# RAPPORT DE STAGE

Du lundi 23 mai au vendredi 24 juin 2022

**Tuteur de stage** : Monsieur PRAUD Alain

**Superviseur académique** : Madame FAUGERAS Sophie

**Stagiaire:** Monsieur ICART Timothé

**Établissement** : Lycée Saint Sauveur, 16 Pl. Saint-Sauveur, 35600 Redon

**Entreprise d'accueil** : EPSYLAN (Etablissement Psychiatrique de Loire-Atlantique Nord), Le Pont Piétin, 44130 Blain

## REMERCIEMENTS

Je tiens sincèrement à remercier Monsieur Alain Praud, mon tuteur de stage et Directeur du service Informatique d'EPSYLAN ainsi que les employés Messieurs Christophe DALIBERT, Xavier COTTINEAU et Arnaud L. EVANS pour la confiance et les nombreux conseils et suggestions qu'ils m'ont accordés durant ce stage, et l'opportunité qu'ils m'ont offert d'acquérir de nouvelles compétences en informatique tout en profitant d'une immersion dans le milieu professionnel .

# SOMMAIRE

## INTRODUCTION

Du 23 mai au 24 juin 2022 qui fut la durer de mon stage au sein du service

Informatique d'EPSYLAN (Etablissement psychiatrique de Loire atlantique Nord).

J'ai pu m'investir au projet d'un SIEM (Security Information & Event

Management).

EPSYLAN situé à BLAIN, créée en 1960, est spécialisé en psychiatrie. Mon tuteur Monsieur Alain PRAUD directeur du Service Informatique m'a formé et guidé dans mon projet.


Mon stage a consisté en la mise en place d'un réseau SIEM donc la collecte de données sur les postes Informatiques de l'hôpital via le collecteur d'événement Windows.

Cette expérience a été l'opportunité pour moi de rencontrer la difficulté de monter un projet de toutes pièces et de constater avec l'entreprise le défi à laquelle elle était confrontée par le risque d'intrusion permanente.

L'élaboration de ce rapport a pour principale source la pratique journalière des missions qui m'étaient affectées, mises en parallèle avec les enseignements théoriques de ma formation.

Afin de rendre compte de manière fidèle du temps passé au sein de EPSYLAN je vais d'abord introduire et présenter l'entreprise ainsi que son développement. Puis, il sera précisé les différentes missions et tâches que j'ai pu effectué et les qualités professionnelles et personnelles que j'ai pu en retirer.

## Présentation d'EPSYLAN

EPSYLAN ou Etablissement Psychiatrique de Loire-Atlantique Nord est un établissement public de santé mentale, EPSYLAN répond aux besoins de soins psychiatriques d'une population (enfants, adultes et personnes âgées) de 350 682 habitants (25% de la population de la Loire Atlantique) sur le territoire étendu du Nord Loire (55% de la surface du département et 101 communes).

Le site d'hospitalisation de Blain est construit sur le terrain d'une ancienne propriété de 120 hectares nommé le Pont-Piétin. Le château et les dépendances, en mauvais état, furent rasés. Les travaux s'étalèrent de septembre 1957 à avril 1960, et les premiers malades arrivèrent en novembre 1960. L'hôpital comptait à l'époque 672 lits répartis dans 12 pavillons organisés en «hôpital-village» selon la conception des années 50. Cette notion a depuis évolué pour privilégier désormais les soins ambulatoires, au plus proche de la population.

# Les missions

Au cours de mon stage j'ai pu découvrir le développement d'un projet dans un milieu professionnel.

Donc de sa création en passant par la phase de recherche puis la phase de test et son application , bien sûr en rencontrant des obstacles qui permettent de s'interroger sur la manière de les résoudre et si cette manière est forcément la bonne pour enfin arriver à la résolution qui nous permet d'avancer. Grâce à ce cheminement ,je vais pouvoir vous expliquer le déroulement de ce projet qui est la mise en place d'un système SIEM.

Tout d'abord la première mission de mon projet a été de mettre en place un collecteur d'événement entre deux postes Windows.

