RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Biaou Satournin **DIMON**

Mise en place d'un système de réponse automatisée aux cyberattaques avec la suite ELK : Cas du Port Autonome de Cotonou (PAC)

Sous la supervision :
M. Laurel **LISHOU**
Ingénieur en Systèmes et Réseaux Informatiques

Membres du jury :

Eugène C. EZIN	Professeur	IFRI,IMSP	Président
Aboussidikou ODJO	Ingénieur	Ministère de la justice	Examinateur
Laurel LISHOU	Ingénieur	BGFI	Rapporteur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction 1

1 Présentation de la structure d'accueil et déroulement du stage 3

2 Étude, analyse et choix de la solution 10

3 Déploiement et mise en place de la solution 22

Bibliographie 34

Webographie 35

Table des matières 36

Dédicace

À mon père défunt **Daniel DIMON** et ma mère **ODJOULAGBO Rosine** mes frères et sœurs. À nos proches et à ceux qui nous sont chers, pour vos sacrifices et votre soutien tout au long de notre cursus.

Remerciements

Je tiens à exprimer ma profonde gratitude envers l'Éternel Dieu pour sa protection, l'inspiration et la force qu'il me prodigue chaque jour. Je souhaite adresser mes remerciements les plus sincères à mes parents, qui m'ont soutenu et encouragé tout au long de ce travail.

Mes remerciements vont également à M. Eugène C. EZIN, le directeur, ainsi qu'à toute l'administration et au corps professoral d'IFRI pour la qualité de la formation que j'ai reçue durant ces trois dernières années. Je voudrais également remercier mon maître de mémoire, M. Laurel LISHOU, pour sa patience, sa disponibilité et surtout ses précieux conseils, qui ont grandement enrichi ma réflexion.

Je remercie M. Symphorien DOFFON, mon maître de stage, pour ses idées et sa disponibilité, qui m'ont aidé à affiner le choix de mon thème. Je suis également reconnaissant envers tous les employés de la Direction des Systèmes d'Information (DSI) du Port Autonome de Cotonou (PAC) pour leur soutien. Mes vifs remerciements vont également aux membres du jury qui ont accepté d'examiner mon travail et de l'enrichir par leurs observations et remarques. Je souhaite également exprimer ma sincère gratitude à mon mentor, M. Fawaz MOUSSOUGAN, pour son soutien moral et son accompagnement dans mon parcours professionnel au cours de ces deux dernières années.

Je remercie également mes oncles paternels et maternels, en particulier M. Julien ATCHADE, ma grande sœur Annick DIMON et son époux, ainsi que mes frères et sœurs : Obed DIMON, Urbain AGNICHOLA, Romuald DIMON , Klarita AFFOGNON et Chimène DIMON. À tous ceux qui m'ont accompagnés de près ou de loin dans ce parcours, je vous adresse mes plus sincères remerciements.

Résumé

Dans un environnement informatique, les composants tels que les ordinateurs, les serveurs et divers terminaux forment un réseau complexe. La protection de ces systèmes contre les compromissions est cruciale pour préserver l'intégrité économique et la réputation des entreprises. Ce mémoire se concentre sur l'étude approfondie des Systèmes de Gestion des Informations et des Événements de Sécurité (SIEM) en conjonction avec les solutions de Détection et de Réponse sur les Terminaux (EDR), dans le contexte spécifique du Port Autonome de Cotonou (PAC). Une analyse de marché a permis de sélectionner Elastic Security, une solution open source évolutive répondant aux exigences de performance et de stabilité. Déployée dans un environnement virtualisé Linux en configuration "All-in-One", elle assure une surveillance efficace des serveurs. Deux tests fonctionnels sur des serveurs Linux simulés ont validé ses capacités à détecter et à répondre aux incidents de sécurité, démontrant ainsi son potentiel pour renforcer la sécurité des systèmes portuaires. Cette approche innovante s'inscrit dans une vision stratégique de la lutte contre les cybermenaces dans le secteur portuaire.

Mots clés : Cybermenaces, SIEM (Système de Gestion des Informations et des Événements de Sécurité), EDR (Détection et Réponse sur les Terminaux)

Abstract

In an IT environment, components such as computers, servers, and various terminals form a complex network. Protecting these systems against compromises is crucial to preserve companies' economic integrity and reputation. This thesis focuses on the comprehensive study of Security Information and Event Management (SIEM) systems in conjunction with Endpoint Detection and Response (EDR) solutions, specifically in the context of the Autonomous Port of Cotonou (PAC). A market analysis led to the selection of Elastic Security, a scalable open-source solution meeting performance and stability requirements. Deployed in a Linux virtualized environment with an All-in-One configuration, it ensures effective server monitoring. Two functional tests on simulated Linux servers validated its ability to detect and respond to security incidents, demonstrating its potential to strengthen port system security. This innovative approach is part of a strategic vision to combat cyber threats in the port sector.

Key words: Cyber threats, SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response)

Liste des figures

1.1 Organigramme du Port Autonome de Cotonou (Source : RSSI) 5
1.2 Organigramme de la DSI (Source : RSSI) 7

2.1 Objectifs de la sécurité informatique 11
2.2 HIDS [13]. 15
2.3 NIDS [13]. 15
2.4 Architecture de SIEM 17
2.5 La différence entre SIEM, SIM et SEM 18

3.1 Architecture SIEM de la Stack ELK 23
3.2 Architecture Simplifié du Port Autonome de Cotonou (PAC) 24
3.3 Configuration de l'environnement sur aws 25
3.4 Configuration de la suite ELK 27
3.5 Configuration de la suite ELK 28
3.6 Configuration de l'environnement Windows serveur 2016 28
3.7 Sécurisation de Kibana 29
3.8 Détection de connexion à SSH 30
3.9 Filtrage des connexions SSH 30
3.10 Détection de connexion à SSH 31
3.11 Détection d'attaque par force brute sur notre server web 32

Liste des tableaux

2.1 Comparaison des solutions de sécurité 21

3.1 Comparaison entre EDR et XDR 23

Liste des acronymes

CERT :

Computer Emergency Response Team 20

CIA :

Confidentiality, Integrity, Availability 10

CSIRT :

Computer Security Incident Response Team 20

EDR :

Endpoint detection and response 2, 10

ELK :

Elastic Logstash Kibana 2

IDS :

Intrusion Detection System 14–16, 37

SIEM :

Security Information and Event Management 2, 10

SIM :

Security Information Management vi, 18

SOC :

Security Operations Center 20

XDR :

extended detection and response 23, 37

XSS :

Cross-site scripting 12

Introduction Générale

Le système d'information d'une entreprise est l'ensemble des ressources qui permettent la bonne gestion de l'information, c'est-à-dire collecter, stocker, traiter et communiquer ou partager les informations, ce qui participe à la bonne marche des activités de l'entreprise. Parmi ses ressources, les terminaux (Serveurs, les ordinateurs, etc.) jouent un grand rôle, ils permettent aux employés d'être efficaces et rapides lors du traitement de certaines informations. Il est indispensable de pouvoir particulièrement surveiller des ressources qui sont sensibles en temps réel

1.Contexte

Le Port Autonome de Cotonou (PAC) fait face à des défis croissants en cybersécurité, avec la nécessité de protéger ses infrastructures critiques, telles que les serveurs, postes utilisateurs et systèmes névralgiques, pour assurer la continuité des opérations. Pour répondre à ces enjeux, le PAC a décidé de déployer une solution de surveillance et de réponse proactive, basée sur un système SIEM, enrichie par une solution EDR (Détection et Réponse aux Incidents sur les Terminaux). La stack ELK (Elasticsearch, Logstash, Kibana) a été retenue pour sa capacité à collecter, analyser et visualiser efficacement les données, permettant ainsi une détection proactive des menaces et une réponse automatisée pour sécuriser le port.

2.Problématique

La mise en place d'une solution SIEM robuste basée sur la stack ELK, enrichie par un système EDR, est une réponse stratégique face aux cybermenaces visant les infrastructures critiques du Port Autonome de Cotonou. La problématique réside dans la conception d'une solution optimisée, alliant performance, flexibilité et sécurité. La solution doit détecter rapidement les menaces invisibles aux antivirus traditionnels, tout en préservant les ressources techniques et humaines. L'enjeu principal est de garantir une protection continue et fiable contre les cyberattaques, tout en étant économe en ressources et facile à intégrer dans l'infrastructure existante, tout en favorisant la collaboration entre les équipes de sécurité.

3.Objectifs

3.1 Objectif général

L'objectif général est de mettre en œuvre d'une solution SIEM robuste basée sur la suite ELK, enrichie par un EDR, afin d'améliorer significativement la posture de sécurité du Port Autonome de Cotonou. Cette solution permettra une détection proactive des menaces, une analyse approfondie des incidents et une réponse automatisée, tout en optimisant la collaboration entre les équipes de sécurité.

3.2 Objectifs spécifiques

- **Améliorer la visibilité** : Obtenir une vue en temps réel et centralisée de l'activité du réseau et des systèmes portuaires afin de détecter rapidement les anomalies, les comportements suspects et les menaces avancées non détectées par les solutions de sécurité traditionnelles.
- **Accélérer la détection des incidents** : Mettre en place des règles de corrélation et des alertes personnalisées, utiliser l'analyse comportementale pour détecter les menaces émergentes, et enrichir les données avec l'EDR afin d'améliorer la précision des alertes de sécurité.
- **Automatiser les réponses aux incidents** : Mettre en place des playbooks d'automatisation pour les actions de réponse courantes afin de réduire le temps de réponse aux incidents et minimiser leur impact sur les opérations.
- Effectuer des mises à jour et des ajustements, en tenant compte des contraintes et des besoins évolutifs de l'équipe portuaire, pour garantir la performance continue de la solution au fil du temps.

4.Organisation du mémoire

Le présent mémoire est structuré en trois (03) chapitres :

- Le premier chapitre présente le Port Autonome de Cotonou, son organisation, ses rôles et ses activités, en mettant l'accent sur la Direction IT et ses services, notamment la gestion des systèmes d'information portuaires.
- Le deuxième chapitre, "Étude, analyse et choix de la solution", traite des fondements de la sécurité informatique, analyse les solutions existant sur marché et justifie le choix de la solution la plus adaptée aux besoins portuaires face aux cybermenaces.
- Le troisième chapitre, "Déploiement et mise en place de la solution", décrit l'implémentation de la solution retenue et présente les tests de validation réalisés.

Chapitre 1

Présentation de la structure d'accueil et déroulement du stage

Introduction

Dans ce chapitre, nous présenterons d'une part la structure du Port Autonome de Cotonou (PAC) à travers son historique et sa situation géographique, sa vision et ses services, ses activités, son domaine de compétence, son Organigramme et d'autre part, nous aborderons son organisation ainsi que le déroulement du stage.

1.1 Présentation de la structure d'accueil (PAC)

1.1.1 Localisation

Le Port Autonome de Cotonou (PAC) est situé à la bordure Nord-Est de l'océan Atlantique ou encore à l'extrême sud de Cotonou, capitale économique du Bénin. Il est limité au nord par la Société Béninoise des Manutentions Portuaires (SOBEMAP) et la poste, à l'Est par la Loterie National du Bénin (LNB) à l'Ouest par l'hôtel NOVOTEL puis au Sud par une ère opérationnelle d'environ 4km. Il faut noter que le Port Autonome De Cotonou se reconnait même à 500m à la ronde grâce au grand paquebot, navire et grue d'embarquement ou de débarquement que l'on peut apercevoir dans les airs.

1.1.2 Historique

Le Port Autonome de Cotonou (PAC) est un organisme public à caractère industriel et commercial doté depuis 2022, d'un capital social d'environ plus de trois cent quarante-deux milliards (342.625.216.490) de francs CFA. Créé le 31 décembre 1964 par la loi n°64-39 modifiée par l'ordonnance N°76-55 du 12 octobre 1976, il est inauguré le 1er août 1965 par l'accostage de son tout premier navire, le « Marechal FOCH », après avoir cédé la place au wharf de Wxlacodji, passerelle métallique de 400m avancée sur la mer, construite en 1891 et exploité pendant plusieurs années. Le Port Autonome de Cotonou représente l'autorité portuaire chargé d'assurer l'entretien et l'exploitation des installations du Port de

Cotonou, de gérer le domaine portuaire et d'exécuter les travaux d'amélioration et d'extension dudit port. Désigné comme poumon de l'économie du Bénin pour sa fonction de moteur de développement de l'économie nationale, le Port de Cotonou bénéficie d'une position géostratégique optimale qui lui permet de jouer un rôle important dans l'économie sous-régionale notamment dans les pays de l'hinterland et le Nigéria, pour lesquels il constitue un débouché naturel. Depuis plus d'un demi-siècle, le Port de Cotonou accompagne le développement de l'import-export dans la sous-région et en est une référence. Ces expériences cumulées au fil des ans lui permettent aujourd'hui d'être une plateforme écocitoyenne certifiée ISO 14001 :2015, ISO 9001 :2015 et ISO 45001 :2018, respectivement pour sa politique Environnementale et ses systèmes de Management de la Qualité, puis Santé Sécurité au Travail. Dans son évolution et pour booster sa rentabilité afin d'assurer sa mutation technologique et infrastructurelle, le Port Autonome de Cotonou, obtient un partenariat en 2018, avec le Port of Antwerp Bruges International (POABI – Ex PAI), filiale du Port anversois de Belgique. Cette nouvelle collaboration sera axée sur la modernisation, le repositionnement et le transfert de compétences. Le Port Autonome de Cotonou emploie aujourd'hui plus de six cent (600) personnes. C'est une équipe intergénérationnelle composée d'hommes et de femmes, experts des secteurs portuaire, maritime et logistique, mais aussi avec des parcours différents, parfois atypiques et d'une diversité de métiers et de profils. La plupart sont issus du secteur des télécoms, autant du secteur privé, que du secteur public, et cumulent jusqu'à plus de 20 années d'expériences significatives. À l'horizon 2026, grâce à la mise en œuvre de ses douze (12) grands travaux, le Port de Cotonou sera doté de nouvelles infrastructures et d'équipements de pointe grâce à la mise en œuvre d'un ambitieux plan directeur financé à hauteur de plus de quatre cent cinquante (450) milliards de francs CFA. Le Port Autonome de Cotonou ambitionne ainsi de faire du Port de Cotonou une plateforme logistique moderne, sécurisée et offrant des services de qualité.
Source : DRH

1.1.3 Missions

Les missions assignées au Port Autonome de Cotonou sont variées et comprennent notamment :

- L'exploitation, la gestion et l'entretien des installations portuaires ;
- L'élaboration des règlements de police et d'exploitation et leur application.
- La surveillance et la sécurité des biens et des personnes sur toute l'étendue du domaine portuaire, plan d'eau y compris ;
- L'exécution de toutes les prestations liées à l'assistance et à la navigation (entrée, sortie et séjour à quai de navire)
- Mise en œuvre de toutes les actions susceptibles de traduire, dans les faits, la politique maritime et portuaire béninoise dont les grandes lignes sont définies par le gouvernement du Bénin.

