STORMSHIELD ENDPOINT SECURITY EVOLUTION

NOTES DE VERSION

Version 2

Dernière mise à jour du document : 18 décembre 2023

Référence : ses-fr-notes_de_version-v2.5.3

Table des matières

Nouvelles fonctionnalités et améliorations de SES Evolution 2.5.3 3
Correctifs de SES Evolution 2.5.3 7
Versions de Microsoft Windows compatibles 9
Préconisations 10
Mise à jour des politiques de sécurité intégrées et du parc d'agents 10
Mise en œuvre des politiques de sécurité 12
Mise à jour du système d'exploitation des postes de travail 12
Problèmes connus 13
Précisions sur les cas d'utilisation 14
Ressources documentaires 15
Télécharger cette version 16
Versions précédentes de SES Evolution v2 17
Contact 75

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.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.5.3

Avertissement

ATTENTION
Avant de mettre à jour une version 2.3.x de la solution vers la version 2.5.3, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Protection du parc

Isolation des ordinateurs des utilisateurs

En cas de soupçon d'attaque sur un poste de travail du parc, vous pouvez désormais l'isoler du reste du réseau en coupant ses connexions entrantes et sortantes depuis la console d'administration.

L'isolation d'un poste avec SES Evolution permet d'arrêter rapidement la propagation d'une attaque à l'ensemble du parc si celle-ci est avérée.

Depuis la console d'administration, vous pouvez isoler les ordinateurs, consulter la liste des ordinateurs isolés et arrêter l'isolation.

En savoir plus

Mise en quarantaine de fichiers malveillants

Lorsque vous créez une tâche de remédiation en cas d'attaque, vous pouvez désormais choisir de mettre en quarantaine un fichier suspecté d'être malveillant. Le fichier est placé dans un répertoire protégé du poste de travail. Il ne peut plus être exécuté ni causer de dommage le temps que vous l'analysiez. Après analyse, vous choisissez de restaurer le fichier ou de le supprimer.

Vous pouvez établir dans la console d'administration une liste de dossiers à exclure. Les fichiers qu'ils contiennent ne seront jamais mis en quarantaine.

Vous pouvez également paramétrer la mise en quarantaine automatique de fichiers exécutables depuis une règle de protection dans les politiques de sécurité.

Les fichiers mis en quarantaine sont automatiquement supprimés au bout de 40 jours ou lorsque la taille du répertoire atteint 1 Go.

En savoir plus

Envoi de notifications par e-mail

En cas d'alerte de sécurité, les administrateurs de SES Evolution peuvent maintenant être alertés par e-mail. Vous êtes ainsi prévenus rapidement lorsque certains événements se produisent sur votre parc, sans avoir à surveiller la console d'administration en permanence. Grâce à des règles de notification, vous pouvez choisir les types de logs qui doivent déclencher l'envoi d'une notification, la fréquence d'envoi et l'adresse e-mail des destinataires.

En savoir plus

Envoi de rapports d'activité par e-mail

Vous pouvez configurer l'envoi de rapports par e-mail. Ces rapports fournissent des informations sur l'activité de votre parc en reprenant les indicateurs de sécurité et les indicateurs opérationnels affichés dans le tableau de bord de la console. Ils peuvent par exemple être adressés à des personnes qui ne sont pas administratrices de la solution SES Evolution. Grâce à des règles de notification, vous pouvez paramétrer la fréquence d'envoi de ces rapports ainsi que leur langue (français, anglais, allemand, espagnol).

En savoir plus

Protection contre le contournement des moyens de détection des EDR (Endpoint Detection and Response)

Dans l'onglet **Menaces** des politiques de sécurité, la nouvelle protection **Contournement des détections EDR** est disponible. Elle protège contre les attaques cherchant à désactiver les modules de détection des EDR.

En savoir plus

Protection contre les attaques sans fichier

Dans l'onglet **Menaces** des politiques de sécurité, la nouvelle protection **Attaque sans fichier** est disponible. Elle protège contre les attaques qui agissent sans écriture de fichiers malveillants sur les postes de travail.

En savoir plus

Nouvelles politiques par défaut

Depuis la version 2307a des politiques de sécurité, la politique par défaut a été découpée en trois niveaux. Il existe donc désormais trois politiques par défaut :

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.
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.
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.

Nouveaux jeux de règles intégrés

Depuis la version 2307a des politiques de sécurité, les deux jeux de règles partagés suivants ont été ajoutés.

Durcissement contre les logiciels portables	Ce jeu bloque tous les exécutables lancés en dehors des dossiers standards d'installation.
Durcissement des dossiers d'installation des logiciels	Ce jeu empêche un attaquant de modifier les fichiers d'un logiciel dans les dossiers d'installation, pour prendre leur place dans le système.

Depuis la version 2310a des politiques de sécurité, les deux jeux de règles partagés suivants ont été ajoutés.

Audit pour la fonctionnalité EDR	Ce jeu permet de faire de la détection de WMI à des fins de recherche d'informations sur les mises à jour installées sur le système d'exploitation utilisé.
Syslog - Modèle d'audit sans lecture pour envoi vers Syslog	Ce jeu est sous forme de modèle. Il permet de capturer tous les événements autres que des lectures fichier et des lectures registre et de les envoyer à une autre solution de sécurité via Syslog.

Modularisation des jeux de règles

Depuis la version 2307a des politiques de sécurité, les jeux de règles suivants ont été découpés pour rendre leur utilisation plus modulaire. Les fonctionnalités peuvent être activées indépendamment, sans impacter les autres jeux de règles :

Le jeu de règle ...	devient ...
Audit pour contextes d'attaques	Trois jeux de règles : • Audit pour contextes d'attaques • Audit de la protection ARP Spoofing • Audit des chargements de pilotes
Prévention des fuites d'informations	Quatre jeux de règles : • Prévention des fuites d'informations - Windows • Prévention des fuites d'informations - Navigateurs web • Prévention des fuites d'informations - Coffres-forts numériques • Prévention des fuites d'informations - Outils d'accès à distance

Pour plus d'informations sur les politiques de sécurité et jeux de règles intégrés, consultez les Notes de version du paramétrage de sécurité de SES Evolution sur votre espace client MyStormshield (dans la rubrique **Téléchargements**, puis dans les **Ressources de sécurité** de SES Evolution).

API publique de SES Evolution

Stormshield fournit une nouvelle API publique permettant d'administrer SES Evolution via des solutions d'orchestration (comme des solutions SOAR). En version 2.5.3, l'API publique permet d'utiliser entre autres les fonctionnalités suivantes de SES Evolution :

- Interrompre un processus,
- Supprimer un fichier, une clé ou une valeur de registre,
- Isoler un poste de travail du réseau,
- Effectuer des tâches de remédiation en cas d'attaque par ransomware. Les fichiers chiffrés par le ransomware sont alors restaurés dans leur version initiale

Dans la console d'administration SES Evolution, vous pouvez générer les clés API qui sécurisent l'accès aux routes API.

L'API publique de SES Evolution est accompagnée d'une documentation. Pour la consulter, cliquez sur le lien en haut à droite du panneau **Clés API** dans la console d'administration. Elle contient une description des routes API, la liste des paramètres et des exemples.

La documentation est également disponible sur le site de la Documentation technique Stormshield.

En savoir plus

Console d'administration

Nouveau tableau de bord

Le tableau de bord de la console d'administration affiche de nouveaux indicateurs clés décrivant l'état de votre parc. Ils vous permettent de répondre aux besoins de maintien en condition de sécurité et en condition opérationnelle en vous alertant notamment sur les événements de sécurité nécessitant une analyse rapide.

En savoir plus

Nouvelle organisation du menu principal

L'affichage des menus de gauche constituant le menu principal de la console a été réorganisé. Ils sont maintenant classés par catégories **Environnement**, **Sécurité**, **Réponses** et **Backoffice**.

Mise à jour des ressources Stormshield

Lorsque vous utilisez le serveur public Stormshield pour télécharger les mises à jour des ressources dans la console d'administration, vous pouvez maintenant paramétrer et utiliser un serveur proxy pour contacter le serveur Stormshield.

En savoir plus

Configuration d'un serveur Syslog

Formatage des messages Syslog

Si vous avez paramétré l'envoi des logs des agents vers un serveur Syslog, vous pouvez maintenant ajouter des "structured data" dans l'en-tête des messages. Un nouveau champ **Structured data** est disponible dans le menu **Gestionnaires d'agents** de la console d'administration. Pour connaître le format attendu des données, consultez la RFC 5424.

