Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
spécialité Réseaux et Télécommunications
parcours cybersécurité

Le SIEM, outil de supervision indispensable

Léo GORIOT

Centre hospitalier du pays d'Aix

Responsable entreprise : Pascal Sabatier

Responsable académique : Djamal Merad

2023

Table des matières

1. Introduction

Le Centre Hospitalier d'Aix-Pertuis, regroupe le CH du pays d'Aix et celui de Pertuis. Sur le site d'Aix au sein de la DSNB, Direction des Services Numériques et Biomédicaux j'ai travaillé sur le SIEM, système de gestion des informations et des événements de sécurité (security information and event manager).

L'objectif du stage était d'améliorer le contenu du SIEM afin de rendre son utilisation plus fréquente et plus agréable pour les administrateurs système et réseau. Ceci représente l'identification des besoins des administrateurs, la création de tableaux qui suivent ces besoins, la connexion de nouvelles sources de traces afin de donner une vision d'ensemble sur le réseau et ainsi détecter ou prévenir des éventuelles pannes et attaques.

Comment utiliser le SIEM pour rendre la détection des problèmes sur le réseau plus facile ?

Dans ce rapport, nous aborderons plusieurs points :

- Tout d'abord une présentation du CH d'Aix-Pertuis et du service de la Direction des Services Numériques et Biomédicaux.

- Le sujet de stage :
  - Définition des objectifs du stage
  - Comment remplir ces objectifs
  - Qu'est-ce qu'un SIEM et pourquoi en utiliser un ?

- Puis, la présentation du travail réalisé, dont :
  - Pourquoi utiliser Logpoint, quel est l'état du marché du SIEM ?
  - Travail effectué
  - Analyse des problèmes rencontrés

- Enfin, une conclusion pour faire un bilan sur le travail effectué, les objectifs atteints ou non, l'apport du stage et les perspectives d'évolution.

2. Présentation du CHIAP, Centre Hospitalier Intercommunal d'Aix Pertuis

2.1 Le CHIAP

Le CHIAP Fonctionne 24h/24 et 7j/7, Il abrite 54 services médico-chirurgicaux et médicotechniques et 944 lits. En 2022, on recense 83 580 passages aux Urgences soit environ 229 admissions/jour pour un total de 153 848 journées d'hospitalisation complètes. Le CHIAP emploie plus de 3000 agents médicaux et non médicaux.

Tous ces services dépendent du système d'information qui s'est inséré dans tous les métiers de l'hôpital. On peut dire qu'il est la colonne vertébrale de l'hôpital, le système d'information est un rouage essentiel dans le fonctionnement d'un hôpital devenu très numérique. La DSNB s'occupe de l'ensemble du système d'information.

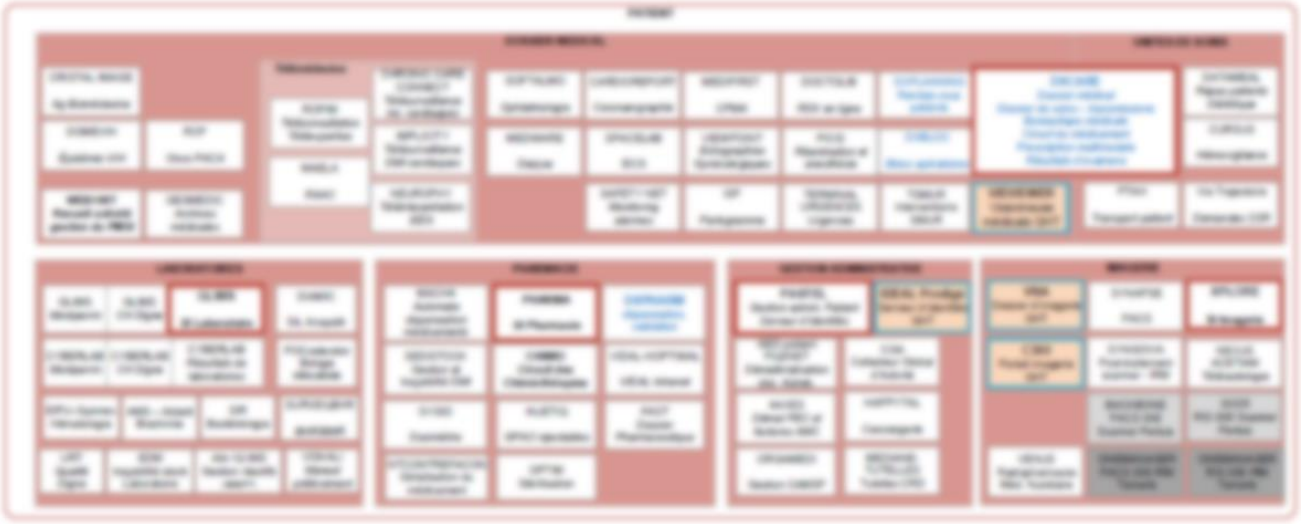

Figure 1 : Extrait de la cartographie du système d'information (flouté pour raison de confidetialité)

2.2 La DSNB

Cette direction est pilotée par le Directeur du SI, elle s'occupe des services informatiques et biomédicaux. Elle regroupe le RSSI, Responsable Sécurité Système d'Information/DPO, Data Protection Officer, le responsable SI, les administrateurs réseaux ainsi que les techniciens qui s'occupent de la maintenance et aussi de la hotline pour le support.

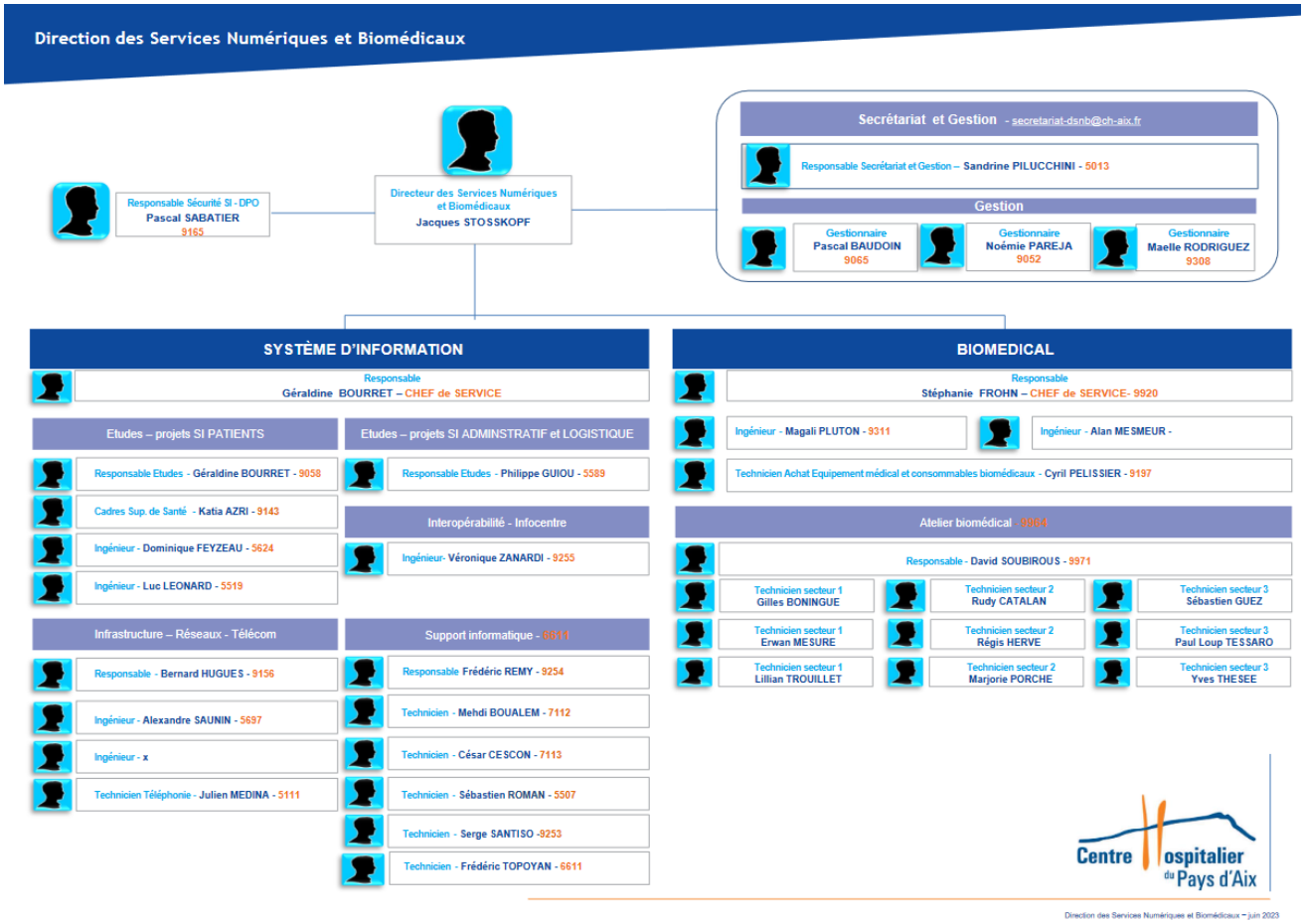

Figure 2 : Organigramme de la DSNB

Sans elle, l'informatique ne fonctionne pas et les capacités de l'hôpital sont alors dégradées car le temps pour assurer la bonne prise en charge des patients est multiplié.

