Implémentation d'un SIEM : Système de gestion des informations et des évènements de sécurité.

Réalisé par "SMART NET[1]" : Messar Cylia, Tagzirt Elissa, Bousba Neda, Kedadsa Islam Chakib, Sadi Lina, et Bessaha Sofiane.
Sous l'encadrement académique de : M.Hamani Nacer[1], et M.Amrouche Hakim[1].

[1] École Nationale Supérieure d'Informatique, Oued Smar, Alger, Algérie

Abstract :

Ce projet vise à mettre en place un système de gestion des informations et des événements de sécurité (SIEM) pour renforcer la sécurité d'un réseau d'application spécifique. Nous explorons les différentes étapes du déploiement d'un SIEM, telles que la sélection de la solution appropriée, la conception de l'architecture, la configuration des capteurs, l'intégration des sources de données, l'analyse des événements et la réponse aux incidents. Nous commençons par une introduction mettant l'accent sur l'importance de sécuriser un réseau, suivie de la présentation de la problématique du projet. Pour y répondre, une étude théorique est entreprise sur les SIEM afin de comprendre leur fonctionnement et leurs capacités, ainsi que la comparaison des différents outils disponibles. Cette étude théorique est suivie par la mise en œuvre de l'outil choisi dans le réseau d'application. Nous concluons par l'évaluation de la robustesse de la solution à travers la simulation de plusieurs attaques, ainsi que par l'intégration des différents composants réseaux. À travers ce projet, notre objectif est d'améliorer la détection précoce des menaces, la gestion des incidents et la conformité aux normes de sécurité.

Mots clés : SIEM, Sécurité, Réseau.

1 Introduction

Dans l'ère digitale actuelle, la sécurisation des réseaux et des données est devenue un enjeu crucial pour les organisations de toutes tailles. Face à une augmentation constante des menaces de sécurité, la nécessité de disposer d'outils efficaces pour détecter, prévenir et répondre aux incidents de sécurité n'a jamais été aussi pressante. Cette évolution a été accompagnée par le développement continu de divers outils de sécurité informatique, allant des pare-feu et des systèmes de détection d'intrusion (IDS) aux solutions plus avancées telles que les SIEM. En 2005, Gartner, une entreprise de premier plan spécialisée dans le conseil et la recherche technologique, introduisit pour la première fois la notion de SIEM (Security Information and Event Management), établissant ainsi un nouveau standard essentiel pour la protection continue de l'information sur la base de deux générations précédentes: SEM(Security Event Management) et SIM(Security Information Management). Dans cette optique, cette recherche vise à explorer en profondeur l'importance des SIEM dans le paysage actuel de la sécurité informatique, en mettant en lumière leurs avantages potentiels ainsi que les défis associés à leur déploiement et à leur utilisation efficace.

1.1 Problématique

Notre cas d'application concerne la simulation de l'opération du baccalauréat, un événement national qui se déroule chaque année à l'ESI. Plusieurs serveurs web, organisés en cluster, sont utilisés pour répondre aux requêtes des utilisateurs. Dans ce projet, il est demandé d'effectuer une étude théorique sur la technologie SIEM et les différents outils associés. Le défi est de déterminer les critères appropriés pour choisir, parmi les 86 outils SIEM existants, celui qui est le plus adéquat pour notre cas d'application, en se limitant à la surveillance :

- D'un reverse proxy nginx.
- De deux serveurs Web apache sous Linux.
- D'un serveur Web IIS sous Windows.

À la fin de ce projet, nous devons être en mesure de déterminer les lacunes en termes de sécurité dans le réseau donné, ainsi que les fonctionnalités apportées par un SIEM par rapport aux outils traditionnels de sécurité informatique. Il est demandé d'inclure la configuration d'un pare-feu et d'un système de détection d'intrusion. Plus important encore, nous devons comprendre comment configurer ces éléments ensemble pour fournir une solution complète servant le Centre des Opérations de Sécurité (SOC).

1.2 Objectifs

- Analyse approfondie des SIEM.
- Identifier les lacunes du réseau d'application et ses besoins nécessaires.
- Élaboration d'une stratégie de comparaison des outils SIEM existants.
- Choix d'une solution adaptée aux besoins spécifiques de réseau donné.
- Évaluation de la solution choisie face à diverses attaques.

2 Étude de l'existant

Pour garantir la protection de réseau étudié, il est essentiel de comprendre les spécifications de sécurité actuelles et d'identifier les lacunes qui existent. Cette section présente une étude de l'existant des spécifications de sécurité auxquelles ce réseau doit répondre, afin de poser les bases nécessaires pour combler ces lacunes et renforcer son infrastructure.

2.1 Existant:

Dans le réseau donné, seuls un IDS (Système de Détection d'Intrusion) et un pare-feu ont été configurés pour assurer la sécurité. Ces outils sont indéniablement essentiels pour identifier les menaces et contrôler le trafic entrant et sortant. Cependant, ils présentent des limitations importantes en termes de fonctionnalités avancées nécessaires pour un Centre des Opérations de Sécurité (SOC) efficace.

2.2 Spécifications pour la solution SIEM:

Notre solution doit être capable de répondre à ces différents types de spécifications:

2.2.1 Spécifications de sécurité:

- Identifier les menaces système et réseau.
- Générer des alertes en temps réel.
- Répondre rapidement aux incidents.
- Offrir des fonctionnalités de forensics.
- Surveiller les comportements des utilisateurs internes.
- S'intégrer avec d'autres outils de sécurité.
- Générer automatiquement des rapports détaillés sur l'état de sécurité.
- Collecter et centraliser les logs.
- Offrir une visualisation sophistiquée des logs.
- Corréler les logs pour détecter les menaces.

2.2.2 Spécifications pour l'évaluation des données: Notre solution doit être capable de:

- Collecter, stocker et analyser les journaux de sécurité provenant de diverses sources.
- Accepter différents formats de données.
- Être dimensionné pour être capable de collecter, stocker et analyser une quantité importante de données.
- Être évolutif et capable de s'adapter à la croissance du SI.

2.2.3 Spécifications pour l'évaluation des capacités : Notre solution doit être capable de :

- Offrir un support technique et une documentation complète.
- Fournir des règles de corrélation prédéfinies et régulièrement mises à jour.
- Intégrer des flux de threat intelligence pour enrichir les événements de sécurité avec des indicateurs de menace connus.
- Être facile à déployer et à maintenir, avec une configuration initiale simplifiée.

2.2.4 Coûts et réglementations: Notre solution SIEM doit satisfaire aux critères suivants:

- Être open-source et ne pas engendrer de coût d'acquisition ou de licence.
- Fournir une rétention des données à long terme pour répondre aux exigences réglementaires.
- Offrir une solution de stockage hors cloud pour garantir la confidentialité et le contrôle des données sensibles.