Ma deuxième mission a été d'élargir cette recherche à une nouvelle liste de postes afin d'accumuler plus de types de données.

Ma troisième mission consistait en la mise en place d'un environnement ELK (Elasticsearch Logstash Kibana) sur Windows afin de visualiser et de traiter les données.

Ma dernière mission fut de mettre en place un environnement ELK sur un serveur Linux et de récupérer les données du collecteur d'évènement Windows.

Le projet dans une vision globale était la mise en place d'un systeme SIEM récupérant et analysant les données pour prévenir d'événements suspects comme des attaques par forces brutes ou pour isoler certaines connexions.

## Les outils mis à ma disposition

Afin de mener à bien les différentes tâches listées dans mes missions j'ai eu l'accès a deux postes physiques un Laptop HP et une unite centrale Lenovo ThinkCentre très facile à déplacer grâce à sa petite taille.  Plusieurs machines virtuelles m'ont été confié:

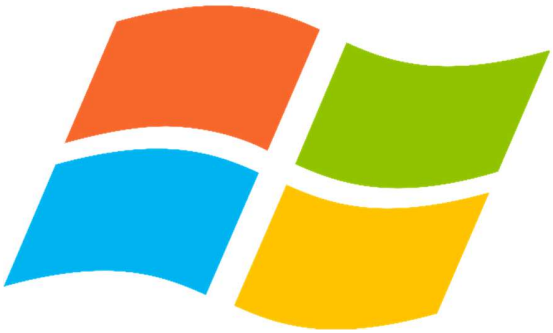
-Une machine Windows Server 2022

-Une machine Windows Server 2019

-Une OVA LINUX Debian

Ainsi qu'une connexion internet et le réseau intranet de l'hôpital.

L'utilisation du groupe de logiciel ELK m'a été grandement recommandé et ainsi que le collecteur d'évènement Windows. De par leur documentation en grandes quantités et fiables.




## Résultats du travail effectué

Dans cette partie, je fais état de ma contribution à l'entreprise.  Voici en exemple, un certain nombre de résultats que j 'ai pu fournir:

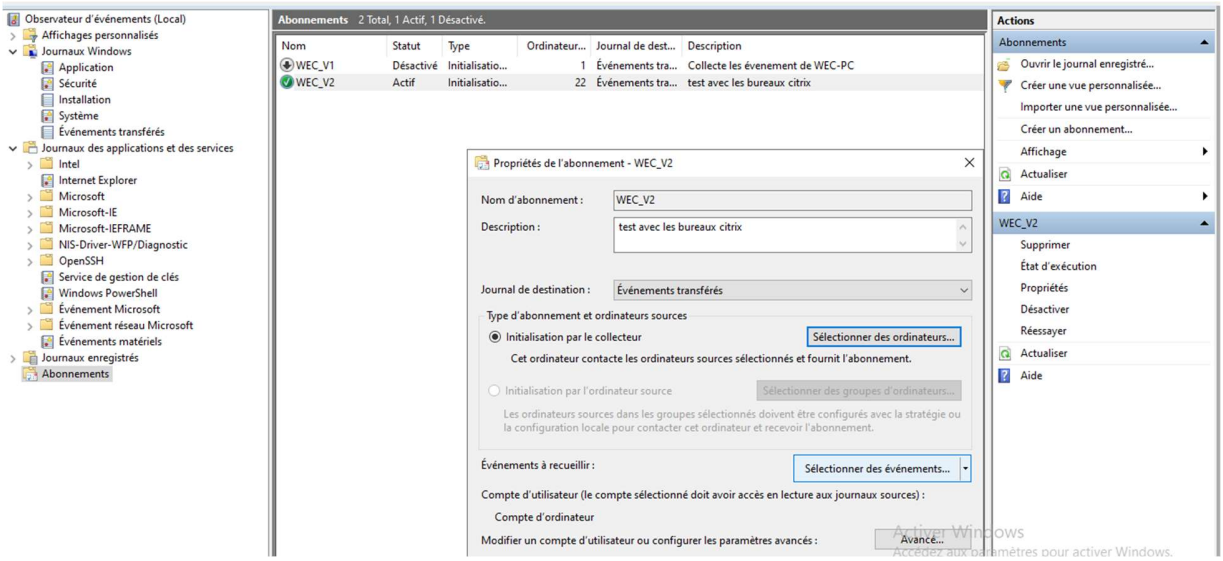
Lors de ma première mission la documentation a été la partie la plus importante car le sujet d'un SIEM étant totalement nouveau pour moi, j'ai dû me documenter. La documentation qui m'a permis le plus de m'informer a été celle de Microsoft car le collecteur d'événement Windows est leur propriété donc les informations fournies sont officielles et ne présente aucun risque de fraude.