3. Sujet de stage

3.1 Définition des objectifs du stage

L'objectif principal du stage était d'améliorer le SIEM pour le rendre plus facilement utilisable et agrandir le nombre de sources de logs. Il était aussi demandé de faire un tableau destiné à la sécurité de l'AD, Active Directory de l'hôpital.

Il faut alors :

- Définir quelles sources sont exploitables et pertinentes
- Définir les besoins des administrateurs et analyser la faisabilité des demandes
- Définir des indicateurs de compromission AD
- Connecter les différentes sources de logs non connectées
- Construire les tableaux de la façon la plus ergonomique possible pour faciliter la lecture
- Créer des rapports automatique hebdomadaires sur la sécurité et la santé du système
- Créer des alertes pour notifier les administrateurs en cas de compromission

3.2 Comment remplir ces objectifs ?

Afin d'atteindre les objectifs définis plus haut, j'ai défini les étapes suivantes :

- étude du réseau actuellement en place par rapport au SIEM ;
- familiarisation avec le SIEM Logpoint et sa documentation ;
- prise en compte des recommandations de l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information afin de déterminer les indicateurs de compromission de l'AD pertinents et en garantir la sécurité.

3.3 Qu'est-ce qu'un SIEM et pourquoi en utiliser un ?

Un SIEM permet de centraliser les logs des équipements présents sur le réseau pour les stocker et les présenter de manière simple et facile à interpréter afin de détecter et prévenir d'éventuelles attaques, pannes ou faiblesses du réseau.

Après une attaque il peut aussi faire office de preuve légale dans le cas d'une analyse post-attaque dite forensic car tous les logs y sont stockés et permettent de déterminer qui est responsable de l'attaque et comment l'attaque a été réalisée. Il répond en ce sens à une exigence sécurité et réglementaire qui est la conservation des traces.

L'hôpital a choisi d'utiliser le SIEM Logpoint. Pour arriver au résultat final, Logpoint collecte les logs, les stocke puis effectue une normalisation afin de les rendre interprétables par le langage de query (requête). Ensuite, les tableaux contiennent des widgets qui effectuent des queries sur la DB, Data Base de Logpoint. Enfin, l'information est présentée sous la forme souhaitée par l'utilisateur (graphes, tables, carte).

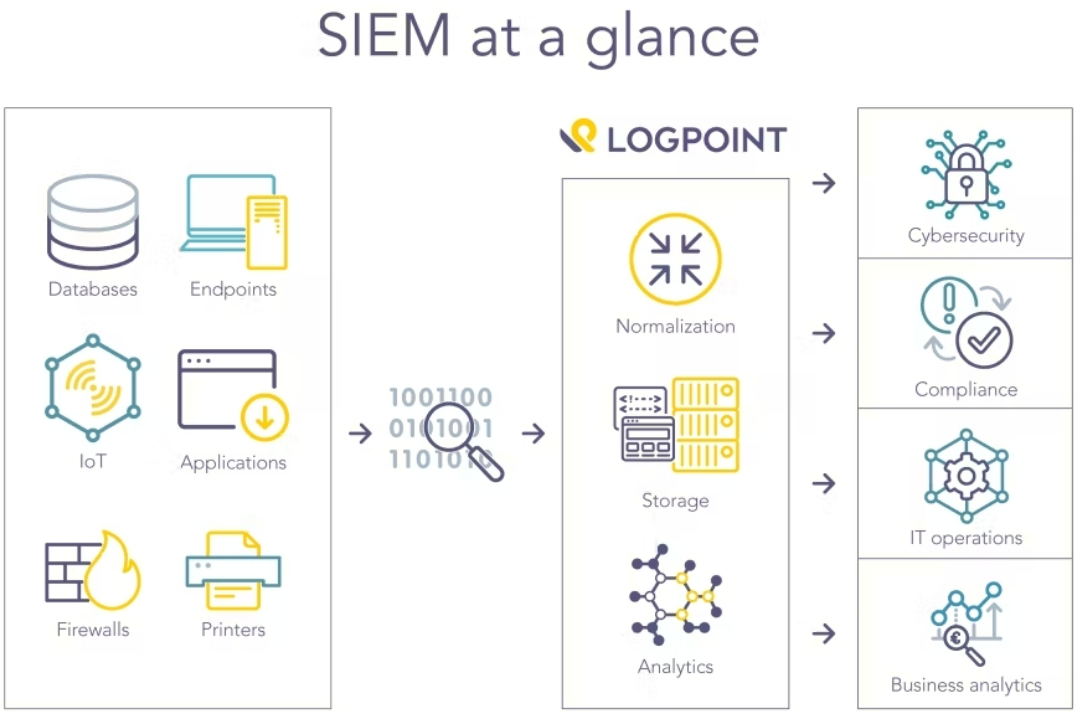

Figure 3 : Schéma de fonctionnement du SIEM Logpoint

Le SIEM est un élément indispensable car il permet en quelques secondes d'analyser la santé et le niveau de sécurité du réseau. Il permet aussi de notifier les administrateurs en cas de problème avec les alarmes. La centralisation des logs et leur rétention est aussi un des aspects les plus importants du SIEM afin de respecter la politique de sécurité de l'hôpital.

4. Travail réalisé

4.1 Pourquoi utiliser Logpoint, quel est l'état du marché du SIEM ?

Au début de mon stage, il m'a été demandé de créer une étude de marché pour connaitre le SIEM Logpoint et ses concurrents, donc l'état du marché des SIEM, car il est en constante évolution.

Mes conclusions sont les suivantes :

Dans le marché du SIEM, Splunk, Logrythm, Logpoint et Qradar semblent avoir les plus grandes parts du marché. Cependant les leaders du marché en termes de meilleur produit sont Microsoft, IBM, Splunk et Secutronix, d'après le 2022 Gartner Magic Quadrant for SIEM, un indicateur des capacités et du rayon d'action d'un SIEM créé par Gartner, une entreprise Américaine de conseil et de recherche dans le domaine des techniques avancées. (Cependant une grosse partie de la note est basée sur les ventes).

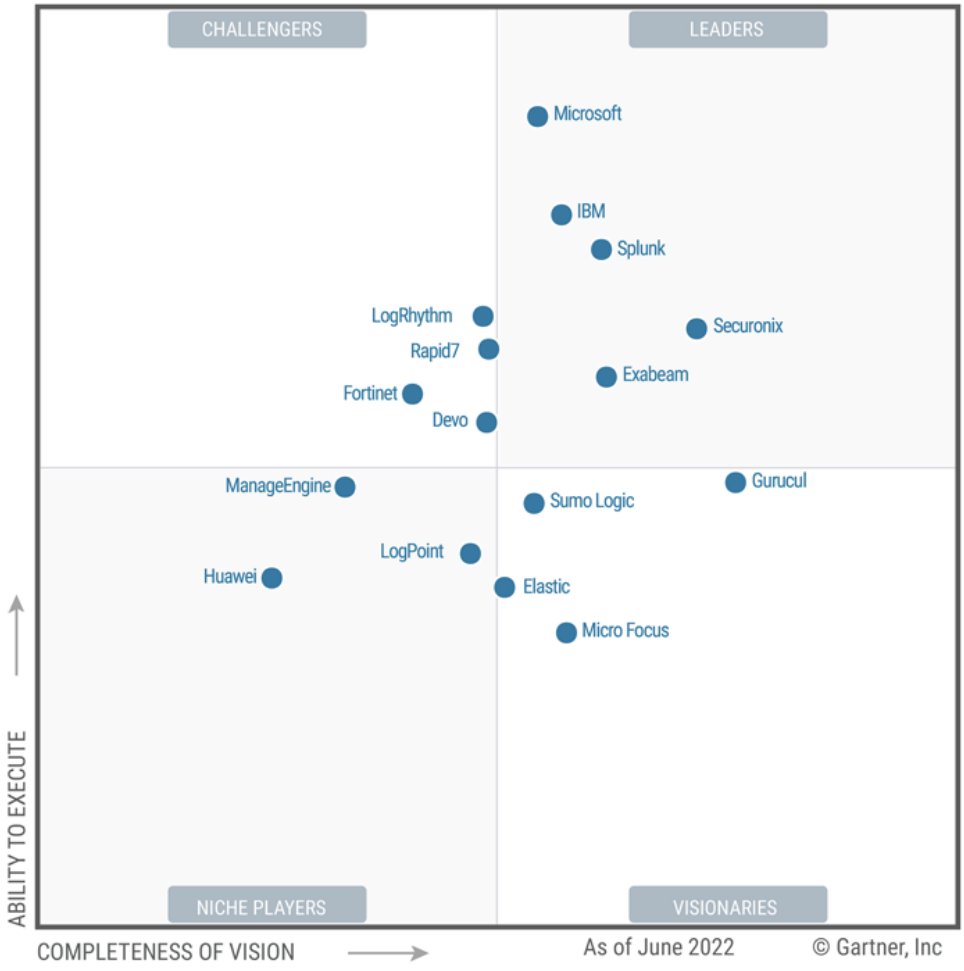

Figure 4 : Gartner Magic Quadrant for SIEM

Leurs offres sont similaires, mais le SIEM Microsoft propose une symbiose quasi parfaite avec ses outils tels que Office 365 et les services Azure cloud. Mais il est aussi compatible avec des services d'autres fabricants tels que AWS, Amazon Web service et GCP, Google, Cloud Platform, il met également en avant son faible coût par rapport à la concurrence. Splunk et Logpoint offrent une

interface agréable et insistent sur la facilité d'utilisation de leur logiciel et leur aspect « prêt à l'emploi » pour de nombreux services. Splunk offre aussi une application mobile permettant de visualiser le SIEM de n'importe où et également une fonctionnalité de réalité augmentée pour des capacités de visualisation accrues, pour un technicien dans une salle de serveurs par exemple. Splunk dispose aussi d'une communauté très active et des milliers de modules et tableaux pré-faits communautaires et officiels.

