CFCM IDF-FOD

NSY115-Conduite d'un projet informatique

2018-2019

Projet :

Déploiement de la solution de sécurité Stormshield Endpoint Security au sein de la Caisse de Paris de Couverture Maladie

Expression des besoins

Nom du projet	StormShield	**Version**	3.0
Auteur	Vincent Draghi	**Date de mise à jour**	02/01/209
Destinataire	Chef de projet	**Référence**	Expression des besoins

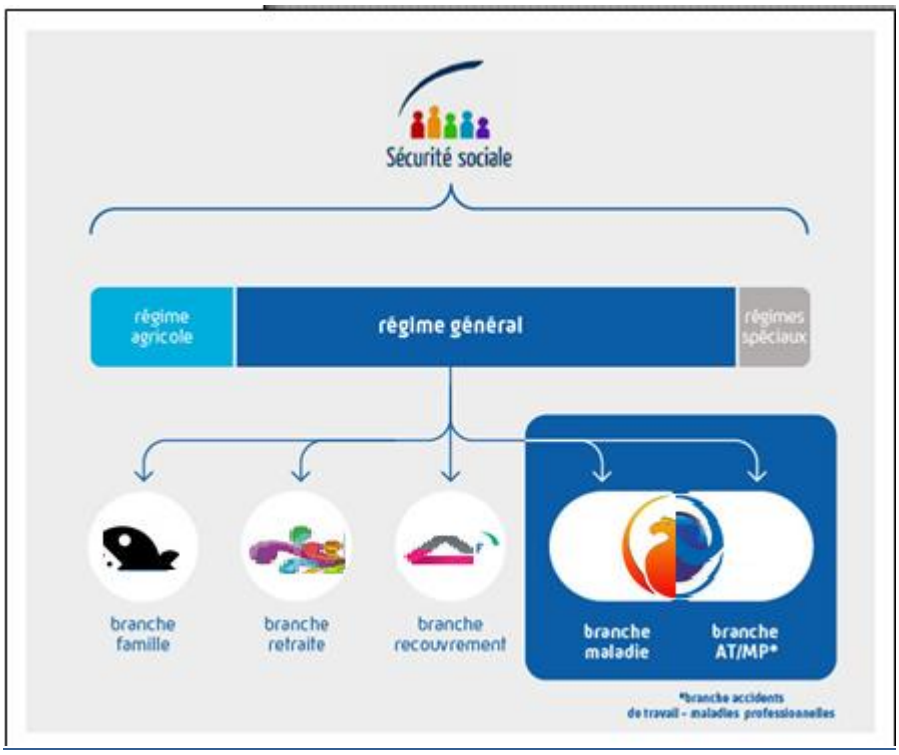
TABLE DES MATIERES

I. Présentation de la CPCM

A. La CPCM

La CPCM (Caisse de Paris de Couverture Maladie) est un organisme de droit privé à mission de service public, appartenant à la Sécurité Sociale. Elle est déclinée en différentes antennes locales.
Créée en 1945, la Sécurité sociale est la garantie donnée à chacun qu'en toutes circonstances il disposera des moyens nécessaires pour assurer sa subsistance et celle de sa famille dans des conditions décentes. En clair, elle a pour mission de protéger les Français contre tous les risques de la vie, en les accompagnants à chaque étape de leur existence.

La Sécurité sociale se compose de 5 branches :



La CPCM rembourse notamment les prestations maladies, maternité, accidents du travail et maladies professionnelles. Elle assure la prise en charge des dépenses de santé des assurés et garantit l'accès aux soins via l'immatriculation et l'affiliation des assurés. Elle effectue de la prévention de maladies et des actions sanitaires. C'est l'interlocutrice incontournable des assurés du régime général au niveau local (département 75). Plus 2 millions de personnes sont bénéficiaires des prestations offertes par la CPCM.

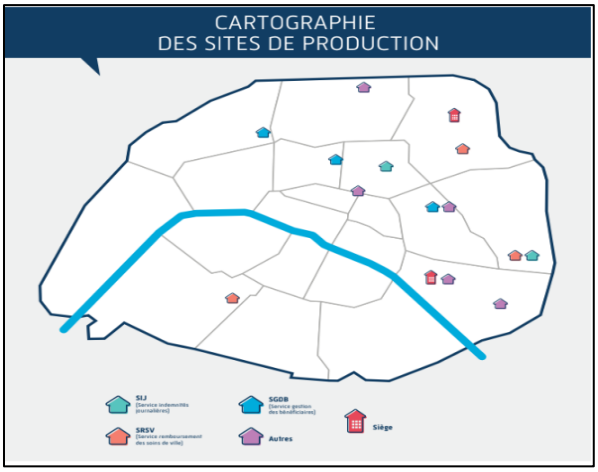
B. Les locaux

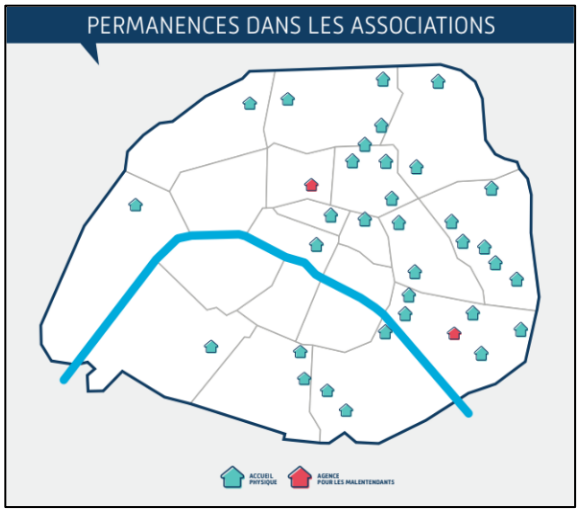
La CPCM comprend **49 locaux accessibles aux assurés**, déclinés sous plusieurs types :