Suite à la compréhension du sujet je me suis lancé dans la mise en place des éléments en découvrant mon environnement pour cette mission mes outils pour cette mission ont été un laptop HP, une unité centrale Lenovo ainsi qu'une machine virtuelle Windows serveur 2022.

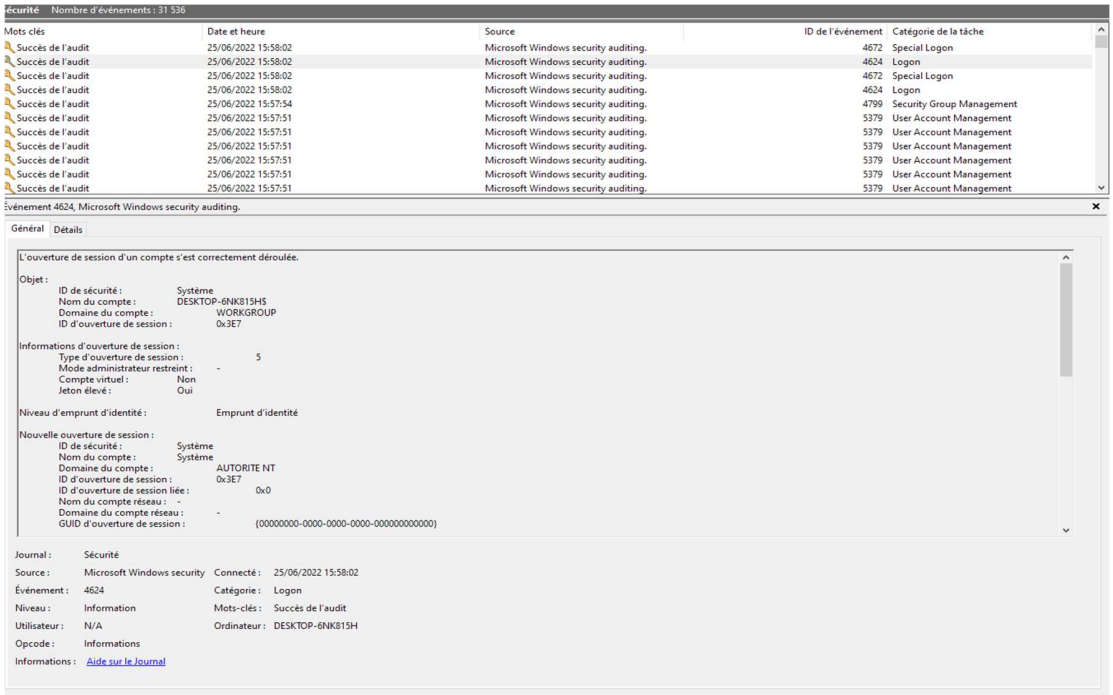
Tout d'abord j'ai configuré la machine Windows server 2022 et l'unité centrale afin de travailler dans un environnement correspondant aux besoins du projet.

Mon premier objectif était de pouvoir les faire communiquer ensembles en ouvrant les ports des Firewalls , sans cette communication la collecte de données m'était impossible.

