



STORMSHIELD

ÉTUDE TECHNIQUE

Nom du projet	Déploiement de la SES	Version	1.0
Auteur	Vincent Draghi	Date de mise à jour	01/02/2019
Destinataire	Chef de projet	Référence	Étude Technique



STORMSHIELD

TABLE DES MATIÈRES

I. INTRODUCTION	3
A. Objectifs du document	3
II. ÉTUDE TECHNIQUE	3
A. Architecture technique	3
1. Installation commune	5
2. Configuration de la solution : côté serveur	7
3. Configuration de la solution : côté agent	10
B. Analyses techniques des fonctionnalités	12
1. Mécanismes de Protection	12
2. Politique de sécurité	14
3. Chiffrement	21
4. Surveillance de l'activité	24
III. PLANNING	27
IV. BILAN DES COÛTS	29
V. SUIVI DU PROJET	30



STORMSHIELD

I. INTRODUCTION

Le 13 mars 2018, lors d'une réunion plénière consacrée à l'analyse fonctionnelle détaillée des modules, le comité de direction et de pilotage du projet accepte les paramétrages par l'équipe MOE. L'équipe projet ne rencontre pas de difficultés techniques ou organisationnelles et le planning estimé reste inchangé. Le budget a pris en compte le coût matériel.

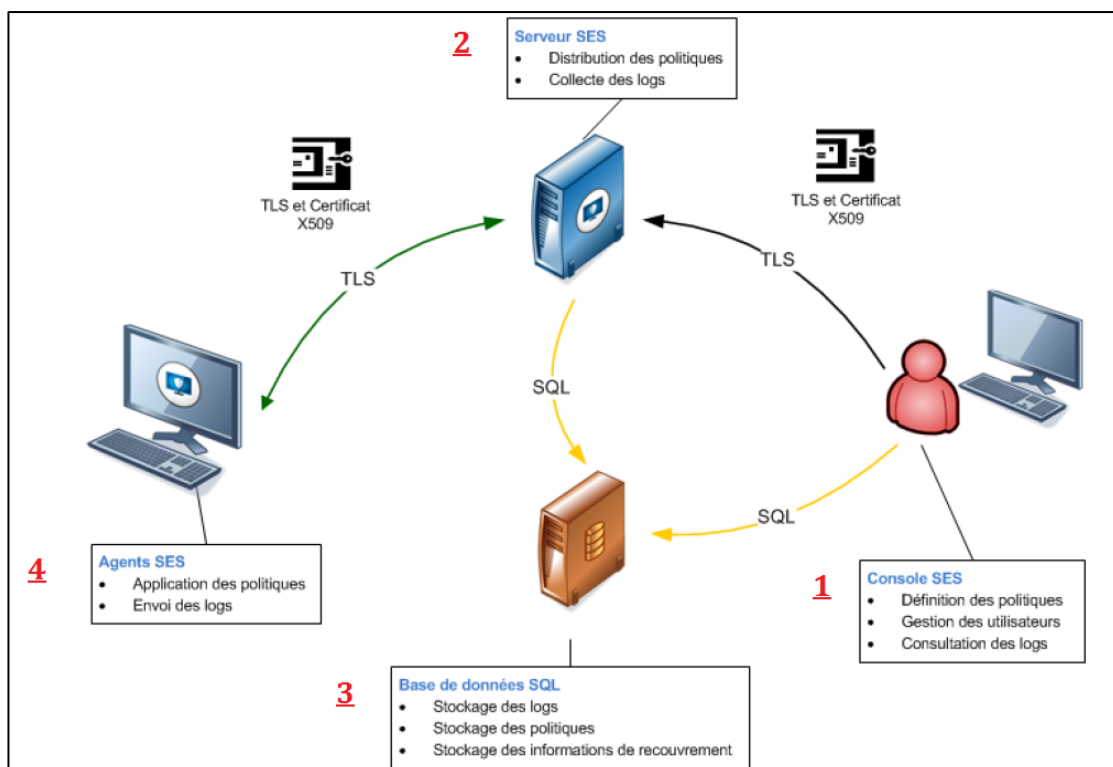
A. Objectifs du document

Le document explique comment configurer chaque module selon l'avis du groupe projet MOE qui s'était basé sur le mode d'emploi fourni par la CFCM. Ce document n'est pas un manuel d'utilisation exhaustif mais constitue un cahier des charges de réalisation pour les prochaines phases du projet.

II. ÉTUDE TECHNIQUE

A. Architecture technique

L'exploitation de Stormshield Endpoint Security (SES) fait intervenir les composants et acteurs projets suivants :





■ Configuration de la console d'administration

La console d'administration permet de définir la politique de sécurité, d'administrer les utilisateurs et de consulter les journaux (logs) remontés par les postes clients.

- Systèmes d'exploitation : Windows 10 Enterprise 2015 LTSB, 64 bit.
- Intel Core 2 Duo E6850 3 GHz
- RAM : 4 Go
- Espace disque principal : 200 Go desktop HDD
- Adresse Ip: 192.168.15.5
- Communications sortantes: Port TCP 16007, TCP 1434

■ Configuration des serveurs Stormshield Endpoint Security

La politique de sécurité est déposée sur un serveur, à partir duquel elle est régulièrement téléchargée par les postes clients. Ce serveur permet également de déployer une mise à jour du logiciel et réceptionne les journaux générés par les postes clients.

- Systèmes d'exploitation : Windows 2016 R2 64 bits.
- RAM : 32 Go.
- 8 cœurs à 3 GHz ou plus.
- 1 carte réseau Ethernet D-Link PCIe, 10 Gigabits Ethernet pour la liaison vers les postes agents.
- 1 carte réseau Ethernet Intel PCI-Express 3.0, 10 Gigabits Ethernet pour la liaison au serveur SQL de logs.
- Espace disque principal : 500Go HDD.
- Adresse IP: 192.168.15.3 et 192.168.15.4
- Pour les communications entrantes: Port TCP 16004 – 16007
- Pour les communications sortantes: Port TCP 16006, TCP 80, Port UDP 1450

■ Configuration du serveur de base de données

Poste situé au DSI, au Service Infrastructure réseau et systèmes, pôle réseau

- Systèmes d'exploitation : Windows 2012 R2.
 - SES stormshield étant optimisé pour SQL server 2012, la base de données utilise actuellement SQL 2014 version 64 bits entreprise (aucun impact significatif sur les performances)
 - RAM : 32 Go.
 - Intel i7-9700K, 8 cœurs, 3,6 GHz
- 1 carte réseau Ethernet Intel PCI-Express 3.0, 10 Gigabits Ethernet relié à le serveur Stormshield Endpoint Security.



STORMSHIELD

- Espace disque principal : 2 T0 (Partition Système, C :100 Go, Partition D : 10 Go SQL, 900 Go de bases de données des logs, 700 Go pour la sauvegarde de la base de donnée des logs.
 - Adresse IP: 192.168.15.8
 - Communication avec les serveurs et la console SES: Port TCP 1433
- Configuration des postes agents
- Les 2800 unités centrales sont en cours de migration d'après le schéma directeur de l'amélioration du SI d'ici 2022. Le siège central (Direction-DSI) bénéficie de changements majeurs en cours.

Voici la configuration variable actuelle, qui remplit les prérequis à l'installation de Stormshield :

- Systèmes d'exploitation : Windows 7 SP1 / Windows 8.1
- RAM : entre 2 à 4Go.
- Processeur : Amd Mono-cœur 2Ghz/ Intel Dual-core i3-6100
- Pour les communications sortantes: Port TCP 16006

Communications sortantes entre l'agent et le serveur Stormshield Endpoint Security : Port TCP 16004-16006

1. Installation commune

Le 15 mars 2018, une réunion technique d'avancement avec les membres de l'équipe MOE a eu lieu avec la présence d'un membre du comité de pilotage : Mr Gilbert Saduc, consultant sécurité à la CFCM. La solution a été livrée par la caisse nationale avec des pré-configurations à ajuster pour notre SI et faciliter les configurations et l'installation. Il a été jugé plus efficace d'utiliser les fichiers de configuration, certificats de sécurité, paramètres pare-feu, clés de sécurité dans une clé USB sécurisée à double authentification. MOA valide cette solution.

