

Dans le panneau d'un jeu de règles, les liens vers les politiques sont désormais conservés lorsque l'action **Tout mettre à jour** est utilisée.

Règles de protection

Références support : SESNG-8345

Dans les règles fichiers ou les identifiants d'applications, il était possible de saisir certains chemins de fichiers erronés. Désormais un contrôle est effectué.

Règles OSSEC

Références support : SESNG-8345

Certains chemins de fichiers à surveiller dans les règles OSSEC empêchaient l'application de la politique. Ce problème est corrigé.

Logs

Références support : 183722CW

Les règles créées lors de l'ajout d'une exception depuis un log sont désormais correctement configurées.

Références support : 167478PW

SES Evolution ne génère plus d'erreurs lorsque les logs de contexte sont très nombreux.

Agent SES Evolution

Références support : 184781CW

L'export des événements sur l'interface de l'agent SES Evolution ne provoque plus l'affichage d'une liste d'erreurs techniques.

Nouvelles fonctionnalités de SES Evolution 2.1

Nouvelles protections

Protections avancées

Des protections avancées permettent de protéger votre parc contre des opérations malveillantes telles que le vol d'informations d'authentification, l'usage malveillant d'outils Windows, l'usage de techniques de persistance, etc.

En savoir plus

Nouvelle politique intégrée : Protection des composants backoffice

Une politique de sécurité intégrée est désormais fournie pour renforcer la sécurité des composants backoffice SES Evolution. Cette politique doit être appliquée aux groupes d'agents contenant les gestionnaires d'agents, backend et console d'administration.
Elle reprend les sécurités de la politique par défaut et apporte plusieurs jeux de règles modulaires, chacun correspondant à un composant backoffice. Elle est constituée des jeux de règles suivants :

- Audit pour contextes d'attaque,
- Protection du backend (Nouveau),
- Protection du gestionnaire d'agents (Nouveau),
- Protection de la console d'administration (Nouveau),
- Protections avancées (Nouveau),
- Socle de protections.

En savoir plus

Modification des politiques existantes

La Politique par défaut a été enrichie avec de nouveaux jeux règles portant des protections avancées et une protection contre le vol d'informations sensibles.

Elle se compose désormais des jeux de règles suivants :

- Audit pour contextes d'attaque,
- Protections avancées (Nouveau),
- Prévention de fuite d'information (Nouveau),
- Socle de protections.

Lors d'une mise à jour de SES Evolution 2.0.x vers la version 2.1, consultez les Préconisations pour connaître le marche à suivre concernant la mise à jour des politiques.

Nouveaux jeux de règles intégrés

Les jeux de règles suivants ont été ajoutés :

Protection du backend	Protection du serveur applicatif IIS (programmes, paramétrage, injection), de la base de données et du centre d'installation de SES Evolution.
Protection du gestionnaire d'agents	Protection du gestionnaire d'agents (programmes, paramétrage, injection) et du centre d'installation de SES Evolution.

Protection de la console d'administration	Protection de la console d'administration SES Evolution (programme, paramétrage, injection, keylogging) et du centre d'installation de SES Evolution.
Protections avancées	Par opposition aux protections réagissant à la présence d'un événement unitaire fort, les protections avancées réagissent à la présence de plusieurs événements faibles mais qui combinés représentent une menace.
Prévention de fuite d'informations	Protection de certaines applications spécifiques communément utilisées dans les entreprises (navigateurs Web, outils de transfert de fichier, coffres forts, autorité de sécurité Windows et outils de contrôle à distance). Cette protection couvre les accès non autorisés aux fichiers, emplacements registre et tentatives d'enregistrement des frappes clavier pour contrer un vol de données sensibles. L'autorité de sécurité Windows est également protégée contre les accès inter-processus, ce qui bloque l'extraction de mots de passe Windows. Une attention particulière a été portée aux programmes permettant d'exécuter du code extérieur (moteurs de script, chargeurs de DLL, ...) afin que leurs actions soient systématiquement bloquées. De même, les programmes fournis par défaut avec Windows (LOLBIN) qui permettent indirectement d'accéder à de l'information sont bloqués.
Transfert des événements de Windows Defender	Consolidation dans la console d'administration des alertes de sécurité intéressantes émises par Windows Defender sur les postes de travail protégés du parc SES Evolution. Il n'est pas inclus dans les politiques intégrées, et vous devez donc l'ajouter manuellement dans vos politiques.