1.1.4 Structure organisationnelle

1. **Le Conseil d'Administration (CA)**
   C'est l'organe suprême de décision du port. Il prend des décisions relatives à la vie de l'entreprise, et est doté des pouvoirs pour agir en toutes circonstances au nom de la société. Il se réunit deux (02) fois l'année en session ordinaire :

- En décembre pour approuver le budget à présenter en conseil des ministres ;
- En avril pour l'approbation du bilan de fin d'exercice ;

Le conseil d'Administration est composé de sept (07) membres dont trois représentants des pays de l'hinterland. Sa composition est la suivante :

- un représentant du Ministère des Infrastructures et des Transports (Président du Conseil d'Administration) ;
- un représentant du Ministre du Commerce et de l'industrie ;

2. **Les observateurs sont** :

- Le Représentant de la COBENAM ;
- Le Représentant de la SOBEMAP ;
- Le Représentant de la l'OCBN.

:

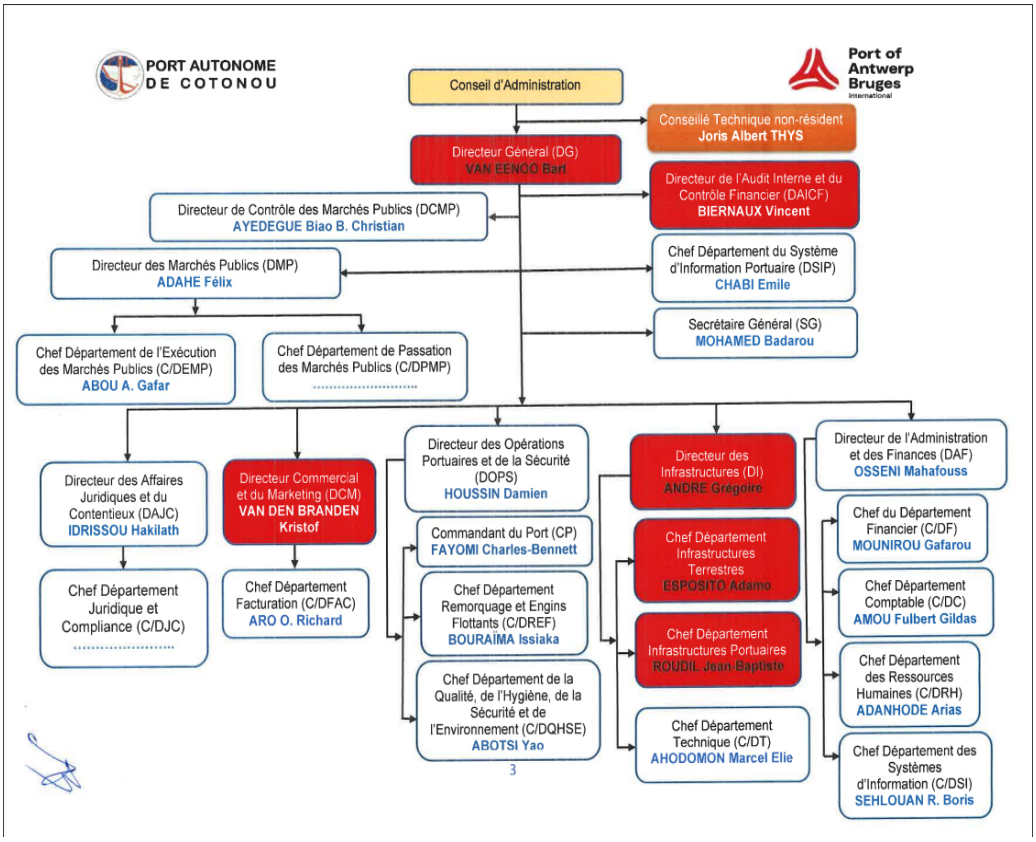


FIGURE 1.1 : Organigramme du Port Autonome de Cotonou (Source : RSSI)

1.1.5 Présentation du département des Systèmes d'Information

Le département des systèmes d'information (DSI) fut appelé Cellule Informatique (CI) qui était la structure qui gouverne toutes les actions liées au système informatique plus précisément au maintien des divers matériels informatiques au sein de Port Autonome de Cotonou. Suite à l'indispensabilité du système informatique au niveau des différents départements et à l'intégration des divers logiciels

de gestion, la Cellule Informatique (CI) a subi des modifications et devient la Direction des Systèmes d'Information et de l'Informatique (DSII) qui est pris en compte par l'organigramme du 19 mars 2008. Dans l'optique de mieux structurer le secteur informatique et comprenant l'ampleur technologique du PAC, avait vu le jour la Direction des Systèmes d'Information et de la Qualité (DSIQ) en mars 2009. Au fil des années, elle devient département des Systèmes d'Information (DSI) jusqu'à nos jours pour donner place au détachement du Service de la Qualité.

1.1.6 Missions des différents secteurs de la DSI

Le département des Systèmes d'Information a pour mission de :

- planifier le développement du système d'information de l'entreprise et en assurer la gouvernance ;
- apporter aux utilisateurs l'aide nécessaire à l'outil informatique ;
- assurer l'acquisition, la mise en place, la sécurité et l'évolution du système d'information ;
- apporter aux utilisateurs l'aide nécessaire à l'outil informatique ;
- garantir la sécurité et l'intégrité des systèmes d'information contre les cybermenaces et les attaques informatiques ;
- assurer la conformité aux normes et réglementations en matière de sécurité informatique.

La Direction des Systèmes d'Information (DSI) dispose de **trrois services** justes après le **secrétariat.**

1. Le service Développement et Projet (SPD). Ce service se charge de la gestion des projets et développement.
2. Le Service Infrastructures et Réseaux (SIR). Il a pour tâche de :
    - Concevoir l'architecture, faire évoluer l'architecture du système, du réseau, de la vidéosurveillance, de la sécurité informatique et de procéder aux configurations nécessaires.
    - Élaborer, mettre en œuvre les politiques et plans de maintenance des ressources matérielles, du réseau informatique et de la vidéo surveillance, ainsi que pour la sécurité informatique
    - Élaborer et mettre en œuvre les stratégies et plans de sauvegarde et de reprise des activités sinistres.
3. Le Service Support et Applications (SSA) Le Service Support et Applications (SSA)
    - Élaborer et mettre en œuvre la politique et maintenance des postes de travail et des logiciels
    - Assurer le bon fonctionnement de l'intranet, de l'internet et des applications ;

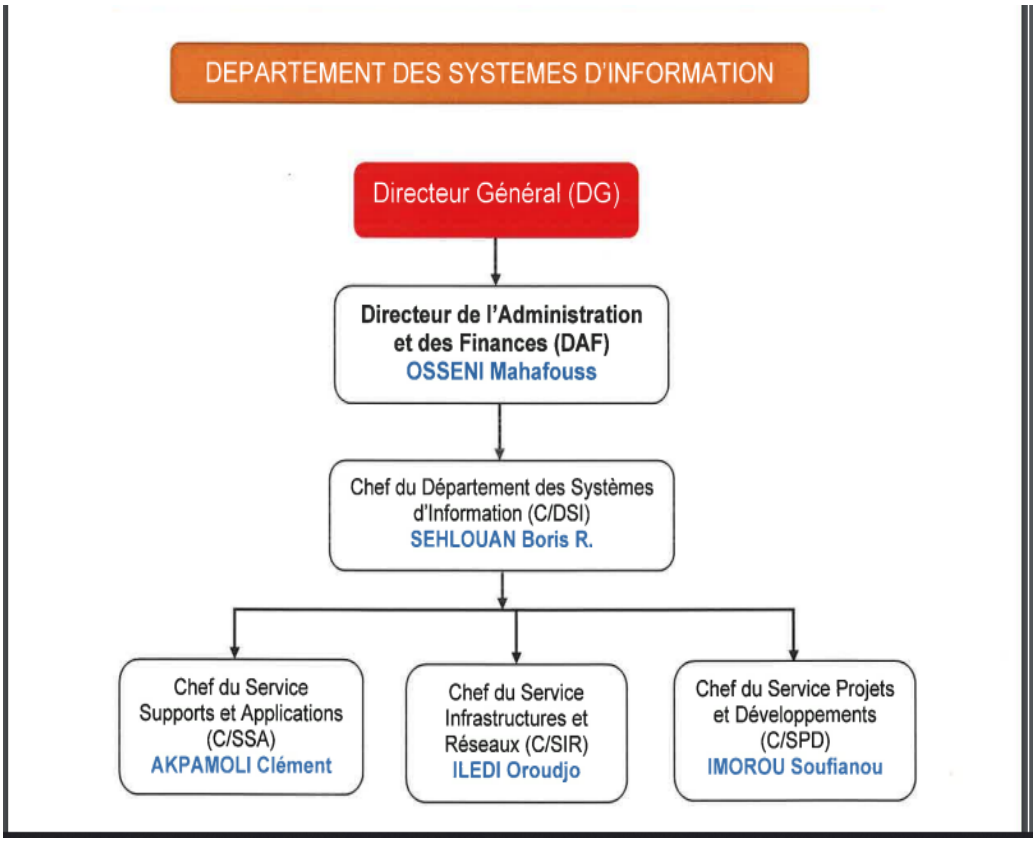


FIGURE 1.2 : Organigramme de la DSI (Source : RSSI)

1.2 - Déroulement du stage

1.2.1 Travaux effectuent et acquis du stage

- **Analyse forensique d'un fichier issu d'une attaque de phishing**
  Nous avons fait une analyse détaillée d'un fichier lié à une attaque de phishing. L'objectif était de regarder attentivement les fichiers et les données récupérées après une attaque de phishing pour comprendre les méthodes utilisées par les pirates et vérifier s'il y a eu des compromissions. Nous avons rassemblé toutes les preuves possibles, comme les emails suspects, les pièces jointes, les liens et toutes les autres données pertinentes. Ensuite, nous avons examiné les détails des fichiers, comme les créateurs et les dates de modification, ainsi que le code source des emails HTML ou des scripts malveillants.
  Ensuite, nous avons identifié et noté les éléments, tels que les adresses IP, les domaines et les empreintes des fichiers, pour pouvoir les utiliser plus tard dans la prévention et la détection d'attaques similaires.

- **Footprinting (Reconnaissance) sur les domaines ifri-uac.bj, uac.bj**
  Nous avons également effectué un travail de reconnaissance, ou footprinting, sur les domaines ifri-uac.bj, uac.bj. Cette activité visait à collecter des informations détaillées sur ces domaines pour identifier les vulnérabilités potentielles et comprendre la structure et les technologies utilisées. Nous avons commencé par une recherche WHOIS pour obtenir des informations sur l'enregistrement des domaines, telles que les noms des propriétaires, les dates de création et d'expiration, ainsi que les serveurs DNS utilisés.

Ensuite, nous avons utilisé des outils comme nslookup, dig, wapiti, maltego et theHarvester pour recueillir des informations sur les enregistrements DNS, les sous-domaines, les adresses IP associées et les adresses email liées aux domaines. L'analyse des en-têtes HTTP des sites web associés nous a permis de découvrir les technologies et les serveurs web utilisés. De plus, une exploration approfondie des sites eux-mêmes a révélé des informations supplémentaires, telles que les structures de répertoires, les scripts actifs et les possibles points d'entrée pour les attaques.

- **Attaque d'ingénierie sociale avec l'outil SEToolkit**
  Enfin, nous avons réalisé une attaque d'ingénierie sociale en utilisant l'outil SEToolkit (Social Engineering Toolkit). Cet outil, disponible sur Kali Linux, permet de créer des attaques de phishing, des fausses pages de connexion et d'autres vecteurs d'ingénierie sociale [18]. Pour mener cette attaque, nous avons sélectionné le type d'attaque dans SEToolkit, comme le clonage d'une page de phishing. Nous avons ensuite configuré les paramètres de l'attaque, y compris le site cible, les messages de phishing personnalisés et les vecteurs de distribution (par exemple, email, médias sociaux). Une fois l'attaque configurée, nous l'avons déployée en envoyant les messages de phishing aux victimes ciblées. Les victimes, croyant interagir avec un site légitime, pouvaient alors divulguer leurs informations de connexion ou autres données sensibles. L'efficacité de cette attaque reposait sur la crédibilité du contenu et notre capacité à inciter les victimes à agir.
  Ces travaux nous ont permis de développer des compétences pratiques et de contribuer activement à la sécurisation des systèmes et des réseaux de l'organisation.

1.2.2 Difficultés rencontrées

Nous avons rencontré des difficultés à établir des relations solides, ce qui a limité notre collaboration et l'utilisation optimale de l'expertise disponible. De plus, des problèmes de connexion fréquents ont perturbé l'accès aux ressources essentielles, retardant notre travail et compliquant la coordination des outils de sécurité. Ces difficultés ont également entravé notre communication avec nos mentors et les membres de l'équipe, rendant difficile la réception de conseils et de feedback opportun.Malgré ces obstacles, nous avons su nous adapter et improviser pour maximiser notre productivité et atteindre nos objectifs de stage.

