



ISOLER UN POSTE DE TRAVAIL AVEC LE FIREWALL SES

Produits concernés : SES Date : 29 novembre 2018 Référence : ses-fr-how_to-isoler_un_poste_de_travail





Table des matières

| Isoler un poste de travail avec le firewall SES | 3 |
|---|-----|
| Comprendre le mécanisme de déclenchement d'action sur détection d'événement | 3 |
| Créer la politique de sécurité et le test dans les ressources de scripts | 4 |
| Créer le script Visual Basic et le télécharger sur le poste de travail | 6 |
| Créer les scripts d'isolation et de fin d'isolation | 6 |
| Assigner les scripts d'isolation et de fin d'isolation | . 7 |
| Script "start quarantine" | 7 |
| Script "end quarantine" | 8 |

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



Isoler un poste de travail avec le firewall SES

Ce document s'applique aux versions 7.2.11 et supérieures de Stormshield Endpoint Security.

Il donne un exemple de comment isoler un poste de travail du réseau en cas d'attaque : une tentative de "heap spray" par exemple.

Pour atteindre cet objectif, une des possibilités est d'utiliser le déclenchement automatique d'actions lorsque l'agent SES détecte un événement donné.

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

Comprendre le mécanisme de déclenchement d'action sur détection d'événement

<u>Prérequis :</u> pour que l'agent soit capable de détecter la tentative de "heap spray", la protection contre les débordements mémoire doit être activée dans la politique de sécurité en vigueur sur le poste de travail (onglet *Comportement système*, menu **Contrôle du comportement du système** de la politique de sécurité).

En résumé, lorsque l'agent SES détecte un événement donné, son comportement est le suivant :



Actions de l'agent SES sur détection d'événement

| 1 | Détection |
|-------------|---|
| Agent SES | Une tentative de "heap spray" est détectée sur un poste de travail du parc de l'entreprise. |
| | Actions |
| Corsole SIS | Un log de type Logiciel de blocage de "heap spray" remonte dans la console SES. Un script SES précédemment associé à ce type de log dans le menu Configuration des logs de la console SES est automatiquement exécuté. |
| 7 | Actions |
| 3 | Ce script crée un fichier « quarantine.protected » sur le poste de travail affecté et force l'agent à revérifier les conditions indiquées dans les politiques liées à l'objet de l'annuaire auquel il appartient. L'agent détecte la présence de ce fichier « quarantine.protected » et applique alors immédiatement la politique de sécurité de quarantaine préalablement définie par l'administrateur. |
| | Le script SES lance également l'exécution d'un script Visual Basic permettant de récupérer sur la machine des informations sur l'événement ayant déclenché l'isolation et d'arrêter le processus incriminé. |
| 4 | Actions |
| Utilisateur | Lorsque le problème est résolu sur la machine, l'utilisateur du poste de travail demande à l'administrateur une restauration de la politique précédente afin de mettre fin à l'isolation du poste, via un challenge. |

Consultez la suite du document pour les détails de la mise en place de chaque étape. Il s'agit d'un exemple, que vous pourrez adapter à d'autres situations du même type.

Créer la politique de sécurité et le test dans les ressources de scripts

 Dans Gestion des environnements > Politiques > Sécurité, créez une politique de sécurité nommée "quarantine". La politique suivante par exemple isole le poste de travail du réseau et autorise seulement les communications agent/serveur (implicitement) :

| 📽 Network security control | N | etwo | ork Firewall / D | Defa | ult Group | | | | | | | |
|----------------------------|---|------|------------------|------|-----------|---|----------------|-------------|-----------|----------|--------------|---------------|
| General Settings | - | + - | × • 🖬 • | Ŧ | † ↓ | Ŧ | <u>+</u> + +++ | | | | | |
| Network Firewall | # | | Status | 5 | Action | + | Direction | 👤 Remote IP | P Over IP | Stateful | Y Local Port | Y Remote Port |
| WiFi Access Points | 0 | ~ | Enabled | 8 | Block | + | Outgoing | All | TCP [6] | 🔽 On | All | All |
| Default Group | 1 | ~ | Enabled | 8 | Block | + | Incoming | All | TCP [6] | 🔽 On | All | All |



