HOW TO
STORMSHIELD ENDPOINT SECURITY

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

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.

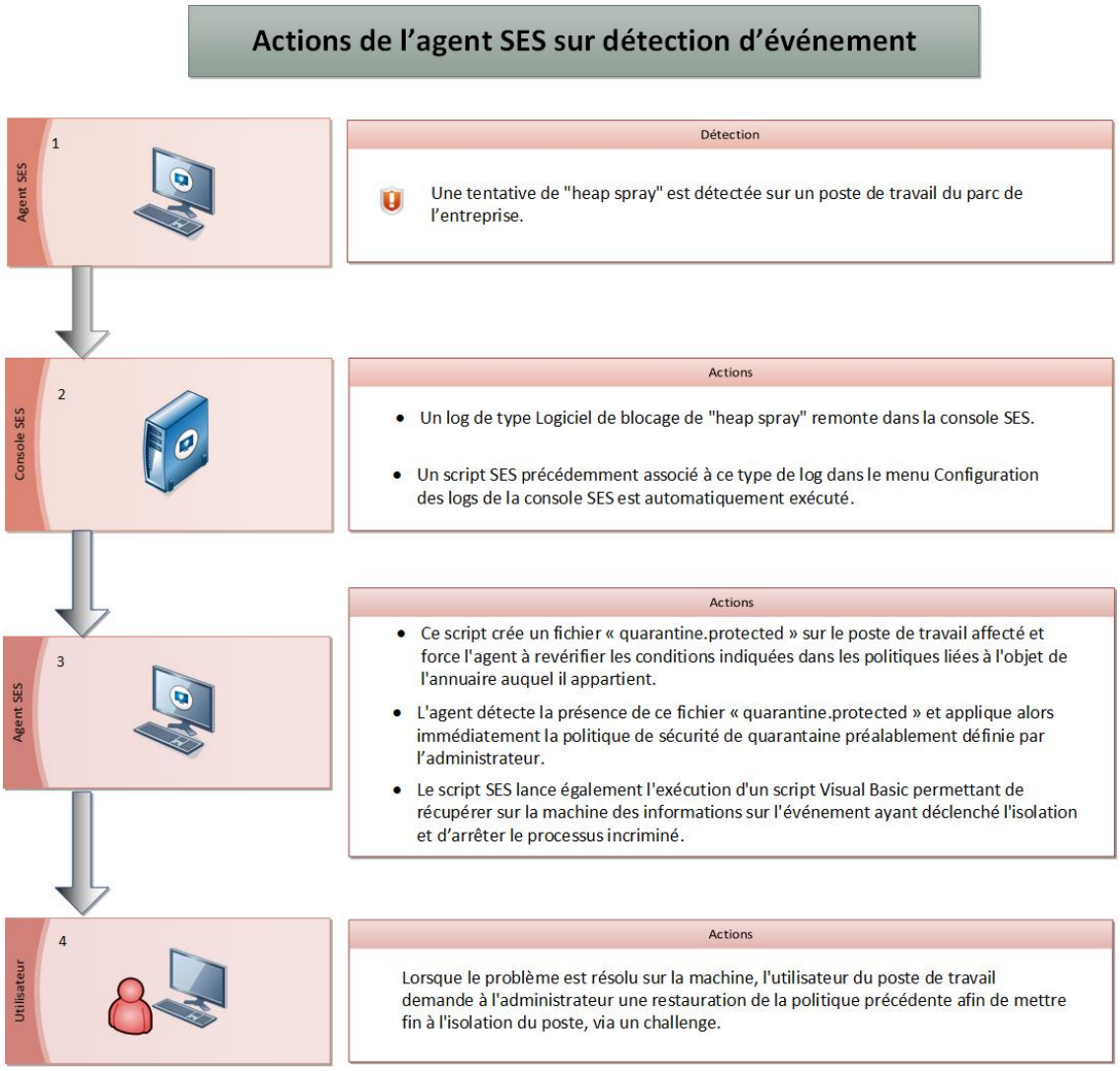
Pour atteindre cet objectif, une des possibilités est d'utiliser le déclenchement automatique d'actions lorsque l'agent SES détecte un événement donné.

