

Royaume du Maroc
UNIVERSITÉ MOHAMED V - RABAT
ECOLE NATIONALE SUPÉRIEURE D'INFORMATIQUE
ET D'ANALYSE DES SYSTÈMES
Direction des Systèmes d'Information et du Numérique
MINISTÈRE DE L'EQUIPEMENT ET DE L'EAU



Rapport de Projet de stage 1-ère année

Etude et intégration de nouveaux modules dans la plateforme ELK

Filière : Sécurité des Systèmes d'Information (SSI)

Présenté par :
AGOULZI Imane

Encadrante :
Mme. MISSAOUI Ilham

Année universitaire : 2021 - 2022

Remerciement

Louange à ALLAH seul, que ses bénédictions soient sur notre seigneur et maître Mohamed et sur les siens.

Avant de commencer ce rapport, je tiens à exprimer mon vif remerciement et ma profonde reconnaissance à ma encadrant madame MISSAOUI Ilham, qui n'a épargné aucun effort pour que ce travail prenne forme. je la remercie pour l'attention particulière qu'il a portée à ce travail et la confiance qu'elle m'a accordé tout au long de ce parcours, ainsi que pour son soutien, ses remarques pertinentes et son encouragement.

On voudrait aussi exprimer nos remerciements les plus loyaux envers tous les enseignants et le personnel de la direction des systèmes d'information et du numérique, Ministre de l'Équipement et de l'eau, ainsi que tous ceux qui ont participé à ma formation. On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Résumé

L'objectif de mon sujet de mon projet de stage est la mise en place d'une solution de supervision des informations et des événements de sécurité que je l'ai effectué au sein de la direction des systèmes d'information du ministère de l'Équipement. Cette dernière souhaite renforcer la sécurité de son SI, en introduisant la technique SIEM.

Après une étude et comparaison des solutions SIEM Open Source, nous avons décidé de mettre en place la pile ELK d'Elastic Stack, qui est une solution Open Source et qui a la capacité de traitement d'un nombre infini d'événements par jour.

Une fois la solution ELK a été déployer, nous avons pu voir ses fruites. Parmi aux, on a l'endpoint security dans j'ai fait des recherches pour bien comprendre sa fonctionnalité.

Abstract

The objective of my subject of my internship project is the implementation of a solution for the supervision of information and security events that I carried out within the information systems directorate of the Ministry of Equipment. The latter wishes to strengthen the security of its IS, by introducing the SIEM technique.

After a study and comparison of SIEM Open Source solutions, we decided to set up the Elastic Stack ELK stack, which is an open source solution and can process an infinite number of events per day.

Once the ELK solution was deployed, the results were visible. Among them, we have the endpoint security in I made some searches to understand its functionality.

Table des matières

Remerciement	3
Résumé	4
Abstract	5
Introduction Générale	13
1 Présentation du cadre du stage :	15
1.1 Présentation de l'organisme d'accueil :	15
1.1.1 Structure organisationnelle de Ministère de l'équipement et d'eau :	15
1.1.2 Organigramme du Direction des Systèmes d'Information et du Numérique :	16
1.1.3 Missions :	17
1.2 Cadre du projet :	17
1.2.1 Contexte et motivation du projet :	17
1.2.2 Problématique :	17
1.2.3 Objectifs de projet :	18
1.3 Conclusion :	18
2 Etude théorique du SEIM et présentation de ELK :	19
2.1 Security Information and Event Management (SIEM) :	19
2.1.1 Présentation de la technologie SEIM :	19
2.1.2 Les briques de SIEM :	19
2.1.3 Principe de fonctionnement de SIEM :	20
2.1.4 Les types des solutions SIEM :	21
2.2 La solution choisie Elastic Stack :	23

2.2.1	Généralités :	23
2.2.2	La pile ELK :	24
2.3	Conclusion :	27
3	Integration des modules endpoint et alerting dans la solution ELK	28
3.1	Les modules de la pile ELK exploiter par la direction de ministère : .	28
3.2	Ressources Matérielles :	29
3.3	Installation et la configuration de la pile ELK :	29
3.3.1	Installation de java :	29
3.3.2	Installation de Elasticsearch :	30
3.3.3	Installation de Kibana :	32
3.3.4	Installation de Logstash :	34
3.3.5	Installation de Filebeat :	35
3.4	Activer la sécurité minimale de la pile ELK :	38
3.4.1	Configurer une sécurité minimale pour Elasticsearch : . . .	38
3.4.2	Configurer la sécurité de base pour la pile ELK :	40
3.4.3	Configurer la sécurité de base pour la pile ELK et le trafic HTTPS sécurisé :	42
3.5	Integration des nouveaux modules :	45
3.5.1	Endpoint security :	45
3.5.2	Alerting sur Kibana :	51
3.6	Conclusion :	54
	Conclusion Générale	55

Table des figures

1.1	Organigramme du DSIN	16
2.1	les composantes du SIEM	21
2.2	les solutions SIEM OpenSource	22
2.3	les solutions SIEM propriétaires	22
2.4	Schéma ELk	24
2.5	Logo de Logstash	24
2.6	Structure de Logstash	25
2.7	Logo de Elasticsearch	26
2.8	Logo de Kibana	27
3.1	Installation de Elasticsearch	28
3.2	Java version	30
3.3	Téléchargement des packages nécessaires	30
3.4	Installation de Elasticsearch	30
3.5	La chemin où stocker les logs	31
3.6	Configurer l'adresse IP et le port d'ecoute de Elasticsearch	31
3.7	Enable and start Elasticsearch	31
3.8	Status de Elasticsearch	31
3.9	Elasticsearch bien installer et configurer	32
3.10	Installation de Kibana	32
3.11	Donner à kibana l'adresse IP de ELasticsearch	33
3.12	Enable and start Kibana	33
3.13	Status de Kibana	33
3.14	Interface de kibana	33
3.15	Changer l'adresse IP et le port d'ecoute de Kibana	34
3.16	Installation de Logstash	34

3.17	Status de Logstash	34
3.18	Les fichiers de configuration de Logstash	35
3.19	Le fichier Input.config	35
3.20	Le fichier Output.conf	35
3.21	Installation de Filebeat	36
3.22	Configuration de Filebeat	36
3.23	Configurer l'output de Filebeat	37
3.24	Les fichiers de configuration de Logstash	37
3.25	Test de la pile ELK	38
3.26	Set up minimal security	39
3.27	Site de ELasticsearch après enable TSL	39
3.28	Interface kibana	40
3.29	generate a CA for our cluster	41
3.30	generate a certificate and private key for the nodes in our cluster	41
3.31	modification de fichier elasticsearch.yml	41
3.32	generate a Certificate Signing Request (CSR)	42
3.33	Unzip the file elasticsearch-ssl-http.zip	43
3.34	Enable HTTPS en Elasticsearch	43
3.35	Le https est bien configuré dans Elasticseach	43
3.36	Encrypt le trafic entre Kibana et Elasticsearch	44
3.37	Generate a server certificate and private key for Kibana	44
3.38	Enable https Kibana	45
3.39	Install endpoint security	46
3.40	Click sur endpoint security après installation	47
3.41	Remplicage des données pour Endpoint Security	47
3.42	Install Elastic Agent sur Linux	47
3.43	Enroll fleet	48
3.44	Enroll fleet 2	48
3.45	Enroll Fleet 3	48
3.46	Enroll Fleet 4	48
3.47	Enroll and start elastic agent	49
3.48	Enrollement is done	49
3.49	Endpoint dans notre machine	49

3.50	Verification sur notre machine linux	50
3.51	Les propriétés gratuites donnés par endpoint security	50
3.52	Les propriétés gratuites donnés par endpoint security 2	50
3.53	Les propriétés gratuites donnés par endpoint security 3	51
3.54	Rule 1	52
3.55	Rule 2	53
3.56	Rule 3	53
3.57	Rule 4	53
3.58	Rule 5	54

Liste des tableaux

- 2.1 Comparaison entre Splunk et ELK 23
- 2.2 Input of Logstash 25
- 2.3 Filter of Logstash 26

Liste des abréviations

- 1 ELK Elasticsearch, Logstash and Kibana
- 2 DSIN Direction des Systèmes d'Information et du Numérique
- 3 SEM Security Event Management
- 4 SIEM Security Information and Event Management
- 5 SIM Security Information Management
- 6 SPL Splunk Search Processing Language

Introduction Générale

Aujourd'hui, l'information est devenue une ressource essentielle pour toute organisation, privée comme publique. Cette évolution rend la sécurité informatique de plus en plus importante, car les réseaux d'organisations font face à toutes sortes de cyberattaques.

Les attaques peuvent être classées en deux catégories : externes (menées des hackers ou des organisations via le réseau Internet) ou internes (menées par les employés au sein de l'organisation elle-même qui cherche à prouver leur efficacité). Les collaborateurs et les employés sont devenus de plus en plus mobiles ; ce qui a mené les entreprises à se doter d'un certain nombre de réseaux intranet et extranet nationaux (voire même mondiaux), avec un grand nombre de réseaux d'accès variés.

C'est pourquoi il est devenu complexe et coûteux de protéger et de prévenir les attaques informatiques. En effet, une entreprise qui cherche à se protéger elle-même doit déployer plusieurs dispositifs de défense et outils d'observation efficaces pour détecter toute faille possible. Les responsables sécurité doivent donc disposer d'outils parfaitement opérationnels et sécurisés, qui assurent la gestion du réseau (gestion des alertes, suivi des pannes, gestion des données de configuration et maintenance ...) par la collecte des alertes provenant de tous les équipements (détecteurs d'intrusion, firewalls, serveurs, systèmes d'exploitation...), les traiter et les classer en éliminant les alertes inutiles et en se basant sur des algorithmes de corrélation d'alertes.

Grâce à ces algorithmes, il est possible d'identifier des attaques réelles à partir d'un ensemble d'alertes. Ces alertes sont ensuite affichées via une interface graphique ou elles sont étiquetées et résolues soit automatiquement à travers des recommandations déjà prédéfinies, soit manuellement par l'administrateur.

Le présent projet consiste à étudier les différentes solutions SIEM (Security Information and Event Management) Open Source présentes sur le marché et mettre en place une solution adaptée aux spécificités et aux contraintes du réseau du ministère de l'équipement.

Le présent rapport s'articule autour de trois chapitres. Le premier décrit le contexte général de notre stage : la présentation de l'organisme d'accueil, les objectifs et la gestion de notre projet. Le deuxième chapitre présente une étude sur la technologie SIEM, une étude comparative des principales solutions SIEM présentes sur le marché et le choix de la meilleure qui répond au besoin du réseau du ministère de l'équipement. Le troisième chapitre décrit la procédure de la mise en place de la solution SIEM choisie, le test du bon fonctionnement et l'exploitation de la solution.

La conclusion générale résume le travail réalisé au cours de ce projet et propose quelques perspectives à court et à moyen terme pour le perfectionnement du travail réaliser.

Chapitre 1

Présentation du cadre du stage :

1.1 Présentation de l'organisme d'accueil :

Le Ministère de l'Équipement et de l'Eau prend en charge des secteurs vitaux qui jouent un rôle essentiel dans le développement économique et social du pays, participe directement ou indirectement à l'aménagement du territoire, à la réduction des disparités régionales et à la création d'un environnement propice pour l'investissement.

Sa mission consiste à élaborer, mettre en œuvre et coordonner la politique du Gouvernement relative au secteur des infrastructures routières, portuaires, hydrauliques et de la météorologie.

Or, la direction des systèmes d'information et du numérique (DSIN) anime le réseau informatique du ministère, et évaluer l'état et le fonctionnement des outils informatiques au sein du ministère, aussi elle assure le développement des outils informatiques et l'introduction des nouvelles technologies.

1.1.1 Structure organisationnelle de Ministère de l'équipement et d'eau :

Le Ministère de l'Équipement et de l'Eau comprend, en outre du cabinet du Ministre, l'administration centrale et les services déconcentrés.

1. L'administration centrale comprend :

- Le Secrétariat Général
- Le Conseil Général de l'Équipement et de l'Eau
- L'Inspection Générale
- La Direction Générale de la Stratégie, des Ressources et du Numérique qui comprend :
 - La Direction de la Stratégie et du Financement
 - La Direction des Ressources Humaines
 - La Direction des Affaires Administratives et Juridiques

- La Direction des Systèmes d'Information et du Numérique
- La Direction des Affaires Techniques et des Relations avec la Profession
- La Direction Générale des Routes qui comprend :
 - La Direction des Etudes, du Développement et de la Recherche Routière
 - La Direction des Travaux et de l'Exploitation Routière
- La Direction Générale de l'Hydraulique qui comprend :
 - La Direction de la Recherche et de la Planification de l'Eau
 - La Direction des Aménagements Hydrauliques
- La Direction Générale de la Météorologie qui comprend :
 - La Direction des Prévisions et des Recherches Météorologiques
 - La Direction des Systèmes d'Observation.
- La Direction des Ports et du Domaine Public Maritime

1.1.2 Organigramme du Direction des Systèmes d'Information et du Numérique :

cette figure illustre la structure du Direction des Systèmes d'Information et du Numérique (DSIN).

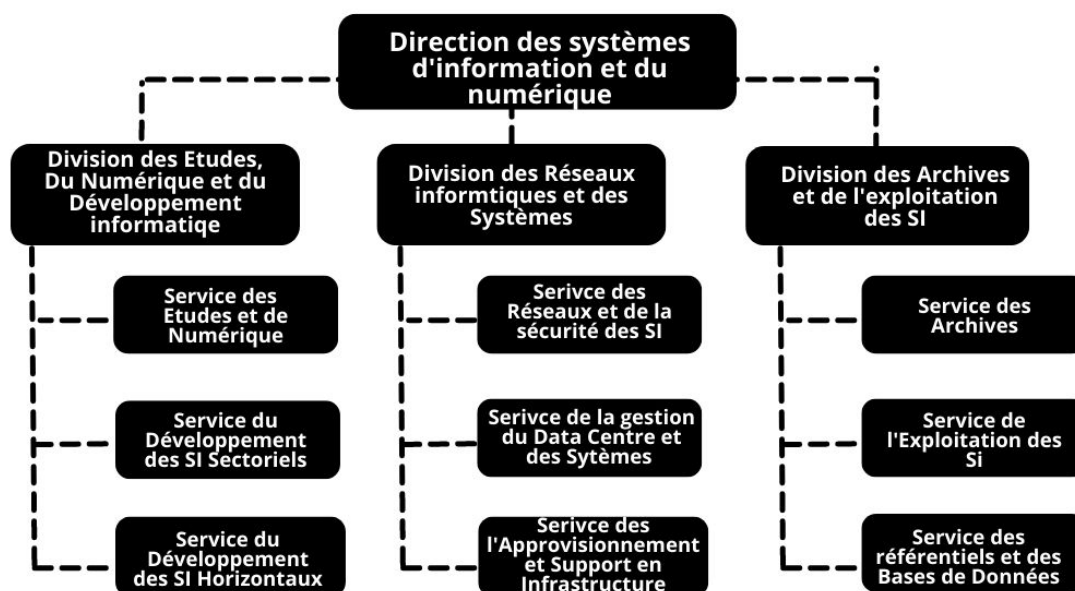


FIGURE 1.1 – Organigramme du DSIN

1.1.3 Missions :

La DSIN est chargée des missions suivantes :

- Participer à la définition des objectifs généraux du ministère en matière des systèmes d'information ;
- Élaborer la politique du ministère en matière de développement de systèmes d'information ;
- Participer à l'élaboration des schéma directeurs informatiques sectoriels ;
- Assurer le développement de l'outil informatique et l'introduction des technologies nouvelles au sein du ministère ;
- Assurer l'exploitation et la maintenance du système informatique du ministère ;
- Animer le réseau informatique du ministère ;
- Évaluer l'état et le fonctionnement de l'outil informatique au sein du ministère ;
- Négocier les acquisitions des licences d'exploitation de logiciels.