1.3 - Bilan de notre stage

Notre stage au Port Autonome de Cotonou (PAC) a été une expérience enrichissante qui nous a permis d'acquérir des compétences pratiques et de mettre en pratique nos connaissances théoriques. Nous avons approfondi nos connaissances en matière de sécurité informatique, en comprenant les différentes techniques d'attaque, les mesures de prévention et de détection, ainsi que les meilleures pratiques en matière de gestion des incidents de sécurité grâce au RSSI. Nous avons utilisé kali linux sur nos ordinateurs pour faire tout ce que nous voulons plus précisément les travaux pratiques. Nous avons travaillé en étroite collaboration avec d'autre stagiaire et du personnel, ce qui nous a permis de partager nos idées, de résoudre des problèmes ensemble et de renforcer notre capacité à travailler en équipe dans un environnement professionnel. Nous avons eu l'occasion de mettre en pratique nos

compétences en matière de sécurité informatique en travaillant sur des projets concrets tels que l'analyse des risques, l'investigation numérique, les tests de pénétration et la configuration des systèmes de sécurité. Notre stage en sécurité informatique au (PAC) a été une expérience précieuse qui nous a permis de mettre en pratique nos connaissances et compétences en matière de sécurité informatique. Nous avons contribué à renforcer la sécurité de l'entreprise en identifiant et en résolvant les vulnérabilités, en mettant en place des mesures de sécurité préventives et en sensibilisant le personnel aux bonnes pratiques de sécurité.

Conclusion

Grâce à ce stage, nous avons développé des compétences clés en matière de sécurité informatique, telles que l'analyse des risques, les tests d'intrusion et la gestion des incidents, tout en travaillant en étroite collaboration avec les équipes du RSSI.

Chapitre 2

Étude, analyse et choix de la solution

Introduction

Dans cette étude, nous présentons une architecture de sécurité robuste et évolutive pour le Port Autonome de Cotonou. En s'appuyant sur une solution SIEM Elastic enrichie par un EDR, nous proposons une approche proactive pour détecter et répondre aux menaces, renforçant ainsi la cyberrésilience du domaine portuaire et la protection de ses actifs critiques. Nous détaillerons les choix technologiques et les étapes de mise en œuvre de cette solution.

2.1 - La Sécurité Informatique

2.1.1 Définition

La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés. Autrement dit, qu'elle s'assure que les exigences de sécurité sont respectées dans un environnement

2.1.2 Les objectifs de la Sécurité Informatique

Pour assurer la sécurité d'un système d'information, trois objectifs primordiaux doivent être atteints : la **confidentialité** des données, leur **intégrité** et leur **disponibilité**(souvent désigné par l'acronyme CIA). Ces objectifs sont complétés par des mécanismes d'authentification pour contrôler les accès et de non-répudiation pour garantir la traçabilité des actions.

- **L'intégrité** : garantir que les données soient bien celles que l'on croit être ;
- **La disponibilité** : maintenir le bon fonctionnement du système d'information ;
- **La confidentialité** : rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction ;
- La non-répudiation : garantir qu'une transaction ne peut être niée ;
- L'authentification : assurer que seules les personnes autorisées aient accès aux ressources [9] .



FIGURE 2.1 : Objectifs de la sécurité informatique

2.2 - Les Menaces informatiques

La sécurité informatique protège contre différents types de menaces. On distingue notamment :

- **Failles de sécurité** :
  Les failles de sécurité sont constituées par les défauts d'un logiciel ou de configuration de sécurité, qui fragilisent la sécurité globale du réseau.

- **Logiciels espions** :
  Un logiciel espion peut être téléchargé à partir de sites Web, d'e-mails, de messages instantanés et de connexions directes de partage de fichiers. Par ailleurs, un utilisateur peut, sans le savoir, recevoir un logiciel espion en acceptant un contrat de licence utilisateur final d'un programme informatique.

- **Courrier indésirable** :
  Le courrier indésirable consiste à recevoir des messages non sollicités, la plupart du temps de la publicité, à un grand nombre de destinataires. Le courrier indésirable pose un sérieux problème de sécurité, car il peut être utilisé pour envoyer un e-mail susceptible de contenir des chevaux de Troie, des virus, des vers, des logiciels espions et des attaques ciblées qui visent à obtenir des informations d'identification personnelles et confidentielles.

- **Programmes malveillants** :
  Les programmes malveillants font partie des programmes hostiles, comprenant les virus, les vers et les chevaux de Troie. Ils tentent également d'exploiter les failles existantes des systèmes en s'introduisant de façon aisée et transparente.

- **Attaque XSS** :
  Une attaque XSS, ou**Cross-Site Scripting**, est une technique permettant à un attaquant d'injecter du code malveillant, généralement du code JavaScript, dans des pages Web ou des applications Web. Ce code est ensuite exécuté dans le navigateur des utilisateurs qui visitent la page compromise, ce qui peut entraîner le vol de données sensibles, la prise de contrôle de sessions

utilisateur, ou d'autres actions malveillantes. Les attaques XSS peuvent être classées en trois principales catégories : stockée, réfléchie et basée sur le DOM, chacune ayant des méthodes d'injection et des conséquences spécifiques. Pour se protéger contre les attaques XSS, il est essentiel d'appliquer des pratiques de sécurité telles que la validation des entrées utilisateurs et l'échappement des données avant de les afficher sur une page Web. **Typologie des attaques XSS**

1. **Attaque XSS stockée (Stored XSS)** :
   Les attaques XSS stockées se produisent lorsque du code malveillant est injecté dans une application Web et stocké sur le serveur ou dans une base de données. Ce code est exécuté chaque fois qu'un utilisateur accède à la page affectée, compromettant potentiellement la session utilisateur, volant des cookies ou redirigeant l'utilisateur. Ces attaques sont dangereuses, car elles peuvent affecter un grand nombre d'utilisateurs et sont difficiles à détecter et corriger. Pour se protéger, il est crucial d'implémenter l'échappement des données et la validation des entrés utilisateurs.
2. **Attaque XSS réfléchie (Reflected XSS)** :
   Le XSS réfléchi se produit lorsque du code malveillant est injecté et immédiatement reflété sans stockage sur le serveur, souvent via un lien ou une URL spécialement conçue. Lorsque la page est chargée, le code s'exécute, permettant à l'attaquant de voler des cookies ou de rediriger l'utilisateur vers des sites malveillants.
3. **Attaque XSS basée sur le DOM (DOM-based XSS)** :
   Le XSS basé sur le DOM se produit lorsque du code malveillant est injecté dans le DOM d'une page Web après son chargement. Il se produit lorsque le JavaScript de la page incorpore des entrées non fiables directement dans le DOM sans échapper les caractères spéciaux, entraînant l'exécution du code malveillant et des conséquences similaires au XSS réfléchi [10] .

- **Attaques par injection SQL** :
  Les injections SQL peuvent être classées en plusieurs catégories selon la technique utilisée par l'attaquant et ses objectifs. Voici les principaux types d'injections SQL :

  1. **Injection basée sur l'erreur (Error-Based SQLi)** : L'attaquant analyse les messages d'erreur de l'application pour obtenir des informations sur la structure de la base de données et injecter du code SQL en conséquence.
  2. **Injection basée sur le temps (Time-Based SQLi)** : L'attaquant utilise des requêtes SQL qui mesurent le temps d'exécution pour récupérer des informations de la base de données caractère par caractère
  3. **Injection basée sur l'union (Union-Based SQLi)** :L'attaquant utilise l'opérateur SQL UNION pour combiner des requêtes malveillantes avec la requête d'origine de l'application.
  4. **Injection aveugle (Blind SQLi)** :L'attaquant n'a pas de retour visuel immédiat sur le succès de son injection et doit utiliser des techniques itératives pour extraire des informations de la base de données [11].

2.3 Le monitoring

2.3.1 Définitions

Le monitoring informatique est une des importantes fonctionnalistes d'un SIEM (Security Information and Event Management) qui implique la collecte, l'analyse et la corrélation des données de sécurité provenant de diverses sources pour détecter, analyser et répondre aux incidents de sécurité en temps réel. Cette supervision permet une visibilité complète sur l'infrastructure IT, assurant ainsi la sécurité et la conformité.

2.3.2 Objectifs du monitoring

Le monitoring informatique permet d'anticiper les défaillances et donc d'éviter les pannes en étant alerté des dysfonctionnements. La supervision a pour objectif la surveillance du système d'information. Elle permet à l'administrateur d'être au courant en temps réel de l'état du système informatique et d'agir en cas d'anomalie. C'est donc pour répondre aux préoccupations suivantes :
- **Technique** : surveillance du réseau et des systèmes (elle permet d'avoir un œil sur la santé du réseau en tenant compte des éléments qui peuvent nuire à sa performance tels que les nouvelles charges et la latence), détecter les indicateurs de compromission ;
- **Applicative** : surveillance des applications et des processus métiers. (Elle permet de connaître tout ce qui est comme logiciels ou programme qui tourne en temps réel sur les points de terminaisons ou sur le réseau) [12].

2.3.3 Les types de Monitoring qu'un SIEM possède

Les principaux types de monitoring que les systèmes de détection et de réponse possèdent sont entre autres :

- **Monitoring des journaux d'événements** : Ce monitoring surveille les journaux d'événements générés par les systèmes, applications et équipements réseau. Le SIEM collecte et analyse ces journaux pour détecter les activités suspectes ou malveillantes, telles que les connexions réseau, tentatives d'accès et erreurs système.
- **Monitoring du trafic réseau** : Ce monitoring analyse le trafic réseau entrant et sortant pour détecter les schémas de communication inhabituels, tentatives d'intrusion et attaques . Le SIEM identifie les comportements anormaux et les signatures d'attaques connues en temps réel.
- **Monitoring applicatif et Services** : Ce type de supervision informatique est dédié à la surveillance de vos applications, logiciel métier et services fonctionnels. Cette prestation vous assure du bon fonctionnement quotidien des applicatifs et services nécessaires à la bonne marche de votre structure. L'ensemble des collaborateurs est ainsi en mesure d'accomplir en toute sérénité la mission qui lui est confiée.
- **Monitoring des comportements utilisateur** : Ce monitoring se concentre sur les activités des utilisateurs sur le réseau et les systèmes informatiques. Le SIEM détecte les activités anormales,

comme les tentatives d'accès non autorisées et les changements de privilèges, permettant de repérer les utilisateurs malveillants ou compromis.

- **Reporting global**
  Avec un contrat de monitoring informatique, plus de 95% des dysfonctionnements potentiels sont identifiés et corrigés avant que votre activité ne soit impactée. C'est la raison pour laquelle le rapport de monitoring qui vous est transmis affiche souvent que tous les indicateurs de sécurités de votre système informatique sont au vert. Dans le cas contraire, nous déclenchons une intervention dans le cadre de votre contrat d'infogérance d'exploitation afin de revenir dans le mode de fonctionnement normal.

2.3.4 Les avantages du monitoring

la mise en place d'une supervision apporte à l'entreprise de nombreux bénéfices pour son activité :
- Une réduction des coûts : tout risque anticipé est immédiatement constaté avec des seuils d'alerte, le temps de réaction est réduit et permet d'éviter le dysfonctionnement. L'impact financier est limité au minimum.
- Une amélioration du pilotage : vous mesurez l'activité, vous maîtrisez et comprenez instantanément la situation des systèmes et infrastructures, avec une cartographie dynamique, les moyens sont sous contrôle. Vous gagnez du temps avec une analyse de la situation permanente et immédiate et facilitez le travail des administrateurs systèmes et réseaux grâce aux fonctions d'inventaire des outils de supervision.
- Une anticipation plus forte : le reporting met en évidence l'évolution des mesures et des dégradations potentielles. Avant que les seuils d'alerte ne soient atteints, vous êtes en capacité de prendre les meilleures décisions pour adapter la capacité du système d'information aux besoins de l'entreprise. Surveiller et détecter au plus tôt une évolution inquiétante, une indisponibilité ou défaillance d'un composant concourt à améliorer la qualité, répond aux objectifs de la DSI et impacte positivement et directement le business de l'entreprise dans son ensemble [12].

2.4 Les IDS (Intrusion Detection System)

2.4.1 Clarification conceptuelle

La détection d'intrusion est le processus qui consiste à surveiller les événements qui se produisent sur votre réseau et à les analyser pour détecter les signes d'éventuels incidents, violations ou menaces imminentes à vos stratégies de sécurité. Il existe deux principaux types d'IDS, nous avons les HIDS (Host based Intrusion Detection System) et NIDS (Network Host Based Intrusion Detection System).

- **Les HIDS (Host based Intrusion Detection System)** :
  Ils analysent le fonctionnement et l'état des machines sur lesquels ils sont installés afin de détecter les attaques en se basant sur des daemons. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées. Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux (tels que les attaques de type DOS) [13].

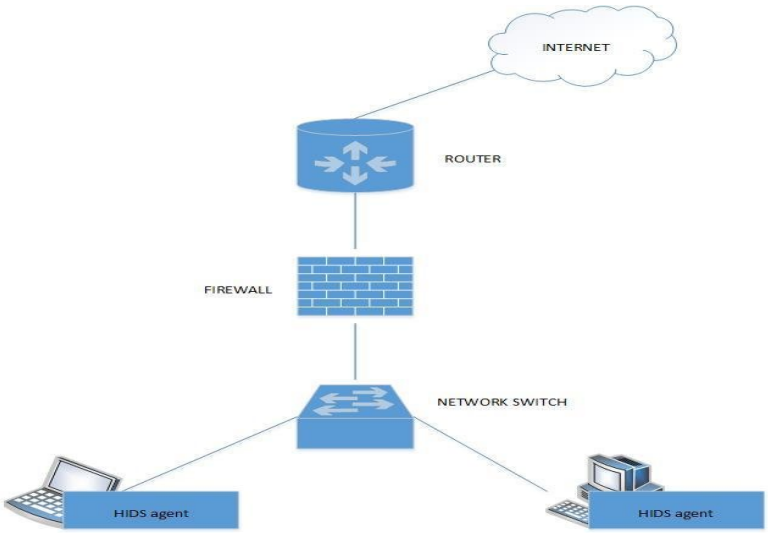


FIGURE 2.2 : HIDS [13].