En savoir plus

Indicateurs de fonctionnement des serveurs Syslog

Un nouvel indicateur dans le bandeau supérieur de la console d'administration permet de connaître l'état des serveurs Syslog paramétrés.

Remplacement de la notion d'Incident

La notion d'*incident* a été remplacée par la notion de *contexte*. Par défaut, tous les logs de niveau Urgence et Alerte sont désormais accompagnés d'un contexte qui permet 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. Le graphique d'attaque se nomme désormais *graphique de contexte*.

Correctifs de SES Evolution 2.5.3

Console d'administration

Export d'incidents

Référence support : 174891PW

La fonctionnalité d'export d'incidents ne fonctionnait plus en version 2.4.4. Le problème est résolu. En version 2.5.3, la notion d'*incident* est remplacée par la notion de *contexte*.

Mise à jour de la console d'administration

Référence support : 209980CW

Après une mise à jour de la solution, il pouvait être impossible de rouvrir la console d'administration. Le problème est maintenant résolu. Cependant la console peut mettre quelques minutes à démarrer lors de la première ouverture après la mise à jour.

Maintenance de la base de données de logs

Référence support : 211396CW

Il n'est dorénavant plus possible d'exécuter une suppression manuelle de logs alors qu'une maintenance de la base de données est en cours.

Affichage des logs d'analyse Yara et IoC

Les logs d'analyse Yara et IoC sont désormais systématiquement affichés dans la console d'administration. Il n'est plus possible de modifier le paramètre d'affichage des logs lors de la création d'une tâche manuelle ou d'une tâche planifiée.

Gestion des identifiants de périphériques USB

Référence support : 211108CW

La modification du paramètre **Vendeur** dans les identifiants utilisés dans une règle de type USB, ou dans le comportement spécifique d'une règle de type Stockage USB, pouvait entraîner une modification automatique du paramètre **Produit**. La règle ne fonctionnait alors plus comme attendu. Ce problème est résolu.

Suppression automatique des agents inactifs

Référence support : 175102PW

La suppression automatique des agents déconnectés ne génère plus de log d'erreur dans la console d'administration lorsque des tâches d'analyse Yara ou IoC sont liées à ces agents.

Détection des périphériques USB

Référence support : 208241CW

Lorsque aucun paramètre de la section **Confiance des périphériques** n'est sélectionné dans la configuration d'un groupe d'agents, les périphériques USB branchés sur les postes de travail ne sont plus signalés dans le menu **Périphériques** de la console d'administration.

Déploiement de l'environnement

Référence support : 199390CW

Lors d'un déploiement de l'environnement sur le parc d'agents, certaines requêtes des tuiles du tableau de bord de la console d'administration échouaient. Des logs d'erreur s'affichaient dans les logs Système. Ce problème est résolu.

Agent SES Evolution

Utilisation de l'outil de diagnostic de l'agent

Il est désormais possible de mettre à jour un agent sur un poste de travail, de le réparer ou bien de modifier les fonctionnalités actives d'un agent lorsqu'une prise de traces est en cours sur le poste.

Versions de Microsoft Windows compatibles

Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.

Préconisations

Mise à jour des politiques de sécurité intégrées et du parc d'agents

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

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

Les jeux de règles intégrés fournis par Stormshield sont automatiquement mis à jour dans la console d'administration lors de la mise à jour de la solution. Ce n'est pas le cas des politiques de sécurité intégrées. Le cas échéant, vous devez mettre à jour manuellement vos politiques dans la console si les jeux de règles qu'elles contiennent présentent une flèche verte, comme décrit à l'étape 4 de la procédure ci-dessous.

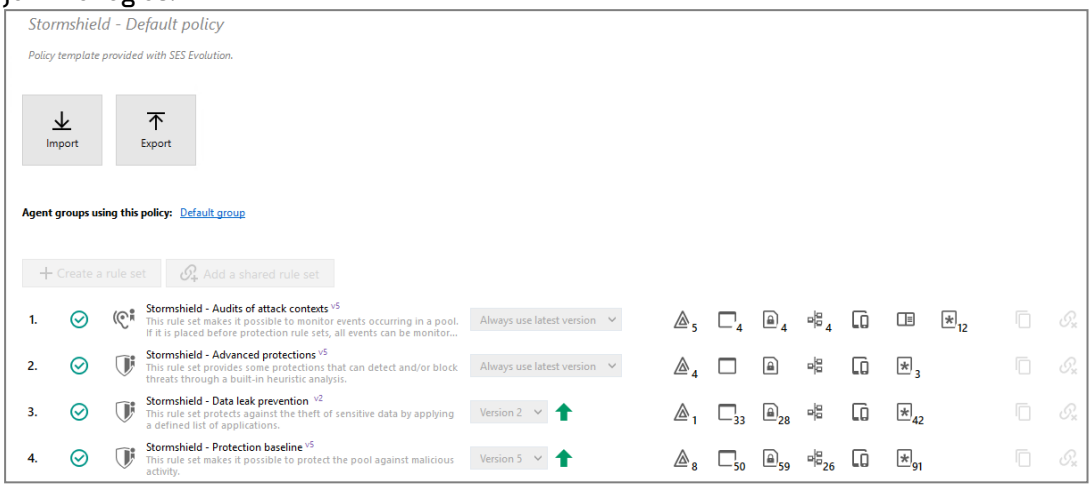
La mise à jour des politiques et du parc dans cette nouvelle version comprend les grandes étapes suivantes :

1	Mise à jour de la solution SES Evolution via le Centre d'installation
2	Mise à jour des politiques de sécurité pour utiliser les dernières versions des jeux de règles
3	Création d'un groupe d'agents de test
4	Sélection d'agents pilotes pour le groupe de test et surveillance de leur comportement pendant quelques jours
5	Mise à jour de tous les agents en version 2.5.3

Nous vous recommandons de suivre la procédure détaillée ci-dessous pour la mise à jour :

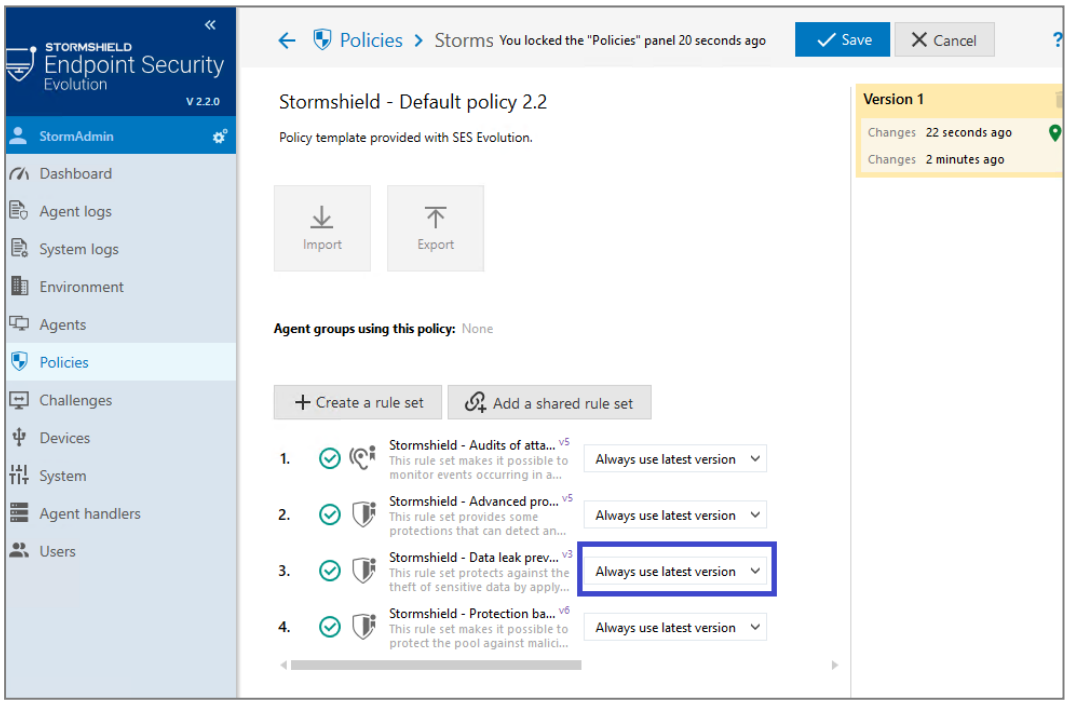
1. Si des modifications sont en cours dans vos consoles d'administration, sauvegardez-les puis fermez les consoles.
2. Suivez la procédure de mise à jour des composants de la solution SES Evolution via le Centre d'installation, comme indiquée dans le Guide d'installation.
3. Lorsque la mise à jour est terminée via le Centre d'installation, rouvrez les consoles pour finaliser la mise à jour. Un message vous avertit que les politiques de sécurité n'utilisent pas la dernière version des jeux de règles. Les politiques n'ont pas été mises à jour automatiquement pour éviter des problèmes d'incompatibilité avec les agents en versions antérieures à la version 2.5.3.