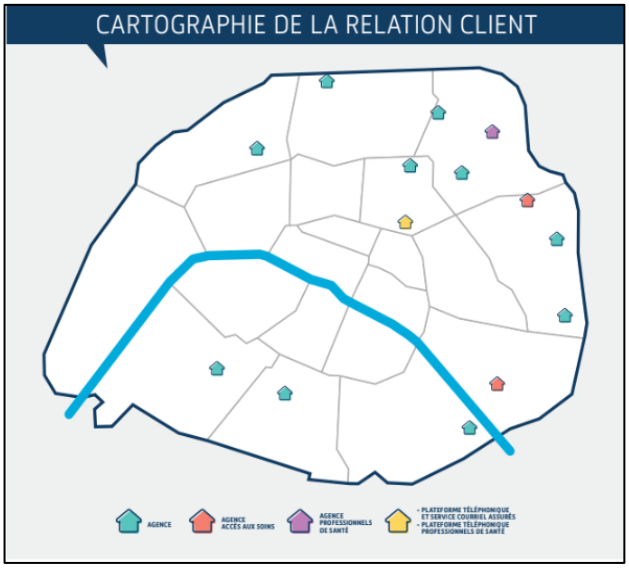
- 10 agences d'accueil du public - 1 plateforme téléphonique - 2 agences accès aux soins - 1 agence professionnelle
- 33 points d'accueil dans des associations - 2 agences pour malentendants

À cela s'ajoute **15 locaux réservés à l'administration de la CPCM :**

- 2 sièges
- 3 SRSV (Service de remboursement des soins de ville)
- 2 SIJ (Service indemnités journalières)
- 3 SGBD (Service de gestion des bénéficiaires)
- 5 Autres



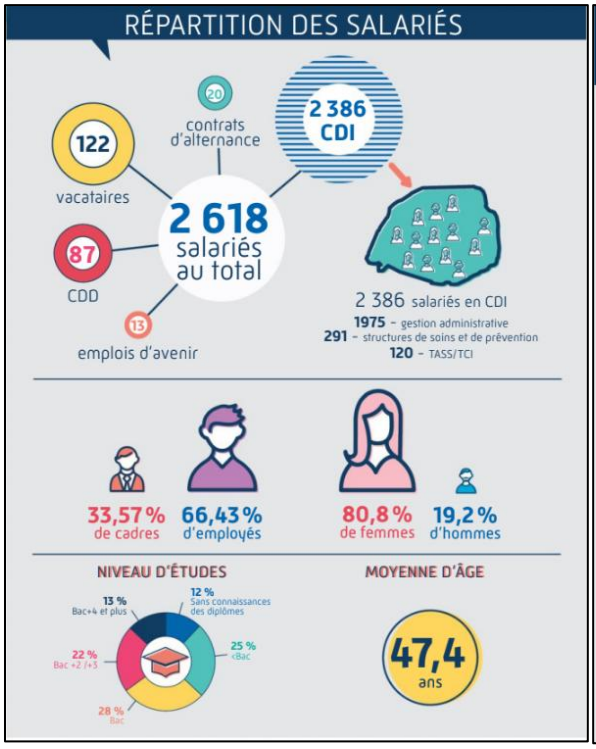


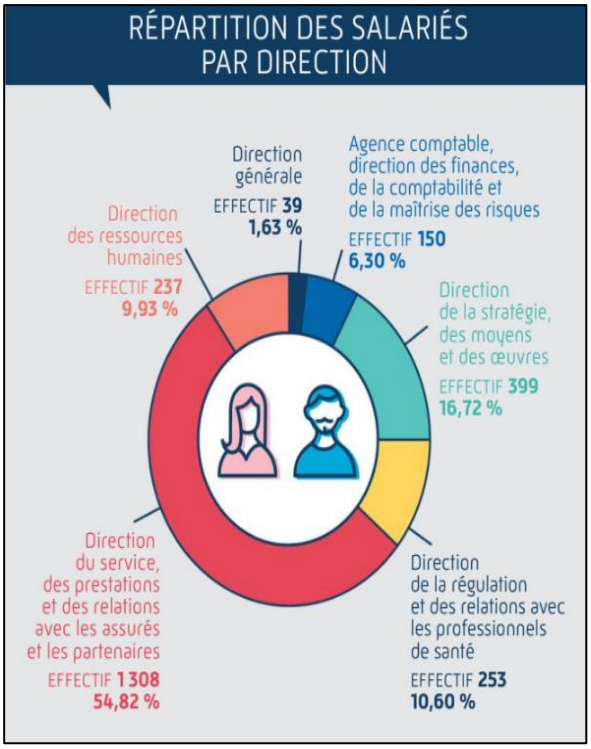


C. Les collaborateurs

La CPCM regroupe un ensemble de **2618 collaborateurs** répartis selon les grandes sections suivantes :

- ❑ Gestion administrative
  - ❑ Ressources Humaines
  - ❑ Comptabilité
  - ❑ Stratégie des moyens et des œuvres
  - ❑ Relations assurés et partenaires
  - ❑ Relations professionnelles
- ❑ Structure de soins
- ❑ Service contentieux





D. Le parc informatique

Tous ces services cumulent **3238 équipements informatiques principaux :**

- 2800 PC Fixes
- 78 Serveurs (Machines hôtes et physiques)
- 360 PC Portables
- Auxquels s'ajoutent 720 équipements divers (imprimantes, bornes multiservices, etc.)