L'installation de la console SES, des deux serveurs SES, de la base de données et des postes agents suivent la même procédure (sauf au moment du choix des composants). Les administrateurs, comme établis dans l'étude détaillée, se chargent de l'installation. Les serveurs et les postes agents nécessitent des paramétrages supplémentaires spécifiques développés dans les parties techniques suivantes.

Pour installer Stormshield Endpoint Security, procéder de la façon suivante :

1. Double-cliquer sur « setup.exe ».
2. Sélectionner la langue souhaitée.
3. Choisir le type d'installation : « personnalisée »
3. Définir les paramètres selon le rôle attribué :



STORMSHIELD



Vérifiez que la case « Déploiement des agents » n'est pas cochée.
Cliquez sur « suivant ». Les administrateurs et consultants sécurité ont déjà paramétré le reste de l'installation commune.

Pour le serveur de la base de données (Boris Denvert, administrateur) : cochez la case « SQL Server 2012 Express Edition » dans la fenêtre précédente.

2. À l'étape Super Admin, choisissez choisir le compte « MSSQL SA » (Identifiant et mot de passe prédéfinis)
3. Dans l'étape de l'instance de base données, les ports fixes sont déjà affichés ; Cliquez sur suivant.
4. Dans l'étape finale, cochez « Installer la base de donnée principale » et « Installer la base de données d'alertes »





STORMSHIELD

2. Configuration de la solution : côté serveur

Les administrateurs Xavier Klein et Michel Kali se chargent de la configuration des deux serveurs pour permettre une collecte efficace des logs tout en diffusant les politiques de sécurité.

Dans la partie « Gestion des environnements de la console » (cf ci-dessous), le panneau « Serveurs » permet d'ajouter, modifier ou supprimer un serveur. Tous les serveurs Stormshield sont listés dans ce panneau. Il faut vérifier que les serveurs apparaissent bien et soit détectés.

Si ce n'est pas le cas, pour ajouter des serveurs, il faut effectuer une recherche dans l'annuaire Active Directory, ou, si le serveur n'appartient pas à Active Directory il faut rechercher par l'adresse IP ou par le nom NetBIOS.

Deploy to the environment		ENVIRONMENT MANAGER / SERVERS			
+ Add ✕ Remove					
Server list					
		Name	Console connection IP	Agents synchronization IP	Policy Name
		\S1-SSO-W2K12	192.168.128.69	192.168.128.69	Server 1
					Active Directory

La politique de configuration du serveur comprend différentes zones :

- Gestion des connexions agent.
- Configuration de la surveillance des logs.
- Configuration Syslog.
- Configuration SMTP.
- Chiffrement.
- Mises à jour du logiciel.
- Service d'authentification.

(voir capture d'écran suivante)



STORMSHIELD

Deploy to the environment

Environment Manager

Servers

Policies

Environment

Log Manager

Monitoring

Console Manager

Devices

Policies

Server Configuration

Server 1

Dynamic Agent Configuration

Static Agent Configuration

Security

Encryption

Script

Script Resources

Files Deployment

POLICIES / SERVER CONFIGURATION / Server 1 (Version: 1)

Check In Undo CheckOut Export Import

Policy

Agent connection management

Number of simultaneous connections100

Maximum number of handled clients1000

Token refresh time (sec.)300

Reconnection time (sec.)300

Logs upload period (sec.)1800

Minimum agent version allowedNot limited

Maximum agent version allowedNot limited

Log Monitoring Configuration

SQL server instance192.168.129.252\SES

Database password*****

Reporting languageEnglish

Syslog Configuration

Address/Hostname

Port514

ProtocolUdp

Facility0 ~ kernel messages

Severity0 ~ Emergency

SMTP Configuration

From

To

SMTP server

Subject

Number of events per mail10

Encryption

Decrypt data at uninstallation☒ Disabled

Start date of allow uninstall13/07/2018 00:00:00

End date of allow uninstall13/07/2028 00:00:00

SQL server instance192.168.129.252\SES

Database password*****

Software Updates Settings

Check update interval03h00m00s

Gestion des connexions agents

Il faut prendre en compte dans notre contexte, la limite de connexions simultanées des postes agents. Dans notre cas, la moyenne est estimée entre 1300 à 1800 connexions (dont périodes de sollicitations intensives) par jour. L'interface de la gestion des connexions agents est le suivant :

Agent connection management	
Number of simultaneous connections	2000
Maximum number of handled clients	100000
Token refresh time (sec.)	300
Reconnection time (sec.)	300
Logs upload period (sec.)	1800
Minimum agent version allowed	Not limited
Maximum agent version allowed	Not limited

Les définitions des termes figurant sur l'interface sont les suivantes :



STORMSHIELD

- **Nombre d'agents pouvant se connecter simultanément:** fixer la valeur à 1800. Si trop d'agents sont connectés en même temps, le serveur sera considéré comme inaccessible pour les agents en surnombre. La situation ne devrait pas se produire.
- **Nombre maximum d'agents assignés au serveur :** fixer la limite à 50000. Lorsque ce nombre est atteint, le serveur refuse les connexions de nouveaux agents. Ils sont alors dirigés vers le deuxième serveur SES.
- **Temps de rafraîchissement des jetons (sec) :** fixer la valeur à 450 secondes. Cela correspond à l'intervalle de temps entre chaque envoi de jeton par le serveur aux agents.
- **Temps de reconnexion (sec) :** fixer la valeur à 450 sec. Cela correspond à l'intervalle de temps pour la tentative de reconnexion automatique des agents au(x) serveur(s) lorsque l'agent est en mode déconnecté.
- **Période de remontée des logs (sec) :** fixer la valeur à 1500 sec. Cela correspond à l'intervalle de temps entre chaque remontée de logs des agents vers leurs serveurs. La remontée des logs se fait sur un canal distinct de la récupération de politiques. Le port utilisé pour la communication des logs est le port TCP sécurisé 16004.
- **Version d'agent minimale autorisée :** mettre comme valeur= version 1.2.version de l'agent minimale requise pour se connecter au serveur. Ce paramètre est important, surtout vis-à-vis de la critique de l'existant concernant les portables nomades à maintenir à jour.

Configuration de la surveillance des logs

Voici l'interface de la configuration de la surveillance des logs :

Log Monitoring Configuration	
SQL server instance	192.168.128.69\SES
Database password	*****
Reporting language	English

Les définitions des termes figurant sur l'interface sont les suivantes :

- **Instance de la base de données :** il faut entrer l'adresse IP du serveur SQL utilisé pour la base de données de logs.
- **Mot de passe de la base de données :** mot de passe du compte utilisé pour la base de données de log. Il a été défini pendant l'installation de la base de données Stormshield.
- **Langue de remontée de logs :** langue utilisée pour la remontée de logs.

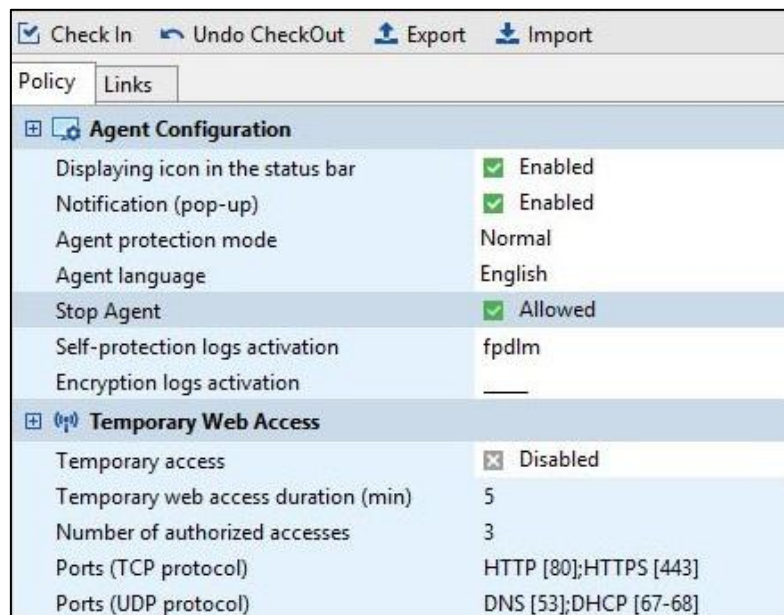


STORMSHIELD

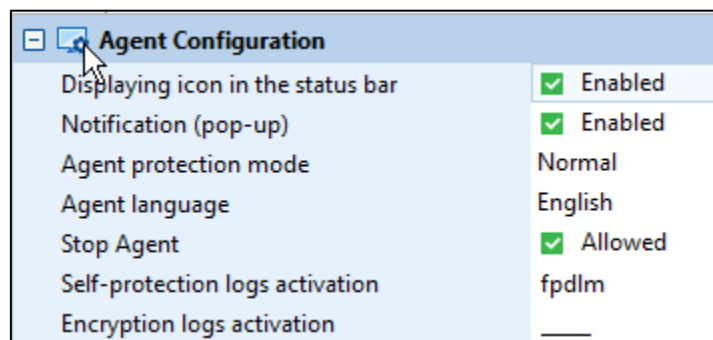
3. Configuration de la solution : côté agent

Sarah Valerbe (pôle déploiement) et son équipe sont chargées de la configuration côté agent.