4. Choisissez une console. Dans le menu **Sécurité** > **Politiques** de la console, une flèche verte orientée vers le haut signale les politiques n'utilisant pas la dernière version de certains jeux de règles.



Dupliquez une politique présentant une flèche verte, la politique par défaut par exemple.

5. Sélectionnez la copie de la politique et cliquez sur **Modifier**.
6. Renommez la politique en ajoutant le numéro de version "2.5.3" par exemple.
7. Sélectionnez **Toujours utiliser la dernière version** pour tous les jeux présentant une flèche verte.



8. Enregistrez la politique.
9. Depuis le menu **Environnement** > **Agents**, dupliquez maintenant l'un de vos groupes d'agents de production pour tester le déploiement en version 2.5.3 avec la nouvelle politique mise à jour.
10. Dans l'onglet **Politiques**, sélectionnez la politique créée précédemment.
11. Assurez-vous que la version logicielle sélectionnée dans la section **Version** de l'onglet **Paramètres** est bien 2.5.3.
12. Enregistrez le nouveau groupe.

13. Vous allez maintenant choisir un ou plusieurs agents dans votre groupe initial qui serviront d'agents pilotes. Depuis l'onglet **Agents** du groupe initial, sélectionnez les agents pilotes et cliquez sur **Déplacer les agents vers**. Choisissez le nouveau groupe de test.
14. Depuis le menu **Sécurité** > **Déploiement**, cliquez sur **Déployer** pour déployer les changements sur votre environnement.
15. Du côté des agents pilotes, après leur reconnexion au gestionnaire d'agents, le redémarrage des postes de travail est requis. Après le redémarrage, vérifiez que les agents sont bien passés en version logicielle 2.5.3 et qu'ils utilisent bien la nouvelle politique.

Testez pendant quelques jours le comportement des agents pilotes. Lorsque vous vous êtes assuré de leur bon fonctionnement, vous pouvez procéder à la mise à jour de tous les agents du parc. Vous avez deux possibilités :

- Sélectionner la nouvelle politique et la version logicielle 2.5.3 dans vos groupes d'agents de production. Si vous optez pour cette solution, pensez à supprimer le groupe de test.

- ou -

- Dupliquer tous vos groupes de production et les mettre à jour, puis éventuellement supprimer les anciens groupes.

Si un retour à une version antérieure des agents s'avérait nécessaire après la mise à jour en version 2.5.3, la version ne serait plus compatible avec les politiques contenant des fonctionnalités de la version 2.5.3. Nous vous recommandons alors de déplacer de nouveau les agents concernés dans leur groupe d'origine.

Mise en œuvre des politiques de sécurité

Avec la version 2.5.3, Stormshield fournit la version 2310b du paramétrage de sécurité. Ce paramétrage par défaut inclut des politiques ainsi que des jeux de règles de protection et des jeux de règles d'audit partagés. Ces jeux de règles peuvent être utilisés dans vos propres politiques.

Pour consulter les Notes de version de la version 2310b du paramétrage de sécurité, rendez-vous dans la rubrique **Téléchargements** de votre espace client MyStormshield, puis dans les **Ressources de sécurité** de SES Evolution.

Pour construire vos politiques, vous pouvez vous appuyer sur les recommandations mentionnées dans les Notes de version du paramétrage de sécurité concernant l'ordre des jeux et le choix des jeux à utiliser.

Pour plus d'informations, reportez-vous aux sections Comprendre les jeux de règles intégrésset Personnaliser les jeux de règles intégrés du *Guide d'administration* SES Evolution

Mise à jour du système d'exploitation des postes de travail

Avant de mettre à jour le système d'exploitation Microsoft des postes de travail hébergeant les agents SES Evolution, assurez-vous de disposer des jeux de règles Stormshield les plus récents. Si ce n'est pas le cas, vous devez télécharger les derniers jeux de règles comme décrit à la section Télécharger les mises à jour Stormshield du *Guide d'administration*, puis mettre à jour vos politiques de sécurité.

Problèmes connus

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

Précisions sur les cas d'utilisation

Utilisation de l'outil Sysprep sous Windows Server 2019

Si vous avez besoin d'utiliser l'outil Sysprep de Microsoft sur un poste de travail sous Windows Server 2019, nous vous recommandons d'appliquer auparavant une politique de sécurité vide pour éviter un écran bleu. Après redémarrage du poste, vous pouvez appliquer de nouveau la politique de sécurité nominale.

Contrôle d'accès aux fichiers et copie de fichiers

Lors d'une copie de fichiers sur un partage réseau, les règles d'accès aux fichiers ne s'appliquent pas si les fichiers source et destination se trouvent sur le même partage. En revanche, elles s'appliquent bien lors d'une copie d'un partage vers la machine locale, ou d'un partage vers un autre partage.

Compatibilité avec la protection Smart Application Control de Windows

À partir de la version 2.4, SES Evolution est compatible avec la protection Smart Application Control, disponible lors d'une nouvelle installation de Windows 11 22H2 (désactivée par défaut). Cependant l'installation de l'agent génère des messages d'avertissement non bloquants concernant les pilotes démarrés par l'agent.

Aide en ligne de SES Evolution

La version de l'aide en ligne accessible depuis la console d'administration est toujours la dernière version disponible, indépendamment de la version de la console installée.

Challenges

Depuis une console à partir de la version 2.4, il n'est pas possible d'utiliser le mécanisme des challenges avec des agents en version 2.3.x ou inférieure.

Protection contre la persistance via WMI

La protection avancée contre la persistance via WMI est incompatible avec le système d'exploitation Microsoft Windows 10 LTSB 2015 en versions 32 et 64 bits. Même si elle est activée, elle ne se déclenche pas sur ce système d'exploitation. Cette incompatibilité n'empêche pas le fonctionnement normal de l'agent SES Evolution.

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
- Guide des préconisations SQL Server
- Documentation de l'API publique

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 2.5.3 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.

2.5.0	Nouvelles fonctionnalités		
2.4.5			Correctifs
2.4.4			Correctifs
2.4.3		Vulnérabilités résolues	Correctifs
2.4.2			Correctifs
2.4.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
2.3.2	Nouvelles fonctionnalités		Correctifs
2.3.1	Nouvelles fonctionnalités		Correctifs
2.2.3	Nouvelles fonctionnalités		Correctifs
2.2.2	Nouvelles fonctionnalités		Correctifs
2.1.2		Vulnérabilités résolues	
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		

Version 2.5.2 mode SaaS

La version 2.5.2 de SES Evolution est disponible uniquement en mode SaaS.

Version 2.5.1 mode SaaS

La version 2.5.1 de SES Evolution est disponible uniquement en mode SaaS.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.5.0

SES Evolution en mode SaaS

SES Evolution est désormais disponible en mode SaaS. Vous pouvez donc bénéficier de la protection de SES Evolution avec des politiques de sécurité adaptées sans installer de serveur d'administration dans votre infrastructure. La configuration, l'administration et la surveillance de la solution peuvent maintenant être effectuée à distance via le cloud par un fournisseur de services expert en sécurité (MSSP). Seul l'agent SES Evolution doit être déployé sur les postes de travail des utilisateurs.

La version 2.5.0 de SES Evolution est disponible uniquement en mode SaaS.

Correctif de SES Evolution 2.4.5

Avertissement

ATTENTION
Avant de mettre à jour une version 2.3.x de la solution vers la version 2.4.5, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Console d'administration

Gestion du volume de la base de données de logs

Références support : 211151CW, 211647CW

En cas de génération très importante de logs, la base de données de logs pouvait être rapidement saturée. Pour éviter ce problème, un mode dégradé s'active désormais lorsque la base de données de logs atteint le seuil de remplissage critique de 81%. Il est représenté par un bandeau d'alerte rouge 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 désactiver ce mode dégradé, cliquez sur le bouton **Retour au mode standard**. L'opération n'est réalisable que si le volume de la base de données de logs est repassé sous le seuil de 81%. Vous devez donc auparavant ajuster votre politique de sécurité et supprimer manuellement des logs agents.