Modification des jeux de règles existants

Les jeux de règles suivants ont été modifiés :

Audits pour contextes d'attaques	• Les actions des programmes permettant d'exécuter du code extérieur (moteurs de script, chargeurs de DLL, ...) sont maintenant systématiquement tracées, même s'ils sont signés. • La liste des certificats reconnus par le jeu de règles a été enrichie. • Le niveau de sévérité des règles a été revu pour qu'aucune ne se trouve en dessous du seuil par défaut du groupe d'agent (niveau *Remarque* au plus faible). • La détection avancée d'ARP Spoofing a été ajoutée dans ce jeu de règles afin de détecter des tentatives d'interception de données "*Man In The Middle*. • Optimisation afin de minimiser son empreinte en termes de performances sur le système sans perdre en qualité d'audit. Cela aura aussi pour rôle de réduire les éventuelles pertes de logs en cas d'activité intensive.

Socle de protections	Ce jeu de règles a été enrichi et durci : • Blocage sur les changements de paramétrage du mode sans échec, • Protection de la base BCD (Boot Configuration Data), • Enrichissement des applications reconnues comme outils de piratage, • Blocage de démarrage des moteurs de scripts depuis les navigateurs, • Protection des fichiers de configuration système (hosts, services et network) contre les modifications indésirables, • Contrôle avec blocage de démarrage de programmes tiers depuis les applications MS-Office, • Amélioration de l'heuristique de détection de programmes malveillants de type vol de données basée sur le nom du fichier accédé, • Contrôles bloquant le démarrage des services non signés.

Gestion des agents

Groupes d'agents selon les critères Active Directory

Les agents peuvent être placés automatiquement dans un groupe d'agents en fonction des groupes Active Directory ou des unités d'organisation auxquels ils appartiennent. Cette fonctionnalité permet de gagner du temps et de réduire les risques d'erreur lors de la constitution des groupes d'agents.

En savoir plus

Désinstallation des agents

Vous pouvez désormais empêcher l'administrateur local d'un poste de travail de désinstaller l'agent SES Evolution. Dans ce cas, la désinstallation reste possible via un challenge.

En savoir plus

Filtrage des agents

De nouveaux filtres permettent d'afficher la liste des agents en fonction de critères tels que le système d'exploitation, l'état, la politique de sécurité, etc.

En savoir plus

Tableau de bord

Un nouveau diagramme est présent sur le tableau de bord de la console d'administration et affiche le nombre d'agents dans le parc pour chaque version de SES Evolution.

En savoir plus

Base de données

Rétention des logs dans la base de données

La durée de rétention des logs dans la base de données de logs est paramétrable, soit à l'installation de SES Evolution, soit à tout moment via le nouveau menu **Système** de la console d'administration. Les logs qui atteignent la fin de leur durée de rétention sont supprimés par une tâche s'exécutant régulièrement.

En savoir plus

Version des politiques et jeux de règles

La gestion des versions des politiques et jeux de règles a été améliorée afin d'optimiser l'espace de stockage de la base de données d'administration.

En savoir plus

Périphériques

Dans la console d'administration, la liste des périphériques USB connus (vendeur et produit) a été mise à jour.

Surveillance de l'activité

Suivi d'événements Windows

Les événements Windows de votre choix peuvent être transférés à SES Evolution permettant d'afficher des informations de sécurité concernant votre environnement.

En savoir plus

Enregistrement de l'activité des utilisateurs

L'activité des utilisateurs de la console d'administration SES Evolution est désormais tracée à travers un audit complet des actions effectuées.

En savoir plus

Logs des composants backoffice

Un nouveau menu de la console d'administration, **Logs système**, affiche l'activité des gestionnaires d'agents, des serveurs backend, et de la console d'administration de SES Evolution.

En savoir plus

Moteur d'analyse OSSEC

Il est maintenant possible d'importer des règles OSSEC dans une politique de sécurité depuis la console d'administration. Cela permet aux agents de s'abonner à des journaux de logs textuels ou à des événements Windows et de les remonter comme des logs SES Evolution dans la base de données de logs ou un SIEM.

En savoir plus

Export vers des serveurs Syslog

L'export des logs est désormais possible vers plusieurs serveurs Syslog et les formats d'export IDMEF et CEF ont été ajoutés pour une meilleure intégration à vos outils.