Ensuite via la documentation Microsoft j'ai mis en place un abonnement. Un abonnement c'est une option du collecteur qui permet de récupérer les logs ou événements des autres postes. Cela se présente comme ceci :




Une fois avoir configuré l'ordinateur à l'écouté et choisi les événements à collecter ,nous avons dû sélectionné un fichier pour recevoir les événements. Voici à quoi ressemble la liste de tous les événements collecter :

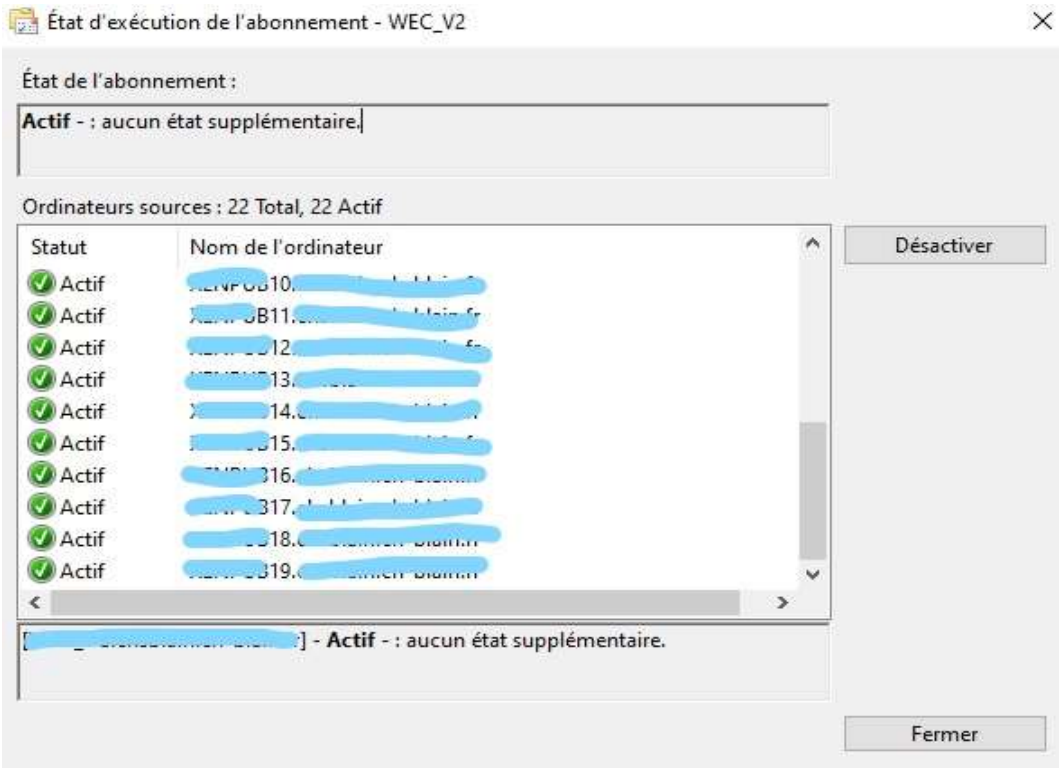



Nous pouvons voir sur cette capture d'écran que cet événement en particulier nous spécifie le succès de connexion du DESKTOP-6NK815H.

Ce qui acheva ma première mission qui était de collecter les événements de l'unité centrale qui m'avait été fourni.