Correctifs de SES Evolution 2.4.4

Avertissement

ATTENTION
Avant de mettre à jour une version 2.3.x de la solution vers la version 2.4.4, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Console d'administration

Règles de contrôle d'accès aux fichiers

Après l'installation des dernières versions de Windows 10 et 11, les règles d'accès en lecture et écriture de fichiers n'étaient pas appliquées lors d'une copie de fichiers.

Ce problème est apparu à partir des mises à jour suivantes de Windows :

- Windows 10 20H2 build 19042.2788, KB5023773 (21/03/2023)
- Windows 10 21H2 build 19044.3086, KB5027215 (13/06/2023)
- Windows 10 22H2 build 19045.2913, KB5025297 (25/04/2023)
- Windows 11 21H2 build 22000.1761, KB5023774 (28/03/2023)
- Windows 11 22H2 build 22621.1105, KB5022303 (10/01/2023)

Il est désormais corrigé, à l'exception d'une limitation pour les partages réseau, décrite dans la section Précisions sur les cas d'utilisation.

Export d'incidents

Référence support : 207668CW

La fenêtre de sélection du chemin d'export s'affiche désormais immédiatement après un clic sur le menu **Exporter les incidents**.

Affichage des logs agents

Dans le panneau des logs agents, la description de la règle s'affiche désormais correctement dans les logs concernant des règles de sécurité.

Suppression de ressources IoC ou Yara

Il est désormais possible de supprimer les ressources IoC ou Yara liées à un agent préalablement supprimé.

Logs des recherches IoC

Les paramètres de logs spécifiés lors de la création d'une tâche d'analyse IoC sont désormais correctement pris en compte.

Rôle Assistance

Un utilisateur ayant le rôle Assistance parvient désormais à ouvrir la console d'administration et à changer la langue.

Agent SES Evolution

Transfert d'événements Windows

Référence support : 209227CW

Les agents SES Evolution remontent désormais systématiquement à la console d'administration tous les éléments détectés par les règles de transferts d'événements Windows.

Traitement des requêtes DNS

Référence support : 208562CW

Dans des cas rares, l'agent pouvait mal interpréter des requêtes DNS effectuées par des applications. Ce phénomène pouvait entraîner un dysfonctionnement des applications en question. Ce problème est résolu.

Composants Backoffice

Collecte des données de bases de données

Référence support : 208562CW

Le travail de collecte de données de diagnostic dans les bases de données n'échoue plus lorsqu'une mise à jour de SES Evolution est exécutée simultanément ou qu'elle est incomplète.

Envoi des logs agents vers un serveur Syslog

La description synthétique des logs agents visible dans la console d'administration est désormais transmise aux serveurs Syslog, au format d'export JSON.

Vulnérabilités résolues de SES Evolution 2.4.3

Agent SES Evolution

Deux vulnérabilités de sévérité basse ont été corrigées.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2023-021/
- https://advisories.stormshield.eu/2023-022/

Correctifs de SES Evolution 2.4.3

Avertissement

ATTENTION
Avant de mettre à jour une version 2.3.x de la solution vers la version 2.4.3, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Console d'administration

Détail des logs agent

Dans certains cas, la console d'administration s'arrêtait inopinément lors de l'affichage des informations détaillées d'un log agent. Ce problème a été corrigé.

Serveur Syslog

Logs au format JSON

L'adresse IP de l'agent n'était pas communiquée dans les logs agents au format JSON envoyés au serveur Syslog. Ce problème a été corrigé.

Correctifs de SES Evolution 2.4.2

Avertissement

ATTENTION
Avant de mettre à jour votre solution en version 2.4.2, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Agent SES Evolution

Compatibilité de l'agent SES Evolution avec les systèmes d'exploitation Microsoft Windows

La méthode de signature des pilotes SES Evolution a été revue afin de conserver la compatibilité avec les systèmes d'exploitation Windows 7, Windows 8.1, Windows Server 2008 R2 et Windows Server 2012 R2.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.4.1

Avertissement

ATTENTION
Avant de mettre à jour votre solution en version 2.4.1, vous devez télécharger et déployer la politique de sécurité 2304a. Pour la télécharger, rendez-vous sur votre espace client MyStormshield ou bien dans le panneau des Mises à jour Stormshield de votre console d'administration.

Protection du parc renforcée

Intégration de la recherche d'indicateurs de compromission

SES Evolution permet désormais de rechercher des indicateurs de compromission (IoC) sur tout ou partie de votre parc informatique. Les IoC permettent de détecter une attaque sur un poste utilisateur, de prévenir sa diffusion, voire même d'assainir les systèmes avant que la compromission ne soit exploitée.

Ces indicateurs peuvent être par exemple des noms de fichiers, des adresses IP particulières, des hashes de fichiers malveillants, des adresses URL ou des textes suspects.

Les recherches d'IoC peuvent être déclenchées lorsqu'une règle de sécurité détecte ou bloque un comportement inhabituel. Mais vous pouvez également déclencher des recherches manuellement, à tout moment, pour surveiller un ou plusieurs postes à la demande. Vous avez également la possibilité de planifier des analyses IoC par groupe d'agents, à intervalles réguliers et pendant une durée définie.

Pour rechercher des IoC, vous devez en fournir une description à SES Evolution. Les IoC peuvent provenir de votre propre parc informatique si vous avez détecté une compromission avec SES Evolution ou par un autre moyen, ou bien d'une source externe privée ou publique.

En savoir plus

Actions de remédiation sur un ensemble de postes de travail

En cas d'attaque ou d'action malveillante sur votre parc informatique, vous pouvez maintenant lancer des actions de remédiation sur plusieurs postes, à partir des logs agents remontés dans la console d'administration. Il s'agit d'un ensemble d'actions permettant de limiter l'impact des attaques et de réparer les éventuels dommages.

En fonction du type du log agent, SES Evolution propose différentes actions de remédiation, par exemple : supprimer un fichier ou une clé de registre, interrompre un processus ou bien récupérer les fichiers chiffrés par un ransomware.

En savoir plus

Détection des applications Windows Store

SES Evolution est désormais capable de détecter les signatures d'applications validées par Microsoft pour leur diffusion via le Windows Store. Cette vérification permet d'étendre le

contrôle des applications légitimes aux applications provenant de Windows Store et s'appuie sur l'analyse des informations contenues dans le certificat des applications.

Gestion des bases de données

Supervision des bases de données d'administration et de logs

SES Evolution permet désormais de surveiller le remplissage des bases de données et d'éviter leur saturation grâce à un calcul prévisionnel et à des alertes. Dans le menu **Système** de la console d'administration, des graphiques permettent de visualiser rapidement l'occupation des bases et d'estimer leur saturation dans l'avenir.

Afin d'anticiper la saturation des bases de données et de réduire leur taille, SES Evolution vous permet de :

- Planifier des tâches de maintenance quotidiennes afin d'optimiser les performances des bases de données,
- Réaliser des suppressions manuelles immédiates de logs,
- Planifier des suppressions automatiques de logs antérieurs à une période définie.

De plus, SES Evolution permet dorénavant d'exporter les incidents remontés en cas d'attaque. Vous pourrez ainsi les soumettre à un service externe pour analyse par exemple, et également les archiver sur un serveur de stockage afin de libérer de l'espace sur la base de données des logs.

En savoir plus

Résolution des problèmes

Outil de diagnostic

En cas de fonctionnement anormal, le nouvel outil de diagnostic de SES Evolution collecte des données concernant le composant qui pose problème (agent et backoffice) et le système Windows de la machine. Ces données peuvent être analysées par le Support technique de Stormshield pour établir un diagnostic.

En savoir plus

Console d'administration

Nouvelles icônes de raccourcis

Dans la console d'administration, un nouveau bandeau en haut de la fenêtre affiche plusieurs icônes proposant des accès directs à des menus de la console :

- Trois icônes indiquant l'état du serveur backend, des bases de données et des gestionnaires d'agents. Cliquez sur les icônes pour afficher plus de détails.
- Une icône pour accéder au menu **Environnement**. Lorsqu'un déploiement est nécessaire, l'icône devient orange.
- Une icône pour accéder aux préférences de l'utilisateur.
- Une icône pour accéder au menu **Mises à jour Stormshield**.

