



**STORMSHIELD**

## ÉTUDE DÉTAILLÉE

Nom du projet	Déploiement de la SES	Version	1.0
Auteur	Vincent Draghi	Date de mise à jour	28/01//2019
Destinataire	Chef de projet	Référence	Étude détaillée



# STORMSHIELD

<b>I. INTRODUCTION</b>	<b>3</b>
A. Objectifs du document	3
<b>II. ÉTUDE DETAILLÉE</b>	<b>4</b>
A. Architecture fonctionnelle	4
1- Configuration de la console d'administration	5
2- Configuration des serveurs Stormshield Endpoint Security	5
3- Configuration du serveur de base de données	5
4- Configuration des postes agents	5
B. Analyses des fonctionnalités	6
1-Mécanismes de Protections	6
2- Politique de sécurité	7
3- Chiffrement	14
4- Surveillance de l'activité	17
<b>III. PLANNING</b>	<b>21</b>
<b>IV. BILAN DES COÛTS</b>	<b>25</b>
<b>V. SUIVI DU PROJET</b>	<b>26</b>



# STORMSHIELD

## I. INTRODUCTION

Le 23 février 2018, lors d'une réunion consacrée au choix du type de déploiement à mettre en œuvre, le comité de direction et de pilotage du projet accepte sans détour la première solution proposée par MOE. Il a été jugé pertinent et efficace de déployer la Solution sur l'ensemble du parc informatique. L'estimation des charges suit la méthodologie basée sur l'avis des experts de l'équipe projet et du comité de pilotage, et d'un planning validé pour le reste des phases à exécuter.

MOE, avec le soutien de MOA, souhaite s'appuyer sur la même équipe qu'il y a deux ans, lors de la mise en œuvre de projets qui s'était déroulée avec succès. Il s'agissait respectivement en mars 2016, de la migration de la protection anti-malware Panda Adaptive Defense vers Kaspersky Total Security et en Juin 2017, de l'installation du Pare feu Stormshield SN210 (imposées par la caisse nationale).

### A. Objectifs du document

Le document vise à définir les spécifications fonctionnelles de Stormshield Endpoint Security (SES), détaillées par catégories :

- Mécanismes de Protections
- Politique de sécurité
- Chiffrement
- Surveillance de l'activité

Ce document a pour intérêt sur le plan organisationnel d'actualiser les charges et le planning déjà engagés et qui se poursuivent pour les prochaines phases du projet (dont l'étude détaillée, l'étape de réalisation, la mise en œuvre).



# STORMSHIELD

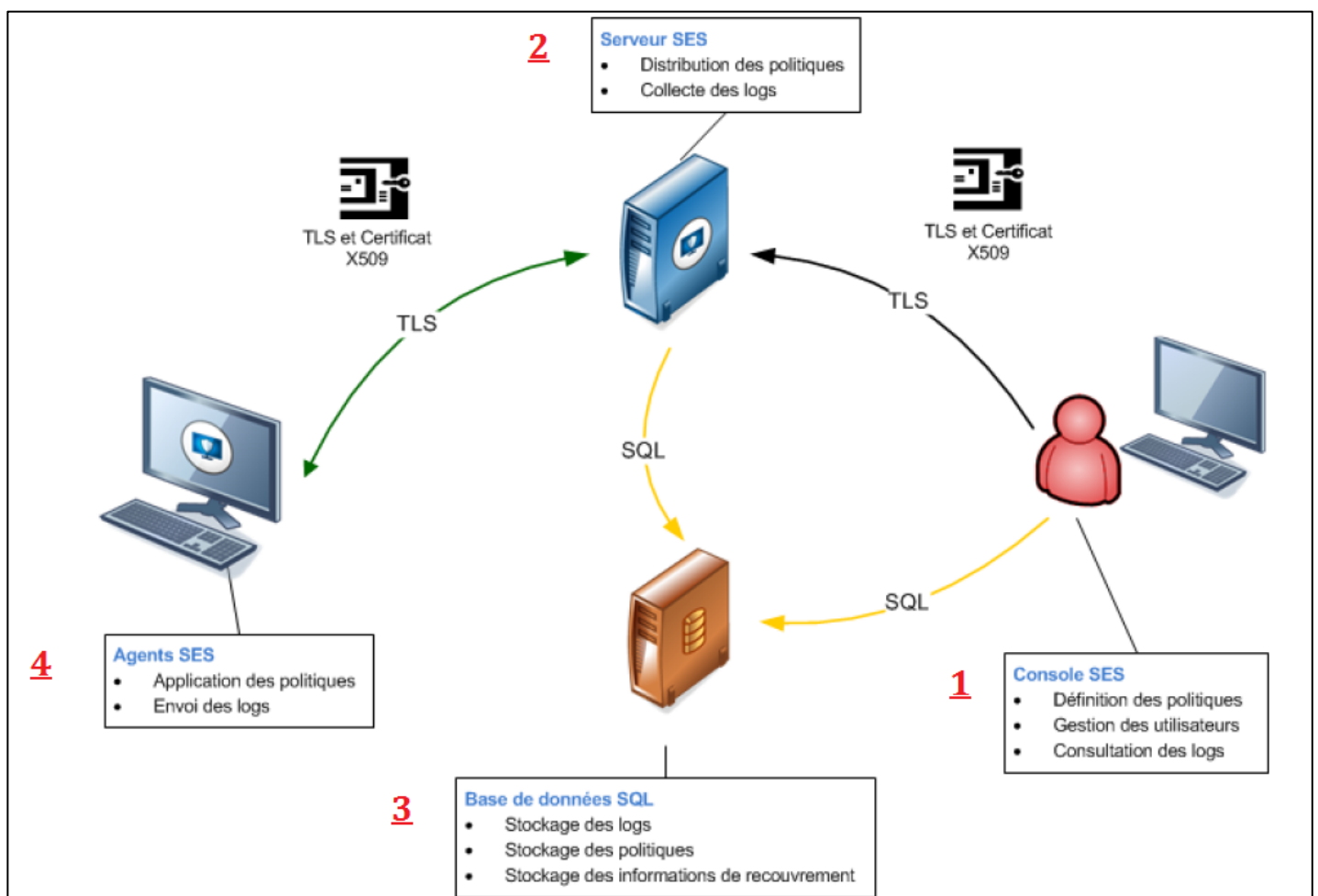
## II. ÉTUDE DÉTAILLÉE

Entre le 26 février 2018 et le 02 mars 2018, MOA (**Mme Eléonore Lauren**, directrice du département des systèmes d'informations) a spécifié les besoins et les principaux modules de la solution à analyser, tester, puis proposer une configuration optimale.