- **Les NIDS (Network Host Based Intrusion Detection System)**
  Ils analysent en temps réel les trafics entrant et sortant du réseau qu'ils aspirent à l'aide d'une sonde afin d'y déceler les attaques. Ensuite, les paquets sont décortiqués puis analysés. En cas, de détection d'intrusion, des alertes peuvent être envoyées [13].

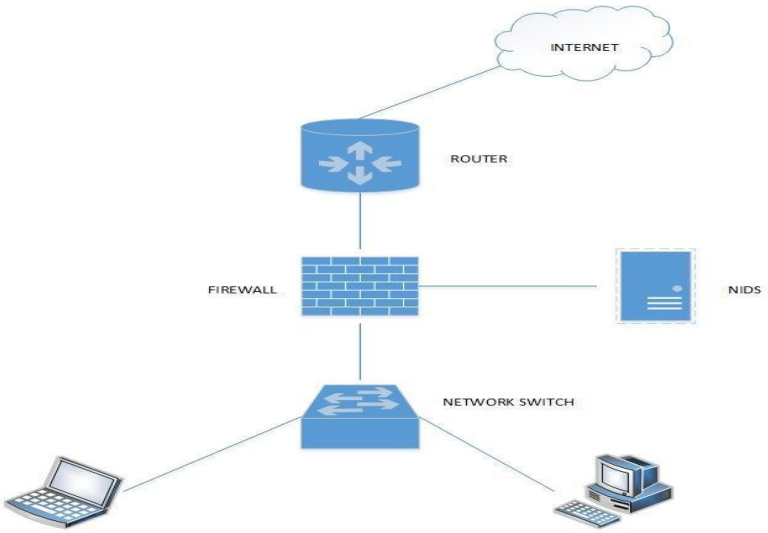


FIGURE 2.3 : NIDS [13].

2.4.2 Fonctionnement des IDS

Les IDS disposent de deux approches différentes, afin de déceler les intrusions :

- Systèmes de détection d'intrusion par signatures : Reposent sur des bibliothèques de description des attaques (appelées signatures).En effet, ils se basent sur un ensemble de signatures qui représentent chacune le profil d'une attaque (Une attaque par déni de service, exemple). Cette approche consiste à rechercher dans l'activité de l'élément surveillé (un flux réseau) les empreintes d'attaques connues, à l'instar de l'antivirus.
- Systèmes de détection d'intrusion par anomalies ou Les IDS comportementaux : Les IDS com-

portementaux ont pour principale fonction la détection d'anomalie. Leur déploiement nécessite une phase d'apprentissage pendant laquelle l'outil va apprendre le comportement "normal" des flux applicatifs présents sur son réseau. Ainsi, chaque flux et son comportement habituel doivent être déclarés ; l'IDS se chargera d'émettre une alarme, si un flux anormal est détecté.

2.4.3 Avantages des IDS et quelques exemples d'outils

Les systèmes de détection d'intrusion ont certains avantages : l'impact d'une attaque peut être constaté et permet une meilleure réaction, des attaques dans un trafic chiffré peuvent être détectées, les activités sur l'hôte peuvent être observées avec précision. Il existe plusieurs Intrusions Détection Système, il y en a des Open Source et d'autres qui sont propriétaires.Citons-en quelques Opens Source présents sur le marché :

2.4.3.1 Systèmes de détection d'intrusion réseaux (NIDS)

- **Snort** :
  SNORT est un puissant système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) Open Source qui fournit une analyse du trafic réseau en temps réel et une journalisation des paquets de données. SNORT utilise un langage basé sur des règles qui combinent des méthodes d'inspection des anomalies, des protocoles et des signatures pour détecter les activités potentiellement malveillantes.

- **Bro ou zeek** :
  C'est un IDS qui a les mêmes caractéristiques que Snort mais intègre une fonctionnalité d'analyse de flux

- **Suricata** :
  C'est un IDS/IPS basé sur des signatures qui sont distribuées sous licence.

2.4.3.2 Systèmes de détection d'intrusion hôtes(HIDS)

- **Tripwire** :
  C'est un système de détection d'intrusion Linux (IDS) populaire qui s'exécute sur les systèmes afin de détecter si des modifications non autorisées du système de fichiers se sont produites au fil du temps.

- **Chkrootkit** :
  C'est un logiciel libre sous licence GNU GPL permettant de détecter si un système UNIX n'a pas été compromis par un rootkit.

- **OSSEC** :
  C'est un système de détection d'intrusion basé sur l'hôte (HIDS) gratuit et open source. Il effectue l'analyse des journaux, la vérification de l'intégrité, la surveillance du registre, Windowsla détection des rootkits, les alertes temporelles et la réponse active. Il fournit une détection d'intrusion pour la plupart des systèmes d'exploitation, y compris Linux, Open, BSD, FreeBSD, OS, Solaris et Windows. L'OSSEC dispose d'une architecture centralisée et multiplateforme permettant de surveiller et de gérer facilement plusieurs systèmes [19].

Ceci n'est pas bien entendu une liste exhaustive des Systèmes de détection d'intrusion, juste quelques exemples.

2.5 Généralité sur les Systèmes automatisés de détection, d'analyse et de réponse aux incidents de sécurité

2.5.1 Définition SIEM

SIEM ou Gestion de l'information des événements de sécurité est un système centralisé qui offre une visibilité totale sur l'activité du réseau, Il assimile et parcourt un grand volume de données en quelques secondes pour détecter et signaler les comportements inhabituels. Il génère ensuite des alertes de sécurité lorsqu'il identifie des problèmes potentiels et il nous permet ainsi de réagir aux menaces en temps réel et il aide à la surveillance et la conformité de la sécurité et de l'activité des utilisateurs.

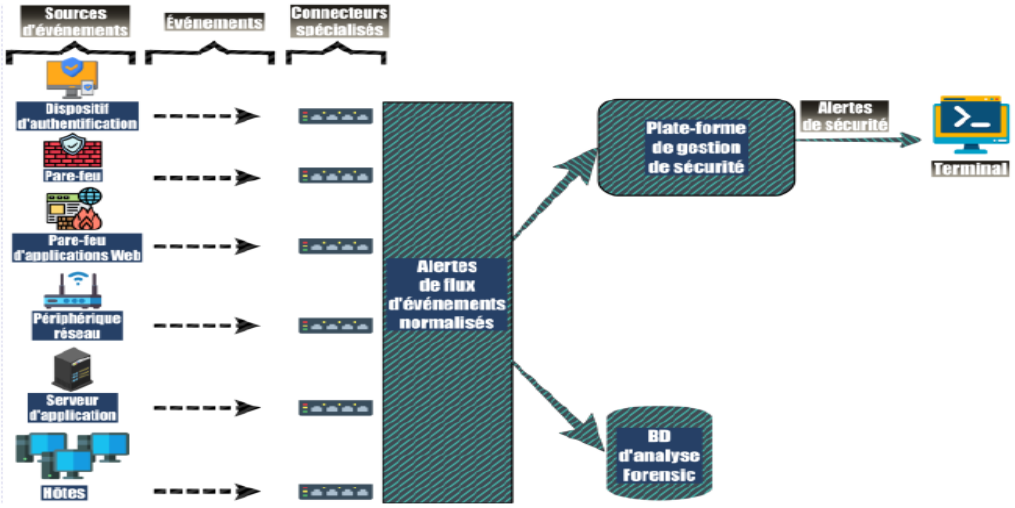


FIGURE 2.4 : Architecture de SIEM

Au début, il y avait relativement peu d'outils de sécurité informatique, notamment des pare-feux pour la protection du périmètre du réseau d'entreprise, les systèmes de détection des intrusions (IDS) et les systèmes antivirus pour la surveillance des hôtes. Chacun de ces systèmes est livré avec sa propre interface utilisateur spécifique au fournisseur. Au fur et à mesure que ces outils sont devenus plus largement utilisés et que de plus en plus d'outils sont apparus, deux problèmes se sont posés :
Premièrement, il y avait trop d'interfaces utilisateur à gérer.
Deuxièmement, il n'y avait pas d'outils pour corréler les événements entre les différents outils de sécurité.
Le SIEM il est composé de deux concepts qui sont : SEM (gestion des événements de sécurité) et le SIM (gestion des informations de sécurité).

- **SIM** : Il traite les données des journaux et des événements des dispositifs de sécurité,, systèmes et applications en temps réel pour assurer la sécurité, la surveillance, la corrélation des

événements et les réponses aux incidents. SIEM soutient les activités de surveillance des menaces externes et internes de l'organisation de la sécurité informatique et améliore la gestion des incidents.

- **SIM** : Le SIM (Security Information Management) assure la gestion des journaux, la collecte, la création de rapports et l'analyse des données provenant des systèmes hôtes, des applications, des périphériques réseau et de sécurité. Il supporte les rapports de conformité réglementaire, la gestion des menaces internes, et surveille l'accès aux ressources. Le SIM traite également les activités de surveillance des utilisateurs privilégiés, les besoins en rapports d'audit interne et les exigences de conformité [14].

SIEM = **SIM** + **SEM**

	Gestion des informations de sécurité (SIM)	Gestion des événements de sécurité (SEM)	Gestion de l'information et des événements de sécurité (SIEM)
Aperçu	Collecte et analyse des données relatives à la sécurité à partir des logs.	Analyse, visualisation et réponse aux incidents en temps réel.	SIEM, comme son nom l'indique, combine les capacités SIM et SEM.
Caractéristiques	Facilité de déploiement. Capacités de gestion des journaux.	Plus complexe à déployer. Supérieur dans la surveillance en temps réel.	Plus complexe à déployer. Fonctionnalité complète.
Exemples d'outils	OSSIM	Sentinelle NetIQ	SolarWinds

FIGURE 2.5 : La différence entre SIEM, SIM et SEM

2.5.2 Fonctionnement des SIEM

Examinons de plus près les principales fonctionnalités des solutions SIEM :

- **Agrégation** : Rassemblement de logs similaires pour simplifier l'analyse, réduire le stockage et faciliter la corrélation. Nécessite une configuration soignée pour éviter la perte d'informations.
- **Corrélation** : Analyse d'événements pour établir des liens et générer des alertes. Utilise des règles spécifiques et des informations sur l'infrastructure. Permet une détection proactive des incidents de sécurité.
- **Les rapports** : Les rapports générés contiennent à la fois un résumé des alertes et un aperçu de la sécurité du système à instant T. SIEM peut également créer et générer des tableaux de bord et des rapports. Ainsi, différents acteurs, administrateurs, utilisateurs peuvent connaître le SI (nombre d'attaques, nombre d'alertes par jour, etc.).
- **Tableaux de bord** : Les outils SIEM prennent les données des événements et les transforment en d'événements et les transforment en graphiques informatifs pour aider à voir les l'activité qui ne forme pas un modèle standard

- **Alertes** Le SIEM fournit l'analyse automatisée des événements corrélés et la production d'alertes, afin de notifier les destinataires de problèmes immédiats. Le schéma ci-dessous (figure) représente les fonctionnements d'un SIEM.

2.6 Elastic Security et EDR (Endpoint Detection and Response)

2.6.1 Elastic Security

ELastic Security : st une solution de sécurité complète, basée sur la plateforme Elastic Search, qui offre une vue unifiée de votre environnement informatique. En collectant et en analysant des données provenant de multiples sources, elle permet aux équipes de sécurité de détecter, d'analyser et de répondre rapidement aux menaces [21].
- Les principaux avantages d'Elastic Security

- **Vue unifiée** : Elastic Security rassemble toutes les données de sécurité dans une seule plateforme, ce qui facilite l'analyse et la corrélation des incidents.
- **Détection proactive** : Grâce à des algorithmes d'apprentissage automatique, Elastic Security peut détecter des menaces avancées et des comportements suspects que les solutions traditionnelles pourraient manquer.
- **Réponse rapide** : a plateforme permet aux équipes de sécurité d'agir rapidement en fournissant des informations détaillées sur les incidents et en automatisant certaines tâches.
- **Économies de coûts** :En réduisant le temps consacré aux enquêtes manuelles et en améliorant l'efficacité des équipes de sécurité, Elastic Security permet de réaliser des économies significatives.
- **Extensibilité** : Elastic Security est hautement personnalisable et s'adapte à l'évolution de vos besoins en matière de sécurité.

2.6.2 EDR (Endpoint Detection and Response

EDR (Endpoint Detection and Response) est une solution de sécurité qui se concentre sur la protection des terminaux (ordinateurs, serveurs, etc.). Lorsqu'elle est couplée à Elastic Security, elle offre des avantages supplémentaires :

- **Protection en temps réel** : L'EDR d'Elastic Security surveille en permanence les activités sur les terminaux pour détecter les comportements malveillants.
- **Investigation approfondie** : En combinant les données de l'EDR avec celles d'autres sources, Elastic Security permet d'effectuer des investigations plus complètes et de remonter à la source des attaques.
- **Automatisation des réponses** : Les actions de remédiation peuvent être automatisées, ce qui accélère la réponse aux incidents.

2.7 Quelques solutions open sources

Plusieurs outils open source existent, bien qu'ils puissent nécessiter une configuration approfondie ou des systèmes supplémentaires pour être pleinement opérationnels. Parmi ces outils, on trouve :

- **Wazuh** : Une solution de surveillance de sécurité open source adaptée aux entreprises, offrant la détection des menaces, la surveillance de l'intégrité, la réponse aux incidents et la conformité.
- **TheHive Cortex** :Une plateforme gratuite et open source de réponse aux incidents, intégrée à MISP, conçue pour faciliter le travail du SOC, CSIRT, CERT et autres professionnels de la sécurité pour enquêter et réagir rapidement aux incidents.
- **Graylog** :Une plateforme de gestion des journaux open source qui collecte, indexe et analyse les données en temps réel. Elle permet la recherche en temps réel, propose des tableaux de bord personnalisables, des alertes et notifications, ainsi que des règles de détection des menaces pour transformer la plateforme en un SIEM efficace.
- **Elastic Endpoint Security** : Bien que partiellement open-source, Elastic Endpoint Security est une solution EDR (Endpoint Detection and Response) puissante. Elle offre une visibilité approfondie sur les activités des endpoints, une détection proactive des menaces et des capacités d'investigation avancées.