Agent SES Evolution

Compatibilité avec Smart Application Control

L'agent SES Evolution est désormais compatible avec l'option Smart Application Control du système d'exploitation Windows 11 22H2. Veuillez cependant consulter la section Précisions sur les cas d'utilisation pour plus d'informations.

Politiques de sécurité

Règles Réseaux Wi-Fi

Le mode d'authentification WPA3 est désormais disponible dans les règles Réseaux Wi-Fi des politiques de sécurité afin de bloquer, autoriser ou surveiller ce type de connexion.

En savoir plus

Versions de SQL Server compatibles

Nouvelle compatibilité

SES Evolution est désormais compatible avec les bases de données SQL Server 2022 et SQL Server Express 2022.

Vulnérabilités résolues de SES Evolution 2.4.1

Backend

Deux vulnérabilités de sévérité basse ont été corrigées.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2023-001/
- https://advisories.stormshield.eu/2023-002/

Correctifs de SES Evolution 2.4.1

Agent SES Evolution

Vérification de l'intégrité de l'agent

Référence support : 199381CW

La vérification de l'intégrité de l'agent a été optimisée et le niveau de sévérité des logs générés par cette vérification a été revu pour être cohérent avec le niveau de sévérité de l'information remontée.

Connexions UDP sortantes

Référence support : 192545CW

Le firewall applicatif SES Evolution traite désormais les connexions UDP sortant du poste de l'utilisateur de façon optimisée afin de ne plus ralentir l'émission de certains types de paquets réseau et de ne plus perturber de ce fait le fonctionnement de logiciels tiers.

Console d'administration

Utilisation simultanée de plusieurs consoles

La stabilité du serveur backend de SES Evolution a été améliorée pour supporter l'utilisation simultanée de plusieurs consoles d'administration.

Actions sur les périphériques

Toutes les actions réalisées dans le menu **Périphériques** de la console sont désormais journalisées dans les Logs système : ajouts de clés, modifications, suppressions, etc. De plus la liste des vendeurs et périphériques USB dans les politiques de sécurité a été mise à jour.

Création automatique d'identifiants d'application

Référence support : 172154PW

Lorsque vous ajoutez une exception sur un log généré par le déclenchement des protections avancées **Découverte de l'environnement** ou **Utilisations malveillantes de Certutil**, l'identifiant automatiquement créé dans la règle d'exception inclut désormais les enfants de l'application identifiée.

Nom du critère Ligne de commande dans les identifiants d'application

Référence support : 172856PW

Dans les identifiants d'application, lorsque vous ajoutez un critère Ligne de commande, le lien **Afficher plus** reste affiché dans le panneau principal de l'identifiant, même si le nom du critère est très long.

Challenges

Référence support : 201634CW

Un problème de fonctionnement du mécanisme des challenges a été corrigé.

Import de jeux de règles personnalisés

Référence support : 201083CW

Lors de l'import d'un jeu de règles dans une politique de sécurité, il n'est désormais plus possible d'écraser un jeu de règles partagé avec un jeu de règles privé, sauf si vous avez supprimé le premier de la console.

De plus, lorsque vous supprimez un jeu de règles, il reste présent en base de données. Ainsi, si vous importez un jeu personnalisé qui possède le même identifiant qu'un jeu supprimé, le numéro de version du jeu importé est incrémenté de un par rapport à la version du jeu supprimé.

Suppression des jeux de règles partagés

Référence support : 201151CW

Vous pouvez désormais restaurer un jeu de règles partagé supprimé, en restaurant une version ou une révision d'une politique ayant contenu ce jeu.

Protection Découverte de l'environnement

Référence support : 172473PW

La protection **Découverte de l'environnement** a été améliorée afin de réduire le nombre de faux positifs.

Surcharge de la base de données en cas d'échec d'insertion de logs de contexte d'incident

Référence support : 205490CW

Lorsqu'un agent génère des logs de contexte simple dans le cadre d'un incident, dorénavant si l'insertion de ces logs en base de données échoue, les nouvelles tentatives du gestionnaire d'agent de les insérer sont limitées les premiers jours. Elles sont ensuite abandonnées au bout de neuf jours. Un log système prévient alors l'utilisateur que les logs de contexte sont supprimés. Cette correction permet de ne plus surcharger de logs la base de données.

Version 2.4.0 non publiée

La version 2.4.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.3.2

Agent SES Evolution

Désinstallation de l'agent SES Evolution

Le nouvel outil *AgentRemovalTool.exe*, disponible sur votre espace client MyStormshield, permet de désinstaller un agent SES Evolution lorsque la désinstallation standard n'est pas possible. Il fonctionne via le mode sans échec de Windows. L'outil est compatible avec toutes les versions de l'agent. Il sera mis à jour régulièrement afin de rester compatible.

En savoir plus

Correctifs de SES Evolution 2.3.2

Centre d'installation

Amélioration de l'installation de démonstration

Lors de la configuration des paramètres d'authentification dans l'installation de démonstration, le centre d'installation pouvait générer une erreur dans certains cas. Ce problème est résolu.

Agent SES Evolution

Branchement d'un périphérique USB sur station blanche

Dans certains cas, le niveau de confiance maximum ne pouvait être accordé à un périphérique USB sur une station blanche en raison d'un problème de droits d'accès. Ce problème est résolu.

Vérification de l'intégrité et réparation des agents

Référence support : 199298CW

La vérification de l'intégrité des agents et leur réparation par le service EsaUpdateSvc ont été améliorées et la réparation ne se déclenche maintenant que lorsque cela est nécessaire.

Compatibilité avec les logiciels de contrôle des périphériques

Référence support : 197055CW

Dans le cas de l'installation ou de la mise à jour de l'agent, la compatibilité avec des logiciels de contrôle des périphériques tiers a été améliorée.

Arrêt des processus de l'agent

Références support : 197090CW, 197091CW et 197092CW

Les logs remontés lorsque les processus permettant d'interagir avec l'agent SES Evolution (*EsSetup.exe* et *EsGui.exe* par exemple) s'arrêtent, comportent désormais le niveau de gravité Remarque. Auparavant, ils comportaient le niveau Erreur.

Autoprotection de l'agent

L'autoprotection de l'interface de l'agent a été nettement améliorée. Il est fortement recommandé d'installer cette nouvelle version.

Console d'administration

Téléchargement d'une politique depuis le serveur de mise à jour public Stormshield

Il est désormais possible de télécharger de nouveau une politique de sécurité intégrée disponible sur le serveur de mise à jour public Stormshield et de l'installer dans la console d'administration, même si celle-ci avait déjà été installée auparavant puis avait été supprimée de la console.

Communication entre la console et le serveur backend

Référence support : 199390CW

Le délai maximal du temps de réponse lorsque la console d'administration envoie des requêtes au serveur backend a été rallongé afin d'éviter des faux logs d'erreur et de réduire le volume de logs système.

Centre d'installation et console d'administration

Option Garder les logs indéfiniment

Il est de nouveau possible de cocher l'option **Garder les logs indéfiniment** dans le Centre d'installation et dans l'onglet **Système** de la console d'administration. Cette option est disponible uniquement avec l'utilisation de SQL Server Enterprise.

Librairies tierces

Mise à jour de la librairie Yara

La librairie Yara utilisée par Stormshield a été mise à jour en version 4.2.3 car cette version corrige une vulnérabilité.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.3.1

Protection du parc renforcée

Intégration de l'outil d'analyse Yara

SES Evolution intègre désormais l'outil d'analyse Yara. Il se base sur des règles permettant de détecter des schémas binaires ou textuels dans des fichiers ou des processus en cours d'exécution. Grâce à cette reconnaissance de schémas connus, les menaces ou attaques visant des postes de travail sont identifiées. L'administrateur peut ainsi mettre en place des actions de remédiation.

Les analyses Yara peuvent être déclenchées lorsqu'une règle de sécurité détecte ou bloque un comportement inhabituel. Mais vous pouvez également déclencher des analyses Yara manuellement, à tout moment, pour surveiller un ou plusieurs agents à la demande. Vous avez également la possibilité de planifier ces analyses par groupe d'agents, à intervalles réguliers et pendant une durée définie.

Yara est un outil libre et vous pouvez vous aider de la documentation Yara en libre accès sur Internet pour concevoir les règles. En fonction de l'actualité, Stormshield proposera également des règles Yara afin de détecter les nouvelles menaces potentielles.