1.2 Cadre du projet :

1.2.1 Contexte et motivation du projet :

Ce projet sere à définir plateforme ELK ainsi que ces modules qui peut être intégré selon le besoin de la DSIN du ministère de l'Équipement, pour répondre aux besoins du marché de la sécurité.

Vu que les administrateur sécurités du Ministère utilise la pile ELK juste pour analyser les logs sur l'interface de Kibana, donc leur utilisation de la pile est limiter alors qu'il existe beaucoup de fonctionaliter interessante.

1.2.2 Problématique :

La pile open source ELK offre plusieurs fonctionnalités intéressantes à l'utilisateur, non seulement au niveau de la surveillance mais aussi au niveau de la sécurité à savoir endpoit security, alerting

Malheureusement, la pile n'est pas exploitée à 100% par les administrateurs du Ministère, car ils font la majorité de leur travailler manuellement.

La pile ELK est la solution pour améliorer la sécurité automatiquement, soit on générant les alertes lors d'un problème dans le réseau de ministère au bien en l'utilisant comme un antivirus pour tous les appareillents connecter au réseau

Alors, au lieu de configurer et d'implémenter une sécurité système renforcée sur chaque périphérique géré de leur réseau séparément, l'outil Endpoint Security peut faire ce travail en une seule taché.

Sans oublier les concepts d'alerting qui sont vraiment intéressants pour le ministère lors d'un problème dans leur réseau, car il peut générer les alertes en temps réel.

1.2.3 Objectifs de projet :

Le but de ce projet est de définir les modules à intégrer dans la plateforme selon le besoin sécurité du Ministère.

De ce fait, le projet a pour objectifs :

- L'étude du SIEM : avantages, limitation, risque et outils de déploiement
- La Comparaison entre les solutions SIEM Open Source les plus populaires dans le marché.
- Le choix de la meilleure solution.
- Le test de la solution choisie dans un environnement virtuel.
- Le listing détaillé des fonctionnalités proposées par la suite
- Le choix de ou des modules à intégrer

1.3 Conclusion :

Dans ce chapitre, nous avons donné un aperçu général sur l'organisation DSIN du ministère de l'Équipement et de l'Eau et sur ses différentes missions au sein de laquelle nous avons réalisé notre Projet de Fin d'Études. Et après avoir élaboré la problématique et la méthodologie de gestion de projet, nous allons introduire, dans le chapitre suivant, l'étude de l'Etat de l'art sur les solutions SIEM.

Chapitre 2

Etude théorique du SEIM et présentation de ELK :

2.1 Security Information and Event Management (SIEM) :

2.1.1 Présentation de la technologie SEIM :

Le Security Information Event Management (SIEM) permet aux équipes de sécurité de détecter rapidement des attaques dans l'infrastructure informatique grâce à l'exploitation, au filtrage et à la corrélation de tous les logs collectés.

2.1.2 Les briques de SIEM :

Deux briques constituent une solution de SIEM :

A La première brique appelée SEM, pour Security Event Management, permet l'analyse des logs en temps réel (ou quasi réel) en provenance des systèmes de sécurité, réseaux, d'exploitation et applicatifs :

- Gestion des événements de sécurités,
- Corrélation des événements,
- Réponse aux incidents sur des menaces internes comme externes,
- Analyse en temps réels.

B La seconde brique appelée SIM, pour Security Information Management, permet de fournir des rapports en conformité avec la réglementation, et de surveiller les menaces internes :

- Gestion des logs,
- Rapports,
- Analyses différées.

En regroupant ces deux fonctions, les systèmes SIEM accélèrent l'identification et l'analyse des événements de sécurité, ainsi que la restauration qui s'ensuit. Ils permettent aux responsables de satisfaire aux exigences légales de conformité de l'entreprise.

2.1.3 Principe de fonctionnement de SIEM :

la figure ci-dessus montre les composantes essentielles de SIEM qui permettent son bon fonctionnement, il s'agit de :

- **Source** : Il s'agit des équipements sources qui vont enrichir le SIEM avec des informations. Un équipement source peut être un équipement (PC, Routeur, Switch, Firewall), une application, ou tout autre type de données qui peuvent être surveillées. Bien que n'étant pas un composant en soi du SIEM, celui-ci ne pourrait fonctionner sans ces sources de logs.
- **La collecte des logs** : La première étape du processus d'exploitation des logs est la collecte. Les mécanismes de récupération diffèrent suivant les SIEM utilisés.
- **Le Découpage** : Les journaux d'événements natifs (propres à chaque constructeur) sont découpés pour faire apparaître les éléments unitaires d'information (exemple : l'adresse IP source, l'IP destination, le port source, le port destination)
- **La Normalisation** : Les informations collectées sont normalisées sous un format plus lisible et reformatées en un format unique. Cette normalisation permet de faire des recherches multicritères sur un ou plusieurs champs. Ce sont ces événements qui seront enrichis avec d'autres données et envoyés par la suite vers le moteur de corrélation.
- **La corrélation/ règle** : Le moteur de règle permet de créer des règles dont le but est d'avertir l'administrateur d'une attaque sur le réseau.
Le but du moteur de corrélation est de faire correspondre plusieurs événements standards à partir de sources différentes dans un unique événement corrélé. La corrélation permet de simplifier les procédures de réponse aux incidents, en montrant un seul événement qui a déclenché de multiples événements à venir, à partir d'appareils provenant de diverses sources.
- **Archivage** : Pour utiliser les logs récoltés, Le SIEM a besoin de les stocker pour des raisons de rétention afin d'avoir un historique, si l'administrateur a besoin de regarder ce qui s'est passé quelques heures ou jours avant une attaque.
- **Monitoring** : Le dernier composant d'un SIEM est la façon d'interagir avec les logs après qu'ils ont été collectés, normalisés, corrélés, et stockés. Une interface console (web ou applicative) permet aux personnes s'occupant de la gestion des incidents d'avoir une unique vue de tout l'environnement. Elle permet de voir les logs, de créer des règles, d'afficher des rapports, de personnaliser le SIEM, etc. Elle peut être définie comme une interface d'une base de données où l'utilisateur peut utiliser le langage interne du SIEM pour créer des requêtes permettant d'accéder aux informations.

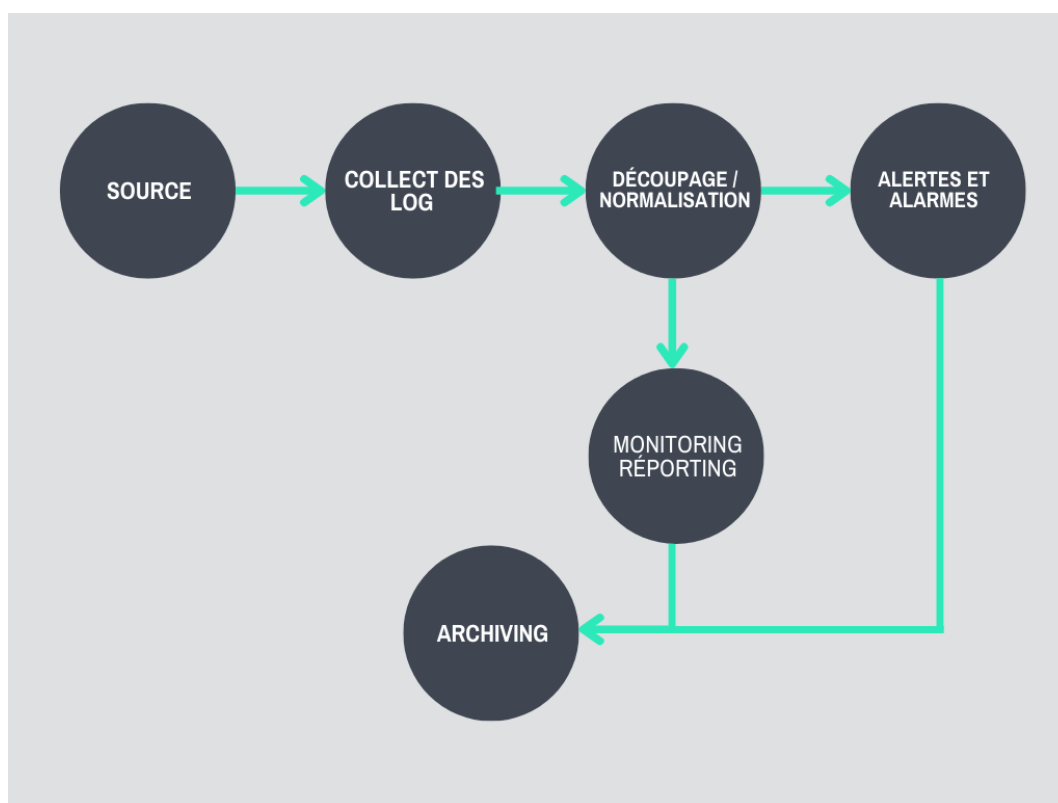


FIGURE 2.1 – les composants du SIEM

2.1.4 Les types des solutions SIEM :

Une solution SIEM doit avant tout être évolutive car la réglementation et les sources de données peuvent évoluer. Elle doit être donc relativement simple à déployer et à maintenir, et doit pouvoir apporter le stockage à long terme des rapports associés.

Les solutions SIEM OpenSource :

Ce sont des solutions gratuites mais des fois des fonctionnalités payantes. Parmi eux on retrouve OSSIM d'Alien Vault, Wazuh couplé de l'HIDS (Host-based Intrusion Detection System) Ossec. Enfin, la « stack » ELK composé d'Elasticsearch Logstash et Kibana qui est la SIEM open source la plus utilisée aujourd'hui.



FIGURE 2.2 – les solutions SIEM OpenSource

Les solutions SIEM propriétaires :

Ce sont des solutions payantes à la base. Splunk s'impose comme le leader des solutions SIEM actuelles. Il en existe cependant beaucoup d'autres qui peuvent rivaliser comme LogRhythm ou encore IBM QRadar.



FIGURE 2.3 – les solutions SIEM propriétaires

Comparaison entre une solution openSource et autre propriétaires :

Dans le tableau suivant, on va faire une comparaison simple, suivant des critères spécifiques, entre une solution Open Source ; on a choisi dans notre cas ELK, et une autre solution propriétaire à savoir Splunk.

Capacités	Splunk et ELK / Elastic Stack sont des plates-formes d'analyse et de gestion de logs puissantes et complètes. Les deux sont hautement personnalisables et disposent de plusieurs fonctions : rapports avancés, capacités de recherche avancée, alertes / notifications, visualisations des données et plus encore.
Installation	Splunk est très complet et très simple d'installation. En effet, il suffit de récupérer l'archive sur leur site officiel, de suivre les procédures d'installation et l'interface de Splunk est déjà accessible. Pour ce qui est de la configuration, elle est aussi relativement simple puisqu'elle se fait principalement via l'interface web. Du côté d'ELK, son installation et sa configuration sont plus complexes.
Traitement des données	L'envoi de données à Splunk est relativement facile. Depuis l'interface web, il est possible d'importer directement des données ou de configurer un port d'écoute ou encore de transmettre d'autres types de données grâce aux différents forwarders de Splunk. Autre avantage pour Splunk, celui de pouvoir extraire des champs de données à tout moment, les données étant stockées au format brut. Pour ELK, il est nécessaire de configurer Logstash de sorte que celui-ci transmette les données à Elasticsearch. La configuration de Logstash peut être compliquée pour ceux qui ne travaillent pas avec les langages de script tels que Bash, Python ou Ruby. Il existe tout de même un bon support en ligne et une communauté importante.
Interface web et recherche	Pour visualiser les différentes données, les interfaces web de Splunk et Kibana pour ELK sont similaires. Il est possible pour les deux plateformes de générer des tableaux, graphiques et d'enregistrer le tout dans des tableaux de bords. La recherche d'information des logs se fait sur l'interface web de Splunk et Kibana. La syntaxe de requête de Kibana est basée sur la syntaxe de requête Lucene (bibliothèque open source écrite en Java qui permet d'indexer et chercher du texte). Splunk utilise lui sa propre syntaxe de requête SPL (Splunk Search Processing Language). Ceux qui connaissent les langages de scripts peuvent se familiariser plus rapidement avec Kibana étant donné qu'il utilise une bibliothèque open source. Pour Splunk, SPL est propriétaire et il faudra donc l'apprendre.
Prix	Splunk dispose de plusieurs versions. La version gratuite limitée à 500 Mo de données par jours ne bénéficie pas entre autre des fonctions d'alertes et de supervision. Il faut en effet passer à la version Splunk Enterprise si vous souhaitez profiter pleinement de toutes les fonctionnalités de Splunk (alertes, monitoring, pas de limite de données...). De plus, avec la version free, en cas de problème vous n'aurez que l'aide de la communauté. Il faut en effet souscrire à un des abonnements pour bénéficier du support total de Splunk. ELK repose sur trois solutions open source mais s'il on veut profiter de plusieurs fonctionnalités comme les alertes, le monitoring, il est possible d'investir dans le « X-Pack ». Ce pack comporte un ensemble de plugins qui viendront compléter la stack de base ELK. Cela permet de rivaliser avec Splunk qui comporte plus de 1000 add-ons et applications dans son portail d'application.
Gestion des utilisateurs et sécurité	Les versions gratuites de Splunk et ELK (sans le X-pack), ne permettent par exemple pas de gérer plusieurs utilisateurs ce qui peut être problématique dans certaines organisations. De plus, pour ELK, tout le monde a accès à l'interface de Kibana puisque celle-ci n'est pas protégée par un mot de passe, il faut la aussi investir dans le X-Pack qui est gratuit 30 jours puis nécessite une licence.