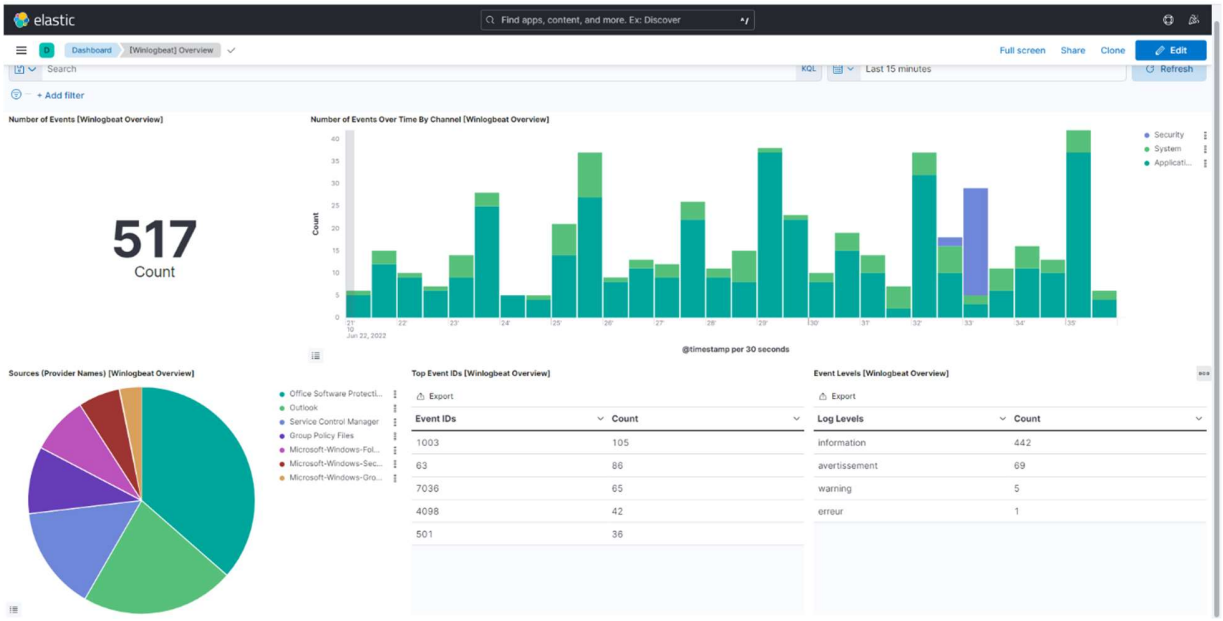
Pour ma deuxième mission on m'a demandé d'élargir la quantité et le type d'événement à récupérer. Pour ceci on m'a fourni une liste d'une vingtaine de postes utilisés au sein de l'hôpital.

La première étape a été de configurer les postes pour pouvoir ainsi communiquer entre la machine Windows serveur 2022 et la liste des postes de l'hôpital. Suite à la configuration des postes, j'ai pu procéder à la mise en place d'un nouvel abonnement.



La mission 3 se concentre principalement autour de Kibana et la visualisation des données, ce nouvel outil qui m'a été donné sera héberger sur une machine virtuelle Windows server 2019 qui me permet d'héberger Kibana.

Lors de cette troisième mission j'ai commencé par me renseigner sur Kibana, j'ai pu comprendre que Kibana permet de visualiser les données par des graphiques et des tableaux afin d'avoir une représentation concrète des données. Par exemple :




J'ai procédé ensuite à installation de Kibana via la documentation officielle https://www.elastic.co/guide/en/kibana/current/windows.html ,une fois ceci fini j'ai injecté un fichier .CSV car c'est un des formats de fichier ou l'on enregistre les événements, mais il y a aussi le format EVTX. Une fois le fichier injecté j'ai pu voir mes événements de manière graphique. Comme sur l'exemple ci-dessus.

Maintenant je peux visualiser les événements dans un temps donné qui se limite au fichier CSV que j'injecte directement dans Kibana. Pour pouvoir améliorer l' injection de données et qu'elle ne soit pas manuelle mais automatique dans Kibana, je dois passer par deux compléments ElasticSearch et LogStash. ElasticSearch permet de stocker et analyser les événements qu'il reçoit afin de les fournir a Kibana. LogStash quant à lui permet de créer des pipelines ou canaux afin de collecter les données et de les transférées vers ElasticSearch. Le groupe ELK donc ElasticSearch LogStash Kibana est un système de BIG DATA, sa définition d'après *TECHTARGET* « Le Big Data est une combinaison de données structurées, semi-structurées et non structurées collectées par des organisations qui peuvent être extraites pour obtenir des informations et utilisées dans des projets d'apprentissage automatique, de modélisation prédictive et d'autres applications d'analyse avancées. ».