En savoir plus

Ressources Stormshield

Mises à jour automatiques des politiques et jeux de règles

Lorsque vous installez une nouvelle version de SES Evolution, elle contient les versions les plus récentes des politiques de sécurité intégrées et des jeux de règles intégrés. Cependant Stormshield peut publier une mise à jour de l'une de ces ressources indépendamment d'une version afin de réagir rapidement face aux nouvelles menaces ou aux évolutions des produits tiers. Vous pouvez désormais accéder facilement à ces mises à jour depuis la console et choisir de les installer automatiquement. Le nouveau panneau de téléchargement des ressources est accessible par l'icône  .

Les ressources sont par défaut disponibles sur le serveur public Stormshield. Vous pouvez également paramétrer un serveur local de votre choix si vous travaillez dans un environnement déconnecté du réseau Internet.

Des descriptions détaillent les changements apportés dans les nouvelles versions des politiques et jeux de règles. Ces descriptions sont disponibles en français et en anglais uniquement.

En savoir plus

Nouvelles protections

Protection Usurpation de processus parent (Parent PID Spoofing)

La nouvelle protection contre l'usurpation de processus parent est disponible dans l'onglet **Menaces** d'un jeu de règles de protection. Elle empêche le démarrage de programmes qu'un

attaquant déclarerait comme enfants de processus existants arbitrairement choisis.

Nouveaux jeux de règles partagés II 901

Les jeux de règles suivants ont été ajoutés dans les jeux partagés dans la console d'administration. Ils permettent de protéger les systèmes d'informations sensibles, conformément à l'Instruction Interministérielle française n° 901, élaborée par l'ANSSI. Ces cinq jeux sont des modèles. Pour les utiliser, vous devez les adapter à votre environnement en les dupliquant dans vos politiques.

II901 - Modèle de durcissement des applications courantes
II901 - Modèle de durcissement des périphériques courants
II901 - Modèle de durcissement des programmes utilisant des services réseau
II901 - Modèle de durcissement des programmes offrant des services réseau
II901 - Modèle de durcissement pour stations blanches USB

De plus, les nouveaux jeux de règles partagés suivants peuvent être téléchargés depuis votre espace personnel MyStormshield ou sur le serveur public Stormshield :

Protection contre l'utilisation malveillante des LOLBIN	Ce jeu de protection empêche les attaquants d'utiliser certains binaires Microsoft de type LOLBIN de façon malveillante.
Blocage des applications malveillantes connues	Ce jeu de protection bloque le démarrage des applications malveillantes connues, identifiées par hash ou certificat.
Surveillance des pilotes malveillants ou vulnérables	Ce jeu d'audit alerte lorsqu'un pilote malveillant ou vulnérable est chargé.

En savoir plus

Modification des jeux de règles existants

Des jeux de règles intégrés existants ont été modifiés. SES Evolution 2.3.1 inclut les jeux de règles v2.3.2.2208a.

Pour connaître les détails de ces modifications, reportez-vous au document *Notes de version des jeux de règles Stormshield* dans le menu **Téléchargements** de votre espace personnel Mystormshield.

Consultez les Préconisations pour connaître nos recommandations concernant la mise en œuvre des politiques de sécurité.

Surveillance de l'activité

Regroupement des logs similaires

Lorsque des événements similaires se produisent sur un ou plusieurs agents, les logs générés s'affichent désormais de façon groupée dans le menu **Logs agents** de la console d'administration. Ceci permet de réduire considérablement le nombre de lignes de logs à consulter en cas de besoin, tout en distinguant facilement les logs groupés des logs isolés. De nombreux détails sont affichés dans les regroupements de logs, tels que les dates et heures des premiers et derniers logs.

Vous pouvez également ajouter des exceptions sur l'ensemble des logs d'un regroupement en une seule action.

En savoir plus

Liens de recherche Google et VirusTotal depuis les logs agents

Dans les détails d'un log émis par un agent, accessibles depuis le menu **Logs agents** de la console d'administration, deux nouveaux liens permettent de vérifier le caractère malveillant de chaque processus impliqué sur le moteur de recherche Google ou sur le site VirusTotal.

En savoir plus

Nouvelles informations dans les logs système

Les logs système indiquent désormais toutes les modifications concernant les groupes d'agents et les gestionnaires d'agents faites dans la console d'administration.

Versions de Microsoft Windows compatibles

Nouvelles compatibilités

SES Evolution supporte désormais les systèmes d'exploitation Windows Server Core 2012 R2, 2016, 2019 et 2022 pour tous ses composants sauf la console d'administration.

Politiques de sécurité

Activation du mode "Détection" sur les politiques et jeux de règles

SES Evolution propose un mode "Détection" pour les politiques de sécurité et jeux de règles. Lorsque ce mode est activé, les agents ne bloquent pas les opérations mais émettent des logs indiquant quelles opérations auraient été bloquées par une règle. Ainsi vous pouvez tester facilement des politiques de sécurité ou des jeux de règles sur un parc avant de les mettre en production et sans bloquer les utilisateurs, afin de vérifier les impacts des restrictions et de procéder à des ajustements.

Vous pouvez activer le mode "Détection" sur une politique complète dans les paramètres d'un groupe d'agents, ou bien sur un jeu de règles à l'unité dans une politique.

En savoir plus

Périphériques

Filtrage des périphériques USB au démarrage du poste de travail

Les règles de sécurité permettant de contrôler l'usage des périphériques USB s'appliquent désormais dès le démarrage du poste de travail, avant l'ouverture de la session Windows.

En savoir plus

Console d'administration

Aide contextuelle

La documentation de la solution SES Evolution est désormais accessible de façon contextuelle depuis les panneaux de la console d'administration.

Versions des jeux de règles et protections avancées

Lorsqu'une politique utilise des jeux de règles ou des protections avancées qui ne sont pas dans leur version la plus récente, un nouvel indicateur visuel s'affiche dans la console. Un bouton sur la ligne d'un jeu de règles concerné permet de mettre à jour le jeu facilement.

En savoir plus

Utilisation du tableau de bord

Vous pouvez désormais naviguer depuis le tableau de bord vers les panneaux de la console grâce à plusieurs liens répartis sur les graphes, icônes et textes du tableau de bord.

En savoir plus

Copier-coller de règles

Il est possible de copier et coller des règles entre jeux de même type (audit ou protection) et entre politiques.

Duplication d'un groupe d'agents

Dans la console d'administration, vous pouvez dupliquer un groupe d'agents existant pour créer un nouveau groupe. Le groupe dupliqué conserve tous les paramètres du groupe d'origine mais ne contient pas d'agent.

Correctifs de SES Evolution 2.3.1

Centre d'installation

Version minimale de SQL Server

Le Centre d'installation refuse désormais d'installer ou de mettre à jour SES Evolution si votre version de SQL Server est inférieure à la version minimale requise, soit SQL Server 2017 Cumulative Update 25 (14.0.3401.7).

Console d'administration

Connexion avec le backend

Référence support : 194069CW

La configuration de la console d'administration a été modifiée afin de conserver et réutiliser au maximum les connexions TCP. Cela réduit légèrement le trafic réseau et la latence de la console.

Agents SES Evolution

Affichage de l'interface de l'agent

Les commandes *EsGui.exe* et *EsGui.exe /ShowPanel* affichent désormais correctement l'interface de l'agent, même lorsque celle-ci est déjà lancée mais non visible.

Fichier d'export des agents

Référence support : 167578PW

Dans la console d'administration, l'export dans un fichier *.csv* des informations sur les agents a été amélioré :

- Il contient des titres de colonne qui facilitent la lecture,
- Les colonnes du fichier *.csv* correspondent aux informations visibles dans la liste des agents de la console d'administration,
- Il est possible de sélectionner le type de séparateur (virgule, point-virgule ou tabulation).

Politiques de sécurité

Protection Élévation de privilèges

Référence support : 192169CW

La protection d'élévation de privilèges ne génère plus de logs lorsqu'un utilisateur sans droit d'administration tente de désinstaller une application.

Version d'un jeu de règles

Après un déploiement, un jeu de règles affiche toujours quelle version du jeu a été déployée. En revanche, en mode "modification", un jeu de règles configuré sur **Toujours utiliser la dernière version** conserve désormais ce paramètre et n'affiche plus la version déployée.

Logs agents

Filtre Application

Référence support : 189842CW

Le filtre **Application** des logs agents a été scindé en deux filtres : **Application** et **Application cible**, afin de différencier les applications qui ont effectué l'action de celles sur lesquelles l'action a été appliquée.