TABLE 2.1 – Comparaison entre Splunk et ELK

2.2 La solution choisie Elastic Stack :

2.2.1 Généralités :

ELK est une collection de programmes Open Source, qui est principalement utilisée pour enregistrer et explorer les logs d'une application, et cela en temps réel. Des nombreuses entreprises autour du monde utilisent les produits ELK, car celles-ci fournissent des informations critiques sur leur application, en temps réel, rendant

la recherche et l'analyse de ces données faciles.

Elle permet en outre :

- la collecte des données à travers de **Logstash**.
- le stockage des données dans le moteur d'indexation **Elasticsearch**
- l'exploitation et l'analyse des données à travers de **Kibana**.

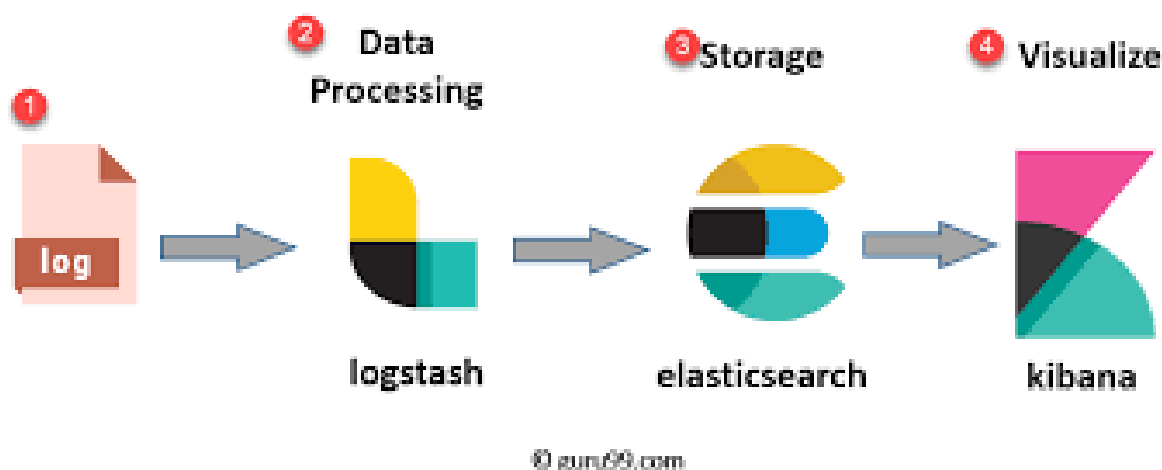


FIGURE 2.4 – Schéma ELk

2.2.2 La pile ELK :

Logstash :

Logstash joue le rôle d'un collecteur de données, ainsi que l'analyseur. Une fois configurée proprement, il peut analyser et filtrer les données qu'il reçoit, afin de les convertir à une forme lisible et indexable.



FIGURE 2.5 – Logo de Logstash

Logstash est composé d'une entrée, d'un filtre et d'une sortie. Son fonctionnement, peut se diffère un utilisateur à un autre, est décrit dans un fichier de configuration.

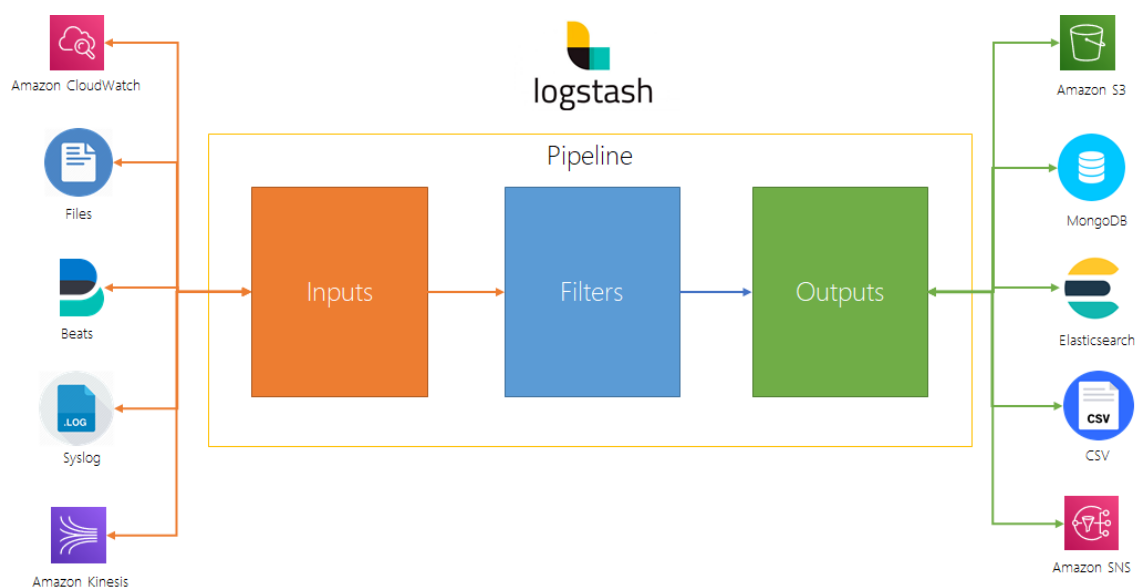


FIGURE 2.6 – Structure de Logstash

Cette figure explique les démarches utiliser par logstash pour extraire les données pertinentes des logs.

1. **Input** : Il existe de nombreux types d'entrées permettant de collecter des données de sources diverses, comme par exemple des fichiers, des bases de données, les résultats d'un exécutable, ou encore depuis des systèmes de messageries comme RabbitMQ ou Kafka et beaucoup d'autres

Plugging	Description
File	Lit le flux d'événements à partir de fichiers
Beats	Reçoit les événements du Framework Elastic Beats
http	Reçoit les événements via HTTP ou HTTPS
Kafka	Lit les événements d'un sujet de Kafka
Tcp	Lit les événements d'un socket TCP
Unix	Lit les événements sur un socket UNIX
Syslog	Lit les messages syslog en tant qu'événements

TABLE 2.2 – Input of Logstash

2. **Filtre** : Les filtres permettent de modifier les données récupérées en entrée. Il existe plusieurs plugins permettant de gérer la plupart des types de données à savoir : le JSON, le CSV, le XML, des données non structurées (texte). Il est donc possible de créer de nouveaux champs à partir de champs existants, de supprimer des champs, ou encore de modifier des champs. Il est également possible de gérer les types et ainsi obtenir en sortie le type le mieux adapté à l'exploitation des données.

Plugging	Description
Grok	Analyse les données d'événement non structurées dans des champs
Mutate	Effectue des modifications générales sur les champs comme : renommer, supprimer, remplacer et modifier des champs dans les événements
Kv	Permet d'analyser les paires clé-valeur
Geoip	Ajoute des informations géographiques sur une adresse IP
Date	Analyse les dates des champs à utiliser comme horodatage Logstash pour un événement

TABLE 2.3 – Filter of Logstash

3. **Output** : le déversement des données ; une fois lues et transformées, il est nécessaire de déverser les données. Ici encore, Logstash dispose d'un certain nombre de plugins.

Une fois son travail fini, il envoie ces données généralement vers Elasticsearch.

Elasticsearch :

Elasticsearch est un moteur de recherche et d'analyse de données open source distribué, basé sur Apache Lucene et développé en Java. Le projet a commencé comme une version extensible (scalable) du framework de recherche open-source Lucene. La capacité d'étendre horizontalement les indices Lucene a ensuite été ajoutée.



FIGURE 2.7 – Logo de Elasticsearch

ElasticSearch est un moteur distribué de stockage, de recherche et d'analyse de contenu.

- Moteur de stockage : il stocke les données en format JSON, annulant ainsi le besoin de joindre à son application de recherche un support de stockage.
- Moteur de recherche : il utilise Apache Lucene pour les fonctionnalités d'indexation et de recherche de contenu sur ces documents JSON.
- Moteur d'analyse de contenu : il s'appuie sur Logstash, un logiciel de gestion de logs et Kibana, une plateforme d'exploration et de visualisation des données, pour effectuer des analyses sur les données qu'il stocke.

ElasticSearch possède six concepts dont leur rôle est de bien réaliser l'indexation et la recherche du contenu. Il est nécessaires de comprendre ses concepts pour pouvoir l'utiliser efficacement : le nœud, le cluster, l'index, le type /mapping le document, la partition (shard) et la réplique.

Kibana :

Kibana se présente sous la forme d'une application web à laquelle vous pouvez vous connecter depuis votre navigateur. Cette application est en quelque sorte la porte d'entrée vers votre cluster Elastic et les données qu'il héberge.



FIGURE 2.8 – Logo de Kibana

Le rôle de Kibana est de proposer une interface graphique et de rassembler au même endroit les outils et les informations nécessaires pour analyser vos données et surveiller votre infrastructure.

2.3 Conclusion :

Dans ce chapitre, nous avons effectué une étude détaillée sur les solutions de gestion des événements et des informations de sécurité Open Source les plus répondues dans le marché, pour choisir une solution qui va s'adapter avec les spécificités et les contraintes du réseau du ministère. Dans le prochain chapitre, on va détailler les étapes suivies lors de l'installation, la configuration et l'exploitation de la solution.

Chapitre 3

Integration des modules endpoint et alerting dans la solution ELK

3.1 Les modules de la pile ELK exploiter par la direction de ministère :

Après l'étude fait par l'équipement de direction des solutions SIEM, et le choix de la solution Open Source d'Elastic Stack, ils sont maintenant capables de faire la collecte, la normalisation, le stockage et le traitement des événements de journalisations de plusieurs sources de manière illimitée.'

La figure suivante montre l'architecture existant exploité par la direction du Ministère.

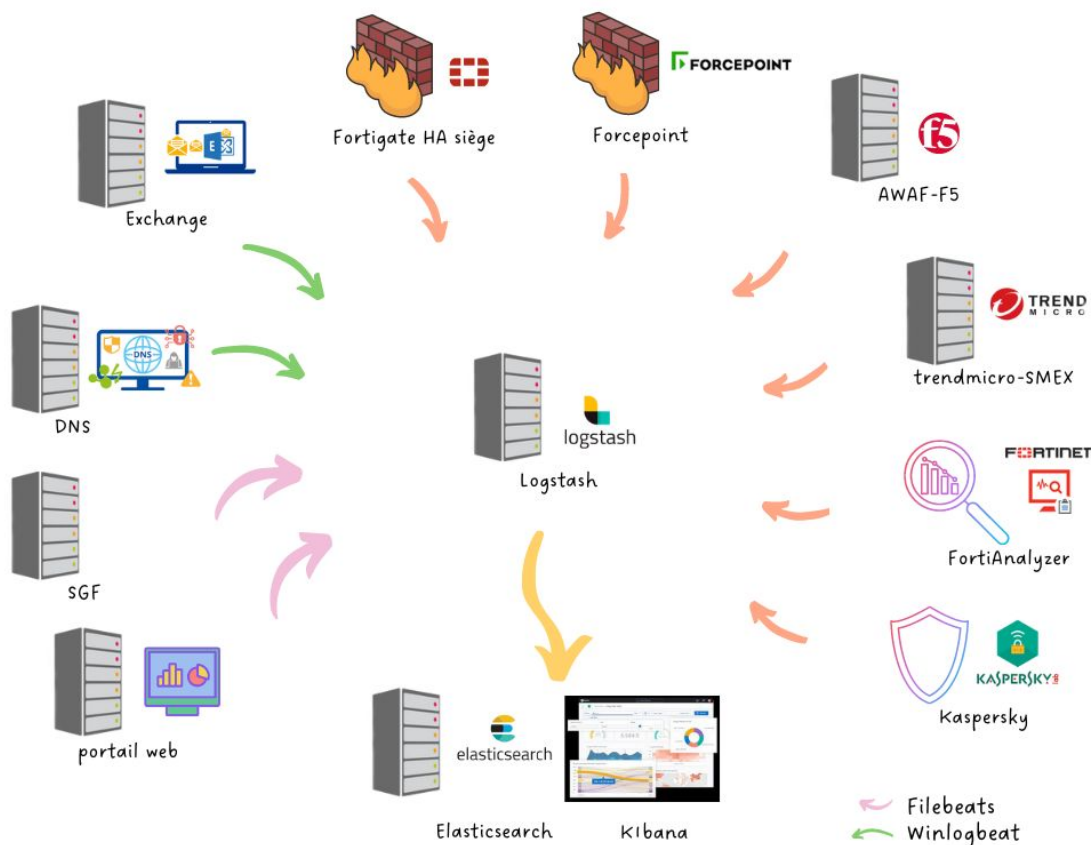


FIGURE 3.1 – Installation de Elasticsearch

Alors, la figure explique l'exploitation de la pile. Comme récapitulatif, logstash, qui est installé tout seul dans un serveur, fait la collecte des logs données par Filebeat, Winlogbeat, Fortigate, AWAf, TrendMicro et Kaspersky, puis il les transmet à Elasticsearch pour les analyser et les transmet à Kibana pour la visualisation. Les deux applications sont installées dans un autre serveur.

Le ministère utilise comme version de toutes les applications Filebeat, Logstash, Elasticsearch, Kibana la version **7.16.2**.

3.2 Ressources Matérielles :

L'environnement génère des GO d'événements par jour, qu'il faut superviser, stocker et analyser. Donc il est nécessaire d'avoir de bonnes ressources matérielles.

Pour cela, le ministère a choisi d'installer Logstash dans un serveur avec des caractéristiques techniques performantes, et d'installer Elasticsearch et Kibana dans un autre serveur aussi performant.

Logstash occupe 582 G de disque et Elasticsearch occupe 7.3 T de disque.

Dans notre cas nous allons travailler avec un serveur Linux, installer sur une machine virtuelle, avec une distribution Kali Linux 2022.1.

Notre serveur comporte les trois applications Logstash, Elasticsearch et Kibana avec les spécifications matérielles suivantes :

- 4 Go de RAM;
- 4500 Mo de stockage;
- 2 vCPU
- Une carte réseau Ethernet.

3.3 Installation et la configuration de la pile ELK :

Dans cette partie, je vais vous montrer les étapes à suivre pour installer la pile ELK sur votre machine Linux :

3.3.1 Installation de Java :

Comme prérequis, il est nécessaire d'avoir une JVM installée pour faire tourner Logstash et Elasticsearch. Concernant Kibana, il n'y a pas de dépendance particulière puisque le logiciel embarque son propre serveur web.