Le chef de projet est MOE (**Mr Simon Fournier** du service infrastructure réseau et système) est responsable de la solution technique en mettant en œuvre la réalisation. Il s'engage à faire part à la MOA de l'avancement du projet (rapports) ainsi que des livrables (modules). Le recettage des livrables n'aura lieu que lors de la mise en œuvre.

### A. Architecture fonctionnelle

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





## STORMSHIELD

En tant que chef de projet, **Mr Simon Fournier** a proposé la constitution de l'équipe en définissant les futurs postes clés et responsabilités. La configuration ci-dessous et les attributions des rôles avaient été acceptés lors de l'instance plénière du 28 février 2018.

### 1) 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.

Le poste sera situé au DSI, au Service Infrastructure réseau et systèmes, pôle système, sous la responsabilité de deux administrateurs (en cas d'absence ou congé) : Michel Kali et Xavier Klein.

### 2) 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.

Les deux serveurs seront situés au DSI, au Service Infrastructure réseau et systèmes, pôle réseau sous la responsabilité de Romain Helios et de Nathan Ambert.

### 3) Configuration du serveur de base de données

La politique de sécurité et les journaux sont stockés dans une base de données SQL qui peut être hébergée sur une machine dédiée.

Le poste sera situé au DSI, au Service Infrastructure réseau et systèmes, pôle réseau. L'administrateur de la base de données est Boris Denvert (Maxime Lauris en suppléant).

### 4) Configuration des postes agents

Sur chaque poste client, l'agent SES applique la politique de sécurité et remonte sur le serveur les événements qu'il génère.

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.

- Sarah Valerbe (pôle déploiement) sera chef d'équipe et supervisera le bon déroulement du déploiement lors de la phase de mise en œuvre.

- Patrick Wilson (pôle assistance) sera chef d'équipe pour la partie assistance aux utilisateurs lors de la phase d'exploitation-maintenance.



# STORMSHIELD

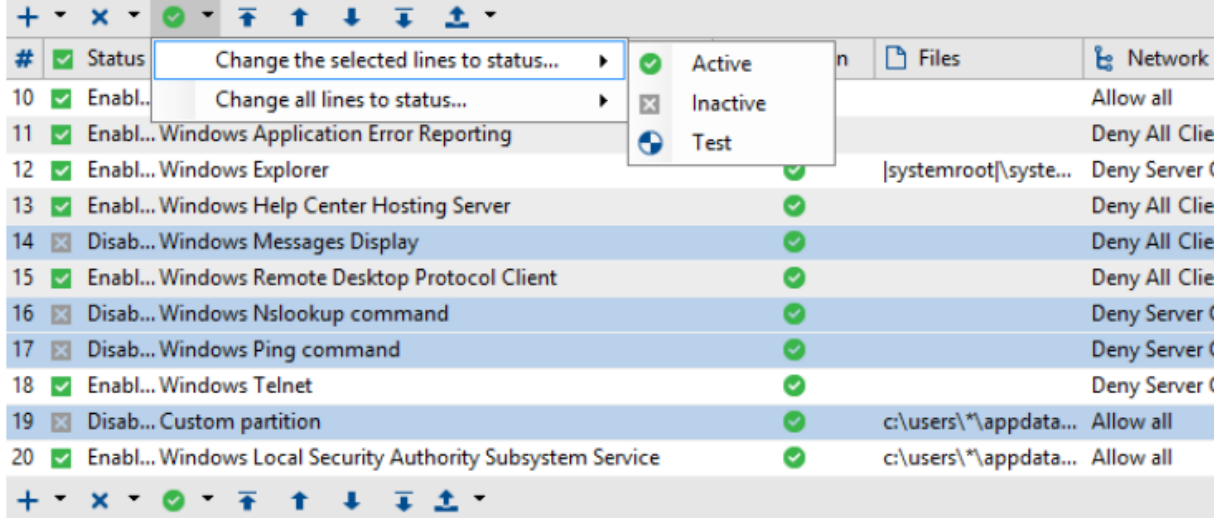
## B. Analyses des fonctionnalités

### 1- Mécanismes de Protections

Fonction détaillée	Mécanismes de protection
Description	<p>*Protections automatiques : elles protègent l'activité système et réseau au niveau du poste Client. On peut désactiver totalement ou partiellement ces protections.</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>Ces deux modes de protection sont appliqués selon un ordre défini : d'abord la protection par règles, puis les protections automatiques. Cet ordre fait prévaloir la politique définie explicitement par l'administrateur (protection par règles).</p> <p>Les protections automatiques détectent et bloquent les anomalies. Elles ne nécessitent pas de configuration de la part de l'administrateur. Cependant, ce dernier peut affiner le niveau de réaction de Stormshield Endpoint Security à différents types d'événements. Les informations ainsi collectées permettent de défendre le poste contre :</p> <ul style="list-style-type: none"><li>• Les tentatives de corruption des exécutables.</li><li>• Les tentatives d'accès à certains services ou données sensibles du système.</li></ul> <p>En général, la protection consiste en un rejet de l'appel système en cause, l'application continuant dans ce cas à fonctionner.</p> <p>Sept catégories de règles sont possibles :</p> <ul style="list-style-type: none"><li>• <u>Composants kernel</u> : cette catégorie sert à contrôler le chargement des drivers et à détecter les drivers suspects sur les postes de travail en 32 bits uniquement.</li><li>• <u>Périphériques amovibles</u> : cette catégorie détermine les périphériques amovibles susceptibles d'être utilisés par les postes clients.</li><li>• <u>Firewall réseau</u> : cette catégorie permet un contrôle statique et dynamique du firewall réseau.</li><li>• <u>Règles applicatives</u> : cette catégorie regroupe :<ul style="list-style-type: none"><li>◦ Toutes les règles associées à l'exécution des applications.</li><li>◦ Toutes les règles associées à la modification des applications.</li><li>◦ L'ensemble des applications locales de notre SI et nationales seront intégrées.</li></ul></li><li>• <u>Extensions</u> : cette catégorie sert à définir des règles en fonction du type de fichier, quelle que soit l'application qui y accède.</li><li>• <u>Applications de confiance</u> : cette catégorie permet de libérer certaines applications de tout type de contrôle afin d'éviter un éventuel blocage intempestif.</li></ul> <p>- <u>Politique de liste blanche et liste noire à configurer</u> : L'approche liste blanche consiste à interdire tout ce qui n'est pas explicitement autorisé.</p>



# STORMSHIELD

	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.
Acteurs concernés	<ul style="list-style-type: none"> <li>- Michael Taudili, conseiller du système d'information</li> <li>- Maxime Lauris, expert infrastructure du SI</li> <li>- Paul Mileme, coordinateur projet SI</li> <li>- Romain Hélios, technicien réseau Télécom Expert.</li> </ul>
Contrainte	Paramétrage au cas par cas des listes avec le MSSSI (AMOA)
Interface	
DÉCISION	05/03/2018 : vu avec AMOA et validé par MOA