Figure 5 : Réalité augmentée par Splunk

Mais Logpoint reste nettement moins cher que Splunk. IBM, International Business Machines Corporation lui, insiste sur la sécurité et les capacités de détection des menaces de son SIEM et Secutronix offre une solution basée nativement sur le cloud.

Ils partagent néanmoins tous certaines fonctionnalités, comme la capacité de gérer les logs de n'importe quelle source, l'intégration de machine learning pour se prévenir des menaces, ou encore un moteur d'automatisation pour une réaction plus rapide aux menaces ainsi que la possibilité de customiser son SIEM. Tout ces produits répondent à un besoin de protection du réseau d'entreprise. Elle comprend la protection contre des menaces externes ou internes (DDOS, Distributed Denial of Service, malwares, hacks, pannes, erreurs de configuration…) et aussi une protection légale (lors d'une attaque réussie par exemple) pour pouvoir tracer l'étendue des dégâts, remonter à la source de l'attaque et identifier les vulnérabilités ou le responsable.

Les SIEM qui étaient à la base des systèmes exclusivement chargés de collecter et stocker les logs, sont aujourd'hui capables de les interpréter pour en faire divers graphes, pour lever des alertes et permettent une analyse poussée du réseau s'ils sont bien configurés.

Néanmoins on voit l'apparition de systèmes d'automatisation et d'optimisation du SIEM par IA, Intelligence Artificielle, ainsi que des architectures basées sur cloud, déjà prêtes à l'intégration avec les services les plus connus. Les SIEM deviennent de plus en plus poussés et automatisés, capables de traiter des flux de n'importe quelle source.

On pourrait imaginer dans le futur un système totalement automatique, hébergé sur cloud et déjà configuré, constamment amélioré par IA en fonction du réseau qu'il supervise.

4.2 Travail effectué

Dans un premier temps, dans une optique de familiarisation avec le système, quelques essais ont été fait avec la création de tableau mais surtout avec le langage de query Logpoint (mix entre python, bash et SQL).

```
label=User label=Login label=Fail and user != admin and user != oracle | chart count() by user, workstation, source_address
```

Figure 6 : Une des premières query que j'ai réalisée

Dans la Figure 6 on demande à la BDD, Base De Données de Logpoint, quels utilisateurs n'ont pas réussi à s'authentifier, en excluant les user admin et oracle (faux positifs à ce moment). On demande ensuite au logiciel de faire un graphe qui compte par utilisateur, machine et adresse source.

Après cette période de familiarisation avec le système, j'ai entamé la recherche des indicateurs de compromission de l'AD, tâche la plus importante. J'ai consulté différent sites web et les recommandations de l'ANSSI, j'en ai conclu avec mon maitre de stage que les indicateurs à surveiller étaient les suivants :

- Les actions des groupes, qui est ajouté dans quel groupe et par qui et quand ?
- Les actions des comptes avec privilèges
- Les utilisateurs créés, supprimés, désactivés, bloqués, débloqués, par qui et quand ?
- Les utilisateurs en échec d'authentification et ceux qui se sont authentifiés le plus
- Les utilisateurs authentifiés sur le plus de machines différentes
- Les logs avec un niveau critique (graves)
- L'authentification sur le compte administrateur du domaine
- Le honeypot (appât)

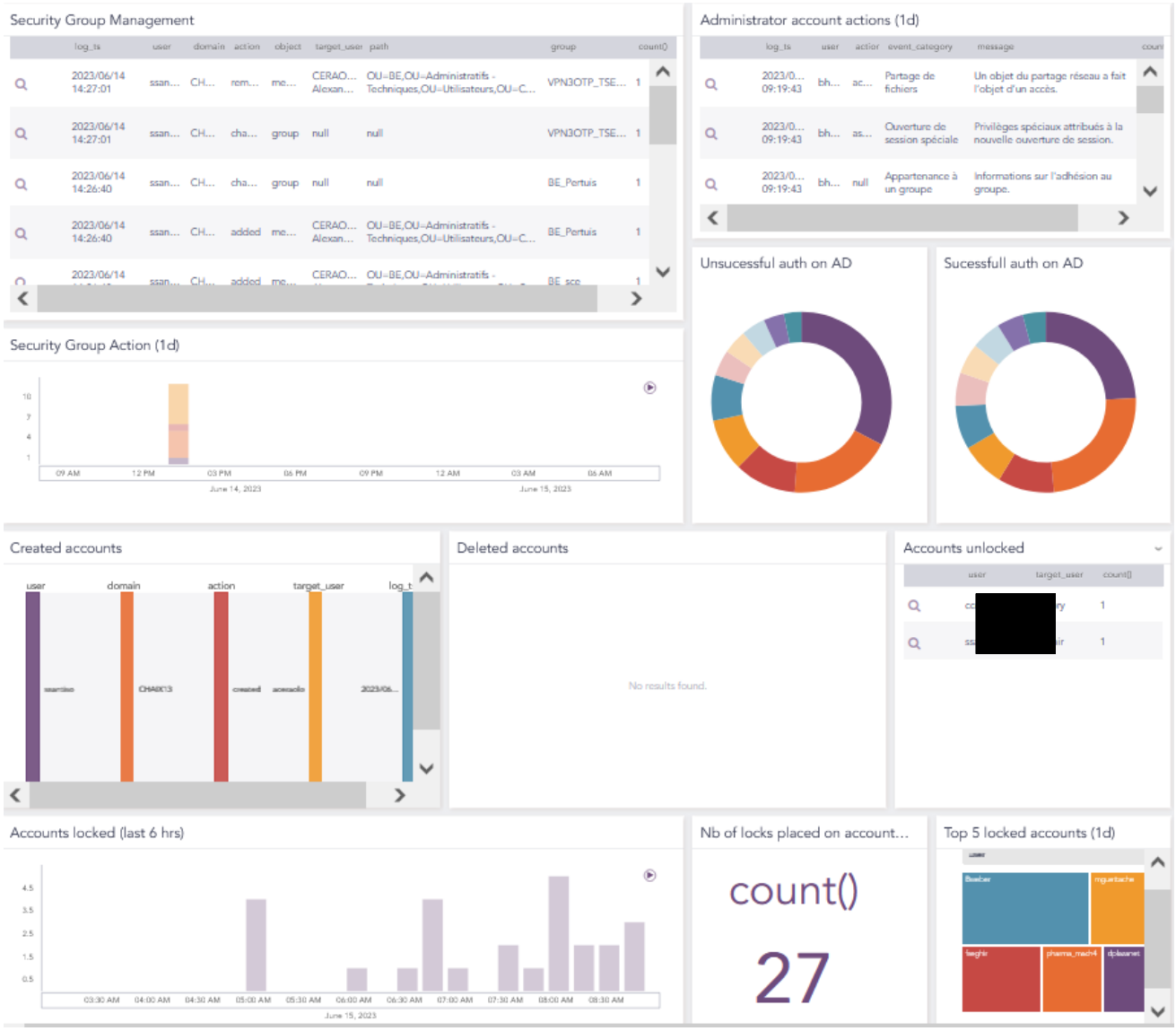

Figure 7 : Aperçu du tableau sécurité AD

Le tableau de l'AD créé, il a servi immédiatement car des comptes constamment en échec d'authentification (plusieurs millions de retry) ont été détectés. L'équipe technique a été avertie pour régler le problème. Ce scénario se répètera plusieurs fois durant le stage car un projet de suppression de comptes génériques cause certaines applications sur des ordinateurs d'essayer de s'authentifier avec des credentials alors obsolètes.

Par la suite, j'ai étudié quels autres services présents sur le réseau pouvaient être reliés à Logpoint, en commençant par dresser le schéma du réseau et de ses services.