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

Prérequis : 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).

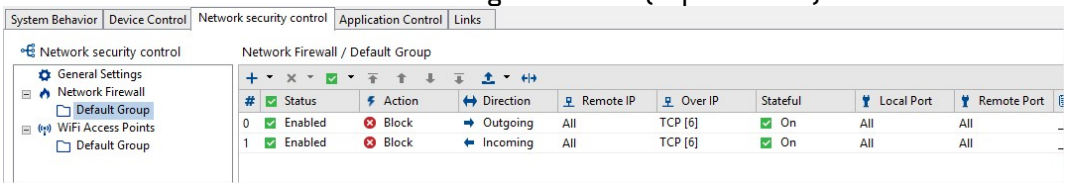
En résumé, lorsque l'agent SES détecte un événement donné, son comportement est le suivant :



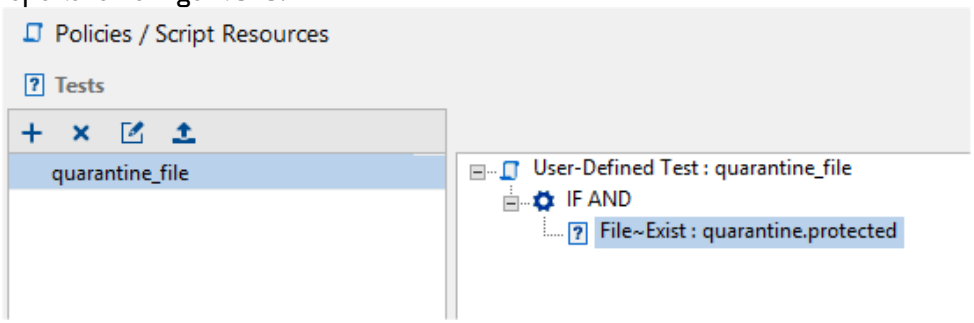
Consultez la suite du document pour les détails de la mise en place de chaque étape. Il s'agit d'un exemple, que vous pourrez adapter à d'autres situations du même type.

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

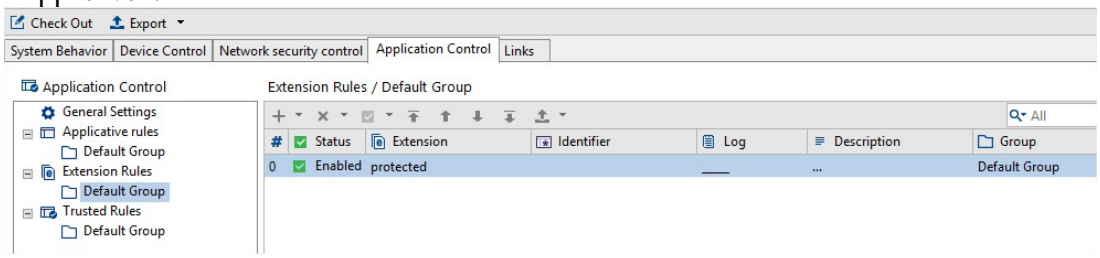
1. Dans **Gestion des environnements** > **Politiques** > **Sécurité**, créez une politique de sécurité nommée "quarantine". La politique suivante par exemple isole le poste de travail du réseau et autorise seulement les communications agent/serveur (implicitement) :



2. 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.