Récupération des logs agents

Référence support : 193939CW

Les requêtes de récupération des logs agents ont été améliorées afin de réduire le délai d'affichage dans la console d'administration.

Ajout d'une exception sur un log déclenché par une règle d'accès aux fichiers

Référence support : 197182CW

La création d'une règle d'exception à partir de certains logs déclenchés par une règle contrôlant l'accès aux fichiers ne provoque désormais plus d'erreur d'application de la politique de sécurité après un nouveau déploiement sur les agents.

Périphériques de stockage USB

Affichage dans la console d'administration

Références support : 192880CW - 193078CW

Lorsqu'un périphérique USB est branché sur un agent et que son enrôlement échoue, il s'affiche désormais dans la console d'administration de SES Evolution. Son niveau de confiance est de 0.

Logs liés aux périphériques USB

Référence support : 183857CW

Lorsque les informations sur le nom du constructeur et le nom du produit sont manquantes, elles ne sont plus affichées avec la valeur *<NULL>* dans SES Evolution. Elles sont désormais remplacées par l'ID du constructeur et l'ID du produit.

Version 2.3.0 non publiée

La version 2.3.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités et améliorations de SES Evolution 2.2.3

Agents

Prise de traces via un script

En cas de problème sur un poste de travail, il est désormais possible de démarrer une prise de traces via un script, en lançant le programme EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) avec l'option de ligne de commande `/StartDiagnostic`.

Vous pouvez indiquer le nom du fichier de traces final : `EsGui.exe /StartDiagnostic /DiagnosticFile <path\to\file.cab>`.

Vous pouvez également arrêter la prise de traces : `EsGui.exe /StopDiagnostic`.

En savoir plus

Déploiement des agents via une stratégie de groupe

Stormshield met désormais à disposition sur votre espace client MyStormshield un script PowerShell permettant de déployer des agents SES Evolution sur un parc via une stratégie de groupe (GPO). Retrouvez-le dans la rubrique Téléchargements > Stormshield Endpoint Security > Evolution > Tools.

En savoir plus

Modification des jeux de règles existants

Des jeux de règles intégrés existants ont été modifiés. SES Evolution 2 inclut les jeux de règle v2.2.3.2204a.

Pour connaître les détails de ces modifications, reportez-vous au document *Notes de version des jeux de règles Stormshield* dans le menu **Téléchargements** de votre espace personnel Mystormshield.

Consultez les Préconisations pour connaître nos recommandations concernant la mise en œuvre des politiques de sécurité.

Correctifs de SES Evolution 2.2.3

Compatibilité avec les produits tiers

Compatibilité avec Windows Sandbox

Référence support : 192983CW

Une incompatibilité entre SES Evolution et Windows Sandbox provoquant un écran bleu (BSOD) a été corrigée.

Logs

Baisse de la sévérité

Référence support : 189040CW

SES Evolution émet des logs lorsque des composants backoffice accèdent à une clé de registre connue pour permettre l'injection de DLL. La sévérité de ces logs a été baissée du niveau Remarque au niveau Information.

Mise à jour ou réparation de l'agent

Référence support : 168746PW

Dans l'interface de l'agent, le log indiquant qu'une mise à jour ou une réparation de l'agent s'est terminée avec succès a été modifié pour indiquer qu'un redémarrage est nécessaire pour finaliser l'opération.

Agents SES Evolution

Démarrage du poste de travail

Référence support : 191475CW

Les processus SES Evolution *EsaRulesEngDrv* et *EsaKrnlCtrlDrv* ne provoquent plus d'écran bleu (BSOD) au démarrage de certains postes de travail.

Modification de l'identifiant de l'agent

L'exécutable *EsSetup.exe* accepte désormais l'option « /newagentid » ou « -newagentid » afin d'abandonner l'identifiant unique de l'agent déjà installé. Un nouvel identifiant unique est alors attribué à l'agent lorsque ce dernier récupère un nouveau certificat de communication auprès d'un gestionnaire d'agents.

Mise à jour de l'agent

Dans certains cas, le démarrage du poste de travail pouvait être fortement ralenti. Le lancement des différents services de l'agent a été optimisé pour réduire ce délai.

Retour à une version antérieure

Pour permettre le retour vers une version antérieure de l'agent en cas de problème, des modifications ont été apportées dans la version 2.2.3 afin que le retour soit possible depuis les futures versions de SES Evolution.

Déblocage de l'agent

Référence support : 192599CW

Le système d'autoprotection des agents a été amélioré afin de permettre le déblocage des agents non connectés et possédant une politique de sécurité très restrictive.

Périphériques USB

Visualisation des périphériques USB dans la console

Référence support : 193035CW

Lorsqu'un périphérique USB était manuellement supprimé de la console d'administration mais non débranché du poste de travail, le périphérique s'affichait de nouveau dans la liste lorsque l'utilisateur débranchait le périphérique. Ce problème est résolu.

Un périphérique USB supprimé de la console, s'affichera bien de nouveau dans la console lors de sa prochaine réinsertion.

Nouvelles fonctionnalités de SES Evolution 2.2.2

Nouvelles protections

Protection anti-ransomware

SES Evolution 2.2.2 protège désormais 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 et de les arrêter rapidement.

Dans ce cadre, SES Evolution fournit un nouveau jeu de règles "Protection anti-ransomware". Il est disponible dans les jeux de règles partagés et est inclus dans la Politique par défaut. Une règle de protection contre les ransomware figure également dans l'onglet **Menaces** des jeux de règles.

Dans le cas où le ransomware a modifié ou chiffré des fichiers avant le blocage de l'attaque, SES Evolution fournit une liste de ces fichiers afin de vous aider à les restaurer. Dans ce même but, SES Evolution propose aussi désormais un mécanisme de création et de protection de clichés instantanés Windows décrit dans les points suivants.

En savoir plus

Protection des clichés instantanés Windows

Microsoft Windows propose un mécanisme de sauvegarde des données en permettant la création de clichés instantanés (*shadow copy* en anglais) des volumes NTFS locaux d'un poste de travail. En cas de perte de données, ces clichés permettent de les restaurer.

Désormais, SES Evolution détecte et bloque les suppressions ou corruptions de clichés instantanés sur les postes de travail. Ce comportement malveillant est souvent l'une des premières actions exécutées par les ransomware.

Enregistrement de clichés instantanés Windows

SES Evolution permet également d'enregistrer des clichés instantanés de votre parc. Chaque agent SES Evolution crée alors un cliché par jour par volume NTFS local sur les postes protégés. Les cinq derniers clichés sont conservés.

Pour utiliser cette fonctionnalité, vous devez avoir auparavant autorisé la création de clichés instantanés pour tous les volumes NTFS sur les postes de travail et vous assurer qu'ils disposent d'espaces réservés suffisants.

En savoir plus

Mise à jour de la Politique par défaut

La Politique par défaut a été enrichie avec le nouveau jeu de règles de protection contre les ransomware.

Lors d'une mise à jour de SES Evolution 2.1.x vers la version 2.2.2, consultez les Préconisations pour connaître la marche à suivre concernant la mise à jour des politiques.

En savoir plus

Nouveaux jeux de règles intégrés

En plus du jeu de règles "Protection anti-ransomware", les deux jeux de règles partagés suivants ont été ajoutés. Avant SES Evolution 2.2.2, les règles composant ces jeux étaient présentes dans le jeu de règles "Socle de protections" qui faisait partie de la Politique par

défaut. Elles ont été supprimées du Socle de protections pour constituer des jeux indépendants, disponibles dans les jeux partagés.

Durcissement des applications courantes	Le jeu permet de mieux maîtriser le comportement des applications courantes qui pourrait être parfois dangereux même s'il n'est pas d'origine malveillante.
Durcissement des accès au réseau	Le jeu permet de mieux maîtriser les applications qui pourraient engendrer du trafic réseau non souhaité.

En savoir plus

Modification des jeux de règles existants

Des jeux de règles intégrés existants ont été modifiés et enrichis. Pour connaître les détails de ces modifications, reportez-vous au document *Notes de version des jeux de règles Stormshield* sur votre espace personnel MyStormshield.

Consultez les Préconisations pour connaître nos recommandations concernant la mise en œuvre des politiques de sécurité.

Versions de Microsoft Windows compatibles

Nouvelles compatibilités

SES Evolution supporte désormais les systèmes d'exploitation Windows 10 21H2, Windows 11 et Windows Server 2022.