2.8 Comparaison de quelques solutions open source

Le tableau [22] ci-après fait part d'une étude comparative entre les logiciels SIEM abordés précédemment : Vu que nous choisissons une solution gratuite open source, il sera inutile de comparer les solutions propriétaires existantes à une solution open source.

TABLE 2.1 : Comparaison des solutions de sécurité

Caractéristiques	Wazuh	TheHive Cortex	Graylog	Elastic Endpoint Security
Fonctionnalités principales	Surveillance de la sécurité, détection des menaces, réponse aux incidents, conformité	Réponse aux incidents, intégration avec MISP	Gestion des journaux, SIEM	EDR, détection des menaces, réponse aux incidents, investigation
Open-source	Oui	Oui	Oui	Partiellement (base Elastic open source, fonctionnalités avancées payantes)
Flexibilité	Haute	Haute	Haute	Haute
Intégration	MISP (Malware Information Sharing Platform)	MISP (Malware Information Sharing Platform)	Variée	Suite Elastic, SIEM, autres outils de sécurité
Détection des menaces	Basée sur des règles et des signatures	Basée sur des règles et des corrélations	Basée sur des règles et des analyses	Basée sur le machine learning et l'analyse comportementale
Réponse aux incidents	Basée sur le machine learning et l'analyse comportementale	Manuelle et automatisable	Manuelle	Automatique et manuelle
Visibilité des endpoints	Limitée	Non spécifique	Non spécifique	Excellente (EDR)
Coût	Gratuit	Gratuit	Gratuit	Gratuit (base), payant (fonctionnalités avancées)

Conclusion

La solution Elastic-EDR peut permettre de surveiller et protéger de manière efficace le SI d'une entreprise contre des menaces évoluées, mais ne reste pas l'outil magique pour un client qui devra prévoir les moyens humains, techniques et financiers pour pouvoir opérer la solution.

Chapitre 3

Déploiement et mise en place de la solution

Introduction

Pour renforcer la sécurité de nos systèmes d'information et faire face aux menaces cybernétiques toujours plus sophistiquées, nous avons choisi d'implémenter une solution SIEM basée sur le stack ELK, complétée par une solution EDR. Cette combinaison nous permettra de bénéficier d'une visibilité accrue sur l'ensemble de notre infrastructure, de détecter les menaces de manière proactive et de répondre rapidement aux incidents. En nous appuyant sur les capacités avancées de Elastic Security, reconnue par Forrester comme un acteur majeur du marché, nous visons à améliorer significativement notre posture de sécurité.

3.1 - Présenation de la Stack ELK

- **Elasticsearch** : C'est un moteur de recherche et d'analyse distribué, conçu pour gérer de grandes quantités de données en temps réel. Il permet de stocker, rechercher et analyser des données de manière rapide et efficace, offrant des capacités avancées d'indexation et de requêtage.
- **Kibana** : C'est une interface de visualisation qui permet aux utilisateurs d'interagir avec les données stockées dans Elasticsearch. Kibana propose des outils pour créer des tableaux de bord, visualiser des tendances, effectuer des recherches et générer des rapports, facilitant ainsi l'analyse des données
- **Logstash** : Cet outil est responsable de la collecte, de la transformation et de l'envoi des données vers Elasticsearch. Il peut ingérer des données de diverses sources (logs, métriques, etc.), les traiter en appliquant des filtres et les formater avant de les envoyer à Elasticsearch pour stockage et analyse [15].

3.1.1 EDR

En plus de détecter les menaces, l'EDR offre une gamme de fonctionnalités complémentaires. Il permet de collecter et d'analyser de vastes quantités de données sur les événements survenus sur les

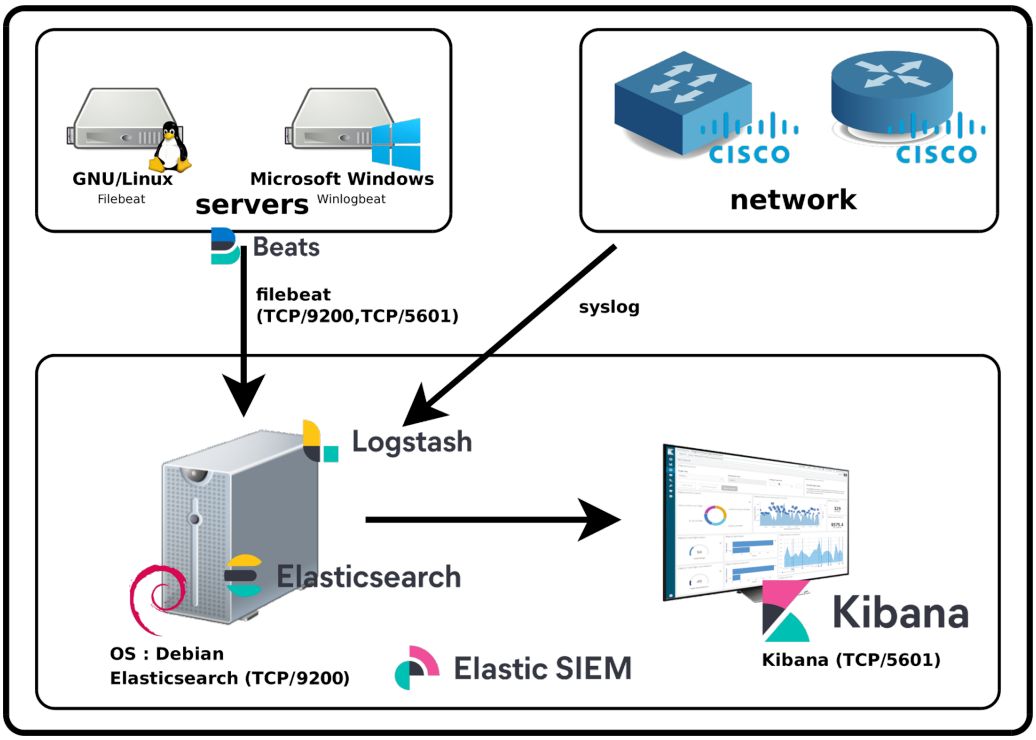


FIGURE 3.1 : Architecture SIEM de la Stack ELK

terminaux, ce qui facilite les investigations en cas d'incident. De plus, l'EDR est souvent intégré à d'autres outils de sécurité, tels que les SIEM, pour offrir une vision globale de l'environnement de sécurité. Grâce à son approche proactive et à ses capacités d'analyse avancées, l'EDR est devenu un élément indispensable de toute stratégie de cybersécurité moderne.

3.1.2 Diffence entre XDR et EDR

TABLE 3.1 : Comparaison entre EDR et XDR

Caractéristique	EDR (Endpoint Detection and Response)	XDR (Extended Detection and Response)
Portée	Endpoints (ordinateurs, serveurs)	Endpoints + réseau, cloud, applications, IoT
Données collectées	Données des endpoints	Données de l'ensemble de l'infrastructure
Réponse	Automatisée sur les endpoints	Automatisée sur toutes la pile de sécurité
Intégration	Souvent intégrée à un SIEM	Souvent intégré à un SIEM et à des outils de sécurité complémentaire

3.2 - Nouvelle Architecture du réseau

Le réseau sur lequel notre solution va être implémentée et constituée d'un pare-feu pour filtrer les paquets depuis internet, de plusieurs switches interconnectant les différents serveurs du réseau local,

dont le Serveur Ubuntu sur lequel notre solution est installée. Le réseau inclut également des postes clients qui accèdent au réseau via la Switch d'Accès, des serveurs en production connectés via les Switch de Distribution, et une DMZ hébergeant des serveurs accessibles publiquement pour des raisons de sécurité. Le schéma suivant illustre notre environnement de travail où nous avons mis en place notre solution SIEM Open-source basé sur la Stack ELK

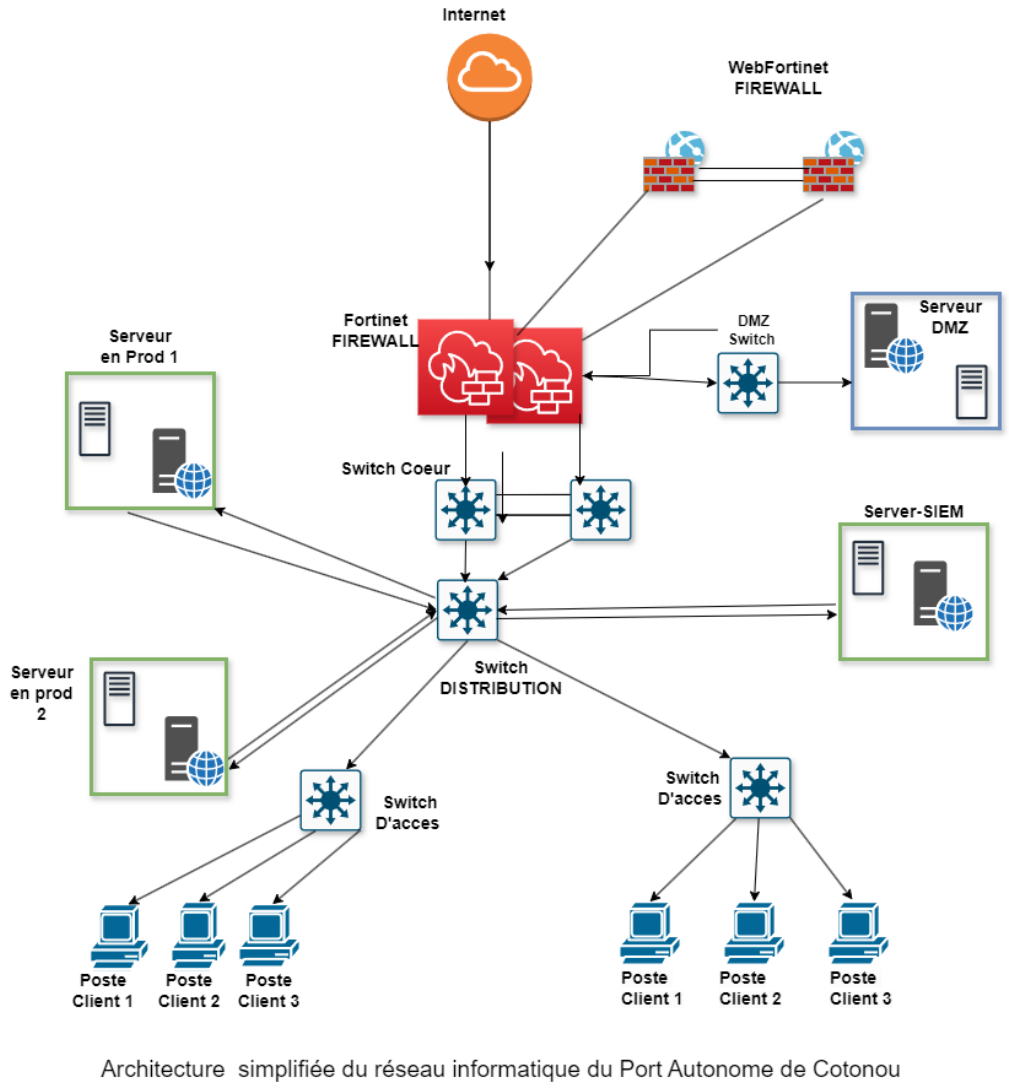


FIGURE 3.2 : Architecture Simplifié du Port Autonome de Cotonou (PAC)

Préparation de l'environnement de travail AWS pour notre solution SIEMS

Dans le cadre de notre projet, j'ai déployé une instance EC2 sur AWS pour mettre en place une solution SIEM basée sur la stack ELK. et une autre instance EC2 pour la mise en place de windows server 2016 ?

- **Instance Ubuntu 24.02 LTS** : Cette instance, dotée de ressources plus importantes (8 Go de RAM et 4 processeurs), est dédiée à l'hébergement de notre solution SIEM. Le choix d'Ubuntu 24.02 LTS nous permet de bénéficier des dernières mises à jour de sécurité et des fonctionnalités les plus récentes, essentielles pour une solution SIEM performante.

- **Instance Windows Server 2016** : Cette instance, avec ses 2 Go de RAM et 2 processeurs, est configurée pour répondre aux besoins spécifiques de notre infrastructure. Elle héberge des services Windows complémentaires, assurant ainsi une intégration fluide entre nos systèmes Windows et Linux.

3.3 Mise en œuvre de la solution SIEM

3.3.1 Configuration de l'environnemenet sur aws

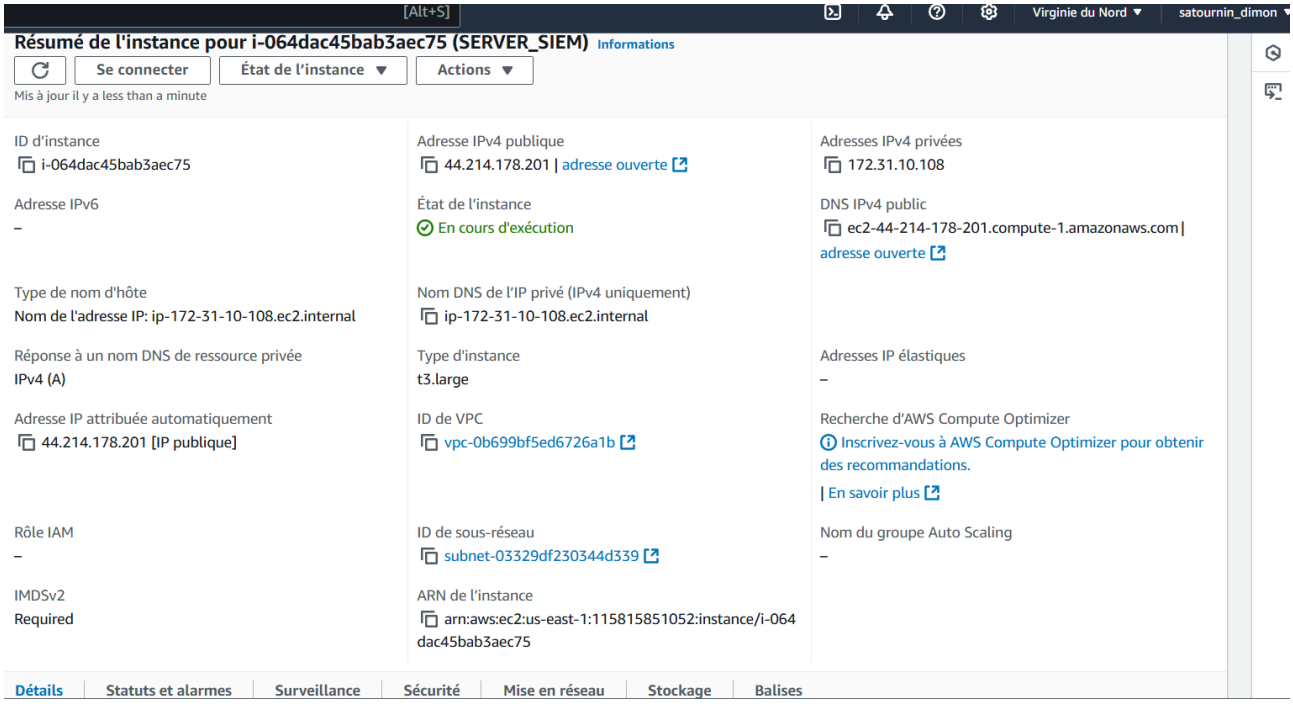


FIGURE 3.3 : Configuration de l'environnement sur aws

3.3.2 Justification du déploiement de deux instances sur AWS

Le choix de déployer deux instances sur AWS repose sur la nécessité de surmonter les limitations des infrastructures matérielles locales. En raison du manque de moyens matériels et de ressources physiques, nous avons opté pour une solution virtualisée, permettant ainsi de garantir une surveillance centralisée et une gestion efficace de notre solution SIEM.