Heureusement, dans Kali Linux, Java est déjà installé.

```
(root@kali)-[~]
# java --version
openjdk 11.0.15 2022-04-19
OpenJDK Runtime Environment (build 11.0.15+10-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.15+10-post-Debian-1, mixed mode, sharing)
```

FIGURE 3.2 – Java version

3.3.2 Installation de Elasticsearch :

Une fois que Java est installée, nous ajoutons le référentiel de pile ELK qui fournit les packages de pile ELK. En exécutons les commandes ci-dessous en tant qu'utilisateur Root :

```
(root@kali)-[~]
# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch.gpg

(root@kali)-[~]
# echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-7.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main

(root@kali)-[~]
# sudo apt update
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [102 kB]
Get:3 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Contents (deb) [3,021 kB]
Hit:2 http://kali.download/kali kali-rolling InRelease
Fetched 3,137 kB in 15s (205 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1287 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

FIGURE 3.3 – Téléchargement des packages nécessaires

Puis on commence par l'installation de Elasticsearch :

```
(root@kali)-[~]
# sudo apt install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 1287 not upgraded.
Need to get 0 B/308 MB of archives.
After this operation, 512 MB of additional disk space will be used.
Selecting previously unselected package elasticsearch.
(Reading database ... 310275 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.5_amd64.deb ...
Unpacking elasticsearch (7.17.5) ...
Setting up elasticsearch (7.17.5) ...
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
```

FIGURE 3.4 – Installation de Elasticsearch

Nous éditons ensuite le fichier de configuration `/etc/elasticsearch/elasticsearch.yml`, afin de modifier la configuration par défaut. On indique le chemin dans lequel nous souhaitons stockés les logs, ainsi que l'adresse IP de la machine Elasticsearch et le port correspondant à savoir :

```

29 # ----- Paths -----
30 #
31 # Path to directory where to store the data (separate multiple locations by comma):
32 #
33 path.data: /var/lib/elasticsearch
34 #
35 # Path to log files:
36 #
37 path.logs: /var/log/elasticsearch
38 #

```

FIGURE 3.5 – La chemin où stocker les logs

```

51 # ----- Network -----
52 #
53 # By default Elasticsearch is only accessible on localhost. Set a different
54 # address here to expose this node on the network:
55 #
56 network.host: localhost
57 #
58 # By default Elasticsearch listens for HTTP traffic on the first free port it
59 # finds starting at 9200. Set a specific HTTP port here:
60 #
61 http.port: 9200
62 #
63 # For more information, consult the network module documentation.
64 #

```

FIGURE 3.6 – Configurer l'adresse IP et le port d'écoute de Elasticsearch

Une fois cette configuration est sauvegardée, nous pouvons activer et démarrer le service Elasticsearch.

```

(root@kali)-[~]
# systemctl start elasticsearch

(root@kali)-[~]
# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.

```

FIGURE 3.7 – Enable and start Elasticsearch

```

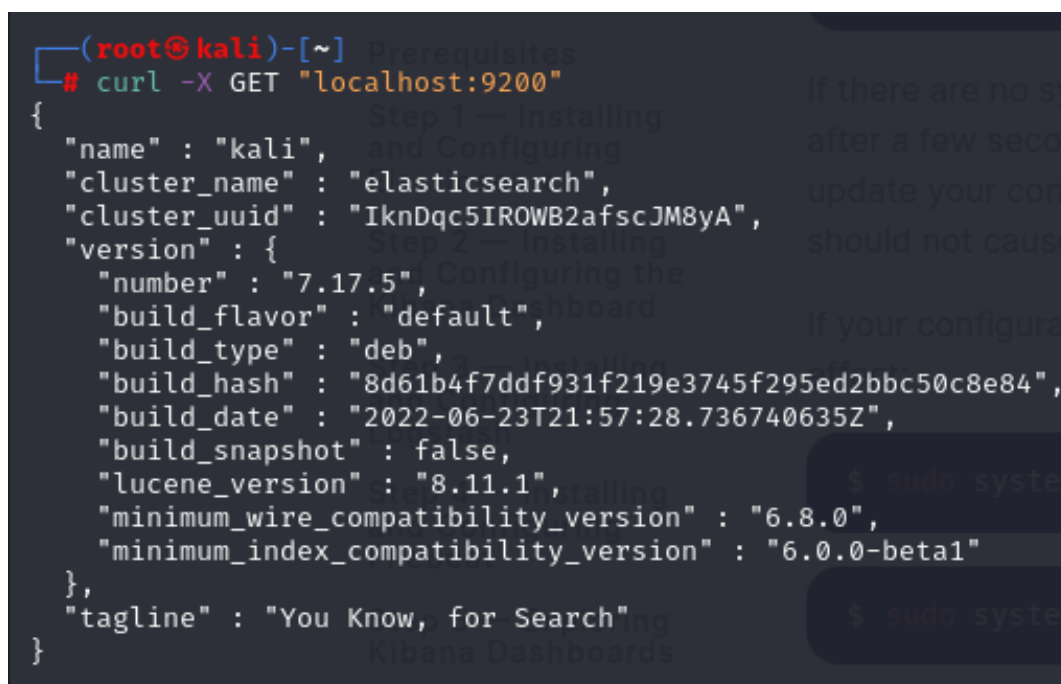
(root@kali)-[~]
# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-07-08 17:38:07 +01; 11min ago
     Docs: https://www.elastic.co
    Main PID: 8576 (java)
      Tasks: 64 (limit: 5081)
     Memory: 1.9G
        CPU: 2min 37.228s
    CGroup: /system.slice/elasticsearch.service
            └─8576 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des>
              8823 /usr/share/elasticsearch/modules/x-pack-ml/platform/linu>

Jul 08 17:37:02 kali systemd[1]: Starting Elasticsearch ...
Jul 08 17:38:07 kali systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)

```

FIGURE 3.8 – Status de Elasticsearch

Pour vérifier le bon fonctionnement d'Elasticsearch, nous exécutons la commande suivante pour voir si Elasticsearch peut écouter à **http ://localhost :9200** :



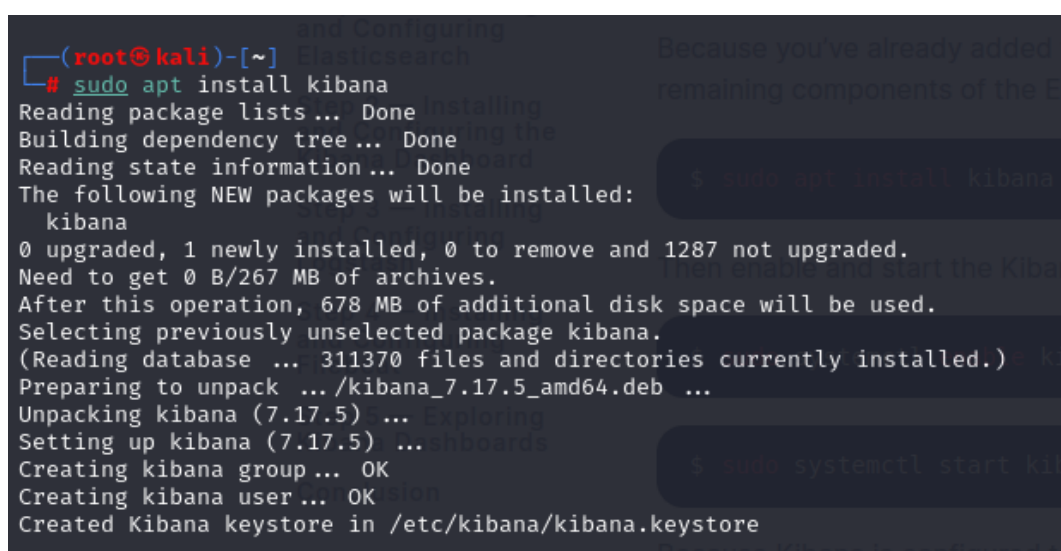
```
(root@kali)-[~]
# curl -X GET "localhost:9200"
{
  "name" : "kali",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "IknDqc5IROWB2afscJM8yA",
  "version" : {
    "number" : "7.17.5",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "8d61b4f7ddf931f219e3745f295ed2bbc50c8e84",
    "build_date" : "2022-06-23T21:57:28.736740635Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

FIGURE 3.9 – Elasticsearch bien installer et configurer

3.3.3 Installation de Kibana :

Kibana est l'interface de visualisation et d'analyse des données des données indexées par Elasticsearch. Nous installons Kibana dans la même machine Kali Linux avec Elasticsearch, à partir du dépôt déjà utilisé pour installer Elasticsearch.

On Commence l'installation de Kibana.



```
(root@kali)-[~]
# sudo apt install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 1287 not upgraded.
Need to get 0 B/267 MB of archives.
After this operation, 678 MB of additional disk space will be used.
Selecting previously unselected package kibana.
(Reading database ... 311370 files and directories currently installed.)
Preparing to unpack ... /kibana_7.17.5_amd64.deb ...
Unpacking kibana (7.17.5) ... Exploring
Setting up kibana (7.17.5) ... shboards
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
```

FIGURE 3.10 – Installation de Kibana

Ensuite il faut apporter quelques modifications sur les paramètres par défaut dans

le fichier de configuration kibana.yml, afin de pointer sur Elasticsearch en spécifiant son adresse IP :

```
30
31 # The URLs of the Elasticsearch instances to use for all your queries.
32 elasticsearch.hosts: ["http://localhost:9200"]
33
34 # Kibana uses an index in Elasticsearch to store saved searches, visualizations and
```

FIGURE 3.11 – Donner à kibana l'adresse IP de Elasticsearch

Nous sauvegardons cette configuration, et nous activons le service Kibana.

```
(root@kali)-[~]
# systemctl start kibana

(root@kali)-[~]
# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
```

FIGURE 3.12 – Enable and start Kibana

```
(root@kali)-[~]
# systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor pre>
   Active: active (running) since Fri 2022-07-08 17:47:59 +01; 1min 28s ago
     Docs: https://www.elastic.co
    Main PID: 11886 (node)
      Tasks: 11 (limit: 5081)
     Memory: 752.8M
        CPU: 1min 7.410s
    CGroup: /system.slice/kibana.service
           └─11886 /usr/share/kibana/bin/../node/bin/node /usr/share/kiban>

Jul 08 17:47:59 kali systemd[1]: Started Kibana.
lines 1-12/12 (END)
```

FIGURE 3.13 – Status de Kibana

Une fois que Kibana a bien été lancé, nous pouvons accéder à son interface graphique en ouvrant un navigateur à l'URL **http://localhost:5601**.

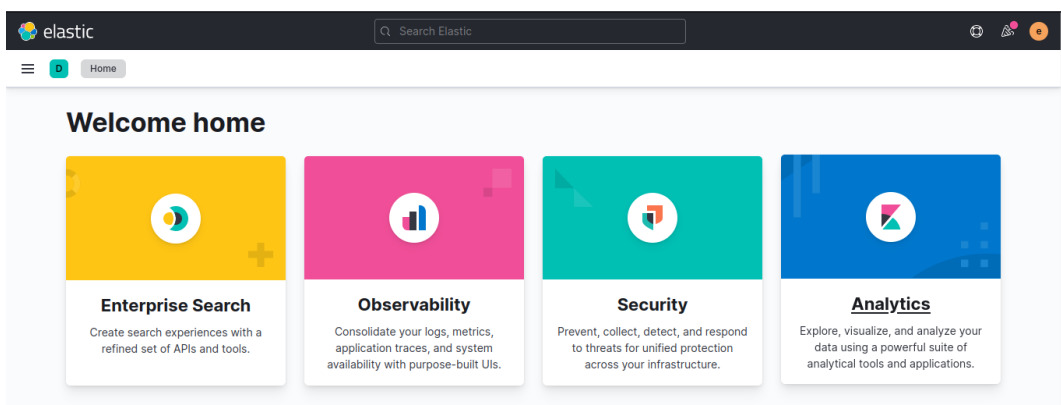


FIGURE 3.14 – Interface de kibana

Là aussi, si nous désirons changer cette adresse, nous pouvons modifier les paramètres `server.port` et `server.host` dans le fichier de configuration de Kibana.

```
1 # Kibana is served by a back end server. This setting specifies the port to use.
2 server.port: 5601
3
4 # Specifies the address to which the Kibana server will bind. IP addresses and host names are
  both valid values.
5 # The default is 'localhost', which usually means remote machines will not be able to connect.
6 # To allow connections from remote users, set this parameter to a non-loopback address.
7 server.host: "localhost"
8
```

FIGURE 3.15 – Changer l'adresse IP et le port d'écoute de Kibana

3.3.4 Installation de Logstash :

Le service Logstash s'installera à partir du dépôt déjà importé pour elasticsearch, il suffit donc de taper la commande suivante.

```
(mineag@kali)-[~]
$ sudo apt-get install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 1270 not upgraded.
Need to get 366 MB of archives.
After this operation, 627 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash
  amd64 1:7.17.5-1 [366 MB]
Fetched 366 MB in 7min 23s (824 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 338212 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.5-1_amd64.deb ...
Unpacking logstash (1:7.17.5-1) ...
Setting up logstash (1:7.17.5-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in
  version 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleas
  erun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
```

FIGURE 3.16 – Installation de Logstash

Une fois l'installation se termine, il faut l'activer. Pour vérifier le bon fonctionnement de logstash :

```
(root@kali)-[~]
$ systemctl status logstash.service
logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
Active: active (running) since Tue 2022-07-26 12:47:20 +01; 14min ago
Main PID: 475 (java)
Tasks: 38 (limit: 5081)
Memory: 646.5M
CPU: 4min 29.671s
CGroup: /system.slice/logstash.service
└─475 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -D>
```

FIGURE 3.17 – Status de Logstash

Nous devons créer un fichier de configuration **.conf** dans le répertoire **/etc/logstash** **/conf.d** pour chaque source de logs. En effet, c'est souvent que les équipements ne génèrent pas des logs avec même format, donc on doit traiter chaque source indépendamment ce fichier est configuré en fonction de nos besoins. Il comporte 3 parties : input, filter et output. Dans mon cas, j'ai séparé les parties dans trois fichiers.

```
(root@kali)-[~]
# ls /etc/logstash/conf.d/
filtre.conf  input.conf  output.conf
```

FIGURE 3.18 – Les fichiers de configuration de Logstash

Rappel :

- **Input** : Ingestion de données de toutes formes, tailles et sources.
- **Filter** : Qui sert à analyser les données et les transformer indépendamment du format ou de la complexité
- **Output** : Permet de faire rediriger les logs d'entrées vers d'autres entrées (Dans notre cas : Elasticsearch).