- Édition de la politique de configuration dynamique de l'agent :



Interface graphique de la configuration d'agent :

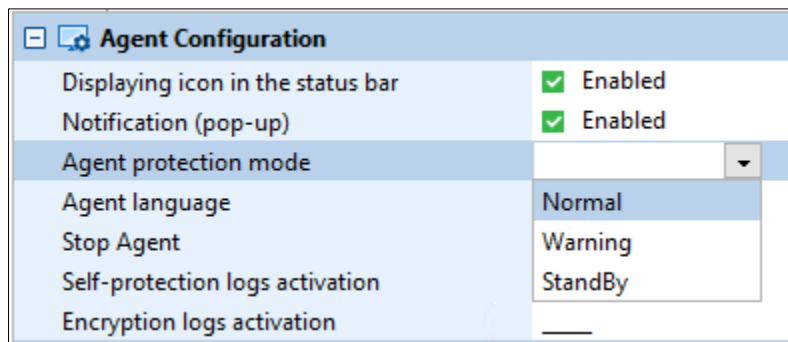


- Affichage de l'icône dans la barre d'état : option à activer dans notre situation.
- Notification (pop-up) : pour ne pas gêner les utilisateurs et éviter des démarches de ticketing inutiles de la part des agents, cette fonctionnalité est désactivée. Il faut s'assurer qu'elle soit bien désactivée.

L'interface graphique du mode de protection de l'agent se présente comme suit :



STORMSHIELD

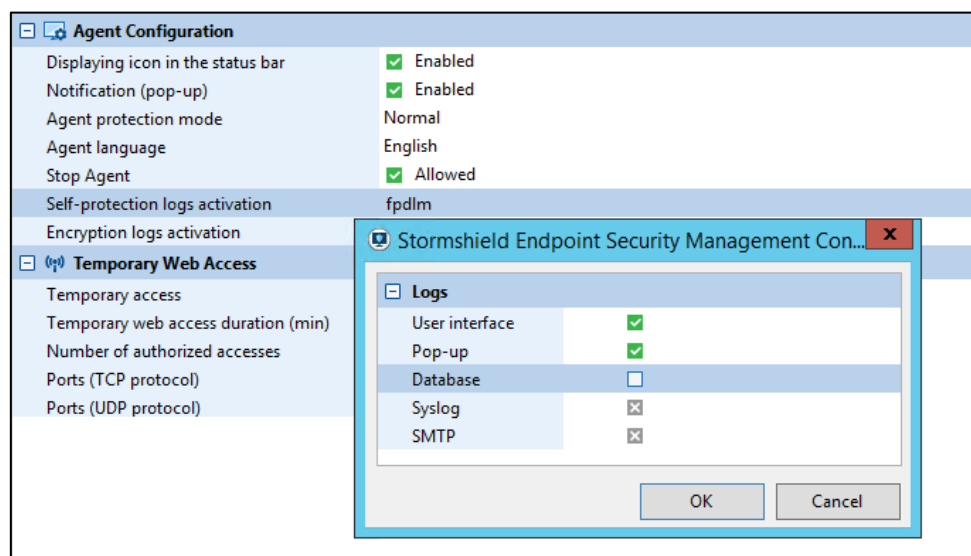


- Activation des logs : il faut activer les logs au niveau de Configuration d'agent.

* Activation des logs d'autoprotection : mettre en mode « StandBy »

* Activation des logs de chiffrement : mettre en mode « Warning »

Les deux options permettent de contrôler les logs Stormshield Endpoint Security qui sont affichés et filtrés dans Surveillance > Logs Logiciel.



Chaque type d'activation de logs contient les paramètres suivants pour enregistrer et consulter les logs :

- Interface utilisateur : ces logs sont affichés dans l'interface utilisateur.
- Pop-Up : fenêtre de notification utilisateur.
- Base de données : remontée des logs dans la base de données. Ils sont alors visibles dans la console depuis le menu Surveillance.
- Application externe : les logs sont envoyés à un système externe comme Syslog ou un serveur SMTP.

Gestion des mises à jour : elle permet de définir la version vers laquelle l'agent se mettra à jour lorsque des mises à jour sont déployées sur le serveur Stormshield Endpoint Security. => Vérifier si par défaut, le module est actif.



STORMSHIELD

B. Analyses techniques des fonctionnalités

Le 3 mars 2018, une instance avec l'équipe projet MOE et MOA a établi les principales consignes pour rédiger le cahier des charges technique sur l'ensemble des fonctionnalités.

Une prochaine réunion d'avancement aura lieu le 11 mars 2018 pour valider l'analyse technique des paramétrages, dans le respect du planning fixé.

1- Mécanismes de Protection

Fonction détaillée	Mécanismes de protection												
Fonctionnement et paramétrage	<div><pre>graph TD A((Évènement système ou réseau)) --> B{La règle est-elle applicable?} B -- Autorise --> C((Action autorisée)) B -- Interdit --> D{Action dangereuse?} D -- Oui --> E((Action bloquée)) D -- Non --> C</pre></div> <p>*Protections automatiques : elles protègent l'activité système et réseau au niveau du poste client. On peut désactiver totalement ou partiellement ces protections.</p> <div><div><input type="checkbox"/> System Behavior Control</div><table><tbody><tr><td>Executable file creation</td><td><input checked="" type="checkbox"/> Disabled</td></tr><tr><td>Protection against privilege escalation</td><td><input checked="" type="checkbox"/> Disabled</td></tr><tr><td>Protection against spontaneous reboots</td><td><input checked="" type="checkbox"/> Disabled</td></tr><tr><td>Protection against keyloggers</td><td><input checked="" type="checkbox"/> Disabled</td></tr><tr><td>Protection against memory overflow</td><td><input checked="" type="checkbox"/> Disabled</td></tr><tr><td>Kernel component protection</td><td><input checked="" type="checkbox"/> Disabled</td></tr></tbody></table></div> <p>Choisir le mode : « Activer » et le niveau de sécurité : « Bas »</p> <p>* Protection par règles : elle permet de définir une politique spécifique à chaque entreprise. Les règles seront à affiner en respectant la PSSI, en indiquant de manière explicite les droits et les interdictions d'accès aux ressources du poste client.</p> <p>Voici la barre d'outils :</p>	Executable file creation	<input checked="" type="checkbox"/> Disabled	Protection against privilege escalation	<input checked="" type="checkbox"/> Disabled	Protection against spontaneous reboots	<input checked="" type="checkbox"/> Disabled	Protection against keyloggers	<input checked="" type="checkbox"/> Disabled	Protection against memory overflow	<input checked="" type="checkbox"/> Disabled	Kernel component protection	<input checked="" type="checkbox"/> Disabled
Executable file creation	<input checked="" type="checkbox"/> Disabled												
Protection against privilege escalation	<input checked="" type="checkbox"/> Disabled												
Protection against spontaneous reboots	<input checked="" type="checkbox"/> Disabled												
Protection against keyloggers	<input checked="" type="checkbox"/> Disabled												
Protection against memory overflow	<input checked="" type="checkbox"/> Disabled												
Kernel component protection	<input checked="" type="checkbox"/> Disabled												



STORMSHIELD



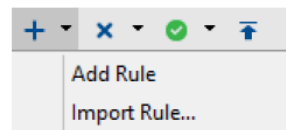
Sept catégories de règles sont à activer

- Composants kernel : cette catégorie sert à contrôler le chargement des drivers et à détecter les drivers suspects sur les postes de travail en 32 bits uniquement.
- Périphériques amovibles : cette catégorie détermine les périphériques amovibles susceptibles d'être utilisés par les postes clients.
- Firewall réseau : cette catégorie permet un contrôle statique et dynamique du firewall réseau.
- Règles applicatives : cette catégorie regroupe :
 - Toutes les règles associées à l'exécution des applications.
 - Toutes les règles associées à la modification des applications.
 - L'ensemble des applications locales de notre SI et nationales seront intégrées.
- Extensions : cette catégorie sert à définir des règles en fonction du type de fichier, quelle que soit l'application qui y accède.
- Applications de confiance : cette catégorie permet de libérer certaines applications de tout type de contrôle afin d'éviter un éventuel blocage intempestif.