## 2- Politique de sécurité

Fonction détaillée	1- Identifiants d'applications
Description	<p>Avant de créer une politique de sécurité et de mettre en place un contrôle applicatif, il est nécessaire de créer des identifiants d'applications.</p> <p>Chaque identifiant est constitué d'un nombre potentiellement illimité d'entrées. Chaque entrée permet d'identifier une application selon plusieurs critères :</p> <ul style="list-style-type: none"> <li>• Un chemin partiel ou complet vers le fichier exécutable</li> <li>• Un hash MD5 ou SHA-1 du fichier exécutable</li> <li>• Une signature numérique effectuée par un certificat spécifique</li> <li>• Une combinaison de chemin (partiel ou complet) de l'exécutable ainsi que la signature numérique de celui-ci.</li> </ul> <p>Dans notre situation il a été choisi l'identification par certificat de signature.</p> <p>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,</p>



# STORMSHIELD

	<p>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.</p> <p>Lorsqu'une application signée est exécutée, sa signature est vérifiée afin de s'assurer que son intégrité n'a pas été altérée. Une fois cette opération terminée, l'agent recherche le certificat qui a servi à signer l'application dans ceux qui lui ont été transmis par la console d'administration. Si celui-ci est dans sa liste, alors il appliquera la règle applicative associée.</p>
Acteurs concernés	<ul style="list-style-type: none"> <li>- Frédéric Odenrio, conseiller système d'informations (pôle application)</li> <li>- Xavier Klein, expert infrastructures SI</li> <li>- Sarah Valerbe, référent support technique utilisateur</li> <li>- Boris Denvert, administrateur de base de données confirmé</li> </ul>
Contrainte	Mise en place des certificats de signature
Interface	
DÉCISION	<b>07/03/2018 : MOA valide l'identification des applications par signature</b>

Fonction détaillée	2- Comportement Système
Description	<p>Permet de paramétrer le contrôle du comportement du système ainsi que le contrôle du comportement des applications.</p> <p>Liste des fonctionnalités et niveau de sécurité pour notre SI :</p> <ul style="list-style-type: none"> <li>- <u>Blocage des attachements</u> : le mécanisme d'attachement aux applications permet à un code malveillant de : <ul style="list-style-type: none"> <li>○ Arrêter le fonctionnement d'une autre application.</li> <li>○ Corrompre l'application.</li> <li>○ Prendre le contrôle de l'application.</li> </ul> </li> </ul>





## STORMSHIELD

	<ul style="list-style-type: none"><li>- <u>Contrôle des exécutions</u>: ce mécanisme contrôle le lancement des applications installées sur le poste. Un code malveillant peut en effet être dissimulé dans une application autorisée.</li><li>- <u>Contrôle des exécutions sur périphérique amovible</u> : une confirmation est demandée à l'utilisateur lorsqu'un fichier exécutable (.exe) est lancé depuis un périphérique amovible.</li><li>- <u>Accès au réseau</u> : politique de liste blanche dans laquelle aucun accès réseau n'est autorisé à moins qu'il ne soit explicitement déclaré.</li><li>- <u>Accès aux fichiers</u> : toute tentative de renommage d'un fichier est soumise à une vérification. Toute tentative de modification d'un exécutable est bloquée.</li><li>- <u>Composants Kernel</u>: contrôle automatique du chargement des drivers et détection des drivers suspects.</li></ul>																																																																		
Acteurs concernés	<ul style="list-style-type: none"><li>- Michel Kali, expert infrastructures du SI</li><li>- Michael Taudili, conseiller du système d'informations</li><li>- Nathan Amber, technicien réseau et Télécom</li></ul>																																																																		
Contrainte	Niveau de paramétrage de ce module à ajuster selon les faux positifs lors des phases de test.																																																																		
Interface	<div><div><div><div></div><div></div><div>Application Behavior Control</div></div><div><div>Applications access</div><div>Execution control</div><div>Execution control on removable device</div><div>Socket access</div><div>File access</div></div></div><div><div>Kernel Components</div><table><tr><th>#</th><th>Name</th><th>Checksum</th><th>Loading</th><th>Log</th><th>Description</th></tr><tr><td>0</td><td>\rasppoe.sys</td><td>01FEF58A6D2AE...</td><td>✓</td><td>—</td><td></td></tr><tr><td>1</td><td>\vmmouse.sys</td><td>02B6C2294C394...</td><td>✓</td><td>—</td><td></td></tr><tr><td>2</td><td>\CompositeBus.sys</td><td>051AD6A2FF362...</td><td>✓</td><td>—</td><td></td></tr><tr><td>3</td><td>\WdNisDrv.sys</td><td>07733E0BA667E...</td><td>✓</td><td>—</td><td></td></tr><tr><td>4</td><td>\luafv.sys</td><td>0877F73680E8F1...</td><td>✓</td><td>—</td><td></td></tr><tr><td>5</td><td>\intelide.sys</td><td>08BC74F4973B2...</td><td>✓</td><td>—</td><td></td></tr><tr><td>6</td><td>\storahci.sys</td><td>09B93F4899933B...</td><td>✓</td><td>—</td><td></td></tr><tr><td>7</td><td>\intelpep.sys</td><td>0A73324FBADC...</td><td>✓</td><td>—</td><td></td></tr><tr><td>8</td><td>\ksecdd.sys</td><td>0B0AAA0263585...</td><td>✓</td><td>—</td><td></td></tr><tr><td>9</td><td>\kbdclass.sys</td><td>0C58E22140B16...</td><td>✓</td><td>—</td><td></td></tr></table></div></div>	#	Name	Checksum	Loading	Log	Description	0	\rasppoe.sys	01FEF58A6D2AE...	✓	—		1	\vmmouse.sys	02B6C2294C394...	✓	—		2	\CompositeBus.sys	051AD6A2FF362...	✓	—		3	\WdNisDrv.sys	07733E0BA667E...	✓	—		4	\luafv.sys	0877F73680E8F1...	✓	—		5	\intelide.sys	08BC74F4973B2...	✓	—		6	\storahci.sys	09B93F4899933B...	✓	—		7	\intelpep.sys	0A73324FBADC...	✓	—		8	\ksecdd.sys	0B0AAA0263585...	✓	—		9	\kbdclass.sys	0C58E22140B16...	✓	—	
#	Name	Checksum	Loading	Log	Description																																																														
0	\rasppoe.sys	01FEF58A6D2AE...	✓	—																																																															
1	\vmmouse.sys	02B6C2294C394...	✓	—																																																															
2	\CompositeBus.sys	051AD6A2FF362...	✓	—																																																															
3	\WdNisDrv.sys	07733E0BA667E...	✓	—																																																															
4	\luafv.sys	0877F73680E8F1...	✓	—																																																															
5	\intelide.sys	08BC74F4973B2...	✓	—																																																															
6	\storahci.sys	09B93F4899933B...	✓	—																																																															
7	\intelpep.sys	0A73324FBADC...	✓	—																																																															
8	\ksecdd.sys	0B0AAA0263585...	✓	—																																																															
9	\kbdclass.sys	0C58E22140B16...	✓	—																																																															
DÉCISION	09/03/2018 : MOA impose l'activation de ces modules liés à la surveillance du comportement du système.																																																																		