Donc, on va configurer logstash à collecter les beats et les données à elasticsearch.

```
(root@kali)-[~]
# cat /etc/logstash/conf.d/input.conf
input {
  beats {
    port => 5044
  }
}
```

FIGURE 3.19 – Le fichier Input.conf

```
(root@kali)-[~]
# cat /etc/logstash/conf.d/output.conf
output {
  elasticsearch {
    hosts => ["https://localhost:9200"]
    user => "elastic"
    password => "qwerty123@@@"
    ssl_certificate_verification => false
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
}
```

FIGURE 3.20 – Le fichier Output.conf

3.3.5 Installation de Filebeat :

Comme les autres applications, on commence par l'installation de Filebeat directement, puisque les packages sont installés au début.

```
(mineag@kali)-[~]
$ sudo apt-get install filebeat
[sudo] password for mineag:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 1270 not upgraded.
Need to get 35.3 MB of archives.
After this operation, 130 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt/stable/main/amd64/filebeat amd64 7.17.5 [35.3 MB]
Fetched 35.3 MB in 3min 12s (184 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 354254 files and directories currently installed.)
Preparing to unpack .../filebeat_7.17.5_amd64.deb ...
Unpacking filebeat (7.17.5) ...
Setting up filebeat (7.17.5) ...
Processing triggers for kali-menu (2021.4.2) ...
```

FIGURE 3.21 – Installation de Filebeat

Le fichier de configuration par défaut de Filebeat est **/etc/filebeat/filebeat.yml**

La première chose que vous devez faire est de configurer Filebeat pour collecter les données du journal.

Filebeat peut utiliser différents types d'entrée Filebeat ou des modules Filebeat pour collecter manuellement ou automatiquement des données.

Dans notre cas, on va configurer Filebeat pour collecter les log de notre system Linux.

```
13 # ===== Filebeat inputs =====
14
15 filebeat.inputs:
16
17 # Each - is an input. Most options can be set at the input level, so
18 # you can use different inputs for various configurations.
19 # Below are the input specific configurations.
20
21 # filestream is an input for collecting log messages from files.
22 - type: log
23
24 # Unique ID among all inputs, an ID is required.
25 #id: my-filestream-id
26
27 # Change to true to enable this input configuration.
28 enabled: true
29
30 # Paths that should be crawled and fetched. Glob based paths.
31 paths:
32   - /var/log/*.log
33   #- c:\programdata\elasticsearch\logs\*
34
```

FIGURE 3.22 – Configuration de Filebeat

Filebeat peut être configuré pour envoyer les données du journal vers diverses destinations, y compris Elasticsearch, Logstash, fichier...

Par défaut, Filebeat est configuré avec la sortie Elasticsearch activée. Mais notre but est de appliquer un traitement supplémentaire et le routage des événements générés. Pour cela , on va envoyer vos données à Logstash.

Et donc, on commente l'output elasticsearch et son host, puis on uncommente celle de Logstash.

```
# ----- Elasticsearch Output -----
#output.elasticsearch:
# Array of hosts to connect to.
#hosts: ["localhost:9200"]

# Protocol - either `http` (default) or `https`.
#protocol: "https"

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
#username: "elastic"
#password: "changeme"

# ----- Logstash Output -----
output.logstash:
# The Logstash hosts
hosts: ["localhost:5044"]

# Optional SSL. By default is off.
# List of root certificates for HTTPS server verifications
#ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

# Certificate for SSL client authentication
#ssl.certificate: "/etc/pki/client/cert.pem"

# Client Certificate Key
#ssl.key: "/etc/pki/client/cert.key"
```

FIGURE 3.23 – Configurer l'output de Filebeat

Une fois l'installation se termine, il faut l'activer.

```
(root@kali)-[~] # systemctl start filebeat
# systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
```

FIGURE 3.24 – Les fichiers de configuration de Logstash

Pour vérifier son bon fonctionnement, il suffit d'accéder à l'interface **Kibana** dans la partie **Discover** pour voir les beats.

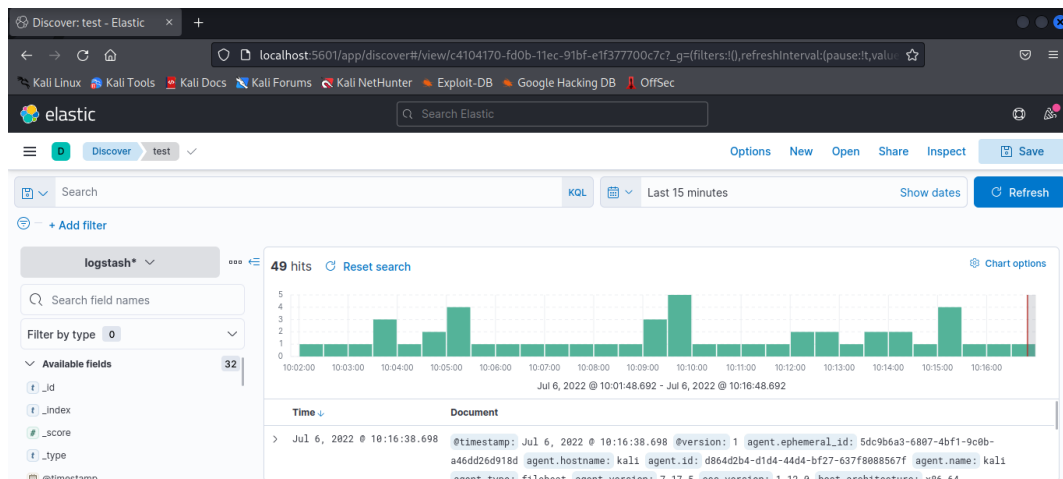


FIGURE 3.25 – Test de la pile ELK

3.4 Activer la sécurité minimale de la pile ELK :

Les fonctions de sécurité Elastic Stack vous permettent de sécuriser facilement un cluster. Grâce à la sécurité, vous pouvez protéger vos données par mot de passe et mettre en œuvre des mesures de sécurité plus avancées telles que le cryptage des communications, le contrôle d'accès basé sur les rôles, le filtrage IP et l'audit.

3.4.1 Configurer une sécurité minimale pour Elasticsearch :

Vous activez les fonctions de sécurité Elasticsearch, puis créez des mots de passe pour les utilisateurs intégrés. Vous pouvez ajouter plus d'utilisateurs plus tard, mais l'utilisation des utilisateurs intégrés simplifie le processus d'activation de la sécurité pour votre cluster.

Lorsque vous utilisez la licence de base, les fonctions de sécurité Elasticsearch sont désactivées par défaut. L'activation des fonctions de sécurité Elasticsearch permet une authentification de base afin que vous puissiez exécuter un cluster local avec authentification par nom d'utilisateur et mot de passe.

Sur chaque nœud de votre cluster, ajoutez le paramètre **xpack.security.enabled** au fichier **elasticsearch.yml** et définissez la valeur à **true**.

Notre cluster a un seul nœud, nous ajoutons le paramètre **discovery.type** dans le même fichier et nous définissons la valeur à **single-node**. Ce paramètre garantit que votre nœud ne se connecte pas par inadvertance à d'autres clusters qui pourraient fonctionner sur votre réseau.

On démarre Elasticsearch. Si vous souhaitez utiliser vos propres mots de passe, exécutez la commande **elasticsearch-setup-passwords** avec le paramètre interactif au lieu du paramètre auto. Ce mode vous permet de configurer les mots de passe pour tous les utilisateurs intégrés.


```
(root@kali)-[/usr/share/elasticsearch]
# ./bin/elasticsearch-setup-passwords interactive
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]y

the console that Set up basic security
Enter password for [elastic]: Set up basic security plus HTTPS
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana_system]:
Reenter password for [kibana_system]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
```

FIGURE 3.26 – Set up minimal security

Lorsque les fonctions de sécurité Elasticsearch sont activées, les utilisateurs doivent se connecter à Kibana avec un nom d'utilisateur et un mot de passe valides.

Isi, vous pouvez voir qu'on est besoin d'un mot de passe pour accéder au site de Elasticsearch.

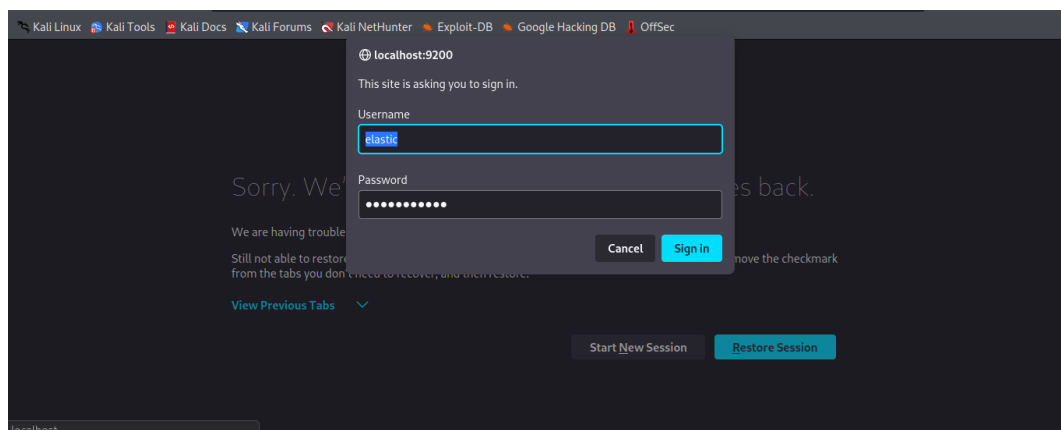


FIGURE 3.27 – Site de ELasticsearch après enable TLS

Vous configurerez Kibana pour utiliser l'utilisateur kibana_system intégré et le mot de passe que vous avez créé précédemment. Kibana effectue certaines tâches de fond qui nécessitent l'utilisation de l'utilisateur kibana_system.

Ceci on Ajoutant le paramètre **elasticsearch.username** au fichier kibana.yml et définir la valeur sur l'utilisateur kibana_system.

Comme vous voyez, pour accéder à Kibana, il faut un mots de passe.

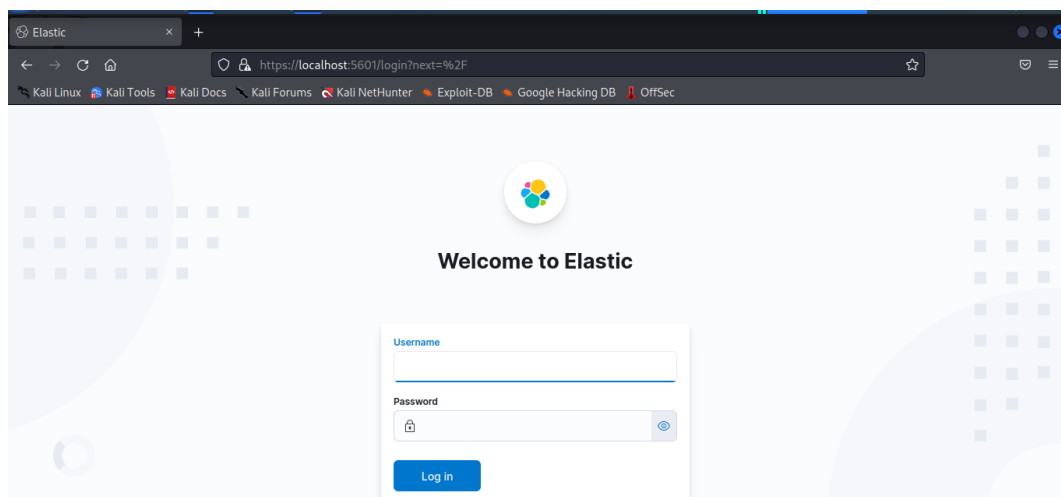


FIGURE 3.28 – Interface kibana

3.4.2 Configurer la sécurité de base pour la pile ELK :

Après avoir ajouté la protection par mot de passe dans la configuration de sécurité minimale, vous devrez configurer Transport Layer Security (TLS). La couche de transport gère toutes les communications internes entre les nœuds de votre cluster.

La couche de transport s'appuie sur un protocole TLS mutuel pour le chiffrement et l'authentification des nœuds. L'application correcte du protocole TLS garantit qu'un nœud malveillant ne peut pas rejoindre le cluster et échanger des données avec d'autres nœuds. Alors que la mise en œuvre de l'authentification par nom d'utilisateur et mot de passe à la couche HTTP est utile pour sécuriser un cluster local, la sécurité de la communication entre les nœuds nécessite TLS.

Et donc il faut Configurer le protocole TLS entre les nœuds pour empêcher les nœuds non autorisés d'accéder à votre cluster.

Pour sécuriser votre cluster, vous devez vous assurer que les communications entre les nœuds sont cryptées et vérifiées, ce qui est réalisé avec TLS mutuel.

Dans un cluster sécurisé, les nœuds Elasticsearch utilisent des certificats pour s'identifier lorsqu'ils communiquent avec d'autres nœuds.


```
(root@kali)-[/usr/share/elasticsearch]
# ls
bin  jdk  lib  modules  NOTICE.txt  plugins  README.asciidoc

(root@kali)-[/usr/share/elasticsearch]
# ./bin/elasticsearch-certutil ca
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'ca' mode generates a new 'certificate authority'
This will create a new X.509 certificate and private key that can be used
to sign certificate when running in 'cert' mode.

Use the 'ca-dn' option if you wish to configure the 'distinguished name'
of the certificate authority

By default the 'ca' mode produces a single PKCS#12 output file which holds:
* The CA certificate
* The CA's private key

If you elect to generate PEM format certificates (the -pem option), then the output
will
be a zip file containing individual files for the CA certificate and private key

Please enter the desired output file [elastic-stack-ca.p12]:
Enter password for elastic-stack-ca.p12 :
```

FIGURE 3.29 – generate a CA for our cluster

```
(root@kali)-[/usr/share/elasticsearch]
# ./bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'cert' mode generates X.509 certificate and private keys.
* By default, this generates a single certificate and key for use
on a single instance.
* The '-multiple' option will prompt you to enter details for multiple
instances and will generate a certificate and key for each one
* The '-in' option allows for the certificate generation to be automated by describing
the details of each instance in a YAML file

* An instance is any piece of the Elastic Stack that requires an SSL certificate in your cluster.
Depending on your configuration, Elasticsearch, Logstash, Kibana, and Beats
may all require a certificate and private key.
* The minimum required value for each instance is a name. This can simply be the
```

FIGURE 3.30 – generate a certificate and private key for the nodes in our cluster

Maintenant que vous avez généré une autorité de certification et des certificats, vous allez mettre à jour votre cluster pour utiliser ces fichiers.

Ceci on ajoutant au file **elasticsearch.yml** les paramètre suivant qui sere à activer la communication entre les nœuds et donner accès au certificat du nœud. :

```
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.client_authentication: required
xpack.security.transport.ssl.keystore.path: /etc/elasticsearch/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: /etc/elasticsearch/elastic-certificates.p12
```

FIGURE 3.31 – modification de fichier elasticsearch.yml

3.4.3 Configurer la sécurité de base pour la pile ELK et le trafic HTTPS sécurisé :

Dans un environnement de production, certaines fonctionnalités Elasticsearch telles que les jetons et les clés API seront désactivées à moins que vous n'activiez TLS sur la couche HTTP. Cette couche de sécurité supplémentaire garantit que toutes les communications vers et depuis votre cluster sont sécurisées.