 Dans Gestion des environnements > Politiques > Ressources de scripts, créez un test nommé "quarantine_file" qui vérifie l'existence d'un fichier "quarantine.protected" dans le répertoire de l'agent SES.

| Policies / Script Resources | |
|-----------------------------|---------------------------------------|
| ? Tests | |
| + × 🗹 土 | |
| quarantine_file | □ User-Defined Test : quarantine_file |
| | 🚊 🗠 🏠 IF AND |
| | File~Exist : quarantine.protected |
| | |
| | |

 Vous devez protéger ce fichier "quarantine.protected" afin qu'il ne soit pas supprimé ou modifié par des applications tierces ou par l'utilisateur. Pour cela, créez une règle d'extension dans la politique de sécurité nommée "quarantine". Ne spécifiez pas d'identifiant d'application.

| ystem Behavior Device Control N | etwork security control | Application Control Lin | iks | | | | |
|-------------------------------------|-------------------------|---------------------------------|------------------|-------|-------------|------|------------|
| Application Control | Extension Rules | / Default Group | | | | | |
| General Settings | + • × • 🖻 | - - + + - | <u>+</u> - | | | | Q- All |
| Applicative rules Default Group | # 🗹 Status | Extension | \star Identifier | 🗎 Log | Description | | Group |
| Extension Rules | 0 🗹 Enabled | protected | | | | Defa | ault Group |
| Default Group | | | | | | | |
| Trusted Rules | | | | | | | |

Tous les fichiers portant l'extension ".protected" sont ainsi protégés par Stormshield Endpoint Security.

4. Placez-vous sur votre **Environnement** et dans l'onglet *Politiques liées*, catégorie **Sécurité**, ajoutez la condition "quarantine file" et la politique "quarantine". Ainsi, si l'agent SES détecte le fichier "quarantine.protected" sur le poste de travail, il appliquera immédiatement la politique d'isolation du poste.

| 🖻 🖵 Dyna | niic Agent | com | guia | | | | | |
|--|---|-------------------------|--------|---|---|---|---|-------------------------------|
| + Add × | Remove | Ŧ | Ť | ÷ | Ŧ | | | |
| Link order | Condition | | | | | Policy Name | | Inherited from |
| 1 | (true) | | | | | DefaultDynamicAgentPolicy | 2 | Environment |
| 🗉 📮 Static Agent Configuration - 1 link | | | | | | | | |
| + Add × | Remove | 1 | 1 | + | + | | | |
| Link order | Condition | | | | | Policy Name | | Inherited from |
| 1 | (true) | | | | | DefaultStaticAgentPolicy | | Environment |
| | 🗉 🗘 Security - 2 links | | | | | | | |
| 🗆 🗘 Secur | rity - 2 links | 5 | | | | | | |
| □ ⑦ Secur + Add × | rity - 2 links Remove | 5 | t | Ŧ | Ŧ | | | 1 |
| O Secur Add × Link order | rity - 2 links Remove Condition | 5 | Ť | t | Ŧ | Policy Name | | Inherited from |
| O Secur Add × Link order | rity - 2 links Remove Condition quarantine | 5 ₮ e_file | Ť | t | + | Policy Name quarantine + | | Inherited from |
| O Secur Add × Link order 1 2 | rity - 2 links Remove Condition quarantine (true) | 5 ∓ e_file | Ť | t | + | Policy Name quarantine <i>DefaultSecurityPolicy</i> | | Inherited from Environment |
| Secur Add × Link order 1 2 Secur Secur | rity - 2 links Remove Condition quarantine (<i>true</i>) rption - 0 li | s ┲_file | Ť | ţ | • | Policy Name quarantine DefaultSecurityPolicy | | Inherited from Environment |
| O Secur Add × Link order 1 2 S Encry + Add × | ity - 2 links Remove Condition quarantine (<i>true</i>) ption - 0 li Remove | 5 a_file ink T | † t | + | • | Policy Name quarantine • DefaultSecurityPolicy | | Inherited from Environment |