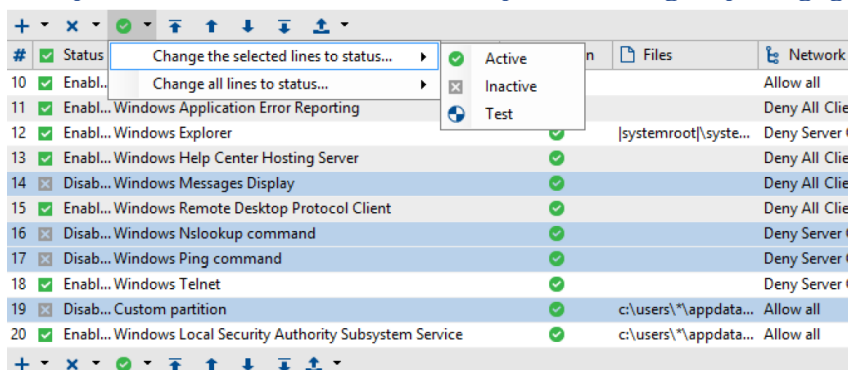
- Politique de liste blanche et liste noire à importer

L'approche liste blanche consiste à interdire tout ce qui n'est pas explicitement autorisé. L'approche liste noire consiste à autoriser tout ce qui n'est pas explicitement interdit. Ces deux approches sont combinées pour tout ce qui a trait à l'accès réseau et une approche liste noire pour l'accès aux applications utilisables par les utilisateurs.

Les listes et règles sont à importer depuis la clé USB sécurisée de configuration SES qui contient le fichier (FirewallGlobalCFCM.scer) de notre firewall applicatif géré par Panda Adaptive Defense.



Il est possible d'activer et désactiver plusieurs règles pour gagner en efficacité.



Acteurs
concernés

- Michael Taudili, conseiller du système d'information
- Maxime Lauris, expert infrastructure du SI
- Paul Mileme, coordinateur projet SI
- Romain Hélios, technicien réseau Télécom Expert.



STORMSHIELD

2- Politique de sécurité

Fonction
détailée

1- Identifiants d'applications

Fonctionnement
et paramétrage

Name	Creation	Last modification	Policy(ies) linked	Comment
*.tmp, *.dat	6/25/2018 10:35:07 ...	6/25/2018 10:35:16 ...	1	.tmp, .dat
*\setup.exe	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	For Win10 Upgrade
*\sources\setupprep.exe	6/25/2018 10:35:08 ...	7/13/2018 9:31:47 AM	1	W10 Upgrade
*\sources\setupprep.exe - 1709	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	W10 Upgrade 1709
systemroot system32\background...	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	systemroot system32\backgroundtaskhost.exe
systemroot system32\lsass.exe	6/25/2018 10:35:07 ...	6/25/2018 10:35:16 ...	1	lsass.exe
systemroot system32\spssvc.exe	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	Microsoft Software Protection Platform Service
systemroot system32\svchost.exe	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	Services Control Manager
systemroot system32\wimserv.exe	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	Wimfltr v2 extractor
All	6/25/2018 10:35:07 ...	6/25/2018 10:35:16 ...	1	
c:\\$windows~bt\sources\mighost...	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	Win10 Upgrade
c:\\$windows~bt\sources\setupho...	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	processus maj windows
c:\\$windows~bt\sources\setuppla...	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	
c:\windows\system32\drvinst.exe	6/25/2018 10:35:08 ...	6/25/2018 10:35:16 ...	1	

1. Ouvrir le panneau Identifiants d'applications et choisir « Ajouter en haut du panneau »
 2. Entrer un nom d'identifiant et une description.
 3. Cliquer sur le bouton Valider en haut du panneau « Identifiants d'applications ».
- Le focus reste sur l'identifiant validé.

Type	Value
------	-------

Il faudra manuellement ajouter nos applications locales et nationales et cliquer sur « Ajouter ».



STORMSHIELD

Stormshield Endpoint Security Management Console

Parameters

Description:

Path:

Certificate:

Helper

Allows identifying an executable according to the path or the certificate which signs it.

- If only one field is completed, any executable matching the entered value will be identified.
- If both fields are completed, only the executables matching both fields will be identified.

OK Cancel

Dans notre situation il a été choisi l'identification par certificat de signature. L'identification par certificat présente l'avantage de ne pas reposer sur une version ou un chemin d'une application mais uniquement sur sa signature numérique. Ainsi, il est plus pratique et rapide d'autoriser ou de bloquer l'ensemble des applications quel que soit leur emplacement sur le poste de travail. Mettre : « Certificats des applications » et choisir le dossier « Certificats X509 » contenant les certificats depuis la clé USB sécurisée de configuration SES

Stormshield Endpoint Security Management Console

Search...

Description	Subject	Issuer	Validity	Details
Oracle America, Inc. [3B75816D15A...	Oracle America, Inc.	Symantec Class 3 SHA256 ...	4/14/2018 1:59:59 AM	Details
Microsoft Corporation.cer (Microso...	Microsoft Corporation	Microsoft Code Signing PCA	7/22/2015 7:39:00 PM	Details
Microsoft Corporation [AD16FFEA1...	Microsoft Corporation	Microsoft Windows Produ...	8/3/2017 7:17:19 PM	Details
Opera Software AS [49B00D844B474...	Opera Software AS	DigiCert EV Code Signing ...	6/27/2019 2:00:00 PM	Details
Microsoft Corporation [98ED99A67...	Microsoft Corporation	Microsoft Code Signing PCA	11/2/2017 9:17:17 PM	Details
Mozilla Corporation [50600FD63199...	Mozilla Corporation	DigiCert SHA2 Assured ID ...	7/13/2018 2:00:00 PM	Details
Windows Defender.cer (Microsoft ...	Microsoft Corporation	Microsoft Code Signing P...	5/9/2018 9:17:21 PM	Details
Microsoft Windows [B8037C46D0D...	Microsoft Windows	Microsoft Windows Verific...	5/9/2018 8:46:04 PM	Details
Microsoft Corporation.cer (Microso...	Microsoft Corporation	Microsoft Code Signing PCA	9/4/2016 7:42:45 PM	Details

OK Cancel

On valide pour intégrer la liste des certificats et finaliser la liste de la création des entrées.

Acteurs concernés

- Frédéric Odenrio, conseiller système d'informations (pôle application)
- Xavier Klein, expert infrastructures SI
- Sarah Valerbe, référent support technique utilisateur
- Boris Denvert, administrateur de base de données confirmé

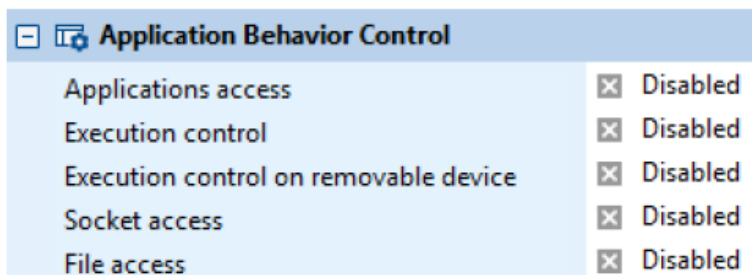


STORMSHIELD

Fonction
détaillée

2- Comportement Système

Permet de paramétrer le contrôle du comportement du système ainsi que le contrôle du comportement des applications.