Lorsque vous exécutez l'outil `elasticsearch-certutil` en mode `http`, l'outil pose plusieurs questions sur la façon dont vous souhaitez générer des certificats. Bien qu'il existe de nombreuses options, les choix suivants donnent lieu à des certificats qui devraient fonctionner dans la plupart des environnements.

```
(root@kali)-[/usr/share/elasticsearch]
# ./bin/elasticsearch-certutil http

## Elasticsearch HTTP Certificate Utility

The 'http' command guides you through the process of generating certificates
for use on the HTTP (Rest) interface for Elasticsearch.

This tool will ask you a number of questions in order to generate the right
set of files for your needs.

## Do you wish to generate a Certificate Signing Request (CSR)?

A CSR is used when you want your certificate to be created by an existing
Certificate Authority (CA) that you do not control (that is, you don't have
access to the keys for that CA).

If you are in a corporate environment with a central security team, then you
may have an existing Corporate CA that can generate your certificate for you.
Infrastructure within your organisation may already be configured to trust this
CA, so it may be easier for clients to connect to Elasticsearch if you use a
CSR and send that request to the team that controls your CA.

If you choose not to generate a CSR, this tool will generate a new certificate
for you. That certificate will be signed by a CA under your control. This is a
quick and easy way to secure your cluster with TLS, but you will need to
configure all your clients to trust that custom CA.
```

FIGURE 3.32 – generate a Certificate Signing Request (CSR)

Après on trouve un fichier compressé sous le nom **elasticsearch-ssl-http.zip** puis on le Décompresse. Ce fichier compressé contient un répertoire pour Elasticsearch et Kibana.

```
(root@kali)-[/usr/share/elasticsearch]
# ls
bin          elastic-stack-ca.p12  modules  README.asciidoc
elastic-certificates.p12  jdk      NOTICE.txt
elasticsearch-ssl-http.zip  lib      plugins

(root@kali)-[/usr/share/elasticsearch]
# unzip elasticsearch-ssl-http.zip
Archive: elasticsearch-ssl-http.zip
  creating: elasticsearch/
  inflating: elasticsearch/README.txt
  inflating: elasticsearch/http.p12
  inflating: elasticsearch/sample-elasticsearch.yml
  creating: kibana/
  inflating: kibana/README.txt
  inflating: kibana/elasticsearch-ca.pem
  inflating: kibana/sample-kibana.yml

(root@kali)-[/usr/share/elasticsearch]
# ls
bin          elasticsearch-ssl-http.zip  kibana  NOTICE.txt
elastic-certificates.p12  elastic-stack-ca.p12      lib      plugins
elasticsearch            jdk                      modules  README.asciidoc
```

FIGURE 3.33 – Unzip the file elasticsearch-ssl-http.zip

Puis on ajoute les paramètres suivant dans le fichier **elasticsearch.yml**.

```
101 xpack.security.http.ssl.enabled: true
102 xpack.security.http.ssl.keystore.path: /etc/elasticsearch/http.p12
```

FIGURE 3.34 – Enable HTTPS en Elasticsearch

Comme vous voyez ici, le HTTPS est bien configuré pour Elasticsearch. Le site est devenu **https://localhost:9200**.

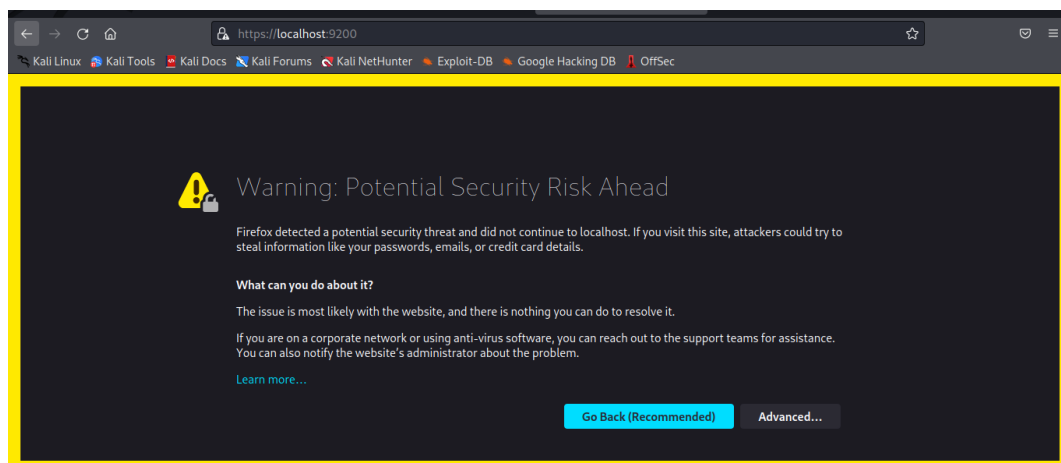


FIGURE 3.35 – Le https est bien configuré dans Elasticsearch

Les navigateurs envoient du trafic à Kibana et Kibana envoie du trafic à Elasticsearch. Ces canaux de communication sont configurés séparément pour utiliser TLS. Vous cryptez le trafic entre Kibana et Elasticsearch, puis cryptez le trafic entre votre navigateur et Kibana.

Encrypt le trafic entre Kibana et Elasticsearch :

Cette configuration est très simple est facile basée sur ce qui prése. Dans on va just faire des petite modification dans le file **kibana.yml** on ajoutant et modifiant l'adresse IP de Elasticsearch à la nouvelle adresse **https ://localhost :9200**.

Lorsque vous avez lancé l'outil **elasticsearch-certutil** avec l'option http, il a créé un répertoire **/kibana** contenant un fichier **elasticsearch-ca.pem**. Vous utilisez ce fichier pour configurer Kibana afin de faire confiance à Elasticsearch CA pour la couche HTTP.

```
64 # Optional setting that enables you to specify a path to the PEM file for the certificate
65 # authority for your Elasticsearch instance.
66 elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/elasticsearch-ca.pem" ]
67
68 # To disregard the validity of SSL certificates, change this setting's value to 'none'.
69 elasticsearch.ssl.verificationMode: none
70
```

FIGURE 3.36 – Encrypt le trafic entre Kibana et Elasticsearch

Encrypt le trafic entre votre navigateur et Kibana :

Vous créez un certificat de serveur et une clé privée pour Kibana. Kibana utilise ce certificat de serveur et la clé privée correspondante lors de la réception des connexions des navigateurs web.

Les instructions suivantes créent une demande de signature de certificat (CSR) pour Kibana. Un CSR contient des renseignements qu'un CA utilise pour produire et signer un certificat de sécurité. Le certificat peut être fiable (signé par un CA public de confiance) ou non fiable (signé par un CA interne). Un certificat auto-signé ou signé à l'interne est acceptable pour les environnements de développement et la construction d'une preuve de concept, mais ne devrait pas être utilisé dans un environnement de production.

```
(root@kali)-[/usr/share/elasticsearch]
# ./bin/elasticsearch-certutil cert -pem \
-ca /usr/share/elasticsearch/elasticsearch-ca.pem \
-name kibana-server \
-dns localhost,www.mykibana.com
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'cert' mode generates X.509 certificate and private keys.
* By default, this generates a single certificate and key for use
on a single instance.
* The '-multiple' option will prompt you to enter details for multiple
instances and will generate a certificate and key for each one
* The '-in' option allows for the certificate generation to be automated by de
scribing
the details of each instance in a YAML file
* An instance is any piece of the Elastic Stack that requires an SSL certifica
te.
Depending on your configuration, Elasticsearch, Logstash, Kibana, and Beats
may all require a certificate and private key.
* The minimum required value for each instance is a name. This can simply be t
he
hostname, which will be used as the Common Name of the certificate. A full
distinguished name may also be used.
* A filename value may be required for each instance. This is necessary when t
```

FIGURE 3.37 – Generate a server certificate and private key for Kibana

Cette commande génère un fichier `csr-bundle.zip` par défaut qui contient deux fichiers.

Maintenant on va ajouter les commandes suivantes dans le fichier **kibana.yml**.

```
51
52 # Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
53 # These settings enable SSL for outgoing requests from the Kibana server to the browser.
54 server.ssl.enabled: true
55 server.ssl.certificate: /etc/kibana/kibana-server.crt
56 server.ssl.key: /etc/kibana/kibana-server.key
57
```

FIGURE 3.38 – Enable https Kibana

Après tous ces modifications l'interface de kibana est maintenant sécurisé. le site est **https ://localhost :5601**.

3.5 Intégration des nouveaux modules :

3.5.1 Endpoint security :

Définition :

L'outil Endpoint Security est un ensemble d'outils et de paramètres complémentaires, qui vous permettent de configurer et d'implémenter une sécurité système renforcée sur les périphériques gérés de votre réseau.

Vous pouvez limiter les connexions réseau des périphériques gérés, limiter l'accès à ces machines depuis d'autres types de périphérique, et utiliser les outils Système de prévention des intrusions (HIPS) et pare-feu Ivanti Firewall pour interdire les opérations d'application non autorisées.

Les composants de Endpoint Security :

Les composants Endpoint Security sont les suivants :

- Reconnaissance de l'emplacement : Contrôle les connexions réseau grâce à des fonctions de reconnaissance de l'emplacement et de définition d'emplacements de confiance. Pour en savoir plus, reportez-vous « Aide d'Endpoint Security ».
- Contrôle des applications : Protège votre système des intrusions. Pour en savoir plus, reportez-vous à « Présentation du contrôle des applications ».
- Pare-feu Ivanti Firewall : Interdit les opérations d'application et les connexions non autorisées. Pour en savoir plus, reportez-vous à « Paramètres d'agent : Ivanti Firewall : Pare-feuParamètres d'agent : Ivanti Firewall ».
- Contrôle de périphériques : Limite l'accès vers et depuis les volumes de stockage, périphériques, interfaces, etc. Pour en savoir plus, reportez-vous à « Présentation de Contrôle des périphériques ».

- Listes d'autorisations et de refus, et liste des fichiers de confiance : Fournit des listes qui répertorient les fichiers configurés avec un ensemble de droits spécifiques (privilèges ou autorisations). Ces listes permettent d'autoriser ou d'interdire l'exécution de certaines actions sur ces fichiers par une application.

Recap :

Bien que Endpoint Security soit un seul agent déployé sur les périphériques cibles, il est entièrement configurable et il est conçu pour regrouper les services des composants de sécurité. Vous pouvez configurer ces composants séparément ou dans le cadre d'un déploiement combiné. Par exemple, vous pouvez déployer uniquement le contrôle des applications, ou bien à la fois Contrôle des applications et Contrôle des périphériques (via leurs paramètres respectifs), ou toute autre combinaison de composants de sécurité.

Configuration de Endpoint Security dans Kibana :

Comme les autres intégrations Elastic, Endpoint Security peut être intégré à l'Agent Elastic via Fleet. Lors de la configuration, l'intégration permet à Elastic Agent de surveiller les événements sur votre hôte et d'envoyer des données à l'application Elastic Security.

Si ce n'est pas la première fois que vous utilisez Elastic Security. Dans l'interface de kibana, <https://localhost:5601>, on suit le chemin suivant : integrations → Browse integration.

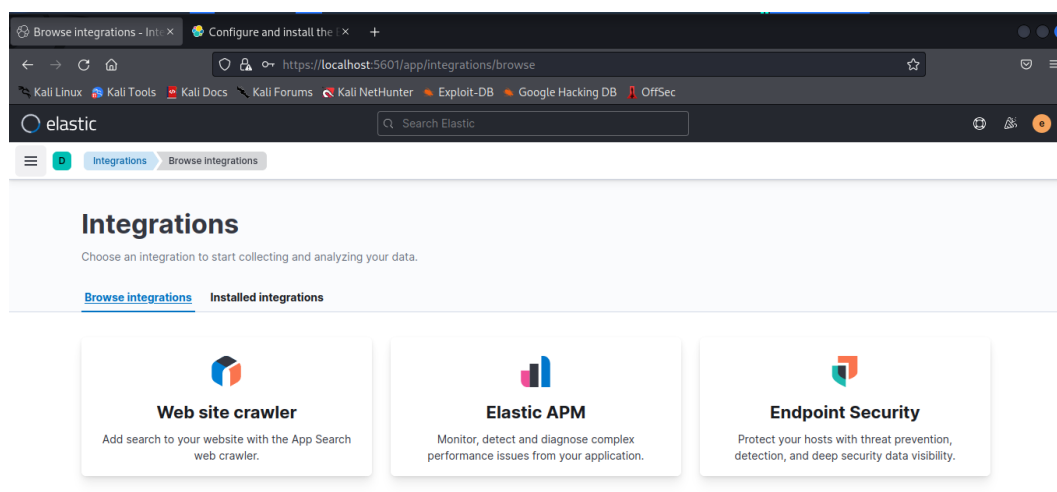


FIGURE 3.39 – Install endpoint security

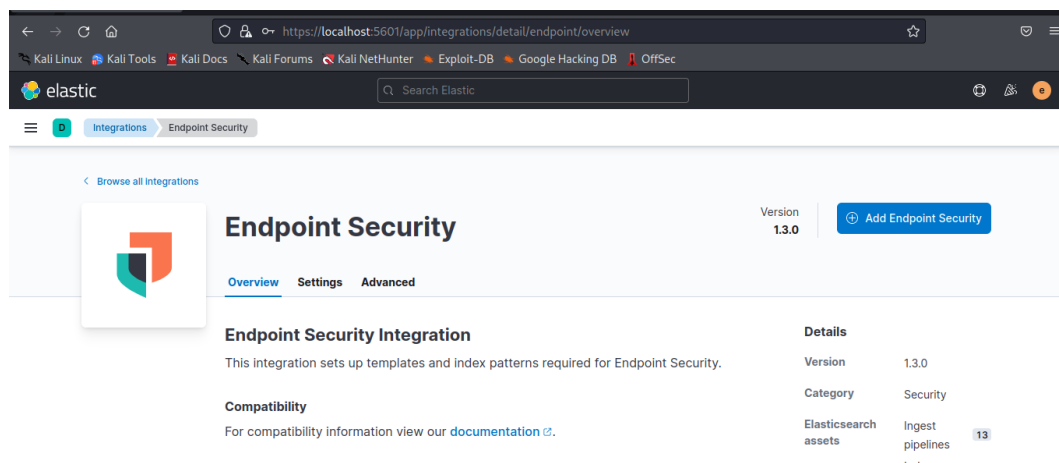


FIGURE 3.40 – Click sur endpoint security après installation

Sélectionnez Add Endpoint Security sur la page Endpoints de l'application Elastic Security ou sur la page d'intégration Endpoint Security (Management → Integrations). La page de configuration d'intégration apparaît.