Type de matériel	Quantité
Unités centrales	2800
Ecrans	4125
Serveurs (Machine hôte et physique)	78
Portables	360
Imprimantes bureautiques monochromes	340
Imprimantes bureautiques couleurs	36
Imprimantes multi- fonctions	76
Imprimantes multi- fonctions petit modèle	124
Scanners (Synergie et Diadème)	28
Onduleurs	18
BMS (Bornes Multi-Services sur pied ou en façade)	45

E. Le budget informatique et l'importance de la CPCM

Il est à noter que sur l'année 2017 la CPCM a investi 129 000€ en logiciels et 934 000€ en matériel informatique.

	2017 MONTANT EN MILLIERS D'€	2016 MONTANT EN MILLIERS D'€	ÉVOLUTION 2016/2017
IMMOBILISATIONS INCORPORELLES			
logiciels	129	63	104,76 %
IMMOBILISATIONS CORPORELLES			
terrain	-	-	-
constructions	12 371	5 629	119,77 %
matériel informatique	934	516	81,01 %
matériel de bureau	26	61	-57,38 %
autres	1 203	182	560,99 %
IMMOBILISATIONS FINANCIÈRES			
dépôts, cautionnements, autres créances immobilisées	5	3	66,67 %
TOTAUX	14 668	6 454	127,27 %

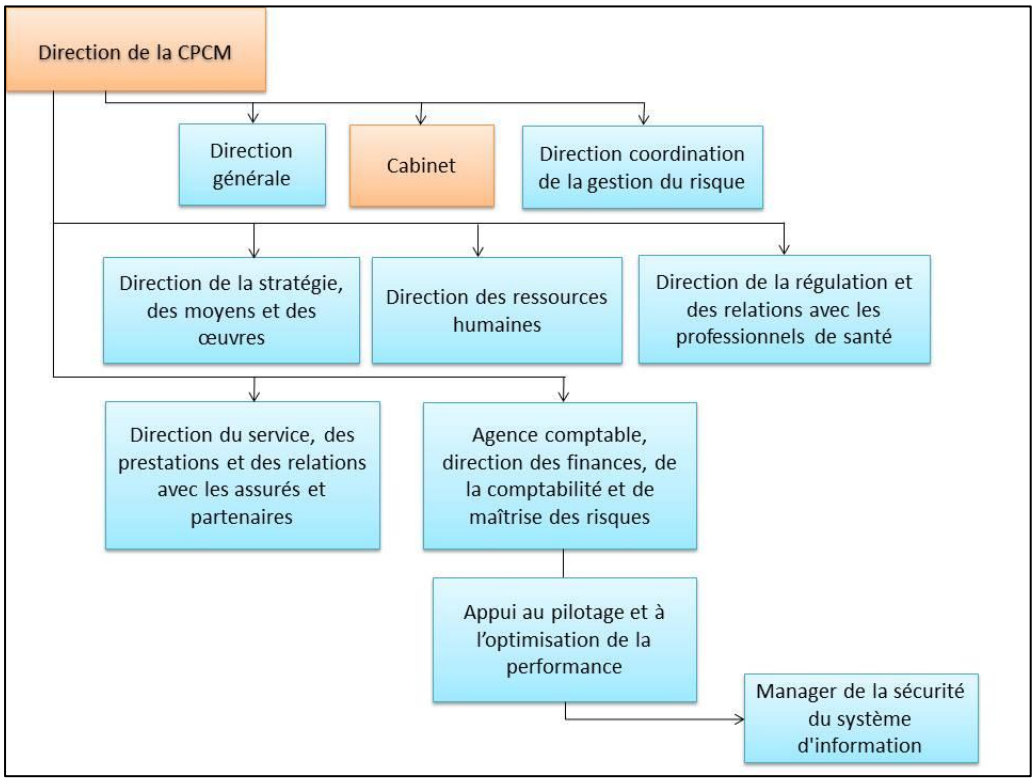
Douze secteurs d'activité d'importance vitale ont été définis dans un arrêté du 2 juin 2006, modifié par un arrêté du 3 juillet 2008, au sein desquels ont été identifiés des Opérateurs d'importance vitale (OIV) chargés de la protection de leur Point d'importance vitale (PIV). Chaque secteur est rattaché à un ministère coordonnateur chargé du pilotage des travaux et des consultations.

Différentes mesures ont été prises pour définir et renforcer la Sécurité des activités d'importance vitale du 23 février 2006, qui définit les activités d'importance vitale comme « un ensemble d'activités, essentielles et difficilement substituables ou remplaçables, concourant à un même objectif ou visant à produire et à distribuer des biens ou des services indispensables ».

L'importance de la CPCM réside dans le fait qu'elle correspond à une institution d'utilité publique et agit comme acteur principal dans le suivi et le remboursement des frais de santé. Les organismes de la Sécurité Sociale (dont la CPCM) sont considérés comme des OIV. L'ensemble des assurés a besoin de pouvoir faire appel à ces services sur les heures d'ouvertures de ses agences d'accueil et en permanence via le site Ameli.fr. Les assurés dépendent surtout des remboursements et des suivis que la CPCM prodigue et ils ne peuvent admettre une interruption de services qui la paralyse.

F. Les services et responsables de la CPCM

Son directeur général est M. Albert Drouet, en poste depuis 4 ans.



