République Algérienne Démocratique Et Populaire
Ministère De L'enseignement supérieur Et De La Recherche Scientifique
Université Abderrahmane Mira - Bejaia
Faculté des sciences éxacte
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du Diplôme de Master en Informatique

Option : Administration et Sécurité des Réseaux

Etude d'un cas de mise en place d'un système de gestion des informations et des événements de sécurité (SIEM)

Réalisé par :

- ⋆ **Mr. YOUSFI L'hadi**
- ⋆ **Mlle. MEKHNECHE Lynda**

Encadré par :

Mr. BENNAI Yani Athmane

Membres de jury :

Soutenu le 26 Juin 2023 devant le jury composé de :

Président	**Mr. SADI Mustapha**	**Université A MIRA-BÉJAIA**
Examinateur	**Mr. DJEBBARI Nabil**	**Université A MIRA-BÉJAIA**

Promotion 2022 - 2023

REMERCIEMENTS

En premier lieu, nous tenons à exprimer notre gratitude envers le Dieu tout-puissant de nous avoir donné le courage, la santé et la volonté de mener à bien ce travail.

Nous souhaitons exprimer nos sincères remerciements à M. Bennai, notre directeur de mémoire, pour son encadrement de qualité, sa gentillesse, ses précieuses suggestions et le temps qu'il nous a consacré. Nous sommes reconnaissants de la confiance qu'il a placée en nous et de l'opportunité qui nous a été offerte de travailler sous sa direction.

Nous tenons également à remercier sincèrement les membres du jury d'avoir accepté d'examiner et de juger notre travail. Leur expertise et leurs commentaires constructifs ont contribué à l'amélioration de notre projet.

Dédicace :

Je dédie ce travail à :

Du fond de mon cœur, je dédie ce travail à tous ceux qui me sont chers :

À ma très chère mère :

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien-être. Je vous remercie pour tout le soutien et l'amour que vous m'avez porté depuis mon enfance, et j'espère que votre bénédiction m'accompagne toujours.

À mon très cher père :

Ce travail est dédié à mon père, qui m'a toujours poussé et motivé dans mes études. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie.

À mes chers frères Yacine, Halim et ma sœur Nadia, ainsi qu'à mon oncle Houcine et Hakim et toute leurs famille :

Je tiens à vous remercier pour votre encouragement, votre attachement et surtout pour votre patience et votre disponibilité dans les moments les plus difficiles de ma vie.

À ma binôme Lynda et à toute sa famille :

Je vous suis reconnaissant pour votre soutien et votre collaboration précieuse tout au long de ce projet.

À tous mes amis :

Je souhaite exprimer ma gratitude à tous mes amis qui ont toujours été présents pour moi, m'encourageant et me motivant à donner le meilleur de moi-même.

L'hadi

Dédicace

Je dédie ce travail à :

A ma très chère mère

Maman tu as été la lumière qui a éclairé mon chemain tout au long de ma vie et de mes études.Tes priers tes encouragement inlassables tes sacrifices et ton soutien inconditionnel ont été des piliers essentils de ma résussite.Merci du fond du coeur pour tout ce que tu as fait et continues de faire pour moi.Quoique je diserai les mots sont peu pour exprimer le respect et l'amour éternel que je tien a toi maman.Que dieu te garde pour nous.Je t'aime plus que les mots ne peuvent t'exprimer.

A mon très cher père

Papa tu as été mon guide et mon modèle tout au long de ma vie et mes études,tu m'as encouragé à poursuivre mes reves et à croire en mes capacités.Tu as fait d'innombrables sacrifices pour moi et pour toute la famile, tu as travaillé sans relache pour m'offrir les meilleurs opportunités pour m'assurer une éducation de qualité et me donner les outils nécessaire pour résssire dans la vie, tu es mon héros.Que dieu te garde pour nous.Je t'aime plus que les mots ne peuvent t'exprimer.

A mes chers frères **Lyes,Idir** et à ma chère sœur **Sonia**, je vous remercie pour vos soutiens indéfectible,votre fierté et votre confiance en moi qui ont été des moteurs pour ma réussité Que dieu vous donne santé, bonheur et beaucoup de succès.Je remercie le dieu pour votre existance dans ma vie.

A la mémoire de mes chères grands-mères et grand pères

Que dieu les accueils dans son veste paradis.

A mon binôme **L'hadi** ainsi qu'à toute sa famille.

A tous **mes proches**,**mes chers voisins qui son ma deuxieme famille** , **mes amis/es Saliha**,**Djida**,**Djadja**,**Tarik** et à tous ceux qui m'ont toujours encouragé et étaient à mes cotés.

A tous ceux que j'aime et qui m'aiment.

Je vous dis merci.

Lynda

Sommaire

Table des figures

Table des figures

Acronymes

SI	**S**ystème d'**I**nformation
IP	**I**nternet **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
SCTP	**S**tream **C**ontrol **T**ransmission **P**rotocol
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
FDDI	**I**nternet **C**ontrol **M**essage **P**rotocol
IPS	**I**ntrusion **P**revention **S**ystem
IDS	**I**ntrusion **D**etection **S**ervices
DoS	**D**enial **O**f **S**ervices
BSoD	**B**lue **S**creen **o**f **D**eath
SQL	**S**tructured **Q**uery **L**anguage
HIDS	**H**ost s**I**ntrusion **D**etection **S**ystem
NIDS	**N**etwork **I**trusion **D**etection **S**ystem
IDS	**I**ntrusion **D**etection **S**ystem
IPS	**I**ntrusions **P**revintion **S**ervices
DMZ	**D**emilitarized **Z**one
VPN	**V**irtual **P**rivate **N**etwork
IPSec	**I**nternet **P**rotocol **S**ecurity
SSL	**S**ecure **S**ockets **L**ayer
TLS	**T**ransport **L**ayer **S**ecurity
SSH	**S**ecure **Sh**ell
PKI	**P**ublic- **K**ey **I**nfrastructure
PCI DSS	**P**aiement **C**ard **I**ndustry **D**ata **S**écurity **S**atndard
SOC2	**S**ystem and **O**rganisations **C**ontrôle **2**
CLF	**C**ommon **L**og **F**ormat
ELF	**E**xtended **L**og **F**ormat
CSV	**C**omma-**S**eparated **V**alues
JSON	**J**avaScript **O**bject **N**otation
XML	**E**xtensible **M**arkup **L**anguage
SIEM	**S**ecurity **I**nformation and **E**vent **M**anagement.
SOC	**S**ecurity **O**peration **C**enter
SIM	**S**ecurity **I**nformation **M**anagement
SEM	**S**ecurity **E**vent **M**anagement
ELK Stack	**E**lasticsearch **L**ogstash **K**ibana Stack
UBA	**U**ser **B**ehavior**A**nalytics

Prelude OSS	**P**relude **O**pen **S**ource **S**iem
OSSIM	**O**pen **S**ource **S**ecurity **I**nformation **M**anagement
GNS3	**G**raphical **N**etwork **S**imulateur

Introduction général

Dans le contexte actuel des entreprises, où la manipulation automatisée des données et des systèmes d'information sous un environnement numérique joue un rôle central, la sécurité informatique est devenue une problématique majeure. Les tentatives de cyberattaques continuent de croître en ampleur et en sophistication, mettant en péril la confidentialité, l'intégrité et la disponibilité des données critiques. Les niveaux de sécurité traditionnels reposent souvent sur des solutions ponctuelles qui ne fournissent qu'une vision partielle de la sécurité globale, laissant les systèmes vulnérables aux attaques sophistiquées.

Face à cette réalité, il devient essentiel pour les entreprises d'ajuster leurs systèmes et leurs politiques de sécurité, ainsi que de déployer des outils de supervision continue en temps réel. C'est là que le SIEM (Security Information and Event Management) entre en jeu en offrant aux équipes SOC (Security Operations Center) une visibilité claire et détaillée sur les activités de sécurité suspectes dans les systèmes d'information. Il permet une analyse approfondie des événements de sécurité, la reconstitution des séquences d'attaques et la prise de mesures appropriées pour une réponse rapide et efficace aux incidents de sécurité.

Dans ce contexte, notre travail vise à étudier et mettre en œuvre une solution de gestion des informations et des événements de sécurité (SIEM) qui puisse répondre aux besoins spécifiques de l'entreprise. Pour atteindre cet objectif, nous avons structuré le mémoire de la manière suivante :

- Le premier chapitre est consacré à la présentation de l'organisme d'accueil, SONATRACH.
- Dans le deuxième chapitre, nous détaillerons la mise en œuvre du SIEM et nous présenterons une étude comparative pour mettre en évidence le choix de Splunk comme solution optimale.
- Le troisième chapitre de notre travail se concentre sur le déploiement de la solution Splunk Enterprise dans l'environnement de simulation proposé.

Chapitre 1

Présentation de l'organisme d'acceuil et Etude de l'existant

1.1 Introduction

La multiplication des réglementations de conformité et les menaces de sécurité informatique en perpétuelle évolution font peser une lourde pression sur les entreprises du monde entier. Pour protéger leur activité, elles ont besoin d'une surveillance en temps réel des écarts de conformité et des violations de sécurité. Nous avons ainsi fait le choix d'effectuer notre stage au niveau de l'entreprise Sonatrach, en vue de trouver une solution pour améliorer le niveau de sécurité de leur système informatique en temps réel.

Dans ce chapitre, nous avons pour objectif de présenter une vue d'ensemble de Sonatrach, en mettant en évidence ses services organisationnels et leur fonctionnement. Nous abordons ensuite une étude descriptive approfondie du parc informatique de l'entreprise, y compris les équipements matériels, logiciels et systèmes qui gèrent son bon fonctionnement et son infrastructure réseau. Enfin, nous proposons une contribution visant à renforcer les contrôles de sécurité qui pourront être appliqués pour améliorer la protection des données. Pour cela, nous décrivons le contexte du projet, la problématique à résoudre et le travail à réaliser.

1.2 Présentation de l'organisme d'acceuil

1.2.1 Présentation de SONATRACH

La SONATRACH, également connue sous le nom de "Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures", est une entreprise algérienne qui exerce des activités de recherche, d'exploitation, de transport par canalisation, de transformation et de commercialisation de pétrole et de gaz naturel, ainsi que de leurs dérivés [7]. Elle est considérée comme un acteur majeur de l'industrie pétrolière, souvent surnommée la "major africaine". Elle est classée comme la première entreprise d'Afrique.

En outre, elle est impliquée dans d'autres secteurs tels que la production d'électricité, les énergies nouvelles et renouvelables, le dessalement de l'eau de mer, etc. Elle emploie plus de 50 000 employés.

1.2.2 Activités de base et missions de SONATRACH

La société SONATRACH élabore régulièrement ses visions et des objectifs dans le cadre de son plan stratégique, les objectifs de la société comprennent notamment :

- ▷ Mettre en œuvre les politiques et stratégies définies par l'entreprise, ainsi que de gérer et développer les installations de raffinage dans le cadre de l'activité aval.
- ▷ Accélérer sa transformation digitale en exploitant toutes sortes de technologies afin d'améliorer l'efficacité fonctionnelle, optimiser les couts et améliorer la qualité des services .
- ▷ Garantir la sécurité de ses travailleurs et une exploitation efficace en utilisant des meilleures pratiques environnementales.
- ▷ La société est constamment à la recherche d'investissements pour développer ses activités et augmenter la production d'hydrocarbures.
- ▷ Renforcer sa recherche et son développement pour trouver de nouvelles solutions pour la production d'hydrocarbure .
- ▷ Améliorer l'expertise locale en développent les compétences et l'expertise de ses travailleurs pour renforcer l'industrie pétrolière et gazière nationale .

1.2.3 Branches de SONATRACH

SONATRACH est divisé en cinq branches différentes qui sont les suivantes :

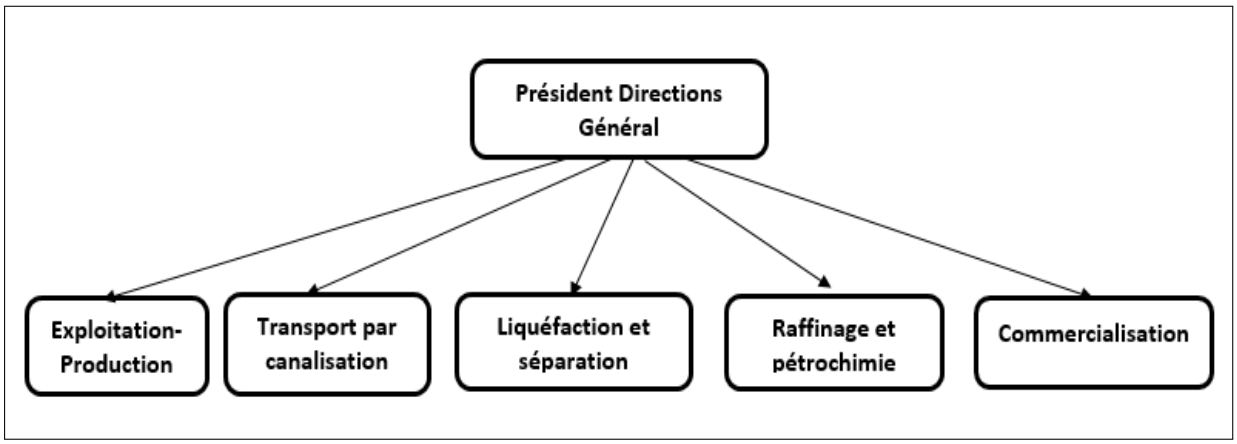

FIGURE 1.1 – Organigramme des branches de SONATRACH

Notre étude se concentre sur l'une de ces branches, qui est la branche de transport par canalisation sur laquelle nous allons présenter plus de détails.

1.2.4 Missions de la branche de transport par canalisation

- ▷ Planifier l'installation des pipelines pour répondre aux besoins de transport de SONATRACH.
- ▷ S'assurer que les canalisations sont construites conformément aux normes de sécurité et de qualité établies.
- ▷ Assurer la maintenance régulière des canalisations pour garantir leur bon fonctionnement et leur sécurité afin de minimiser les perturbations dans le transport des produits.
- ▷ Surveiller en permanence les pipelines grâce à des systèmes de surveillance et de détection avancées mis en place pour détecter les fuites et les problèmes de sécurité, et assurer le fonctionnement efficace des canalisations.
- ▷ Gérer et exploiter les sauvegardes et les canalisations de transport d'hydrocarbures.
- ▷ Gérer l'interface de projet internationaux du groupe ou en partenariat.

1.2.5 Présentation de la RTC de Bejaia

La Région Transport Centre (RTC) est l'une des sept Régions de Transport par Canalisations (TRC) des hydrocarbures. Elle possède un important réseau de canalisations qui s'étend sur plusieurs centaines de kilomètres et qui relie les principales installations de la région. La RTC est chargée de transporter le pétrole brut et les produits raffinés des installations de production vers les terminaux d'exportation ou les centres de distribution locaux, ainsi que de gérer et d'entretenir les infrastructures de transmission telles que les stations de pompage, les réservoirs de stockage et les pipelines.

1.2.6 Structure de la DRGB

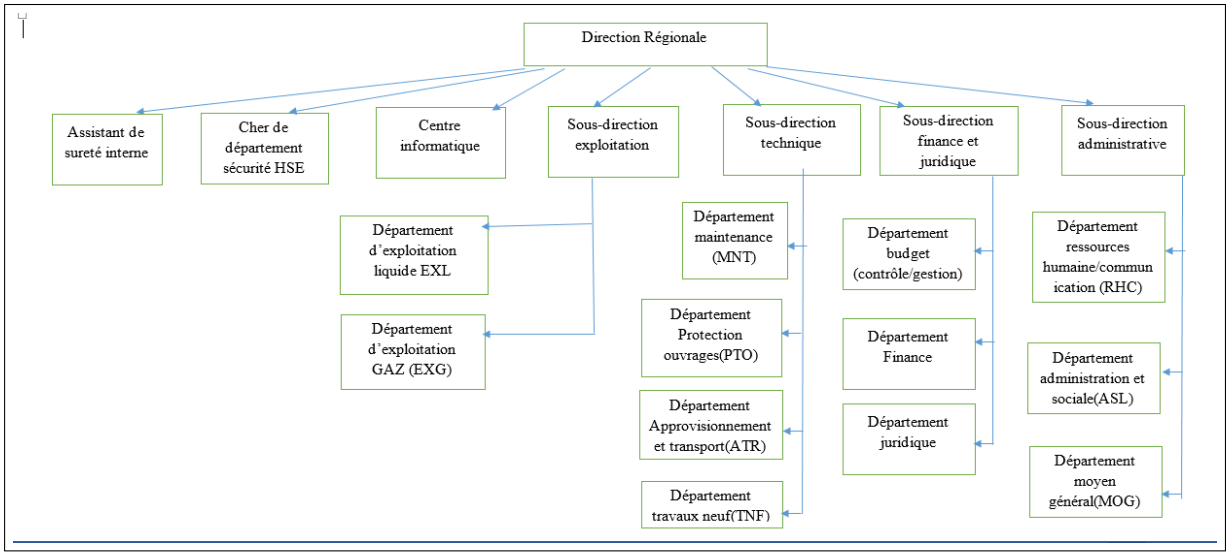

FIGURE 1.2 – Organisation de la direction régionale de Béjaïa

1.2.7 Présentation du centre informatique

Le Centre Informatique est l'un des cinq départements de la Direction de Planification, elle-même l'une des composantes du Pôle de Raffinage faisant partie de Sonatrach.

Le Centre Informatique est un élément indispensable pour l'activité d'une entreprise. Il est nécessaire de gérer et garantir l'accès en temps réel aux informations. Le parc informatique peut être composé de plusieurs éléments, qui peuvent varier d'une entreprise à l'autre. Comme toutes les organisations économiques, SONATRACH à Béjaia dispose de nombreux parcs informatiques. Le parc informatique de la DRGB de Béjaia regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des régions de la division transport.

- **Organisation structurelle :**

  Le centre informatique est partitionné en trois services fonctionnels tels qu'ils sont schématisés ci-dessous :

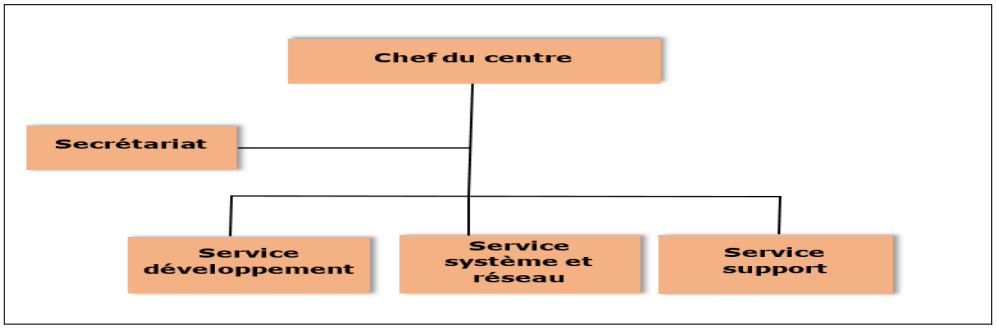

FIGURE 1.3 – Centre informatique

▷ **Organisation Fonctionnels :**

Chaque service constituant l'organisation structurelle de centre informatique de cette entreprise assure un ensemble déterminé de taches qui définissent son fonctionnement, on définit chaque un ces derniers ci-dessous :

a) **Service système et réseaux :** Ce service est un élément indispensable du centre informatique. Le personnel de ce service est chargé de choisir les équipements informatiques et les logiciels nécessaires pour chaque poste de travail. Ils s'occupent également de l'installation et de la configuration système initiales sur ces équipements. Après une planification et une construction du réseau, des équipes techniques s'engagent à le mettre en œuvre dans la totalité de l'entreprise. Ils veillent à garantir la haute disponibilité du service en surveillant les performances réseau et en assurant les objectifs de sécurité sur leur système informatique en mettant en place des politiques de sécurité approfondies.

b) **Service base de données et logiciels :** Les équipes de ce service sont chargées en premier lieu de la conception, de la mise en œuvre et du développement de nouvelles versions logicielles ou applicatives de gestion et de manipulation de données du système informatique de l'entreprise. Elles formalisent également les utilisateurs sur les bonnes pratiques de manipulation des logiciels informatiques. Ces équipes s'occupent également de l'installation, de la configuration et de l'exploitation du SGBD et de ses bases, ainsi que d'assurer l'intégrité des données introduites par les utilisateurs, etc.

c) **Service supports techniques :** Ce service est responsable de l'installation des logiciels de gestion, technique et bureautiques, ainsi que d'assurer l'assistance en cas de problèmes logiciels et matériels pour garantir que les utilisateurs d'un système puissent continuer à profiter de la disponibilité de l'ensemble de ses composants pour l'accomplissement de leurs tâches.

1.3 Etude de l'existant

1.3.1 Présentation du réseau SONATRACH

Dans le but de régir des activités informatiques collectives, de centraliser et de répartir des tâches et des ressources à travers le système, SONATRACH dispose d'un réseau informatique Gigabit Ethernet a 10/100/1000GB/s.

a) **Modèle de conception de l'infrastructure réseau**

Le réseau informatique de SONATRACH est fondé sur un modèle d'architecture hiérarchique et maillé, également appelé LAN Campus, qui implique la division du réseau en trois couches distinctes et n'utilise aucun sous-réseau.

b) **principes du modéle d'un réseau hiearchique**

Le modèle de réseau hiérarchique est une méthode de conception de réseau qui implique l'utilisation de couches fonctionnelles, chacune ayant une tâche spécifique. Ce modèle est conçu pour offrir des performances optimales, une gestion de réseau efficace et une évolutivité. Les principes clés de ce modèle incluent la modularité, la hiérarchie, la redondance, la séparation des fonctions et l'agrégation. La modularité permet une évolutivité et une flexibilité accrues, tandis que la hiérarchie facilite la gestion du réseau et la répartition des tâches. La redondance est utilisée à tous les niveaux pour améliorer la disponibilité et la résilience, et la séparation des fonctions facilite la maintenance et le dépannage. Enfin, l'agrégation réduit la complexité du réseau et améliore les performances globales en permettant l'agrégation des données et des connexions à chaque niveau de la hiérarchie.

c) Modèle structure en couche

Dans le domaine des réseaux, la conception d'une structure réseau hiérarchique est organisée en des couches distinctes, dont chaque niveau hiérarchique détermine des fonctions spécifiques qui définissent son rôle dans les réseaux. [8].

1. **Couche d'accès :**

   Cette couche représente généralement un VLAN de type Ethernet ou token-ring. Elle fournit des points d'extrémité aux terminaux et leur garantit un accès direct de première ligne au réseau. Cette couche fournit une connectivité filaire et sans fil avec une très grande bande passante, afin de pouvoir prendre en charge un pic de trafic . Elle contient également des fonctionnalités et services qui garantissent la sécurité et le bon fonctionnement du réseau, tout en contrôlant les autorisations d'accès déterminées.

2. **Couche de distribution :**

   La couche de distribution sert d'interface entre les sites distants de la couche d'accès et la couche cœur de réseau. Elle assure le regroupement des données de réseaux étendus d'armoires de câblage en vue d'impliquer des fonctions intelligentes de commutation et de routage entre les réseaux locaux virtuels définis au niveau de la couche d'accès, et les règles d'accès (filtrage ACL) pour l'accès au reste du réseau. Ainsi, cette couche assure la haute disponibilité du réseau pour les utilisateurs en limitant les risques de pannes dans des zones plus petites [9] .

3. **Couche cœur :**

   La couche cœur est la partie la plus essentielle d'un réseau évolutif qui permet de centraliser et optimiser la conception. Elle correspond à la dorsale du réseau qui relie et connecte les blocs fonctionnels d'équipements d'un réseau. C'est le point d'extrémité qui relie les périphériques de la couche distribution au reste du réseau.

   Les éléments d'interconnexion qui composent cette couche offrent une vitesse importante de connectivité et un débit binaire utile afin d'optimiser les performances. Les objectifs de ce niveau sont la stabilité et une complexité minimale.

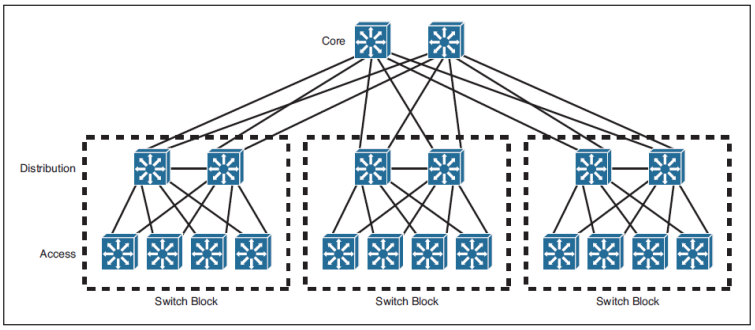

FIGURE 1.4 – Modéle structure en couche

1.3.2 Centre de données

L'entreprise SONATRACH dispose de deux centre de données. un centre de données est un ensemble de serveurs informatiques et d'équipements de stockage de données regroupés dans un même lieu physique. Ces installations sont conçues pour stocker, gérer et traiter de grandes quantités de données de manière efficace et fiable.

1.3.3 Architecture réseau de la RTC de Béjaia

L'infrastructure réseau WAN de Sonatrach est répartie sur plusieurs stations(voir la figure 2.5). Chaque station est dotée d'un réseau LAN (voir la figure 2.6) qui facilite la communication entre les acteurs présents dans chaque station, ainsi que l'utilisation des ressources centralisées situées au siège.

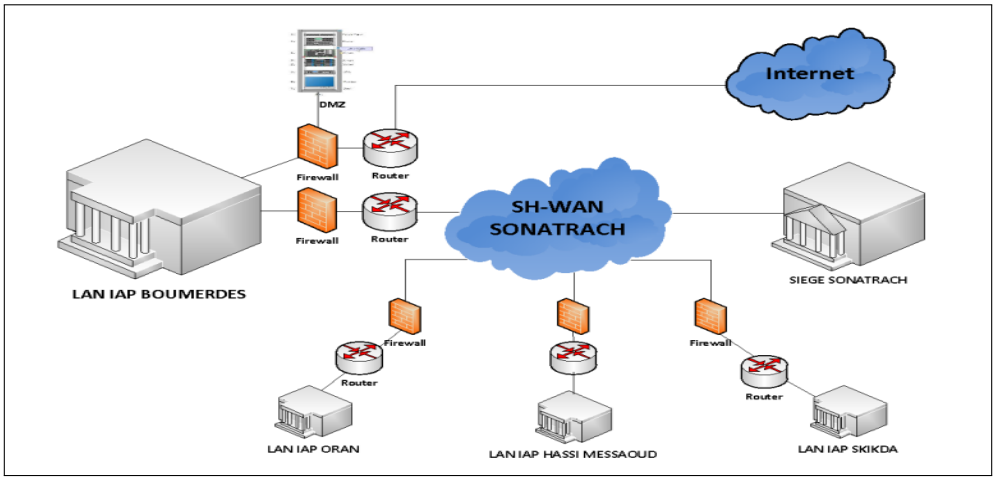

FIGURE 1.5 – Architecture WAN de SONATRACH

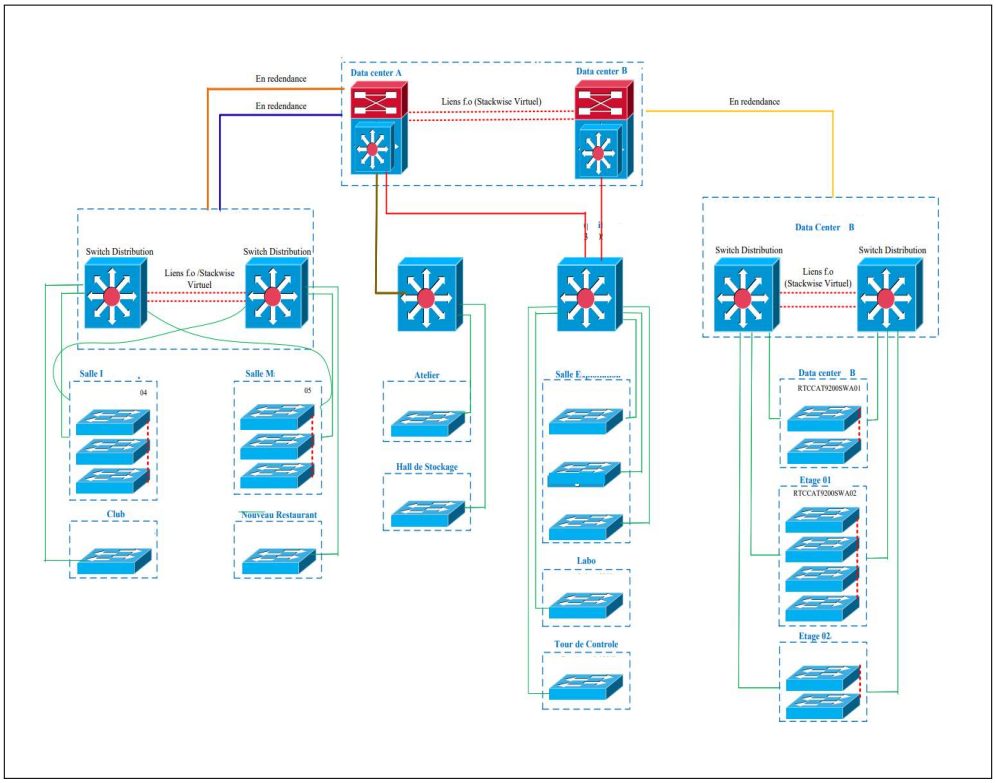

FIGURE 1.6 – Architecture LAN de la TRC-DRGB

1.3.4 Analyse du parc Informatique

a) Aspect système

▷ **Les stations utilisateurs** L'entreprise SONATRACH englobe un parc informatique constitué de plus de 40 postes.

Type	System
Hp	windows 10 + linux
Fujitsu ESPRIMO P420	Windows 11 Entreprise +RedHat 5.7
Alfatron	windows 10 pro
Poste téléphonique(IP Phone 7960)	Android 8.1 oreo
Delle	Windows 7/8.1/10

Table 1.1 – Récapitulatif des stations utilisateurs et des systèmes d'exploitation installés.

▷ **Les stations de travails**

Un nombre important de stations de travail sont mises en place au sein de cette entreprise, des stations de travail sous système d'exploitation Windows 10, utilisées pour les tâches qui nécessitent une puissance de calcul et de traitement importante. Elles sont équipées de matériel de haute performance comme des processeurs multi-core et une grande quantité de RAM, etc.

▷ **Les postes serveurs du parc informatique :** Le réseau informatique de l'organisme campus « Sonatrach TRC Bejaia » comprend huit serveurs sous une structure configurée avec la technologie RAID (pour le principe de stocker des données sur plusieurs espaces de stockage afin de tolérer les pannes et d'augmenter les performances de l'ensemble) dont on définit :

- ◇ **Serveur de fichier :**c'est le serveur hébergeant le service applicatif, utilisant les protocoles (FTP, SMB, CIF, NFS, NCP) pour partager les données à travers les réseaux. Il centralise le stockage des fichiers et des dossiers de l'entreprise et est configuré pour permettre aux utilisateurs de l'entreprise d'y accéder à partir de leurs propres ordinateurs en suivant un contrôle d'accès. Le serveur de fichier utilise les protocoles de sécurité tels que l'authentification, la confidentialité et l'intégrité pour assurer la sécurité des fichiers et des données qu'il sauvegarde.
- ◇ **Serveur de base de données (Oracle) :** sert à stocker, extraire, gérer et interroger les données en recourant au langage SQL.
- ◇ **Serveur de messagerie « Microsoft Exchange » :** il s'agit d'une application du serveur de messagerie collaborative. Son rôle initial est le stockage de courrier électronique. Son utilisation est étendue au calendrier, à la liste des tâches, à la gestion des contacts et à bien d'autres données qui sont partagées entre les utilisateurs.

Type de fourniseur	Role	Capacité
Dell	Voi ip/asterisk	RAM 16 Go
Hp	Serveur AD, DNS, DHCP	RAM 32 Go

Table 1.2 – Récapitulatif des fournisseurs, rôles et capacités des serveurs.

b) Aspect réseau

Dans cette partie, nous allons détailler et définir l'ensemble des équipements réseau utilisés au sein de l'entreprise "SONATRACH".

L'infrastructure de réseau "Sonatrach" locale comporte quatre types de commutateurs Cisco déployés en cascade définis ci-dessous :

- **Gamme commutateur catalyst 2950 :** Série de commutateurs intelligents à configuration fixe empilable, offrant une sécurité intégrée sur le réseau, fournissant de nombreuses fonctionnalités de qualité de service (QOS) avancées et de traitement de flux multicast. L'interface de gestion web fournit des fonctions d'administration facile à utiliser.
- **Commutateurs gamme Catalyst Cisco 3750 :** Série de commutateurs efficaces, permettant de maximiser l'efficacité de l'exploitation des LAN grâce à leur facilité d'utilisation et leur résistance maximale pour les commutateurs compilables. Ce type de commutateur prend en charge un taux de transfert de données jusqu'à 100 Mbits/s, utilise SNMP comme protocole de gestion et QOS, BPDU, STRG, VMPS comme protocole de commutation.
- **Commutateurs gamme Catalyst Cisco 6509 :** Série Cisco 6509 offrant une plateforme haute performance destinée au réseau fédérateur et faisant partie de la classe des commutateurs modulaires. Ils permettent de prendre en charge les réseaux à sécurité intégrée car deux blocs d'alimentation peuvent être installés pour fournir une alimentation redondante. De plus, ils prennent en charge l'alimentation par Ethernet (PoF), qui alimente des terminaux connectés par les câbles réseau.
- **Commutateurs gamme Catalyst Cisco 9200 :** Série de commutateurs Ethernet de couche deux et trois de Cisco, utilisant le système d'exploitation IOS-XE et utilisée dans les entreprises de taille moyenne. Ils sont conçus pour prendre en charge plusieurs types de connexion et sont équipés de fonctionnalités de sécurité avancées.

  Le tableau(2.3) offre un aperçu des différents types de commutateurs, en fournissant des informations sur leur fréquence d'utilisation et leur capacité d'acheminement, ce qui nous permet de mieux comprendre la composition de notre réseau.