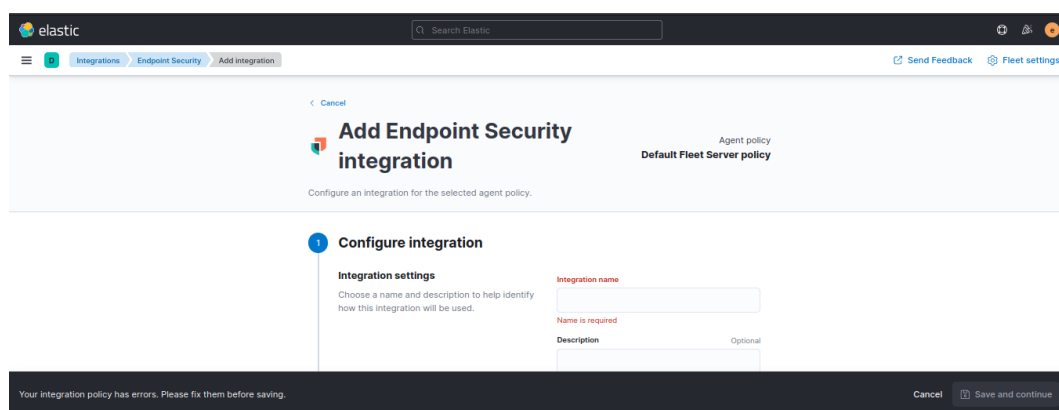


FIGURE 3.41 – Rempilage des données pour Endpoint Security

Il faut maintenant installer elastic-agent sur notre machine linux, et de suivre les étapes suivantes :

- la configuration des agents.
- la configuration de fleet.

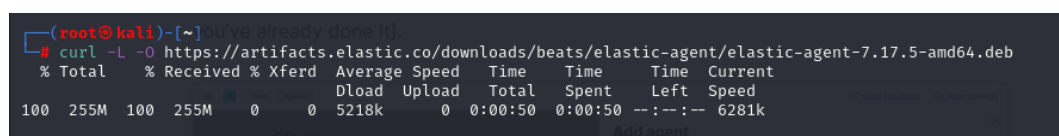


FIGURE 3.42 – Install Elastic Agent sur Linux

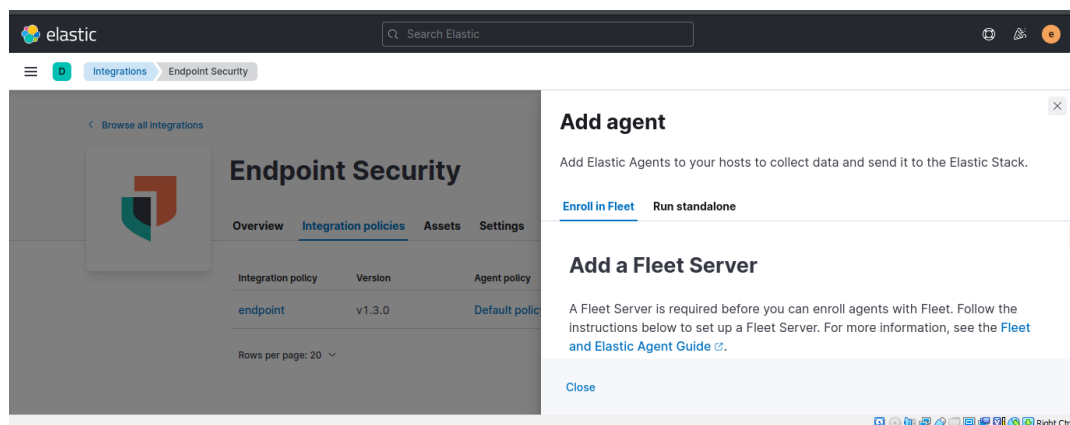


FIGURE 3.43 – Enroll fleet

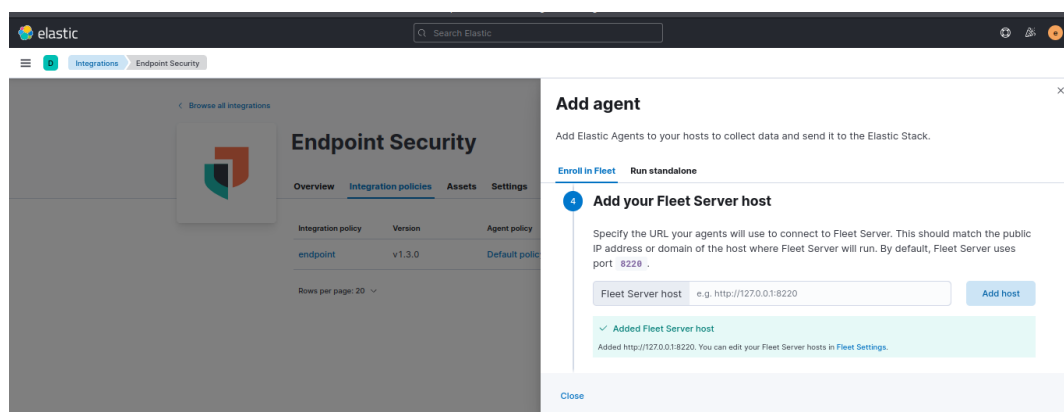


FIGURE 3.44 – Enroll fleet 2

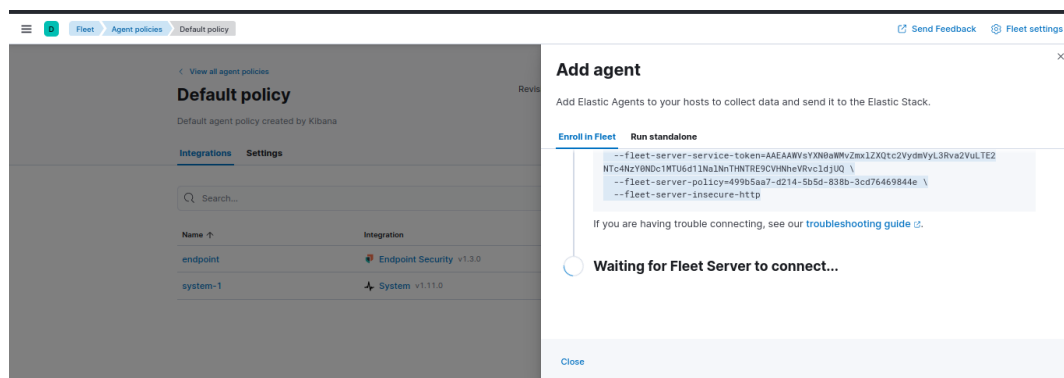


FIGURE 3.45 – Enroll Fleet 3



FIGURE 3.46 – Enroll Fleet 4

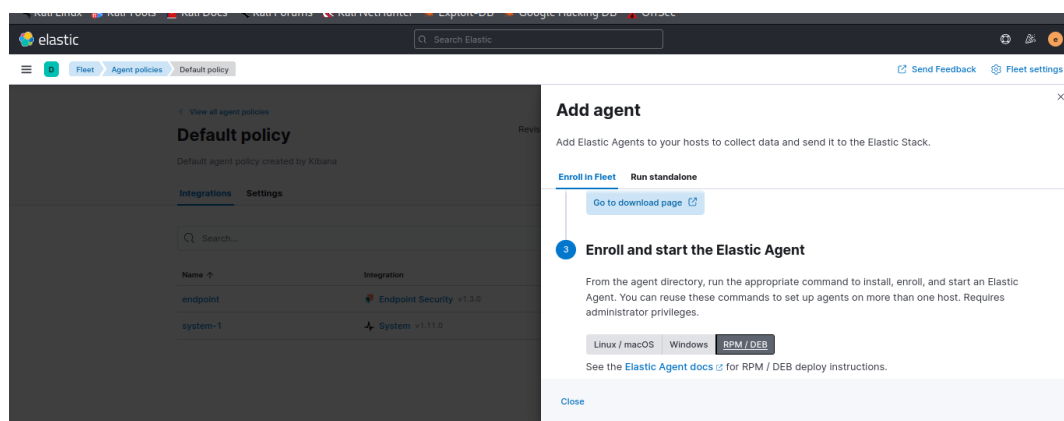


FIGURE 3.47 – Enroll and start elastic agent

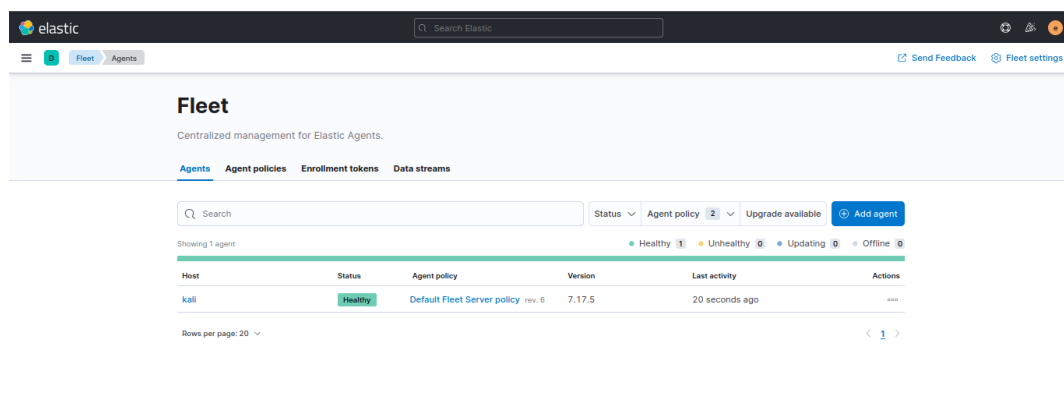


FIGURE 3.48 – Enrollement is done

Maintenant endpoint est bien configurer et lier a notre machine on utilisant elastic-agent.

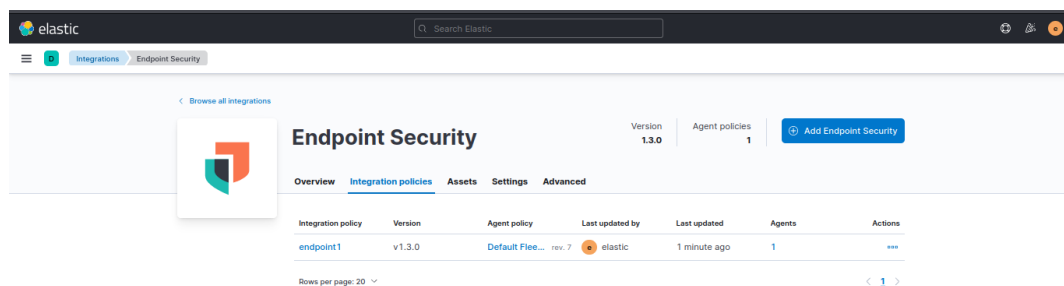


FIGURE 3.49 – Endpoint dans notre machine

```
(root@kali)-[/opt/Elastic/Endpoint]
# /usr/bin/elastic-agent status
Status: HEALTHY
Message: (no message)
Applications:
* fleet-server (HEALTHY)
  Running on policy with Fleet Server integration: 2016d7cc-135e-5583-9758-3ba01f5a06e5
* filebeat_monitoring (HEALTHY)
  Running
* metricbeat_monitoring (HEALTHY)
  Running
* metricbeat (HEALTHY)
  Running
* endpoint-security (HEALTHY)
  Protecting with policy {82ca146c-2cb7-4eb6-a936-24bf61c184e4}
* filebeat (HEALTHY)
  Running
```

FIGURE 3.50 – Verification sur notre machine linux

Les propriétés gratuites donnés par endpoint security :

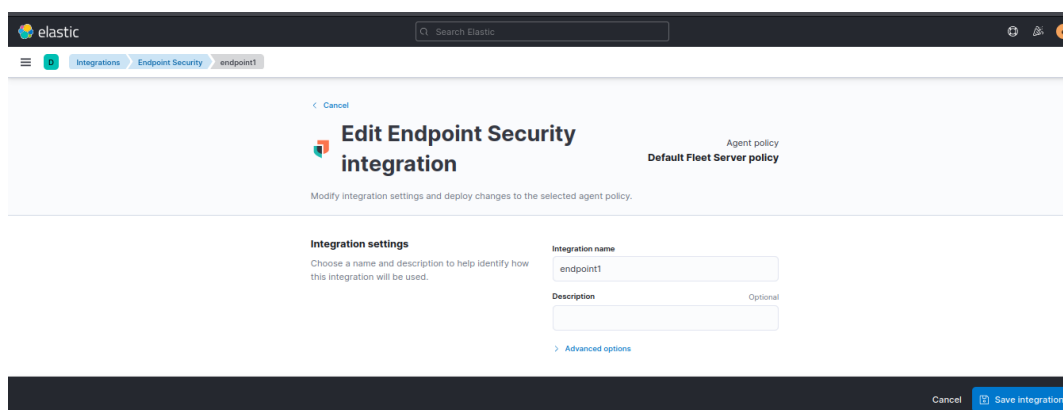


FIGURE 3.51 – Les propriétés gratuites donnés par endpoint security

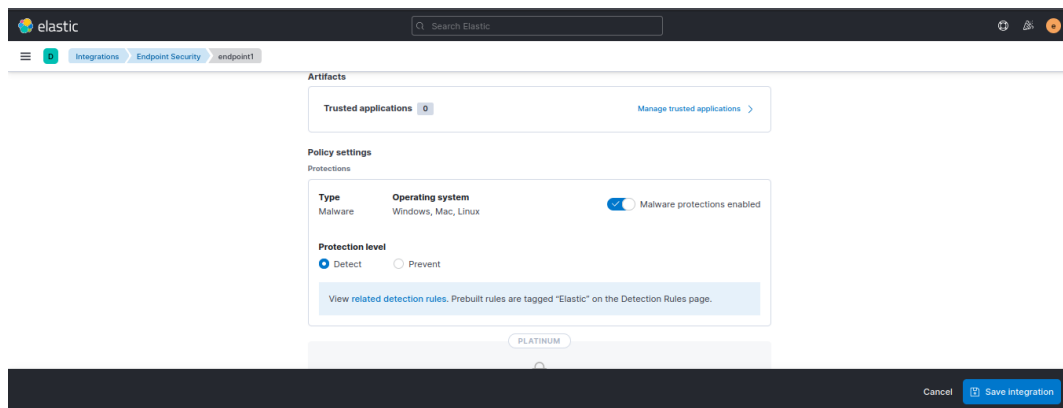


FIGURE 3.52 – Les propriétés gratuites donnés par endpoint security 2

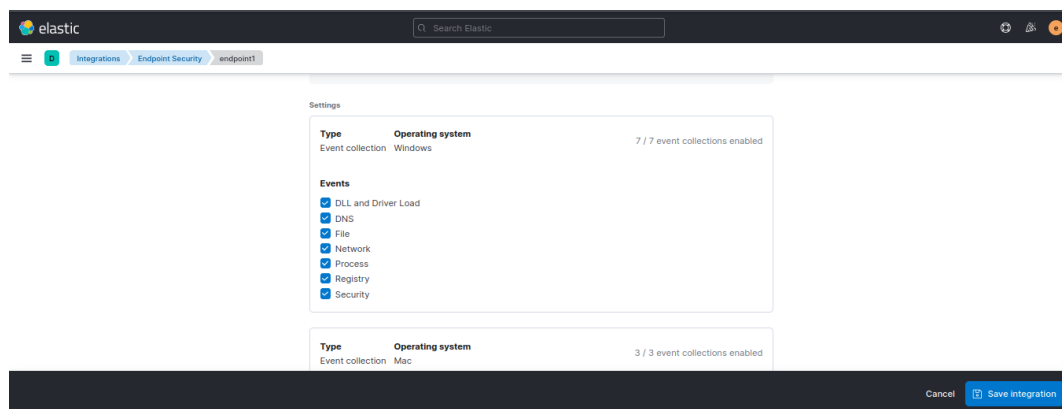


FIGURE 3.53 – Les propriétés gratuites donnés par endpoint security 3

3.5.2 Alerting sur Kibana :

Généralité :

Alert est la technique qui peut délivrer une notification lorsque certaines conditions particulières sont remplies. Cette fonctionnalité que nous pouvons utiliser dans différentes applications de la Kibana de sorte que la gestion peut surveiller toutes les activités du flux de données et si une erreur se produit ou quelque chose arrive au système, la gestion peut prendre des mesures rapides. Les actions sont les services qui fonctionnent avec l'application tierce Kibana en arrière-plan. Les applications seront des notifications par e-mail, ajouter des informations de logs sur le serveur, etc.