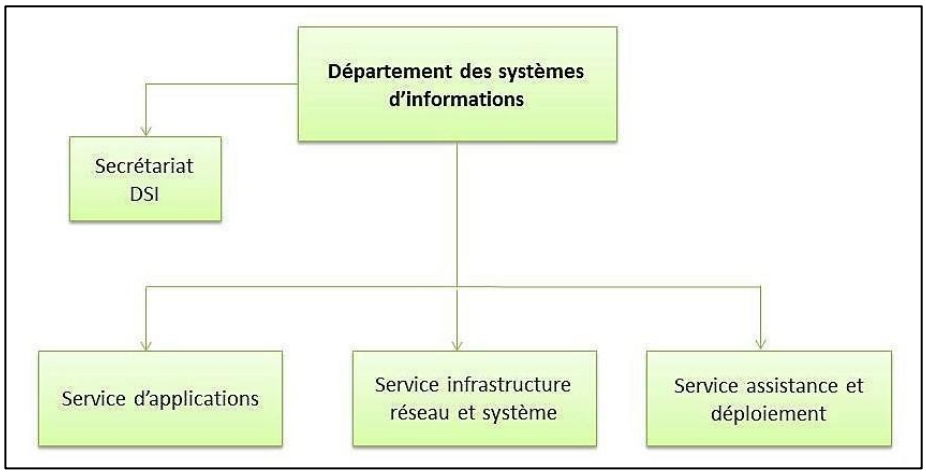
II. Présentation de la MOA et de la MOE

A. La MOA (celui qui Exprime le besoin)

La MOA est **Mme Eléonore LAUREN,** directrice du département des systèmes d'informations.

B. La MOE (Maîtrise d'œuvre)

La MOE est **Mr Simon FOURNIER** du service infrastructure réseau et système. Ce dernier, ainsi que les agents de son service, seront appuyés par les autres services informatiques (service d'applications, service assistance et déploiement) qui participeront à la rédaction et aux tests des différentes études antérieures et postérieures à la mise en place.

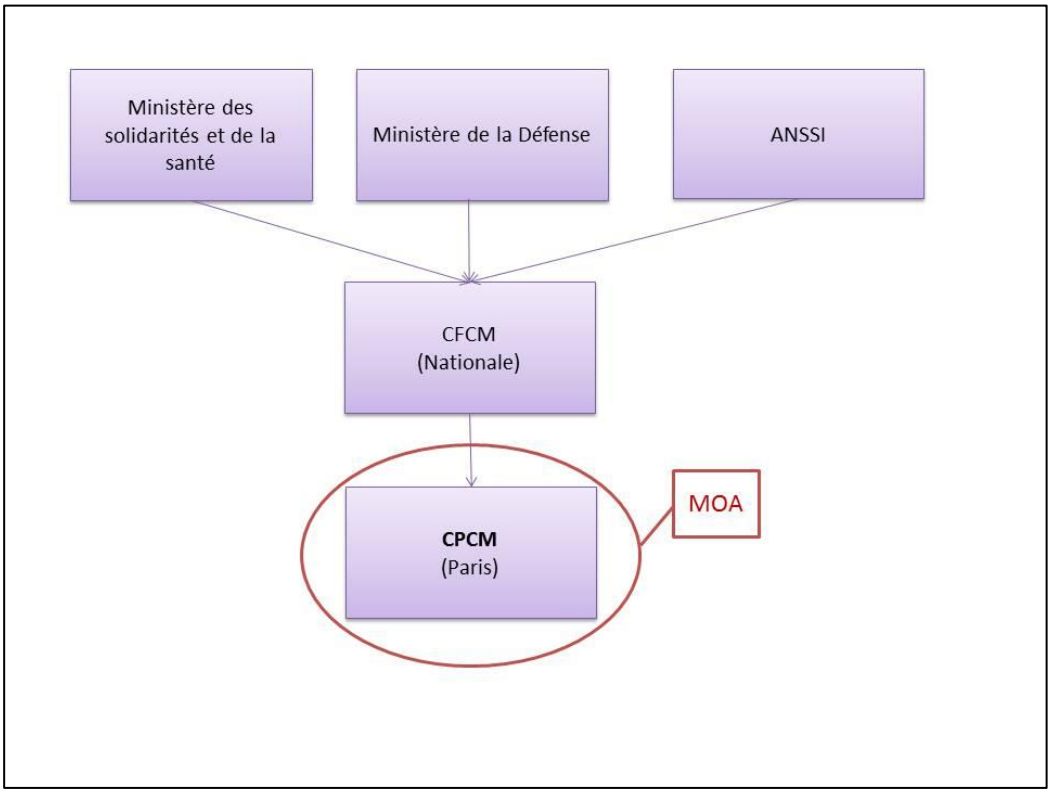


AMOA (Assistance à Maîtrise d'ouvrage)

L'AMOA est la manager de la sécurité du système d'information, **Mme Julie TEVENARD.**

III. Présentation du projet

Le projet est de déployer une solution de sécurité sur les établissements de la CPCM suite à une directive de la Caisse Française de Couverture Maladie (CFCM), qui elle, exécute les instructions du Ministère des Solidarités et de la Santé ainsi que celui du Ministère de la Défense. L'Agence Nationale de la sécurité des systèmes d'informations (ANSSI) émet également des recommandations. Les attentes de la CFCM sont simples : implémenter des outils augmentant la sécurité des CPCM au travers d'une nouvelle solution de sécurité.



Le projet actuel s'inscrit dans la continuité de la "défense en profondeur" des OIV. Après une étude de marché et un appel d'offre lancé par le Ministère des solidarités et la santé entre Novembre 2017 à Mars 2018, un prestataire a été choisi. Il s'agit de l'entreprise Française **Stormshield** et de sa solution de sécurité **Stormshield Endpoint Security**. Elle est également accréditée par l'ANSSI et déjà utilisée sur une partie des infrastructures du Ministère de la Défense.

Ce produit fut choisi car c'est la solution qui répondait le plus aux besoins de la CFCM en terme de complémentarité avec l'existant et de fiabilité de l'éditeur de la solution.