3 SIEM

Selon Gartner, La technologie SIEM (En anglais, Security Information and Event Management) prend en charge la détection des menaces et la réponse aux incidents de sécurité grâce à la collecte en temps réel et à l'analyse historique des événements de sécurité provenant d'une grande variété de sources de données. Les SIEM constituent la plate-forme centrale des centres d'opérations de sécurité modernes. Ils recueillent les événements provenant de multiples capteurs, les mettent en corrélation et fournissent des vues synthétiques des alertes pour le traitement des menaces et l'établissement de rapports sur la sécurité. Cela correspond parfaitement à nos attentes pour la solution à fournir. La technologie SIEM est idéale pour répondre aux spécifications et renforcer la sécurité de réseau étudié.

3.1 Fonctionnement d'un SIEM

Tout outil SIEM est équipé au minimum de cet ensemble de fonctionnalités essentielles pour assurer une gestion efficace des événements de sécurité:

- La collecte des données de sécurité.
- L'agrégation de ces données.
- Traitements des données.
- Corrélation des événements de sécurité.
- Visualisation facile des résultats des traitements et des corrélations effectués sur les événements collectés.

3.1.1 Collecte de données de sécurité: Il existe plusieurs sources qui génèrent des journaux d'évènements, parmi lesquelles on trouve:

- Des outils de sécurité: Pares-feu.
- Des outils réseau: Routeurs.
- Des serveurs.
- Des applications.
- Des points-terminaux: Les ordinateurs et les téléphones portables.

La première étape de tout SIEM consiste à collecter les évènements concerné par la sécurité, ce qui peut être effectué selon deux méthodes: soit par Pull, soit par Push, en fonction de la source.

- Push: Les sources transmettent périodiquement les données de sécurité, qui peuvent être envoyées soit via un agent, soit sans agent, en utilisant des protocoles tels que Syslog, NetFlow ou SNMP.
- Pull: Les sources envoient automatiquement leurs données de sécurité au SIEM en temps réel.

3.1.2 Agrégation: Il s'agit de rassembler les données ou bien les logs collectées dans un référentiel centralisé qui peut être une base de données ou toute autre infrastructure de stockage capable de gérer de grands volumes de données de journal.

3.1.3 Traitements des logs collectés: Le traitement des journaux est l'art de prendre des journaux système bruts provenant de plusieurs sources, d'identifier leur structure ou leur schéma, et de les transformer en une source de données cohérente et normalisée. Le traitement des journaux peut comprendre ces différentes étapes:

- Parsing: C'est l'analyse des logs pour extraire des informations pertinentes telles que les adresses IP, les noms d'utilisateur, les horodatages et les types d'événements.
- Normalisation: Les mettre dans un formats standard.
- Catégorisation: Catégoriser le log collecté, par exemple un log d'authentification.
- Enrichissement: Ajouter un champ supplémentaire apportant une information qui peut aider par la suite dans la corrélation ou la visualisation.

3.1.4 Corrélation: La corrélation permet d'analyser et de comparer les journaux de plusieurs sources et d'identifier des relations entre différents événements qui pourraient indiquer un incident de sécurité réel, une menace potentielle ou une vulnérabilité. La corrélation vous permet d'automatiser la détection des événements qui ne devraient pas se produire sur votre réseau. Par exemple, un simple message d'erreur sur un serveur peut être le signe d'un incident de sécurité lorsqu'il est corrélé avec d'autres événements tels que le blocage de connexion sur un pare-feu et une tentative de mot de passe incorrect sur un portail d'entreprise.

3.1.5 Visualisation: Les SIEM génèrent des visualisations sous forme de tableaux de bord pour afficher les situations des données en temps réel, permettant ainsi aux administrateurs d'identifier les anomalies. Tout cela est illustré de manière structurée à travers des tableaux de logs, des graphiques d'alertes par degré, ainsi que résumé dans des rapports.

4 Étude comparative des outils SIEM existants

4.1 Outils SIEM:

En nous appuyant sur une méthodologie rigoureuse, nous avons consulté le site officiel de Gartner, qui propose un classement de 86 outils SIEM basé sur des critères tels que l'expérience client, les capacités du produit, la distribution des évaluations, ainsi que les analyses détaillées des évaluateurs et les facteurs de décision. Ces critères ont été essentiels pour nous permettre de cibler les outils les plus pertinents pour notre étude. Vu le grand nombre d'outils disponibles, nous avons complété cette démarche en menant une étude préliminaire ciblée sur notre domaine d'application, à savoir le réseau des inscriptions au baccalauréat. Cela nous a permis d'affiner notre sélection initiale et de nous concentrer sur les 6 outils les plus significatifs et les mieux adaptés à nos besoins d'analyse et de comparaison, ainsi qu'aux spécifications données précédemment. Les outils sélectionnés sont les suivants:

- Splunk, lancé en 2003 par Splunk Inc.
- QRadar, lancé en 2001 par IBM.
- Exabeam, lancé en 2012 par Exabeam Inc.
- ELK Stack, lancé en 2010 par Elastic.
- Wazuh, lancé en 2017 par Wazuh Inc.
- Security Onion, lancé en 2008 par Security Onion Solutions.

4.1.1 Fonctionnement de Splunk: C'est un outil sophistiqué pour la gestion des données de sécurité. Il s'appuie sur des agents, connus sous le nom de Forwarders, pour la collecte des données, un indexeur pour leur stockage et leur indexation, ainsi qu'une interface de recherche pour l'analyse. Pour assurer une coordination efficace des déploiements distribués, Splunk utilise un Cluster Master. La gestion des licences est confiée à un License Master, tandis que la surveillance des performances est réalisée à l'aide d'une Monitoring Console. En outre, le Deployment Server se charge de la distribution des configurations, et les systèmes d'authentification et d'autorisation contrôlent l'accès aux ressources.

4.1.2 Fonctionnement de QRadar: La QRadar Console joue un rôle central dans la surveillance des événements et des activités de sécurité. Les données sont collectées par le QRadar Event Collector, puis traitées par le QRadar Event Processor afin de détecter les menaces potentielles. Pendant ce temps, le QRadar Flow Collector et le Flow Processor analysent les flux réseau pour offrir une visibilité accrue. Les données sont ensuite stockées et gérées par les QRadar Data Node et App Host, assurant ainsi une extensibilité et une gestion efficaces du système QRadar.