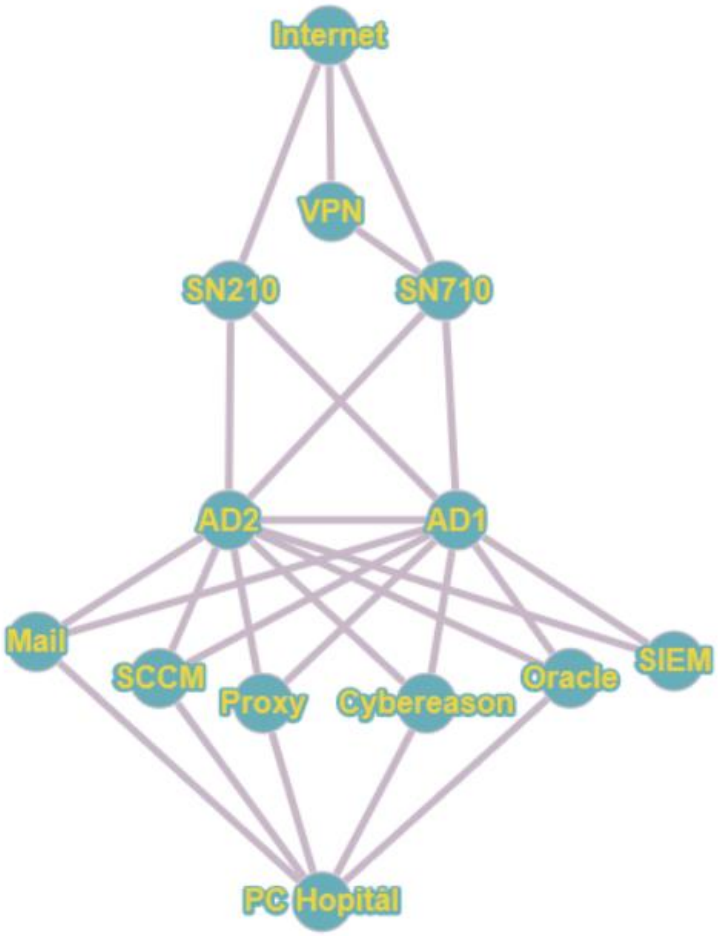

Figure 8 : Schéma simplifié du réseau

Avec la figure 8, on repère des éléments intéressants à surveiller :

- Les deux AD (déjà connectés au SIEM et exploités)
- Le serveur de mail (connecté mais lien ne fonctionne plus)
- L'antivirus SCCM, System Center Configuration Manager (pour avoir un état de tous les PC)
- Le proxy
- Le VPN, Virtual Private Network SSL, Secure Sockets Layer
- Les firewalls (déjà connectés et partiellement exploités)
- La DB Oracle (connectée et exploitée)
- Cybereason

J'ai ensuite exploré la librairie Logpoint de tableaux pré-faits ; celui de Stormshield sera le seul que j'utiliserai tel quel, quasiment sans modification.

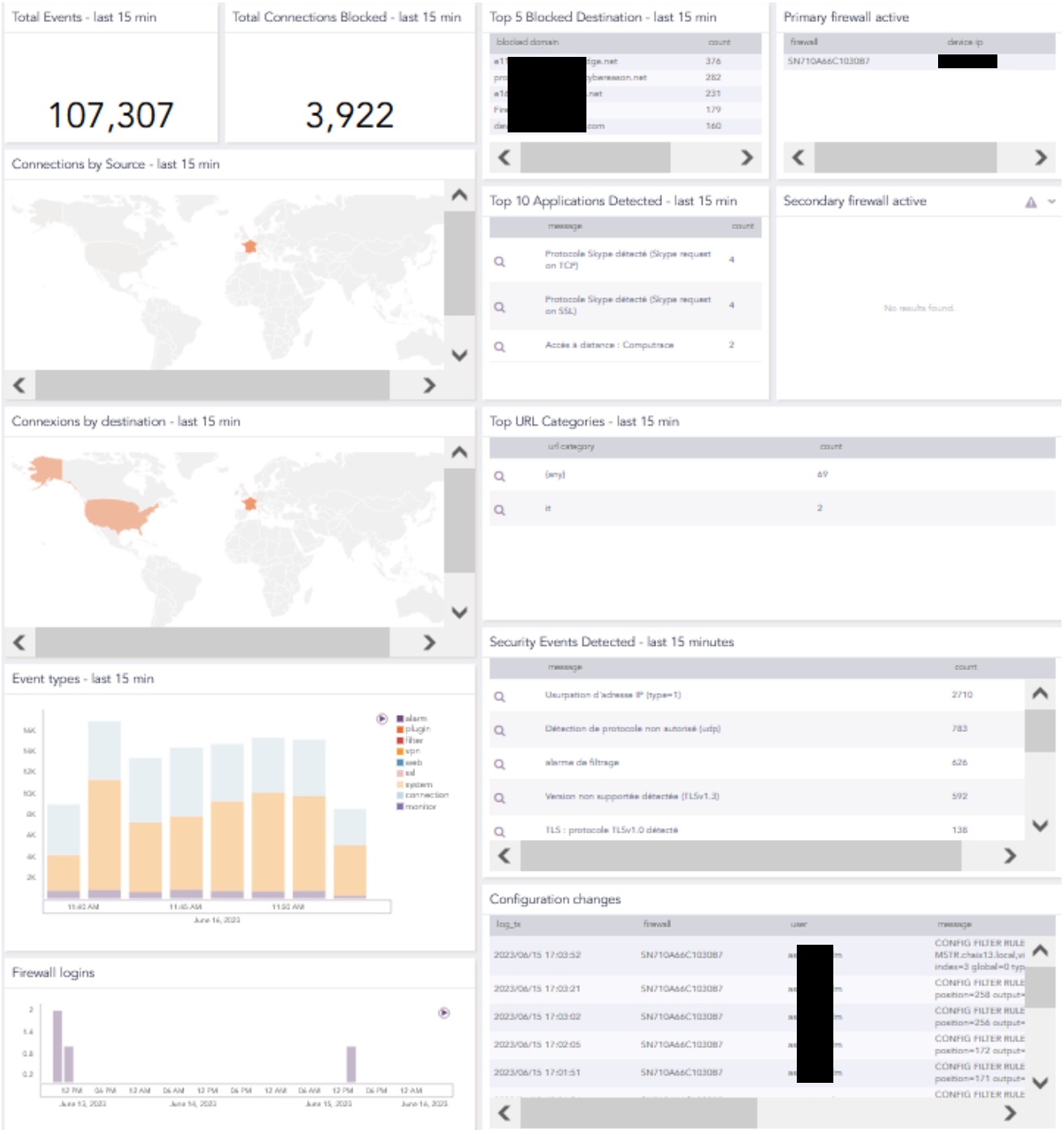

Figure 9 : Tableau sécurité du firewall (fait par Stormshield)

L'étape suivante a été d'essayer de connecter et d'exploiter de manière intéressante les autres éléments comme :

- La DB Oracle
- Le serveur mail
- Le proxy
- Le serveur SCCM
- Le VPN
- Cybereason

La DB Oracle est déjà exploitée et bien qu'il soit techniquement possible d'en tirer plus d'informations, cela aurait très compliqué. De plus, la DB a déjà un système intégré pour se diagnostiquer. Après en avoir discuté avec mon maitre de stage, je n'ai pas poursuivi pas plus loin cette piste.

Le serveur mail est connecté mais n'envoie plus d'informations, car l'agent présent sur le serveur ne répond plus. En effet il est obsolète et a besoin d'être réinstallé sous sa dernière version.

Après l'avoir réinstallé et redirigé les logs dans le bon répertoire, on peut à nouveau exploiter les logs du serveur mail. Je créé alors un tableau pour évaluer la santé et la sécurité du serveur mail.

Le serveur SCCM contient déjà un outil de supervision des antivirus intégré, il n'y a donc pas besoin de le relier à Logpoint et, tout comme la DB Oracle, récupérer ces informations aurait été trop compliqué par rapport à l'utilité que cela représente.

Le VPN et le proxy nous envoient des logs grâce à un simple changement de configuration, l'envoi des logs étant déjà prévu par ces application (pas besoin d'installer un agent).

Le proxy et le firewall ont surtout été utilisés pour traquer les flux obsolètes toujours présents sur le réseau (http, ftp, ntlm, telnet…)

Cybereason est un EDR, Endpoint Detection and Response, c'est un antivirus nouvelle génération qui contrôle le réseau pour détecter les comportements anormaux et les stoppe automatiquement si nécessaire. Cybereason créé des logs seulement sur l'état de son serveur, ces informations n'ont pas éré jugées pas assez intéressantes pour justifier de le relier à Logpoint.

J'ai également créé un tableau spécialisé regroupant plusieurs sources dédiées à l'astreinte des administrateurs pour leur donner la capacité d'analyser rapidement la santé du réseau, ainsi que des alarmes si certains seuils sont dépassés pour alerter en cas de gros problème.