L'ensemble des structures de la CFCM est chargé de déployer la solution de sécurité. Suite à cette demande la CPCM représentée par la MOA doit installer la solution de sécurité Stormshield afin de répondre aux nouvelles attentes de sécurité d'une part, et se mettre en conformité comme le reste des caisses régionales de France d'autre part.
Il faut donc appliquer la demande de la CFCM, élever le niveau de sécurité des installations et obligatoirement utiliser Stormshield Endpoint Security, et ce en complément des mesures de sécurité déjà appliquées.
La CFCM n'ordonne pas un pilotage imposé mais laisse les caisses régionales effectuer les différentes phases du projet et de sa mise en place.

La MOA a donc pour obligation d'installer la solution Stormshield Endpoint Security au sein de son parc informatique.

C'est la MOE qui propose et exécute le projet avec le soutien de MOA à chaque étape de la mise en œuvre. MOE doit déterminer quelles fonctionnalités de la solution de sécurité qui seront appliquées. Il s'agit tout d'abord d'une complémentarité avec les mesures existantes, puis d'une amélioration de l'existant dans le cas où la solution serait plus performante.

Il est à noter que les coûts d'achats de la solution seront bien budgétés mais intégralement pris en charge par la CFCM. Les coûts de mise en place et fonctionnement sont à prendre en compte. L'étude préalable proposera divers solutions de déploiement avec un planning et des coûts respectifs.

A. Les attentes de la CFCM

Via son projet de mise en place de la solution de sécurité Stormshield Endpoint Security, la CFCM souhaite tout d'abord réduire les risques de sécurité qui pèsent sur la CPCM. Tout d'abord venant de l'extérieur tels que la réduction du nombre de cyberattaques réussites, la réduction drastique du nombre de postes infectés par des logiciels malveillants, et d'un nombre réduit de failles de sécurité. Puis venant de l'intérieur, une meilleure protection contre l'exfiltration de données, une réduction du risque de failles des logiciels et OS, une gestion accrue des périphériques type clés usb, afin de réduire le risque d'infection ainsi qu'une protection réseaux renforcée. La réduction de tous ses risques devrait s'accompagner d'une réduction des coûts en matière de sécurité et de maintenance des différents parcs informatiques.
Toutes ces attentes de la CFCM n'ont pas été chiffrées mais listées. Elles font suite aux rapports de ces dernières années concernant l'augmentation des cyberattaques et de l'augmentation de failles de sécurité diverses.

La CFCM attend donc de voir se réduire les problèmes de sécurité présents au sein des caisses régionales. Chacune d'entre elles devra donc, suite à l'installation de la solution de sécurité, pouvoir se justifier d'une sécurité informatique accrue au travers de statistique et de comparatif avant et après l'installation, ainsi que via des tests des nouvelles protections. Elle espère une réduction globale d'environ 50% des différents problèmes de sécurité présents sur les rapports de l'année passée.

IV. Les besoins

Les besoins émanent de la CFCM au niveau national (démarche d'harmonisation des règles de sécurité sur tout le territoire avec une PSSI commune). La CFCM impose au MOA de la CPCM la mise en place de la solution de sécurité Stormshield Endpoint Security.

La solution propose des fonctionnalités par défaut et une grande flexibilité quant au paramétrage et aux modules à activer. Ainsi les caisses régionales auront la possibilité d'effectuer des choix en matière de fonctionnalités à exploiter. Il s'agit tout d'abord d'une complémentarité avec les mesures existantes, puis d'une amélioration de l'existant dans le cas où la solution serait plus performante.

Il est attendu que la MOA intègre la solution de sécurité au sein de la CPCM et que la MOE en définisse les paramètres d'intégrations.

Le pilotage du projet est entièrement géré par la CPCM.

V. Les contraintes

La MOA :

- ➔ A pour obligation d'utiliser la solution Stormshield Endpoint Security sur l'ensemble des équipements de la CPCM.
- ➔ Doit avec la MOE déterminer quelles fonctionnalités de la solution seront appliquées. La solution doit pouvoir s'intégrer aux mesures de sécurité déjà présentes sur la CPCM. L'objectif était d'ajouter le plus de mesures pertinentes aux protections déjà présentes et d'améliorer celles qui peuvent l'être.
- ➔ Doit pouvoir justifier d'un gain de sécurité suffisant auprès de la CFCM.
- ➔ Doit avoir une équipe formée à l'utilisation et à la maintenance de la solution de sécurité.
- ➔ Doit, suite à la mise en place de la solution, réduire les coûts inhérents à la sécurité du parc informatique.
- ➔ Doit avoir terminé la mise en place de la nouvelle solution de sécurité avec un statut opérationnel au plus tard pour décembre 2018.

Le budget alloué à ce projet est une enveloppe de maximum 70 000 euros.

VI. Les indicateurs de réussite

- L'utilisation de la solution Stormshield Endpoint Security (SES) a bien été respectée et l'ensemble du parc est fonctionnel (80 serveurs, 2647 postes et 380 PC portables).

- Les fonctionnalités choisies complètent les mesures de sécurité déjà mises en place et ne font pas doublon avec l'existant. De même que si une des fonctionnalités de la solution de sécurité est meilleure qu'une déjà existante, elle doit être remplacée au profit de la solution Stormshield.
  L'ensemble des protections de sécurité doit agir en synergie et non en conflit à la fin du projet.

- S'assurer que la réduction de la maintenance en termes de sécurité est effective.

- L'ensemble du personnel concerné a été formé à la solution.

- Le délai de mise en place a été respecté.