Créer le script Visual Basic et le télécharger sur le poste de travail

Dans notre exemple d'isolation d'un poste de travail, nous utilisons un script Visual Basic permettant de récupérer des informations sur l'événement ayant déclenché cette isolation et d'arrêter le processus incriminé. Son exécution sera lancée par le script SES d'isolation du poste, comme décrit dans la section suivante.

🕦 NOTE

L'utilisation de ce script VB n'est pas obligatoire pour la mise en pratique de l'isolation du poste, mais il permet de maîtriser le problème sur le poste plus rapidement. Il est simplement donné ici à titre d'exemple.

Des variables d'environnement SES liées à l'événement en cause sont automatiquement communiquées au script VB ou à tout programme exécuté via le menu **Exécuter un programme** dans un script SES. Pour plus d'informations sur ces variables, reportez-vous à la section *Actions sur détection d'événements* dans le chapitre *Surveillance de l'activité > Éditeur de logs* du *Guide d'administration Stormshield Endpoint Security*.

- 1. Créez un script VB et nommez-le "ses_print_system.vbs".
- 2. Copiez le contenu de l'exemple de script fourni à la section Exemple de script Visual Basic. Cet exemple permet de récupérer des informations sur l'événement en cause à partir des variables d'environnement SES et les organise dans un fichier de log "quarantine.log" en les faisant précéder de la date et de l'heure. Il permet également d'arrêter le processus en cause sur la machine.
- 3. Dans la console SES, ajoutez le script VB dans Gestion des environnements > Politiques > Déploiement de fichiers, afin de transférer le fichier vers les agents. Pour plus d'informations sur le transfert de fichiers, reportez-vous à la section Transfert de fichiers vers les agents du chapitre Scripts du Guide d'administration Stormshield Endpoint Security.
- 4. Appliquez les changements à l'environnement.

Créer les scripts d'isolation et de fin d'isolation

Vous allez créer deux scripts dans **Gestion des environnements** > **Politiques** > **Script** : "start_ quarantine" et "end_quarantine".

- Le script "start_quarantine" permet de déclencher l'isolation du poste. Si le fichier "quarantine.protected" n'est pas déjà présent sur le poste de travail, le script :
 - crée le fichier "quarantine.protected" sur le poste de travail infecté, dans le répertoire de l'agent. La règle d'extension que vous avez définie précédemment le protège de toute modification ou suppression.
 - force l'agent à revérifier immédiatement les politiques qu'il doit appliquer, en fonction des conditions définies dans les **Politiques liées** (action "Réévaluer les politiques") et donc isole le poste de travail.
 - lance l'exécution du script Visual Basic décrit à la section précédente. N'oubliez pas l'extension "srn" du script VB, qui est rajoutée par Stormshield Endpoint Security lors du transfert de fichier.



affiche un message de notification à l'utilisateur pour lui indiquer que son poste est isolé.
 POLICIES / SCRIPT / start_quarantine (Version: 2)

| 🗹 Check Out 🛛 🏦 Export |
|--|
| Policy Links |
| ⊡ 📮 Script : start_quarantine, Modified On : 11/26/2018 10:32:39 AM |
| 🖨 🔅 IF AND |
| User-Defined Test : quarantine_file |
| 🖶 🖉 Result True |
| 🛐 Execution~Process : fsutil file createnew "quarantine.protected" 1:Synchronous |
| F Configuration~Review policies |
| 🛐 Execution~Process : cscript.exe /e:vbscript "uploaded\ses_print\system.vbs.srn":Asynchronous |
| Misc.~Message : Your workstation has been isolated from the network |
| 🖃 😳 Result False |
| Execution~Process : cscript.exe /e:vbscript "uploaded\ses_print_system.vbs.srn":Asynchronous |
| |

Si le fichier "quarantine.protected" est déjà présent sur le poste de travail, cela signifie que le poste est déjà isolé. Le script lance l'exécution du script Visual Basic décrit à la section précédente, afin de récupérer des informations sur l'événement déclencheur.