Identifiants d'application

Filtrage des processus et applications par arguments de ligne de commande

Certaines applications peuvent être utilisées légitimement sur un parc par vos administrateurs, mais également de manière malveillante par des attaquants.

Afin de mieux maîtriser l'utilisation des applications, SES Evolution permet désormais de filtrer leurs actions plus finement en fonction des paramètres de leur ligne de commande. Ces paramètres peuvent être spécifiés en tant que critères dans les identifiants d'applications. Cela permet d'appliquer des règles différentes à une même application selon l'usage qui en est fait. Par exemple, vous pouvez bloquer l'exécution de PowerShell uniquement lorsqu'il est exécuté de manière cachée ou lorsque ses paramètres de ligne de commande tentent de contourner des politiques d'exécution Windows.

En savoir plus

Déploiement de configuration

Indicateur de déploiement

La console SES Evolution affiche maintenant un indicateur visuel en face du menu **Environnement** signalant que vous avez modifié la configuration et qu'un déploiement sur le parc d'agents est nécessaire.

En savoir plus

Surveillance de l'activité

Navigation entre les logs et les règles d'exceptions

Dans le panneau des logs des agents de la console d'administration, un nouveau bouton vous permet de vous rendre directement sur une règle d'exception créée à partir d'un log, si vous avez besoin de la consulter ou de la modifier.

Configuration des serveurs

Surveillance de l'espace disque

Dans la console SES Evolution, le tableau de bord indique désormais l'espace disque utilisé sur les serveurs hébergeant les backends, les gestionnaires d'agents et les bases de données. Vous êtes averti lorsque certains seuils d'occupation sont atteints. Cette surveillance vous permet d'anticiper des problématiques d'espace disque et donc d'assurer la continuité des services.

En savoir plus

Console d'administration

De nouvelles fonctionnalités ont été ajoutées dans la console d'administration pour faciliter la gestion des politiques et des règles :

- Si vous souhaitez exporter des politiques ou jeux de règles, vous pouvez maintenant choisir les éléments à exporter. Ils seront exportés dans des fichiers séparés.
- Le nombre de règles existantes est maintenant affiché sur chaque onglet des différents types de règles dans un jeu.
- Lorsque vous sélectionnez des jeux de règles partagés à ajouter dans une politique, ils sont dorénavant ajoutés dans l'ordre de la sélection.
- Vous avez maintenant la possibilité de copier/couper/coller des règles dans un même jeu de règles.

Icône de l'agent sur les postes de travail

Changement de l'icône de l'agent dans la barre des tâches

Sur les postes de travail, l'ancienne icône de l'agent a été remplacée par l'icône dans la barre des tâches.

Correctifs de SES Evolution 2.2.2

Politiques de sécurité

Création d'exception depuis un log de type "Découverte de l'environnement"

Référence support : 167745PW

Dans la console d'administration, il est désormais possible de créer une règle d'exception à partir d'un log déclenché par la protection avancée "Découverte de l'environnement".

Modification du type de volume dans un identifiant d'application

Référence support : 167477PW

Lorsqu'on supprimait le critère **Type de volume** d'un identifiant et qu'on ajoutait de nouveau ce critère dans le même identifiant, il n'était pas possible de modifier les paramètres du critère. Ce problème est résolu.

Import et export de jeux de règles

Référence support : 168385PW

Lors de l'import d'un fichier *.cab* dans le panneau des jeux de règles partagés, un message d'erreur s'affiche lorsque le fichier ne contient pas de jeux partagés. Le message a été amélioré pour indiquer la cause de l'erreur.

Lors de l'export d'un jeu de règles, le nom du fichier d'export précise maintenant s'il s'agit d'un jeu partagé ou privé.

Logs agents dans la console d'administration

Recherche d'agents

Référence support : 167508PW

Dans le panneau des **Logs agents**, la recherche via la colonne **Agent** permet désormais de rechercher parmi tous les agents, et pas seulement parmi la liste affichée dans cette colonne.

Caractères spéciaux et accentués dans le nom des groupes d'agents

Référence support : 167581PW

Dans le panneau des **Logs agents**, les caractères spéciaux ou accentués s'affichent désormais correctement dans la colonne **Groupe d'agents**.

Affichage des logs dans la console

Référence support : 188215CW

Lorsque les logs émis par une règle étaient paramétrés pour ne jamais être affichés sur la console, ils étaient affichés quand même. Le paramétrage fonctionne désormais correctement.

Filtres avancés des logs

Dans les filtres avancés du panneau des **Logs agents**, la touche Entrée ne provoque plus à tort l'ajout d'une ligne supplémentaire, ni la validation automatique du formulaire de saisie.

Logs remontés par des événements d'autoprotection

Référence support : 167586PW

Dans le panneau des **Logs agents**, le bouton **Consulter la règle** n'est désormais plus disponible pour les logs remontés par des événements d'autoprotection, étant donné qu'il n'y a pas de règle correspondante.

Nom d'utilisateur dans les incidents

Référence support : 189879CW

Dans le panneau des **Logs agents**, le nom de l'utilisateur est désormais affiché dans la colonne **Agent** des incidents, comme c'était déjà le cas pour les logs standard.

Gestion des groupes d'agents

Filtrage des agents par groupes d'agents

Dans le menu **Agents** de la console d'administration, le filtre **Groupe par défaut** dans le champ **Groupe** affiche maintenant toujours les agents du groupe par défaut après un changement de la langue de l'interface.

Application des politiques de sécurité conditionnelles

Référence support : 168192PW

Dans la configuration des groupes d'agents, l'ordre d'application des politiques conditionnelles utilisant des scripts en tant que condition d'application est maintenant bien respecté.

Mode Maintenance désactivé

Lorsque le mode Maintenance n'est pas autorisé dans la configuration des groupes d'agents, le bouton d'activation du mode Maintenance dans les paramètres avancés de l'onglet **Préférences** de l'agent est désormais grisé.

Déploiement de l'environnement

Délai d'attente après une erreur de déploiement

Référence support : 189042CW

Dans le cas où un problème survient pendant un déploiement de l'environnement et que celui-ci s'arrête, il faut désormais attendre 15 minutes avant de pouvoir déployer de nouveau. Auparavant le délai d'attente était de 30 minutes.

Agents SES Evolution

Optimisations des performances

Référence support : 187968CW

L'impact de l'agent SES Evolution sur les performances du lancement de processus a été optimisé, ce qui permet notamment d'améliorer la compatibilité avec le SDK Xilinx.

Références support : 185692CW et 186425CW

La protection de l'accès à la base de registre et l'identification des processus ont été améliorées afin de ne plus dégrader les performances des postes de travail.

Mise à jour de l'agent SES Evolution

Référence support : 186717CW

La recherche de mises à jour depuis l'interface de l'agent ne provoque plus d'erreur et fonctionne désormais correctement.

Suppression des logs

Référence support : 167479PW

Les logs SES Evolution sont désormais correctement supprimés du disque des postes de travail au bout du nombre de jours indiqués dans la configuration du groupe de l'agent.

Blocage des processus EsUpdate et EsUpdateHost

Référence support : 167481PW

Désormais les processus EsUpdate et EsUpdateHost ne sont plus bloqués sur le port 80 par le mécanisme d'autoprotection de SES Evolution.

Compatibilité avec Microsoft Excel

Référence support : 186764CW

La protection contre les enregistreurs de frappe n'occasionne plus d'arrêt inopiné de Microsoft Excel.

Amélioration des performances lors du branchement d'un périphérique USB sur une station blanche

Référence support : 187720CW

Une incompatibilité avec la protection en temps réel de Windows Defender déclenchée lors du branchement d'un périphérique USB sur une station blanche engendrait une lenteur du poste. Cette incompatibilité a été corrigée.

Compatibilité avec Microsoft PowerPoint

Référence support : 188228CW

SES Evolution n'occasionne plus de fermeture inopinée de Microsoft PowerPoint à la sortie de la mise en veille prolongée du poste de travail.

Gestionnaires d'agents

Fuseaux horaires

Référence support : 189338CW

Un problème lié aux fuseaux horaires sur la machine du gestionnaire d'agents pouvait bloquer le traitement des logs et leur enregistrement dans la base de données. Ce problème a été corrigé.

Version 2.2.1 non publiée

La version 2.2.1 n'est pas disponible publiquement.

Version 2.2.0 non publiée

La version 2.2.0 n'est pas disponible publiquement.

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/.

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 de 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 la 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 Evolution détectait 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 caractères 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 connaissances 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/.