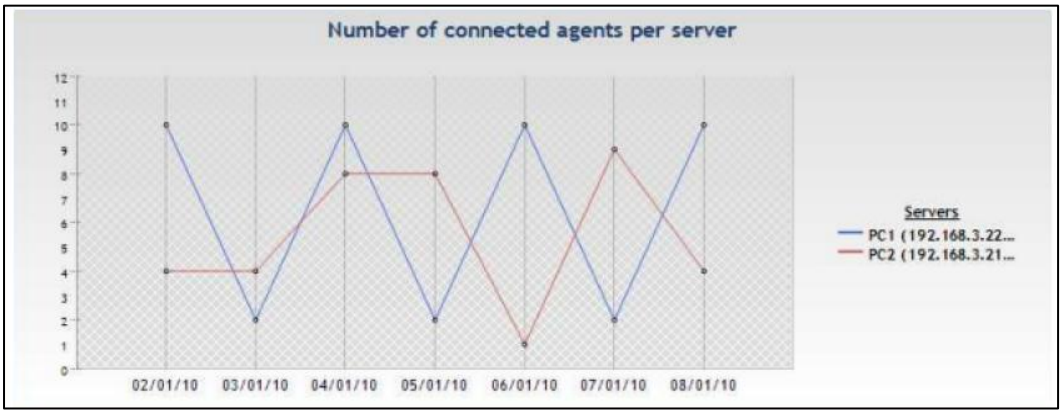
- La politique de sécurité du système d'information est en accord avec les règles strictes appliquées par la solution.

- Les alertes liées à la sécurité du parc sont réduites de 50% sur les indicateurs concernés (Plan de Maîtrise Socle : ordinateurs infectés, intrusions réseaux, fichiers infectés, etc…). Des tests d'intrusion doivent révéler un nombre moins important de failles qu'avant la mise en place de la solution.

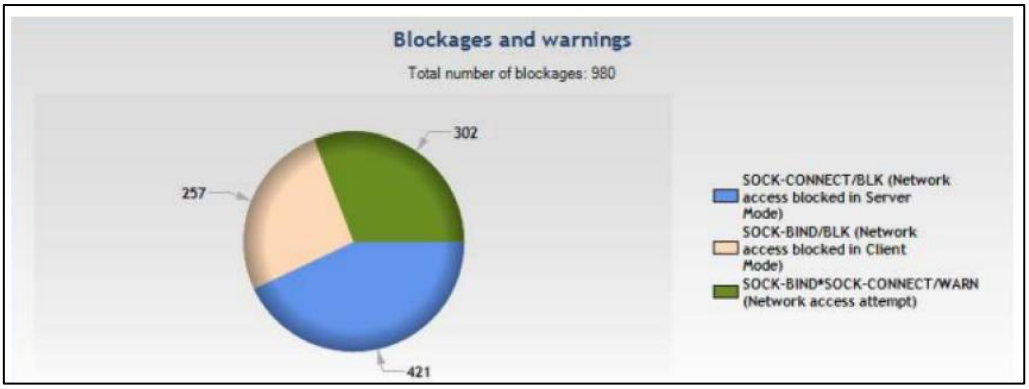
- Les entités dirigeantes valident la mise en place de la solution, notamment le directeur général et le MSSI. Les rapports d'audits complets sont à envoyer à la CFCM après la phase d'implémentation et à la fin de l'ensemble des tests cités précédemment ; puis un rapport est attendu tous les 2 ans afin de constater des gains de sécurité.

Les gains attendus par la MOA s'appuieront sur des rapports générés par la solution SES issus de logs. Plusieurs métriques seront collectées tel que l'efficacité des préventions, blocages et filtrages par la solution (voir les illustrations non exhaustives suivantes) :

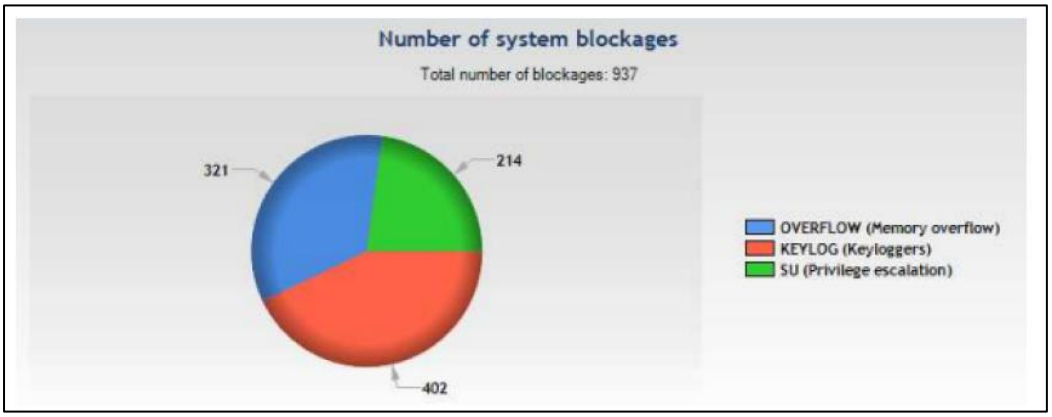
- Nombre d'agents connectés par serveur (métrique de performance pour les deux serveurs où seront installés la console d'administration)



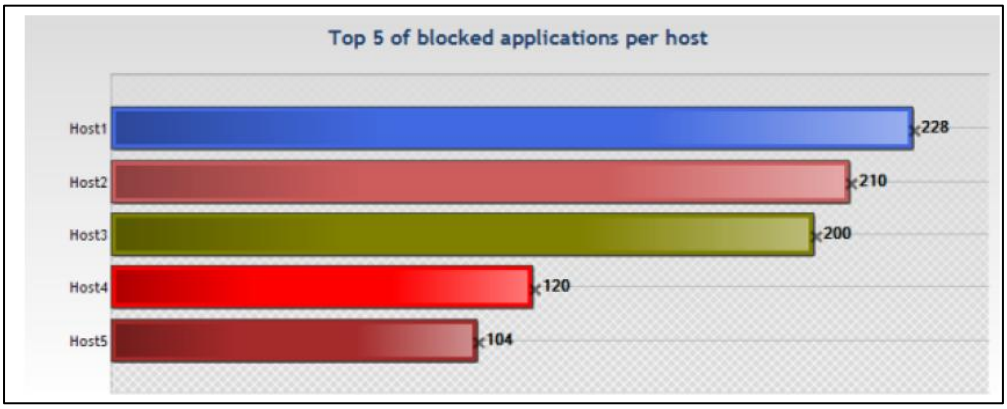
- Intégrité du poste de travail (blocages et alertes)