## STORMSHIELD

Fonction détaillée	3-Contrôle des périphériques
Description	<p>Le contrôle de l'utilisation des périphériques concerne les éléments suivants de notre SI :</p> <ul style="list-style-type: none"><li>◦ Ports infrarouges.</li><li>◦ Ports parallèles.</li><li>◦ Ports séries.</li><li>◦ Lecteurs de cartes à puce USB.</li><li>◦ Dispositifs de pointage (exemples : souris, tablettes graphiques, etc.) et HID (HumanInterface Device) claviers.</li><li>◦ Fonctionnalité U3 : bloque l'exécution des Autorun sur les clés USB U3 et les lecteurs de CD-ROM.</li><li>◦ Périphériques de stockage de masse (exemples : clés et disques durs USB, FireWire, etc.).</li></ul> <p>Il est possible de paramétrer efficacement des groupes de périphériques amovibles via la <u>Gestion des groupes</u> : activation ou désactivation des groupes de périphériques amovibles.</p> <p>Les paramètres du groupe peuvent comprendre les éléments suivants en fonction du type de périphérique sélectionné :</p> <ul style="list-style-type: none"><li>◦ <u>Type du périphérique</u> : stockage amovibles, USB, CD/DVD</li><li>◦ <u>Droit d'accès par défaut</u> : l'utilisateur a les droits d'accès en lecture aux périphériques de stockage de la liste. S'il tente d'écrire sur un de ces périphériques, l'action sera bloquée et l'événement sera enregistré dans le log des périphériques.</li></ul>
Acteurs concernés	<ul style="list-style-type: none"><li>- Maxime Lauris, expert infrastructure SI</li><li>- Charlie Ganegue, consultant infrastructure SI</li><li>- Tourian En'ma, consultant infrastructure SI</li></ul>
Contrainte	S'assurer du rappel des règles utilisateurs vis-à-vis des périphériques, et médias amovibles (contenu à usage strictement professionnel)



**Environment Manager**

- Servers
- Policies**
  - Environment
  - Log Manager
- Monitoring
- Console Manager
- Devices

**App Identifiers**

- Policies
- Server Configuration
- Dynamic Agent Configuration
- Static Agent Configuration
- Security
  - Certificates
  - App Identifiers**
    - Base
    - DefaultSecurityPolicy
    - Process access
- Encryption
  - Script
  - Script Resources
  - Files Deployment

**POLICIES / SECURITY / App Identifiers**

App Identifiers

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\backgroun...	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\spmvsvc.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\setuppho...	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	

App Identifiers entries

Type	Value	Description
------	-------	-------------

**Devices**

Modem	Allowed
Bluetooth	Allowed
IrDA	Allowed
LPT	Allowed
Com	Allowed
USB Smart Card	Allowed
Floppy	Allowed
CD/DVD/Blu-Ray	Allowed
CD/DVD/Blu-Ray Writer	Allowed
PCMCIA card	Allowed
USB audio	Allowed
USB HID	Allowed
USB still imaging	Allowed
USB printer	Allowed
U3 feature	Allowed
USB/FW mass storage	Allowed

**Removable devices settings**

Group management	Enabled
Mass storage recovery	Denied
Mandatory password minimum strength	Low

**11/03/2018 : Le chef de projet n'a pas jugé nécessaire d'activer la surveillance et le contrôle des dispositifs de pointage, ainsi que les lecteurs CD-Rom. MOA a souhaité tout de même activer ces fonctionnalités car certains postes informatiques dans différents locaux emploient toujours ce type de dispositif.**




































## STORMSHIELD

Fonction détaillée	4- Contrôle de la sécurité réseau
Description	<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)). Ils viennent en remplacement aux précédents dispositifs peu satisfaisants (voir existant, étude préalable).</p> <p>L'intérêt de l'IDS proposé est multiple :</p> <ul style="list-style-type: none"><li>• L'IDS embarqué confère au poste client des capacités autonomes de détection d'attaques, même en situation de mobilité hors des systèmes protecteurs du réseau de l'entreprise.</li><li>• L'IDS génère des alertes identifiant précisément les attaques reconnues.</li></ul> <p>L'IDS est associé au firewall intégré dans Stormshield Endpoint Security afin de constituer un système de prévention d'intrusion (IPS). L'IPS alertera les administrateurs et bloquera en temps réel les attaques au niveau du trafic entrant.</p> <p>Le réglage de la sensibilité de l'IDS (&gt;Haute) active les fonctionnalités IPS suivantes :</p> <ul style="list-style-type: none"><li>- <u>Protection contre le flood</u> (suppression des connexions &gt; 20)</li><li>- <u>Protection contre le balayage de ports</u> (filtrage et blocage des paquets au niveau des ports et blocage de l'IP associée si nécessaire)</li><li>- <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).</li></ul>
Acteurs concernés	<ul style="list-style-type: none"><li>- Xavier Klein, expert infrastructures SI</li><li>- Nathan Ambert, technicien réseau et Télécom</li><li>- Frédéric Odenrio, conseiller du système d'informations</li></ul>
Contraintes	<ul style="list-style-type: none"><li>- Ajustement de la sensibilité du réglage de l'IDS et de l'IPS après les tests, et régulièrement après le déploiement.</li><li>- Désinstaller correctement le précédent IDS.</li></ul>