4.1.3 Fonctionnement de Exabeam: Exabeam est une solution basée sur l'Intelligence Artificielle. Cette plateforme intègre un SIEM cloud et des analyses comportementales avancées. Avec la fonctionnalité TDIR(Threat Detection, Investigation, and Response), Exabeam automatise la détection, l'investigation et la réponse aux menaces. Enfin, le composant Exabeam Copilot complète le processus en fournissant des résumés concis des menaces et recommandations.

4.1.4 Fonctionnement de ELK Stack: La suite ELK est composée de : Beats, Elasticsearch, Logstash, et Kibana. Beats récupère les logs de diverses sources et les envoie à Logstash et/ou Elasticsearch pour le traitement. Logstash filtre, enrichit et transforme les logs, tandis que Elasticsearch les indexe pour une recherche et une analyse efficaces. Kibana fournit des outils de visualisation graphique pour explorer les alertes.

4.1.5 Fonctionnement de Wazuh: Wazuh fonctionne grâce à quatre composants principaux : les agents, l'indexeur, le serveur et le tableau de bord. L'indexeur stocke et indexe les alertes générées par le serveur. Ce dernier analyse les données collectées par les agents Wazuh installés sur divers appareils. Enfin, le tableau de bord de Wazuh permet une vue synthétisée des opérations effectuées depuis la collecte jusqu'à la génération d'alertes.

4.1.6 Fonctionnement de Security Onion: C'est un outil qui repose sur différentes architectures d'implémentation en exploitant différents outils dédiés à l'inspection du trafic réseau ainsi qu'à l'analyse et au stockage des données. Cette diversité d'outils confère une efficacité et une robustesse globale au réseau, ainsi qu'au système SIEM en particulier.

4.2 Critères personnalisés:

Nous avons essayé de prendre des critères complémentaires et qui répondent à plusieurs aspects, nous avons pris en considération les lacunes de réseau donnée ainsi que les exigences à respecter:

4.2.1 Satisfaction des critères par les outils à comparer: Dans les tableaux suivants, on illustre les outils selon leur satisfaction des critères (Table 2 - Table 7):

4.2.2 Résultats de la comparaison: Après avoir évalué les outils SIEM, nous avons opté principalement pour Wazuh, qui satisfait 14 critères sur 17 pour répondre à nos besoins immédiats. Nous avons exclu les options payantes en raison de leur coût élevé, bien qu'elles nous aient servi de guide en raison de leur quasi-exhaustivité en termes de fonctionnalités. Pour valider un outil open source, nous avons effectué une comparaison approfondie entre Wazuh et Security Onion. Il apparaît que les deux offrent des avantages distincts. Bien que complémentaires, leur combinaison pourrait constituer une solution robuste surpassant même des outils payants. Cependant, en raison de considérations de complexité de déploiement et de maintenance, nous avons fait le choix de

Table 1
Critères de comparaisons classés par aspect.

Aspect	Critère
Sécurité	Réponse aux incidents
	Analyse de la posture de sécurité du système
	Analyse de la posture de sécurité du réseau
	Corrélation sophistiquée et réduction des faux positifs
	Génération des alertes en temps réel
	Règles de corrélation prédéfinies et à jour
	Intégration avec d'autres outils de sécurité
	Performance (Rapidité, Indexation)
Données	Rétention
	Gros volume de données
Capacité	Intégration de la threat intelligence
	Non Complexe
	Génération de rapports
	Visualisation personnalisée
	Documentation
Coût et réglementation	Hors Cloud
	Non couteux

Table 2
Satisfaction des critères par Splunk.

Critère	Oui	Non
Réponse aux incidents	-	
Analyse de la posture de sécurité du système	-	
Analyse de la posture de sécurité du réseau	-	
Corrélation sophistiquée et réduction des faux positifs		-
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour	-	
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)	-	
Rétention	-	
Gros volume de données	-	
Intégration de la threat intelligence	-	
Non Complexe	-	
Génération de rapports	-	
Visualisation personnalisée	-	
Documentation		
Hors Cloud	-	
Non coûteux		-

Table 3
Satisfaction des critères par QRadar.

Critère	Oui	Non
Réponse aux incidents	-	
Analyse de la posture de sécurité du système	-	
Analyse de la posture de sécurité du réseau	-	
Corrélation sophistiquée et réduction des faux positifs	-	
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour	-	
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)	-	
Rétention	-	
Gros volume de données	-	
Intégration de la threat intelligence	-	
Non Complexe	-	
Génération de rapports	-	
Visualisation personnalisée	-	
Documentation		-
Hors Cloud	-	
Non coûteux		-

Table 4
Satisfaction des critères par Exabeam.

Critère	Oui	Non
Réponse aux incidents	-	
Analyse de la posture de sécurité du système	-	
Analyse de la posture de sécurité du réseau	-	
Corrélation sophistiquée et réduction des faux positifs	-	
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour	-	
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)	-	
Rétention	-	
Gros volume de données	-	
Intégration de la threat intelligence	-	
Non Complexe	-	
Génération de rapports	-	
Visualisation personnalisée	-	
Documentation	-	
Hors Cloud	-	
Non coûteux		-

Table 5
Satisfaction des critères par Wazuh.

Critère	Oui	Non
Réponse aux incidents	-	
Analyse de la posture de sécurité du système	-	
Analyse de la posture de sécurité du réseau		-
Corrélation sophistiquée et réduction des faux positifs		-
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour	-	
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)	-	
Rétention	-	
Gros volume de données		-
Intégration de la threat intelligence	-	
Non Complexe	-	
Génération de rapports	-	
Visualisation personnalisée	-	
Documentation	-	
Hors Cloud	-	
Non coûteux	-	

Table 6
Satisfaction des critères par Security Onion.

Critère	Oui	Non
Réponse aux incidents	-	
Analyse de la posture de sécurité du système		-
Analyse de la posture de sécurité du réseau	-	
Corrélation sophistiquée et réduction des faux positifs		-
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour	-	
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)		
Rétention		-
Gros volume de données	-	
Intégration de la threat intelligence		-
Non Complexe	-	
Génération de rapports		-
Visualisation personnalisée		-
Documentation	-	
Hors Cloud	-	
Non coûteux	-	

Table 7
Satisfaction des critères par ELK Stack.

Critère	Oui	Non
Réponse aux incidents		-
Analyse de la posture de sécurité du système		-
Analyse de la posture de sécurité du réseau		-
Corrélation sophistiquée et réduction des faux positifs		-
Génération des alertes en temps réel	-	
Règles de corrélation prédéfinies et à jour		-
Intégration avec d'autres outils de sécurité	-	
Performance (Rapidité, Indexation)		-
Rétention	-	
Gros volume de données	-	
Intégration de la threat intelligence		-
Non Complexe		-
Génération de rapports	-	
Visualisation personnalisée	-	
Documentation	-	
Hors Cloud	-	
Non coûteux	-	

privilégier Wazuh. Afin de compléter les capacités de surveillance réseau de ce dernier, nous avons décidé d'intégrer l'IDS Suricata, inclus dans l'outil Security Onion, pour assurer la surveillance du trafic réseau.