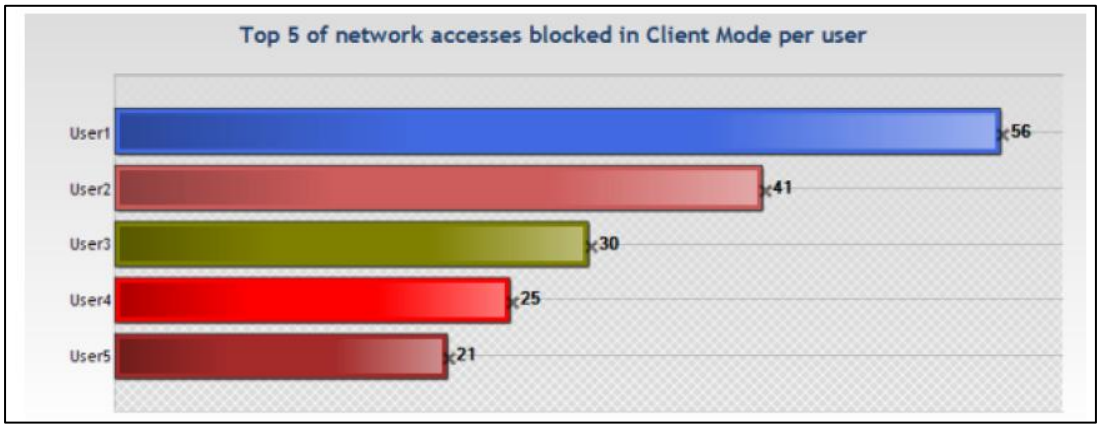
- Nombre de blocages système :



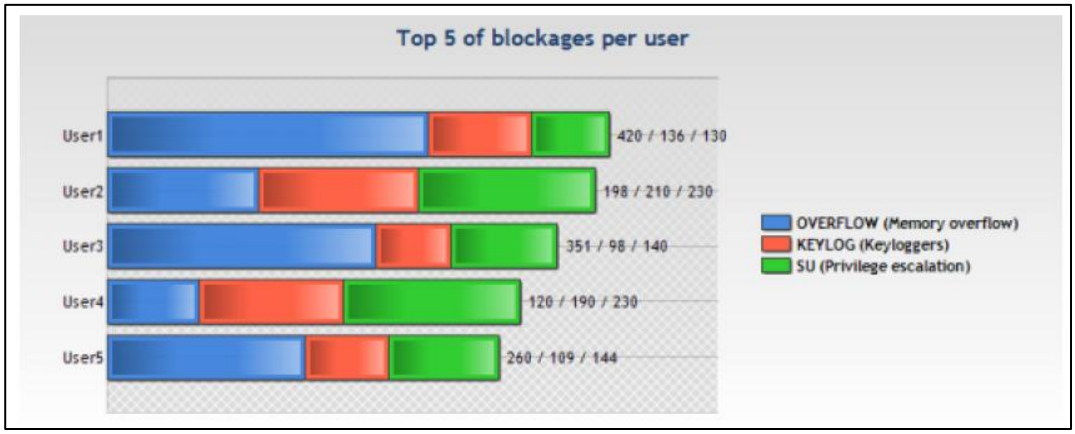
- Palmarès des blocages d'exécution d'applications par hôte :



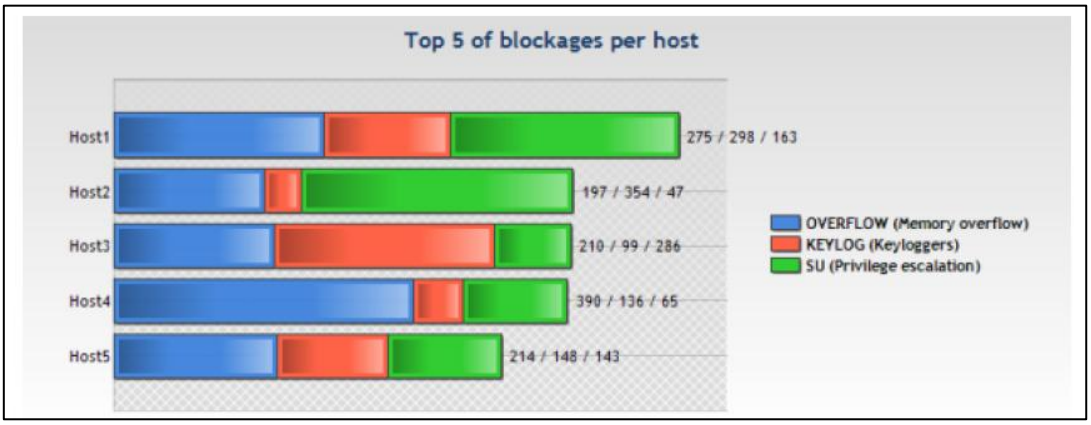
- Palmarès des blocages d'accès au réseau en mode Client par utilisateur :