Enfin, j'ai créé un schéma qui résume les tableaux que j'ai créés et les éléments qu'il contiennent.

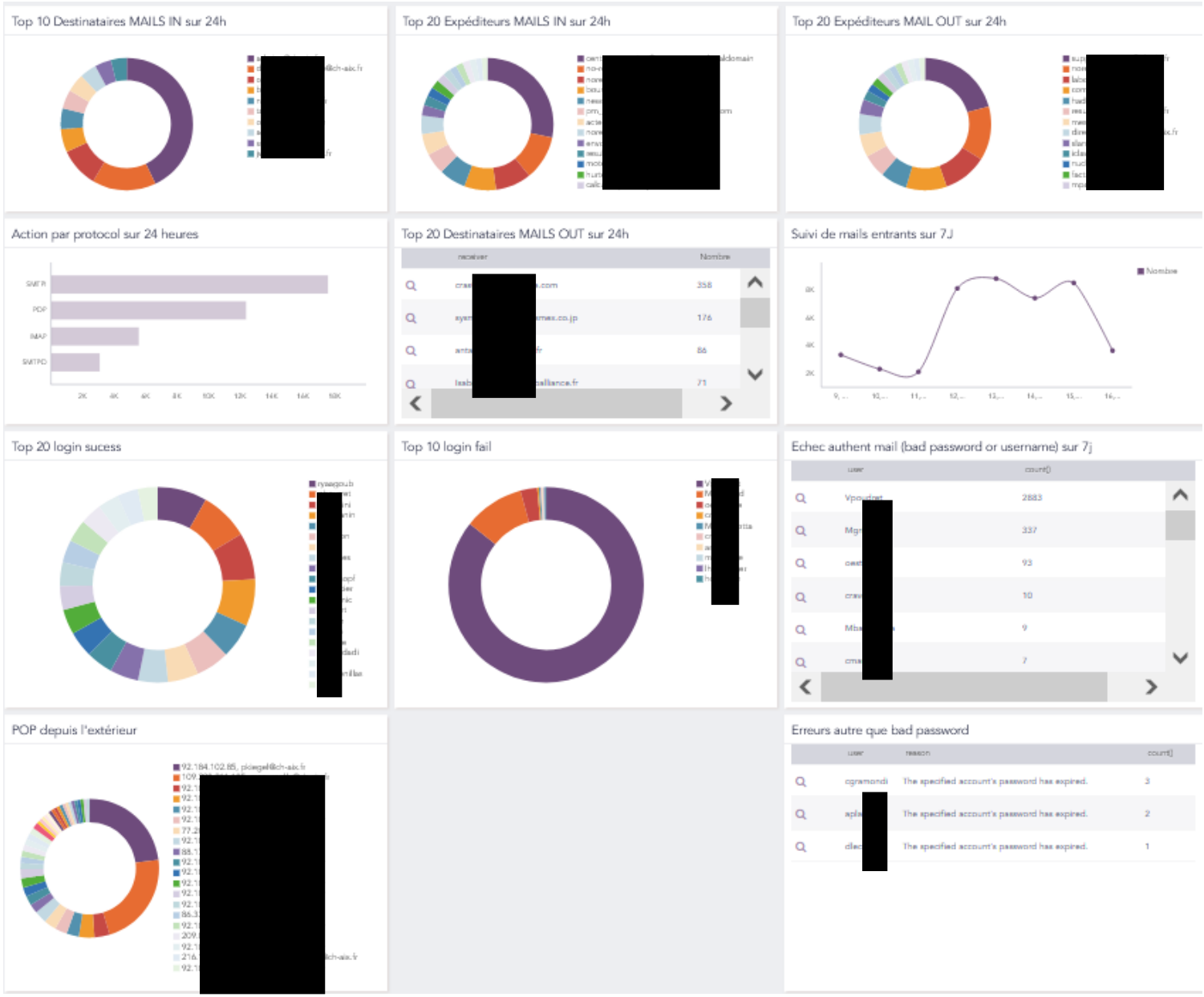

Figure 10 : Tableau sécurité du serveur mail

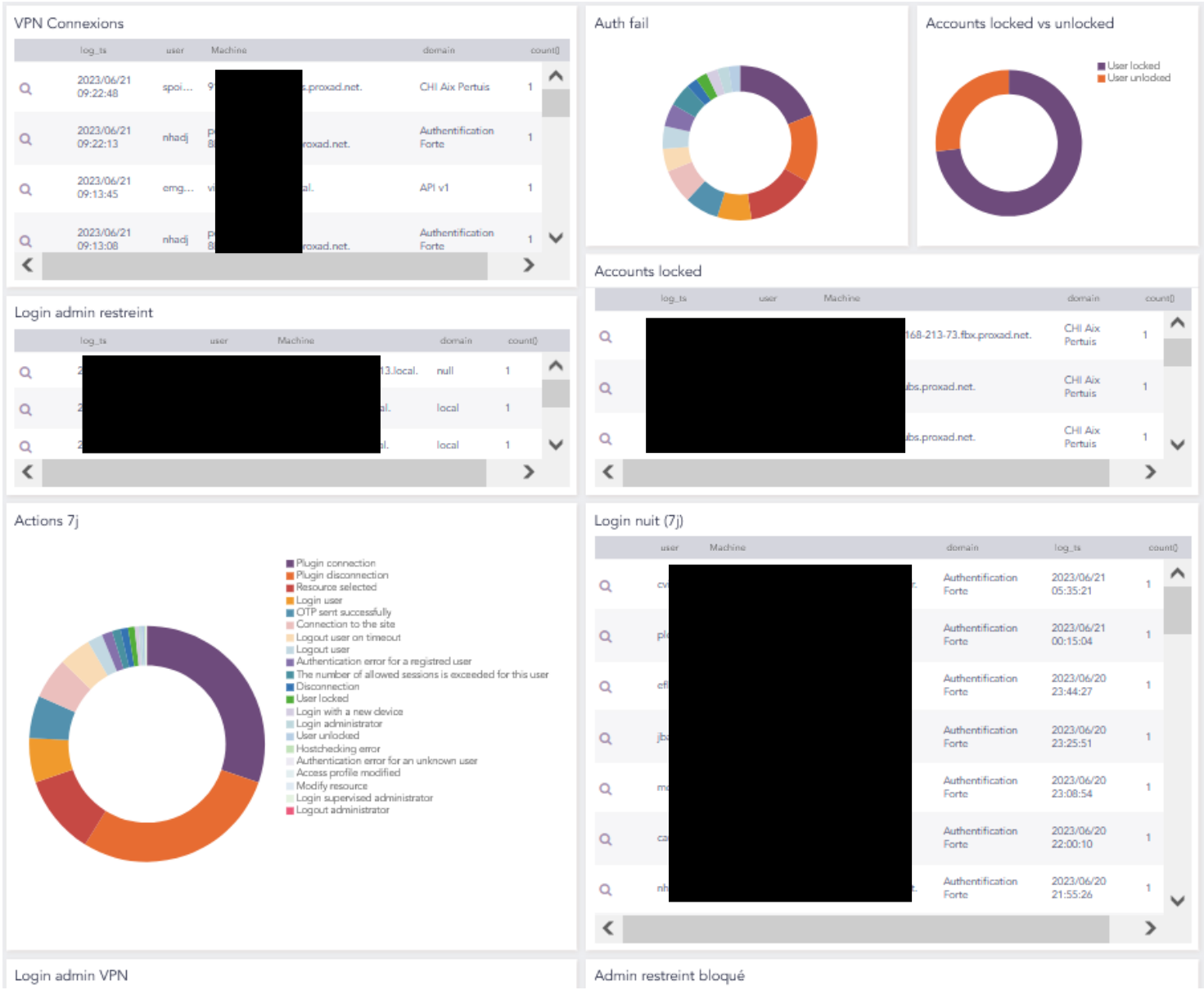

Figure 11 : Tableau VPN

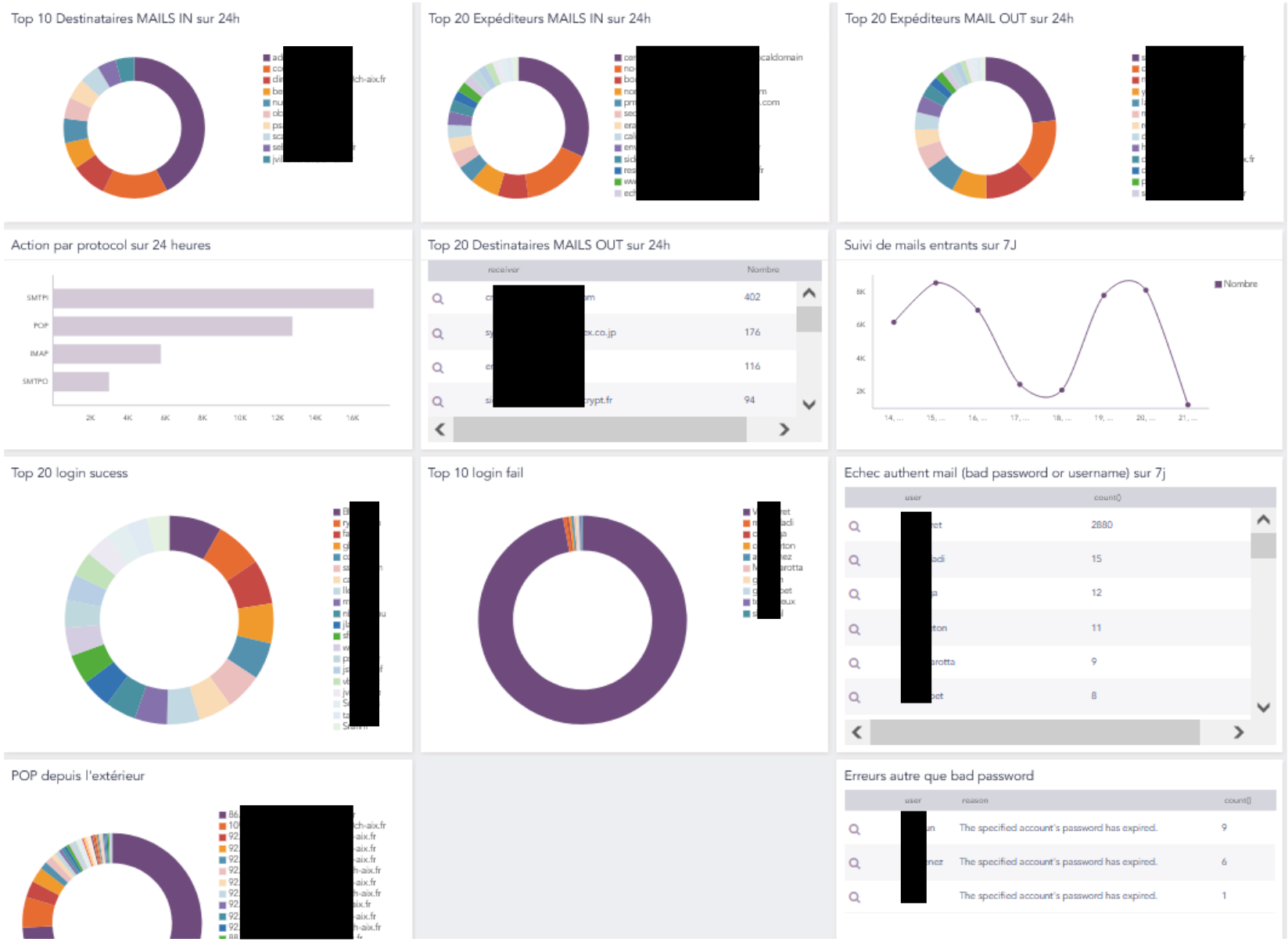

Figure 12 : Tableau Mail

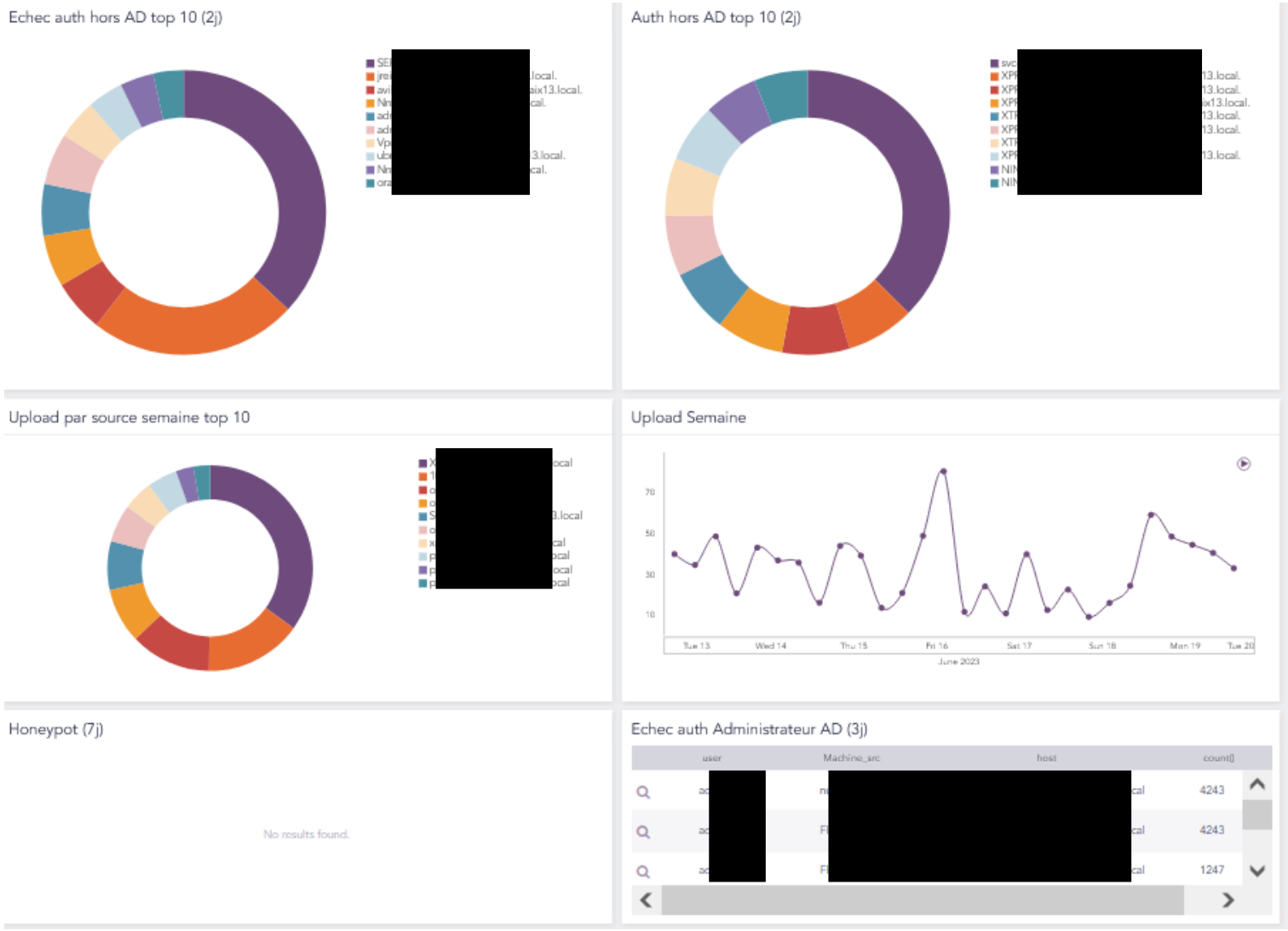

Figure 13 : Tableau d'astreinte

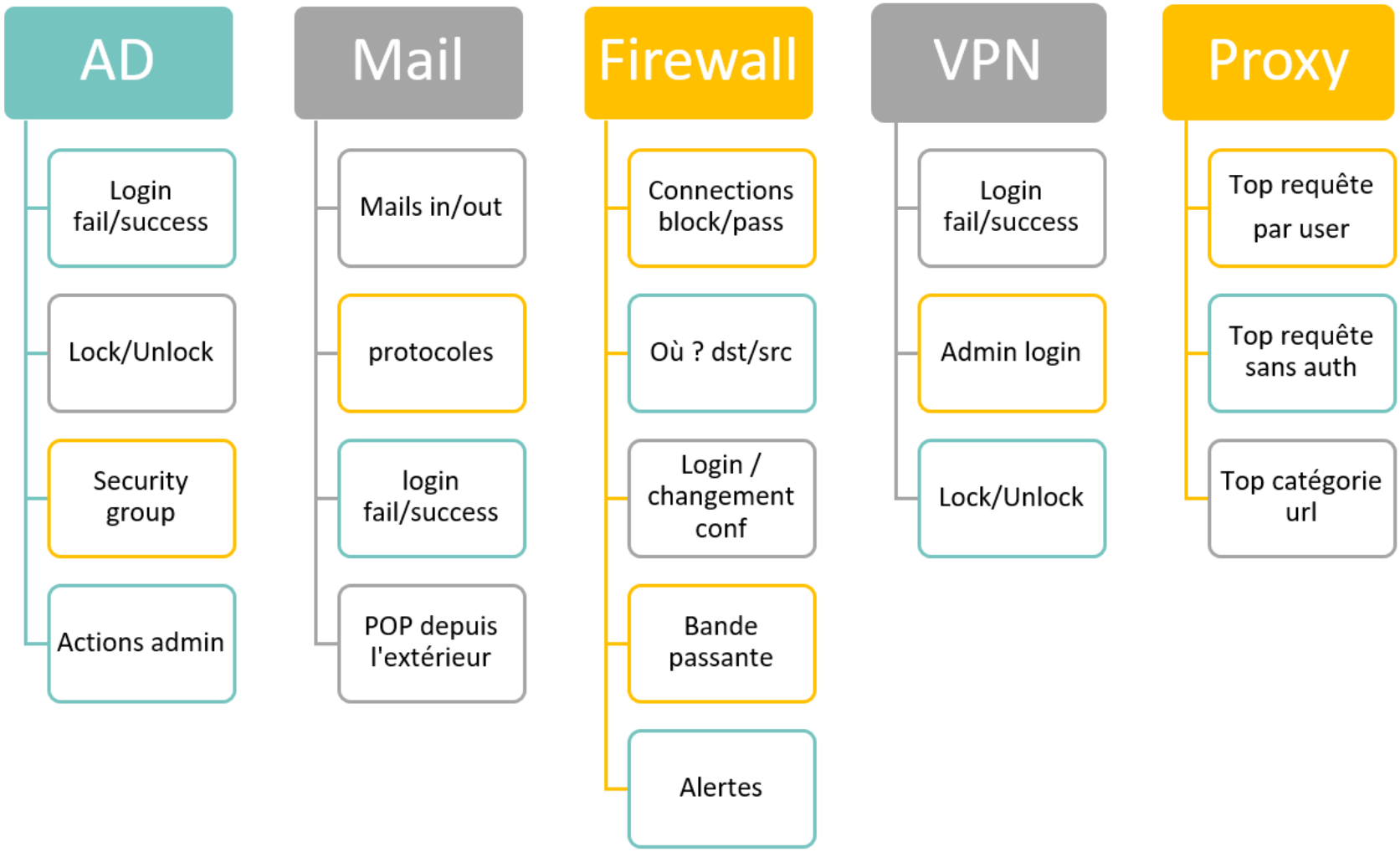

Figure 14 : Equipements et éléments supervisés

4.3 Problèmes rencontrés

Déterminer quels indicateurs sont intéressants à surveiller requiert un certain recul dans le domaine de la cybersécurité. La première complication rencontrée durant mon stage a donc été le manque d'expérience sur ce sujet. Je me suis d'ailleurs rendu compte en créant des tableaux pour différents systèmes que les derniers étaient bien plus simples à conceptualiser.

La seconde difficulté à contourner a été celle de la pauvreté de la documentation fournie par Logpoint. Il est quasiment impossible de faire quelque chose de compliqué en suivant la documentation, pour aller plus loin il faut quasi-obligatoirement une formation Logpoint. De plus la communauté des utilisateurs de Logpoint est très peu présente sur internet (pas de tutos ou de wikis, pas de partage de problèmes et solutions).