Type de commutateur	Nombre d'occurence	capacit´e d'acheminement
Cisco Catalyst 6509	Cinq	40 Gb/s
Cisco C3750	Quatorze	32 Gb/s
Cisco C2950G-24 ports	Cinq	8.8Gb/s
Cisco C2950G -48 ports	Un	13.6Gb/s

Table 1.3 – Récapitulatif des types de commutateurs, occurrences et capacités d'acheminement.

c) Aspect Sécurité

La sécurité est une préoccupation cruciale pour une société comme 'SONATRACH'. Pour cela, elle utilise des mécanismes de sécurité avancés tels que :

▷ **Pare-feu**

Le firewall, aussi appelé pare-feu, utilise des politiques de filtrage et des droits d'accès pour vérifier les accès, que ce soit à partir du réseau Internet vers le réseau de l'entreprise ou du

réseau de l'entreprise vers l'Internet. L'entreprise ''SONATRACH" a mis en place une solution de pare-feu d'entreprise FortiGate nouvelle génération (NGFW).

Un firewall FortiGate effectue une inspection approfondie des paquets pour offrir des performances optimales et une protection avancée, une sécurité multicouche, une visibilité en profondeur ainsi qu'un contrôle granulaire des applications, des utilisateurs et des objets connectés. Autant d'atouts pour se protéger plus simplement des cyberattaques.

▷ **Antivirus**

Le logiciel antivirus est la première ligne de défense contre les menaces et les intrusions les plus élémentaires dans les postes de travail au sein d'une entreprise. L'antivirus Symantec Endpoint Security est installé au sein de l'entreprise SONATRACH. C'est un type d'antivirus qui offre une sécurité inégalée et des performances accrues sur les systèmes virtuels et physiques. Il intègre en toute transparence des technologies de sécurité majeures dans un agent et une console de gestion uniques pour renforcer la protection et réduire le coût total de possession.

Architecture de câblage

Le câblage au sein de "SONATRACH" est structuré pour permettre une interconnexion physique des différents locaux.

On distingue deux types de câblage dans cette entreprise :

— **Le câblage vertical :** Le câblage vertical, également appelé câblage back one, qui relie l'ancien et le nouveau bâtiment ainsi que les différents étages de l'entreprise. Ce type de câblage est souvent réalisé avec des câbles à fibre optique en raison de leur fiabilité, de leur capacité de transmission de données et de leur portée.

— **Le câblage Horizontal :**Le câblage horizontal, qui relie les points de terminaison du réseau aux armoires de télécommunication centrales ou aux routeurs. Ce câblage est limité à une distance maximale de 90 mètres.

1.3.5 Critique de l'existant

L'analyse approfondie de l'infrastructure existante a révélé plusieurs lacunes dans le système de sécurité de l'entreprise. Tout d'abord, les différents outils et terminaux de sécurité sont utilisés de manière isolée, ce qui conduit à un manque de communication entre eux. Lorsqu'un problème se présente, chaque dispositif tente de travailler individuellement sur la situation, mais il est souvent nécessaire de collaborer avec d'autres parties du système, notamment les logs de traces d'événements, pour identifier et neutraliser les menaces.

De plus, l'absence de systèmes de surveillance des risques et de systèmes de gestion automatique des logs entraîne une grave lenteur en termes de temps de réponse et d'analyse des incidents de sécurité

1.3.6 Problèmatique

Le processus d'évaluation et de critique de l'existant de l'entreprise SONATRACH nous a permis de découvrir certains facteurs de faiblesse contribuant à l'échec de la détection d'attaques. Nous allons en exposer certains :

— La grande quantité d'appareils et de logiciels différents utilisés dans l'organisation peut rendre la gestion de la sécurité plus complexe. Les différents appareils et logiciels peuvent avoir des vulnérabilités différentes, des mises à jour de sécurité différentes et des configurations différentes.

— La difficulté d'obtenir une vue globale de la sécurité de l'organisation.

— La difficulté de détecter les attaques sophistiquées affectant plusieurs systèmes (menaces persistantes avancées) ;
— L'énorme quantité de données de journal générées peut rendre les analyses de sécurité difficiles. Les données de journal peuvent contenir des informations précieuses sur les activités de sécurité, mais il est difficile de les trier et de les analyser manuellement.
— La difficulté de trouver des réactions appropriées en cas d'incident de sécurité en raison de l'absence d'un plan de réponse aux incidents clair et efficace. Cela peut entraîner des erreurs et des retards dans la réponse aux incidents. De plus, la gestion de la sécurité est compliquée par le manque de tableau de bord et de rapports d'incidents.

Ces lacunes ont un impact négatif sur la capacité de l'entreprise à détecter, répondre et prévenir certaines menaces de sécurité. Cela souligne l'importance de déployer une solution pour améliorer la sécurité globale du système.

1.4 Objectifs à atteindre

Afin de surmonter les contraintes et problèmes susmentionnés, il est très important d'implémenter une solution de détection, supervision et analyse des événements basée sur les fichiers logs. Cette solution devrait être en mesure de :

— Collecter des données de diverses sources telles que les fichiers logs, les systèmes de détection d'intrusion, les pares-feux, les antivirus, etc.
— Corréler les événements pour détecter les menaces et les incidents de sécurité.
— Stocker les données de sécurité à long terme pour répondre aux besoins de conformité et d'audit.
— Identifier les menaces.
— Offrir les outils nécessaires pour la détection, la signalisation, le suivi et la résolution des problèmes détectés.

1.4.1 Propositions

Dans le but de résoudre le défi consistant à collecter et analyser en temps réel toutes les informations pertinentes générées par les outils de sécurité dans un système centralisé, nous avons proposé la mise en place, l'installation et le déploiement d'une solution SIEM. Cette solution permettra une surveillance et une analyse approfondies des données de sécurité en utilisant des techniques avancées pour identifier rapidement les menaces potentielles et y répondre de manière proactive.

1.5 Conclusion

Le présent chapitre a décrit l'organisme SONATRACH de Béjaia (RTC) en détaillant son infrastructure informatique. Cela permet d'avoir une vision globale du réseau mis en place et des équipements utilisés. Cette analyse nous a également permis de comprendre les lacunes des solutions présentes dans l'entreprise et ainsi de proposer une solution adaptée répondant à ses exigences en termes de sécurité informatique. Dans le chapitre suivant, nous aborderons divers concepts liés à la solution SIEM proposée.

Chapitre 2

Les systèmes de gestion des informations et des événements de sécurité (SIEM)

2.1 Introduction

Les attaquants sont devenus agiles pour "voler sous le radar" en se cachant des contrôles de sécurité [10]. Ils ont recours à des techniques sophistiquées et subtiles, telles que l'exploitation des vulnérabilités de jour zéro et des techniques d'évasion avancées pour éviter d'être détectés [10]. La protection des infrastructures informatiques des entreprises face à ces menaces devient de plus en plus difficile. Ainsi, la plupart des entreprises ont besoin d'un système de gestion des informations et des événements de sécurité (SIEM) intégré dans un centre d'opérations de sécurité (SOC) pour surveiller les événements de sécurité en temps réel, détecter les modèles d'utilisation anormaux et alerter les organisations en cas de besoin. Ce chapitre a donc pour objectif de détailler ces deux composants (SIEM + SOC).

Pour que les SIEM soient efficaces, il est indispensable de mettre en place une stratégie solide de gestion des journaux et des événements de sécurité, ainsi que d'implémenter des processus de réponse aux incidents claire et bien définis. Le SOC est la structure organisationnelle qui permet d'assurer ces fonctionnalités complémentaires. Sa mission est de surveiller et de défendre les systèmes informatiques et les données d'une entreprise contre les cybermenaces. Il s'agit d'un élément clé de la stratégie de cybersécurité d'une organisation qui utilise le SIEM comme outil.

Dans la première section de ce chapitre, nous présenterons une annexe de terminologie qui pourra aider à comprendre ce qu'est le SIEM. Ensuite, nous mettrons en lumière les logs, leurs contenus, leurs types et leur importance. Nous aborderons également le fonctionnement de SIEM et examinerons quelques solutions SIEM payantes et gratuites avant de choisir la meilleure à déployer, et développer son architecture et son fonctionnement. Dans la seconde section, nous parlerons des SOCs.

2.2 SIEM (Security Information and Event Management)

2.2.1 Motivation

Les entreprises, telles que SONATRACH, sont confrontées à des menaces informatiques qui représentent un risque critique de cybercriminalité. Ces menaces sont en constante évolution, se métamorphosent et se diversifient en termes de complexité et de sophistication, car les attaquants utilisent un arsenal d'outils et de techniques très avancées pour échapper à la détection des systèmes de sécurité existants dans l'organisation cible. Les attaquants ne se concentrent pas uniquement sur un système ou un logiciel unique, ils lancent des attaques distribuées sur plusieurs systèmes, ce qui rend la détection encore plus difficile avec l'augmentation du nombre d'équipements et de technologies informatiques et le besoin crucial et croissant en matière de sécurité.

Dans ce contexte, les équipes de sécurité ne sont pas toujours en mesure de prévenir les attaques et sont de plus en plus confrontées à un manque de ressources pour mettre en place des systèmes de sécurité efficaces. Ainsi, il devient difficile de suivre les événements qui se produisent sur le réseau de l'entreprise.

C'est là qu'intervient SIEM, qui est une approche solide pour détecter les menaces, générer des rapports et analyser à long terme les journaux de sécurité. Il apporte un double bénéfice aux entreprises en se servant du centre de contrôle (tableau de bord de visualisation) pour les événements de sécurité de l'information alimentant ainsi le processus de réponse aux incidents de sécurité.Mais aussi comme moyen de supervision et de contrôle d'efficacité des systèmes de sécurité déjà mis en place.

2.2.2 Définitions

Gartner IT Glossary [Gartner Inc. 2018] a défini le SIEM comme suit : « les systèmes SIEM collectent des données pertinentes et effectuent des analyses historiques sur les événements de sécurité à partir d'un large éventail de différents types d'événements ou de sources de données contextuelles. En outre, il prend en charge la création de rapports à des fins de conformité et d'enquête d'analyse criminel en analysant les données historiques stockées provenant des mêmes sources. Les principales fonctionnalités de SIEM sont sa large portée sur les sources d'événements ainsi que sa capacité à corréler et analyser ces événements à travers des sources hétérogènes. » [11].

En se fondant sur cette définition, nous pouvons déduire que SIEM est une extension de la gestion des journaux qui combine la gestion des informations de sécurité (SIM), focalisée sur l'analyse a posteriori, l'archivage, la conformité et le Reporting des informations et la gestion des événements de sécurité (SEM), qui vise à collecter et à traiter des événements en temps réel [12] [13]. Le SIEM représente un système de supervision centralisé qui allie ces deux outils complémentaires pour collecter et analyser les informations et les événements provenant de tous les nœuds et systèmes de sécurité de l'infrastructure technologique d'une organisation, de manière à identifier les incidents de sécurité et les activités suspectes dans un environnement IT. Il offre aux analystes de sécurité une vue complète et centralisée de la posture de sécurité de l'infrastructure IT.

2.2.3 Comparaison entre SIM, SEM et SIEM

Les acronymes SEM, SIM et SIEM ont tendance à semer la confusion chez ceux qui ne sont pas suffisamment familiers avec les processus de sécurité. La racine du problème est la similitude entre SEM et SIM [14]. Cependant, le SIM se concentre sur la collecte des informations depuis différentes sources de journalisation qui peuvent être composées de différents types de données (alertes,instructions,traces, notifications, etc.). Cette collecte est généralement mise en œuvre à travers des agents pré installés sur l'équipement surveillé. Bien évidemment, cette gestion doit être conforme et compatible aux réglementations et aux politiques de sécurité [15]. Les outils SIM gèrent en général tous les journaux et traces d'informations des systèmes, en collectant essentiellement les journaux générés par les applications et les systèmes d'exploitation [13]. Tandis que le SEM est considéré comme une amélioration de SIM, il examine et analyse de plus près et en profondeur des types d'événements spécifiques de ces logs collectés. De plus, il génère des alertes en temps réel aux équipes de sécurité pour accélérer et améliorer les capacités de réaction aux incidents de sécurité, qu'il s'agisse de menaces internes ou externes. Les outils SEM gèrent les événements de sécurité générés par les systèmes de sécurité, tels que les événements générés par l'IDSS, les pares-feux personnels, les scanners, l'IPSS, les pare-feu, etc. Quant à SIEM, il combine les performances de ces deux approches pour offrir des opportunités d'amélioration de la sécurité du système [16] [13].

2.2.4 Missions de SIEM

La première mission d'une solution SIEM est la gestion des logs informatiques, qui consiste à collecter, stocker et analyser en temps réel les données d'événements provenant de diverses sources sur l'ensemble du réseau de l'organisation. Cette technologie peut également s'intégrer à des flux de renseignements sur les menaces tiers pour corréler les données de sécurité internes avec des signatures de menaces précédemment identifiées. En utilisant des analyses avancées pour identifier et comprendre des modèles de données complexes, la corrélation d'événements fournit des informations permettant de localiser et d'atténuer rapidement les menaces potentielles pour la sécurité de l'entreprise. Les solutions

SIEM surveillent également les incidents de sécurité sur tous les utilisateurs, appareils et applications connectés, tout en classant les comportements anormaux lorsqu'ils sont détectés sur le réseau. Enfin, ces solutions sont également utiles pour la gestion de la conformité réglementaire en collectant et en vérifiant les données de conformité sur l'ensemble de l'infrastructure de l'entreprise et en générant des rapports de conformité en temps réel pour différentes normes de conformité [17] [18] [19] [1].

2.2.5 SIEM et la gestion des logs

Le SIEM est un système de gestion de la sécurité qui se concentre sur l'analyse des données historiques des journaux et les alertes en temps réel. Le journal est l'élément clé qui joue un rôle crucial dans le fonctionnement des SIEM. Par conséquent, avant de décortiquer le fonctionnement de SIEM, nous devons d'abord examiner la notion de logs, leurs formats, types, ainsi que leur utilité [20] [21].

A) Que contient un fichier log ?

Les journaux peuvent contenir des informations précieuses sur les activités du système, telles que les tentatives de connexion, les erreurs système, les modifications de configuration et les activités d'utilisateur [22]. Un message journal contient généralement les informations suivantes [22] [23] [24] :

- **L'horodatage :** indique le moment précis où l'événement s'est produit ;
- **Type d'événement :**permet d'indiquer la catégorie de l'évènement (avertissement, erreur, notification,etc.) ;
- **Description de l'événement :** C'est le corps du message qui peut contenir un contexte détaillé sur l'évènement, les données impliquées ainsi que les résultats et les erreurs engendrés.
- **Donnée :** C'est le bloc d'information qui permet d'indiquer la source de l'événement (le processus ou l'utilisateur impliqué), ainsi que les conditions environnementales, etc ;
- **Informations Systèmes :** Représentent l'ensemble des informations supplémentaires sur les ressources système ainsi que les performances d'utilisation.

C) Format d'un fichier log :

Un format de log est un format structuré qui permet aux logs d'être lisibles par la machine et facilement analysables .Cela facilite la recherche des informations utiles dans les journaux et permet de les interpréter plus facilement [25].En utilisant un format de log approprié les logs deviennent utiles, exploitables et ils peuvent être reconnus par les solutions SIEM, on distingue plusieurs types de formats de logs [23] [22] [25] :

- **Format texte brut(non standard)**

  Le contenue d'un fichier log est formaliser sous une structure en texte brute, il peut contenir des informations différentes en fonction de l'application ou de la configuration système qui enregistre les entrées de journalisation.

  Ce type de format est utilisé pour la journalisation de système et le dépannage, il permet de fournir de différentes informations sous un format simple et lisible.

  Exemple :

- **Format CLF :** Type de format de fichiers log standard en texte simple, c'est un type au format ASCII fixe non personnalisable développé par NCSA, facile à analyser [25].

```
2022-02-25 13:45:21 INFO: Starting server
2022-02-25 13:45:21 DEBUG: Listening on port 8080
2022-02-25 13:45:23 ERROR: Connection refused to database at 127.0.0.1:5432
2022-02-25 13:45:24 WARNING: Retrying database connection in 5 seconds
2022-02-25 13:45:29 DEBUG: Connection established to database at 127.0.0.1:5432
```

FIGURE 2.1 – Exemple de journalisation en texte brute pour une application serveur

Les fichiers journaux CLF sont généralement utilisés pour enregistrer les requêtes HTTP sur des serveurs web. Ainsi il peut être utilisé pour analyser des trafics web des audits de sécurité et des analyses de performance.

```
10.10.10.3 - lhadi [24/02/2023:02:42:55 -0500] "GET /home.htm HTTP/1.0" 200 4392
"http://fr.search.yahoo.com/fr?p=peinture" "Mozilla/4.7 [en] (Win20)"
```

FIGURE 2.2 – Exemlpe de journalisation en format CLF

- **Format de log JSON :** type de format qui consiste à sauvegarder les logs en un fichier JSON dans lesquelles les informations des champs de log sont structurées en format compatible adaptable au lagunage de programmations pour être efficacement interprété en objets pour être analyser par des programme informatique , ce qui facilite la filtration et l'analyse des informations de journal [25].
  En somme, le format JSON pour la journalisation est une option populaire en raison de sa facilité d'utilisation, sa structuration claire et sa compatibilité étendue.

```
{"timestamp": "2022-02-25T13:45:21.123Z", "level": "INFO", "message": "Starting server"}
{"timestamp": "2022-02-25T13:45:21.456Z", "level": "DEBUG", "message": "Listening on port 8080"}
{"timestamp": "2022-02-25T13:45:23.789Z", "level": "ERROR", "message": "Connection refused to database at
127.0.0.1:5432"}
{"timestamp": "2022-02-25T13:45:24.012Z", "level": "WARNING", "message": "Retrying database connection in 5
seconds"}
{"timestamp": "2022-02-25T13:45:29.345Z", "level": "DEBUG", "message": "Connection established to database at
127.0.0.1:5432"}
```

FIGURE 2.3 – Exemple de journalisation en format JSON

- **Format de log CSV :** type de format qui permet d'enregistrer et interpréter les champs de log en fichiers journal de plus petite taille que les formats JSON ou texte brute , car les données sont stockées sous forme basé sur un tableau de données simple dont les valeurs sont séparées par des virgules.
  Il est plus adapté aux enregistrements de données de base comme les transactions ou les données d'évènement simple.

Ce format est compatible, il peut être intégrer dans La plupart des applications existantes ainsi facile à utiliser pour la journalisation, mais il reste moins couramment utiliser pour la journalisation que les formats JSON et ceux en texte brute [25].

Exemple :

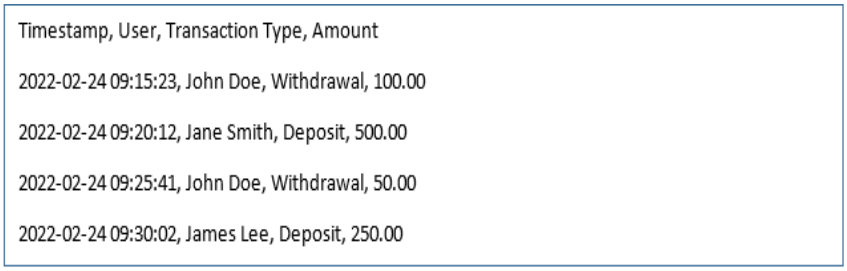

FIGURE 2.4 – Exemple de journalisation en format CSV

- **Format de log XML :** Type de format qui intègre les informations de journalisation de log en format W3C dans des balises XML , sous une syntaxe de journalisation définis à l'aide de L'ABNE ,en constituant un texte plus structuré facile à analyser et à traiter [25] .
- **Format de log binaire :** Ce type de format est utile pour sauvegarder les champs de journalisations brute sous forme binaire de manière compacte, car il n'nécessite moins d'espace sur le disque et efficace, sous une structure de fichier simple.
- **Format ELF :** Certains fichiers logs peuvent être sauvegardé sous Format ELF, plus particulièrement sur les systèmes basés sur linux. Le format ELF consiste à représenter les exécutables, les bibliothèques partagées et les fichiers d'objets sous un format binaire standard qui définit la structure d'un fichier binaire en plusieurs sections dont les parties du programme ou de la bibliothèque partagée sont incluses [25].

D) Catégories des logs

Pour catégoriser les logs, il est possible de les classifier selon plusieurs critères, notamment le type de log, le niveau de gravité et le niveau de journalisation.

a) **Selon le type de fichiers log**
Il existe plusieurs types de fichiers log utilisée afin de sauvegarder une collection de collection de caractéristiques associés à un évènement informatique, on site :

- **Log de serveur web :** Type de logs qui sauvegardent les informations de transaction au serveur web comme tentative d'accès, temps de réponse, et source de demande d'accès, adresse IP ,etc [22].
- **Log réseau :** Corresponds aux logs qui sauvegardent les événements liés aux flux des communications réseau comme les pannes du réseau ou le flux de trafic circulent sur le réseau [22].
- **Logs d'application :** Représente les logs qui comprennent tout évènement associer à l'exécution d'une application en question, comme erreur, requête, temps de réponse ou avertissement,etc [22].
- **Logs de sécurité :** représente les logs qui comprennent les évènements associés à la sécurité comme tentative de connexion, authentification échoué ou accès non autorisé [22].
- **Logs système :** Représente les logs qui sauvegardent et comprennent l'ensemble des événements liés au fonctionnement du système d'exploitation, tels que les erreurs, les mises à jour du système, les dysfonctionnements ou pannes matérielles, etc [22] .

- **Log d'installation :**C'est un type de journalisation qui sauvegarde l'ensemble des instructions exécutées, les étapes et les événements survenus pondant le processus de l'installation d'un logiciels ou d'une application, y compris les messages d'erreur, la configuration système ou les mises jour [22].
- **Logs d'audit :**Représente les logs qui comprennent tout évènement lié à l'audit comme activités utilisateur, accès vers les données sensibles ou tentative de violation ...etc.
- **Logs de performance :** Correspond aux logs qui sauvegardent tout événement lié à l'utilisation de la base de données, tel que les requête SQL, transaction ou opération d'enregistrement [22].

b) **Selon Le niveau de gravité Message :**
Les messages log peuvent être classifiés en fonction de leur niveau de gravité, ce qui indique leur ordre d'importance dans un fichier log. Les niveaux de gravité courants peuvent être résumés dans le tableau suivant [24] :

État	Niveau de journalisation	Description
Critique	Urgence	Plus critique
	Alerte	Intervention sévère
	Fatal (critique)	Sévère
Erreur	Erreur	Non bloquant
	Avertissement	Alerte
Normal	Notification	Normal
	Information	Informel
	Débloquer	Mode développeur

Table 2.1 – Description des états et niveaux de journalisation

E) Les Sources des fichiers logs

Les logs sont des enregistrements horodatés des évènements qui se produisent dans les systèmes informatiques ou les applications, ils sont très utiles notamment pour la détection d'intrusions et les activités malveillantes, le suivie des activités des utilisateurs et même pour garantir la sécurité des systèmes. Nous nous intéressons ici à la source de ces logs.

Les logs parviennent généralement de différentes sources au sein d'un système informatique ou application, voici quelques sources de prévenance de logs et leur emplacement au sein de chaque source [26] [27] :

a) Les systèmes d'exploitation :les logs générés par les systèmes d'exploitation peuvent se trouver dans différents endroits selon le système d'exploitation utilisé :

- Pour le système Windows les logs sont stockés dans l'observateur d'évènement « Event viewer » ou sont organisé en trois catégories :application, sécurité et système.
- Pour le système Linux les logs sont stockés dans les journaux système qui sont également stocké dans le répertoire /var/log ou sont organisés par le type de log (ex authentification :/var/log/athen.log).
- Pour le système MacOS, les logs sont stockés dans la console de l'application Console organisée en plusieurs catégories telles que log du système, log de noyau, log des applications.

b) **Les applications :** Les logs générés par les applications peuvent se trouver à divers endroits en fonction de l'application utilisée et de la manière dont elle est configurée. Les endroits courants sont :
   - Dans le sous -répertoire d'une application.Par exemple pour une application installée dans le répertoire /opt/monapp ses propres logs peuvent se trouver dans le sous- répertoire /opt/monapp/log.
   - Dans une base de données.Certaine application centralise ses logs dans une table spéciale dans une base de données.
   - Dans le répertoire de l'utilisateur.Il existe des applications qui stock ses logs dans le répertoire de l'utilisateur qui l'utilise, par exemple /home/user/log.

c) **Les serveurs web :** Les logs générés par les serveurs web pour surveiller les recherches des utilisateurs, tels que les pages demandées et l'adresse IP, sont stockés à des emplacements différents en fonction de la version du serveur utilisé et de sa configuration :
   - Le serveur Apache : les logs se trouvent dans le répertoire /var/log/apache sur le système linux.
   - Le serveur Nginx : les logs se trouvent dans le répertoire /var/log/ngix.
   - Le serveur web Microsoft IIS : les logs sont généralement stockés dans le répertoire SystemDrive/intepub/log/logFiles sur le système Windows.

d) **Le réseau :** Les logs générés par le réseau incluent des informations sur le trafic réseau telles que les ports utilisés, les adresses IP source et destination, les protocoles utilisés, etc. et peuvent se trouver à différents emplacements en fonction de l'environnement et des équipements réseau utilisés :
   - Pare-feu : les logs générer peuvent être stockés localement ou envoyés à un serveur log centralisé.
   - Routeur et commutateurs : les logs peuvent être stockés localement dans un tampon de mémoire ou un fichier log, ou même être envoyés à un serveur de log centralisé.
   - IPS, IDS… ou autre solution de supervisions mise en place.
   - Proxy http : c'est une source importante de journalisation qui contribue dans l'archivage des traces d'accès afin d'identifier les accès illicite.

e) **La sécurité :** Les logs de sécurité ont pour objectif de suivre les activités de sécurité, de détecter les actions anormales. Ces logs peuvent être stockés à différents endroits en fonction de l'environnement informatique spécifique et des systèmes de sécurité mis en place :
   - Les logs générés par les systèmes d'exploitation tels que Windows, Linux, et macOS peuvent être stockés dans des fichiers de journalisation ou des journaux d'audit spécifiques au système d'exploitation.
   - Les logs générés par les applications peuvent être enregistrés dans des fichiers journaux ou des journaux d'audit propres aux applications.
   - Les serveurs de sécurité tels que les serveurs proxy et les pares-feux génèrent des logs de sécurité qui peuvent être stockés localement sur le serveur de sécurité ou envoyés vers un serveur de log centralisé.

E) L'utilité des logs :

Les fichiers logs sont une source d'une multitude d'informations précieuses pour surveiller et maintenir la sécurité et la fiabilité des systèmes informatiques, car ils enregistrent les actions effectuées par les utilisateurs.

Les journaux de sécurité peuvent être utilisés pour [28] [25] [21] :

- Vérifier le bon fonctionnement des opérations système.
- Détecter les éventuelles compromissions du système ou du réseau.
- Retracer un bug dans un programme.
- Identifier et détecter les anomalies de sécurité.
- Contribuer à l'amélioration des diagnostics des pannes et des erreurs.
- Analyser et comprendre le fonctionnement d'une application ou d'un service.
- D'être prévenus en cas de dysfonctionnement.
- Suivi de l'activité de l'entreprise, de l'activité des composantes et aide aux décisions d'évolution de l'entreprise.

2.2.6 Architecture d'une solution SIEM :

L'architecture SIEM comporte quatre parties principales :

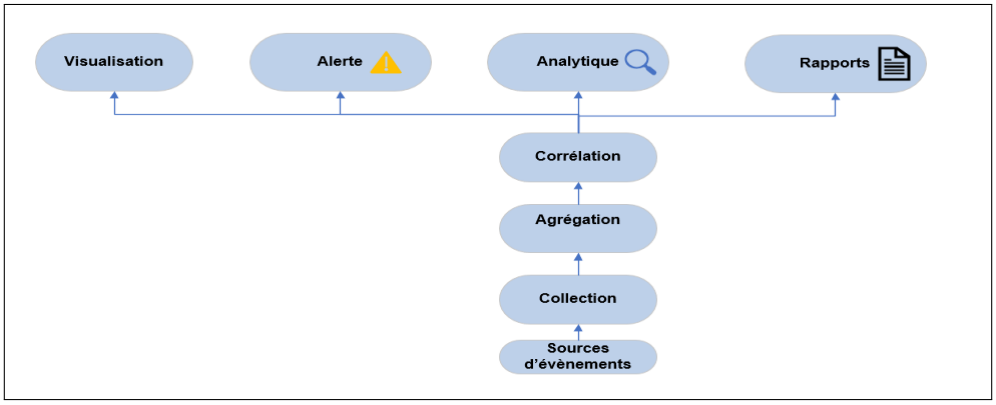

FIGURE 2.5 – Architecture de SIEM

a) Source de données :

C'est l'endroit d'où les informations de sécurité sont générées. Ils peuvent être des systèmes, des applications, des appareils de réseau, des bases de données, des fichiers journaux, des capteurs de sécurité, etc.

b) Collecteur de données :

C'est le composant qui collecte les données provenant des différentes sources de journalisation. Le collecteur de données doit être capable de comprendre différents formats de données et de les normaliser pour une analyse ultérieure.

c) Moteur central :

C'est la partie centrale du système SIEM qui traite les données collectées en temps réel. Le moteur central utilise des algorithmes d'analyse pour détecter les menaces et les anomalies dans les données. Il peut également fournir des alertes en temps réel sur les incidents de sécurité.

d) Base de données :

C'est l'endroit où les données collectées et analysées sont stockées pour une utilisation ultérieure. La base de données doit être capable de stocker des volumes de données importantes et de les indexer pour une recherche et une analyse rapide.

2.2.7 Fonctionnement des SIEMs

Le fonctionnement des différentes solutions SIEM peut varier d'un fournisseur à l'autre en matière de fonctionnalités, d'interfaces utilisateur, de capacités d'analyse de données et de types de données traitées.

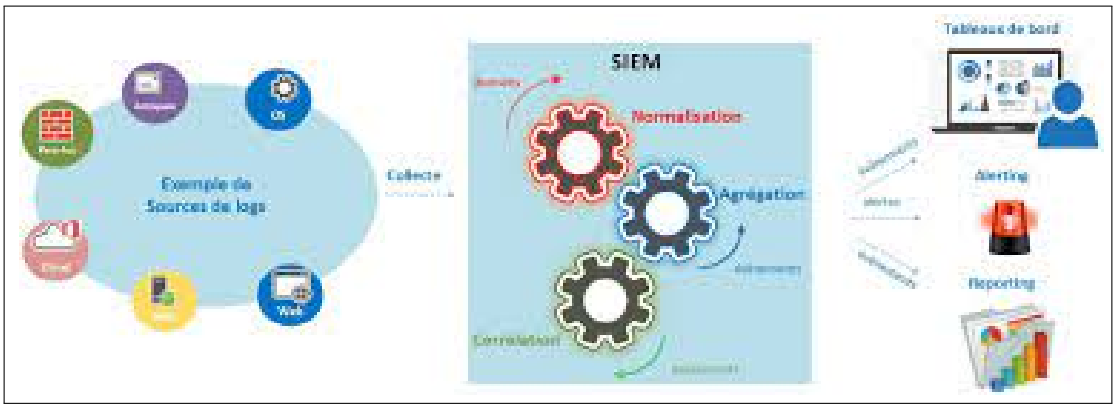

Figure 2.6 – Fonctionnement SIEM [1]

Cependant, le concept fondamental de fonctionnement d'un SIEM reste relativement similaire, dont huit parties fondamentales sont décrites. D'abord, la collecte des données pour récupérer les logs et les envoyer vers la plateforme de corrélation "SIEM" [1]. Ensuite, la normalisation des données pour uniformiser les informations collectées dans un format unique. Puis, l'agrégation des événements pour regrouper les données de sécurité ayant des similarités. La corrélation des événements consiste à analyser ces derniers selon des critères spécifiques. Enfin, la visualisation des données qui permet de présenter les données agrégées et corrélées sous forme de rapports et de tableaux de bord pour une meilleure compréhension et une prise de décision éclairée [29] [1] [17].

Les fonctionnalités décrites ci-dessus seront détaillées dans la sous-section suivante :

A) Collection des données :

Une plateforme SIEM est souvent déployée dans un emplacement centralisé accessible depuis tous les systèmes informatiques à l'intérieur d'une infrastructure réseau [29]. Elle collecte des données à partir de diverses sources de journalisation (voir la section "Les sources de journalisation de logs", pages 10-11) [21].

Il existe deux mécanismes de collecte de données (avec ou sans agents) utilisant des méthodes (pull ou push), en fonction des fonctionnalités et des capacités de chaque produit SIEM. Dans ce qui suit, nous allons détailler ces mécanismes et méthodes de collecte :

- **Collecte avec agent :** La plupart des solutions SIEM utilisent un mécanisme de collecte des événements en temps réel qui consiste à installer une multitude d'agents de collecte sur les équipements à superviser sous un plan hiérarchique. Lorsque ces sources de journalisation génèrent des informations et des événements de sécurité, ces agents générateurs s'engagent à signaler immédiatement, à récupérer et à convertir les entrées de journalisation en fonction des exigences de l'application SIEM via des connexions sécurisées et des protocoles de transport dédiés (WMI, SNMP, JMX). Cela garantit un transport confidentiel, authentifié (pour se protéger contre les faux journaux) et fiable [26]. Un collecteur est configuré pour recevoir ces données, ainsi que d'autres sources de données telles que les capteurs de surveillance de réseau. Il agrège l'ensemble des données et effectue une analyse préliminaire avant les envoyer dans un format plus structurées vers le logger, où elles sont stockées dans des fichiers logs [13].
- **Collecte sans agent :** Dans le mécanisme de collecte de données sans agent, le collecteur est chargé d'interroger les appareils à des intervalles de temps programmés en utilisant différents moyens tels que les protocoles de transmission standards FTP, SFTP, SCP, HTTP, ainsi que des sockets TCP/IP dédiés pour extraire les données à partir de différentes sources de journalisation [26]. Les données collectées sont ensuite transmises à un logiciel de stockage de données qui les enregistre dans des fichiers journaux. Ensuite, l'application SIEM peut être utilisée pour analyser ces données et ces événements de sécurité provenant de différentes sources afin de détecter les menaces de sécurité [13].
- **Méthode pull :** Dans cette méthode, le SIEM doit établir une connexion au partage réseau en utilisant un identifiant. C'est une approche centralisée qui nécessite une puissance de traitement importante au niveau du SIEM [26]. Elle est plus adaptée à la collecte de données sans agent en temps réel programmé [30].
- **Méthode push :** Dans cette méthode, la source/agent envoie directement les données de journalisation au SIEM de manière proactive, sans que le SIEM n'ait besoin de les demander [26]. Cela peut réduire les délais de collecte de données et garantir une réactivité plus rapide aux menaces. Cette méthode est plus adaptée à la collecte de données avec agent en temps réel continu [30].