4.2.3 Fonctionnement de l'outil Wazuh et ses composants:

La solution Wazuh (Voir Figure 1) repose sur les agents Wazuh installés sur les composants principaux et les points terminaux. Les composants principaux sont au nombre de trois: le serveur Wazuh, qui peut être déployé sous forme de cluster; le Wazuh Indexer, qui stocke et gère les données; et le tableau de bord Wazuh, qui représente le point d'accès pour les utilisateurs Wazuh.

Les points terminaux peuvent être des serveurs, des PC ou des laptops, des instances cloud, et même des machines virtuelles.

Prenons une vision plus approfondie(Voir la figure 2) sur la solution. L'agent installé sur les points terminaux offre un accès à un ensemble de fonctionnalités proposées par la solution Wazuh, parmi lesquelles la réponse active, le contrôle de l'intégrité des fichiers, la collecte des logs, la détection des malwares, et bien d'autres. Les données collectées par l'agent sont cryptées et envoyées au serveur Wazuh via une connexion authentifiée et sécurisée. Ce dernier analyse ces données grâce aux décodeurs et aux règles de corrélation existantes ou modifiées, détecte les vulnérabilités, lève les alertes de sécurité, et les envoie au Wazuh Indexer qui va les organiser et les stocker.

Le tableau de bord Wazuh, via une API RESTful, accède aux fonctionnalités et paramètres du gestionnaire Wazuh. Il a également accès aux fichiers sur le Wazuh Indexer et offre une interface utilisateur web pour la visualisation et l'analyse des données. Il comprend des tableaux de bord prêts à l'emploi.

5 Implémentation de la solution proposée

Dans cette section, nous allons détailler l'implémentation de notre solution SIEM, en mettant en évidence l'architecture, la configuration, et les étapes clés réalisées pour intégrer Suricata, PfSense et Wazuh. Nous décrirons également comment ces composants collaborent pour fournir une surveillance et une protection complètes

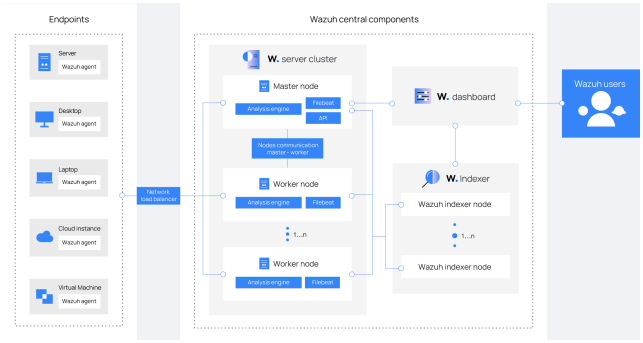

Figure 1. Cette illustration, prise du site officiel de Wazuh, montre les différents composants de la solution Wazuh et leurs interactions..

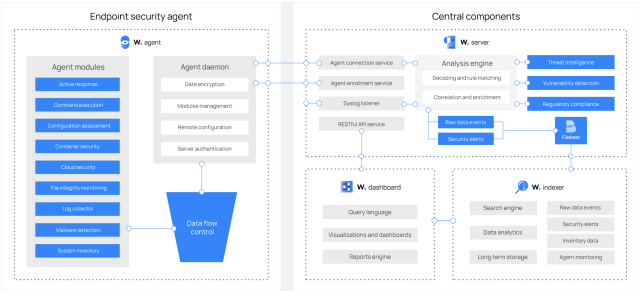

Figure 2. Le diagramme ci-dessous représente les composants et le flux de données de Wazuh.

du réseau. Voici un aperçu des étapes suivies:

5.1 Architecture de la solution:

Notre architecture est constituée de trois zones principales:

- DMZ (Zone Démilitarisée) : La DMZ agit comme un intermédiaire entre le réseau interne et le réseau externe. Elle héberge tous les services accessibles au public et est conçue pour offrir un niveau de sécurité supplémentaire en isolant les services publics des ressources internes sensibles. Elle comprend trois serveurs (deux Apache et un IIS) avec un reverse proxy nginx qui assure l'équilibrage de charge entre les trois serveurs. L'équilibrage de charge est effectué en round robin dans la DMZ.
- LAN (Réseau Interne) : Le LAN désigne le réseau interne de l'organisation. Il englobe les postes de travail et les serveurs internes qui nécessitent une protection et une sécurisation avec un accès restreint. Il intègre également le SIEM déployé et intégré, ainsi qu'une machine d'accès aux tableaux de bord pour les opérateurs de SOC (principalement l'administrateur).
- WAN (Réseau Externe) : Le WAN représente le réseau externe, ou Internet. Il permet aux utilisateurs de l'organisation d'accéder aux ressources externes et aux services en ligne, ainsi qu'aux bacheliers d'accéder aux serveurs de la DMZ. La sécurité dans cette zone est cruciale pour prévenir les attaques extérieures et protéger les données internes.

La connectivité entre ces trois zones est gérée par le pare-feu PfSense, qui occupe une position centrale au sein de notre infrastructure réseau. Pour renforcer la sécurité, nous avons intégré deux instances de Suricata IDS pour détecter les intrusions dans chaque zone (DMZ et LAN).

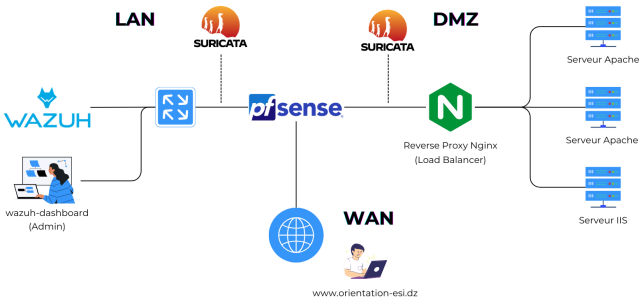

Figure 3. Architecture Solution.

5.2 Choix de Pare-feu "PfSense":

Pour répondre aux exigences du client en intégrant un pare-feu dans notre solution, nous avons choisi PfSense. Ce dernier est un outil open source basé sur le système d'exploitation FreeBSD, conçu pour offrir une protection réseau robuste. Ce choix s'explique par les raisons suivantes:

- Offre une gestion avancée des règles en créant, modifiant et gérant des règles de filtrage de trafic précises pour contrôler exactement ce qui est autorisé ou bloqué sur notre réseau.
- Dispose d'une interface web intuitive pour une gestion simplifiée, même pour les administrateurs non spécialisés.
- Conçue pour des performances élevées et une grande stabilité.
- PfSense est capable de gérer des réseaux de toutes tailles.