## STORMSHIELD

Interface	 <b>Network Activity Control</b>																					
	<table><tr><td>Firewall State</td><td> Enabled</td></tr><tr><td>IDS sensitivity</td><td> Low</td></tr><tr><td>TCP stateful integrity check</td><td> Disabled</td></tr><tr><td>ICMP stateful integrity check</td><td> Disabled</td></tr><tr><td>Integrity check of Ethernet frames</td><td> Disabled</td></tr><tr><td>IPv4 integrity check</td><td> Disabled</td></tr><tr><td>TCP integrity check</td><td> Disabled</td></tr><tr><td>UDP integrity check</td><td> Disabled</td></tr><tr><td>ICMP integrity check</td><td> Disabled</td></tr><tr><td>Protection against fragmented headers</td><td> Disabled</td></tr><tr><td>Protection against port scan</td><td> Disabled</td></tr></table>	Firewall State	 Enabled	IDS sensitivity	 Low	TCP stateful integrity check	 Disabled	ICMP stateful integrity check	 Disabled	Integrity check of Ethernet frames	 Disabled	IPv4 integrity check	 Disabled	TCP integrity check	 Disabled	UDP integrity check	 Disabled	ICMP integrity check	 Disabled	Protection against fragmented headers	 Disabled	Protection against port scan
Firewall State	 Enabled																					
IDS sensitivity	 Low																					
TCP stateful integrity check	 Disabled																					
ICMP stateful integrity check	 Disabled																					
Integrity check of Ethernet frames	 Disabled																					
IPv4 integrity check	 Disabled																					
TCP integrity check	 Disabled																					
UDP integrity check	 Disabled																					
ICMP integrity check	 Disabled																					
Protection against fragmented headers	 Disabled																					
Protection against port scan	 Disabled																					
DÉCISION	12/03/2018 : MOA valide mais pense qu'il faudra ajuster le niveau de paramétrage sur le long terme (lors des phases d'exploitation).																					

Fonction détaillée	5-Firewall réseau - Règles applicatives
Description	<p>Stormshield Endpoint Security dispose d'un firewall réseau dont le fonctionnement est contrôlé à la fois de façon :</p> <ul style="list-style-type: none"><li>• Statique (règles)</li><li>• Dynamique (déterminé par la sensibilité de l'IDS et la gravité des alertes IDS).</li></ul> <p>Le fonctionnement statique est déterminé par les règles.</p> <p>Le filtre ne se basera pas les adresses MAC ou les ports mais un contrôle applicatif (cela nécessite par conséquent la création d'identifiants d'applications (voir <b>Fonction détaillée</b> n°1).</p> <p>En complément avec les listes blanches/noires, il s'agira de paramétrer strictement les attributs suivants :</p> <ul style="list-style-type: none"><li>• les règles applicatives.</li><li>• les extensions.</li><li>• les applications de confiance.</li></ul>
Acteurs concernés	<ul style="list-style-type: none"><li>- Michel Kali, expert infrastructures du SI</li><li>- Maxime Lauris, expert infrastructure du SI</li><li>- Romain Hélios, technicien réseau Télécom expert</li><li>- Tourian En'ma, consultant infrastructure du SI</li></ul>
Contrainte	Essayer d'éviter la redondance des règles déjà mises en place par rapport au boîtier firewall Stormshield SN210



# STORMSHIELD

Interface

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

Trusted Rules / System

#	Status	Identifier	Application scope	Rules evaluation	Access to this application
1	Enabled	Stormshield Endpoint Monitor	Application and children	Go to next rule	✓
2	Enabled	Windows Media Player	Application and children	Go to next rule	✗
3	Enabled	Windows Registry editor	Application and children	Go to next rule	✗
4	Enabled	Windows Update	Application and children	Go to next rule	✗
5	Enabled	Windows Application Layer Gateway Service	Application and children	Go to next rule	✓
6	Enabled	Windows Indexing Service	Application and children	Go to next rule	✓
7	Enabled	Windows Virtual DOS Machine	Application and children	Go to next rule	✗
8	Enabled	Windows Mobility Center	Application and children	Go to next rule	✗
9	Enabled	Windows Client Server Runtime Process	Application and children	Go to next rule	✓
10	Enabled	Windows Defender	Application and children	Go to next rule	✓
11	Enabled	Windows Sidebar	Application and children	Go to next rule	✓
12	Enabled	Windows Explorer	Application and children	Go to next rule	✓

DÉCISION

13/03/2018 : MOA valide mais souhaite que les règles applicatives soient en concordance avec la liste des applications de confiance, comme établie par l'assistance maîtrise d'ouvrage (MSSI)

## 3- Chiffrement

Cette partie aborde les fonctionnalités consacrées au chiffrement. Ce dernier constitue un enjeu majeur imposé au niveau national. Lors d'une réunion de suivi de projet (Étude des différentes fonctionnalités) ayant eu lieu le 11 mars 2018, MOA souhaitait rappeler les contraintes imposées par la caisse nationale, suite aux vols d'ordinateurs portables rapportés. Il appartient cependant à la CPCM d'appliquer localement des paramètres personnalisés en priorisant les services les plus soucieux des principes d'intégrité et de confidentialité. MOA et AMOA (en tant que MSSI et DPO) précisent qu'il s'agit principalement de se préoccuper des ordinateurs portables des agents en télétravail dans le cadre de la protection des données de l'entreprise dans le prolongement de la politique nationale.

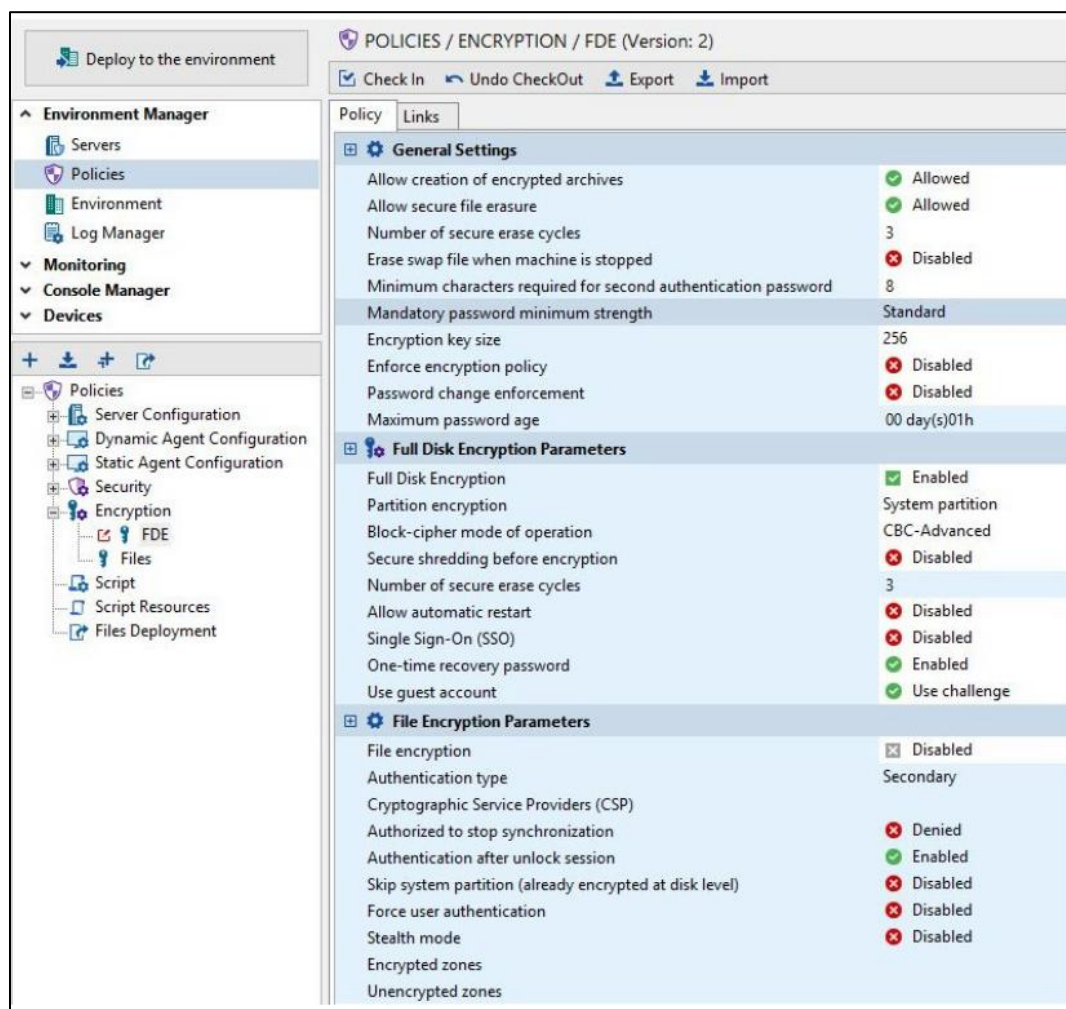
Sur ce point, le 12 mars 2018, le comité de pilotage a souhaité une revue des configurations proposées pour chaque fonctionnalité. Il a également été validé la complémentarité des deux mesures mise en place pour renforcer le chiffrement.