  Il est donc important de choisir la méthode de collecte appropriée en fonction de l'environnement de l'entreprise pour garantir une collecte de données efficace et fiable.

Comment SIEM peut empêcher la collecte des faux journaux ?

Les attaquants ont la possibilité de modifier les journaux de sécurité afin de masquer leurs activités, d'effacer les traces de journalisation ou de générer des journaux falsifiés. Afin d'empêcher l'infiltration de fausses entrées dans les journaux, la plupart des produits SIEM implémentent des techniques restrictives sur les sources de données, notamment l'authentification et la surveillance de l'intégrité des journaux, l'analyse des modèles de comportement et la surveillance de l'accès aux journaux [31].

Quelles sont les exigences de collecte de données ?

- Toutes les données collectées doivent être livrées vers la plateforme SIEM sans aucune perte de données afin de garantir que le processus de collecte soit fiable [31].
- Toutes les données collectées doivent être utiles et pertinentes en empêchant les unités sources de journalisation d'enregistrer des données inutiles [31].

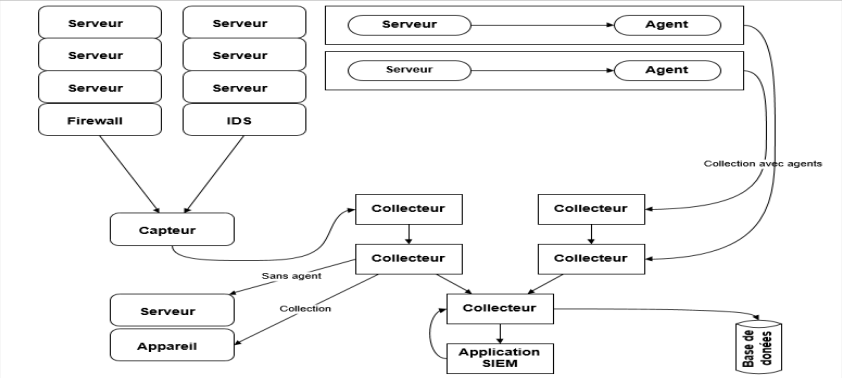

FIGURE 2.7 – Processus de collecte de données

B) Découpage (parsing)

Lorsque les logs d'événements natifs arrivent au SIEM.Cette étape consiste à lire et découper chaque champ d'un log pour faire apparaître les éléments unitaires d'informations pertinents, afin de les normaliser et de les structurer dans un format compréhensible pour le SIEM. Cela implique généralement d'analyser le contenu de chaque événement en utilisant des expressions régulières, des parseurs natifs, des parseurs adaptables ou des parseurs personnalisés développés en fonction du format de log collecté.

C) Normalisation

La normalisation des données est une pratique courante dans les solutions SIEM en raison de la diversité des sources de données de journalisation qui utilisent différents formats pour stocker, transmettre et décrire les entrées de journal [26]. Elle consiste à reformater les données en une sortie standard propre à la solution SIEM déployée afin d'assurer l'interopérabilité, la compatibilité et la cohérence avec les formats et les normes de données standard [32]. Un analyseur peut gérer la normalisation sur plusieurs champs, notamment [31] :

a) **Normalisation de format de données :** Cette technique consiste à convertir toutes les données collectées en un format standard pour faciliter leur traitement et leur analyse.

b) **Normalisation de la terminologie :** Les termes utilisés pour décrire les événements peuvent varier d'un système à l'autre. Par exemple, une attaque de type "SQL injection" peut être appelée "injection de code" dans un autre système. La normalisation de la terminologie implique l'utilisation de termes standards pour décrire les événements, ce qui facilite la compréhension et l'analyse des données de journalisation.

c) **Normalisation de l'heure :**La date et l'heure de collecte des données de journal sont cruciales pour une analyse précise. Il est donc vital de s'assurer que l'heure est correcte par rapport à une horloge commune, pour éviter les erreurs de décalage horaire et les incohérences dans les données.

Il est important de noter que souvent, avant de normaliser les données, les Loggers stockent des copies des journaux d'événements sous leur forme originale (données brutes), afin de conserver un enregistrement complet des journaux au cas où ils devraient être utilisés comme preuve légale ou de conformité.

D) L'agrégation des évènements

L'agrégation des événements est une fonctionnalité assurée par le gestionnaire d'évènements d'un SIEM, qui regroupe des événements de sécurité de même type selon des règles d'agrégation dans un seul magasin de données. Cette fonctionnalité permet de réduire le nombre d'événements à examiner tout en consolidant les enregistrements d'évènements en double, fournissant ainsi une vue d'ensemble plus complète sur l'activité de sécurité du réseau. Un agrégat de messages peut révéler des indices qui auraient été inaperçus dans le cas où les messages seraient traités séparément. Par exemple, un attaquant cherchant à accéder au compte d'un utilisateur spécifique pourrait essayer de deviner le mot de passe en effectuant de nombreuses tentatives de connexion. Les messages de journal, pris individuellement, ne seraient peut-être pas suffisants pour détecter l'attaque. Cependant, un grand nombre de tentatives de connexion infructueuses, réalisées en une courte période de temps, sont plus susceptibles d'être des tentatives d'intrusion [31].

E) Corrélation des évènements

La corrélation des données est un processus en temps réel qui permet de détecter les vecteurs de menace zero-day. Ce processus est géré par un moteur de corrélation connu sous le nom de cerveau du SIEM [26]. Le moteur est responsable de regrouper et d'analyser toutes les informations de sécurité collectées par le système selon un ordre de gravité prédéfini, en cherchant des liens entre elles afin d'identifier des activités anormales qui ne seraient pas évidentes à partir d'un événement singulier [33]. Cette tâche demande beaucoup de traitement avancé, ce qui explique pourquoi les solutions SIEM utilisent des informations contextuelles et des bases de données en ligne sur les menaces, ainsi que des règles de corrélation créées par des analystes humains ou extraites d'autres systèmes ou organisations, pour distinguer ce qui est une attaque de ce qui ne l'est pas parmi les autres événements de sécurité [13] [30]] [31].

La corrélation peut être classée en trois types distincts [13] :

a) **a) Corrélation active :** Elle est capable d'enrichir les évènements reçus en collectant des informations complémentaires pour prendre des décisions.

b) **b) Corrélation passive :** Elle ne peut pas interagir avec son environnement et se contente de recevoir des évènements pour prendre des décisions.

c) **c) Corrélation croisée :** Elle est capable d'associer et de prioriser les évènements de sécurité reçus ainsi que d'autres informations provenant de scanners de vulnérabilités, de systèmes de gestion de réseau (NMS, Network Management System), etc. Il s'agit d'une forme de corrélation active étendue à plusieurs équipements pour une détection plus précise et une meilleure vue d'ensemble de l'environnement de sécurité.

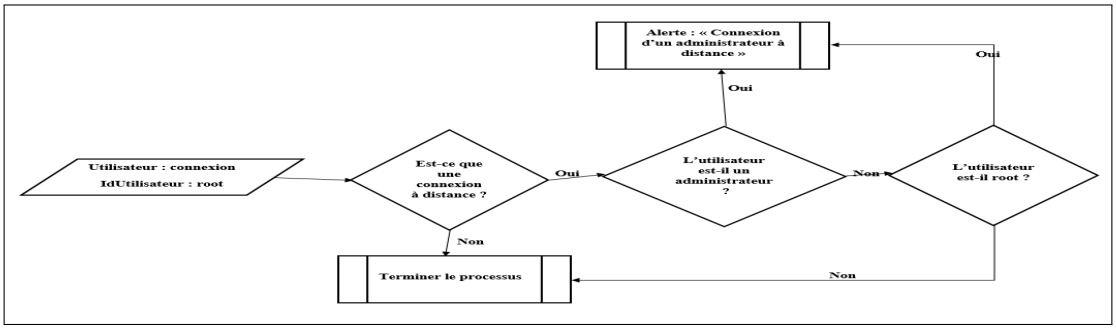

FIGURE 2.8 – Exemple d'une règle de corrélation

Quesque une règles de corrélations ?

Elle correspond à un algorithme de détection plus ou moins complexe qui est conçu par l'équipe SOC ,selon leur besoin et les contraintes d'infiltration de type d'attaque ou d'incident a détecter [30].

F) Analyse des de données de Sécurité :

Une fois que les données de sécurité ont été normalisées et corrélées, un moteur de règles de SIEM est utilisé pour analyser ces données de manière plus approfondie en fonction des lignes de base qui détaillent des règles intégrées et des fonctions analytiques avancées préétablies par les équipes de sécurité. Le moteur de règles utilise une logique booléenne pour identifier les incidents malveillants ou suspects. Il classe les alertes dans différentes catégories, telles que les logiciels malveillants, les échecs de connexion, et d'autres activités potentiellement nuisibles [26]. Voici quelques techniques couramment déployées dans les solutions SIEM pour l'analyse de données :

a) **Analyse par règles de signature :** Les SIEMs utilisent des signatures pour identifier les activités malveillantes connues. Les signatures sont des modèles de comportement qui correspondent à des attaques spécifiques et sont stockées dans une base de données de signatures. Les SIEMs utilisent ces signatures pour identifier les activités malveillantes connues.

b) **Analyse par règles de comportement :**Les SIEM analysent les comportements des utilisateurs, des applications et des systèmes pour détecter les activités anormales. Les SIEM utilisent des algorithmes de machine Learning pour apprendre les comportements normaux et détecter les anomalies. Par exemple, une activité de connexion à un compte à partir d'une adresse IP inhabituelle, pourrait être considérée comme une activité suspecte.

G) Stockage et archivage

Le SIEM procure un processus pour stocker les informations et les événements de sécurité de manière compressée et éventuellement cryptée. Étant donné qu'une quantité massive de données sont impliquée. Il existe généralement deux types de bases de données, l'une pour le stockage général et l'autre pour les événements qui doivent encore être corrélés. Les environnements SIEM sont capables de transférer les données stockées vers tout type de système de stockage compatible.

Une solution SIEM assure plusieurs fonctionnalités informatives d'avertissement ,afin de fournir des informations pertinentes aux analystes de sécurité et aux équipes de supervision. Le SIEM envoie soit une alerte dès la détection d'une anomalie de sécurité,ou un rapport programmé à une heure prédéterminée.

H) Visualisation

La plupart des produits SIEM proposent généralement des visualisations statistiques qui sont générées automatiquement . Ces visualisations prennent souvent la forme de tableaux de bord qui synthétisent les données collectées et fournissent des informations telles que le nombre d'attaques ou d'alertes par jour, offrant ainsi une visibilité et une vue d'ensemble sur les activités du système.

a) **Génération des alertes et des notifications**

SIEM est considéré comme le mécanisme le plus intelligent offrant le taux de faux positifs le plus faible pour la génération d'alertes et de notifications en temps réel. Une alerte fournit une multitude d'informations sur les événements identifiés comme étant malveillants ou potentiellement malveillants, détectés suite à une analyse approfondie des événements et des journaux de sécurité [31]. Ces alertes peuvent comprendre les informations suivantes :

- Un identifiant unique pour l'alerte.
- La date et l'heur a lequel l'alerte a été déclenché.
- Source d'évènement et les règles de détection qui a déclenché l'alerte.
- La gravité d'alerte.
- Des descriptions de l'évènement qui a déclenché l'alerte.
- Des recommandations sur les mesures qui peuvent être prise par les équipements de sécurité pour enquêter et répondre à l'alerte.

b) **Génération des rapports**

Le SIEM génère des rapports essentiels pour l'analyse des tendances, la conformité et l'investigation, afin de prévenir proactivement les attaques et gérer les risques. Ces rapports sont généralement programmés pour être générés régulièrement à des intervalles de temps déterminés. Le SIEM peut fournir trois types de rapports, définis ci-dessous :

- **Les rapports d'analyse de sécurité :** Fournissent des informations sur les activités suspectes détectées et aident les analystes à comprendre les menaces potentielles. Ils peuvent inclure des graphiques et des tableaux pour faciliter la compréhension.
- **Les rapports d'audit :** Fournissent des informations sur les incidents de sécurité, les mises à jour du système, les changements de configuration, etc
- Un rapport SIEM peut être personnalisé pour adaptés aux besoins spécifique d'un utilisateur.

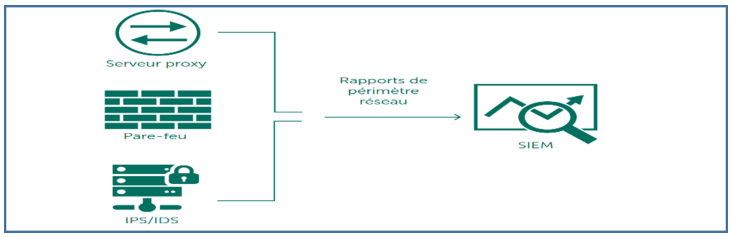

Figure 2.9 – Génération des rapports

2.2.8 Les avantages de SIEM :

Les produits SIEM pour la supervision centralisée des évènements et des informations de sécurité offre de nombreux avantages, en voici quelques-uns [34] [18] [30] [35] :

- ▷ SIEM offre une plateforme de visualisation et une surveillance proactive et réactive en continu sur la sécurité d'un système informatique.
- ▷ Gestion automatique des taches de sécurité tels que la surveillance et les alertes, ce qui permet une prise de mesures défensives plus rapidement.
- ▷ Fournir des rapports personnalisés sur les données de sécurité.
- ▷ L'adaptation ou La conception des produits SIEM déploie des scripts déjà existants sur la gestion des logs.
- ▷ Mettre au jour des activités malveillantes et déclencher des réponses automatisées,
- ▷ SIEM permet de garantir la haute disponibilité des mesures de sécurité.
- ▷ Identifier et signaler les incidents de sécurité potentiels.

2.2.9 Limites de SIEM

SIEM présente certaines Limites, parmi ses limites on peut citer :

- ▷ **Complexité et cherté :** La mise en place d'une solution SIEM est une opération complexe et peut être couteuse en fonction de la licence choisie, du matériels et des ressources humaines nécessaires pour la maintenance et la gestion.
- ▷ **Faux positifs :** Parfois, une erreur de configuration dans les règles et politiques de sécurité rend son fonctionnement peu fiable, ce qui entraîne la génération de fausses alertes. Les équipes IT doivent alors perdre du temps à « chasser » ces faux positifs, risquant de manquer des incidents de sécurité réels [36].
- ▷ **Absence des équipes de sécurité :** Les équipes de sécurité doivent avoir une expertise en cyber sécurité pour utiliser les solutions SIEM et maximiser leurs capacités.
- ▷ **Le volume d'alertes :** Les solutions SIEM générant des alertes en fonction des règles prédéfinies, ces alertes peuvent être nombreuses et rendre leurs gestion compliquée.
- ▷ **Détection des menaces internes :** La détection des menaces internes est difficile car ces attaques proviennent souvent d'individus ayant accès aux systèmes et aux données de l'entreprise, sans comportement malveillant connu. Cela rend difficile la détection de ces attaques par le SIEM.

2.2.10 Mise en place et déploiement d'une solution SIEM dans un réseau

La conception d'une solution SIEM est mise en place pour surveiller l'ensemble du système. Tous les appareils doivent être autorisés à collecter des données d'audit, telles que les journaux système et les alertes de pare-feu, qui sont ensuite envoyées à la console centrale du système SIEM. Cette console agrège, corrèle, analyse et rapporte toute détection d'anomalie . Enfin, afin de garantir l'efficacité du système SIEM dans la détection de la majorité des attaques tout en générant un nombre minimal de faux événements et d'alarmes, des équipes de sécurité spécialisées sont mises en place pour évaluer de

manière approfondie la solution SIEM [37]. Dans ce contexte, le déploiement d'une plateforme SIEM se fait en plusieurs étapes :

1. Planification de haut niveau et définition des scénarios d'attaque cruciaux auxquels il faut remédier, des types d'événements à surveiller et des actions préventives à mettre en place.
2. Conception de l'architecture de déploiement du SIEM en fonction du type adopté pour l'environnement réseau de l'entreprise.
3. Installation de l'appliance et des serveurs nécessaires pour le fonctionnement de la solution SIEM, y compris les serveurs de base de données, etc.
4. Configuration de base, comprenant la synchronisation NTP, la connexion OTX pour se tenir informé des attaques et des menaces en cours, la politique de stockage des données, les sauvegardes de configuration, la définition des utilisateurs et les réglages SSH/SSL.
5. Identification des cibles respectives des appareils les plus critiques pour la sécurité à protéger.
6. Configuration des règles de corrélation et d'analyse pour identifier les événements de sécurité importants..
7. Mise en place d'un processus de gestion des incidents pour répondre rapidement aux incidents de sécurité détectés.
8. Formation du personnel de sécurité pour l'utilisation de la solution SIEM et le processus de gestion des incidents.

2.2.11 Types de déploiement d'une solution de sécurité SIEM

Il existe différents types de déploiement courants pour une solution de sécurité SIEM (en fonction des besoins spécifiques de l'organisation et des contraintes techniques). Voici quelques exemples de déploiements possibles :

A) Le déploiement sur site

C'est une démarche où l'entreprise installe et configure la solution SIEM sur tous ses équipements informatiques et serveurs de son réseau local. Dans cette approche, la gestion de l'infrastructure de la solution est une responsabilité de l'entreprise, y compris le stockage, le traitement et l'analyse des données de sécurité, la surveillance des événements de sécurité, la détection et la réponse immédiate aux menaces, faite via une interface web ou une application installée localement .

B) Déploiement sur Cloud public

C'est une approche où une solution hébergée sur une infrastructure Cloud est utilisée par une entreprise, telle que celle proposée par Amazon Web Services (AWS), Microsoft Azure ou Google Cloud Platform, au lieu que l'entreprise se préoccupe de l'installation et de la configuration de la solution sur chaque équipement de son infrastructure locale [38].

C) Le déploiement en hybride

Le déploiement hybride d'une solution de sécurité SIEM est une combinaison des deux types précédents (sur site et en Cloud). Les entreprises peuvent bénéficier d'un traitement efficace en utilisant des fonctionnalités qui s'exécutent sur le site et d'autres en cloud [38].

D) Le déploiement en tant que service (SIEMasas)

C'est une démarche où les fournisseurs de services s'occupent de gérer la solution SIEM pour les entreprises. Ces dernières peuvent accéder à la solution via une interface web ou une application tout en utilisant une connexion Internet pour surveiller la sécurité de leur infrastructure, détecter et répondre rapidement aux cyberattaques [39].

2.2.12 Produits SIEM disponibles sur le marché

En raison de la croissance rapide et continue des technologies informatiques, un grand nombre de solutions SIEM ont été développées et sont disponibles sur le marché. Chacune de ces solutions à ses propres caractéristiques et fonctionnalités uniques. De manière générale, on peut distinguer deux types de solutions SIEM : on distingue deux types de solution :

A) Produits SIEM open source :

Les solutions SIEM open source ouvrent leur conception au public, elles peuvent être utilisées gratuitement et possèdent un code source personnalisable. Voici quelqu'un des produits open source les plus populaires :

a) **ELK Stack :**
C'est une suite d'outils open-source pour la gestion des logs et la sécurité SIEM qui comprend Elas- ticsearch, Logstash et Kibana, ainsi que la famille Beats pour offrir une solution complète de collecte, de traitement et de visualisation de données en temps réel. File Beat est un autre projet qui a été ajouté à la suite pour former ELK Stack. Cette solution est très utile dans les domaines de la surveillance, de l'analyse des journaux, de la gestion des performances et de la sécurité, offrant aux organisations une solution SIEM complète [2].

Figure 2.10 – Produit ELK Stack [2]

b) **Gray log :**
Gray Log propose une solution open-source de gestion centralisée de journaux et d'événements, offrant de nombreuses fonctionnalités puissantes. Elle est conçue pour l'analyse de journaux modernes et élimine la complexité de l'exploration des données, de la chasse aux menaces et des audits de conformité. Cette solution permet de configurer rapidement un système fonctionnel et fournit une interface de visualisation claire pour les journaux et événements collectés, indexés et analysés en temps réel. Cette interface facilite la recherche d'éléments importants dans les données à travers des graphiques et des tableaux de bord [3].

FIGURE 2.11 – Produit Gray log [3]

c) **Prelude OSS :**

Cette solution complète, universelle, gratuite et open source permet la convergence de la sécurité de l'information et de la gestion des événements (SIEM). Elle propose des fonctionnalités avancées de surveillance en temps réel, de détection de menaces et d'analyse d'incidents de sécurité [4]. Prelude OSS collecte, normalise, trie, agrège, corrèle et signale tous les événements liés à la sécurité. Cependant, il est conçu pour les petits déploiements, ce qui en fait une option intéressante pour les organisations qui cherchent une solution de SIEM performante à faible coût. Il offre moins de fonctionnalités que les SIEM d'entreprise et ses performances sont limitées en conséquence [40]. Cependant, l'avantage de Prelude OSS est qu'il prend en charge plusieurs formats de journaux et s'intègre à d'autres outils tels qu'OSSEC, Snort et Suricata. Prelude OSS utilise le format IDMEF, ce qui permet l'utilisation de ses données avec des systèmes de détection d'intrusion.

FIGURE 2.12 – Produit Prelude OSS [4]

d) **OSSIM :**

OSSIM (Open Source Security Information Management) est une solution de sécurité populaire, développée par AlienVault. Cette solution SIEM est basée sur une architecture modulaire distribuée, composée d'un serveur principal (le "Master") et de plusieurs agents installés sur les différents systèmes de l'infrastructure, offrant ainsi une grande évolutivité [4].

FIGURE 2.13 – Produit OSSIM [4]

OSSIM garantit une surveillance de sécurité complète grâce à la collecte, la normalisation, la corrélation d'événements et l'analyse de données, ainsi que la détection d'intrusions et de vulnérabilités, tout en minimisant les faux positifs. Cette solution de sécurité est dotée d'une interface utilisateur conviviale et intuitive, et des rapports sont générés automatiquement pour aider les équipes de sécurité à obtenir une vue d'ensemble complète de la sécurité de leur infrastructure [4].

Analyse comparative des fonctionnalités des différentes solutions SIEM open source

Solution	Avantages	Inconvénients
ELK (Elasticsearch, Logstash, Kibana)	— Visualisation des données en temps réel — Analyse de données avancée — Prise en charge de multiples sources de données	— Configuration complexe — Coût élevé pour une utilisation professionnelle
Prelude OSS	— Agrégation de logs en temps réel — Analyse de données en temps réel — Intégration avec des outils tiers	— Faible communauté et support — Nécessite des ressources système importantes
Graylog	— Détection d'incidents en temps réel — Analyse de données avancée — Prise en charge de multiples sources de données	— Interface utilisateur peu conviviale — Faible support de la communauté
OSSIM	— Agrégation de logs en temps réel — Analyse de données avancée — Prise en charge de multiples sources de données	— Interface utilisateur peu conviviale — Configuration complexe

Table 2.2 – Comparaison entre les solutions SIEM open source

B) Produits SIEM commerciaux :

Les produits SIEM commerciaux sont généralement développés et vendus par des fournisseurs de logiciels spécialisés dans la sécurité. Ils offrent des fonctionnalités avancées pour la gestion des événements et des alertes de sécurité.

a) **Splunk**

Splunk est une plateforme logicielle intelligente qui permet la collecte, la recherche, l'analyse, l'indexation et la visualisation de données provenant de diverses sources d'un SI, quels que soient leur type (structuré ou non structuré) et leur format, en temps réel. Elle est reconnue comme l'un des outils les plus puissants pour le traitement des données volumineuses [40]. Splunk comprend un moteur de recherche et d'analyse, des outils de visualisation ainsi qu'une variété d'applications et de modules complémentaires pour répondre à différents cas d'utilisation. Ces applications contiennent des objets de connaissance, des configurations, des entrées préconfigurées, des vues et des tableaux de bord [4].

Cette solution est souvent appelée le "Google des logs" et se présente également comme une entreprise SIEM, offrant une solution de sécurité axée sur l'analyse qui va au-delà du SIEM traditionnel. Elle permet de traiter la détection des menaces avancées, la surveillance de la sécurité, la gestion des incidents et la criminalistique en temps réel [41]. Splunk améliore la visibilité sur plusieurs systèmes et fournit un système de sécurité solide grâce à la collaboration croisée pour garantir la sécurité des entreprises.

b) **LogRhythme**

LogRhythm est une solution SIEM très populaire qui intègre des analyses de sécurité avancées telles que l'UEBA, le NDR et le SOAR, grâce à des techniques d'apprentissage automatique et d'intelligence artificielle, dans une plateforme NextGen SIEM de bout en bout. Elle est conçue pour fournir une surveillance et des analyses en temps réel permettant de détecter, de hiérarchiser et d'identifier les modèles et les anomalies de sécurité. La plateforme LogRhythm NextGen SIEM permet de collecter, surveiller et analyser les données de sécurité à partir de multiples sources. [5].

Figure 2.14 – Produit LogRhythm [5]

d) **IBM radar SIEM**

IBM QRadar SIEM est une solution de sécurité informatique complète développée par IBM, conçue pour aider les organisations à détecter et à répondre rapidement aux menaces en temps réel. La solution utilise une gamme d'outils et de techniques automatisés, notamment l'analyse comportementale, le Machine Learning et les outils de chasse aux menaces pour collecter, analyser et corréler les données de sécurité en temps réel. Elle permet également une visualisation rapide des événements de sécurité critiques, facilitant ainsi la détection et la réponse aux menaces de sécurité. En outre, la solution est hautement personnalisable pour répondre aux besoins spécifiques de chaque entreprise [6] [42].

Figure 2.15 – Produit IBM QRadar SIEM [6]

Analyse comparative des fonctionnalités des différentes solutions SIEM commerciaux

Critères	Splunk	IBM QRadar SIEM	LogRhythm
Avantages	— Interface personnalisable et facile à utiliser. — Capacités de recherche puissantes. — Évolutivité horizontale et verticale. — Support multiplateforme. — Installation simple. — Configurabilité élevée.	— Fortes capacités d'analyse. — Utilisation d'algorithmes de machine learning avancés. — Installation et configuration simples. — Intégration facile avec d'autres outils de sécurité. — Interface utilisateur conviviale. — Prise en charge de l'auto-configuration.	— Haute efficacité de détection des menaces. — Automatisation des tâches de réponse aux incidents. — Intégration avec des solutions tierces. — Installation et configuration simples. — Interface utilisateur conviviale. — Prise en charge de l'auto-configuration.
Inconvénients	— Manque de documentation de qualité — Apprentissage initial complexe — Dépendance à un nombre élevé de ressources système	— Coût élevé — Apprentissage initial complexe — Fonctionnalités de personnalisation limitées	— Coût élevé — Manque de documentation détaillée — Limites de performances — Absence de support pour les environnements multiplateformes

Table 2.3 – Comparaison entre les solutions SIEM commerciales

2.2.13 Critères de choix d'une solution SIEM

Avant de poursuivre l'implémentation d'une solution SIEM, il est crucial de prendre en compte plusieurs critères afin de choisir la solution SIEM la plus appropriée qui vaut la peine de consacrer des efforts et du temps pour l'installer sur une infrastructure réseau d'un environnement informatique. Cela permettra d'établir un calendrier de déploiement efficace qui aligne la sécurité SIEM sur les objectifs de l'entreprise [12].

Tout d'abord, il est important de déterminer les besoins de sécurité spécifiques de l'organisation, tels que le nombre de sources de journalisation, le volume de données à traiter, les services à sécuriser, etc. Ensuite, il est primordial de choisir une solution SIEM qui offre une grande flexibilité et évolutivité du périmètre de sécurité ainsi qu'un traitement analytique des données et une visibilité globale de l'état de sécurité de l'environnement.

Il est également crucial de s'assurer que les fonctionnalités de la solution SIEM permettent une détection rapide et complète des incidents de sécurité, avec un taux de détection acceptable. De plus, il est important d'évaluer le budget de l'entreprise et l'efficacité des outils de gestion de la sécurité informatique. Dans l'idéal, la solution SIEM devrait offrir un compromis entre efficacité et coût, avec une licence simple à utiliser [13]

2.2.14 Choix de la solution SIEM

Après avoir effectué des recherches sur diverses solutions disponibles, bien qu'elles ne soient pas toutes présentées dans le tableau précédent, nous avons comparé ces produits en termes de coût, de compatibilité et de facilité de mise en place. Nous avons finalement choisi Splunk pour ce projet. Dans la section suivante, nous allons fournir une étude détaillée de cette solution ainsi que de son fonctionnement [12].

Quels sont les principaux produits proposés par Splunk ? [43]

- **Splunk Enterprise :** Est la version la plus complète de Splunk, offrant une plateforme hautement évolutive et programmable sur laquelle de nombreuses solutions de sécurité peuvent être créées. Cette version inclut des fonctions d'analyse intuitives, d'apprentissage automatique, des applications pré-packagées ainsi que des API ouvertes. Elle est conçue pour répondre aux besoins des entreprises de toutes tailles et de tous secteurs d'activité qui doivent collecter, analyser et visualiser de grandes quantités de données en temps réel [32].
- **Splunk Cloud :** Est une version hébergée de Splunk qui offre aux utilisateurs des fonctionnalités de Splunk en tant que service cloud. Elle est hautement évolutive et peut être utilisée par les entreprises en fonction de leurs besoins, sans avoir à s'occuper de l'installation, de la configuration et de la maintenance de Splunk sur leur infrastructure locale.
- **Splunk Light :** Une version allégée de Splunk Enterprise qui propose les mêmes fonctionnalités de collecte, d'indexation et d'analyse de données, ainsi que des fonctionnalités supplémentaires telles que la génération de rapports et la visualisation en temps réel. Conçue pour les petites entreprises et les environnements de test avec des volumes de données moins importants, elle est facile à déployer et à configurer. En résumé, Splunk Light est une alternative légère à Splunk Enterprise pour les utilisateurs qui n'ont pas besoin de la gamme complète de fonctionnalités de Splunk.
- **Splunk Mint :** Est une solution de surveillance pour les développeurs d'applications mobiles. Elle permet de surveiller en temps réel les performances de leurs applications mobiles et d'identifier les vulnérabilités et les incidents. Cette solution est conçue pour améliorer la performance de l'application en optimisant la vitesse et le temps de réponse du serveur.

- **Splunk User Behavior Analytics (UBA) :** Est une version de Splunk Enterprise conçue pour la détection des menaces internes et des fraudes. Elle utilise des algorithmes avancés pour analyser le comportement des utilisateurs, des dispositifs d'extrémité et des applications, afin de détecter les comportements suspects et anormaux. Cette solution peut être utilisée pour identifier les activités malveillantes telles que la fraude interne, le vol de données et l'abus de privilèges, et elle fournit des alertes en temps réel pour permettre une intervention rapide. Elle est particulièrement utile pour les grandes organisations souhaitant renforcer leur sécurité et protéger leurs données confidentielles.

Bien que Splunk ne soit pas exclusivement un outil SIEM, il peut être utilisé de manière similaire pour la gestion des logs. La plateforme est conçue pour collecter et stocker les données en temps réel sous forme d'événements dans des indexeurs, et offre des fonctionnalités pour visualiser ces données sous forme de tableaux de bord.

2.2.15 Le produit de Splunk pour le SIEM :

Le produit de Splunk compatible pour être une solution de sécurité SIEM est Splunk Entreprise Security (Splunk SE). Splunk SE est une extension de Splunk pour la collecte, l'analyse et l'agrégation des données de sécurité, il aide les entreprises à améliorer leurs postures de sécurité en assurant des fonctionnalités de sécurité avancées tels que la détection des menaces avancées en utilisant des algorithmes d'apprentissage automatique , la surveillance du réseau et de toute l'infrastructure de l'entreprise toute en assurant la conformité réglementaire [19].il génère des rapports et des tableaux de bord détaillées sur les évènements analysée et les incidents de menaces détectés pour aider les équipes de sécurité à comprendre les tendances de sécurité, à effectuer leurs tâches et répondre rapidement aux menaces et aux incidents de sécurité. Cette solution peut être exécutée sur divers environnements tels que des Cloud publics et privés, une infrastructure sur site et des déploiements hybrides.

2.2.16 Architecture fonctionnelle de Splunk :

L'architecture fonctionnelle de Splunk repose sur trois éléments clés qui simplifient sa mise en œuvre dans un environnement distribué, conforme aux principes du Big Data. Les principaux composants sont [44] :

a) **Les "Splunk Forwarders" :**sont des agents légers ou "redirecteurs" installés sur les serveurs sources de données. Ils sont utilisés pour collecter les données et les envoyer vers les indexeurs Splunk pour leur traitement et leur stockage. Splunk dispose de deux types de "Forwarders" typiques : le "Forwarder" universel et le "Forwarder" lourd. Chacun ayant sa propre méthode de fonctionnement.
   - **Le "Forwarder" universel :** est un composant simple qui permet de capturer les données brutes directement depuis un flux de données. Il effectue un traitement minimal sur ces données avant de les transmettre à un indexeur. Parmi ses caractéristiques, il envoie une quantité énorme de données rapidement à l'indexeur tout en consommant moins de ressources sur les machines.
   - **le "Forwarder" lourd :**il effectue une analyse et une indexation préalable des données brutes dans les machines à l'origine. Il est plus lent, mais il envoie uniquement les événements analysés à l'in dexeur, ce qui peut réduire la quantité de données transmises et la charge sur le réseau.

b) Les indexeurs : ils constituent le composant clé et essentiels de Splunk. Ils reçoivent les données du re- directeur, les transforment en événements, les analysent et les indexent selon une syntaxe spécifique, puis les stockent pour permettre des opérations de recherche efficaces. Les indexeurs sont également utilisés pour effectuer des recherches et des analyses sur les données. L'indexeur organise les données indexées en créant trois types de fichiers séparés dans un répertoire appelé « buches ». Le premier type est une forme compressée des données brutes, le deuxième est un fichier de métadonnées et le troisième est un fichier d'index qui pointe vers les données brutes (fichiers d'index ou TSIDX). L'indexeur fonctionne en deux méthodes selon le type de transiter qui à envoyé les données, pour les évènements reçus auprès du transiter lourd, indexeur effectue Seulement l'indexation pour les stocker dans un index, pour les données brutes envoyées par le transiter universel, l'indexeur doit d'abord éliminer les données indésirables puis les Indexer et les stocker dans un index pour une recherche et une analyse ultérieure.

c) Le moteur de recherche : est un serveur qui permet aux utilisateurs d'interagir directement pour effectuer des recherches et des analyses sur les données indexées stockées dans les indexeurs. Il traite les requêtes des utilisateurs en les envoyant aux indexeurs, puis récupère les résultats et les présente aux utilisateurs. Ces résultats peuvent être triés, filtrés et visualisés dans des tableaux de bord interactifs pour aider à mieux comprendre les données.

d) La console de gestion : c'est un outil qui s'ajoute à l'architecture Splunk distribuée pour gérer les composants de Splunk, notamment la configuration, la surveillance et les mises à jour.