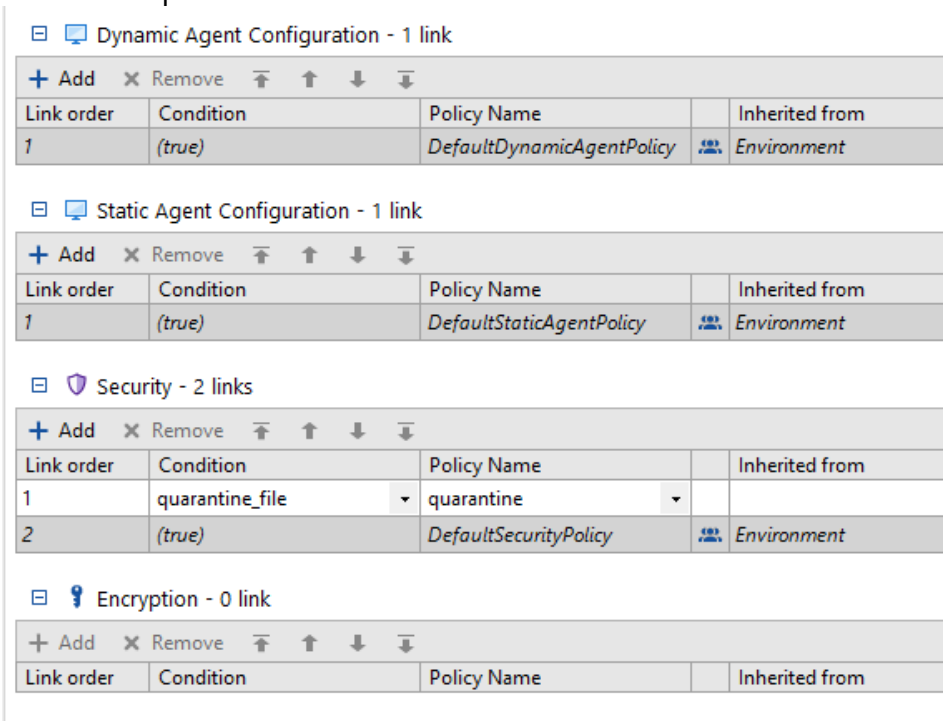


3. Vous devez protéger ce fichier "quarantine.protected" afin qu'il ne soit pas supprimé ou modifié par des applications tierces ou par l'utilisateur. Pour cela, créez une règle d'extension dans la politique de sécurité nommée "quarantine". Ne spécifiez pas d'identifiant d'application.



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.



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*.

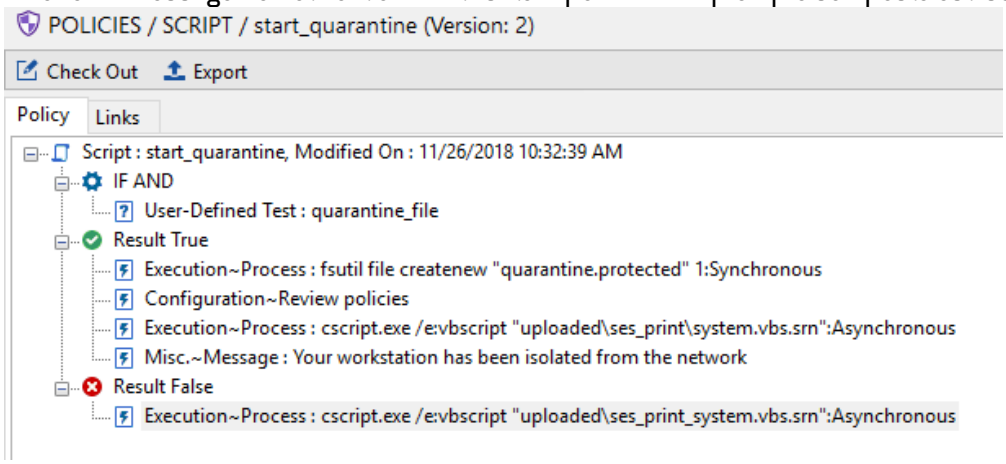
1. Créez un script VB et nommez-le "ses_print_system.vbs".
2. Copiez le contenu de l'exemple de script fourni à la section Exemple de script Visual Basic. Cet exemple permet de récupérer des informations sur l'événement en cause à partir des variables d'environnement SES et les organise dans un fichier 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".