En savoir plus

Vulnérabilités résolues de SES Evolution 2.1

Agent

Chargement de DLL

Une vulnérabilité pouvait provoquer le chargement par certains processus de l'agent, de DLL situées ailleurs que dans les dossiers d'installation de l'agent. Cette vulnérabilité a été corrigée.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Backend

Accès aux scripts personnalisés

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Modification de scripts inutilisés

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Suppression de scripts inutilisés

Une vulnérabilité de niveau faible a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Suppression d'identifiants d'applications

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Modification de politiques de sécurité

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Duplication de politiques de sécurité

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant Backend de SES Evolution.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Correctifs de SES Evolution 2.1

Installation

Dans le Centre d'installation, l'*Installation minimale* a été renommée *Installation de démonstration* afin de signaler qu'elle ne doit pas être utilisée dans un environnement de production mais uniquement à des fins de test ou de démonstration. l'*Installation avancée* a été renommée *Installation standard*.

Références support : SESNG-6898

Le Centre d'installation ne s'arrête plus de manière inopinée lorsque l'utilisateur SQL n'est pas connu. Dorénavant un message explicite informe l'utilisateur de ce problème.

Références support : 182618CW

La langue du Centre d'installation correspond maintenant à celle du système d'exploitation pour le français, l'anglais, l'espagnol et l'allemand. Pour les autres langues, le Centre d'installation est en anglais.

Agent SES Evolution

Références support : 183130CW

Dans certain cas, lors du démarrage de la machine, l'agent SES Evolutiondétectait à tort un problème d'intégrité qui nécessitait un redémarrage. Ce problème est résolu.

Références support : SESNG-7184

Un problème de compatibilité entre l'agent SES Evolution et l'application CCleaner a été corrigé.

Références support : SESNG-5426

Un écran bleu (BSOD) pouvait survenir lors de la mise en veille de la machine. Ce problème a été corrigé.

Règles de sécurité

Références support : 181886CW

Il est désormais possible de créer une règle d'exception à partir d'un log contenant un chemin UNC.

Références support : 182180CW

Il est désormais possible de copier/couper et coller des règles au sein d'un même jeu de règles.

Références support : SESNG-5365

La Protection contre la dissimulation de processus (Process hollowing) a été améliorée.

Références support : SESNG-7226

Les règles de la menace *Élévation de privilèges* dans un jeu de règles d'audit n'empêchent plus l'évaluation des règles présentes dans les jeux de règles suivants.

Références support : SESNG-5295

L'action *Détecter seulement* n'est plus proposée pour les règles de protection contre les enregistreurs de frappe. Elle était redondante avec le mode *Règle passive*.

Références support : SESNG-5370

Il est désormais possible de bloquer tous les accès fichier entrants par le réseau via des règles de contrôle d'accès aux fichiers.

Références support : SESNG-6878

Désormais, un message vous alerte si vous créez un identifiant dont le chemin se termine par un ou plusieurs caractère espace.

Logs

Références support : 182073CW

Dans la console d'administration, le graphique d'attaque des incidents s'affiche désormais correctement lorsqu'il contient des logs wifi.

Références support : SESNG-6372

Dans la console d'administration, les filtres d'exclusion des logs agents ne fonctionnaient pas toujours. Ce problème est résolu.

Références support : 183960CW

Lorsqu'un utilisateur est supprimé, il n'apparaît désormais plus dans la liste des utilisateurs dans l'édition des logs.

Contrôle des périphériques

Références support : SESNG-5580

Dans certains cas, le branchement d'un périphérique USB n'affichait pas de message d'autorisation sur l'agent, alors même que la règle de contrôle d'accès aux périphériques USB l'exigeait. Ce problème a été corrigé.

Tableau de bord

Références support : SESNG-5780

Lorsque l'environnement SES Evolution contient plusieurs gestionnaires d'agents, leur statut est désormais correctement affiché sur le tableau de bord de la console d'administration.

Gestion des agents

Références support : SESNG-5505

Il n'est désormais plus possible de créer un groupe d'agents avec des paramètres invalides.

Références support : SESNG-6910

L'état des agents arrêtés est désormais correctement affiché dans la page **Agents** de la console d'administration.

Références support : SESNG-7391

Le système d'exploitation Windows 10 21H1 est désormais correctement affiché dans la page **Agents** de la console d'administration.

Compatibilité avec les autres firewalls

Références support : SESNG-5309

La compatibilité avec les autres firewalls a été améliorée.

Correctifs de SES Evolution 2.0.2

Mise à jour de SES Evolution

Nouvelle version des politiques

Lors d'une mise à jour de SES Evolution, les politiques de sécurité Stormshield sont désormais mises à jour.