Liste des fonctionnalités et niveau de sécurité à activer pour notre SI :

- Blocage des attachements : le mécanisme d'attachement aux applications permet à un code malveillant de :
 - Arrêter le fonctionnement d'une autre application.
 - Corrompre l'application.
 - Prendre le contrôle de l'application.Choisir le réglage : « Haut »
- Contrôle des exécutions : ce mécanisme contrôle le lancement des applications installées sur le poste. Un code malveillant peut en effet être dissimulé dans une application autorisée.
- Contrôle des exécutions sur périphérique amovible : une confirmation est demandée à l'utilisateur lorsqu'un fichier exécutable (.exe) est lancé depuis un périphérique amovible. Choisir le mode « Discret »
- Accès au réseau : politique de liste blanche dans laquelle aucun accès réseau n'est autorisé à moins qu'il ne soit explicitement déclaré.
- Accès aux fichiers : toute tentative de renommage d'un fichier est soumise à une vérification. Toute tentative de modification d'un exécutable est bloquée. Choisir le mode « Elevé »
- Composants Kernel : contrôle automatique du chargement des drivers et détection des drivers suspects. Choisir le mode « Elevé »

Fonctionnement
et paramétrage

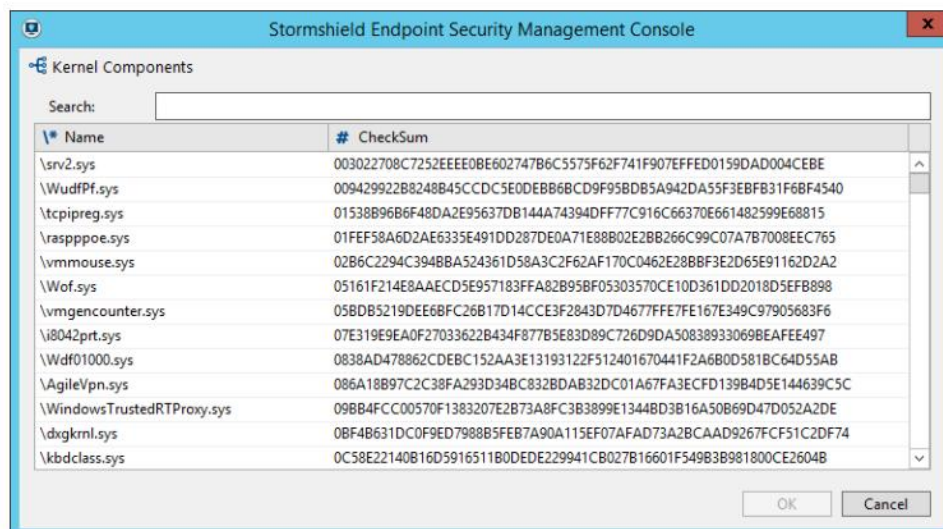


STORMSHIELD

Kernel Components

#	✓	Name	Checksum	Loading	Log	Description
0	✓	\rasppoe.sys	01FEF58A6D2AE...	✓	---	
1	✓	\vmmouse.sys	02B6C2294C394...	✓	---	
2	✓	\CompositeBus.sys	051AD6A2FF362...	✓	---	
3	✓	\WdNisDrv.sys	07733E0BA667E...	✓	---	
4	✓	\luafv.sys	0877F736B0E8F1...	✓	---	
5	✓	\intelide.sys	08BC74F4973B2...	✓	---	
6	✓	\storahci.sys	09B93F4899933B...	✓	---	
7	✓	\intelpep.sys	0A73324FBADC...	✓	---	
8	✓	\ksecdd.sys	0B0AAA0263585...	✓	---	
9	✓	\kbdclass.sys	0C58E22140B16...	✓	---	
10	✓	\mxsmb.sys	0D3F159FB5D9E...	✓	---	
11	✓	\pnpmem.sys	0D5E496871917F...	✓	---	
12	✓	\e1i6332.sys	1494CB4145E42...	✓	---	

Pour ajouter un driver à la liste des composants kernel, cliquez sur  dans la barre d'outils. La fenêtre suivante s'affiche :



La liste des composants kernel est automatiquement construite à partir des drivers chargés sur les postes sur lesquels l'agent est installé.

Acteurs concernés

- Michel Kali, expert infrastructures du SI
- Michael Taudili, conseiller du système d'informations
- Nathan Amber, technicien réseau et Télécom



STORMSHIELD

Fonction
détaillée

3-Contrôle des périphériques

Les paramètres du groupe peuvent comprendre les éléments suivants en fonction du type de périphérique sélectionné :

- Ports infrarouges.
- Ports parallèles.
- Ports séries.
- Lecteurs de cartes à puce USB.
- Dispositifs de pointage (exemples : souris, tablettes graphiques, etc.) et HID (Human Interface Device) claviers.
- Fonctionnalité U3 : bloque l'exécution des Autorun sur les clés USB U3 et les lecteurs de CD-ROM.
- Périphériques de stockage de masse (exemples : clés et disques durs USB, FireWire, etc.).

Sous périphériques amovibles, cliquer sur « Groupe v1 » pour appliquer la liste prédéfinie.

Le panneau des paramètres du groupe sur la droite change en fonction du type de périphérique sélectionné dans la zone « Paramètres du groupe ». Les zones suivantes sont disponibles :

Fonctionnement
et paramétrage

Group Settings

Device Type	Mass storage
Default access rights	Read/Write
Audit	Plug/Unplug
File encryption	Enabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	<input checked="" type="checkbox"/> Allowed

USB Settings

Removable devices enrollment	Disabled
Restore trust status	Disabled

Removable Devices

Device Type	Vendor ID	Product ID
usb	3034	89654
firewire	4569	456789

File Extensions and Rights

Extension	Rights	Description
doc	Read/Write	Word files
exe	Denied	Executable

- Zone A : Paramètres du groupe

Ces paramètres sont applicables à l'ensemble de la liste des périphériques du groupe.

- Zone B : Paramètres USB

Ces paramètres permettent de changer l'état d' enrôlement des périphériques du groupe.

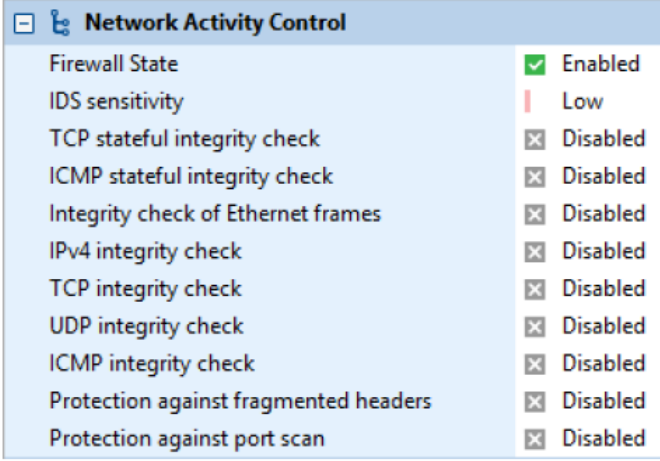
- Zone C : Groupe de périphériques

Il s'agit des périphériques qui constituent le groupe.



STORMSHIELD

	<ul style="list-style-type: none"> • <u>Zone D : Exceptions sur les extensions de fichiers</u> <p>Mettre des droits d'accès par défaut sur « Lecture/écriture »</p>
Acteurs concernés	<ul style="list-style-type: none"> - Maxime Lauris, expert infrastructure SI - Charlie Ganegue, consultant infrastructure SI - TourianEn'ma, consultant infrastructure SI

Fonction détaillée	4- Contrôle de la sécurité réseau
Fonctionnement et paramétrage	<p>La solution Stormshield Endpoint Security protège l'activité réseau à l'aide d'un système de détection d'intrusion (Intrusion Detection System (IDS)) et d'un système de prévention d'intrusion (Intrusion Prevention System (IPS)).</p>  <p> <ul style="list-style-type: none"> - État de Pare-feu : mettre sur « Activer » - Contrôle d'intégrité stateful en TCP : mettre sur « Activer » - Contrôle d'intégrité stateful en ICMP : mettre sur « Activer » - Contrôle d'intégrité des trames Ethernet : mettre sur « Activer » - Contrôle d'intégrité UDP : mettre sur « Activer » </p> <p>Le réglage de la sensibilité de l'IDS (>Haute) active les fonctionnalités IPS suivantes :</p> <ul style="list-style-type: none"> - <u>Protection contre le flood</u> (Suppression des connexions > 20) - <u>Protection contre le balayage de ports</u> (filtrage et blocage des paquets au niveau des ports et blocage de l'adresse IP associée si nécessaire) - <u>Protection contre l'empoisonnement du cache ARP</u> (détecte si la machine sur laquelle se trouve l'agent tente d'usurper l'identité d'une autre machine sur le réseau).
Acteurs concernés	<ul style="list-style-type: none"> - Xavier Klein, expert infrastructures SI - Nathan Ambert, technicien réseau et Télécom - Frédéric Odenrio, conseiller du système d'informations



STORMSHIELD

Fonction
détaillée

5-Firewall réseau - Règles applicatives

Stormshield Endpoint Security dispose d'un firewall réseau dont le fonctionnement est contrôlé à la fois de façon :

- Statique (règles)
- Dynamique (déterminé par la sensibilité de l'IDS et la gravité des alertes IDS).