Les autres problèmes que j'ai rencontrés pendant ce stage étaient d'une nature technique et liés au fonctionnement du SIEM Logpoint. Pour en comprendre la cause et leur solution, il est nécessaire d'avoir plus de détails sur la manière dont Logpoint collecte et normalise les logs. Je vais donc maintenant en faire une brève explication :

Pour envoyer des logs à Logpoint, il faut d'abord créer un équipement source dans le logiciel avec son IP. Ensuite grâce à une politique de stockage on peut choisir vers quel répertoire les logs de cet équipement vont être redirigés. Puis, vient la normalisation des logs avec une politique de normalisation qui se charge de regrouper des signatures qui extraient les champs jugés intéressants dans les logs.

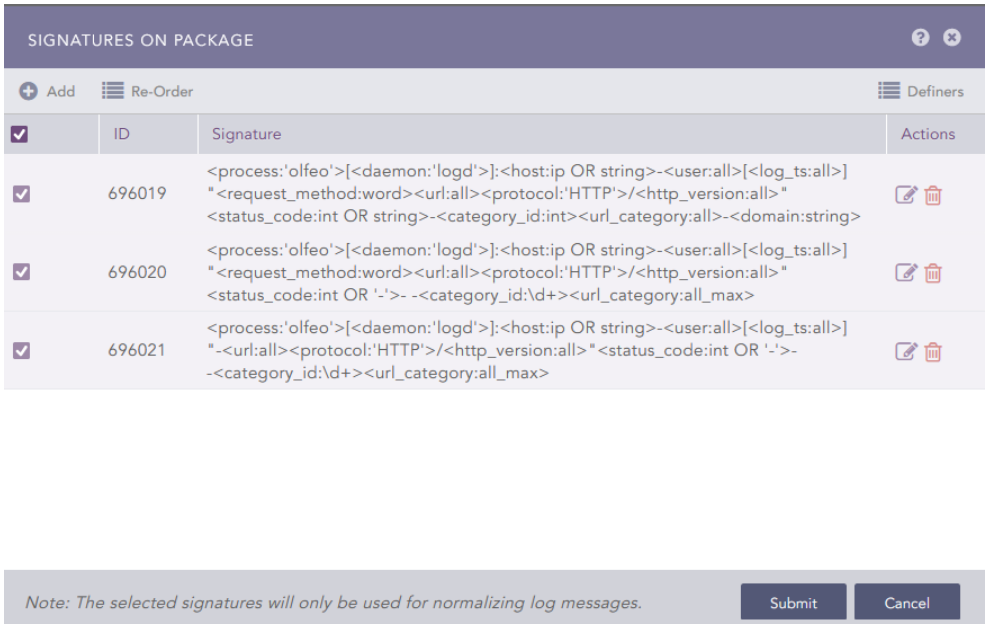

Figure 15 : Signatures Logpoint

Le premier problème concernait la politique de stockage des logs du serveur mail qui étaient redirigés vers le répertoire de l'AD au lieu de celui du mail. Ce problème a été résolu avec un simple changement de la configuration de la politique de stockage des logs du serveur mail.

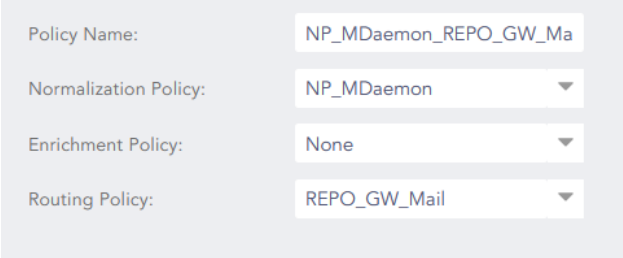

Figure 16 : Politique de stockage du serveur mail

Le problème suivant concernait l'envoi des logs du proxy et du VPN. Ces deux équipements et le SIEM étaient bien configurés mais rien n'était reçu. Le problème venait du firewall qui bloquait ces trafics, l'ajout d'une règle sur le firewall a suffi à régler le problème.