2.2.17 Comment splunk traite les données dans un data center pour assurer ces fonctionnalité ?

Splunk traite les données en trois étapes [44] :

a) **Entrée de données :** Splunk extrait le flux de données brutes de sa source, les découpe en morceaux de 64 ko, les enrichit avec des métadonnées tels que le nom, le type de la source de données, l'encodage de caractère et une valeur indiquant où les données doivent être indexées selon leurs contenu.

b) **Stockage de données :** dans cette étape, les données collectées passent par deux phases :
   - La phase d'analyse qui consiste à analyser les données reçues pour extraire les informations pertinentes en regroupant les données similaires dans un seul emplacement.
   - La phase d'indexation dont le but est de rendre les données accessibles facilement par les utilisateurs, de ce fait Splunk enregistre les évènements indexés dans un index.

c) **La recherche et l'interrogation de données :** à ce stade, les utilisateurs peuvent visualiser les données indexées et créer des tableaux de bord et des rapports en fonction de leurs besoins.

Splunk fonctionne donc de manière similaire à d'autres outils SIEM, mais il offre des fonctionnalités bien plus étendues que la plupart des autres solutions disponibles. Cette plateforme est capable de collecter des données à partir de différentes sources telles que des fichiers journaux, des bases de données, des applications web, des réseaux, ainsi que de recevoir des flux de données en temps réel provenant de capteurs IoT ou de systèmes de télémétrie. Après la collecte des données, Splunk les indexe pour permettre une recherche rapide et facile, ainsi que pour extraire des informations clés, détecter des modèles et des anomalies, et fournir des analyses en temps réel [45]. Cette plateforme utilise également des techniques de traitement des données pour normaliser, enrichir et corréler les données afin d'en tirer des informations exploitables. Splunk offre également des fonctionnalités de détection de menaces et d'incidents de sécurité en collectant et en analysant des données de sécurité

à partir de différentes sources. Enfin, Splunk permet aux utilisateurs d'effectuer des recherches sur les données collectées à l'aide d'une syntaxe de recherche avancée, de visualiser les résultats sous forme de graphiques, de tableaux de bord et de rapports, et de mettre en place des alertes et des notifications pour alerter les utilisateurs en cas d'événements critiques. En résumé, Splunk est une plateforme puissante et flexible, capable de répondre aux besoins de sécurité spécifiques de l'organisation, grâce à sa capacité à collecter, indexer et analyser des données de sécurité provenant de différentes sources, pour fournir des analyses en temps réel et des alertes pertinentes pour aider à protéger l'environnement informatique de l'entreprise [45].

2.3 Soc (Centres d'Opérations de Sécurité)

2.3.1 Quesque le soc ?

Le SOC est une plateforme qui héberge en permanence une équipe interne ou externe d'experts en cyber sécurité chargés d'assurer la sécurité des informations d'une entreprise [46] [19]. Il permet de surveiller et analyser en continu la posture de sécurité de l'ensemble de son infrastructure informatique, 24h/24 et 7j/7, à l'aide d'outils de collecte, de corrélation d'événements et d'intervention à distance pour détecter les comportements anormaux pouvant indiquer un incident ou une compromission de sécurité.Le SOC utilise une combinaison de solutions technologiques et un ensemble robuste de processus pour s'assurer que les incidents de sécurité potentiels sont correctement identifiés, analysés et signalés [47].

2.3.2 Pourquoi investir dans un SOC ?

Les cyberattaques sont devenues de plus en plus sophistiquées, dangereuses et couteuses pour les organisations ciblées (dégâts engendrés), ce qui oblige les entreprises à déployer des centres de sécurité SOC pour garantir une gestion efficace, une surveillance et une protection contre les menaces en ligne, ainsi que pour intervenir en cas de problème [48]. Le SOC convient particulièrement aux organisations qui cherchent à maîtriser les risques et à augmenter le niveau de sécurité de leur système d'information tout en contrôlant les coûts [49]. Pour ce faire, l'organisation doit se concentrer sur trois aspects de la sécurité : la prévention, la détection et la réaction. Elle doit également tenir compte des normes de conformité [50].

2.3.3 Piliers du SOC :

Les SOC (Security Operations Center) reposent sur trois piliers principaux :

A) L'équipe SOC

C'est un groupe de professionnels qualifiés et compétents en matière de sécurité informatique, d'analyse de données et de gestion de crise. Ce groupe veille à surveiller en permanence l'infrastructure d'une organisation en inspectant les journaux capturés à partir de différentes sources d'informations et de systèmes de sécurité, y compris les hôtes, les applications et le réseau, en utilisant des outils comme le SIEM. Les membres de l'équipe SOC doivent être formés régulièrement pour rester à jour avec les dernières technologies et les nouvelles menaces de sécurité [51].

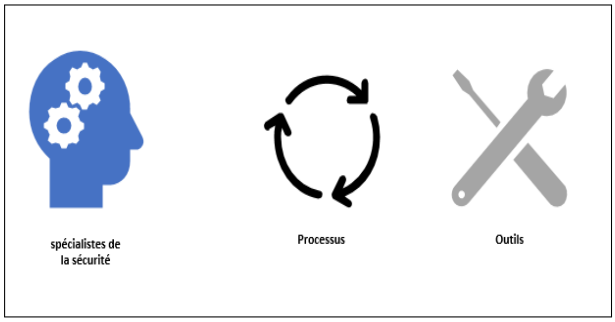

FIGURE 2.16 – Les piliers du SOC

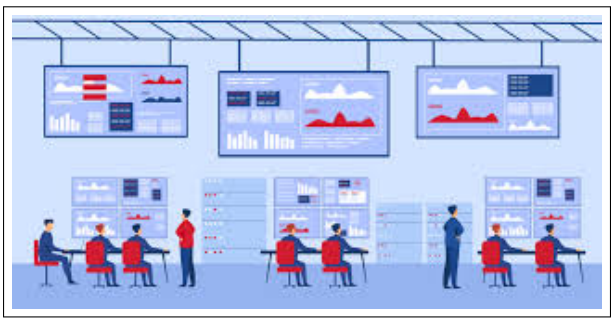

FIGURE 2.17 – Le SOC

B) Processus

Les processus consistent en une suite d'opérations et d'actions de sécurité efficaces, créant ainsi des politiques de sécurité solides et des procédures de réponse aux incidents pertinentes pour gérer efficacement la quantité de données et d'alertes provenant des outils SIEM.

C) Technologies (Solutions)

C'est l'ensemble d'outils qui aident les analystes et toute l'équipe SOC à surveiller en temps réel les actions de sécurité d'une organisation, à détecter et analyser les incidents et à y remédier. Parmi ces outils utilisés par le SOC, on trouve les systèmes SIEM, les outils d'analyse de sécurité, les pare-feu et l'antivirus [49].

2.3.4 Architecture Globale du SOC

Les SOC peuvent être organisés en tant qu'entités centralisées, distribuées ou décentralisées.

A) Soc centralisée :

C'est un centre d'opérations de sécurité qui se situe dans un point central au sein d'une entreprise où toutes les activités de cyber sécurité de toute l'infrastructure de cette organisation sont traitées.

B) SOC distribué :

C'est un centre d'opérations de sécurité conçu pour la gestion de sécurité d'une entreprise ou d'une organisation gouvernementale ayant plusieurs sites répartis dans des zones géographique différents, c'est-à-dire que les SOC distribués sont utilisés dans le cas où il est difficile d'avoir un SOC centralisé [52].

C) SOC décentralisé :

C'est un SOC où les équipes SOC sont réparties dans des différents endroits dans l'entreprise où chaque groupe de cette équipe se spécialise dans une tache de surveillance spécifique. Exemple : un groupe surveille les réseaux tandis qu'un autre surveille les applications, ce qui permet une réponse plus ciblée aux attaques [52].

2.3.5 Types de SOC :

Selon les besoins de l'entreprise, il existe plusieurs types de SOC. Voici quelques exemples courants [6] :

A) SOC interne :

Ce type de SOC est intégré à l'entreprise et est géré par les équipes et les ressources informatiques internes. L'avantage de ce type de SOC est qu'il connaît parfaitement l'entreprise, ce qui permet une communication et une réactivité accrues pour trouver rapidement des solutions aux problèmes de sécurité.

B) SOC externe :

Ce type de SOC est installé chez un fournisseur de services de sécurité qui fonctionne grâce aux équipes et aux outils du fournisseur. Les avantages de ce type de SOC sont multiples : il surveille en permanence plusieurs environnements, il dispose d'une grande expérience et peut trouver des moyens d'attaquer et d'atténuer les menaces plus efficacement.

C) SOC virtuel :

Le SOC virtuel est installé de manière logique et son équipe n'intervient que lorsqu'un incident survient ou qu'une alerte est déclenchée.

2.3.6 Comment un SIEM peut-il renforcer et automatiser les taches de soc ?

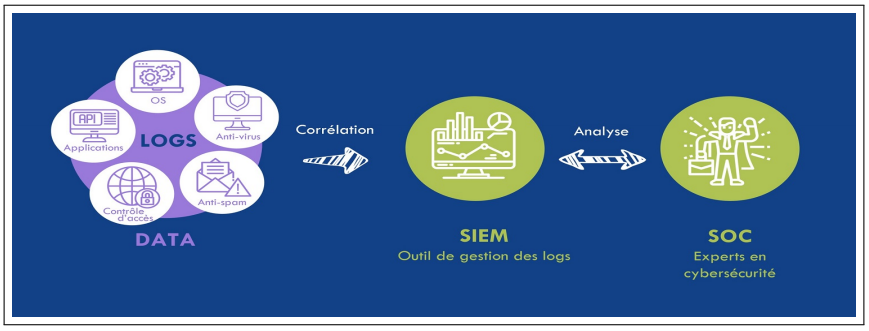

FIGURE 2.18 – SOC + SIEM

Le SIEM est un outil crucial pour les équipes SOC.Ces équipes ne peuvent pas examiner manuellement les flux de données pour détecter les activités malveillantes, et c'est là que le SIEM intervient. Il automatisera la collecte, l'organisation, la corrélation et l'analyse de toutes les données provenant de sources diverses pour signaler à l'équipe de SOC les incidents de sécurité probables. Le SIEM fournit également des outils de rapport pour répondre aux besoins des enquêtes et des obligations de conformité, ce qui peut considérablement améliorer l'efficacité et la capacité des équipes à protéger les systèmes d'information en définissant des réponses automatisées pour les alertes fréquemment détectées [37] [53].

Les capacités de gestion des logs du SIEM sont essentielles pour les tâches du SOC, telles que la surveillance, la réponse aux incidents, la gestion des logs, les déclarations de conformité et l'application des politiques. Le SIEM aide à consolider les logs et à élaborer des règles d'automatisation pour réduire considérablement le taux de fausses alertes, permettant aux analystes de sécurité de se concentrer sur les alertes critiques et à haut risque pour mieux prioriser leurs actions et renforcer la sécurité globale de l'entreprise [47].

2.3.7 Méthodologie de la réaction aux incidents :

En cas de détection d'un incident par une solution SIEM mise en place, il sera nécessaire d'allouer des ressources internes importantes pour diagnostiquer et réagir rapidement, sans avoir beaucoup de temps pour prévenir ou notifier à l'avance. Une équipe de sécurité SOC doit intervenir pour identifier, isoler et neutraliser les activités malveillantes, et enfin mettre en œuvre une réponse complète, qui inclut généralement les étapes ci-dessous :

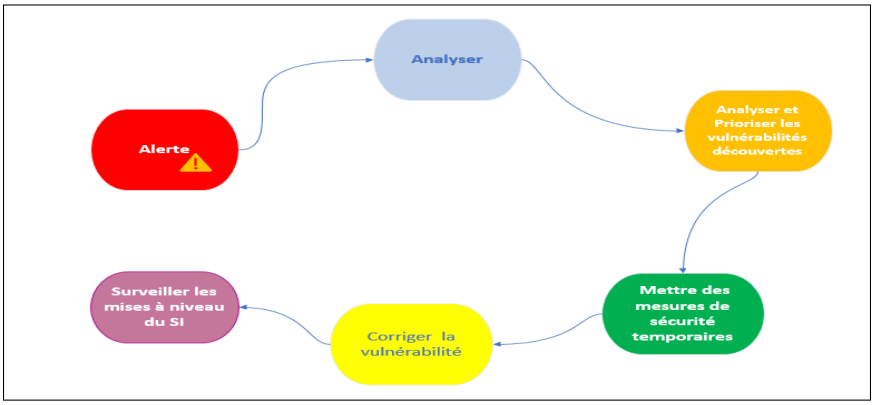

FIGURE 2.19 – Cycle de réponse aux attaques

A) Analyse d'alerte :

Lorsqu'une alerte critique est détectée par le SIEM, telle qu'une exfiltration de données via un pare-feu, une connexion non autorisée à un serveur ou une base de données, la détection d'un virus non supprimé par l'antivirus ou la suppression non autorisée d'un journal d'audit, elle est immédiatement transmise au SOC. Les analystes du SOC utilisent les informations fournies par le rapport d'incidents et le tableau de visualisation pour effectuer une analyse plus approfondie de l'environnement informatique de l'entreprise dans son ensemble. Cette analyse peut nécessiter des investigations supplémentaires pour déterminer la nature de la vulnérabilité et s'assurer qu'elle représente bien une réelle menace en vérifiant la présence ou l'absence de signes de compromission sur le système [48].

B) Analyse et Priorisation des vulnérabilités découvertes

Il s'agit d'une étape cruciale dans le processus de réponse à un incident initié par l'équipe du SOC. Cette analyse permet de comprendre pleinement le comportement et les objectifs des programmes malveillants spécifiques qui ciblent l'entreprise, afin d'évaluer leur criticité, leur impact potentiel et leur niveau de risque pour le système d'information [54]. Elle inclut l'évaluation de la portée de la vulnérabilité, la présence d'attaquants motivés, l'importance des services impactés et l'impact sur la

continuité des activités. Il est également essentiel de déterminer les conséquences probables, telles que la perte de données, l'indisponibilité de services critiques, la violation de la confidentialité des données et la perte de réputation. En fin de compte, cette analyse aide à prioriser les mesures de réponse appropriées pour minimiser les risques et réduire les impacts négatifs de l'incident [48].

L'équipe SOC mène cette phase dans le but de hiérarchiser les vulnérabilités en fonction de leur gravité et de leur impact potentiel sur l'entreprise. Cette hiérarchisation permet de prioriser les mesures de sécurité appropriées pour minimiser les risques et protéger efficacement l'entreprise contre les menaces [48].

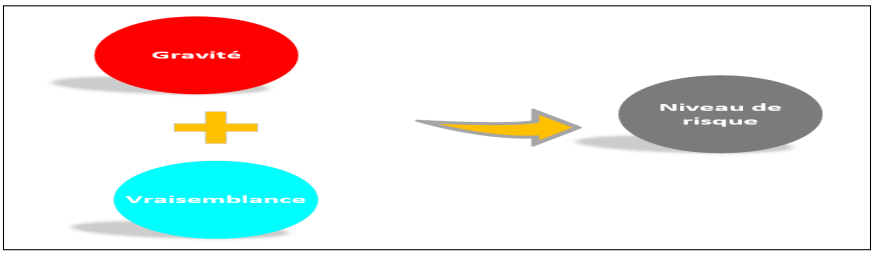

Figure 2.20 – Détermination du niveau de risque

C) Mise en place de mesures de sécurité temporaires :

L'étape suivante dans le processus de réponse à un incident est cruciale pour l'équipe SOC . Les analystes du SOC utilisent les informations du rapport de la solution SIEM et des résultats d'analyse d'alerte pour identifier les systèmes affectés par l'incident. Ils peuvent également utiliser d'autres outils de surveillance pour confirmer les résultats de l'analyse initiale. Ensuite, le SOC informe les parties prenantes concernées, telles que le personnel informatique, les responsables de la sécurité et les fournisseurs de services, afin de coordonner les efforts de réponse. En parallèle, le SOC prend immédiatement des mesures de sécurité temporaires pour minimiser l'impact de l'attaque sur l'entreprise et réduire les temps d'arrêt des services. Ces mesures peuvent inclure la désactivation de certains services ou la restriction de l'accès aux systèmes affectés pour empêcher la propagation de l'attaque et la compromission d'autres systèmes [48] [55].

Mise en place de ces mesures temporaires permet au SOC de contrôler la situation et de protéger l'entreprise en attendant l'application de mesures de sécurité plus permanentes. Les mesures temporaires sont évaluées régulièrement pour s'assurer de leur efficacité et de leur adéquation face à l'incident. Les équipes SOC travaillent en étroite collaboration avec les équipes d'intervention afin de résoudre rapidement les problèmes de sécurité et de minimiser leur impact. Une fois que l'incident a été résolu, le SOC procède à une analyse post-mortem pour identifier les causes profondes et proposer des mesures préventives pour éviter que l'incident ne se reproduise.

D) Mise en œuvre des services de sécurité pour corriger la vulnérabilité

Le service de réponse aux incidents est un service important qui gère l'ensemble du processus de correction des vulnérabilités. Cela comprend la conception d'un plan complet pour éliminer la menace du système informatique [54]. Les SOC doivent se concentrer sur des stratégies de correction efficaces en utilisant des outils de gestion de correctifs ou en les appliquant manuellement sur chaque machine. Cela peut inclure l'installation de correctifs de sécurité et la mise à jour régulière des logiciels. Ils peuvent également désactiver certaines fonctionnalités ou modifier la configuration des systèmes et de la sécurité pour réduire les risques. Par exemple, ils peuvent configurer des pare-feux pour bloquer

les connexions suspectes ou utiliser des outils de détection d'intrusion. Les SOC doivent également suivre la mise en œuvre des mesures de sécurité pour s'assurer que la vulnérabilité a été corrigée avec succès [48].

E) Mise à niveau des SI surveillés

La surveillance continue et la réévaluation sont des éléments essentiels du processus de correction d'incident. Une fois qu'un incident de sécurité a été corrigé, il est important de continuer à surveiller les systèmes de sécurité pour s'assurer que les mesures de sécurité mises en place sont efficaces [54].

2.3.8 Avantages du SOC

Les principaux avantages d'avoir un SOC au sein d'une entreprise sont [46] :

- ▷ Assurer la protection des données sensibles telles que les données clients, les propriétés intellectuelles, les informations financières et les opérations commerciales.
- ▷ Surveillance 24h/24 et 7j/7 des activités suspectes qui peuvent se produire à tout moment au sein de l'infrastructure informatique.
- ▷ Conformité aux règles de l'industrie telles que la norme PCI DSS, HIPAA, GDPR et des règles gouvernementales (SCCEE GPG53).
- ▷ Détection et réponse rapide et efficace aux incidents de sécurité pour minimiser l'impact de l'attaque sur l'entreprise.
- ▷ Prévention et recherche proactive des menaces.
- ▷ Une visualisation globale de l'état de la cyber sécurité de l'entreprise.

2.4 Conclusion

Dans ce chapitre, nous avons abordé les aspects essentiels pour mettre en place un système de sécurité de l'information efficace et proactif, capable de détecter et de prévenir les menaces. Les SIEM et les SOC sont deux éléments clés de la sécurité de l'information pour les organisations. Les SIEM sont des plateformes logicielles qui permettent de collecter des données provenant de différents systèmes et applications, de les corréler et de les analyser pour identifier des modèles et des anomalies. Ils sont également en mesure de détecter les menaces potentielles et de fournir une réponse rapide pour minimiser les impacts sur l'entreprise. Les SOC sont des centres de commandement et de contrôle pour la sécurité de l'information, fournissant une vue d'ensemble de la sécurité des systèmes et des réseaux de l'entreprise. Ainsi, ils peuvent enquêter sur les alertes pour confirmer ou infirmer les menaces et déterminer la meilleure façon d'y répondre. Dans la première section, nous avons commencé par définir les SIEM en définissant les logs, leur importance, leurs différents formats et types. Ensuite, nous avons exploré le rôle du SIEM dans l'entreprise et ses missions, en détaillant son cycle de fonctionnement. Par la suite, nous avons comparé différentes solutions SIEM, en expliquant leur fonctionnement ainsi que leurs avantages et inconvénients. Enfin, nous avons choisi une solution SIEM en fonction de certains critères et avons expliqué son fonctionnement en détail. Dans la seconde section, nous avons vu l'importance des SOCs pour les entreprises, et la manière dont ces dernières peuvent en tirer avantage pour grandement améliorer le niveau de sécurité de leurs données. Dans le prochain chapitre, nous allons détailler les étapes de déploiement et de simulation d'une solution SIEM Splunk sous une architecture proposée de l'infrastructure réseau de l'entreprise SONATRACH.

Chapitre 3

Mise en place de la solution proposée

3.1 Introduction

Après avoir présenté dans les chapitres précédents une étude approfondie sur l'ensemble des concepts théoriques liés à notre cas d'étude, nous nous concentrerons dans ce chapitre sur la mise en œuvre de la solution SIEM proposée pour la réalisation de notre projet d'étude. Nous exposerons les différentes configurations nécessaires afin de créer l'infrastructure réseau fonctionnelle de l'organisme d'accueil sur laquelle notre solution sera déployée (à voir dans l'annexe jointe). Ensuite, nous aborderons les étapes clés de l'installation du serveur Splunk sur cet environnement, notamment la configuration des sources de données, la création de tableaux de bord et l'exploitation des fonctionnalités avancées de Splunk pour la détection de menaces. Enfin, nous évaluerons les performances des résultats de la solution à l'aide de prototypes d'attaque.

3.2 Présentation de l'environnement de travaille

3.2.1 Ressources Matériels utilisés

Pour la simulation et le déploiement de notre projet nous avons utilisé deux ordinateurs portables dont les caractéristiques sont présentées dans le tableau suivant :

Caractéristiques	Lenovo Thinkpad	Dell
Processeur	AMD Ryzen 3 Pro 4450U with Radeon Graphics 2.50 GHz	Intel® Core™(TM) i5-3320M CPU @ 2.60 GHz
Mémoire RAM	8 Go	8 Go
Type du système	Système d'exploitation 64 bits	Système d'exploitation 64 bits
Système d'exploitation	Windows 10 Professionnel	Windows 10 Professionnel
Type du disque dur	256 SSD	256 Go SSD

Table 3.1 – Caractéristiques des ordinateurs

3.2.2 Environnement matériel et outils de simulation

GNS3

Afin de recréer au mieux une architecture réseau réelle, nous avons choisi d'utiliser GNS3, un programme de simulation réseau libre. Il offre une interface graphique intuitive qui permet de connecter et de configurer les équipements virtuels, ainsi que de tester leur connectivité.

VMware Workstation 17

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 17. C'est un logiciel de virtualisation payant. Il nous permet de créer plusieurs machines virtuelles avec différents systèmes d'exploitation sur notre ordinateur physique où on peut créer des applications, faire des tests de sécurité et configurer des réseaux.

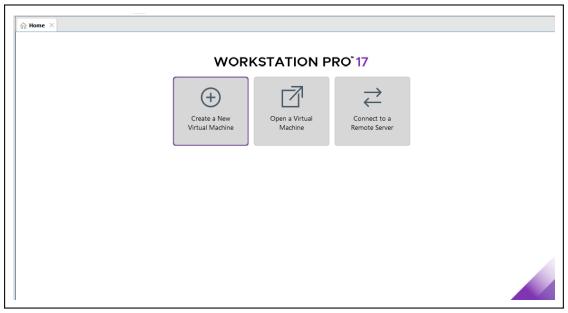

FIGURE 3.1 – L'environnement VMware Workstation

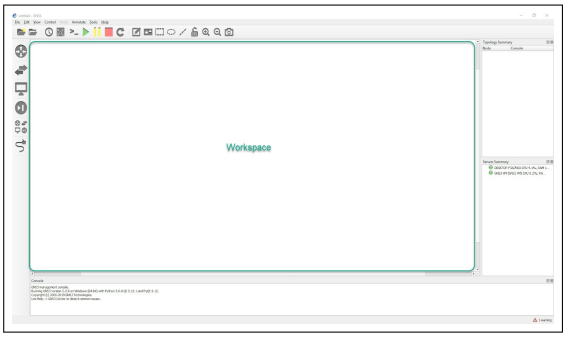

FIGURE 3.2 – Interface GNS3

3.2.3 Prérequis logiciels Systèmes d'exploitations

Composant	Version	Service Installé	Prérequis
Windows Server	2022	Splunk	RAM : 4Go
Windows	10	Splunk Forwarder	RAM : 2Go
Ubuntu	18	Splunk Forwarder	RAM : 2Go
Kali Linux	2021	Poste-hacker	RAM : 1Go

TABLE 3.2 – Les Prérequis logiciels & Systèmes d'exploitations

3.2.4 Préparation du plan d'adressage des différents VLANs

Le tableau 3.3 présente la liste des VLAN disponibles sur l'architecture réseau de la RTC Béjaïa, leurs noms, leurs identifiants ainsi que leurs plages d'adressage.

VLAN id	Description	Plage d'adressage
200	Direction	10.0.200.0/24
201	Informatique	10.0.201.0/24
202	RH	10.0.202.0/24
203	Menager	10.0.203.0/24
204	WiFi	10.0.204.0/24
205	Voice	10.0.205.0/24
206	Servers	10.0.206.0/24
207	HSE	10.0.207.0/24
997	Native 1	/
998	Native 2	/
999	Native 3	/

TABLE 3.3 – Tableau des VLANs

3.3 Mise en place d'une infrastructure réseau proposée pour le déploiement d'une solution SIEM

Il est quasiment impossible d'implémenter toute l'infrastructure réseau de la RTC Bejaia de SONATRACH avec les solutions réseau et système proposées. Du coup, nous avons simplifié l'architecture pour permettre la mise en place de notre solution. La figure 3.3 illustre la nouvelle architecture simplifiée captée sous GNS3.

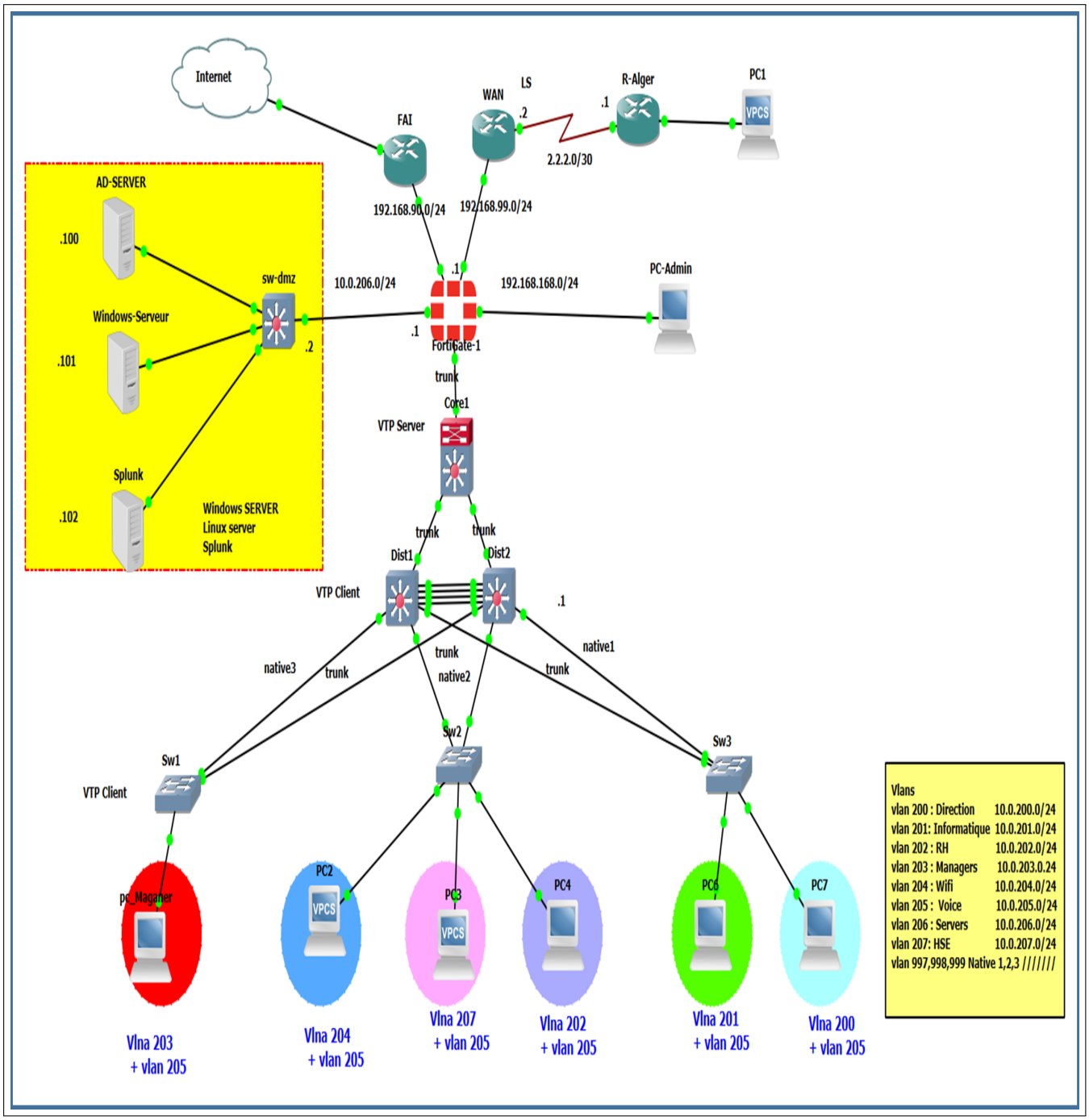

FIGURE 3.3 – L'architecture réseau proposée

3.3.1 Configuration de l'infrastructure réseau pour la rendre fonctionnelle

Ce diagramme présente les étapes de l'ensemble des configurations nécessaires afin de créer l'infrastructure réseau fonctionnelle de l'organisme d'accueil sur laquelle notre solution sera déployée, (voir les étapes d'installation et de configuration du LAB sur l'annexe A).

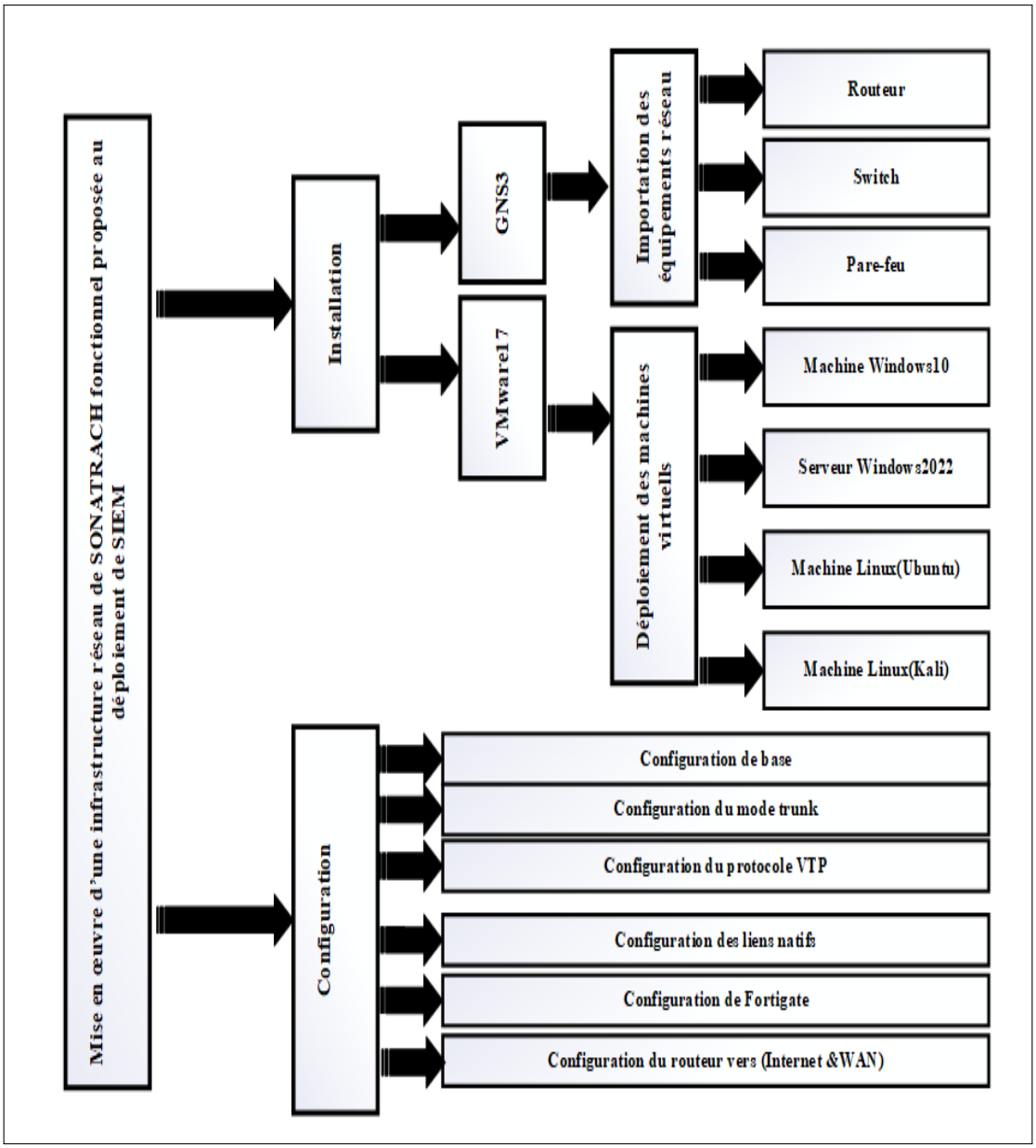

FIGURE 3.4 – Diagramme de déploiement et de configuration de notre infrastructure réseau.