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





# STORMSHIELD



Fonction  
détaillée

## 1- Chiffrement de fichiers

Description

La fonctionnalité de chiffrement de Stormshield Endpoint Security est basée sur le standard de chiffrement avancé (Advanced Encryption Standard (AES)). Nous utiliserons systématiquement des clés en 128 bits (comme pour le cryptage PGP des mails vers nos partenaires sociaux)

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

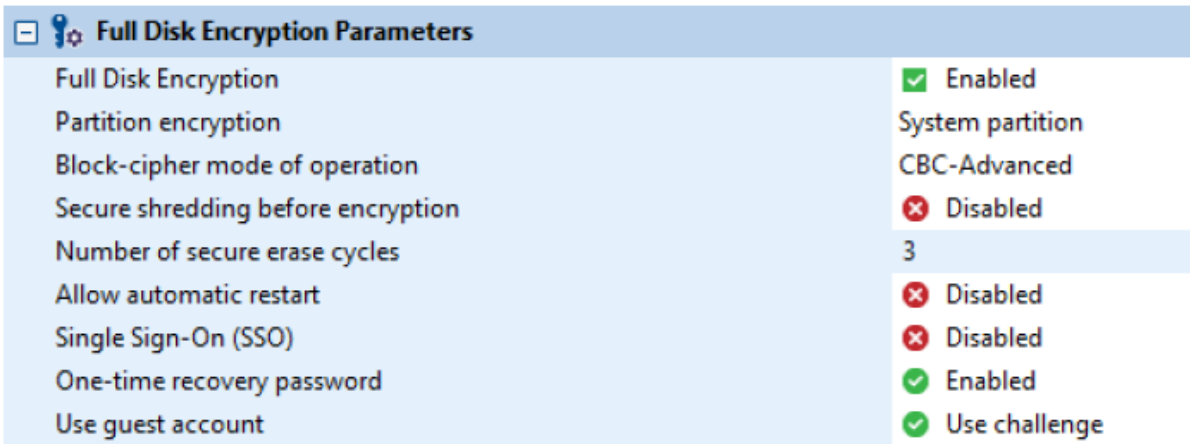
	<p>La politique de chiffrement visera automatiquement les agents en télétravail qui se déplacent avec un ordinateur portable chez eux et les emmènent dans nos locaux sur des bases/d'accueil.</p> <p>Les administrateurs peuvent également agir manuellement à distance après des processus de synchronisation des postes à la politique de chiffrement.</p>
Acteurs concernés	<ul style="list-style-type: none"><li>- Romain Hélios, technicien réseau Télécom Expert</li><li>- Michael Taudili, conseiller du système d'informations</li><li>- Boris Denvert, administrateur base de données confirmé</li></ul>
Contrainte	Néant
Interface	
DÉCISION	<b>14/03/2018 : MOA s'aligne à la proposition du chef de projet et maintient la taille minimale des clés en 128 bits</b>

Fonction détaillée	2- Chiffrement du disque
Description	<p>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).</p> <ul style="list-style-type: none"><li>• Tout est chiffré, même la configuration de l'ordinateur.</li></ul> <p>Il devient encore plus important lorsque les administrateurs souhaitent chiffrer des fichiers ou des configurations sensibles enregistrées directement par un logiciel dans des dossiers de programme.</p> <ul style="list-style-type: none"><li>• Le déploiement du chiffrement total du disque est plus facile que celui du chiffrement de fichiers.</li></ul>





## STORMSHIELD

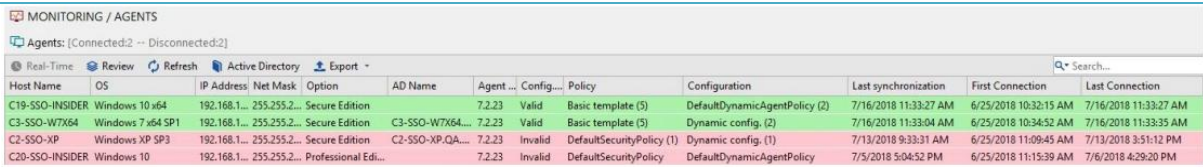
	<p>Les paramètres pour le chiffrement total du disque permettent de contrôler les paramètres suivants :</p> <ul style="list-style-type: none"><li>• Chiffrement des partitions.</li><li>• Mode opératoire de chiffrement.</li><li>• Effacement sécurisé avant chiffrement.</li><li>• Nombre de cycles d'effacement sécurisé (avant le premier chiffrement).</li><li>• Autoriser les redémarrages automatiques.</li><li>• Authentification unique (SSO).</li><li>• Renouvellement automatique du mot de passe de recouvrement.</li><li>• Utilisation d'un compte invité.</li></ul> <p>Des lenteurs peuvent être observées à l'ouverture de session après le redémarrage des postes, juste après l'application d'une politique de chiffrement total de disque.</p>
Acteurs concernés	<ul style="list-style-type: none"><li>- Boris Denvert, administrateur base de données confirmé</li><li>- Maxime Lauris, expert infrastructure du SI</li><li>- Paul Mileme, coordinateur projet SI</li></ul>
Contrainte	Certains types de partitions de nos postes ne sont pas compatibles
Interface	
DÉCISION	<b>14/03/2018 : MOA accepte la configuration proposée, mais estime que cette fonctionnalité sera utilisée uniquement lors d'une procédure particulière à créer.</b>