Le fonctionnement statique est déterminé par les règles.

Sur l'interface du firewall réseau, il faut importer les paramètres sur la clef USB sécurisée de configuration fournie qui provient des règles du pare-feu hardware Stormshield SN210.

Network Firewall / Base network

#	Status	Action	Direction	Remote IP	Over IP	Stateful
0	Enabled	Block	Incoming	All	ICMP [1]	On
1	Enabled	Block	Incoming	All	ICMP [1]	On
2	Enabled	Accept	Outgoing	All	ICMP [1]	Off

Fonctionnement
et paramétrage

Les règles doivent déjà être établies après l'importation.

Network Firewall / Default Group

#	Status	Action	Direction	Local MAC
30	Enabled		Outgoing	All

Rank

Status

Action

Direction

Local MAC

Remote MAC

Over Ethernet

Local IP

Remote IP

Over IP

Stateful

Local Port

Remote Port

Log

Description

Group

Visible

Multiline

Right to left

Mettre le filtrage sur « Mac Local » en « visible » comme indiqué.

Acteurs
concernés

- Michel Kali, expert infrastructures du SI
- Maxime Lauris, expert infrastructure du SI
- Romain Hélios, technicien réseau Télécom expert
- TourianEn'ma, consultant infrastructure du SI



STORMSHIELD

3- Chiffrement

Voici l'interface, volet du chiffrement (politique de chiffrement)

Section	Setting	Value	Status
General Settings	Allow creation of encrypted archives	Allowed	Enabled
	Allow secure file erasure	Allowed	Enabled
	Number of secure erase cycles	3	Enabled
	Erase swap file when machine is stopped	Disabled	Disabled
	Minimum characters required for second authentication password	8	Enabled
	Mandatory password minimum strength	Standard	Enabled
	Encryption key size	256	Enabled
	Enforce encryption policy	Disabled	Disabled
	Password change enforcement	Disabled	Disabled
	Maximum password age	00 day(s)01h	Enabled
Full Disk Encryption Parameters	Full Disk Encryption	Enabled	Enabled
	Partition encryption	System partition	Enabled
	Block-cipher mode of operation	CBC-Advanced	Enabled
	Secure shredding before encryption	Disabled	Disabled
	Number of secure erase cycles	3	Enabled
	Allow automatic restart	Disabled	Disabled
	Single Sign-On (SSO)	Disabled	Disabled
	One-time recovery password	Enabled	Enabled
	Use guest account	Use challenge	Enabled
	File Encryption Parameters	File encryption	Disabled
Authentication type		Secondary	Enabled
Cryptographic Service Providers (CSP)			Enabled
Authorized to stop synchronization		Denied	Disabled
Authentication after unlock session		Enabled	Enabled
Skip system partition (already encrypted at disk level)		Disabled	Disabled
Force user authentication		Disabled	Disabled
Stealth mode		Disabled	Disabled
Encrypted zones			Enabled
Unencrypted zones			Enabled

Fonction
détaillée

1- Chiffrement de fichiers

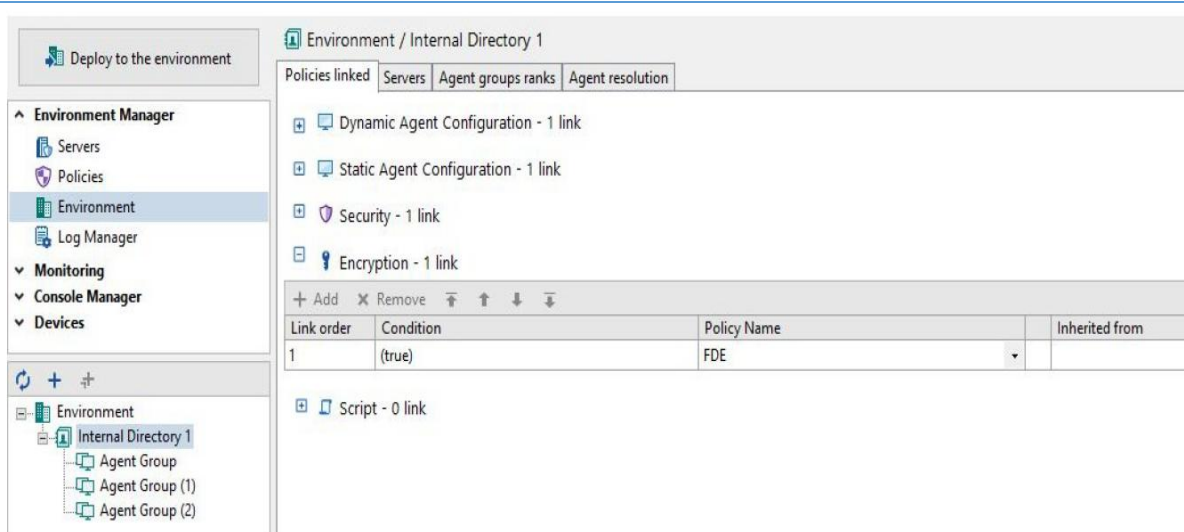
Fonctionnement
et paramétrage

Les fichiers au niveau de confidentialité secret et à l'intégrité complète sont concernés par ce dispositif (direction, RH, cellules contrôles, comptabilité, dossiers assurés sensibles...)

- Chaque fichier est chiffré à l'aide d'une clé de chiffrement distincte.
- Gestion individuelle des fichiers chiffrés.



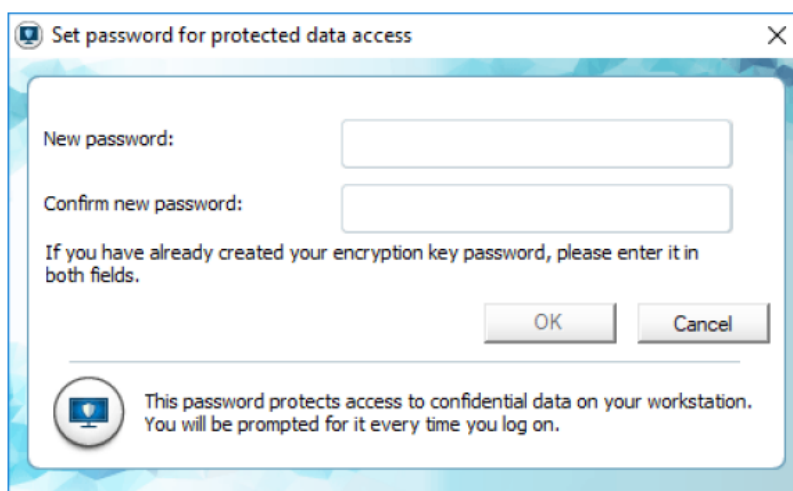
STORMSHIELD



1. Cliquer sur l'objet dans le menu Environnement de la partie Gestion des environnements.
 2. Se placer dans le panneau des Politiques liées.
 3. Sélectionner la politique de chiffrement via la liste déroulante dans la catégorie Chiffrement : « CFCFM politique chiffrement »
 4. Cliquer sur Déployer sur l'environnement.
- Cette action doit être effectuée à chaque modification de la politique de chiffrement.

Les administrateurs peuvent également agir manuellement à distance depuis les postes administrateurs.

Pour s'authentifier, faire un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionner Authentification > Accès aux données protégées.