- **Instance Ubuntu en mode "All-in-One"** : La première instance, déployée sous Ubuntu en mode "All-in-One", héberge l'intégralité de notre solution SIEM. Ce mode de déploiement permet d'installer à la fois le serveur SIEM et tous les services associés au sein d'une même instance virtuelle. Cette approche est choisie en raison de l'absence d'infrastructure physique suffisante. L'instance Ubuntu centralise la collecte et l'analyse des événements de sécurité provenant de l'ensemble des machines surveillées. Elle offre ainsi une vue unifiée sur les activités des systèmes, tant pour la machine elle-même que pour les serveurs distants.

- **Instance Windows Server 2016** : héberge les services et applications à surveiller, avec l'agent de collecte **Winlogbeat** installé, qui récupère les journaux d'événements (logs) de cette instance et les envoie à l'instance Ubuntu abritant la solution SIEM. Le choix de Windows Server 2016 repose sur la nécessité de collecter les logs spécifiques des services et applications Windows, qui représentent une part essentielle des données à analyser dans le cadre de la surveillance de sécurité avec le SIEM.

3.3.3 Installation de la Stack ELK sur Ubuntu 24.02

- **Installer apt-transport-https et les paquets nécessaires :**
  apt update && apt-get install apt-transport-https gnupg curl wget
- **Importer la clé PGP Elasticsearch :**
  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg –dearmor -o /usr/share/keyrings/ela
  keyring.gpg
- **Ajouter le dépot elastic :**
  echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packag
  stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list
- **Installer Elasticsearch et noter le mot de passe super-utilisateur ou le changer :**
  apt update && apt-get install elasticsearch

```
root@ip-172-31-0-214:/etc/kibana# cd
root@ip-172-31-0-214:~# cd /usr/share/elasticsearch/bin/
root@ip-172-31-0-214:/usr/share/elasticsearch/bin# ./elasticsearch-reset-password -u elastic -i interactive
This tool will reset the password of the [elastic] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Re-enter password for [elastic]:
Password for the [elastic] user successfully reset.
root@ip-172-31-0-214:/usr/share/elasticsearch/bin# ./elasticsearch-reset-password -u kibana -i interactive
This tool will reset the password of the [kibana] user.
You will be prompted to enter the password.
Please confirm that you would like to continue [y/N]y


Enter password for [kibana]:
Re-enter password for [kibana]:
Password for the [kibana] user successfully reset.
root@ip-172-31-0-214:/usr/share/elasticsearch/bin#
```

- **Installer Kibana**
  apt update && apt-get install kibana
- Éditer le fichier **/etc/elasticsearch/elasticsearch.yml** pour paramétrer l'interface d'écoute
- **Vérifier l'état du service d'elasticsearch**
- Éditer le fichier **/etc/kibana/kibana.yml** pour paramétrer l'adresse d'écoute sur «toutes les adresses»
- **Démarrer le service et Créer le jeton d'inscription**
  systemctl start kibana.service
  /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

```
root@ip-172-31-0-214:/etc/elasticsearch# ls
certs                           elasticsearch.keystore  jvm.options    log4j2.properties  roles.yml  users_roles
elasticsearch-plugins.example.yml  elasticsearch.yml       jvm.options.d  role_mapping.yml   users
root@ip-172-31-0-214:/etc/elasticsearch# nano elasticsearch.yml
root@ip-172-31-0-214:/etc/elasticsearch# root@ip-172-31-0-214:/etc/elasticsearch# vim
root@ip-172-31-0-214:/etc/elasticsearch# root@ip-172-31-0-214:/etc/elasticsearch#
root@ip-172-31-0-214:/etc/elasticsearch# systemctl start elasticsearch.service
root@ip-172-31-0-214:/etc/elasticsearch# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; preset: enabled)
     Active: active (running) since Tue 2024-10-15 09:32:17 UTC; 43s ago
       Docs: https://www.elastic.co
   Main PID: 2632 (java)
      Tasks: 91 (limit: 9367)
     Memory: 4.3G (peak: 4.3G)
        CPU: 1min 9.614s
     CGroup: /system.slice/elasticsearch.service
             ├─2632 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearc
             ├─2690 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -Djava.secu
             └─2710 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Oct 15 09:31:44 ip-172-31-0-214 systemd[1]: Starting elasticsearch.service - Elasticsearch...
Oct 15 09:31:50 ip-172-31-0-214 systemd-entrypoint[2632]: Oct 15, 2024 9:31:50 AM sun.util.locale.provider.LocaleProviderAdapter <clinit>
Oct 15 09:31:50 ip-172-31-0-214 systemd-entrypoint[2632]: WARNING: COMPAT locale provider will be removed in a future release
Oct 15 09:32:17 ip-172-31-0-214 systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)
```

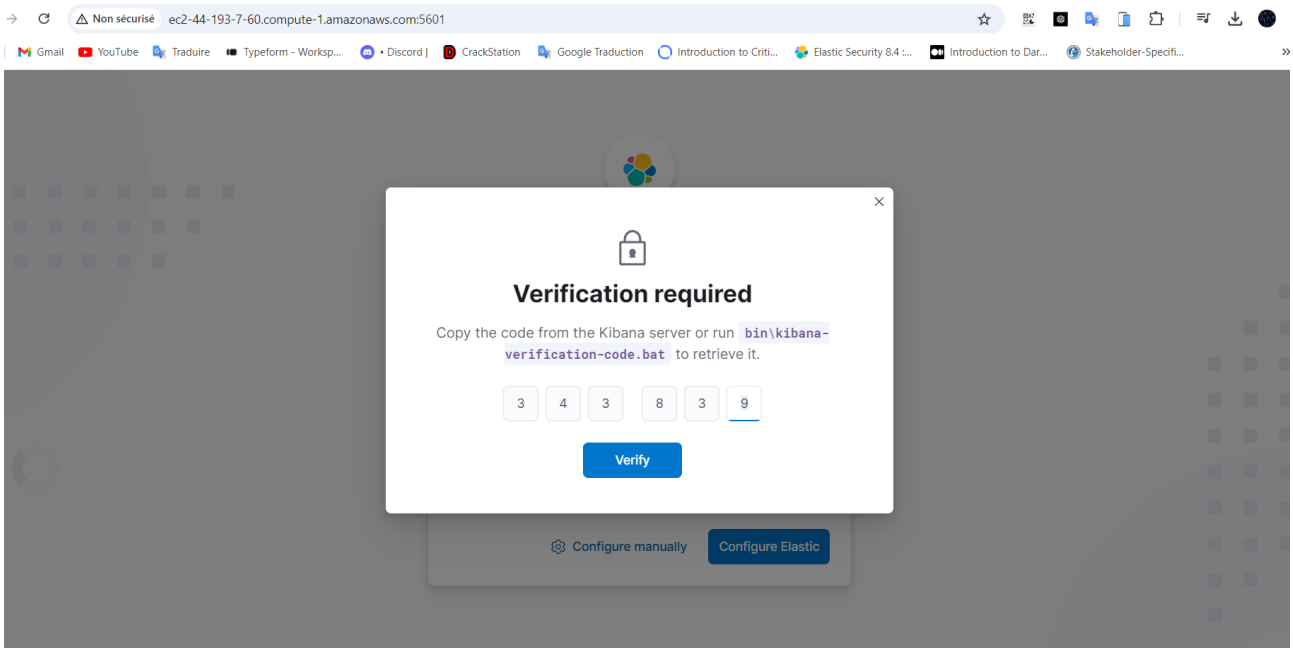


FIGURE 3.4 : Configuration de la suite ELK

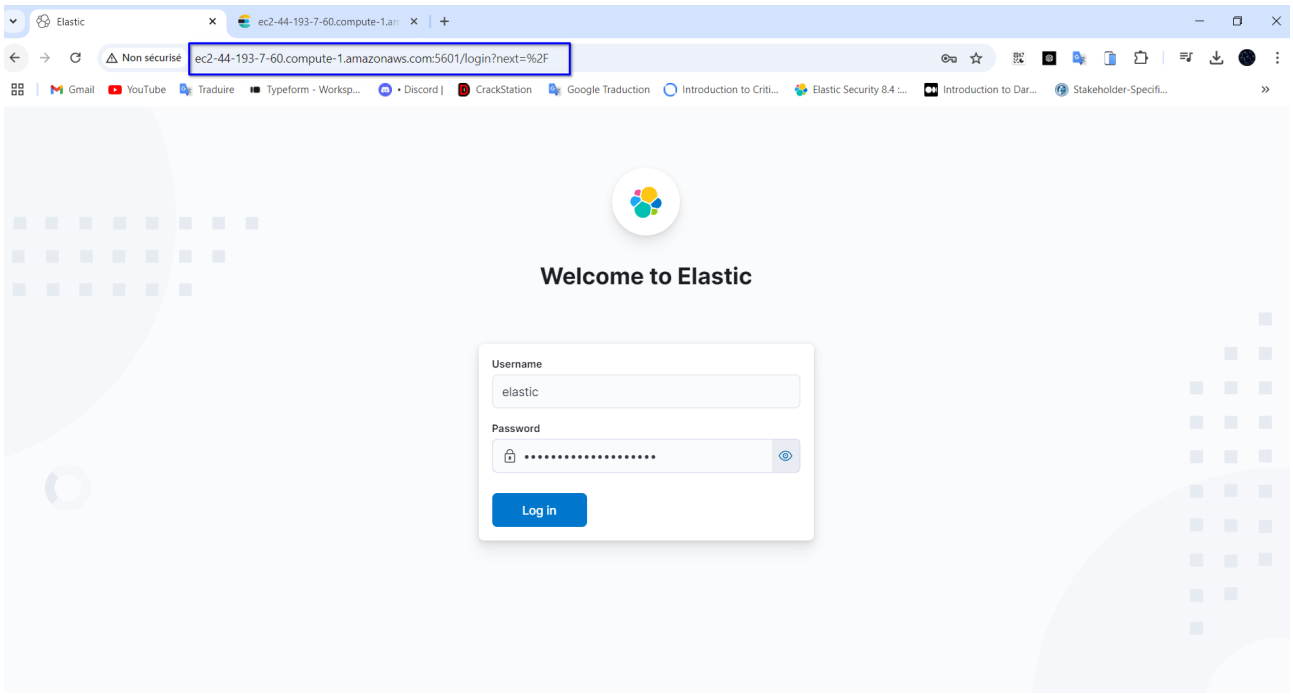


FIGURE 3.5 : Configuration de la suite ELK

– Activer les démarrages automatiques des services installés.

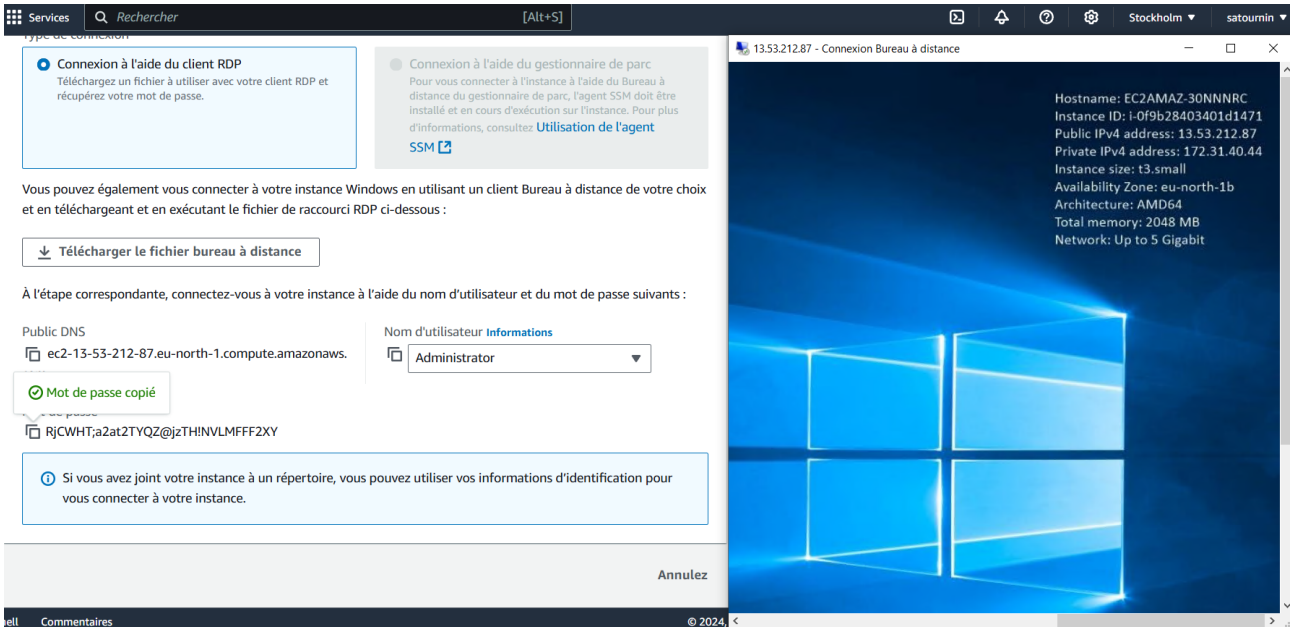


FIGURE 3.6 : Configuration de l'environnement Windows serveur 2016

3.3.4 Sécuriser Kibana

Une des grosses améliorations de la version 8 est qu'Elasticsearch est maintenant sécurisé lors de l'installation par défaut afin de chiffrer ses communications.