Enfin le plus gros problème, qui reste encore partiellement à résoudre à ce jour concerne le proxy.

En premier lieu une grosse partie des logs provenant du proxy n'étaient pas normalisés, ce qui empêche la création d'un tableau de surveillance du proxy. Après une brève investigation, j'ai remarqué que les signatures de la politique de normalisation étaient incomplètes : les signatures prennent en compte les logs contenant une action (POST, GET) mais pas ceux sans (la majorité des requêtes http/https faites sur internet).

Après avoir ajouté une signature pour prendre ce cas en compte, j'ai remarqué une autre anomalie, plus aucun log ne semblait arriver. J'ai regardé les logs des dernières 5 minutes et rien n'apparaîssait, pourtant, le proxy envoyait bien les logs et Logpoint confirmait la réception de logs depuis cet équipement.

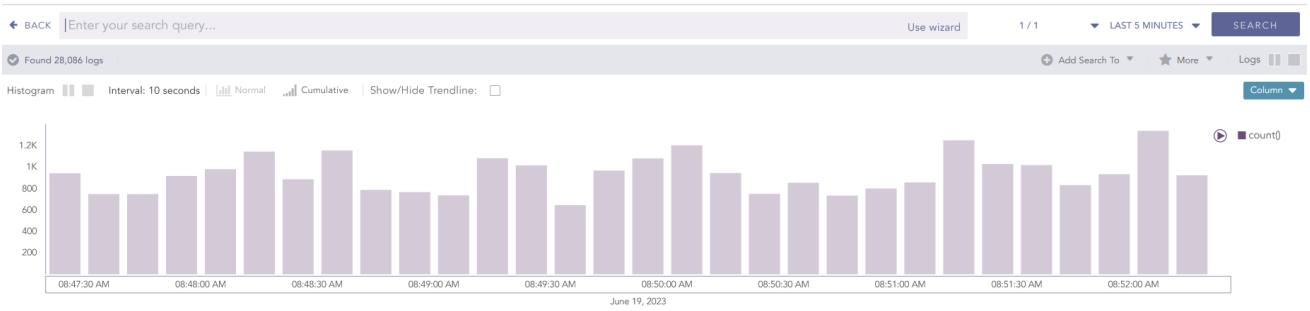

Figure 17 : Recherche des logs en temps normal

Figure 18 : Recherche des logs avec ma signature activée

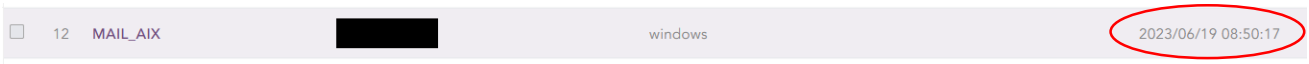

Figure 19 : Equipement serveur mail avec l'horaire du dernier log reçu

Impossible de retrouver ces logs. Enlever la signature ajoutée rendait les logs à nouveau visibles, mais ceux qui étaient invisible restaient introuvables. Nous avons suspecté avec mon maître de stage un bug de Logpoint, le logiciel est assez récent et il est tout à fait probable que des bugs soient toujours présents.