5.2.1 Configuration de PfSense: Dans les figures 4-6 on illustre des exemples de règles configuré au niveau de fire-wall:

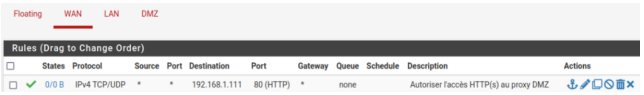

Figure 4. Cette règle permet aux utilisateurs externes d'accéder aux services web via le proxy situé dans la DMZ.

Figure 5. Cette règle permet à toutes les sources situées au niveau de la zone DMZ (wazuh-agents) de communiquer avec le serveur wazuh pour la collecte des logs et pour l'active response.

5.3 Choix de l'IDS "Suricata":

Pour répondre aux exigences du client en intégrant un IDS dans notre solution, nous avons choisi comme IDS Suricata. Ce dernier est un moteur de détection d'intrusions réseau (NIDS), de prévention d'intrusions réseau (IPS) et de surveillance de la sécurité réseau à haute performance. Il est détenu par une fondation à but non lucratif gérée par la communauté, l'Open Information Security Foundation (OISF). Nous l'avions choisi pour ces raisons:

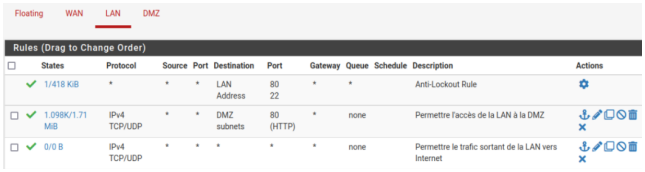

Figure 6. Ces deux règles permettent aux utilisateurs de la zone LAN d'accéder aux ressources dans la DMZ ainsi qu'à Internet tout en restant sécurisés.

- Il est open source.
- Inclue dans les architecture Security Onion. L'intégration de Suricata dans cette plateforme témoigne de sa fiabilité et de son efficacité.
- Répond à une lacune de Wazuh : Analyse de la posture du sécurité de réseau.

5.3.1 Pourquoi choisir un NIDS et non pas un HIDS? Les HIDS (Host IDS) analysent les données historiques pour détecter les vulnérabilités, tandis que les NIDS (Network IDS) agissent en temps réel, permettant de signaler immédiatement les problèmes. Les HIDS se concentrent sur un seul système ou ordinateur, tandis que les NIDS protègent l'ensemble du système en surveillant toutes les activités et le trafic à l'intérieur du réseau. Puisque les agents Wazuh assurent déjà les fonctionnalités d'un HIDS, nous avons préféré opter pour un NIDS en complément de la solution.

5.3.2 Pourquoi avons-nous choisi deux IDSs, un au niveau de LAN et un autre au niveau de DMZ? Définir des règles de détection d'intrusion (IDS) pour chaque zone de réseau, comme le LAN et la DMZ, est une bonne pratique en matière de sécurité informatique. Cela permet de cibler spécifiquement les menaces potentielles qui peuvent affecter chaque segment de réseau. En identifiant les comportements suspects ou malveillants, tout en renforçant la sécurité globale de l'infrastructure. Cela revient aussi à répartir la charge de travail et améliorer les performances globales du système de détection d'intrusion.

5.3.3 Configuration de suricata: Suricata offre des configurations simples grâce à un seul fichier principal de configuration (suricata.yaml) où l'on déclare l'interface d'écoute, les variables à utiliser, ainsi que les chemins vers les règles à appliquer en plus des règles par défaut. On a donc la possibilité de personnaliser nos règles en créant d'autres fichiers et en définissant le chemin vers ceux-ci pour s'assurer que Suricata les prend en considération. Une règle se compose des éléments suivants :

- L'action qui détermine ce qui se produit lorsque la règle correspond(alert, drop, reject, pass, log, drop and alert, reject and alert).
- L'en-tête qui définit le protocole, les adresses IP, les ports et la direction de la règle.
- Les options de la règle qui définissent les spécificités de la règle.

5.3.4 Règles personnalisées pour chaque zone: Il est à noter que Suricata vient avec un ensemble de règles riche qui combine plusieurs aspects et protocoles, mais cela n'empêche pas de personnaliser(Voir Table 8) notre IDS en fonction de nos besoins spécifiques. Voici quelques règles que nous avons mises en œuvre pour détecter toutes anomalies ou menaces:

Table 8
Exemples de règles personnalisées au niveau de l'IDS Suricata pour les deux zones LAN et DMZ.

Zone	Règles

LAN	Règle 1 : Détection de malwares et de communications avec des Command and Control
	`alert ip any any -> $LAN any (msg:"C&C Server Communication"; iprep: blacklist, track by_src; sid:1000006; rev:1;)`
	Règle 2 : Surveillance des tableaux de bord des SOC
	`alert http any any -> $SOC_DASHBOARD any (msg:"Access to SOC Dashboard Outside Working Hours"; flow:to_server,established; content:"dashboard"; http_uri; time:hour,[00,07]; sid:1000008; rev:1;)`

DMZ	Règle 1 : Détection d'attaques web courantes (Injection SQL)
	`alert http any any -> $DMZ_SERVERS any (msg:"SQL Injection Attempt"; flow:to_server,established; content:"select"; nocase; http_uri; content:"union"; nocase; http_uri; content:"-"; nocase; http_uri; sid:1000001; rev:1;)`
	Règle 2 : Détection d'attaques web courantes (XSS)
	`alert http any any -> $DMZ_SERVERS any (msg:"XSS Attack"; flow:to_server,established; content:"<script>"; nocase; http_uri; sid:1000002; rev:1;)`
	Règle 3 : Détection d'attaques DDoS
	`alert http any any -> $DMZ_SERVERS any (msg:"Potential DDoS Attack"; flow:to_server,established; threshold:type both, track by_src, count 50, seconds 10; sid:1000003; rev:1;)`

5.4 Fonctionnalités implémentées au niveau de SIEM Wazuh:

5.4.1 Collecte des données logs: Log Data Collection consiste à rassembler et à consolider les logs provenant de différentes sources de logs au sein d'un réseau. La collecte de données de logs aide les équipes de sécurité à respecter la conformité réglementaire, à détecter les menaces et à y remédier, ainsi qu'à identifier les erreurs d'application et d'autres problèmes de sécurité. Voici un tableau (Table 9) illustrant les différents fichiers journaux auxquels nous nous sommes intéressés pour notre cas de surveillance des points terminaux:

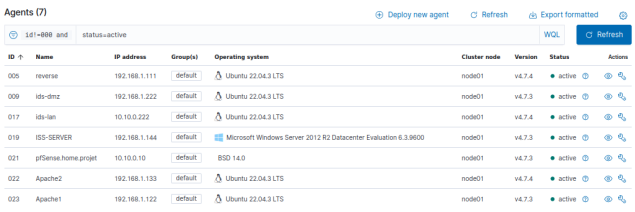

Figure 7. Les différents agents Wazuh sont installés et configurés au niveau des points terminaux et sont visualisables via le tableau de bord Wazuh. La couleur verte indique qu'ils sont en état actif.