Type des alerts :

- Rule : Ceux-ci étaient autrefois appelés Kibana Alerts (pour une raison quelconque Elastic a fait beaucoup de renommage au fil des ans), et dans la plupart des cas, je les ai trouvés pour être le meilleur choix. Vous pouvez les trouver en accédant à Stack Management > Rules and Connectors dans Kibana.

Les règles sont particulièrement bonnes car elles fournissent une interface utilisateur pour créer des alertes et permettent aux conditions d'être réunies à l'aide d'opérateurs logiques. Cependant, il n'existe aucun support pour les opérations avancées telles que les agrégations (calcul du minimum, maximum, somme ou moyenne des champs). Seul le nombre de logs ou un ratio peut être alerté.

Comme condition préalable, l'application Kibana Logs doit être configurée. Cela peut être fait en naviguant vers Logs dans le menu Observability de Kibana. Les journaux ont besoin d'un champ d'horodatage et d'un champ de message.

- Watcher Alerts : Les alertes Watcher sont nettement moins puissantes que les Règles, mais elles ont leurs avantages. Ils peuvent être configurés en accédant à Management > Watcher et en créant une nouvelle « alerte de seuil ».

Une interface utilisateur similaire à celle des règles Kibana est fournie. Des agrégations peuvent être effectuées, mais les requêtes ne peuvent pas être couplées à l'aide d'opérateurs logiques. Cela limite considérablement l'utilité de ces alertes, mais elles pourraient être un bon choix si vous voulez effectuer des agrégations sur un seul champ de log.

- Elastic Security Alerts : Le dernier type d'alerte est certes celui que je n'ai pas eu l'occasion d'utiliser beaucoup. Ceux-ci peuvent être trouvés dans Alertes sous le menu Security dans Kibana. L'IU fournie est semblable à celle du Règlement, de sorte qu'elle présentait les mêmes avantages et inconvénients. Cependant, ces alertes sont limitées à l'utilisation par les intégrations Elastic, les beats Elastic et les systèmes de surveillance. La documentation Elasticsearch contient une liste complète des alertes pré-construites.

Configuration :

Dans cette partie, on va commencer la configuration de Alerting in Kibana. J'ai choisi le premier type **Rules**.

On va donc commencer notre configuration par naviguer dans l'interface Kibana, spécifiquement Stack Management → Rules and Connectors.

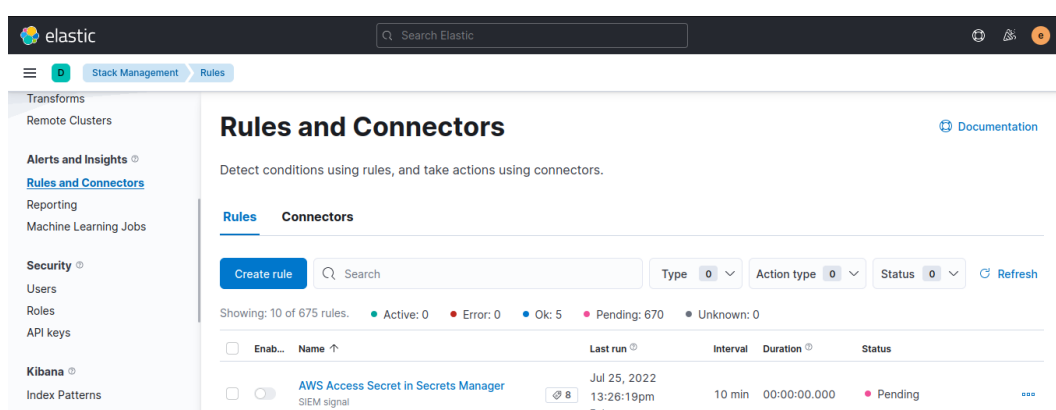


FIGURE 3.54 – Rule 1

Maintenant, on va créer une nouvelle Rule qu'on veut appliquer dans notre système. Moi je vais juste faire un petit test on vérifiant la consommation de CPU s'il dépasse 20 %.

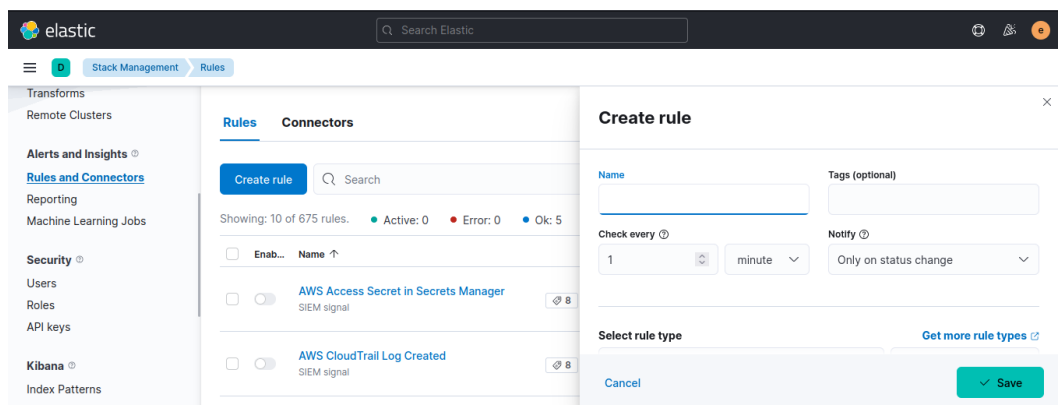


FIGURE 3.55 – Rule 2

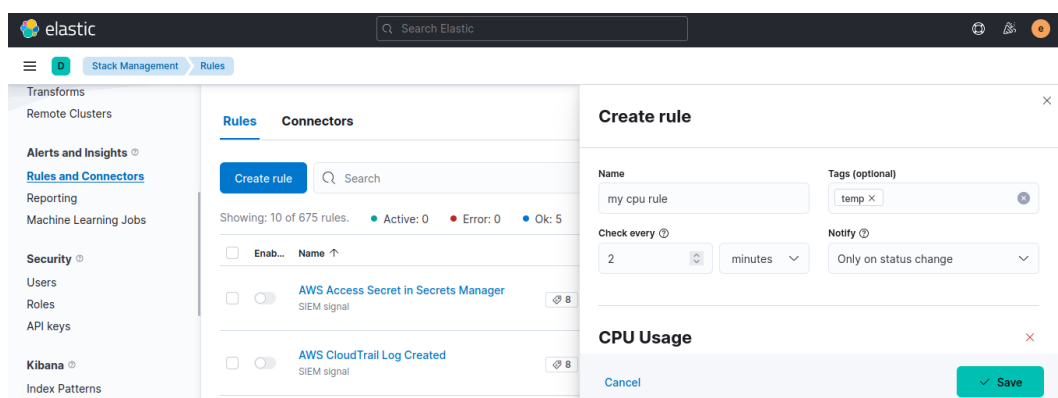


FIGURE 3.56 – Rule 3

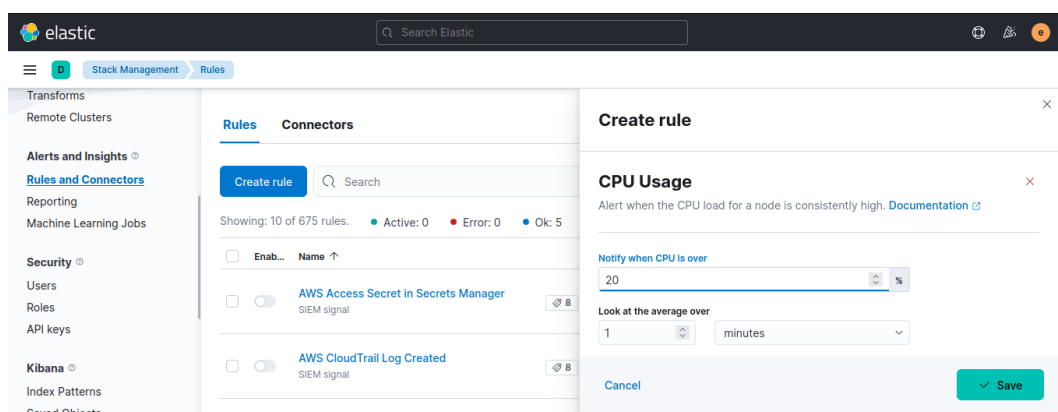


FIGURE 3.57 – Rule 4

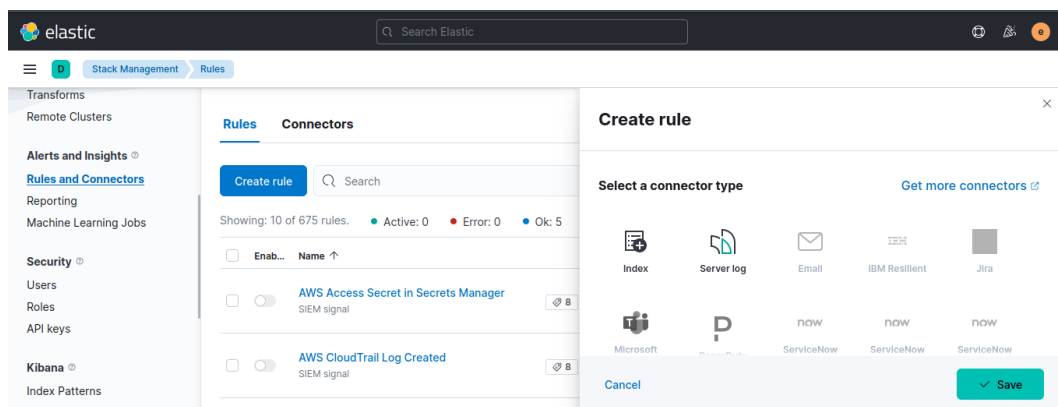


FIGURE 3.58 – Rule 5

3.6 Conclusion :

Dans ce chapitre nous avons présenter les différentes étapes du déploiement d'Elastic Stack ainsi que les cas d'utilisation pratique de cet outil : Nous avons commencé par les spécifications matérielles avec le schéma de déploiement, Ensuite les étapes d'installation des outils nécessaires et la procédure d'intégration des équipements, pour mener enfin à l'exploitation des logs, Endpoint security et la partie alerting.

Malheureusement, j'ai pas eu le temps pour configurer la partie d'alerting dans Kibana.

Conclusion Générale

Pour renforcer la sécurité de son SI, La DSIN souhaite introduire un nouveau service du marché de la sécurité au Maroc, c'est dans ce sens qu'il m'a été confiée de faire le choix et la mise en place d'une solution SIEM.

Nous avons procédé à l'étude des solutions SIEM, et le choix de la solution Open Source d'Elastic Stack, qui permet la collecte, la normalisation, le stockage et le traitement des événements de journalisations de plusieurs sources de manière illimitée. Mais aussi elle est pauvre de d'autres fonctionnalités clés du SIEM, tel que la corrélation, l'alerting, la sécurité, Endpoint Security... On a essayé de compléter ce manque par faire plus des recherches sur les modules de Elastic Stack, comme Endpoint Security pour simplifier la security de SI, le X-Pack pour profiter de l'alerting ainsi que plusieurs fonctionnalités dans la version Beta. Pour mener enfin à une solution SIEM fonctionnelle dans la zone DMZ du réseau de la DSIN, qui nous a permis d'avoir une vue globale sur cette zone et d'éviter plusieurs sources d'attaques.

En guise de perspectives, nous proposons de généraliser la solution Elastic Stack dans les autres zones du réseau de la DSIN, et d'acheter la licence d'X-Pack, pour profiter de toutes les autres fonctionnalités qui sont payantes et intéressantes.

webliographie

- [1] Structure du ministre de l'équipement et d'eau, <http://www.equipement.gov.ma/ministere/Pages/missions-MET.aspx>
- [2] Article Surveillance de votre sécurité avec Elastic stack, Ludovic Paillard : <https://www.linkedin.com/pulse/surveillance-de-votre-s%C3%A9curit%C3%A9-avec-elastic-stack-ludovic-paillard/?originalSubdomain=fr>
- [3] Installatin et la configuration de ELK, <https://newtonpaul.com/how-to-install-elastic-siem-and-elastic-edr/>
- [4] Comparaison entre solution openSource et solution propriétaire de SEIM , <https://www.upguard.com/articles/splunk-vs-elk>
- [5] Comparaison entre solution openSource et solution propriétaire de SEIM , <https://blog.takipi.com/splunk-vs-elk-the-log-management-tools-decision-making-guide/>
webliographie6 Recherche sur Endpoint Security, <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html>
- [6] Information sur Endpoint Security, https://help.ivanti.com/ld/help/fr_FR/LDMS/10.0/Windows/security-endpoint-c-overview.htm