3.3.5 Procédure détaillée pour sécuriser Kibana

Listing 3.1 : Configuration de la sécurité de Kibana

```
# Générer les clés de chiffrement
/usr/share/kibana/bin/kibana-encryption-keys generate

# Copier les valeurs générées dans le fichier de configuration
# Remplacer <valeurs_générées> par les clés obtenues
echo "<valeurs_générées>" >> /etc/kibana/kibana.yml

# Obtenir le mot de passe du conteneur http.p12
/usr/share/elasticsearch/bin/elasticsearch-keystore show xpack.security.http.ssl.keystore.
    secure_password

# Extraire les certificats nécessaires
cd /etc/kibana/
openssl pkcs12 -in /etc/elasticsearch/certs/http.p12 -out server.crt -clcerts -nokeys
openssl pkcs12 -in /etc/elasticsearch/certs/http.p12 -out server.key -nocerts -nodes

# Configurer les permissions
chown root:kibana /etc/kibana/server.*
chmod g+r /etc/kibana/server.*

# Éditer le fichier de configuration Kibana
cat << EOF >> /etc/kibana/kibana.yml
server.ssl.enabled: true
server.ssl.certificate: /etc/kibana/server.crt
server.ssl.key: /etc/kibana/server.key
EOF

# Redémarrer le service Kibana
systemctl restart kibana.service
```

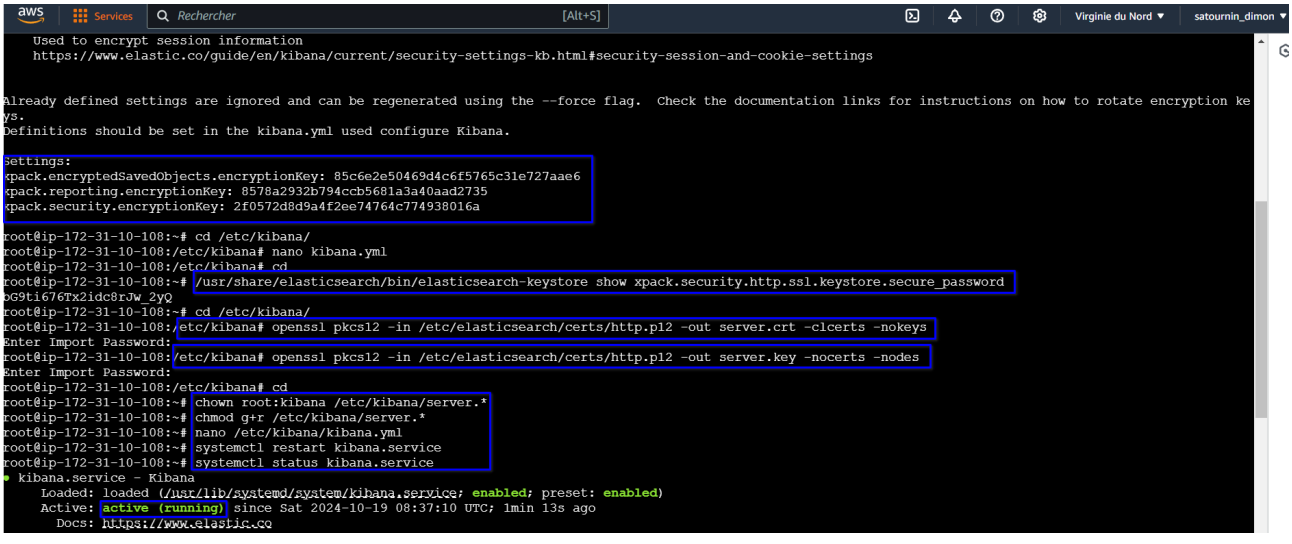


FIGURE 3.7 : Sécurisation de Kibana

3.3.6 Test de fonctionnalité

Pour les tests, nous en ferons deux pour tester une partie des fonctionnalités de notre solution :

3.3.6.1 Premier Test

Nous avons mené une simulation d'attaque en tentant de nous connecter en SSH à notre serveur SIEM depuis une machine Windows à l'aide d'une clé privée invalide. L'objectif était de vérifier si nos règles de sécurité pouvaient détecter cette tentative d'intrusion et générer les logs correspondants, afin de déclencher une alerte nous informant qu'une personne non autorisée tente de se connecter à notre système. Cette simulation nous a ainsi permis d'évaluer l'efficacité de notre outil de surveillance dans des conditions réelles.

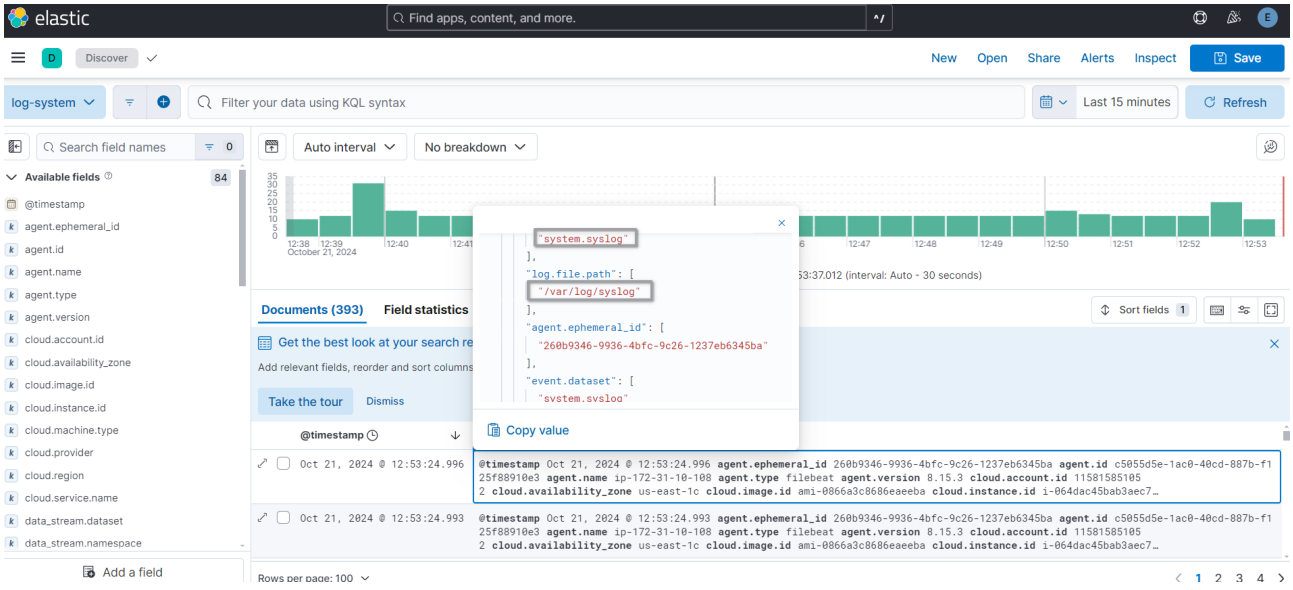


FIGURE 3.8 : Détection de connexion à SSH

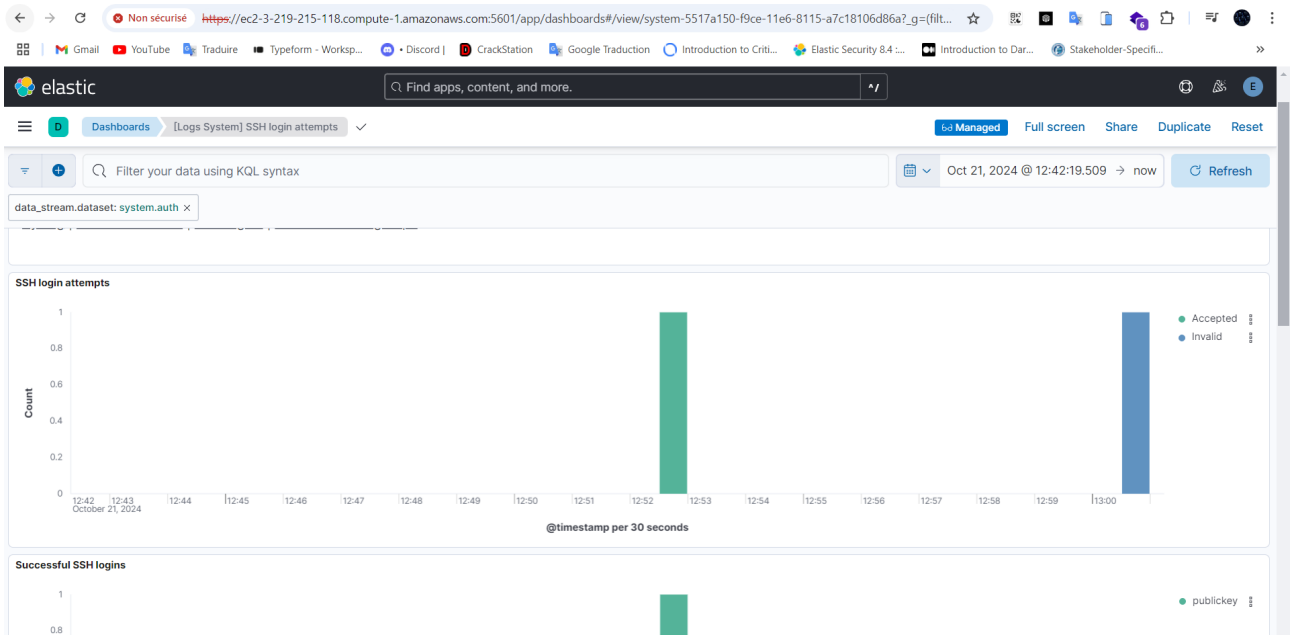


FIGURE 3.9 : Filtrage des connexions SSH

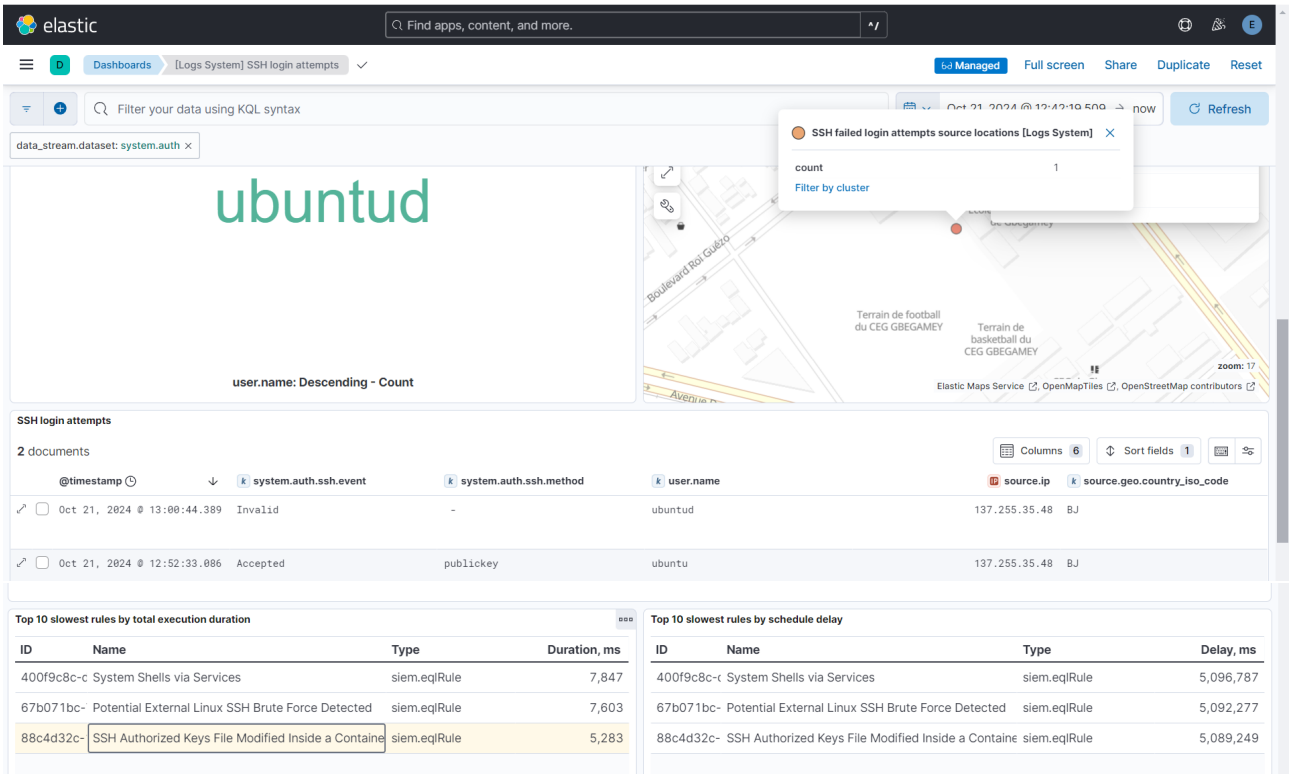


FIGURE 3.10 : Détection de connexion à SSH

3.3.7 Deuxième Test

Lors de ce test, nous avons simulé une attaque par force brute sur notre service web à l'aide de l'outil **FFUF**. Ce service, hébergé dans un conteneur Docker, est accessible sur le port 8080 de notre serveur Ubuntu sur AWS. Nous avons ciblé ce service pour notre test, car il représente un actif critique : il assure la validation des paiements via les comptes des entreprises partenaires au port autonome de cotonou, avant que ces transactions ne soient validées par la banque mandatée pour les opérations commerciales. Cette plateforme est hautement stratégique pour le secteur portuaire, du fait de son importance économique. Ce test effectué permet de détecter les dysfonctionnements de la plateforme et de générer des alertes afin de prendre rapidement les mesures adéquates pour contrer les menaces potentielles. Cela nous permettra également d'anticiper les attaques futures et de maintenir une protection à jour pour préserver la stabilité économique de l'entreprise. Nous avons ensuite vérifié le bon fonctionnement de notre outil de détection d'attaques mise en place, en nous assurant qu'il identifiait correctement cette tentative d'attaque à partir de l'adresse IP de l'attaquant, conformément à notre configuration. Nous avons également confirmé que les logs étaient bien générés et renvoyés.