Table 9
Types de journaux collectés pour chaque point terminal de notre réseau d'application.

Point	Type de Logs
Serveurs	Log Système Access Log Error Log
Suricata	Logs stockés dans le fichier eve.json
PfSense	system.log filter.log
Machine d'Admin	Log Système

5.4.2 Surveillance de l'intégrité des fichiers: FIM (File Integrity Monitoring) consiste à surveiller les chemins de fichiers spécifiés au niveau de ficheirs de configuration "ossec.conf" pour détecter les modifications via des scans périodiques. Le module FIM de Wazuh utilise deux bases de données pour collecter les événements FIM, comme la création, la modification et la suppression de fichiers. L'une est une base de données locale basée sur SQLite sur le point de terminaison surveillé. Celle-ci est synchronisée avec l'autre base de données des agents sur le serveur Wazuh. Le serveur wazuh gère une base de données pour chaque agent, en utilisant l'ID de l'agent pour identifier la base de données. Toute création, modification ou suppression de fichiers, déclenche des alertes envoyées au serveur. On aura donc une détection rapide des modifications non autorisées. Dans notre cas, la configuration est basée sur les répertoires sensibles aux changements.

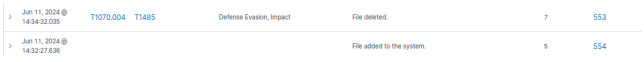

Figure 8. Simulation d'ajout et de suppression d'un fichier au niveau de l'IDS LAN : une alerte de niveau 5 pour l'ajout et de niveau 7 pour la suppression.

5.4.3 Détection des logiciels malveillants: La surveillance des fichiers et répertoires ne suffit pas, c'est pourquoi nous complétons notre solution par la fonctionnalité de détection de malwares. La détection de malwares est le processus d'analyse d'un système informatique ou d'un réseau pour détecter l'existence de logiciels et de fichiers malveillants. La solution proposé implémente différentes stratégies de détéction de logiciels malveillants, en utilisant soit VirusTotal, Yara ou bien Rootcheck.

- VirusTotal : Wazuh détecte les fichiers malveillants grâce à une intégration avec VirusTotal, une puissante plateforme regroupant plusieurs produits antivirus et un moteur d'analyse en ligne. La combinaison de cet outil avec notre module FIM constitue un moyen efficace d'inspecter les fichiers surveillés afin d'en détecter le contenu malveillant.(Voir Figure 6)
- Yara : On a combiné les capacités du module Wazuh FIM avec YARA pour détecter les logiciels malveillants. YARA est un outil open source qui identifie et classifie les artefacts de logiciels malveillants sur la base de modèles textuels ou binaires. Ces modèles sont des indicateurs trouvés dans les échantillons de logiciels malveillants et sont définis dans le fichier de règles de YARA. La communauté YARA met à jour le fichier de règles YARA pour y inclure les nouvelles signatures de logiciels malveillants.
- Module Rootcheck : Wazuh utilise le module Rootcheck pour détecter les anomalies susceptibles d'indiquer la présence de logiciels malveillants dans un terminal. Par défaut, les analyses Rootcheck sont exécutées toutes les 12 heures. Cette dernière peut être personnalisée pour s'adapter à des situations différentes.

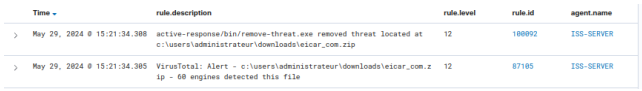

Figure 9. Détection d'un fichier malveillant avec VirusTotal et mise en œuvre de la contre-mesure de suppression.

5.4.4 Évaluation de la configuration de sécurité: Le module d'Évaluation de la Configuration de Sécurité (SCA, Security Configuration Assessement) de Wazuh vérifie que les systèmes respectent des normes de configuration prédéfinies pour le système. Il effectue des scans pour détecter les mauvaises configurations et recommande des actions correctives. Les scans évaluent divers paramètres, tels que les fichiers, les répertoires, les processus en cours d'exécution, et recommandent des actions telles que la modification des configurations de mots de passe ou la désactivation des services inutiles ou l'ajout d'autres services pour renforcer la sécurité et assurer que le réseau respecte les bonnes pratiques de sécurité. Cette action est recommandée après avoir effectué la configuration initiale du réseau, afin de permettre une bonne préparation de la plateforme ainsi que de l'infrastructure avant le lancement des inscriptions.(Voir Figure 7)

Figure 10. Évaluation de la configuration de sécurité avec affichage des recommandations ainsi que des pourcentages de bonnes pratiques requises.

5.4.5 Détection de vulnérabilité: Les agents Wazuh collectent périodiquement une liste des applications installées sur les endpoints et l'envoient au serveur Wazuh, où elle est stockée dans des bases de données SQLite. Le serveur Wazuh construit une base de données globale de vulnérabilités en récupérant des CVE (Common vulnerability and explorer) de plusieurs sources publiques comme Canonical, Red Hat, Debian, Arch Linux, la NVD, et le feed Wazuh pour les mises à jour de sécurité Microsoft et Amazon Linux. Cette base est mise à jour régulièrement.

Processus de Détection : Le module de détection des vulnérabilités compare les versions des applications inventoriées avec les CVE de la base de données pour identifier les packages vulnérables. Des alertes sont générées lors du scan initial et à chaque

détection de nouvelles vulnérabilités ou de corrections. Les résultats des scans sont stockés dans un inventaire propre à chaque agent, permettant aux utilisateurs de suivre les vulnérabilités détectées et non résolues.

Cette action est recommandée au début(avant le lancement), et à la moitié des inscriptions (pendant la période avant la deuxième ouverture), cela a pour but de diminuer la charge des scans et profiter d'une sécurité maximale.