Acteurs
concernés

- Romain Hélios, technicien réseau Télécom Expert
- Michael Taudili, conseiller du système d'informations
- Boris Denvert, administrateur base de données confirmé



STORMSHIELD

Fonction
détaillée

2- Chiffrement du disque

Description

Le chiffrement total du disque permet de tout chiffrer sur une partition donnée du disque. Il est compatible seulement avec l'interface BIOS qui supporte le schéma de partitionnement MBR et il n'est pas compatible UEFI (partitionnement GPT).

Les paramètres pour le chiffrement total du disque permettent de contrôler les paramètres suivants :

Full Disk Encryption Parameters	
Full Disk Encryption	✓ Enabled
Partition encryption	System partition
Block-cipher mode of operation	CBC-Advanced
Secure shredding before encryption	✗ Disabled
Number of secure erase cycles	3
Allow automatic restart	✗ Disabled
Single Sign-On (SSO)	✗ Disabled
One-time recovery password	✓ Enabled
Use guest account	✓ Use challenge

- Chiffrement des partitions : « activer »
- Mode opératoire de chiffrement : « CBC »
- Effacement sécurisé avant chiffrement : « désactivé »
- Nombre de cycles d'effacement sécurisé : 5
- Autoriser les redémarrages automatiques : « activer »
- Authentification unique (SSO) : « activer »
- Renouvellement automatique du mot de passe de recouvrement : « désactiver »
- Utilisation d'un compte invité : « désactiver »

Acteurs
concernés

- Boris Denvert, administrateur base de données confirmé
- Maxime Lauris, expert infrastructure du SI
- Paul Mileme, coordinateur projet SI



STORMSHIELD

4- Surveillance de l'activité

Fonction détaillée

1- Surveillance des agents

Description

Stormshield Endpoint Security permet de contrôler, surveiller et enregistrer l'activité des postes de travail grâce aux fonctionnalités suivantes situées dans les parties Gestion des environnements, Surveillance et Administration de la console :

- Surveillance des agents.
- Tableau de bord.
- Logs.
- Configuration des logs.
- Audit de la console.

Les options d'affichage pour la surveillance des agents citées ci-dessus sont à activer via (menu Surveillance > Agents)

Host Name	OS	IP Address	Net Mask	Option	AD Name	Agent	Config.	Policy	Configuration	Last synchronization	First Connection	Last Connection
C19-SSO-INSIDER	Windows 10 x64	192.168.1...	255.255.2...	Secure Edition		7.2.23	Valid	Basic template (5)	DefaultDynamicAgentPolicy (2)	7/16/2018 11:33:27 AM	6/25/2018 10:32:15 AM	7/16/2018 11:35:00 AM
C3-SSO-W7X64	Windows 7 x64 SP1	192.168.1...	255.255.2...	Secure Edition	C3-SSO-W7X64...	7.2.23	Valid	Basic template (5)	Dynamic config. (2)	7/16/2018 11:33:04 AM	6/25/2018 10:34:52 AM	7/16/2018 11:35:08 AM
C2-SSO-XP	Windows XP SP3	192.168.1...	255.255.2...	Secure Edition	C2-SSO-XP QA...	7.2.23	Invalid	DefaultSecurityPolicy (1)	Dynamic config. (1)	7/13/2018 9:33:31 AM	6/25/2018 11:09:45 AM	7/13/2018 3:51:12 PM
C20-SSO-INSIDER	Windows 10	192.168.1...	255.255.2...	Professional Edi...		7.2.23	Invalid	DefaultSecurityPolicy	DefaultDynamicAgentPolicy	7/5/2018 5:04:52 PM	6/25/2018 11:15:39 AM	7/6/2018 4:29:20 PM

Mettre sur « statut » comme sur le menu déroulant.

Acteurs concernés

- Nathan Ambert, technicien réseau et Télécom
- Michel Kali, expert infrastructures du SI

Fonction détaillée

2-Tableau de bord

Description

Le Tableau de bord offre une vision globale et actualisée de l'état du parc. Il se compose de quatre graphiques paramétrables permettant d'afficher sur un seul écran différentes informations.

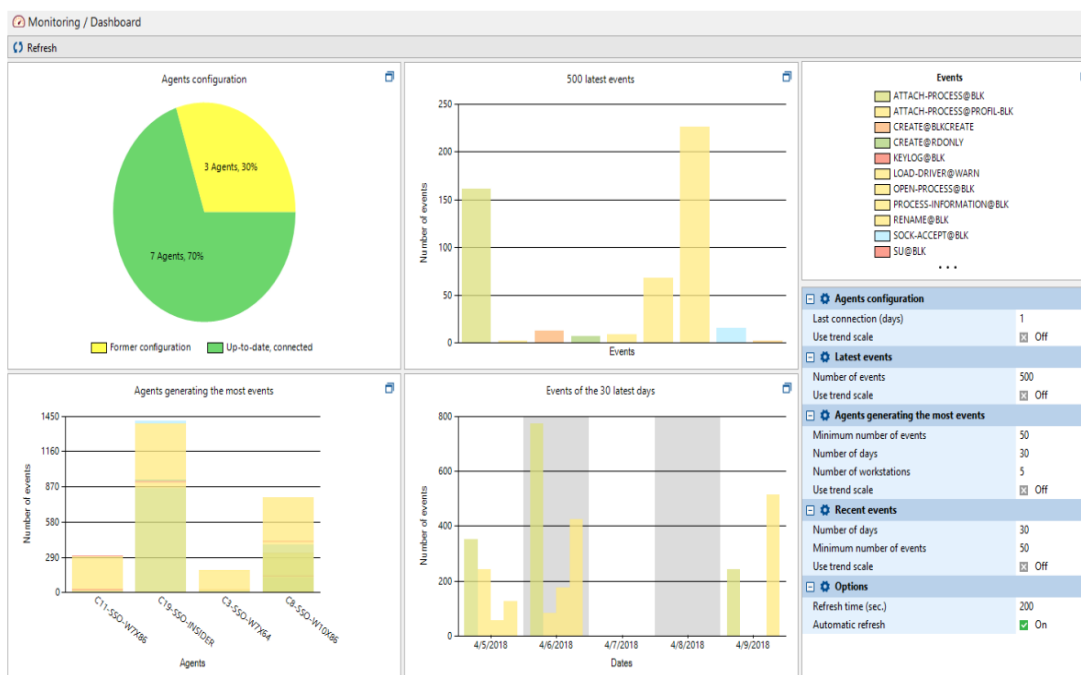
Configuration des agents : choisir « À jour, connecté »

Histogramme des derniers événements : valeur « 500 »

Agents générant le plus d'événements : laisser par défaut



STORMSHIELD



Acteur
concerné

- Xavier Klein, expert infrastructures SI

Fonction
détaillée

3- Surveillance des logs

Les logs Stormshield Endpoint Security contiennent l'enregistrement de tous les événements déclenchés par l'activité des éléments suivants :

- Logiciel
- Système
- Réseau
- Périphériques

Description

Monitoring / Software Logs

Page 1

Export Automatic refresh Advanced filters Options

Logs displayed: Current year Logs: 0-100/356 from 1/1/2018 12:00:00 AM to 1/1/2019 12:00:00 AM - (UTC+01:00) W. Europe Daylight Time

Filters: Action contains Add All conditions

Date	Host Name	Type	Agent Mode	Description	Action	Status
5/9/2018 2:34:12 PM	C20-SSO-INSIDER	Agent	Normal	Security policy	INFO	CONF_APPLY
5/9/2018 2:34:10 PM	C20-SSO-INSIDER	Agent	Normal	Configuration	INFO	CONF_APPLY
5/9/2018 2:34:09 PM	C19-SSO-INSIDER	Agent	Normal	Security policy	INFO	CONF_APPLY
5/9/2018 2:34:09 PM	C20-SSO-INSIDER	Agent	Normal	Connection success	INFO	CONNECT_SUCCESS
5/9/2018 2:34:07 PM	C19-SSO-INSIDER	Agent	Normal	Configuration	INFO	CONF_APPLY
5/9/2018 2:34:06 PM	C19-SSO-INSIDER	Agent	Normal	Connection success	INFO	CONNECT_SUCCESS
5/9/2018 1:59:01 PM	C20-SSO-INSIDER	Agent	Normal	Connection success	INFO	CONNECT_SUCCESS
5/9/2018 1:58:56 PM	C20-SSO-INSIDER	Agent	Normal	Connection to AD server restored	INFO	LDAP_AVAILABLE

- Aller dans le menu « Configuration des logs » dans « Options »
- Déplacer le filtre générique "." à la fin de la liste.
- Cliquer sur « Déployer » sur l'environnement pour actualiser le serveur.