### 4- Surveillance de l'activité

Fonction détaillée	1- Surveillance des agents
Description	<p>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 :</p> <ul style="list-style-type: none"><li>• Surveillance des agents.</li><li>• Tableau de bord.</li></ul>



## STORMSHIELD

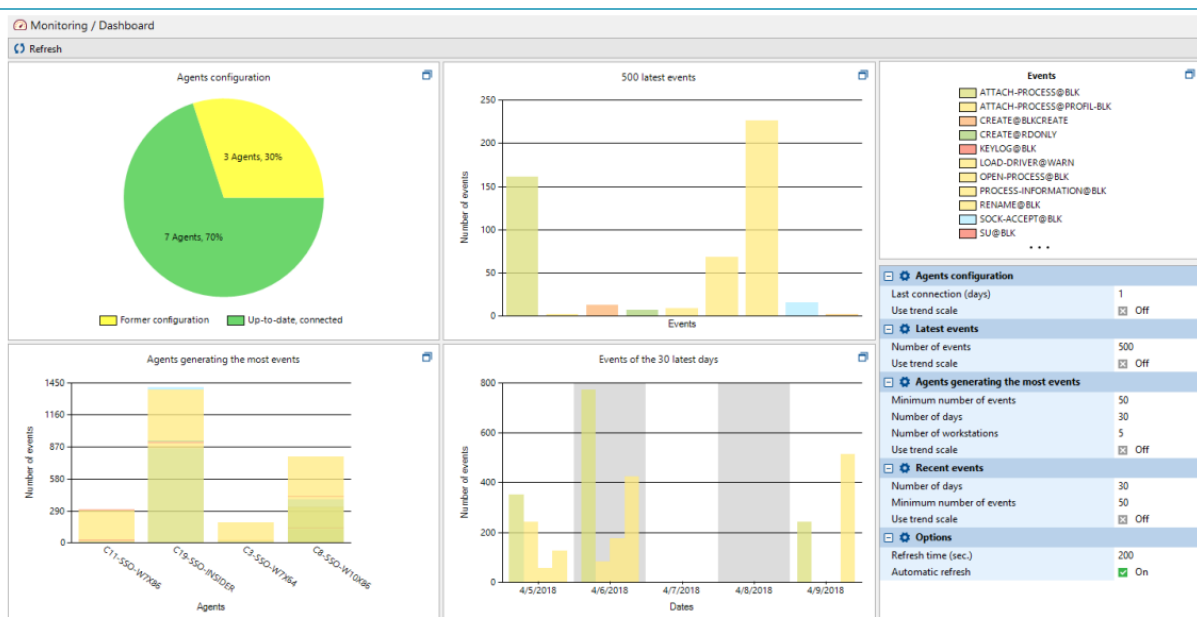
	<ul style="list-style-type: none"><li>• Logs.</li><li>• Configuration des logs.</li><li>• Audit de la console.</li></ul>
Acteurs concernés	- Nathan Ambert, technicien réseau et Télécom - Michel Kali, expert infrastructures du SI
Contrainte	Néant
Interface	
DÉCISION	15/03/2018 : MOA valide.

Fonction détaillée	2-Tableau de bord
Description	<p>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.</p> <p><u>Configuration des agents</u> : ce graphique permet de visualiser l'état de l'ensemble des agents Stormshield Endpoint Security du parc : tous les agents qui se sont connectés à un serveur sont pris en compte dans ce graphique.</p> <p><u>Histogramme des derniers événements</u> : ce graphique permet de lister les N derniers événements système qui se sont produits sur les agents du parc. Il offre un aperçu de l'activité récente sur les agents.</p> <p><u>Agents générant le plus d'événements</u> : ce graphique permet de visualiser les machines ayant généré le plus d'événements sur les derniers jours. Il permet d'identifier de potentielles attaques en cas de génération récente de nombreux logs de protection sur certaines machines.</p> <p><u>Événements récents</u> : ce graphique permet de visualiser les événements générés ces derniers jours par l'ensemble des machines. Les événements sont regroupés par jour et classés par importance.</p>
Acteurs concernés	- Xavier Klein, expert infrastructures SI
Contrainte	Néant



# STORMSHIELD

## Interface



## DÉCISION

**15/03/2018 :** le chef de projet a souhaité que le DSI surveille davantage de paramètres, mais MOA préfère pour l'instant se focaliser que sur les éléments retenus dans la description ci-dessus.

## Fonction détaillée

### 3- Surveillance des logs

## Description

La surveillance des logs enregistre toute activité suspecte sur les postes clients et la réaction correspondante de l'agent Stormshield Endpoint Security. Ces données sont envoyées à une base de données qui est consultable depuis la console d'administration.