Console d'administration ouverte

Dans le Centre d'installation, vous pouvez désormais utiliser le bouton **Forcer la mise à jour** pour poursuivre une mise à jour même si une console d'administration est toujours ouverte.

Erreur de mise à jour de la console d'administration

La mise à jour de la console d'administration ne provoque plus une erreur récurrente dans les logs du composant backend. Désormais, le log est généré une seule fois.

Mise à jour de l'agent SES Evolution

Suite à une mise à jour de l'agent SES Evolution, celui-ci pouvait empêcher le lancement de certains processus. Ce problème a été corrigé.

Politiques de sécurité

Export et import de jeux de règles

Il est maintenant possible d'exporter un jeu de règle puis de le réimporter sur un autre environnement SES Evolution de la même version.

Identifiants d'application

Dans une règle de sécurité, l'utilisation conjointe d'identifiants récursifs et de certificats pour identifier une application pouvait provoquer un écran bleu. Ce problème a été corrigé.

Politique par défaut SES Evolution

La politique par défaut intègre maintenant une compatibilité avec le mode renforcé de Panda Adaptive 360. SES Evolution masque les opérations de Dissimulation de processus lorsqu'elles sont causées de manière légitime par Panda.

Le jeu de règles d'audit de la politique par défaut a été modifié pour limiter les logs qui ne sont pas pertinents pour un administrateur de la sécurité. Ceci permet de réduire le nombre de logs et l'usage de la CPU système par SES Evolution.

Agent SES Evolution

Références support : 178084CW - 180244CW

Sous certaines conditions, les agents SES Evolution envoyaient des informations de statut qui étaient mal interprétées par le gestionnaire d'agents. Dans ce cas, les données affichées sur le panneau **Agents** de la console d'administration pouvaient être incorrectes et des problèmes divers pouvaient survenir, telle que l'impossibilité de répondre à des challenges. Ce problème est résolu.

Les agents en attente de redémarrage suite à un changement de fonctionnalités sont désormais affichés correctement sur le Tableau de bord de la console d'administration.

Périphériques

Références support : 180798CW - 164622PW

L'utilisation de produits *FTDI Chip* ne provoque plus d'écran bleu. La compatibilité avec les périphériques en général a été améliorée.

Vulnérabilités résolues de SES Evolution 2.0.1

Ajout d'une protection contre les attaques par déni de service
Une protection anti DDoS a été ajoutée sur l'API qui enregistre un nouveau gestionnaire d'agents dans le Backend. Désormais un seul gestionnaire d'agents peut être enregistré toutes les 15 secondes.

Suppression d'une valeur dans la base de registre
Une valeur liée à la sécurité des challenges était présente inutilement dans la base de registre. Cette vulnérabilité a été résolue par la suppression de cette valeur.

Correctifs de SES Evolution 2.0.1

Installation de SES Evolution

Champs mots de passe

Dans le Centre d'installation, les champs des mots de passe et leur confirmation sont désormais correctement vérifiés dans tous les cas.

Validité de la licence

Dans le Centre d'installation, le format et la validité de la licence sont vérifiés dès la sélection du fichier de licence et non plus à la fin de l'installation.

Politiques de sécurité

Référence support : 177214CW

Accès réseau

Il est maintenant possible de bloquer certains accès réseau qui n'étaient pas filtrés par les protections applicatives car effectués par le système. Ceci permet par exemple de bloquer les accès distants à un dossier partagé situé sur une machine protégée par l'agent SES Evolution.

En cas de mise à jour vers SES Evolution 2.0.1, la politique par défaut n'est pas mise à jour. Vous pouvez télécharger le jeu de règles correspondant sur votre espace personnel MyStormshield afin d'ajouter les autorisations d'accès réseau pour les processus système. Pour plus d'informations, reportez-vous à la Base de connaissance Stormshield.

Identifiants réseau

L'option **Inverser la portée de l'identifiant** dans l'édition des identifiants réseaux est désormais sauvegardée correctement.

Règles d'audit sur les pilotes

Les comportements spécifiques des règles de protection Chargement des pilotes et Intégrité des pilotes sont désormais bien appliqués. Ces règles ne génèrent plus de logs injustifiés pour les pilotes autorisés.

Logs

Recherche dans les logs agent

Dans la console d'administration, le délai maximum d'une recherche dans les logs agents est passé de 30 secondes à 15 minutes. Un message est désormais affiché lorsque la recherche dépasse ce délai.