- Le script "end_quarantine" permet de mettre à fin à l'isolation du poste de travail une fois le problème résolu. Il :
 - supprime le fichier "quarantine.protected" sur le poste de travail infecté.
 - force l'agent à revérifier immédiatement les politiques qu'il doit appliquer, en fonction des conditions définies dans les **Politiques liées** (action "Réévaluer les politiques").



Assigner les scripts d'isolation et de fin d'isolation

Script "start_quarantine"

- 1. Dans Gestion des environnements > Éditeur de logs, sélectionnez les Logs Système.
- 2. Trouvez le log HSP_HEAP_BLK (pour l'exemple que nous décrivons ici).



3. Dans la colonne Script, sélectionnez le script "start quarantine" :

| 🖶 Log Manager | | | | | | |
|---------------|---|--|--|--|--|--|
| 🗹 Check In 🖷 | ▶ Undo CheckOut 🗘 Refresh | | | | | |
| Types | + × © · ∓ + ∓ ± ± | Q overflow | | | | |
| Software Logs | 🗹 🕈 Action 👔 Status 🏳 🗖 🛢 🛃 🗹 🏋 %SOURCE% 🦞 %DEST% | Y %OPTION% I Script = Descript | | | | |
| Network Logs | ☑ (#.)?OVERFLOW .*LIBC-BLK | * | | | | |
| Device Logs | ☑ (#.)?OVERFLOW .*HSP-HEAP-BLK Ø Ø Ø Ø Ø .*(<.*><.*>(.*>)? .* | .* start_quarantine | | | | |
| | ☑ (#.)?OVERFLOW KERNEL-DBG | * | | | | |

Ainsi, à chaque fois qu'une tentative de "heap spray" sera détectée et qu'un log sera remonté dans la console SES, le script sera exécuté et le poste de travail affecté sera immédiatement mis en quarantaine.

Script "end quarantine"

1. Dans Gestion des environnements > Politiques > Configuration statique de l'agent > Challenges, sélectionnez le script "end_quarantine" :

| VOLICIES / STATIC AGENT | CONFIGURATION / DefaultStaticAgentPolicy (Version: 2) |
|-------------------------------|---|
| 🗹 Check Out 🛛 🏦 Export | |
| Policy Links | |
| 🗆 🏟 Challenges | |
| Script 1 | end_quarantine |
| Script 2 | (none) |
| Script 3 | (none) |
| Script 4 | (none) |
| Script 5 | (none) |
| 🗉 🏟 Manage Update | |
| Update to deploy (ex: 7.2.23) | Limited by server |

- Lorsque le problème est résolu sur le poste de travail, demandez à l'utilisateur de vous fournir un code d'action (clic droit sur l'icône Stormshield sur le poste de travail, Autres opérations > Challenges).
- 3. Dans le menu **Outils** > **Gérer les challenges** de la console SES, sélectionnez le script dans **Type d'action** et conservez la durée par défaut **Jusqu'au redémarrage**.
- 4. Fournissez le code d'autorisation généré à l'utilisateur et redémarrez son poste de travail. Celui-ci a alors de nouveau accès au réseau.

Pour plus d'informations sur la gestion des challenges, reportez-vous à la section Édition de la politique de configuration statique de l'agent du chapitre Configuration de l'agent SES dans le Guide d'administration Stormshield Endpoint Security.





documentation@stormshield.eu

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

Copyright © Stormshield 2018. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.