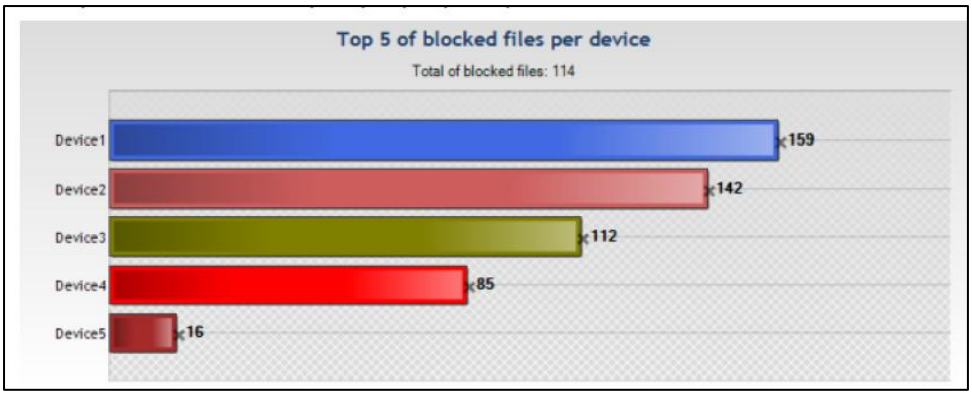
- Palmarès des blocages par utilisateur :



- Palmarès des blocages par hôte :



- Palmarès des fichiers bloqués par périphériques

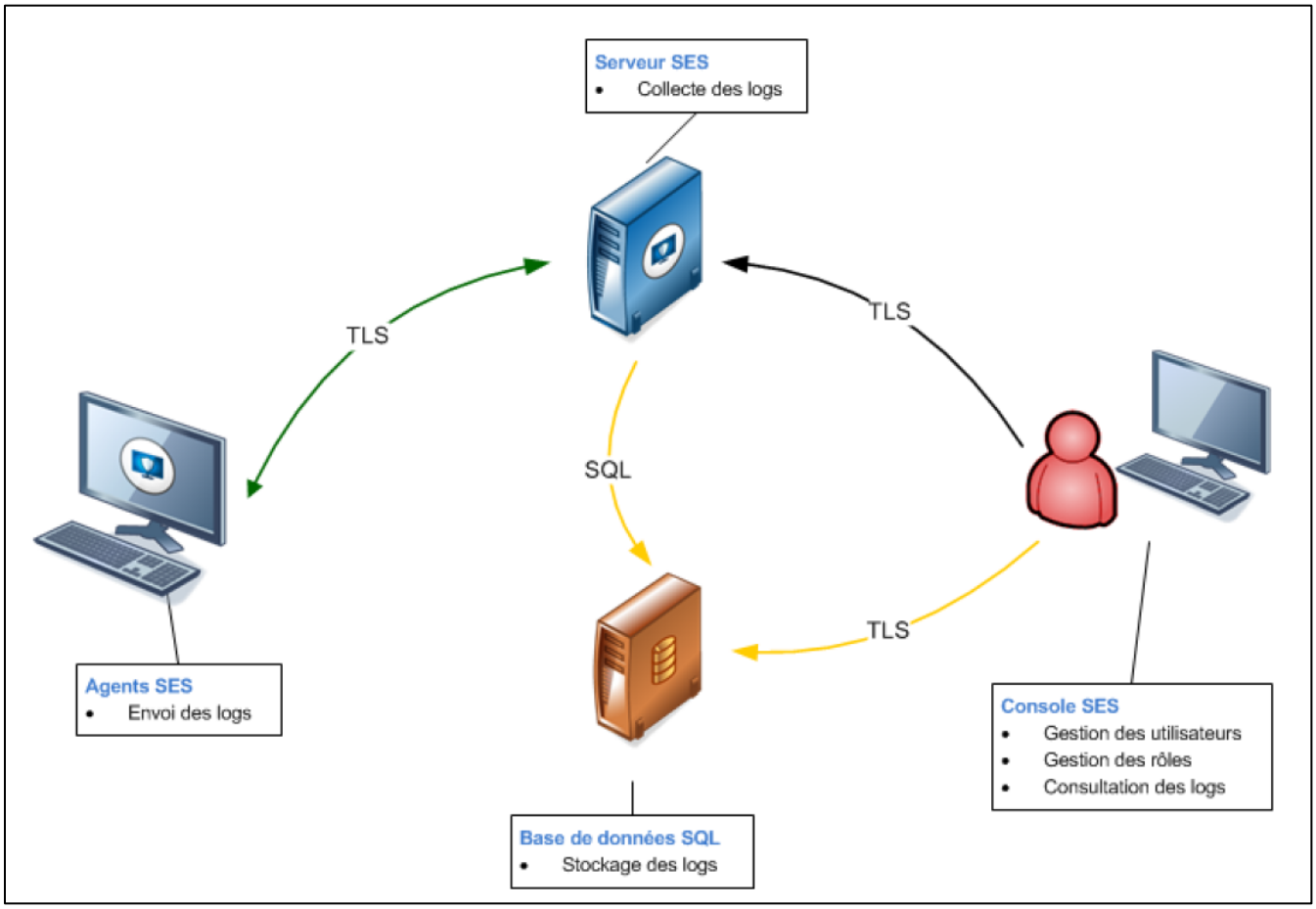


Le parcours des informations utilisées pour générer les rapports est le suivant :

1. Les rapports sont générés à partir des informations envoyées par les agents au serveur Stormshield Endpoint Security.

2. Le serveur envoie ces informations à la base de données Stormshield Endpoint Security.

3. La base de données stocke ces informations (ou logs).


Serveur SES
Collecte des logs
TLS
TLS
SQL
TLS
Agents SES
Envoi des logs
Console SES
Gestion des utilisateurs
Gestion des rôles
Consultation des logs
Base de données SQL
Stockage des logs

VI. Conclusion : résumé de l'avancement 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 - 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