Affichage des incidents

A l'ouverture d'un incident, seuls les logs de type alerte sont désormais affichés, dans la limite de 1000 logs. Le reste des logs est chargé lors de la consultation du graphique d'attaque dans la limite de 100000 logs. Ceci permet de construire le graphique d'attaque avec des logs complets.

Agent SES Evolution

Logs longs

Les logs très longs ne provoquent plus la fermeture inopinée de l'interface graphique de l'Agent SES Evolution.

Règles d'autoprotection

Les règles d'autoprotection sur certaines clés de registre d'un agent SES Evolution n'étaient pas appliquées correctement. Ce problème a été corrigé.

Affichage

Agents Windows 10

Le panneau **Agents** de la console d'administration affiche désormais la version correcte du système d'exploitation pour les agents Windows 10.

Résumé des fonctionnalités

La version 2.0 de SES Evolution offre les fonctionnalités suivantes.

Fonctionnalités de SES Evolution 2.0

Protections	
Contre les débordements mémoire	Protégez votre parc contre des tentatives d'intrusion et des exploitations de vulnérabilités.
Contre la dissimulation de processus	
Contre le vol de jetons de sécurité	
Contre les contournements du système de fichiers	
Contre les enregistreurs de frappes	
Contrôle des accès aux fichiers	Contrôlez l'ensemble des ressources système et des accès qui y sont faits. Autorisez des applications à opérer des changements ou à accéder à ces ressources ou bloquez-les. Vous pouvez également simplement les surveiller.
Contrôle des accès à la base de registre	
Contrôle des accès à la mémoire	
Contrôle des exécutions	
Détection de chargement de pilotes	Détectez les rootkits tentant de charger ou de modifier des pilotes dans le noyau.
Détection d'altération de pilotes	
Pare-feu applicatif	Contrôlez les communications réseau entrantes et sortantes par application.
Contrôle des points d'accès Wi-Fi	Gérez les réseaux Wi-Fi autorisés et empêchez le bridge Wi-Fi-LAN.
Contrôle des lecteurs de disquettes, lecteurs CD/DVD, Ports série	Contrôlez les périphériques autorisés sur votre parc via des règles totalement personnalisables.
Contrôle des périphériques Bluetooth	
Contrôle des périphériques USB	
Sas de décontamination USB	Contrôlez les clés et disques durs USB sur votre parc, gérez les périphériques de confiance et bloquez les périphériques dont le contenu n'a pas été validé.

Paramétrage	
Gestion par groupes d'agents	Organisez votre parc selon vos besoins via un système de groupes d'agents simple et puissant.
Déploiement de configurations	Déployez les nouvelles configurations sur l'ensemble des agents en un clic depuis la console d'administration.
Politique de sécurité Stormshield	Protégez votre parc avec une politique par défaut couvrant les menaces courantes et ajoutez des règles de sécurité personnalisées pour une adaptation totale à votre environnement.

Politiques de sécurité contextuelles	Adaptez la sécurité à l'environnement des agents afin qu'ils appliquent des politiques différentes en fonction de leur emplacement.
Gestion de politiques par jeux de règles	Mutualisez les règles de sécurité dans vos politiques et gérez simplement vos exceptions.
Tâches planifiées	Exécutez des commandes sur les agents en paramétrant des scripts depuis la console d'administration.
Modularité des agents	Gérez les fonctionnalités installées sur chaque agent depuis la console d'administration : désinstallez les fonctionnalités inutiles, supprimez des incompatibilités et limitez la surface d'attaque.
Challenges	Autorisez certaines opérations sur les agents de manière sécurisée via un système de question/réponse.
Connexion simultanée des administrateurs à la console	Organisez vos administrateurs par rôle pour gérer des accès simultanés aux diverses ressources de la console d'administration.

Surveillance de l'activité	
Tableau de bord	Visualisez rapidement l'état de votre parc grâce à un tableau de bord simple.
Suivi des logs	Visualisez les événements produits par les agents en les filtrant par priorité, type, groupe etc.
Analyse d'attaques	Suivez les incidents et analysez les attaques grâce au panneau dédié permettant de revoir graphiquement les étapes et de chercher plus d'informations pour comprendre chaque attaque.
Surveillance des agents	Suivez en temps réel les agents du parc, vérifiez leur état et assignez-les à des groupes.
Export vers un serveur Syslog	Exportez l'ensemble des événements dans votre SIEM pour les intégrer à vos autres sources d'informations de sécurité (firewall, antivirus, etc.).

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Rapporter un incident/Suivre un incident**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.