3.4 Mise en œuvre de la solution Splunk

3.4.1 présentation du Plan de mise en œuvre de la solution

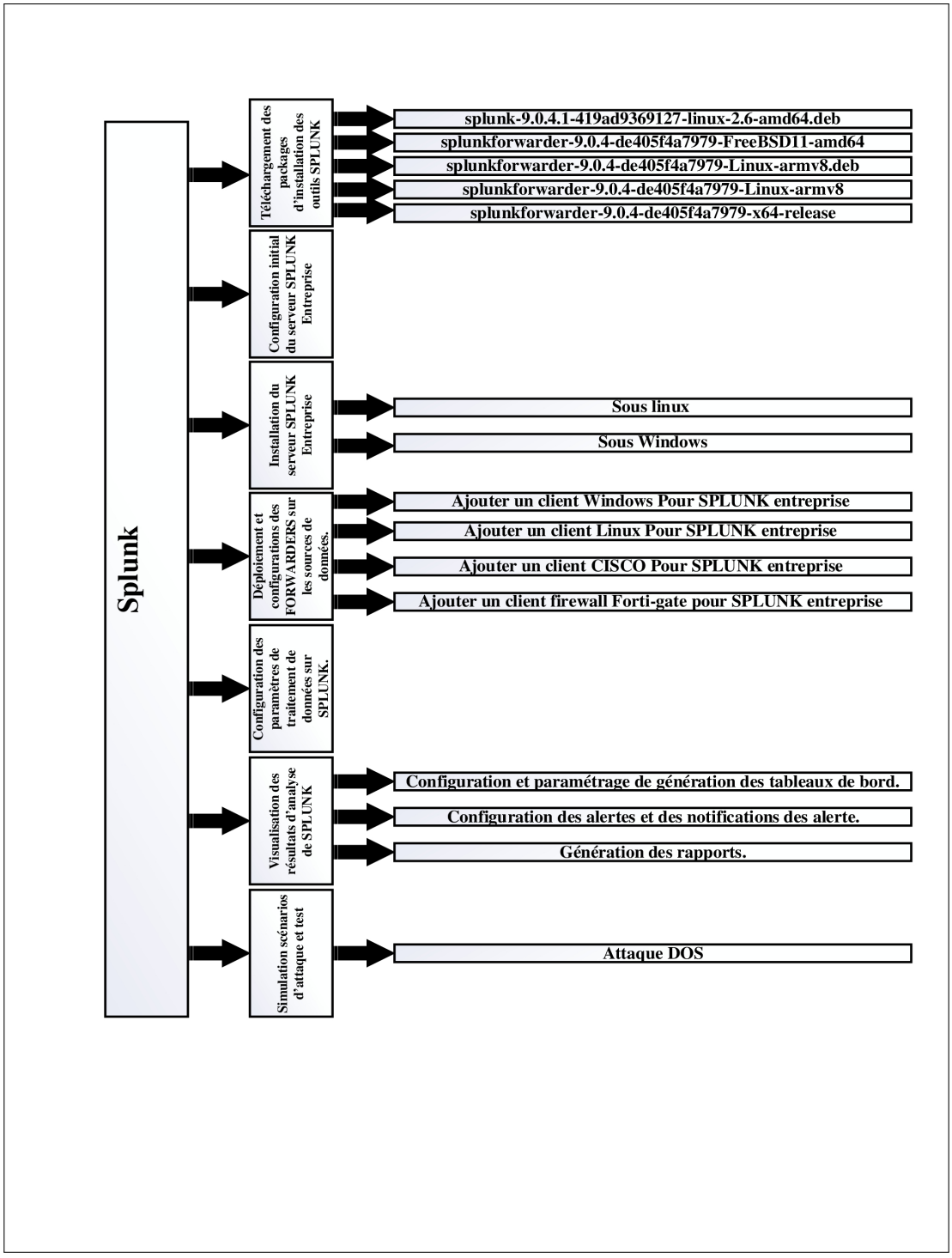

FIGURE 3.5 – Plan du mise en ouvre de la solution

3.4.2 Installation du serveur Splunk Entreprise

Étant donné que notre entreprise déploie des serveurs Windows et Linux, nous avons le choix de déterminer sur quel système installer Splunk.

Dans cette partie, nous lançons l'installation de Splunk Enterprise sur un serveur Windows 2022 en suivant les instructions d'installation, comme le montrent les figures ci-dessous :

— Démarrer le programme d'installation ;

— Accepter les termes du contrat de licence ;

— Sélectionner un utilisateur système local et cliquer sur Suivant ;

— Lancer l'installation de Splunk dans le répertoire d'emplacement par défaut "/ProgramFiles/Splunk".

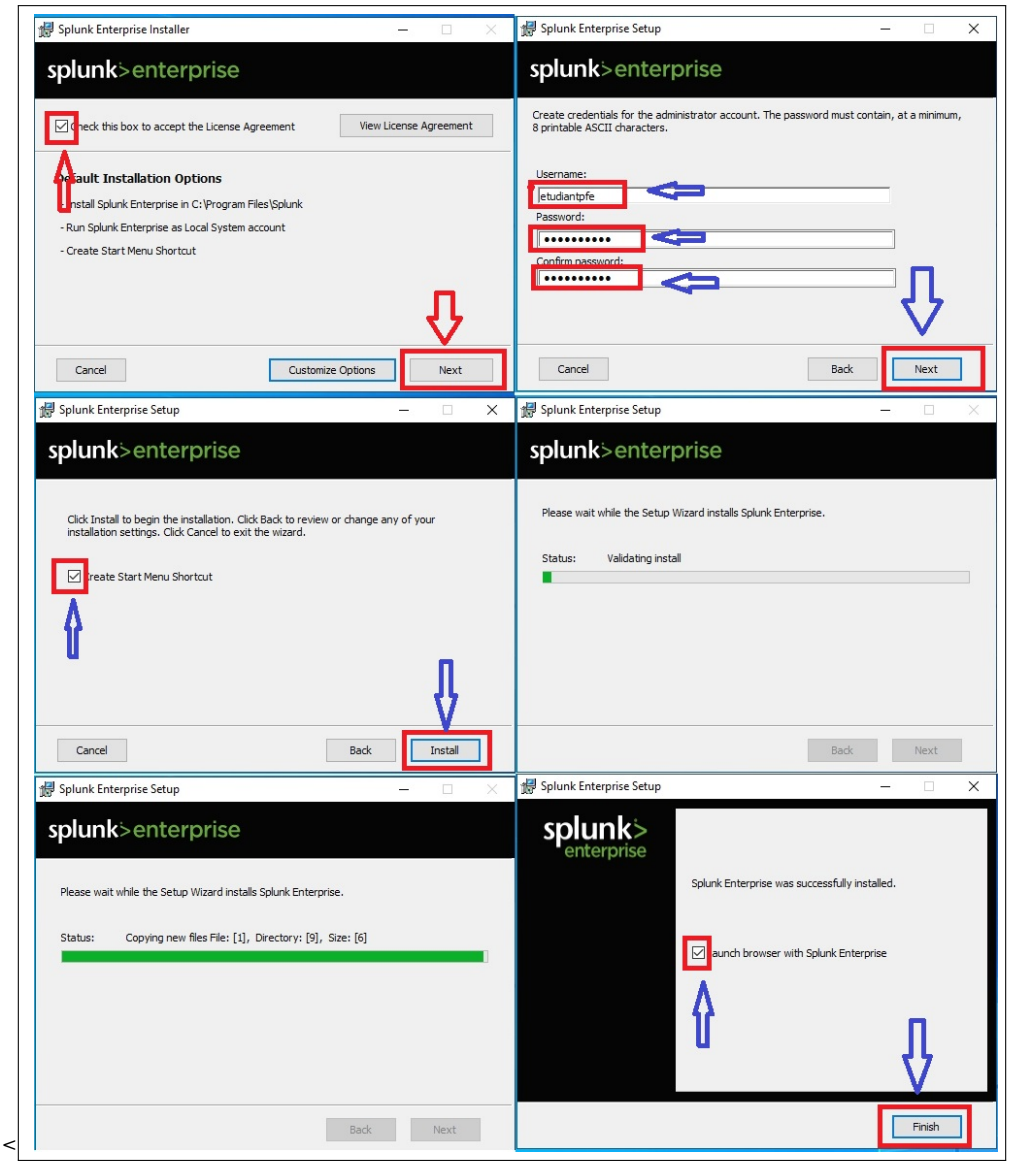

FIGURE 3.6 – Etapes d'installation de Splunk

Pour accéder a l'interface web du serveur Splunk installée, via un navigateur logez (naviguez) vers l'adresse (127.0.0.1 :8000).

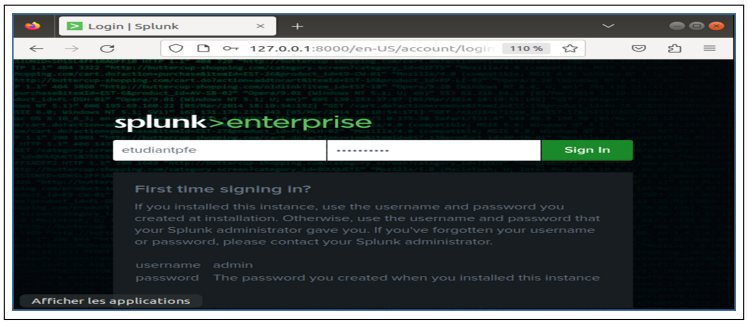

FIGURE 3.7 – Login vers l'interface Utilisateur de Splunk

3.4.3 Déploiement des Forwarders sur les sources de données

Dans cette section, nous présenterons les différentes étapes d'installation des packages des Forwarders sur les différentes sources de journalisation de notre LAB de solution. Cela permettra la collecte de données et de journaux de sécurité.Nous utiliserons principalement des Forwarders universels comme collecteurs de logs, ainsi que le protocole Syslog.

A) Ajouter un client Windows pour Splunk entreprise

Nous commençons par lancer le package d'installation du Forwarder sur un poste utilisateur Windows dans notre cas d'étude. Ensuite, nous suivons les instructions d'installation, y compris l'acceptation du contrat de licence et la configuration des options d'installation, comme le détaille la (figure 3.8) .

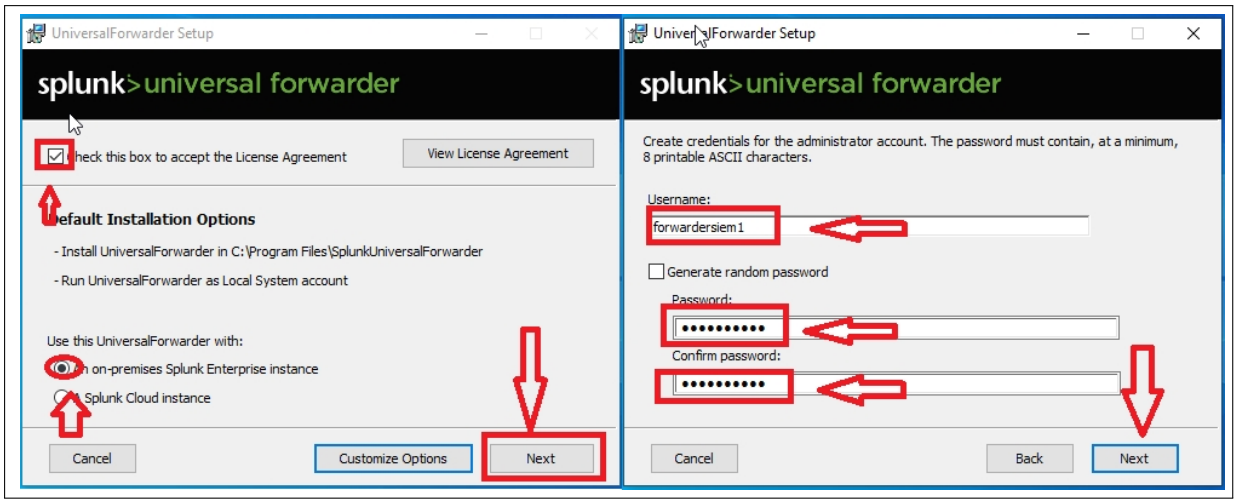

FIGURE 3.8 – Etapes d'installation de Splunk Forwarder sous Windows

Nous spécifions l'adresse et le port du serveur de déploiement utilisés pour recevoir les configurations de manière centralisée et déployer ces configurations sur les Forwarders. Cela inclut l'administration et la gestion du déploiement Splunk, y compris les rôles, les utilisateurs, les autorisations, les configurations d'index, etc.

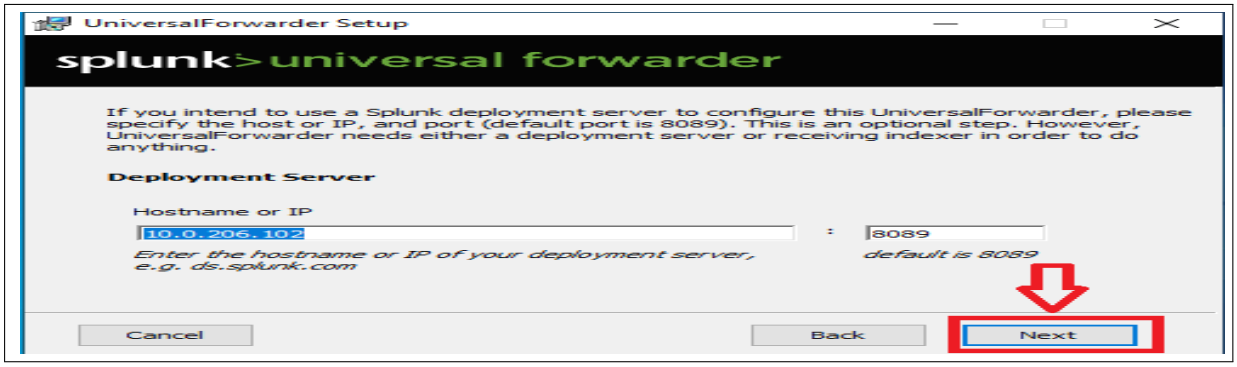

FIGURE 3.9 – Association de l'adresse IP et le port de déploiement serveur Splunk

Nous associons l'adresse et le port d'indexeur serveur utilisée pour spécifier le serveur Splunk qui recevra les données collectées par le Forwarder, pour l'indexation et l'analyse.

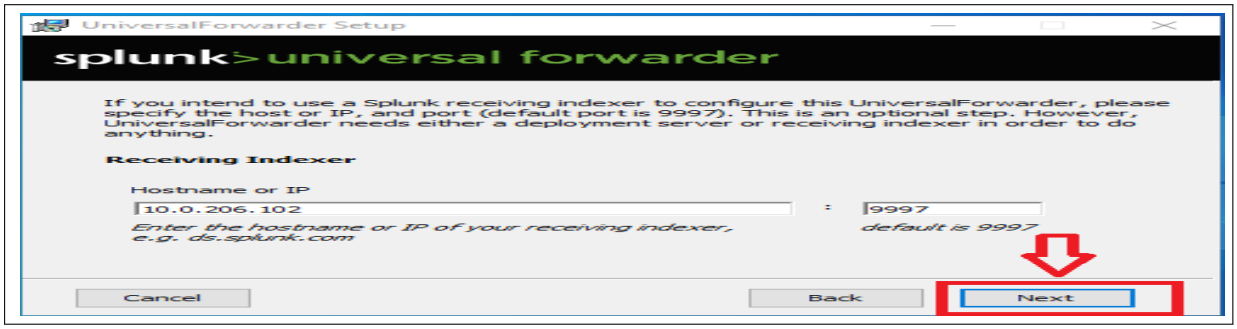

FIGURE 3.10 – Association de l'adresse IP et le Port d'indexeur serveur Splunk

Puis lancer l'installation comme le montre la figure ci-dessous :

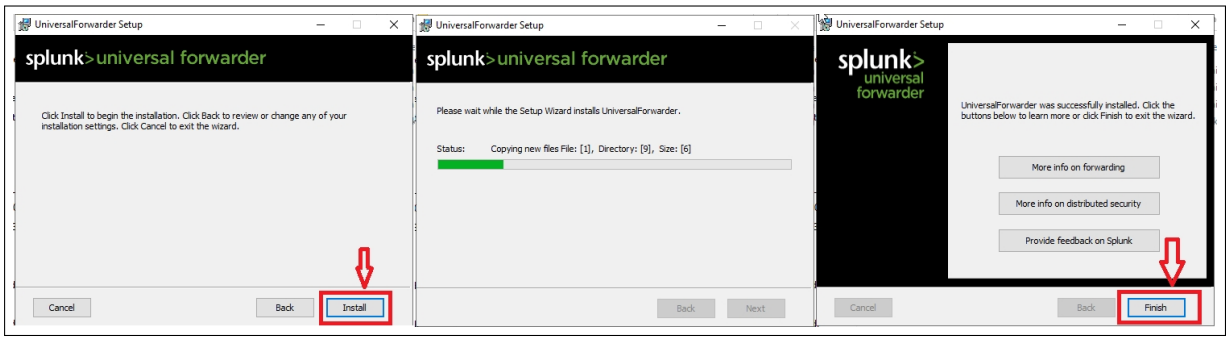

FIGURE 3.11 – Lancement d'installation de Splunk

Les mêmes étapes d'installation de cet agent sont adaptées sur d'autres distribution Windows (serveur/ou poste client).

2) Activer le port de réception de données via les Forwarders

Sous l'interface web de Splunk (dans l'onglet "Paramètres"), nous accédons au paramètre de "Transmission et Réception". Cela nous permettra d'activer la réception via les Forwarders et d'ajouter un port d'écoute, comme le montre la figure (figure 3.12) ci-dessous :

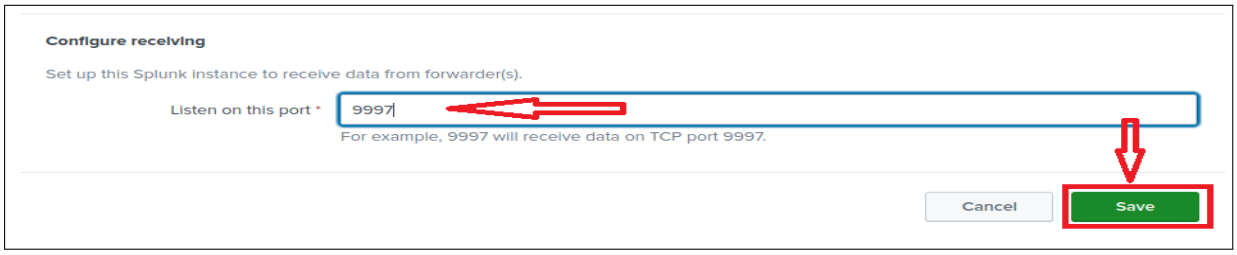

FIGURE 3.12 – Activation du port d'écoute sur le serveur Splunk

Il reste à autoriser la transmission des logs collectés. Nous allons créer une règle de filtrage sortante permissive sur le pare-feu du poste utilisateur. De plus, il faut autoriser la réception des logs en ajoutant une règle permissive sur le pare-feu du serveur Splunk.

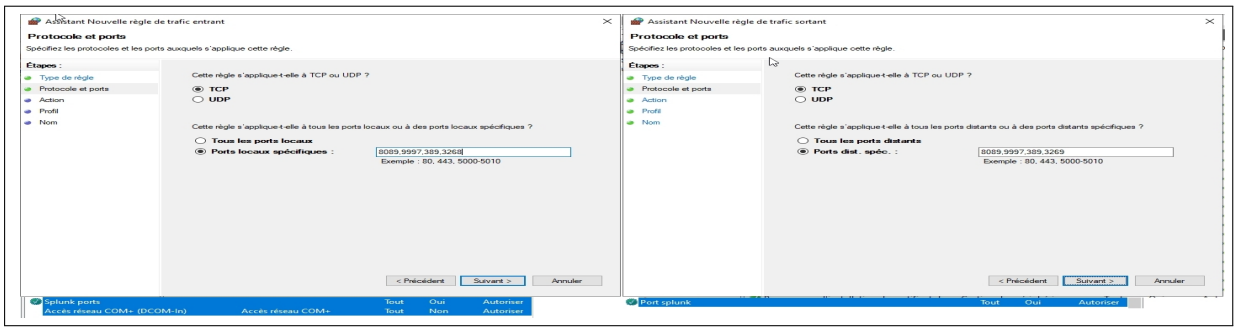

FIGURE 3.13 – Création d'une règle de filtrage

Dans cette sous-partie, nous allons ajouter le Forwarder configuré à Splunk et récupérer les sources de données du poste utilisateur. Pour cela, nous allons naviguer vers l'onglet "Ajouter des données" puis sélectionner "Transmettre des données". Une liste des machines sources de données de Splunk apparaîtra, où nous pourrons assigner un nom de catégorie de logs. Ensuite, nous choisirons ce que nous voulons récupérer comme données ou surveiller, que ce soit les logs d'événements locaux, les fichiers et répertoires, ou configurer la plateforme Splunk pour écouter un port réseau. Tout cela est illustré dans la (figure 3.14).

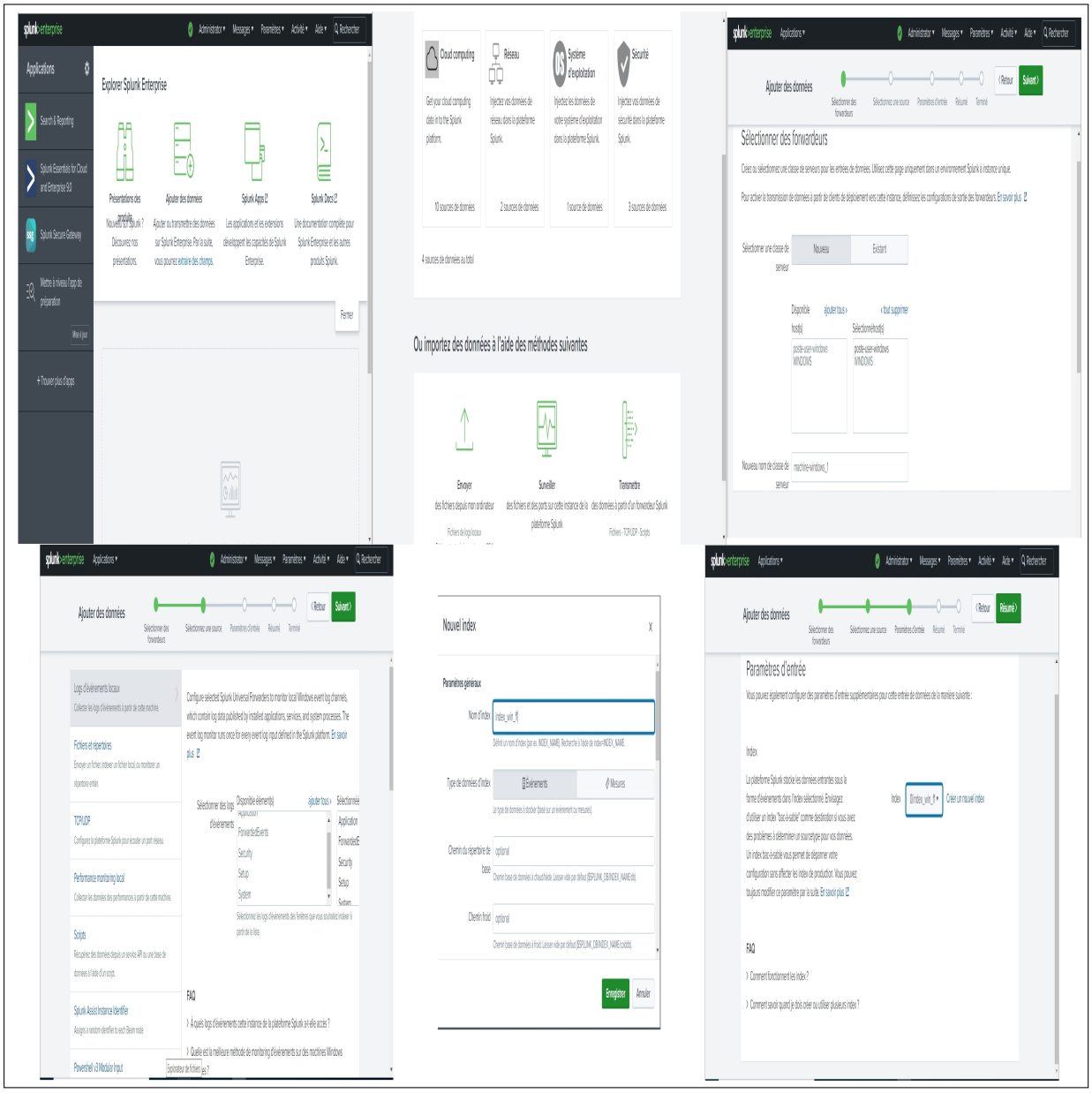

FIGURE 3.14 – Ajout de l'index Windows Forwarder

Nous allons effectuer par la suite une recherche par indexation pour récupérer les événements et informations de sécurité liées a "poste user Windows" comme le montre la (figure 3.15).

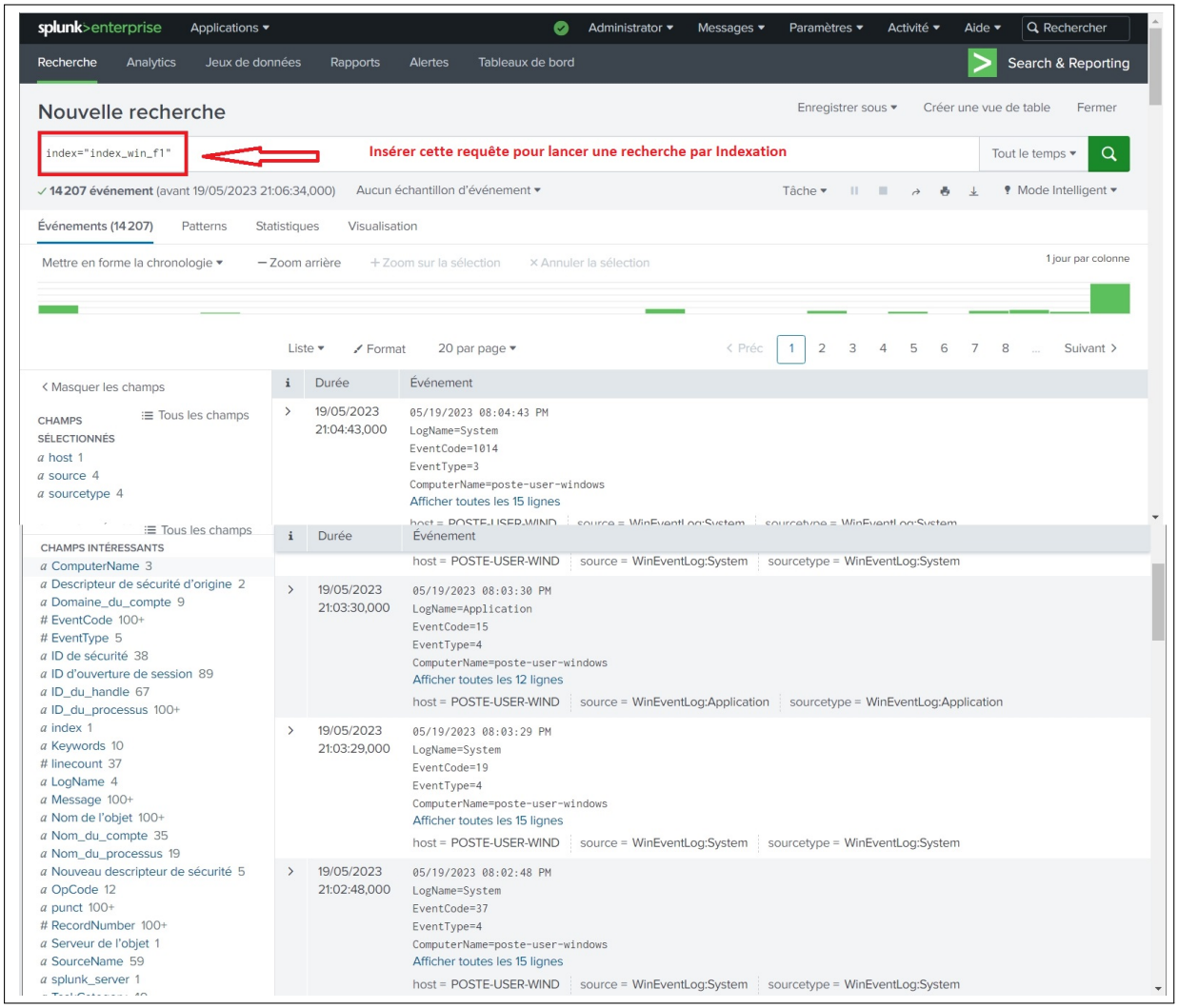

FIGURE 3.15 – Logs récupérés

B) Ajouter un client Linux pour Splunk entreprise

Nous allons déployer un client Linux pour notre serveur Splunk. Pour commencer, nous allons créer un index pour ce Forwarder au niveau de notre serveur Splunk, comme le montre la figure ci-dessous.

FIGURE 3.16 – Création de l'index Forwarder Linux

Puis sur le client Splunk, nous allons installé un serveur NGINX en amont de ce dernier pour des raisons de sécurité et de gestion de trafic. Ensuite, nous lançons l'installation du package de Forwarder en utilisant les lignes de commande illustrées dans la (figure 3.17).

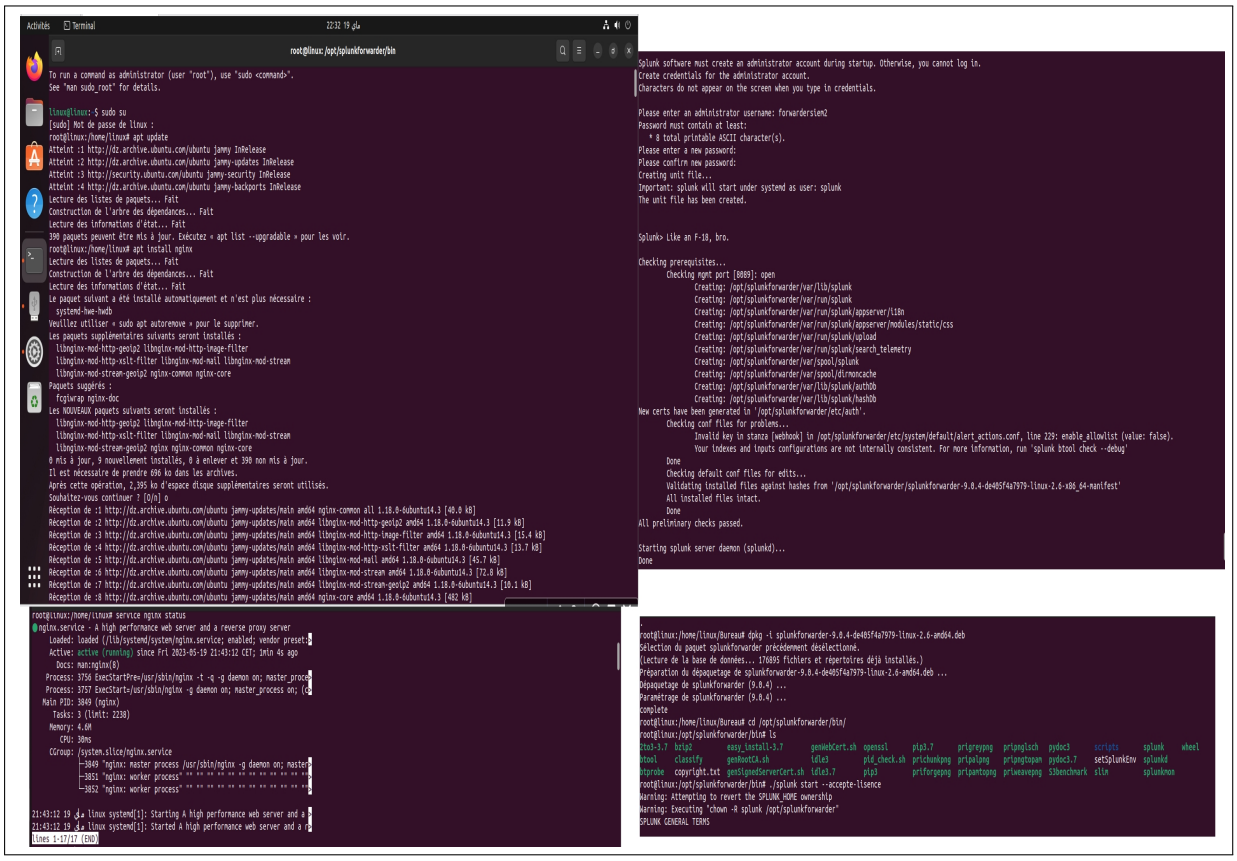

FIGURE 3.17 – Installation du serveur NGINX

Reste à spécifier au Forwarder l'adresse IP vers laquelle envoyer les données collectées .

FIGURE 3.18 – Spécification de l'adresse IP du Serveur Splunk

Les lignes de commande suivantes permettent de spécifier quels fichiers ou répertoires doivent être surveillés et collectés par le Forwarder

FIGURE 3.19 – Répertoires et fichiers à surveiller

Nous allons personnaliser les paramètres de collecte de logs (source type, etc.)

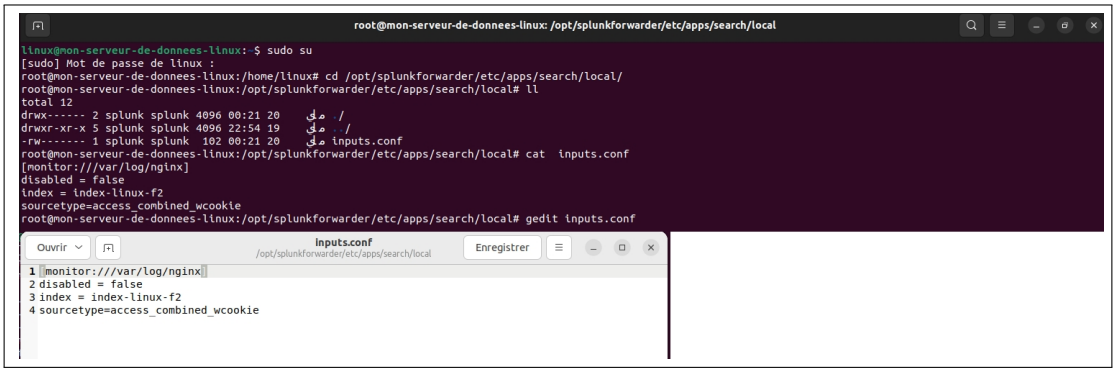

FIGURE 3.20 – Illustration des parametres de collecte de Log

Pour s'assurer que le Forwarder a été bien installé, on effectue une requête de recherche dans la barre de recherche de mon serveur Splunk en utilisant l'indexation, comme illustré dans la figure, afin de récupérer les logs de mon Forwarder.