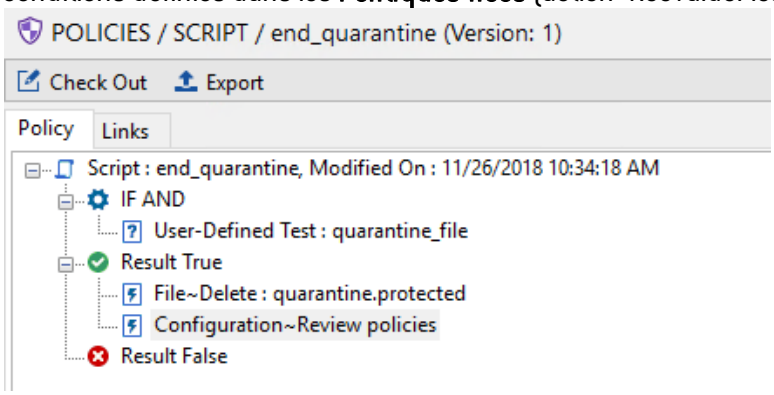
- Le script "start_quarantine" permet de déclencher l'isolation du poste. Si le fichier "quarantine.protected" n'est pas déjà présent sur le poste de travail, le script :
  - crée le fichier "quarantine.protected" sur le poste de travail infecté, dans le répertoire de l'agent. La règle d'extension que 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.



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").

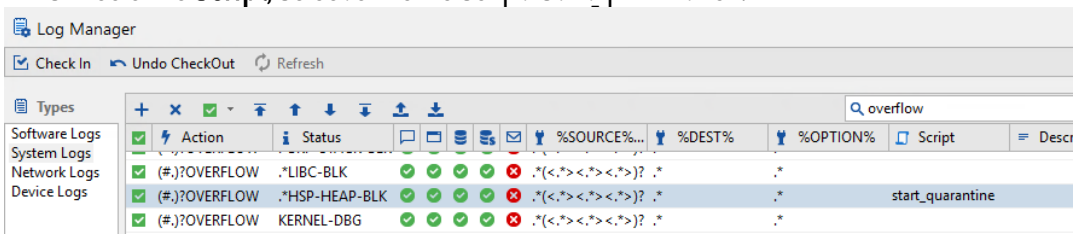


Assigner les scripts d'isolation et de fin d'isolation

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).

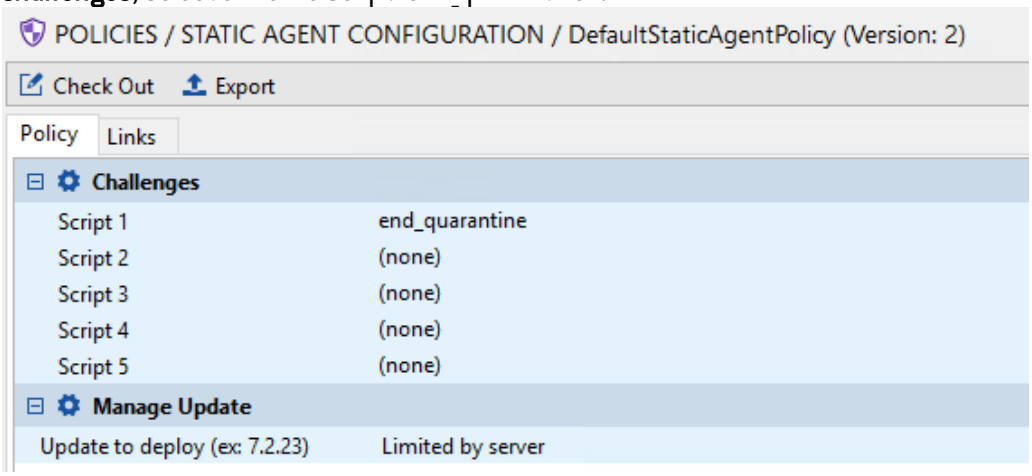
3. Dans la colonne **Script**, sélectionnez le script "start_quarantine" :



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" :



2. 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