Il est important de noter que ces tests ne représentent qu'une partie des performances de notre solution Elastic Security. Cependant, il convient de souligner qu'il s'agit de l'un des meilleurs outils EDR open source disponibles sur le marché. Elastic Security propose plusieurs modules pour assurer une surveillance centralisée des activités au sein d'une grande entreprise.

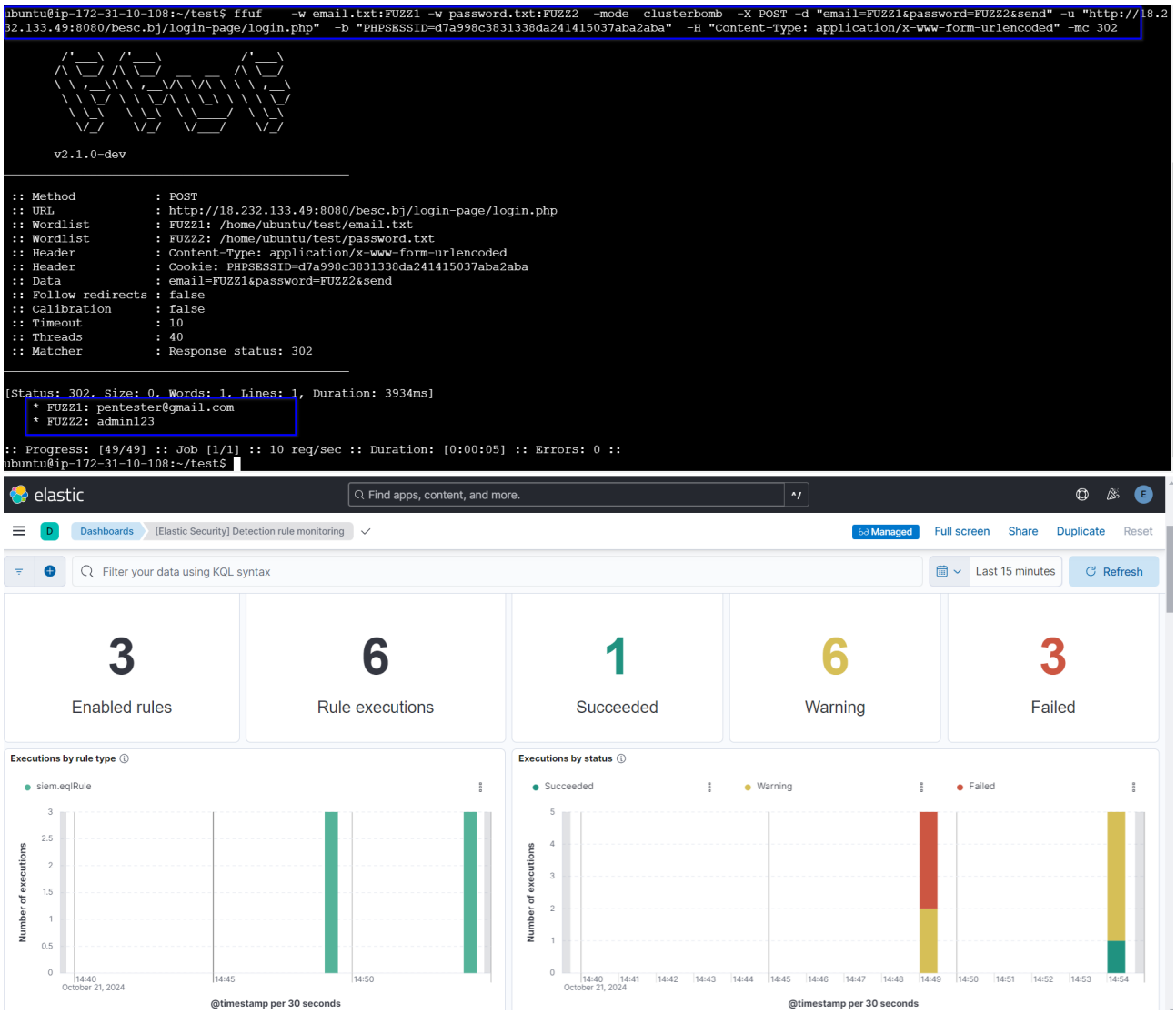


FIGURE 3.11 : Détection d'attaque par force brute sur notre server web

Conclusion

Dans ce chapitre, nous avons expliqué les étapes de configuration de la stack ELK avec l'intégration d'un EDR, en précisant l'ensemble des services à monitoriser et les alertes générées à chaque fois qu'une action a été effectuée, selon les règles que nous avons définies. Nous avons réalisé des tests de fonctionnalité pour valider nos configurations. Nous avons constaté que notre solution SIEM a réussi à détecter et à stopper une attaque par brute force sur SSH avec succès. Cela permettra aux entreprises de mieux protéger leurs actifs contre diverses menaces grâce à ce type de solution

Conclusion générale et perspectives

Ce projet nous a permis d'approfondir nos connaissances théoriques et pratiques acquises tout au long de notre formation. Le développement d'un tel projet n'est jamais totalement finalisé, car chaque jour, les attaquants trouvent de nouvelles méthodes pour contourner les systèmes de sécurité en place. C'est dans cette optique, afin d'améliorer notre travail, que nous proposons plusieurs axes d'évolution majeurs, tels que :

- **Le Déploiement d'un APM intégré à la stack ELK :** qui permettra une détection précoce des comportements anormaux au niveau des applications, renforçant ainsi la capacité à identifier rapidement les tentatives d'intrusion avant qu'elles ne compromettent le système.
- **L'Intégration de la Threat Intelligence :** l'ajout de données contextuelles sur les menaces émergentes enrichira notre SIEM, permettant une adaptation proactive des défenses face aux nouvelles techniques d'attaque.
- **L'Implémentation de l'analyse prédictive par IA :** Cette approche anticipative permettra de détecter les schémas d'attaque potentiels avant leur matérialisation, optimisant ainsi le temps de réponse et améliorant la capacité à réagir rapidement.
- **L'Automatisation via des playbooks :** garantira une réaction immédiate et cohérente, 24/7, afin de contrer efficacement les cyberattaques en temps réel.

Ces quatre axes d'amélioration, complémentaires à notre SIEM existant, formeront un écosystème de défense dynamique capable de s'adapter continuellement aux nouvelles menaces tout en maintenant une efficacité optimale dans la détection et la réponse aux incidents.

Bibliographie

[1] Gabriel Landau. "**Endpoint Security : A Complete Guide**", 2021 Edition, 10 novembre 2020.

[2] Mr Rihab. "**Conception et mise en place d'un SIEM (mémoire 2018)**", Université Djilali Liabès de Sidi Bel Abbés, consulté le 16 juin 2024.

[3] Thibaud Badouard. "**Déploiement d'un SIEM et enrichissement des données**", Premiers retours, JRSSI, 2018, (Source RSSI le 18 juin 2024 à 17h 11).

[4] Khadim Rassoul THIAM. "**Rapport de la mise en place de ELK**", (Source RSSI le 07 juillet 2024), Edition 2023-2024.

[5] Luc Deo-Gracias SEMASSA. "**Detecting AD Attacks with ELK SIEM**", Meetup bjWhite-Hats, 27 juillet 2024.

[6] Joseph Dembele. "**Mise en place d'un système de gestion centralisé des logs et des événements SIEM**", Année 2019-2021.

Webographie

[7] Crowdstrike. "*Comprendre la sécurité informatique*", https://www.crowdstrike.com/fr-fr/cybersecurity-101/cybersecurity/it-security/, consulté le 15 mai 2024.

[8] Cisco. "*Qu'est-ce que la sécurité informatique ?*", https://www.cisco.com/c/fr_fr/products/security/what-is-it-security.html, consulté le 15 mai 2024.

[9] Fortinet. "*Les objectifs de la sécurité Informatique*", https://www.fortinet.com/resources/cyberglossary/cia-triad, consulté le 21 mai 2024.

[10] Kaspersky. "*Qu'est-ce qu'une attaque XSS (Cross-Site Scripting) ?*", https://www.kaspersky.fr/resource-center/definitions/what-is-a-cross-site-scripting-attack, consulté le 22 juin 2024.

[11] Kaspersky. "*Qu'est-ce qu'une injection SQL ?*", https://www.kaspersky.fr/resource-center/definitions/sql-injection, consulté le 22 juin 2024.

[12] Wizard Cyber. "*Qu'est-ce que le security monitoring ?*", https://wizardcyber.com/what-is-cyber-security-monitoring-and-why-it-matters/, consulté le 22 juin 2024.

[13] IBM. "*HIDS (Host-Based Intrusion Detection System)*", https://www.ibm.com/fr-fr/topics/intrusion-detection-system, consulté le 28 juin 2024.

[14] Microsoft "*Qu'est-ce qu'un système SIEM ? "*https://www.microsoft.com/en-us/security/business/security-101/what-is-siem, consulté le 04 juillet 2024.

[15] Elastic. "*Présentation de la Stack ELK."*https://www.elastic.co, consulté le 04 juillet 2024.

[16] UpGuard. *"Les outils NIDS et HIDS"*https://study-ccna.com/firewalls-ids-ips-explanation-comparison/, consulté le 07 juillet 2024.

[17] Elastic Stack 8 "*"Installation de la stack Elk avec configuration de ssl de la version 8.15"*https://std.rocks/fr/gnulinux_siem_01_install_v8.html, consulté le 22 août 2024

[18] Maltego "*"Social Engineer Toolkit (SET) "*https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/, consulté le 22 août 2024

[19] SolarWinds (DNSSTUFF) "*"les Outils HIDS"*https://www.dnsstuff.com/host-based-intrusion-detection-systems., consulté le 22 août 2024

[20] AWScloud. "*"Création des instances AWS "*https://aws.amazon.com/, consulté le 07 juillet 2024.

[21] Agent filebeat. "*"Configuration elastic security "*https://www.elastic.co/guide/en/security/7.17/install-endpoint.html, consulté le 10 octobre 2024.

[22] Tableau comparatif référence. "*"Comparatif de solutions SIEM Splunk et ELK"*https://maximepiazzola.wordpress.com/2018/01/19/introduction-aux-solutions-siem/, consulté le 20 octobre 2024.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction 1

1 Présentation de la structure d'accueil et déroulement du stage 3

Introduction 3

1.1 Présentation de la structure d'accueil (PAC) 3

1.1.1 Localisation 3

1.1.2 Historique 3

1.1.3 Missions 4

1.1.4 Structure organisationnelle 4

1.1.5 Présentation du département des Systèmes d'Information 5

1.1.6 Missions des différents secteurs de la DSI 6

1.2 - Déroulement du stage 7

1.2.1 Travaux effectuent et acquis du stage 7

1.2.2 Difficultés rencontrées 8

1.3 - Bilan de notre stage 8

Conclusion 9

2 Étude, analyse et choix de la solution 10

Introduction 10

2.1 - La Sécurité Informatique 10

2.1.1 Définition 10

2.1.2 Les objectifs de la Sécurité Informatique 10

2.2 - Les Menaces informatiques 11

2.3 Le monitoring . . . 13
2.3.1 Définitions . . . 13
2.3.2 Objectifs du monitoring . . . 13
2.3.3 Les types de Monitoring qu'un SIEM possède . . . 13
2.3.4 Les avantages du monitoring . . . 14
2.4 Les IDS (Intrusion Detection System) . . . 14
2.4.1 Clarification conceptuelle . . . 14
2.4.2 Fonctionnement des IDS . . . 15
2.4.3 Avantages des IDS et quelques exemples d'outils . . . 16
2.4.3.1 Systèmes de détection d'intrusion réseaux (NIDS) . . . 16
2.4.3.2 Systèmes de détection d'intrusion hôtes(HIDS) . . . 16
2.5 Généralité sur les Systèmes automatisés de détection, d'analyse et de réponse aux incidents de sécurité . . . 17
2.5.1 Définition SIEM . . . 17
2.5.2 Fonctionnement des SIEM . . . 18
2.6 Elastic Security et EDR (Endpoint Detection and Response) . . . 19
2.6.1 Elastic Security . . . 19
2.6.2 EDR (Endpoint Detection and Response . . . 19
2.7 Quelques solutions open sources . . . 20
2.8 Comparaison de quelques solutions open source . . . 20
Conclusion . . . 21

3 Déploiement et mise en place de la solution **22**
Introduction . . . 22
3.1 - Présenation de la Stack ELK . . . 22
3.1.1 EDR . . . 22
3.1.2 Diffence entre XDR et EDR . . . 23
3.2 - Nouvelle Architecture du réseau . . . 23
3.3 Mise en œuvre de la solution SIEM . . . 25
3.3.1 Configuration de l'environnemenet sur aws . . . 25
3.3.2 **Justification du déploiement de deux instances sur AWS** . . . 25
3.3.3 **Installation de la Stack ELK sur Ubuntu 24.02** . . . 26
Conclusion . . . 28
3.3.4 **Sécuriser Kibana** . . . 28
3.3.5 Procédure détaillée pour sécuriser Kibana . . . 29
3.3.6 **Test de fonctionnalité** . . . 29
3.3.6.1 Premier Test . . . 30
3.3.7 Deuxième Test . . . 31

Bibliographie **34**

Webographie **35**

Table des matières **36**