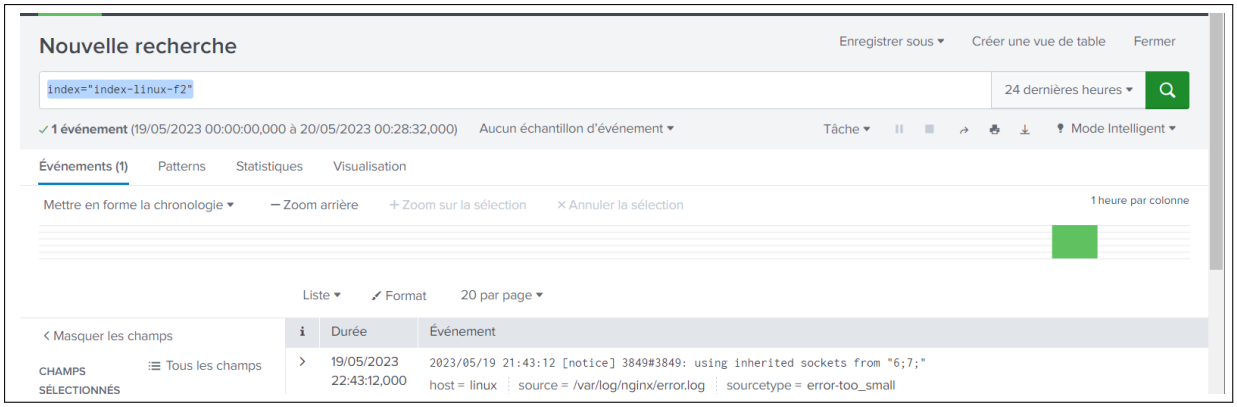

FIGURE 3.21 – Recherche par indexation

C) Ajouter un client CISCO Pour Splunk Entreprise

Cette phase consiste à récupérer les logs des équipements Cisco (routeurs, commutateurs) et les transmettre vers le serveur Splunk en utilisant le protocole Syslog.

a) Configuration de l'infrastructure Cisco pour transmettre les logs

Tout d'abord, nous devons créer une règle de filtrage sur le pare-feu FortiGate pour autoriser le trafic (la transmission des fichiers logs vers le serveur Splunk sur la DMZ).

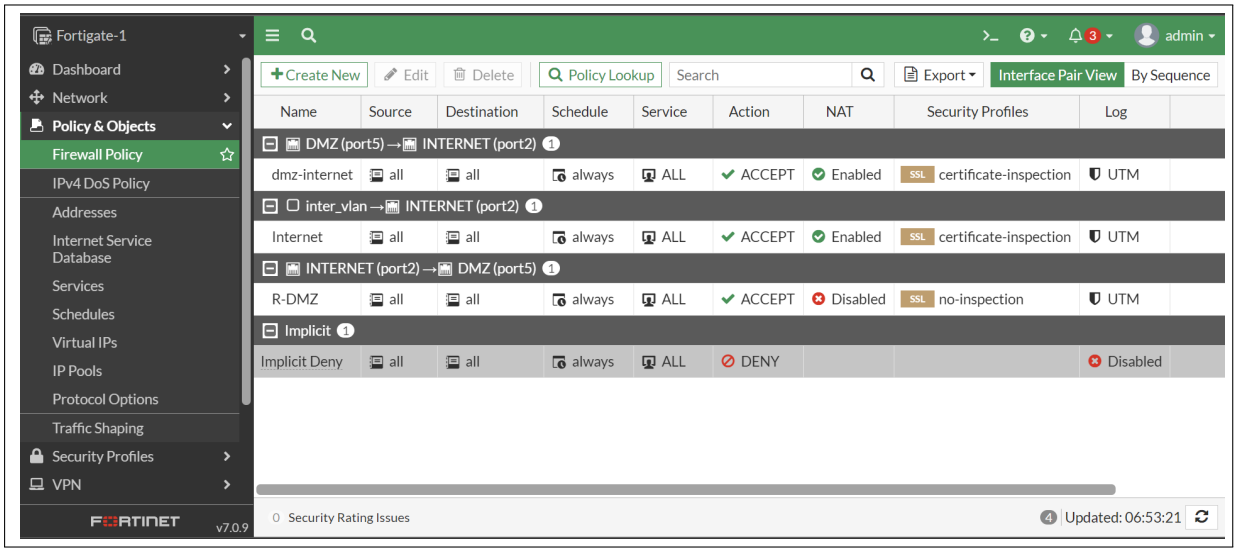

FIGURE 3.22 – Configuration des régles de filtrage

Maintenant, nous allons configurer le logging. Nous commençons par spécifier l'adresse IP et le port du serveur Splunk, puis nous spécifions des options supplémentaires de configuration des logs (type et taille des logs à transmettre). Enfin, nous activons le logging et informons le serveur Splunk. Ces étapes sont illustrées dans la (figure 3.23).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#loggin trap informationnal
                  ^
% Invalid input detected at '^' marker.

R1(config)#loggin trap informational
R1(config)#logging host 10.0.206.102 transport udp port 514
R1(config)#archive
R1(config-archive)#log config
R1(config-archive-log-cfg)#logging enable
R1(config-archive-log-cfg)# logging size 200
R1(config-archive-log-cfg)#notify syslog
R1(config-archive-log-cfg)#
*May 20 09:46:00.114: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:notify syslog
R1(config-archive-log-cfg)#hidekeys
R1(config-archive-log-cfg)#
*May 20 09:46:24.865: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:hidekeys
R1(config)#logging userinfo
R1(config)#
*May 20 09:48:16.620: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:logging userinfo
R1(config)#login on-f
R1(config)#login on-failure
R1(config)#l
*May 20 09:49:13.799: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:login on-failure
R1(config)#login on-su
R1(config)#login on-success
R1(config)#
*May 20 09:49:23.805: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:login on-success
R1(config)#enable sec
R1(config)#enable secret gns3
R1(config)#
*May 20 09:50:15.699: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:enable secret *
R1(config)#exit
R1#
*May 20 09:50:20.044: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
```

FIGURE 3.23 – Configuration de Login

Nous devons ensuite créer une règle entrante de filtrage permissive sur le pare-feu du serveur Splunk, comme indiqué dans la (figure 3.24) .

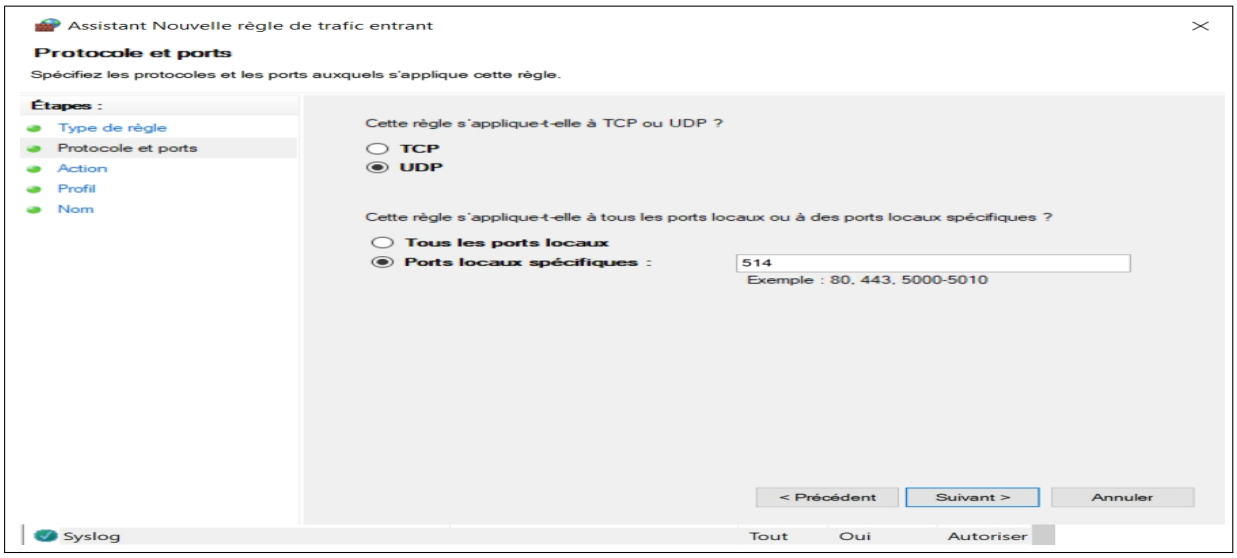

FIGURE 3.24 – Création de la règle de filtrage

b) Installation du module complémentaire Splunk pour Cisco ISE

Dans cette partie, nous allons télécharger et installer le module complémentaire (add-on) qui permet d'intégrer les données de Cisco ISE dans la plateforme Splunk, afin de les analyser et les visualiser de manière centralisée. Nous suivrons les étapes définies dans la (figure 3.25)

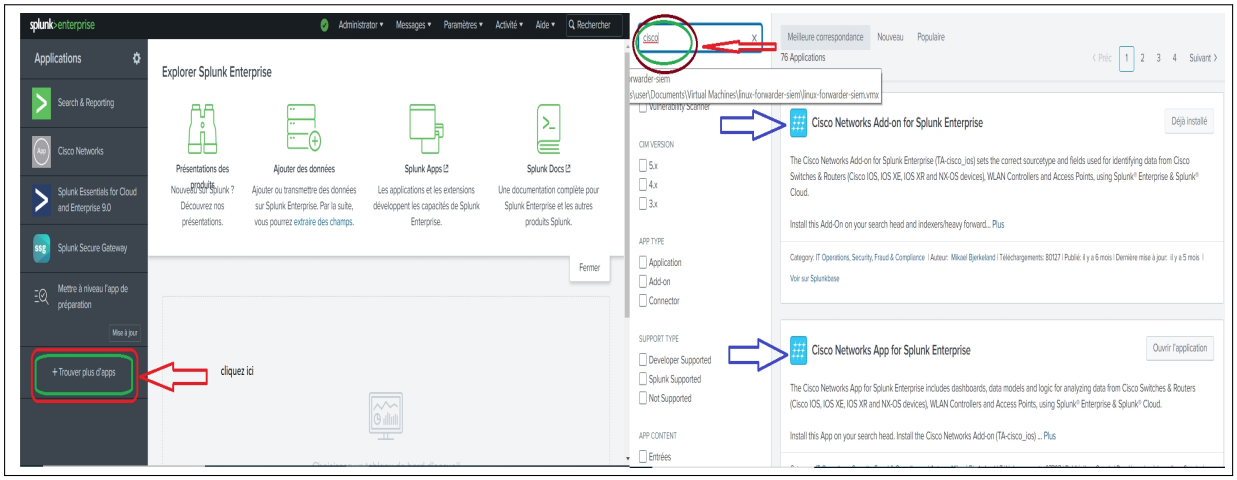

FIGURE 3.25 – Splunk Forwarder sous Routeur CISCO

Maintenant, il est temps de récupérer les logs en utilisant "Protocole Syslog" déployé sous le routeur Cisco, nous générons d'abord des activités de journalisation tests sur le routeur.

```
R1#disable
R1>
*May 20 18:59:35.061: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 1 by unknown on console
R1>enable
Password:
Password:
Password:
% Bad secrets

R1>
*May 20 18:59:45.989: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 15 failed by  unknown on console
*May 20 18:59:45.990: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:!exec: enable failed
R1>enable
Password:
R1#
*May 20 18:59:52.934: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by unknown on console
*May 20 18:59:52.934: %PARSER-5-CFGLOG_LOGGEDCMD: User:console  logged command:!exec: enable
R1#
```

FIGURE 3.26 – Activités de journalisation tests sur le routeur cisco

Pour récupérer ce dernier sur l'instance Splunk, on accède à : Ajouter des Données puis surveiller,et nous allons configurer les paramètres de récupération de logs (index, etc.)

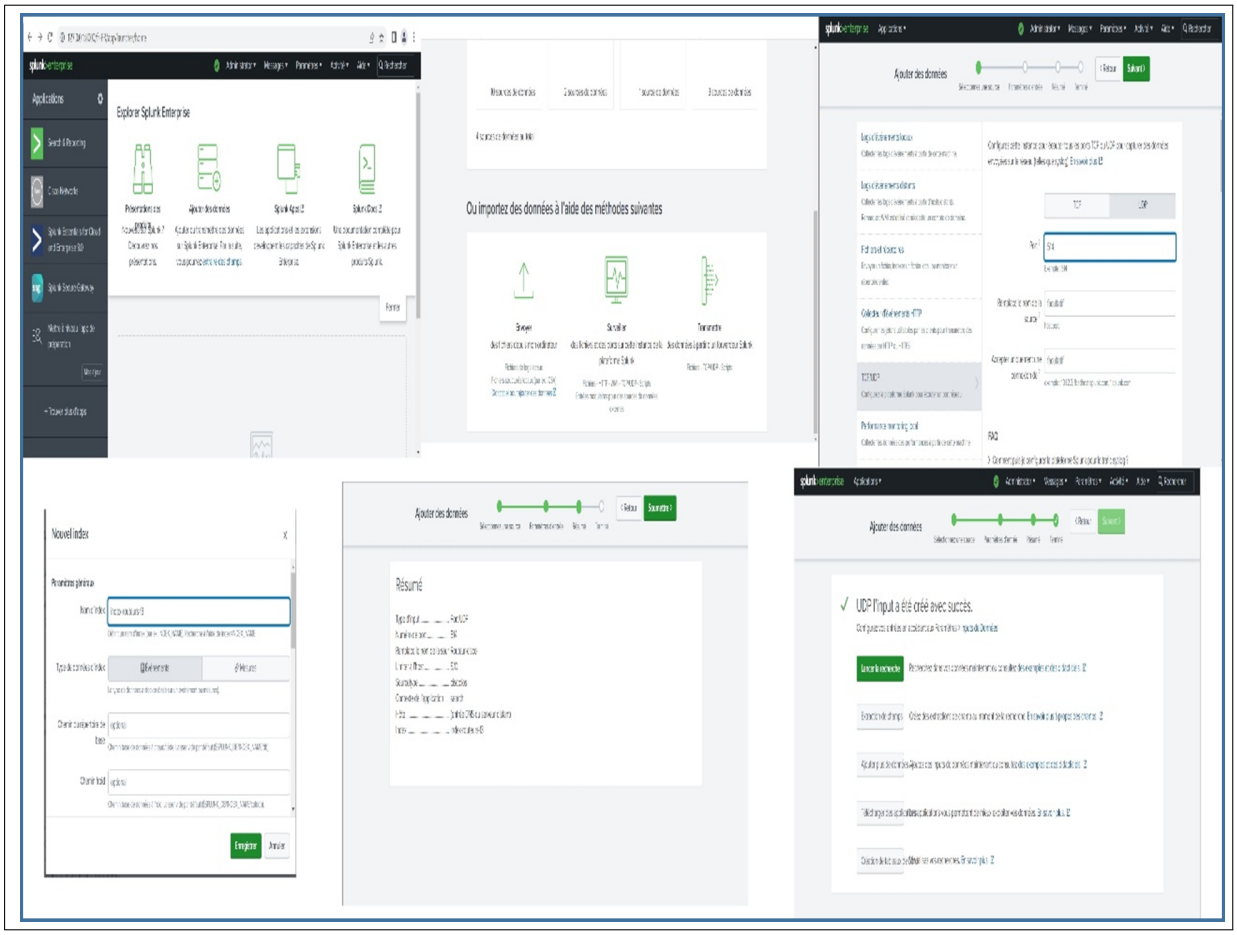

FIGURE 3.27 – Récupération de données(logs) Sur l'instance Splunk

Nous pouvons voir que les logs correspondants à l'activité de journalisation de notre machine cliente commencent déjà à apparaître. Le résultat est illustré dans la capture suivante.

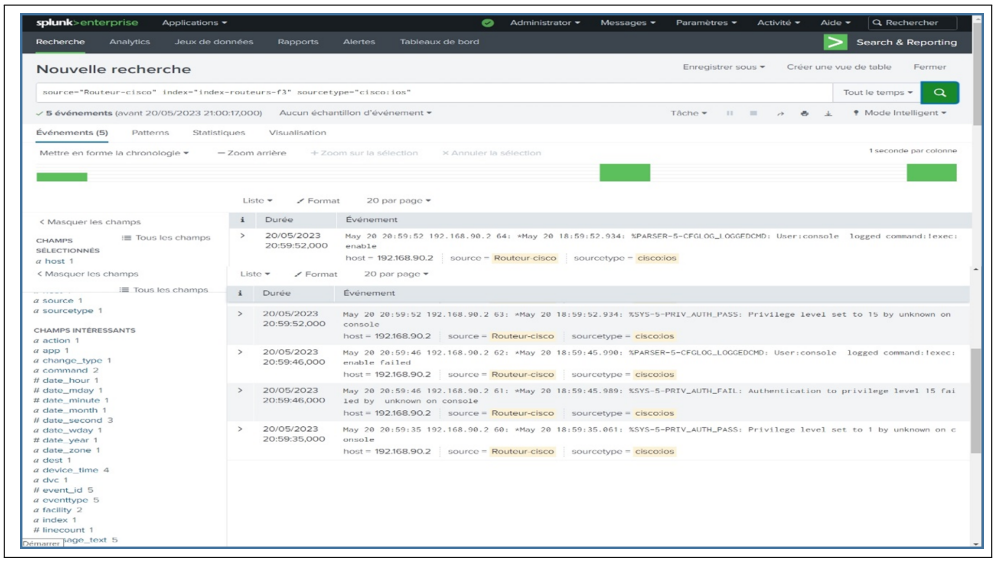

Figure 3.28 – Logs générés

D) Ajouter un client firewall FortiGate pour Splunk entreprise

Cette partie consiste à déployer un client FortiGate pour notre serveur Splunk. Nous allons présenter cela en trois phases principales.

1) Configuration du serveur Splunk

Tout d'abord, nous accédons à l'interface utilisateur de Splunk afin de télécharger et d'installer le module complémentaire FortiGate Add-on pour Splunk. Ce module permet d'intégrer les données générées par le pare-feu FortiGate dans Splunk, offrant ainsi une visibilité étendue et une analyse approfondie de l'environnement de sécurité réseau.

Nous accédons au site Splunk et effectuons une recherche par mot-clé du produit Splunk. Ensuite, nous cliquons sur "Télécharger" pour télécharger le fichier exécutable correspondant.

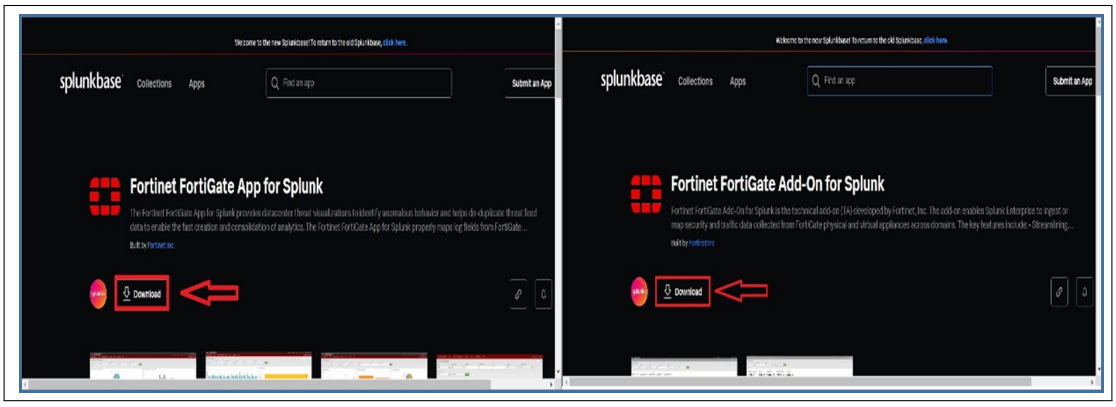

Figure 3.29 – Téléchargement du module complémentaire de fortie-gate add on for Splunk

Maintenant, nous cliquons sur l'onglet "Applications" puis sur "Gérer les applications". Ensuite, nous choisissons l'option "Installer une application depuis un fichier". Ces étapes sont illustrées ci-dessous :

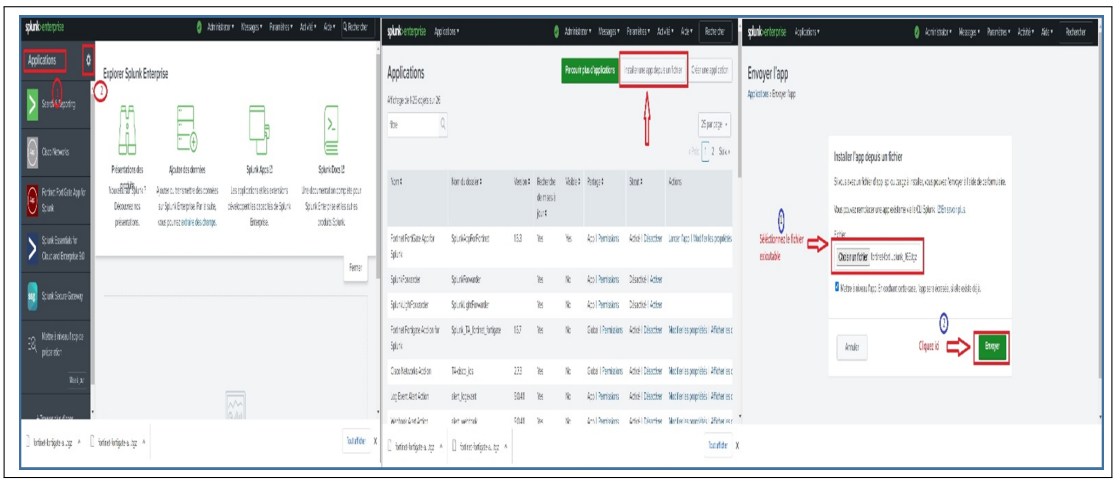

FIGURE 3.30 – Importation du module complémentaire de forti-gate pour Splunk

Il reste à implémenter une configuration initiale sur notre serveur Splunk afin de déployer la source de données sur celui-ci. Dans l'onglet "Paramètres", nous accédons à la section "Entrée de données".

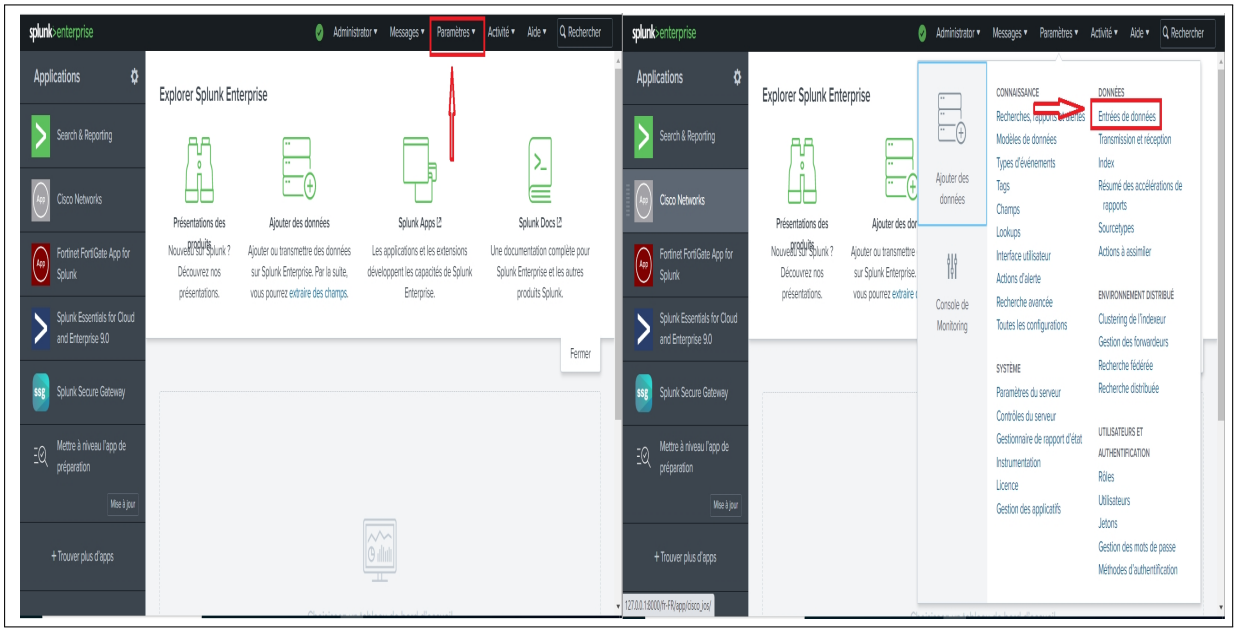

FIGURE 3.31 – Configuration de la reception de données

Sous cette section, nous allons créer une nouvelle entrée de données UDP en cliquant sur "Ajouter Nouveau" dans l'onglet à droite, comme illustré ci-dessous.

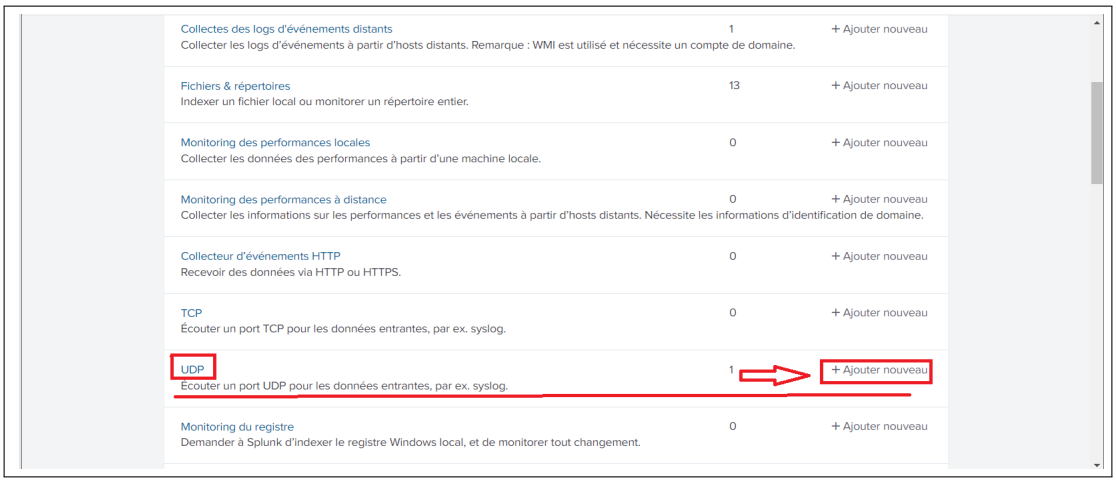

FIGURE 3.32 – Création d'une entrée UDP

À ce niveau, nous allons paramétrer la transmission et la réception entre les instances Splunk. Ainsi, nous allons créer une nouvelle source de données sur le port d'écoute 514 et configurer le type de source de données correspondant à fortie-gate.

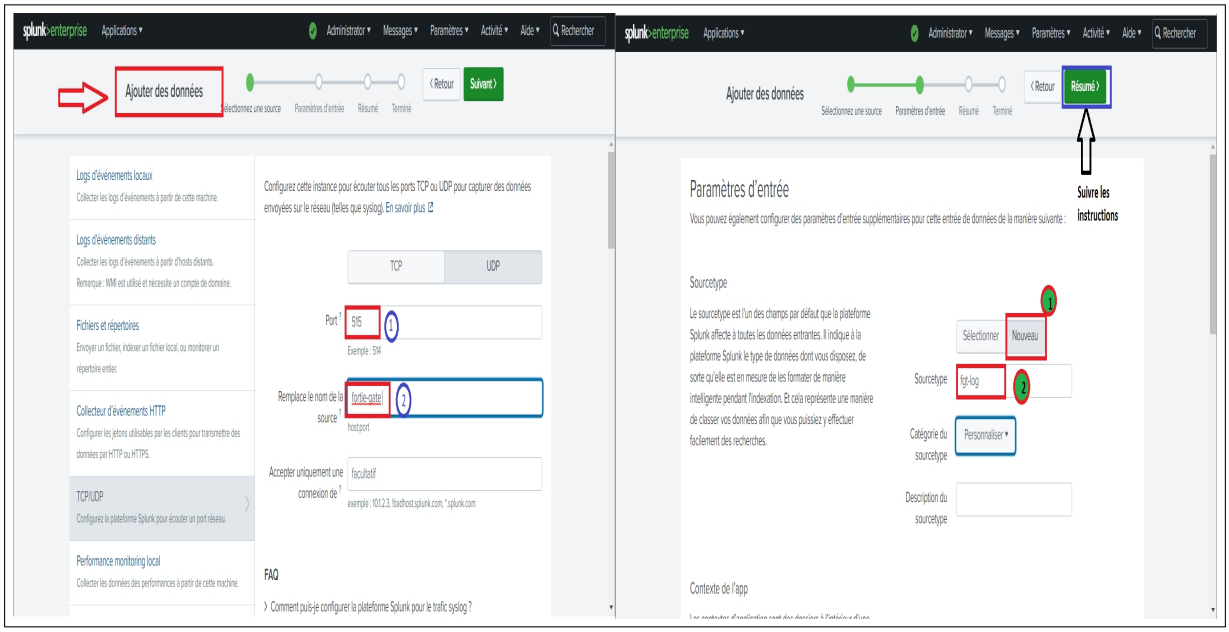

FIGURE 3.33 – Configuration des pramétres de transmission et de réception des logs

2) Configuration du journal (logging) sur le pare-feu FortiGate.

Dans cette partie, nous allons configurer fortie-gate pour envoyer les journaux système vers l'adresse du serveur Splunk. Tout d'abord, nous accédons à l'interface utilisateur de fortie-gate et nous choisissons l'onglet "log setting". Ensuite, nous activons l'envoi des journaux pour syslog .

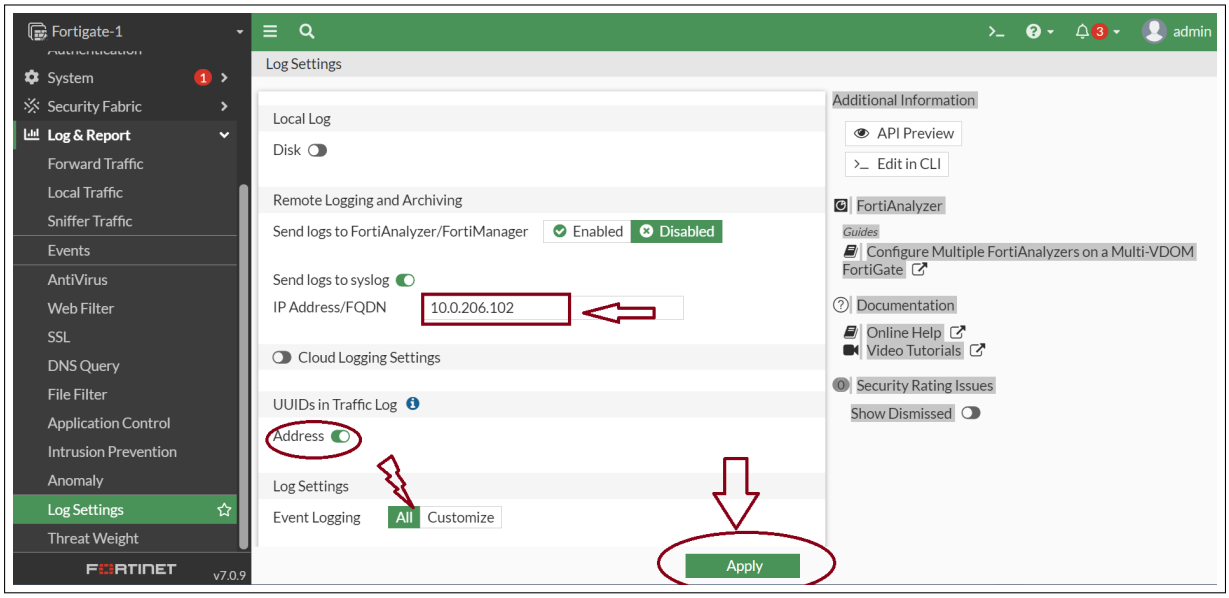

FIGURE 3.34 – Activation de l'envoi des journaux par Syslog

Nous voyons déjà apparaitre les logs correspondant à l'activité de journalisation du pare-feu fortigate déployé dans notre infrastructure réseau, le résultat est illustré dans la (figure 3.35)

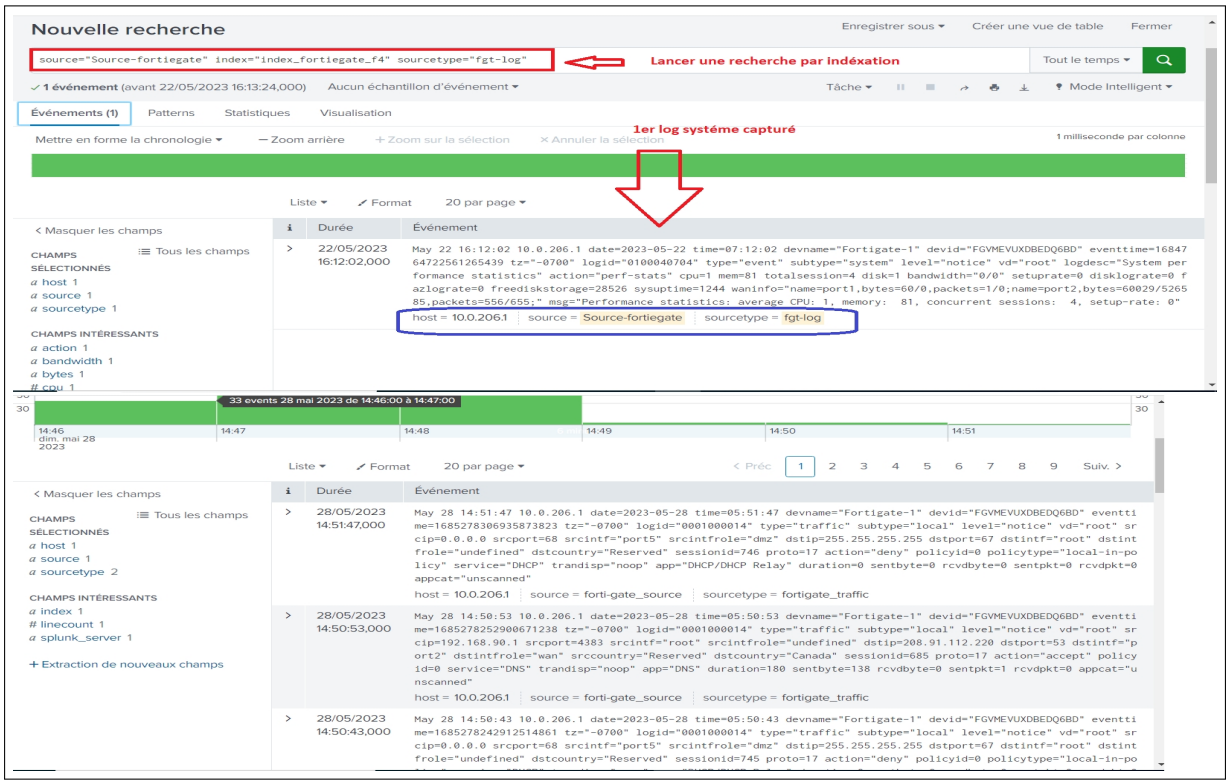

FIGURE 3.35 – Logs d'activité de journalisation du Pare-feu

3.4.4 Configuration des paramètres de traitement de données sur Splunk

Dans cette partie, nous allons nous intéresser à la personnalisation des fichiers de configuration afin d'ajuster le parsing des données selon nos besoins.

Au niveau du client Splunk

Nous illustrons le cas du Forwarder linux. Nous allons personnaliser les configurations qui sont généralement configurées avec des paramètres par défaut lors de l'installation initiale. Nous insérerons alors le script ci-dessous afin de délivrer tous les logs du répertoire Syslog vers le serveur Splunk.

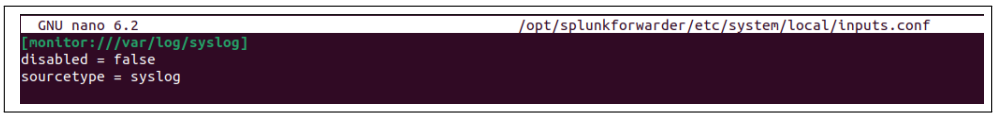

FIGURE 3.36 – Scripte de configuration initiale du client Splunk (cas Serveur linux)

Au niveau de serveur Splunk

Dans ce cas, nous accédons au répertoire de configuration de Splunk et nous ouvrons le fichier "props.conf" avec un éditeur de texte. À ce niveau, nous pouvons personnaliser ces paramètres. Dans notre cas, nous allons configurer l'extraction de champs personnalisée en ajoutant le script.

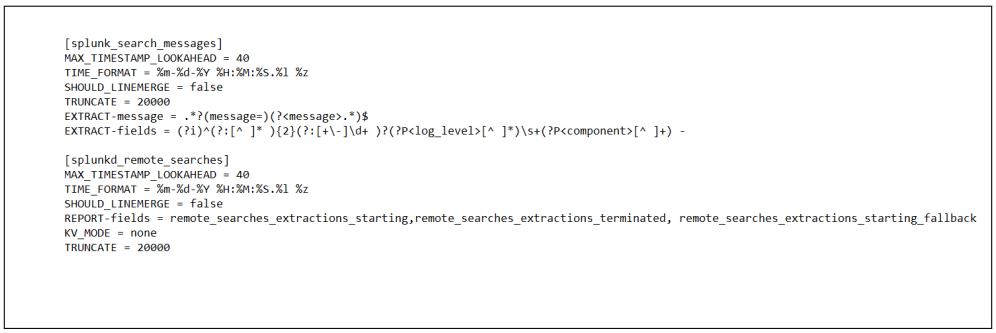

FIGURE 3.37 – Scripte de configuration d'extraction des champs personnalisés

Ensuite, nous accédons au fichier "transform.conf" avec un éditeur de texte. Nous allons définir des règles de transformation basées sur des expressions régulières pour modifier les données et les métadonnées des événements.

En tant que analyste de sécurité dans une équipe SOC on peut aller au De-las nous pouvons importer nos scriptes personnalisée de règles de corrélations et de traitements de données.

3.4.5 Indexation de Splunk

Recherche des données :

Après avoir pu ajouter nos clients Splunk avec succès ,nous allons utiliser à ce niveau la vue de recherche pour lancer des recherches, Nous accédons a l'anglet de recherche suivante :