5.4.6 Envoi d'alerte par mail: Wazuh inclut une fonctionnalité d'envoi d'alertes par mail, permettant aux administrateurs de recevoir des notifications en temps réel sur les événements critiques et les anomalies détectées par le système.

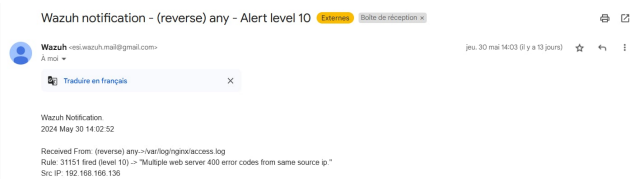

Figure 11. Alerte envoyée par e-mail en utilisant l'adresse e-mail introduite dans le fichier de configuration.

5.4.7 Réponse active: L'Active Réponse dans Wazuh permet l'automatisation des actions en réponse à des alertes de sécurité spécifiques, déclenchées par des critères prédéfinis comme l'ID de règle, le niveau d'alerte ou le groupe de règles. Cette fonctionnalité offre la possibilité d'exécuter des commandes ou des scripts en réponse à des événements de sécurité, il existe des scripts prédéfinies et comme on a aussi la possibilité de définir nos propres scripts.

Nous avons personnalisé d'autres scripts d'Active Response pour la suppression de malwares et le blocage d'adresses IP en cas de détection de SQL Injection, XSS Injection, attaque par force brute et attaque par déni de service (DoS). Les détails des attaques sont expliqués dans la section "Évaluation de la solution".

6 Évaluation de la solution

Pour évaluer l'efficacité de notre SIEM, nous avons réalisé une série d'attaques simulées visant différents aspects de notre infrastructure. Ces attaques ont été soigneusement choisies pour tester la détection et la réponse du SIEM face à diverses menaces. Les principales catégories d'attaques sont:

- Attaques visant le systèmes(Voir Table 10).
- Attaques visant les serveurs(Voir Table 11).
- Attaques visant les sites web(Voir Table 12).

6.1 Réaction de notre système de sécurité face à ses attaques

Pour chaque attaque simulée, notre SIEM a été configuré pour réagir de manière appropriée afin de minimiser les impacts. Voici les mesures spécifiques prises pour chaque type d'attaque:

- Blocage d'IP : Pour contrer les attaques de force brute, de déni de service (DoS) et les injections SQL/XSS, nous avons activé le script « firewall-drop » sur Wazuh afin de bloquer les adresses IP malveillantes. Cette action a empêché les attaquants de poursuivre leurs tentatives après plusieurs

Table 10
Attaques visant le systèmes et leurs descriptions.

Attaque	Description
Force Brute	Classée parmi les principales menaces selon OWASP, cette attaque consiste à essayer différentes combinaisons de noms d'utilisateur et de mots de passe jusqu'à trouver une combinaison valide. Nous avons simulé cette attaque pour tester la robustesse des systèmes de connexion et la capacité de notre SIEM à détecter ces tentatives répétées. Outils utilisé : HYDRA.
Trojan	Les Trojans sont fréquemment utilisés pour obtenir un accès non autorisé aux systèmes. Nous avons créé un Trojan et l'avons inséré dans un fichier PDF, envoyé par e-mail à la cible. Une fois ouvert, le Trojan établit une connexion inverse TCP permettant un accès à distance au système. L'objectif était de vérifier la capacité du SIEM à détecter et bloquer les logiciels malveillants.

Table 11
Attaques visant les serveurs et leurs descriptions.

Attaque	Description
Déni de Service (DoS)	L'attaque DoS, classée parmi les plus dévastatrices, vise à saturer les ressources du serveur en envoyant un grand nombre de requêtes http incomplète , le rendant ainsi indisponible pour les utilisateurs légitimes. Nous avons simulé cette attaque pour tester la capacité du SIEM à détecter et à réagir aux tentatives de saturation du serveur. Outils utilisé : Slowloris.

échecs. De plus, cette mesure a été renforcée par l'intégration de AbuseIPDB, une base de données recensant les adresses IP malveillantes. En cas de correspondance, l'adresse IP est automatiquement bloquée.

- Suppression de fichier malveillant : Cela permet de détecter et de supprimer automatiquement les fichiers identifiés comme malveillants sur les systèmes surveillés. Cette fonctionnalité contribue à renforcer la sécurité en éliminant rapidement les menaces potentielles et en limitant leur propagation dans l'environnement informatique.

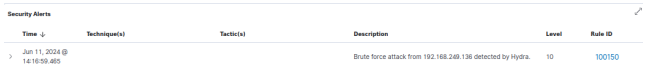

Figure 12. Détection d'une attaque par force brute sur l'application web.

Figure 13. Détection d'une attaque par force brute sur la machine hôte.

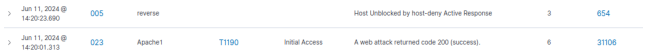

Figure 14. Tentatives d'attaques DoS.

Table 12
Attaques visant le systèmes et leurs descriptions: Pour tester la sécurité de notre SIEM face aux attaques web, nous avons installé DVWA (Damn Vulnerable Web Application) sur un serveur Apache. DVWA est une application web délibérément vulnérable conçue pour aider les professionnels de la sécurité à tester leurs compétences et leurs outils dans un environnement légal.

Attaque	Description
Injection SQL	Classée dans le top des vulnérabilités selon OWASP, l'injection SQL permet d'insérer des requêtes SQL malveillantes dans les champs de saisie de l'application web pour accéder ou manipuler les données de la base. Nous avons réalisé cette attaque sur DVWA pour vérifier si le SIEM peut détecter et bloquer ces requêtes malveillantes.
Cross-Site Scripting(XSS)	Souvent classée 3eme selon OWASP en 2021 , l'attaque XSS permet à un attaquant d'injecter des scripts malveillants dans les pages web, qui sont ensuite exécutés par les navigateurs des utilisateurs. Cette attaque a été testée sur DVWA pour évaluer la capacité du SIEM à détecter et à prévenir ces scripts malveillants.
Brute Force	Similaire à l'attaque visant les systèmes, cette attaque cible les formulaires de connexion du site web pour deviner les identifiants des utilisateurs. Nous avons utilisé DVWA pour vérifier la robustesse du SIEM en termes de détection de tentatives d'accès non autorisées..

7 Outils de mise en oeuvre et d'intégration

7.1 Besoins physiques:

Table 13
Besoins en terme de RAM et Espace Disque pour chaque outil implémenté.