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

- Logiciel
- Système
- Réseau
- Périphériques

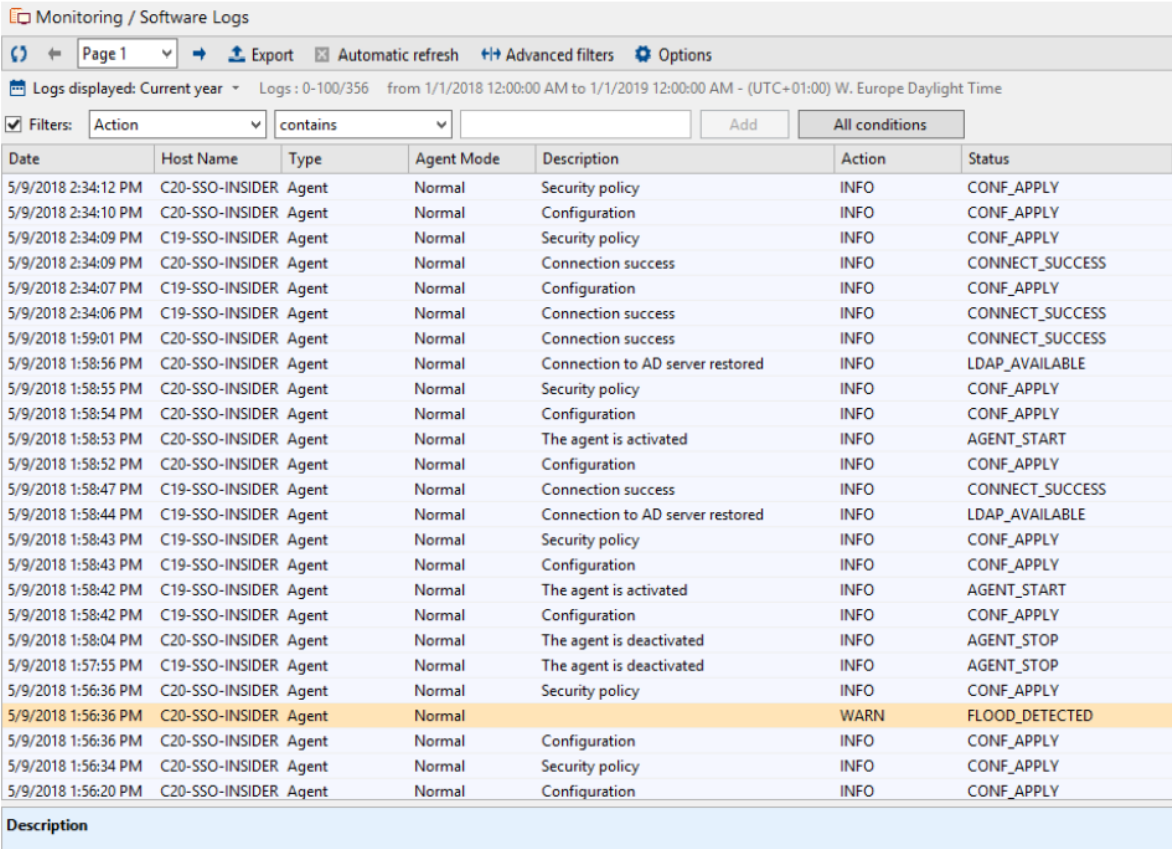
Les activités qui déclenchent un événement sont définies dans les politiques de sécurité. Les logs Logiciel enregistrent le comportement de l'agent à chaque fois que :

- L'agent applique une configuration ou une politique.
- L'agent télécharge un certificat ou une mise à jour.
- Il y a une surcharge de CPU sur un serveur.
- Le nombre d'agents est supérieur au nombre autorisé par la licence.

Les logs Système contiennent des informations sur la protection du système.



## STORMSHIELD

	<p>Les logs Réseau contiennent des informations sur les paramètres suivants :</p> <ul style="list-style-type: none"><li>• Firewall réseau (Catégorie).</li><li>• Système de détection d'intrusion (Paramètres généraux &gt; Protection de l'activité réseau).</li></ul> <p>Les logs Périphérique contiennent des informations sur les paramètres suivants :</p> <ul style="list-style-type: none"><li>• Périphériques amovibles (Catégorie).</li><li>• Contrôle des périphériques (Paramètres généraux).</li><li>• Authentification et chiffrement WiFi (Paramètres généraux).</li></ul>
Acteurs concernés	- Frédéric Odenrio, conseiller du système d'informations - Boris Denvert, administrateur base de données confirmé
Contrainte	Possible difficulté pour filtrer efficacement la grande quantité de logs
Interface	
DÉCISION	<b>16/03/2018 : MOA souhaite une fréquence et une sauvegarde des log hebdomadaires avec une version alternative détaillée en cas d'incident majeur (nécessaire pour les étapes de forensic)</b>



**STORMSHIELD**

### **III. PLANNING**

Le 19 Mars 2018, une réunion plénière a eu lieu en présence du comité de direction et de pilotage du projet, la MOA, la MOE, les administrateurs de la base de données, les administrateurs de la console SES, et les administrateurs des serveurs SES.

Le thème principal porta non seulement sur la validation des configurations et des paramétrages, mais aussi sur un ajustement du planning réaliste ainsi qu'un bilan des coûts. L'estimation des charges repose jusqu'à présent sur l'expertise du groupe projet mais aussi sur l'expérience acquise lors des précédents déploiements.



## STORMSHIELD

Étapes	Mars 2018		
Etude technique	S8	S9	S10
Création des fichiers de configuration sur clé USB sécurisée	MOE, MOA, FO, BD, NA, XK, ML		
Etablissement du cahier des charges technique sur l'ensemble des fonctionnalités		Toute l'équipe	
Vérifications de sécurité			Toute l'équipe

- **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
- 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
- NA = Nathan Ambert, technicien réseau et Télécom
- MK =Michel Kali, expert infrastructures du SI
- XK = Xavier Klein, expert infrastructures SI
- ML = Maxime Lauris, expert infrastructure SI
- RH = Romain Hélios, technicien réseau Télécom Expert.



## STORMSHIELD

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
- **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

- **NA** = Nathan Ambert, technicien réseau et Télécom
- **MK** = Michel Kali, expert infrastructures du SI
- **XK** = Xavier Klein, expert infrastructures SI
- **ML** = Maxime Lauris, expert infrastructure SI
- **RH** = Romain Hélios, technicien réseau Télécom Expert.



## STORMSHIELD

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 = Tourian En'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.

Tout comme le pour le planning, l'estimation des charges et du planning repose sur la méthode Delphi, fort des avis des experts et des projets précédemment réalisés dans une configuration similaire. Voir budget accepté lors de la dernière réunion plénière de l'étude préalable

<b>Ressources Humaines</b>	<ul style="list-style-type: none"><li>- Coût de Technicien informatique par jour mobilisé : 75 euros</li><li>- 11 techniciens informatiques sont mobilisés sur 2.5 mois =&gt; coût de 41250 euros</li><li>- <b>Coût total ressources humaines : 41 250 euros</b>, à partir de l'Etude Détaillée jusqu'à la phase d'exploitation.</li></ul>
----------------------------	--

Le bilan des coûts est le suivant :

	Jours estimés	Jours consommés	Coût HT/jour	Total consommé	Budget de départ
<b>Coût Internes</b>					
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
Réalisation	26	0	825	-	21450
Mise en œuvre (déploiement)	3	0	825	-	2475
Coûts annexes	-	-	-	-	100
Coûts externes					
Achat matériel					4500
<b>TOTAL</b>	<b>89</b>	<b>27</b>		<b>25575</b>	<b>58225</b>



**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
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 administrateursdes 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 administrateursdes serveurs SES - Le comité de direction et de pilotage du projet.
Validation de l'étude préalable → Lancement de l'étude détaillée		
3. ÉTUDE DÉTAILLÉE		



## STORMSHIELD

Définition et préparation de l'architecture fonctionnelle	Du 26 février au 02 mars 2018	- MOA - MOE
Étude des différentes fonctionnalités	Du 03 mars au 11 mars 2018	- MOA - AMOA - MOE
Analyse des configurations proposées pour chaque fonctionnalité	Du 12 mars au 18 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	19 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