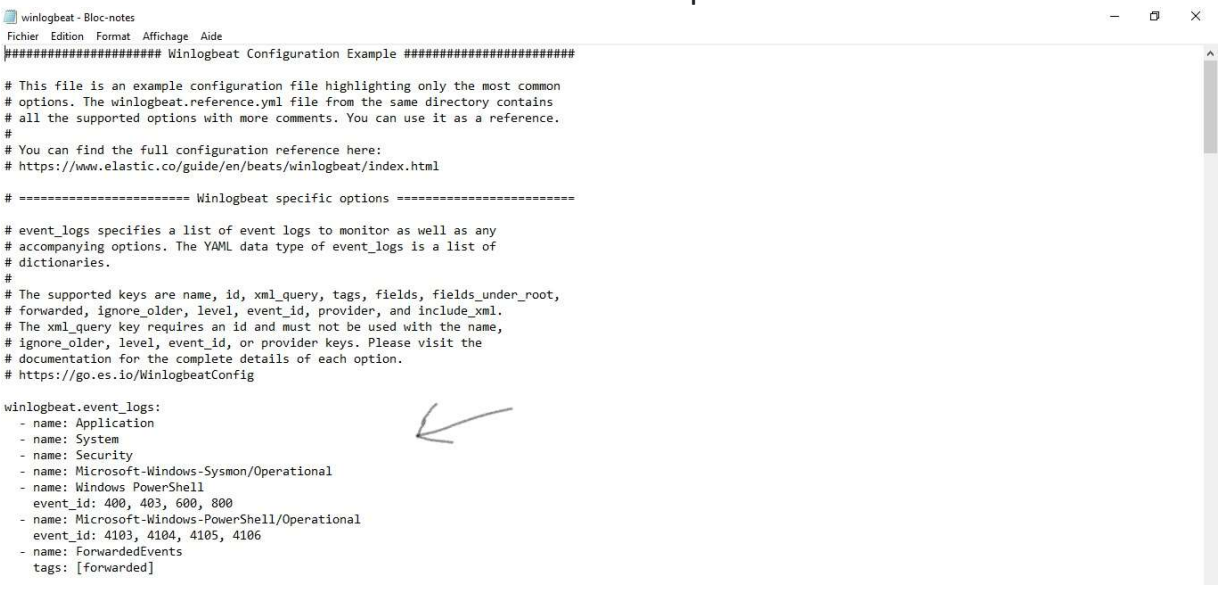
Les outils ELK permette de monitorer les événements afin de prédire des événements indésirables et d'agir en conséquence. Ou aussi alerter quand des événements doivent être réglés dans l'instant.

Tout d'abord j'ai essayé de configurer l'environnement ELK depuis un environnement Windows mais malgré mes nombreuses tentatives des problèmes m'ont empêché de réussir à mettre l'environnement en place.

Le principal problème à été l'installation de LogStash. Tout d'abord un élément est requis pour pouvoir utiliser ELK, c'est l'utilisation de JAVA et de définir un environnement JAVA_HOME ce qui permet le bon fonctionnement du groupe ELK. Mais malgré de nombreuses tentatives de correction j'ai na pas réussi a résoudre ce problème donc l'installation de LogStash m'était impossible car une incompatibilité entre le groupe ELK m'en empêchait.

Suite à cela, l'idée d'installer une OVA Linux Debian m'ont été soumise et grâce à cela l'installation du pack ELK ne m'était plus nécessaire car déjà intégré à l'OVA, pour rappel une OVA est une copie d'une machine virtuelle déjà configurée. Il ne me restait plus qu'à trouver un moyen pour créer un pipeline entre ma machine Windows Server 2022 et mon OVA Debian et pour ceci j'ai utilisé Winlogbeat qui permet la création de pipeline entre Windows et LogStash.