Nous avons donc contacté le support Logpoint via l'entreprise qui a installé le SIEM pour tenter de régler ce problème.

Une réunion a été planifiée pour la semaine suivante. Durant la visioconférence, malgré que les échanges ne se fassent qu'en anglais car le support se trouve en Inde j'ai pu converser avec succès et la raison pour de disparition a finalement été trouvée : Les logs n'ont jamais disparu mais étaient mal horodatés avec un décalage de 2 heures et donc n'apparaissaient pas dans la recherche des dernières 5 minutes (cf fig 18). Il faut savoir que Logpoint calcule ces 5 dernière minutes avec un champ appelé log_ts qui correspond à l'horodatage inscrit sur le log. Toutefois, si la normalisation échoue, le champ log_ts est automatiquement remplacé par l'horaire où le log a été reçu donc 2h plus tôt que ce qui est inscrit sur le log. Logpoint place alors les nouveaux logs normalisés 2h plus tôt que les non normalisés, et, comme tous les logs étaient désormais normalisés, les logs semblaient disparaitre alors qu'ils sont juste classés par Logpoint 2h dans le passé.

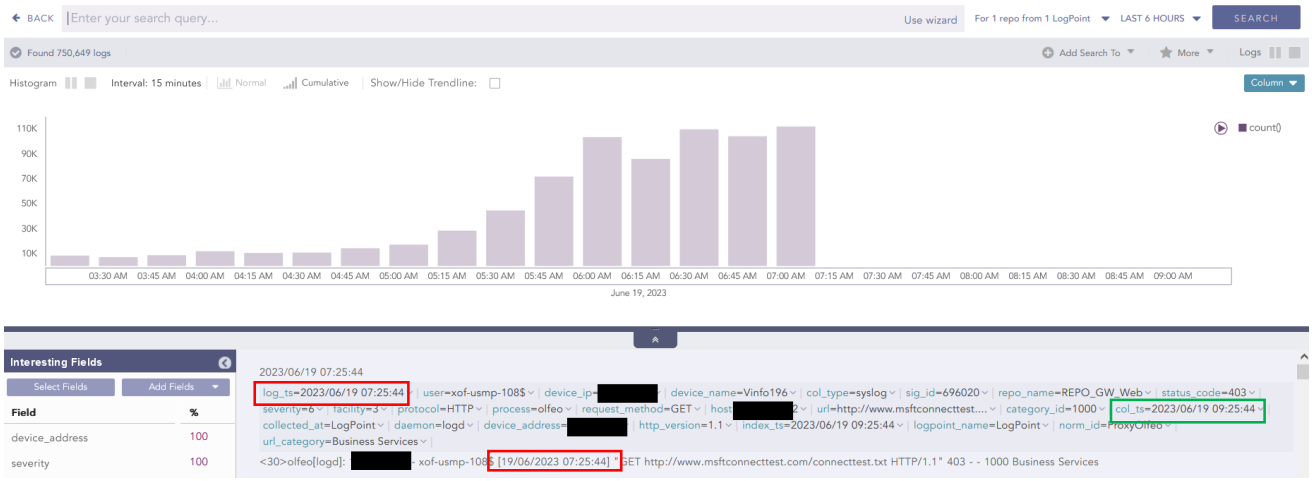

Figure 20 : Recherche des logs du proxy, horodatage par rapport au log et heure de collection du log

La conclusion a donc été que le proxy n'était pas à l'heure et avait un décalage horaire de 2 heures. Changer l'horaire du proxy et des machines qui le font tourner et les redémarrer n'a pas résolu le problème, malgré le fait que toutes les machines soient à l'heure. Encore à ce jour, nous ne savons pas d'où vient ce décalage horaire. Ce décalage n'empêche pas l'exploitation des logs mais la complique fortement.

5. Conclusion

Durant ce stage, j'ai pu me familiariser avec un nouvel outil de supervision et y connecter différents services afin d'en tirer le maximum d'informations pertinentes, aussi bien dans une optique de cybersécurité que de supervision pure. Ce travail a permis de faciliter l'analyse du réseau, de ses problèmes et d'avertir en cas de problème critique. Après ce stage je peux dire que le SIEM est définitivement un élément indispensable pour réseau de l'hôpital, il permet d'extraire rapidement des informations intéressantes parmi des dizaines de millions de logs.

Je suis satisfait que mon travail ait été utile instantanément, pour détecter des anomalies sur le réseau et que les tableaux que j'ai créés soient utilisés quotidiennement par l'équipe. Jusqu'à la fin de mon stage j'ai reçu des demandes pour ajouter/préciser des éléments aux tableaux ce qui témoigne de leur utilité.

Ce stage m'a appris les bases pratiques de la cybersécurité en entreprise en travaillant avec des données sensibles ainsi que les contraintes éventuelles liées aux utilisateurs. Il consolide mon envie de travailler dans le réseau et la cybersécurité.

Tous les objectifs du stage ont été atteints, sauf pour le proxy qui reste décalé de 2 heures. Cependant il y a toujours possibilité d'améliorer le SIEM, notamment en réussissant à y connecter SCCM. Le logiciel pourrait aussi être amélioré en proposant un envoi d'alertes par SMS plutôt que par mail. Il pourrait également bénéficier d'une communauté plus active et axée sur le partage ainsi que d'une librairie de tableaux plus fournie.

À terme, la solution la plus efficace selon moi serait de basculer sur le concurrent de Logpoint, Splunk. Il est en tout point similaire à Logpoint mais beaucoup plus mature. Il comporte un grand nombre de petites fonctionnalités qui rendent l'utilisation plus agréable et plus personnalisable. De plus, Splunk dispose d'une communauté plus active et d'une librairie contenant des milliers de tableaux et modules complémentaires, et ce pour énormément d'application. D'après moi, c'est ce qui fait la vraie force de Splunk, surtout quand on considère la cybersécurité, qui, comme vu en cours, est très difficile à faire tout seul et bien plus efficace quand les solutions sont partagées. Le seul frein à cette amélioration est le prix car Splunk reste bien plus onéreux.

6. Remerciements

Je remercie, tout d'abord la DSNB du CH du pays d'Aix de leur accueil chaleureux durant ce stage, plus particulièrement Mme Géraldine, Responsable SI, pour m'avoir accompagné durant la période de recrutement avec une disponibilité inégalée. Mais aussi Mr Pascal Sabatier, RSSI/DPO et mon maitre de stage pour son guidage et ses précieux conseils, Mr Bernard Hugues et Mr Alexandre Saunin pour leur aide et leur patience. Enfin, je remercie le directeur de la DSNB M Jaques Stosskopf pour avoir accepté de me prendre en stage au CHIAP.

7. Glossaire

Agent Un agent est un programme installé sur un équipement, chargé de relayer des informations à un autre équipement.

Compte générique Dans le cas de l'hôpital, compte utilisé pour une machine ou un service par plusieurs personnes (pas bien !) au lieu de plusieurs comptes sur une machine.

Credentials Mot anglais désignant les informations d'authentification d'un compte

Hack Mot anglais désignant une tentative de gagner frauduleusement accès à un ordinateur.

Honeypot Mot anglais signifiant « pot de miel », dans un cadre informatique cela fait référence à un appât, pour toute personne mal intentionnée ayant accès au réseau afin de lever des alarmes et identifier l'attaquant.

Indicateur de compromission Indicateur qui permet d'indiquer si le système est compromis par un attaquant.

Logs Diminutif de logging, le terme peut être traduit en français par "journal". Le log s'apparente ainsi à un journal de bord horodaté, qui ordonne les différents événements qui se sont produits sur un ordinateur, un serveur, etc

Machine learning Sous-ensemble de l'intelligence artificielle. Cette technologie vise à apprendre aux machines à tirer des enseignements des données et à s'améliorer avec l'expérience, au lieu d'être explicitement programmées pour le faire.

Malware Mot anglais désignant un logiciel malveillant.

Normalisation Dans le cas de Logpoint, il s'agit d'extraire les champs utiles, souvent communs entre logs (user, ip_source, timestamp, …).

Proxy équipement réseau permettant de surveiller et filtrer le trafic http/https afin restreindre l'accès à certains sites ou établir des statistiques.

Query singulier de **queries**, une query un mot anglais utilisé pour désigner (dans un cadre informatique) une requête d'informations faite à une base de données via un langage spécifique.

Signature Dans le cas de Logpoint une signature a la même fonction qu'une expression régulière : détecter et extraire des champs suivant un motif.

Widget Un widget est une extension d'application, les widgets interactifs proposent habituellement des informations ou des divertissements.