Point	RAM	Espace
IDS	4 Go	50 Go
PfSense	2 Go	20 Go
Serveur Apache	2 Go	30 Go
Seveur IIS	2 Go	30 Go
Machine Admin	2 Go	50 Go
SIEM	8 Go	100 Go
Nginx	1 Go	20 Go

7.2 VMware Workstation:

VMware Workstation est un logiciel de virtualisation permettant de créer et de gérer des machines virtuelles sur un ordinateur hôte. Son rôle dans notre projet est crucial, ce dernier se résume par les points suivants:

- Création de machines virtuelles: VMware Workstation permet de créer plusieurs machines virtuelles sur un même ordinateur physique, chacune avec son propre système d'exploitation et ses propres ressources matérielles.
- Personnalisation du réseau: On peut configurer des réseaux virtuels complexes en utilisant les fonctionnalités de mise en réseau de VMware Workstation. Cela nous permet de simuler des environnements réseau variés pour répondre aux besoins spécifiques de notre projet.

- Compatibilité avec GNS3: GNS3 est une plateforme de modélisation de réseaux qui peut être utilisée en conjonction avec VMware Workstation. En connectant des routeurs virtuels GNS3 à des machines virtuelles VMware Workstation, nous pouvons créer des topologies réseau sophistiquées pour tester et déployer nos solutions.

7.3 GNS3:

GNS3 est une plateforme de modélisation de réseaux qui permet de créer des topologies réseau virtuelles en utilisant des équipements réseau virtuels tels que des routeurs, commutateurs et pare-feu. Son rôle dans notre projet a été essentiel pour plusieurs raisons :

- Définition de la topologie réseau: Il nous a permis de concevoir et de définir la topologie réseau de notre projet. En utilisant son interface conviviale, nousa vions pu ajouter et configurer des périphériques réseau virtuels pour représenter notre infrastructure réseau.
- Interconnexion des machines virtuelles: Grâce à GNS3, nous avions pu interconnecter les différentes machines virtuelles configurées sur VMware Workstation déployées sur des machines physiques distinctes. En établissant des liaisons entre les périphériques virtuels de GNS3 et les machines virtuelles de VMware Workstation, nous avons créé un environnement réseau intégré et fonctionnel.
- Utilisation des points d'accès: GNS3 a facilité l'interconnexion des machines physiques en utilisant des points d'accès. Ces points d'accès ont servi de passerelles pour relier les équipements physiques à notre topologie réseau virtuelle, permettant ainsi une communication transparente entre les machines virtuelles et physiques.

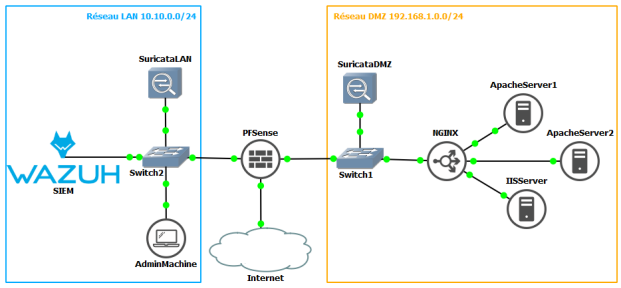

Figure 15. Topologie d'architecture réseau proposée basée sur une DMZ sur GNS3.

7.4 Point d'accés mobile:

Nous avons utilisé des points d'accès mobiles pour permettre la connexion de notre topologie séparée sur trois machines, en raison des performances et des limitations de ressources physiques. Ces points d'accès représentaient les liaisons entre les différents composants configurés virtuellement au niveau de GNS3.

8 Conclusion

En conclusion, l'implémentation d'un SIEM offre une approche proactive pour la gestion de la sécurité de notre organisation. En consolidant et en corrélant les données de sécurité à partir de diverses sources, le SIEM fournit une visibilité accrue sur les activités suspectes et les menaces potentielles. Grâce à l'automatisation des processus de détection et de réponse, nous pouvons réduire les temps de réponse aux incidents et atténuer les risques de sécurité. Cependant, il est essentiel de maintenir une surveillance continue de notre infrastructure de sécurité et d'ajuster notre SIEM en fonction de l'évolution des menaces et des besoins de l'organisation. En investissant dans la mise en œuvre d'un SIEM solide, nous renforçons notre posture de sécurité et nous nous positionnons pour faire face aux défis de sécurité actuels et futurs.

Remerciements

Nous tenons à exprimer notre gratitude envers Monsieur Hamani et Monsieur Amrouche pour leur soutien précieux et leurs conseils avisés tout au long de ce projet. Nous remercions également l'École Nationale Supérieure d'Informatique pour avoir fourni un environnement propice à la recherche et à l'apprentissage. Nos remerciements vont également à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Références bibliographiques

1. "Statistiques Outil SIEM", Gartner, 2024, https://www.gartner.com/reviews/market/security-information-event-management.
2. "Les meilleurs outils SIEM pour 2024 : Classement des fournisseurs et des solutions", Tim Keary, Comparitech, 2024, https://www.comparitech.com/net-admin/siem-tools/.
3. "Qu'est-ce qu'un SIEM?", Splunk, 2024, https://www.splunk.com/fr_fr/data-insider/what-is-siem.html.
4. "Gestion des informations et des événements de sécurité (SIEM) : analyse, tendances et utilisation dans les infrastructures critiques", Gustavo González-Granadillo, Susana González-Zarzosa et Rodrigo Diaz. Alexios Mylonas, rédacteur académique, et Nikolaos Pitropakis, rédacteur académique, National Center for Biotechnology Information, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8309804/#sec1-sensors-21-04759title.
5. "SOC : Security Operations Center", Synapsys Groupe, https://synapsys-groupe.com/blog/soc-security-operations-center/.
6. "Comprendre les avantages et les limites du SIEM", Auteur(s), IT Social, 2021, https://itsocial.fr/tribunes/tribunes-par-thematique/ae-cybersecurite/comprendre-les-avantages-et-limites-du-siem/.
7. "Différents types de journaux dans SIEM et leurs formats de journaux", Manage Engine Log360, https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html.
8. "Cybersécurité and Big Data : comprendre l'intérêt et les limites du SIEM", Juvénal JVC, https://www.data-transitionnumerique.com/cybersecurite-siem/.
9. "Challenges and Directions in Security Information and Event Management (SIEM)", IEEE, 2018, https://www.data-transitionnumerique.com/cybersecurite-siem/.
10. "Installation et Configuration Suricata", https:

//suricata.io/documentation/.
11. "Installation et Configuration PFsense", https://www.pfsense.org/getting-started/.
12. "Installation et Configuration SIEM Wazuh", https://documentation.wazuh.com/current/index.html.
13. "Installation et Configuration d'un reverse proxy NGINX", https://nginx.org/en/docs/.
14. "Installation et Configuration des serveurs apache", https://httpd.apache.org/docs/.