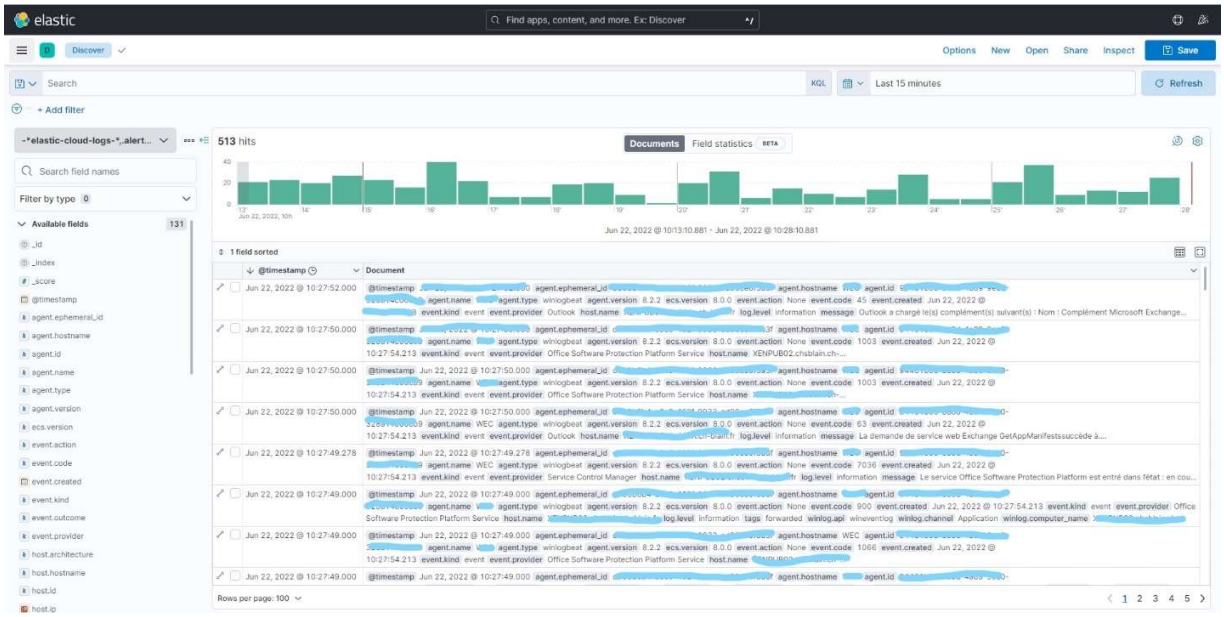
J’ai suivi le tutoriel d’installation WinlogBeat proposé par elastic.co et ai configuré ce dernier voici un exemple du fichier conf :




On peut y voir les répertoires de collectes des évènements.

Pour établir une connexion entre WinlogBeat et LogStash la configuration a été plutôt difficile, plusieurs problèmes de certificat HTTPS m’ont rendu la tâche plus dure mais une fois surmontée des problèmes de SSH se sont imposés à leurs tours sans la résolution de ces deux problèmes la communication est impossible. Et pour cela la configuration du fichier LogStash sur l’OVA Debian et WinlogBeat a dû reconfigurer afin de faire correspondre les canaux SSH et les certificats.

Toutes ces missions ont été réalisées afin d'arriver à cette conclusion :




Cette capture d'écran me permet de vous montrer la réussite de mon projet malgré les difficultés rencontrées.

# Conclusion

Pour conclure, ce stage m'a permis de développer des compétences professionnelles en entreprise et des compétences personnelles dans la mise en place d'un projet.

La compétence qui a le plus été mise à l'épreuve est mon autonomie.

La mise en place d'un projet de A à Z seul m'a permis de me rendre compte de la difficulté de cette tâche. Cela m'a permis de comprendre un nouvel environnement informatique qui est le BIG DATA. Celui-ci est vaste et nécessite de nombreuses connaissances dans le domaine des événements et dans le domaine de la sécurité informatique .Da ns cet environnement qu'est EPSYLAN qui est je le rappelle un hôpital psychiatrique  donc la sécurité est un domaine prédominant au reste car malheureusement aujourd'hui beaucoup d'hôpitaux subissent des cyber-attaques. Toutes ces thématiques viennent conforter mon idée de poursuivre dans ce domaine.