Environment Manager / Log Manager									
<input type="checkbox"/> Check Out <input type="checkbox"/> Refresh <input checked="" type="checkbox"/> Check In <input type="checkbox"/> Undo CheckOut									
Types	<input type="checkbox"/> + <input type="checkbox"/> x <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>								
Software Logs									
System Logs									
Network Logs									
Device Logs									
1	<input checked="" type="checkbox"/>	<input type="checkbox"/> Action	<input type="checkbox"/> Status	<input type="checkbox"/> User interface	<input type="checkbox"/> Pop-up	<input type="checkbox"/> Database	<input type="checkbox"/> Syslog	<input type="checkbox"/> SMTP	<input type="checkbox"/> %SOURCE%...
	<input checked="" type="checkbox"/>	(#.)?CREATE	BLKEXECUTE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	.*	.*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*\\av\\AVTC\\la... .*
	<input checked="" type="checkbox"/>	.*	.*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*\\av\\AVTC\\... .*
	<input checked="" type="checkbox"/>	(#.)?LOCK-KEY	BLK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?AV	.*	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?SUSPECT-D...	.*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?BAD-KEY	BLK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?SOCK-.*	.*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*\\av\\AVTC\\... .*
	<input checked="" type="checkbox"/>	.*-DRIVER	.*	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?HOOKED-D...	.*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?BLOCKED-...	.*	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?*	RDONLY	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?OPEN	BLK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?OPEN	EXT-BLK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?CREATE	BLK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?CREATE	EXT-BLK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*
	<input checked="" type="checkbox"/>	(#.)?CREATE	BLKCREATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	.*(<.*><.*><.*>)? .*

- Frédéric Odenrio, conseiller du système d'informations
- Boris Denvert, administrateur base de données confirmé

Le 18 mars, ce jalon technique est validé, en compagnie de MOE, MOA, AMOA, les administrateurs, le CODIR et COPIL.



STORMSHIELD

III. PLANNING

Étapes	Mars 2018		Avril 2018			
PHASE DE RÉALISATION	S11	S12	S13	S14	S15	S16
Formation technique avec le prestataire Stormshield	Toute l'équipe					
Préparation de l'environnement test	MK, XK, RH, MT					
Tester la compatibilité de SES avec le firewall SN210		BD, MK, ML				
Tester la compatibilité de SES avec les logiciels de cybersécurité existants		ML, MK, XK, FO, NA, BD				
Activation et tests des différents modules de la Solution sur des postes tests			PM, ML, MK, BD			
Activation et tests des contrôles et audits des périphériques				RH, MT, XK, ML		
Étude sur la configuration standard de la Solution et de ses modules						MOA, PM, MK
Recettes fonctionnelles						MOA, MOE, PM, FO

- **Toute l'équipe projet :**

- MOE= Mr Simon Fournier, du service infrastructure réseau et système.
- MT = Michael Taudili, conseiller du système d'informations
- FO= Frédéric Odenrio, conseiller du système d'informations

- NA = Nathan Ambert, technicien réseau et Télécom
- MK =Michel Kali, expert infrastructures du SI
- XK = Xavier Klein, expert infrastructures SI



STORMSHIELD

- BD = Boris Denvert, administrateur de base de données confirmé
- PM = Paul Mileme, coordinateur projet SI
- **MOA= Eleonore Lauren, directrice du système d'informations**
- AMOA= Sandrine Polette, MSSSI-DPO
- ML = Maxime Lauris, expert infrastructure SI
- RH = Romain Hélios, technicien réseau Télécom Expert.

Étapes	Mai 2018			
PHASE DE MISE EN ŒUVRE	S17	S18	S19	S20
Déploiement de la Solution sur l'ensemble des postes fixes	Pôle déploiement			
Activation et coordination du déploiement de la Solution sur les postes nomades			MB, VA	
Réalisation d'un document à usage interne		PW, CG		
PHASE D'EXPLOITATION - MAINTENANCE				Pôle assistance

- **Pôle déploiement :**

- SV = Sarah Valerbe, référent support technique utilisateur
- VA = Victor Anemos, référent technique support utilisateur
- MB = Malika Benaya, référent technique support utilisateur

- **Pôle assistance :**

- TE =TourianEn'ma, consultant infrastructure SI
- PW = Patrick Wilson, référent technique support utilisateur
- CG = Charlie Ganegue, consultant infrastructure SI



STORMSHIELD

IV. BILAN DES COÛTS

Nous rappelons que le coût des licences pour Stormshield Endpoint Security et les frais de formations externes par le prestataire ont déjà été payés par la CFCM.

Le bilan des coûts est le suivant :

	Jours estimés	Jours consommés	Coût HT/jour	Total consommé	Budget de départ
Coût Internes					
Expression des besoins	7	6	825	4950	5775
Étude préalable	8	9	825	7425	6600
Étude détaillée	16	16	825	13200	13200
Étude technique	5	5	825	4125	4125
Réalisation	26	0	825	-	21450
Mise en œuvre (déploiement)	3	0	825	-	2475
Coûts annexes	-	-	-	-	100
Coûts externes					
Achat matériel					4500
TOTAL	89	27		29700	58225



STORMSHIELD

V. SUIVI DU PROJET

Étapes de la mise en place du projet	Date	Intervenants aux réunions
1. EXPRESSION DES BESOINS		
Lancement de la phase d'expression des besoins	05 février 2018	- Comité de direction et de pilotage du projet - MOA - AMOA - MOE - AMOA
Expressions des besoins	06-07 février 2018	
Contraintes du projet	08-09 février 2018	
Définition des indicateurs de réussite	10-11 février 2018	
Validation de l'expression des besoins → Lancement de la phase d'étude préalable	12 février 2018	- MOA
2. ÉTUDE PRÉALABLE		
Bilan de l'existant	13-16 février 2018	- MOE - MOA
Validation du bilan de l'existant	17 février 2018	- MOA
Présentation des trois possibilités d'implémentation de la Solution SES	20 février 2018	- La MOA - La MOE - AMOA - Les administrateurs de la base de données - Les administrateurs de la console SES - Les administrateurs des serveurs SES
Choix de l'implémentation de la Solution	23 février 2018	- La MOA - AMOA - La MOE - Les administrateurs de la base de données - Les administrateurs de la console SES - Les administrateurs des serveurs SES - Le comité de direction et de pilotage du projet.
Validation de l'étude préalable → Lancement de l'étude détaillée		
3. ÉTUDE DÉTAILLÉE		
Définition et préparation de	Du 26	- MOA



STORMSHIELD

l'architecture fonctionnelle	février au 02 mars 2018	- MOE
Étude des différentes fonctionnalités	Du 03 mars au 7 mars 2018	- MOA - AMOA - MOE
Analyse des configurations proposées pour chaque fonctionnalité	Du 8 mars au 12 mars 2018	- Les administrateurs de la base de données - Les administrateurs de la console SES - Les administrateurs des serveurs SES
Validation des configurations et des paramétrages → Lancement de l'étude technique	13 mars 2018	- Le comité de direction et de pilotage du projet. - MOA - AMOA - MOE - Les administrateurs de la base de données - Les administrateurs de la console SES - Les administrateurs des serveurs SES
4. ETUDE TECHNIQUE		
Création des fichiers de configuration sur clé USB sécurisée et paramétrage de l'installation de la solution	Du 13 mars au 16 mars 2018	- MOA - MOE - Consultant CFCM
Etablissement du cahier des charges technique sur l'ensemble des fonctionnalités	Du 03 mars au 11 mars 2018	- MOA - AMOA - MOE - Les administrateurs de la base de données - Les administrateurs de la console SES - Les administrateurs des serveurs SES
Vérification de sécurité	Du 12 mars au 18 mars 2018	- MOA - AMOA - MOE
Validation de l'étude technique et du cahier des charges → Lancement de la phase de réalisation	19 mars 2018	- Le comité de direction et de pilotage du projet. - MOA - AMOA - MOE - Les administrateurs de la base de



STORMSHIELD

		données - Les administrateurs de la console SES - Les administrateurs des serveurs SES
--	--	--