```
[splunk_search_messages]
MAX_TIMESTAMP_LOOKAHEAD = 40
TIME_FORMAT = %m-%d-%Y %H:%M:%S.%l %z
SHOULD_LINEMERGE = false
TRUNCATE = 20000
EXTRACT-message = .*?(message=)(?<message>.*)$
EXTRACT-fields = (?i)^(?:[^ ]* ){2}(?:[+\-]\d+ )?(?P<log_level>[^ ]*)\s+(?P<component>[^ ]+) -

[splunkd_remote_searches]
MAX_TIMESTAMP_LOOKAHEAD = 40
TIME_FORMAT = %m-%d-%Y %H:%M:%S.%l %z
SHOULD_LINEMERGE = false
REPORT-fields = remote_searches_extractions_starting,remote_searches_extractions_terminated, remote_searches_extractions_starting_fallback
KV_MODE = none
TRUNCATE = 20000
```

FIGURE 3.38 – Scripte de configuration des règles de transformation basées sur des expressions régulières

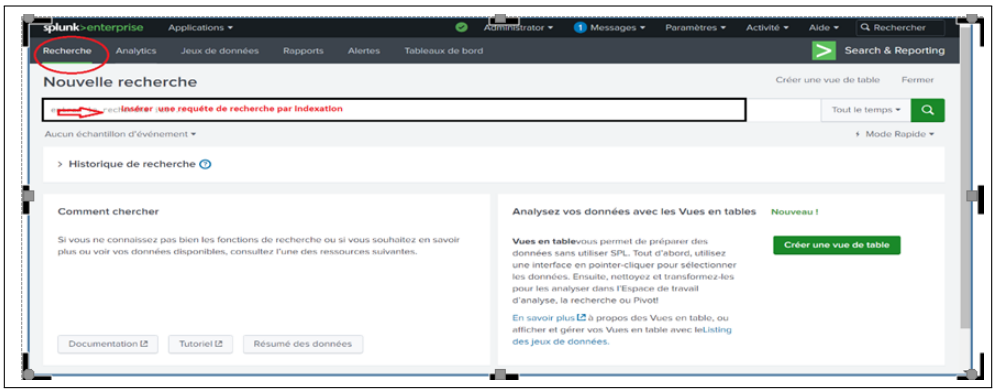

FIGURE 3.39 – Vue d'une nouvelle recherche

Il est nécessaire de limiter la recherche dans le temps pour obtenir des résultats plus efficaces, nous sélectionnant alors une plage de temps pour notre recherche.

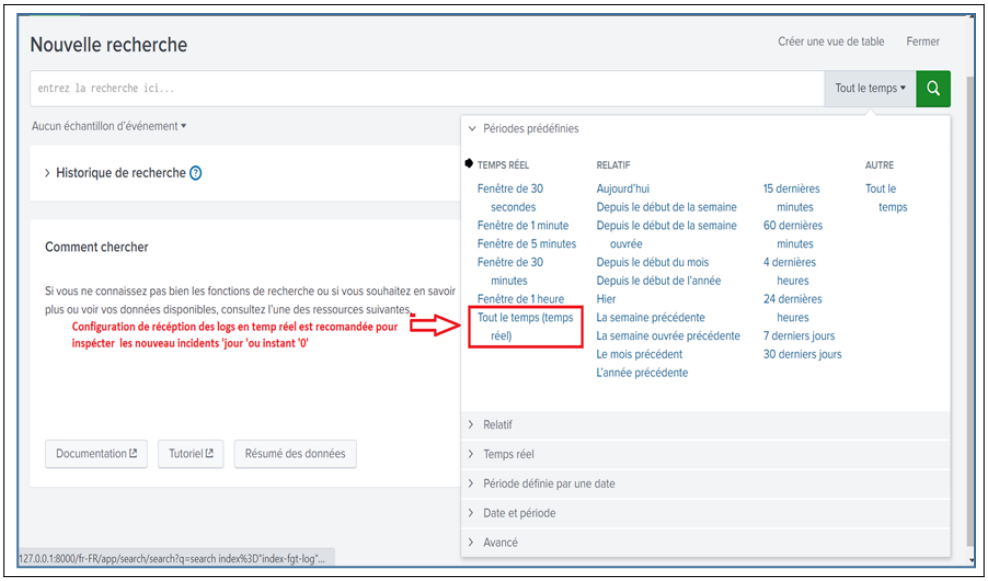

FIGURE 3.40 – Configuration de recherche dans le temps

Nous allons associer par la suite le mode de recherche selon notre cas d'inspection, dans ce cas nous adaptons les modes verbaux pour le traitement approfondi des données journal.

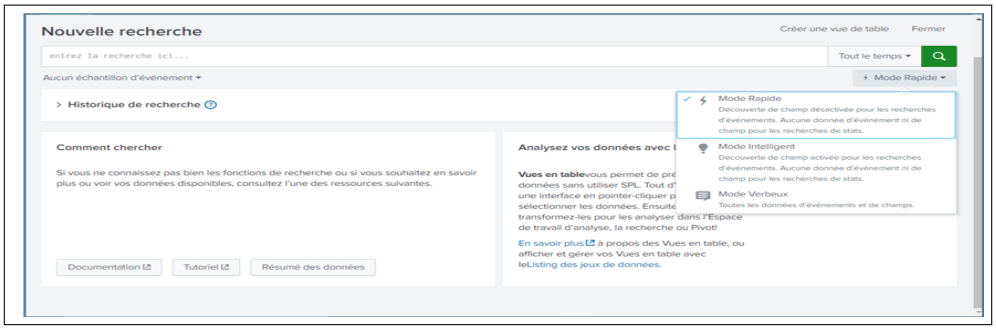

FIGURE 3.41 – Choix du mode de recherche

Nous introduisant des requêtes de recherches personnalisées en utilisant le langage de traitement de recherche Splunk "SPL"(voir la documentation sur l'annexe D) pour explorer les données des clients Splunk, nous le illustrons dans la (figure 3.42)

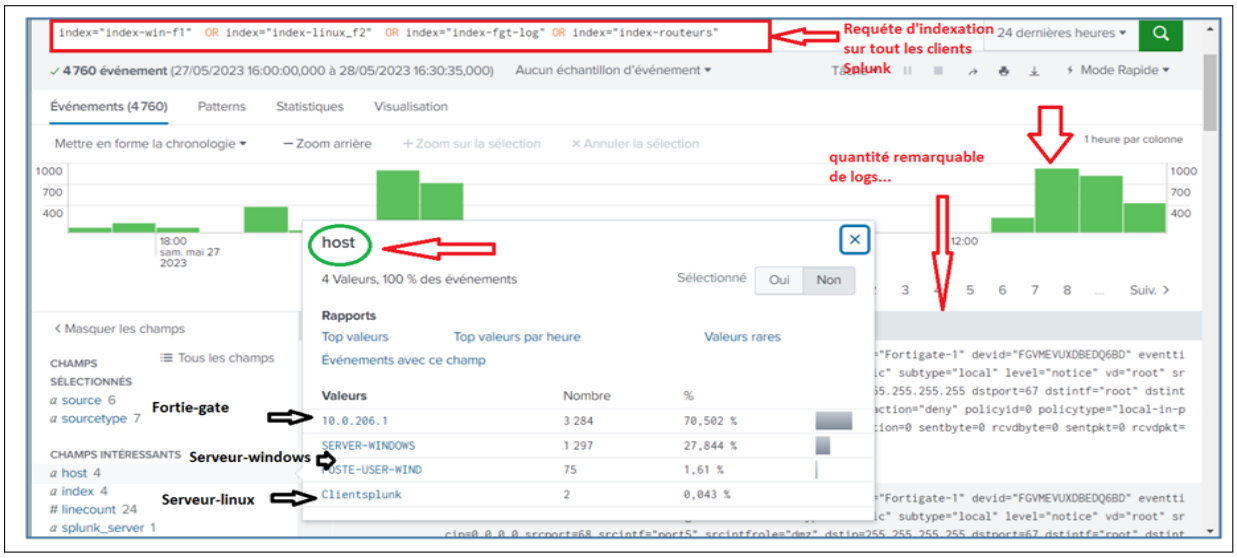

FIGURE 3.42 – Format d'une requête de recherche personnalisée

Enrichissements des champs des évènements :

Nous pouvons enrichir les champs de données de nos événement en ajoutant des informations plus significatives et des champs de recherche à chaque événement et ceci en intégrant un fichier de table de recherche sur l'application de recherche comme le montre la collection de (figure 3.43) :

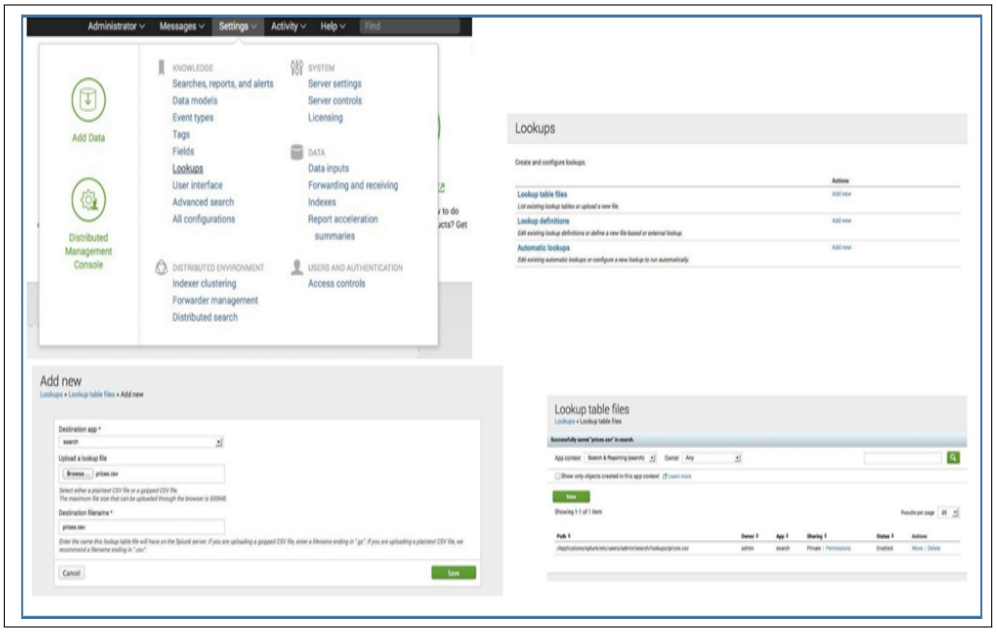

FIGURE 3.43 – Illustration d'ensemble des champs des évènements

Pour limiter les résultats aux seuls évènements qui nous s'intéressent Splunk met en valeur une barre latérale sur laquelle apparaissent les champs d'évènement analysé et agrégé comme illustre la (figure 3.44) :

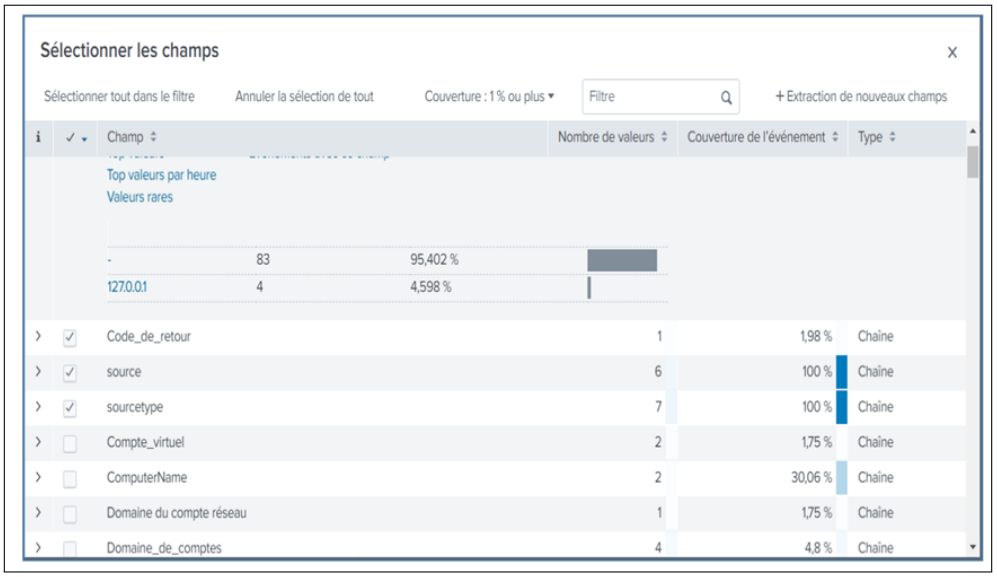

FIGURE 3.44 – Sélection des champs appropriés

3.4.6 Configuration des outils de visualisation ,d'alerte et de notification

A) Configuration des tableau de bord générer par les application add on Splunk :

A ce niveau, nous allons illustrer la configuration des tableaux de bords générer par des applications Splunk pour (app Cisco et app fortigate) .nous illustrons le cas de fortie-gate . Nous travaillerons sur deux niveau :
1) Niveau Sécurité réseau Fortie-net : Pour créer un tableau de bord de visualisation automatique , nous accédons à la section "Tableaux de bord" dans le menu principal de Splunk sous l'anglet " Sécurité réseau Fortie–net"

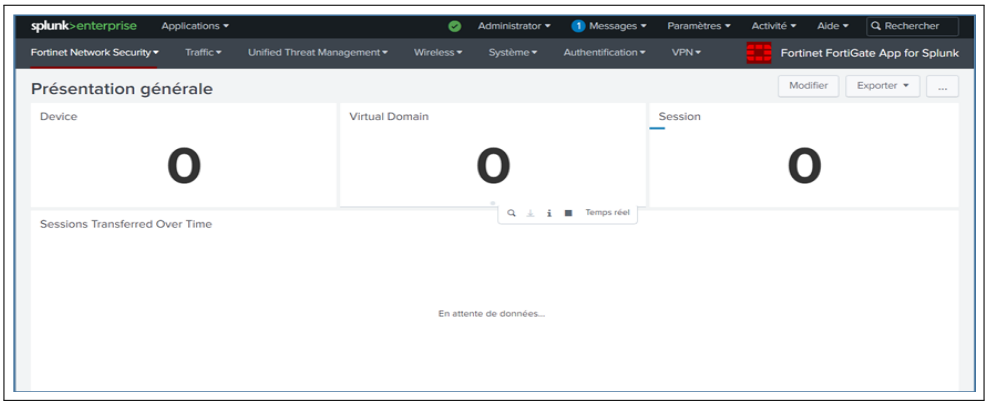

FIGURE 3.45 – Tableau de bord de l'application par défaut

Nous appliquons alors une suite de ligne de requête comme option de recherche pourla création de tableau de bord pour ajouter des graphiques, et d'autres éléments visuels basés sur les logs de FortiGate.

FIGURE 3.46 – Requête d'indexation des vues de visualisation

Voici le tableau de bord résultant des données sécurité réseau Fortie-net

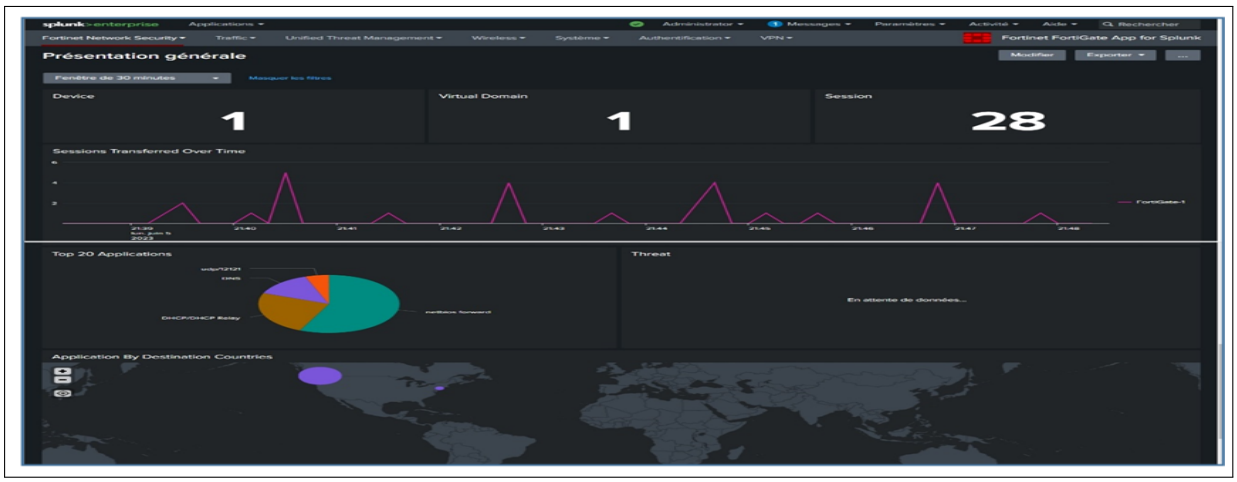

FIGURE 3.47 – Vue de tableau de bord fortieGate

2) Niveau trafic réseau Fortie-net :

Pour créer un tableau de bord de visualisation personnalisé, nous accédons à la section "Tableaux de bord" dans le menu principal de Splunk sous l'anglet « Sécurité réseau Fortie–net «

Nous appliquons encore des ligne de requête (figure) comme option de recherche pour ajouter des graphiques, des tableaux et d'autres éléments visuels basés sur les logs de FortiGate.

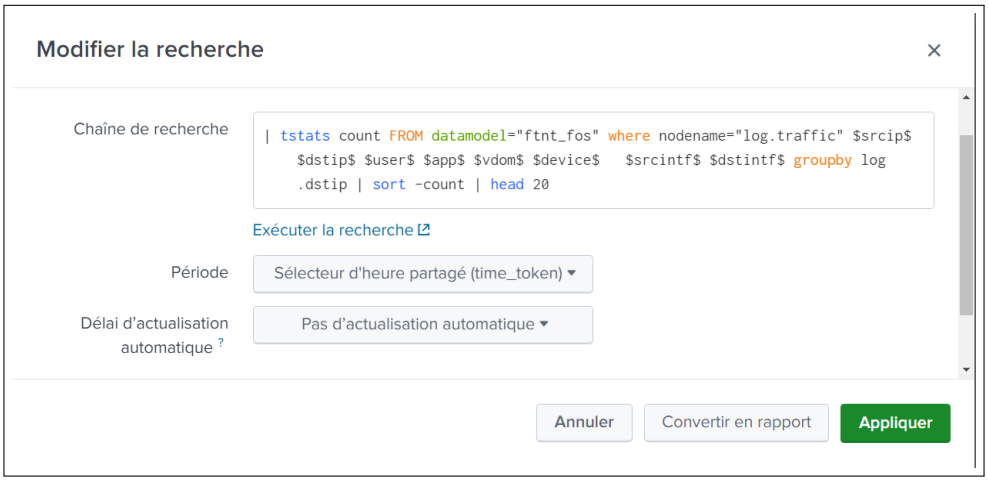

FIGURE 3.48 – Requête d'indexation des vues de visualisation

Voici le tableau de bord résultant des données Trafic réseau Foretie-net

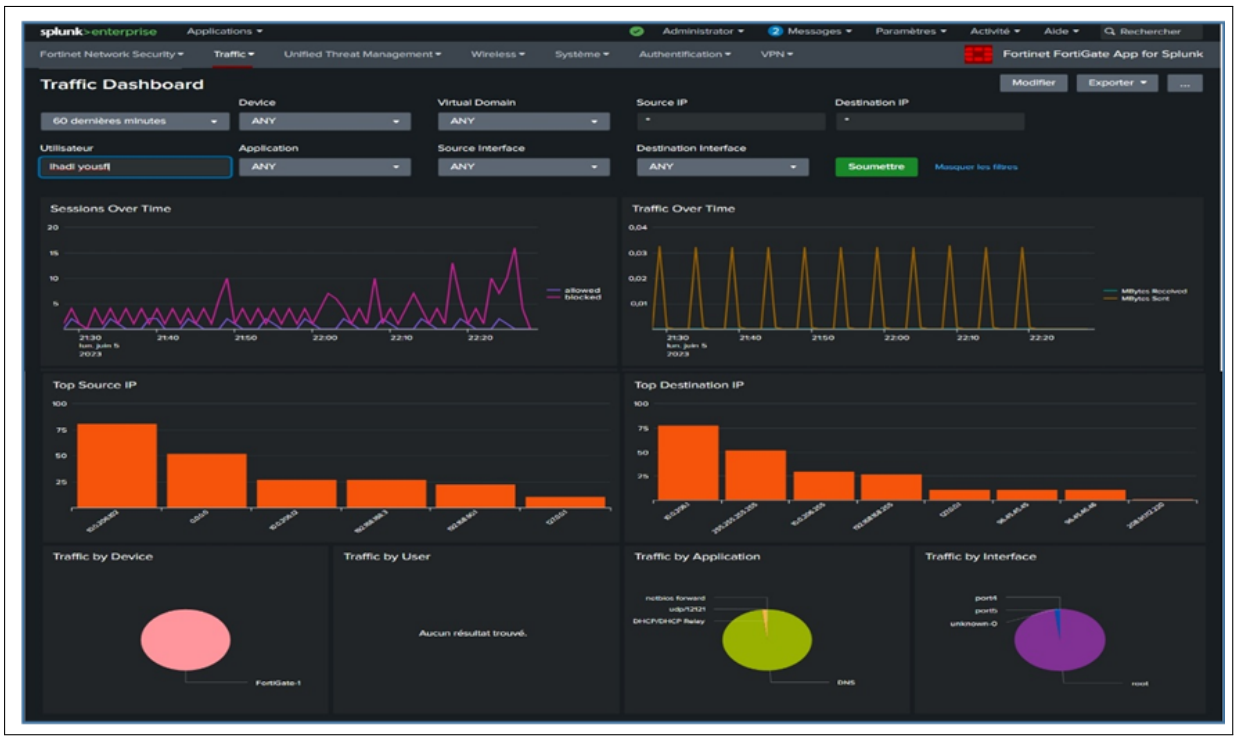

FIGURE 3.49 – Visualisation des données de Sécurité réseau Fortie-net

Remarque : des configurations similaires sont appliqué sur les autres applications Splunk de visualisation (add Splunk cisco).

Configuration manuel des tableau de bord générer par des résultats de recherche

Dans cette partie nous illustrons le cas de Configuration des paramètre de générations de tableau de bord générer par des résultats de recherche des logs indexé.

Pour approfondir la visualisation des résultats d'analyse et d'indexation des fichiers journaux dans Splunk, prenons l'exemple de l'étude et de l'analyse d'un fichier journal de sécurité SSH intégré sous notre serveur linux.

En premier lieux nous allons paramétrer un nouveau tableau de bord de visualisation comme le montre la (figure 3.50).

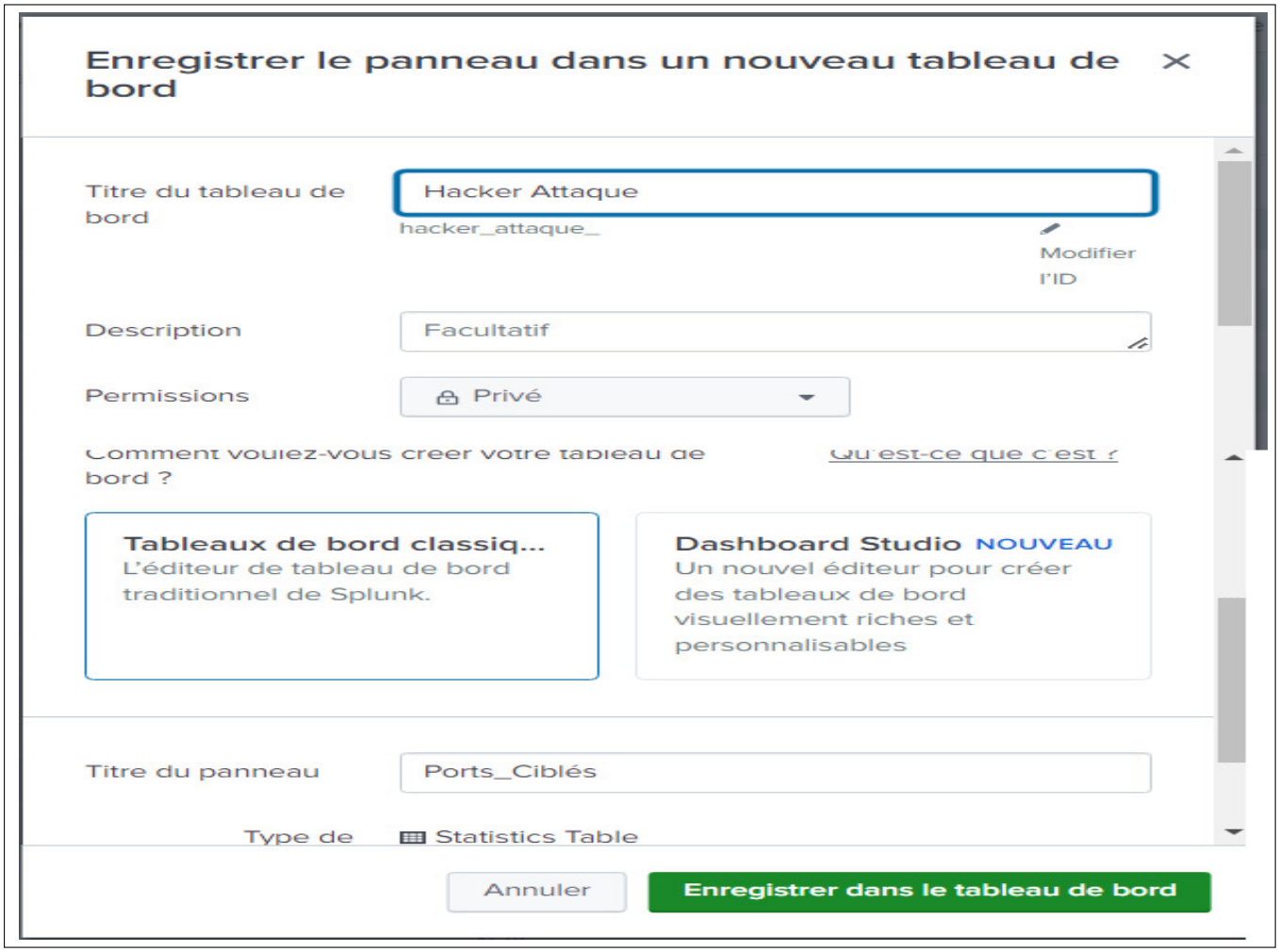

FIGURE 3.50 – Paramètres d'enregistrement d'un nouveau tableau de bord de visualisation

Ensuite nous lançant des requête de recherche par indexation a différents paramètres, afin d'obtenir des vues , des graphes ,des représentation graphiquelier a des événements spécifique, dont les requêtes et les vus obtenue sont illustrer dans la figure (3.51)

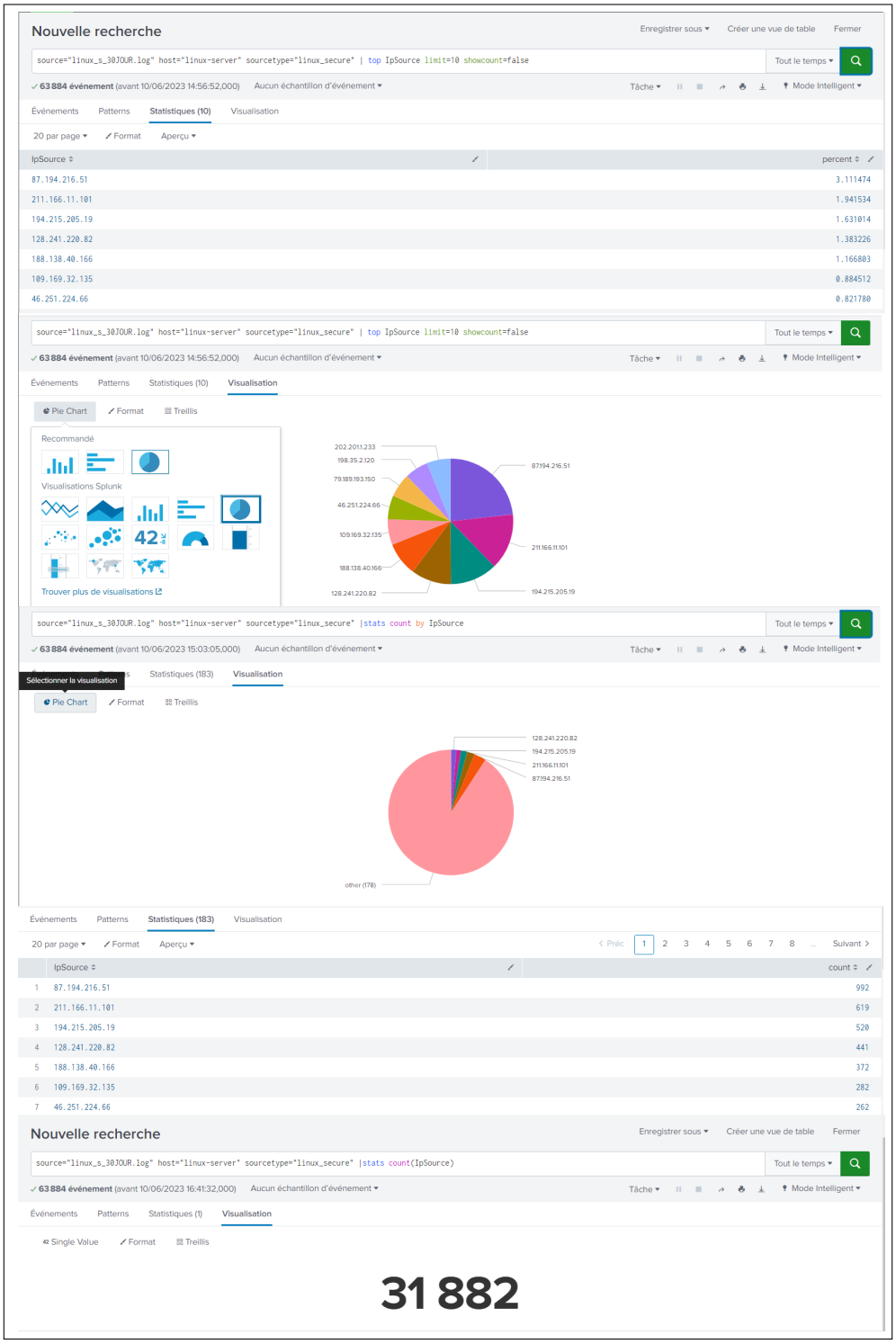

FIGURE 3.51 – L'ensemble des vues indexées

Nous devons superposer ces vue criée une par une sur le tableau de bord précédemment criée comme le montre la figure 3.52 :

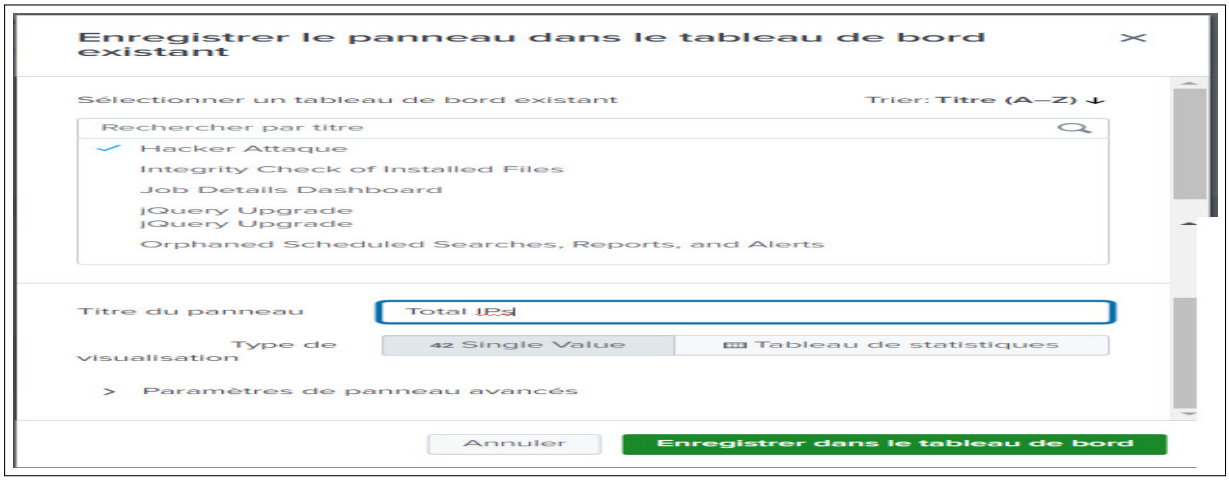

FIGURE 3.52 – L'ajout des vues sur le panel de tableau de bord

Enfin nous allons Choisir et paramétrer le style de visualisation approprié et Personnaliser les options de formatage visuel pour aboutir a un tableau de bord comme le montre la figure ci-dessous :

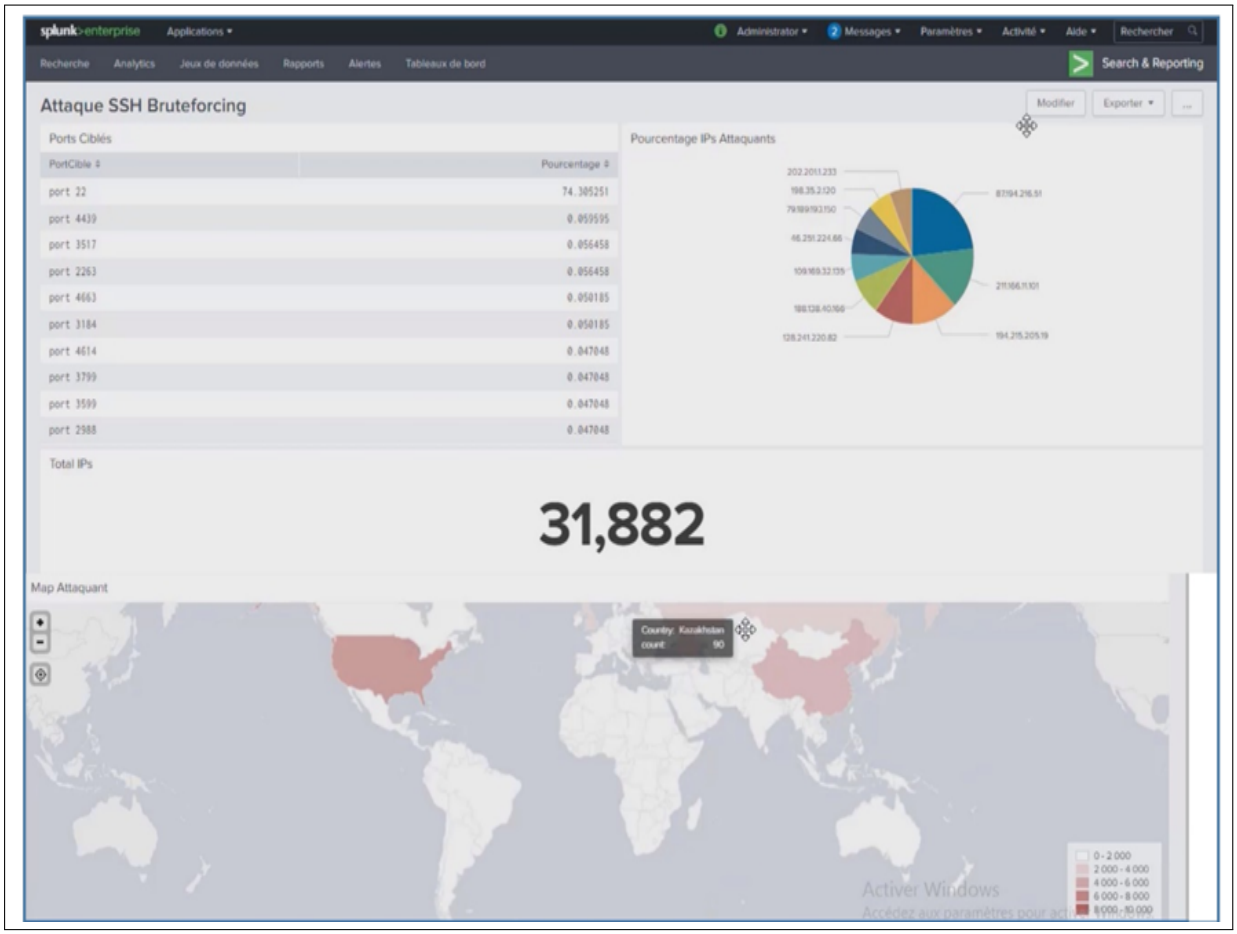

FIGURE 3.53 – Vue de tableaux de bord

Configuration des alertes et des notifications :

Dans cette partie, nous prenons un cas de déclenchement d'alerte suite à une erreur d'authentification sur le serveur Splunk en tant que service sur notre serveur Windows (supervision en local)

Nous allons configurer les notifications d'alerte sous Splunk, en accédons vers « alerte » sous l'anglet « paramètre » sur la barre de navigation supérieure. Nous crions alors une nouvelle alerte.et nous allons spécifier les contraintes et les actions préalable de déclanchements d'alerte.

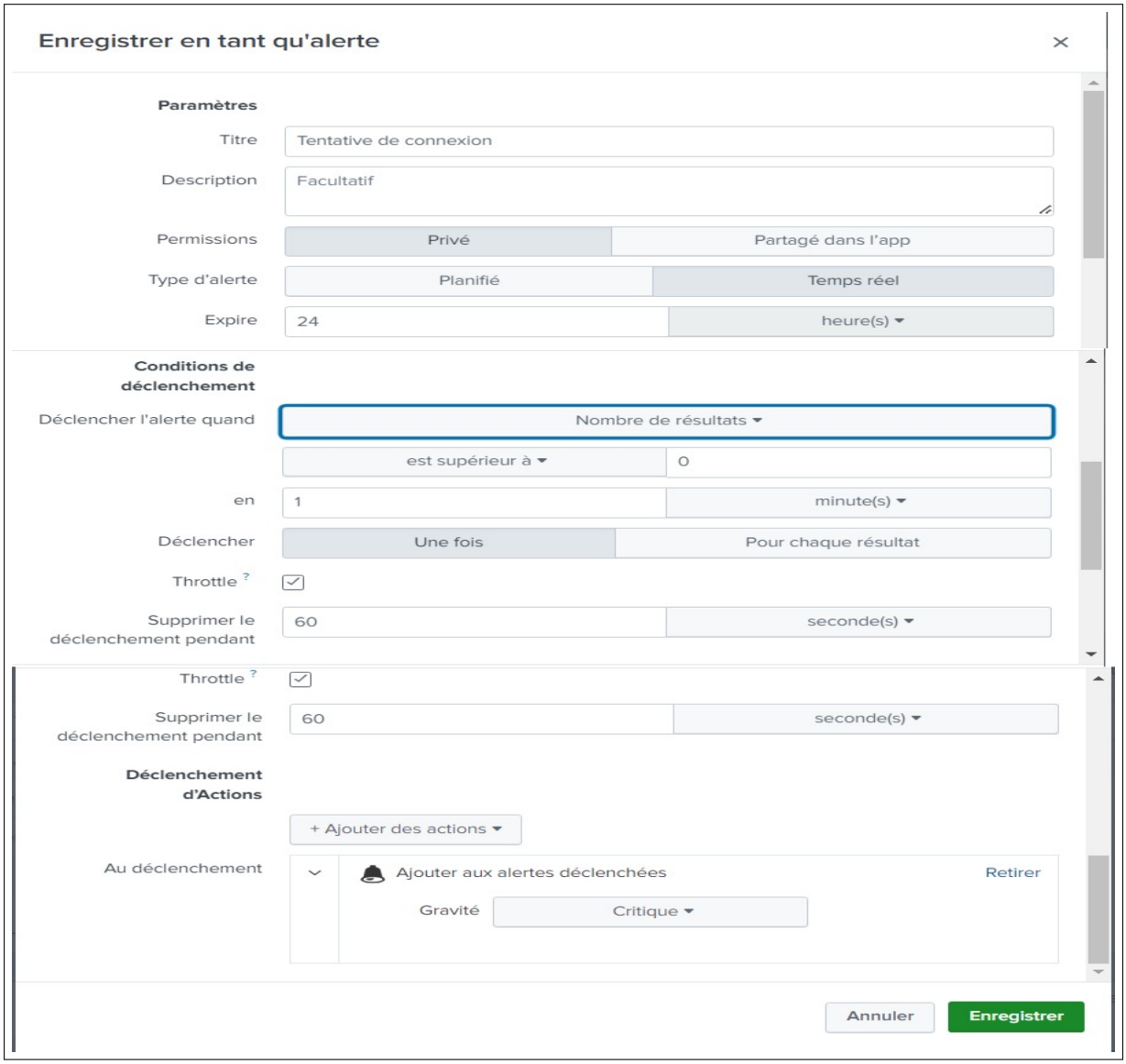

FIGURE 3.54 – Configuration des paramètres de déclanchements d'alerte

3.4.7 Simulation des scénarios d'attaque et tests

Dans cette partie, nous allons effectuer des tests de déploiement du logiciel de sécurité Splunk. Pour ce faire, nous allons configurer une machine virtuelle (Kali Linux) en mode externe. Cependant, il est

important de noter que ces tests doivent être effectués dans un environnement contrôlé et autorisé, conformément aux politiques de sécurité et aux lois en vigueur.

L'objectif de ces tests est de simuler des attaques ciblées sur l'équipement de l'infrastructure réseau supervisé par Splunk, afin d'évaluer l'efficacité de cette solution pour l'identification des attaques, des incidents et des activités malveillantes en temps réel.

Tentatives d'attaques et d'intrusions

Sur la machine virtuelle (Kali Linux), nous menons des tests de sécurité en utilisant plusieurs lignes de commandes pour simuler des tentatives d'attaques sur le serveur Linux (client Splunk) :

"nikto -h http ://10.0.206.104" : Cette commande exécute une analyse de vulnérabilités sur le serveur web (NGINX) accessible à l'adresse IP 10.0.206.104 (scanner de sécurité web).Elle représente une tentative d'accès non autorisé.
"nmap –source-port 80 10.0.206.1" : Cette commande est utilisée pour effectuer un scan de ports sur l'adresse IP 10.0.206.104, en utilisant le port source 80. Cela signifie que les paquets envoyés lors de la numérisation des ports auront le port source défini comme 80.
"nmap 10.0.206.104" : Cette Commande est utilisée pour effectuer un scan de ports sur l'adresse IP 10.0.206.104. Cela permet de détecter les ports ouverts sur cette adresse IP spécifique et d'obtenir des informations sur les services qui peuvent être en cours d'exécution.

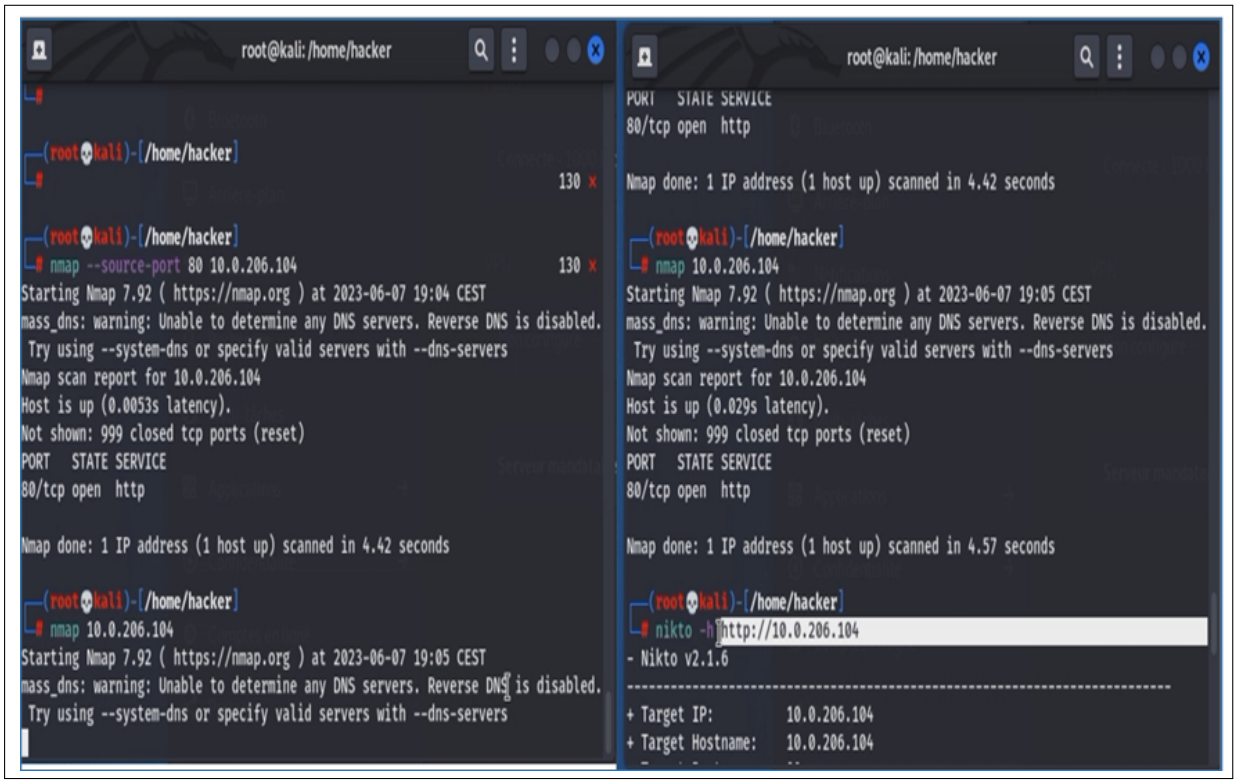

Figure 3.55 – Attaque sur kali linux

Récupération des événements de sécurité du serveur linux

À ce stade, en tant qu'expert en sécurité informatique, nous observons une nette augmentation du nombre d'événements de sécurité sur la plateforme Splunk après avoir subi des attaques massives sur l'un des clients Splunk de l'infrastructure réseau surveillée en temps réel. La (figure 3.56) présente l'ensemble des journaux de sécurité récupérés, y compris l'historique détaillé des traces et du trafic de ce dernier.

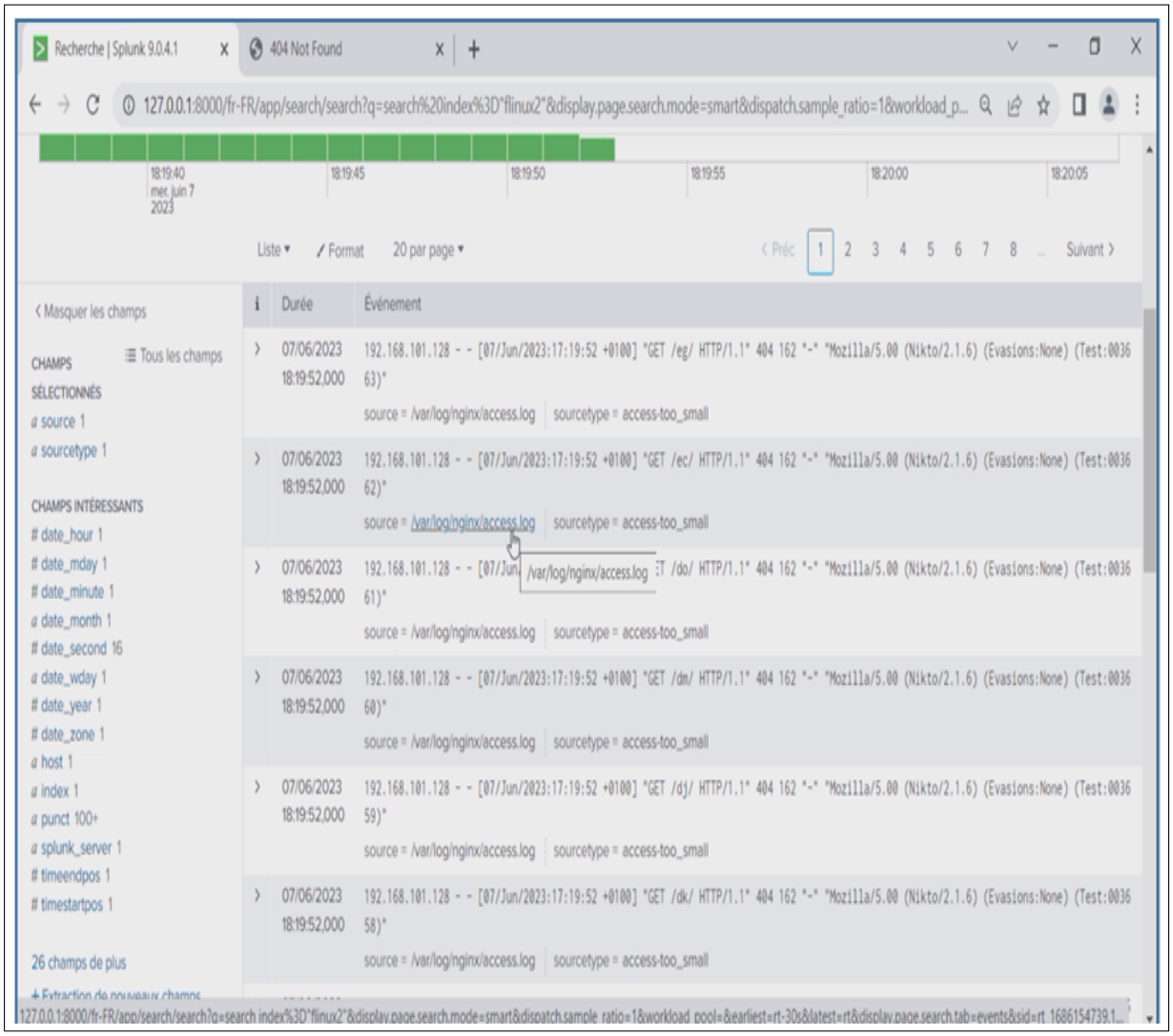

FIGURE 3.56 – Listes des loges d'attaques récupéré

Analyse et visualisation d'incidents

Splunk, en tant qu'outil d'analyse des événements de sécurité, collecte et stocke toutes les informations relatives aux incidents, aux champs et aux détails des événements de sécurité. Ces données sont ensuite normalisées, analysées, agrégées et décortiquées pour faciliter leur interprétation. Elles sont ensuite affichées sur un tableau de bord de visualisation, ce qui permet une analyse facile et simplifiée.

Dans les figures "3.47", "3.49", "3.51" et "3.53", vous pouvez voir des exemples de ces tableaux de bord qui présentent les informations de manière claire et organisée. Ces tableaux de bord offrent une vue d'ensemble des événements de sécurité, ce qui permet aux analystes d'identifier rapidement les attaques, les anomalies et les incidents.

Alerte et notification d'attaque

En temps réel, les analystes de sécurité sont alertés et notifiés des événements. La figure 3.57 présente les alertes de notification déclenchées, indiquant les attaques prédéterminées subies par le client Splunk (serveur Splunk) après une analyse approfondie des événements de sécurité. Ces notifications servent de recommandation pour une analyse ultérieure, ainsi que pour l'éradication et la réponse aux alertes déclenchées.

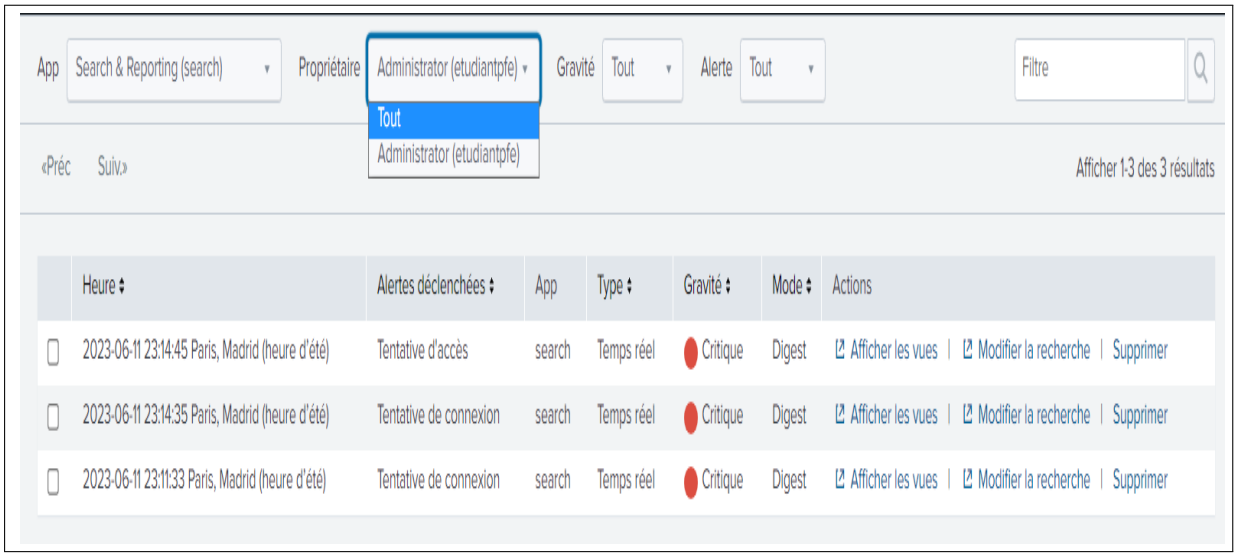

Figure 3.57 – Alertes en temps réel

Résultat final du déploiement :

En ce qui concerne le travail effectué, nous avons débuté par l'installation du logiciel de sécurité Splunk et sa configuration pour le déploiement sur l'infrastructure réseau proposée au début de ce chapitre Cela inclut également la configuration des outils Splunk pour la supervision en temps réel. Les tests effectués ainsi que les résultats de visualisation ont démontré le rôle essentiel de Splunk dans ce contexte.

En effet, Splunk a rempli sa fonction pour laquelle il a été choisi : la détection des différents événements en temps réel survenant sur le système. Il a notamment détecté les intrusions que nous avons

simulées et a fourni des informations approfondis relatives à celle-ci. Cette détection a alerté les responsables du système informatique de l'entreprise, leur permettant d'intervenir par rapport à cette intrusion détectée.

3.5 Conclusion

En conclusion, ce chapitre présente une conception de projet pour l'installation et la configuration d'une plateforme Splunk au sein de notre infrastructure réseau. Nous avons abordé les procédures d'installation et de déploiement des outils Splunk afin de collecter des données à partir de différents systèmes. Grâce à ces installations, notre équipe SOC dispose désormais des capacités nécessaires pour surveiller en temps réel les incidents critiques à l'aide de tableaux de bord personnalisés et d'alertes. De plus, nous sommes en mesure d'analyser les journaux et les événements, de détecter les activités suspectes et de prendre des mesures appropriées en cas de menace ou d'incident.

Conclusion et perspectives

L'objectif de ce travail était de prendre en compte les problématiques de sécurité des systèmes informatiques de l'entreprise SONATRACH en mettant en place une solution SIEM comme outil de visualisation centralisée pour la surveillance en temps réel et la détection des incidents et des anomalies de sécurité. Cependant, la mise en œuvre de notre solution de sécurisation a été entravée par le manque de ressources matérielles et logicielles nécessaires. Malgré cela, nous avons pu mettre en pratique nos connaissances en implémentant SPLUNK Enterprise comme solution de supervision dans un environnement Lab reproduisant partiellement l'infrastructure réseau de l'entreprise d'accueil.

Le traitement de ce sujet a été extrêmement enrichissant pour nous, car nous avons acquis une compréhension approfondie des meilleures pratiques en matière de sécurité informatique. De plus, nous avons eu l'opportunité de travailler en étroite collaboration avec des équipes de professionnels expérimentés, notamment le SOC de l'organisme d'accueil.

Certes, la solution développé lors de ce projet va être amélioré en ajoutant d'autres fonctionnalités et services selon les besoins .Une perspective importante est la mise en place de la solution de manière simulée sur un cas de déploiement réel au sein de l'entreprise Sonatrach.

On vise à étendre la solution à l'avenir pour couvrir un plus large éventail de domaines de sécurité, tels que l'intégration de flux de renseignements sur les menaces et l'analyse du comportement des utilisateurs. Ces ajouts peuvent améliorer son efficacité. L'intégration avec les processus de réponse aux incidents et l'automatisation peut améliorer la gestion des incidents, tout en explorant les technologies émergentes telles que l'apprentissage automatique et l'intelligence artificielle, ce qui peut améliorer la détection des anomalies et l'analyse prédictive.

Bibliographie

[1] "What is siem ?." https://www.criticalinsight.com/resources/news/article/what-is-siem. Consulté le 29 mai 2023.

[2] J. Carr, "Elastic stack." = https ://www.elastic.co/fr/elastic-stack/, organization = Elastic, note = Consulté le 25 avril 2023.

[3] J. Cirelly, "Graylog : Full Review & The Best Alternatives (Paid & Free)." https://www.comparitech.com/net-admin/graylog-review/. Consulté le 27 avril 2023.

[4] R. A. Sep&39 ;ulveda Rodr&39 ;ıguez, "Analysis of alternatives for a security information and event management tool in a virtualized environment," *Computer Science ;*, 2018.

[5] J. Carr, "Logrhythm's security intelligence platform : Siem product overview." https://www.techtarget.com/searchsecurity/feature/LogRhythms-Security-Intelligence-Platform-SIEM-product-overview. Consulté le 20 avril 2023.

[6] Exodata, "Le security operation center (soc) : fonctionnement et avantages." https://www.exodata.fr/blog/security-operation-center, 2020. Consulté le 29 avril 2023.

[7] l. T. l. T. e. l. C. d. H. Société Nationale pour la Recherche, la Production, "Sonatrach." https://www.sonatrach.dz/, 2021. Site officiel de la compagnie pétrolière et gazière nationale de l'Algérie.

[8] Formip, "Accès distribution core - formip." https://formip.com/acces-distribution-core, 2019. Consulté le 10 avril 2023.

[9] G. Valet, *Modèles OSI et TCP/IP*. Dunod, novembre 2010.

[10] "Cybercrime wire : Latest security and privacy news." https://cybersecurityventures.com/today/. Consulté le 13 avril 2023.

[11] Gartner, "Security information and event management (siem)." https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem. 22/03/2023.

[12] Splunk, "What is siem ?." https://www.splunk.com/fr_fr/data-insider/what-is-siem.html. 01/04/2023.

[13] S. Dorigo, "Security information and event management," *Radboud University, Nijmegen*, 2012.

[14] theastrologypage, "What's the difference between sem, sim and siem ?,"

[15] Techopedia, "What's the difference between sem, sim and siem ?,"

[16] Expert-Com, "Siem : Définition et rôle du security information and event management." https://www.expert-com.com/siem-definition/, 2018. Consulté le 16 mai 2023.

[17] J. Walter, "Guide ultime des informations de sécurité et de la gestion des événements." https://geekflare.com/fr/security-information-and-event-management-guide/, janvier 2023. Consulté le 15 mai 2023.

[18] Puneet, "What is siem and how it works ?." https://www.encryptionconsulting.com/education-center/what-is-siem/, septembre 2020. Consulté le 15 mai 2023.

[19] K. Singh, *Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab*. PhD thesis, Marquette University, 2020.

[20] SYNETIS, "SIEM ? : Une vue unique sur le système d'information." https://www.synetis.com/siem-vue-unique-systeme-dinformation/, août 2016. Consulté le 16 mai 2023.

[21] Zuzana, "Guide logpoint : Qu'est-ce que la gestion de logs et pourquoi est-elle si importante ?." Consulté le 17 mai 2023.

[22] T. Ikram, *Dévevloppement d'une application d'annalyse des fichiers Logs et prédiction des attaques*. Mémoire de master, Université Saad Dahlab de Blida 1, 2019.

[23] B. Mezni, *Etude et développement d'une plateforme d'analyse des fichiers logs*. Mémoire de master, Université Virtuelle de Tunis, 2015.

[24] F. Goffinet, "Gestion des logs syslog." https://cisco.goffinet.org/ccna/gestion-infrastructure/gestion-des-logs-syslog/. Consulté le 10 mai 2023.

[25] Graylog, "Log formats : A complete guide." https://www.graylog.org/post/log-formats-a-complete-guide/, date = 21/04/2019, organization = Graylog, note = Consulté le 19 mai 2023,.

[26] T. Sommestad, H. Karlzén, and J. Hallberg, "A meta-analysis of studies on protection motivation theory and information security behaviour," *International Journal of Information Security and Privacy (IJISP)*, vol. 9, no. 1, pp. 26–46, 2015.

[27] C. Bonnotte, "Les bonnes pratiques du siem pour la détection des attaques avancées." https://www.lemagit.fr/conseil/Les-bonnes-pratiques-du-SIEM-pour-la-detection-des-attaques-avancees, 2021. Article de blog présentant les bonnes pratiques à suivre pour détecter les attaques avancées à l'aide d'un SIEM.

[28] HubSpot, "Qu'est-ce qu'un fichier log ? explications, exemples et bonnes pratiques." https://blog.hubspot.fr/marketing/fichier-log, 2021. Article de blog expliquant ce qu'est un fichier log et son utilisation en informatique.

[29] Sumo Logic, "SIEM - Definition & Overview." https://www.sumologic.com/glossary/siem/. Consulté le 19 mai 2023.

[30] J. Oliveira, "Qu'est-ce que la gestion des informations et des événements de sécurité ? (siem)." https://laredoute.io/blog/what-is-security-information-and-event-management-siem/. Consulté le 06 mai 2023.

[31] K. Dimitrios, *Security information and event management systems : benefits and inefficiencies*. PhD thesis, University of Piraeus (Greece), 2014.

[32] A. K., "Qu'est-ce que splunk ? concepts, fonctionnalités produits." https://www.cyberuniversity.com/post/quest-ce-que-splunk-concepts-fonctionnalites-produits. Consulté le 24 avril 2023.

[33] C. Dubuc, "A real-time log correlation system for security information and event management," 2021.

[34] LogPoint, "C'est quoi le siem ?." https://www.logpoint.com/fr/c-est-quoi-le-siem/. 03/04/2023.

[35] M. Vielberth and G. Pernul, "A security information and event management pattern," 2018.

[36] H. A. Khan, *Advancing Security Information and Event Management Frameworks in Managed Enterprises using GeoLocation*. Mémoire de master, University of Capetown, 2015.

[37] M. Korneliussen, "Implementation of a security information event management system in an industrial control system," Master's thesis, 2021.

[38] LeMagIT, "Cloud public, privé, hybride : Quel modèle choisir ?." Consulté le 25 mai 2023.

[39] Difenda, "Siem as a service." https://www.difenda.com/blog/siem-as-a-service/, 2021. Consulté le 14 mai 2023.

[40] R. A. Sepúlveda Rodríguez, "Analysis of alternatives for a security information and event management tool in a virtualized environment," *Computer Science ;*, 2018.

[41] S. M. Zeinali, *Analysis of security information and event management (SIEM) evasion and detection methods*. PhD thesis, Master Thesis, Tallinn University of Technology, 2016.

[42] "Guide de la haute disponibilité." https://www.ibm.com/docs/fr/SS42VS_7.4/pdf/b_qradar_ha_guide.pdf, 2023. Consulté le 14 avril 2023.

[43] A. K, "Quést-ce que splunk ? concepts, fonctionnalités produits." https://www.cyberuniversity.com/post/quest-ce-que-splunk-concepts-fonctionnalites-produits, may 2022.

[44] Edureka, "Splunk architecture - understanding the components of splunk." https://www.edureka.co/blog/splunk-architecture/, 2019.

[45] Y. Azouz, "Comment fonctionne splunk ?," *meritis*, 1953.

[46] A. Informatique, "Définition soc (security operation center)." Consulté le 28 avril 2023.

[47] Splunk, "What is a security operations center (soc) ?." https://www.splunk.com/fr_fr/data-insider/what-is-a-security-operations-center.html, 2023. Consulté le 29 avril 2023.

[48] Clusif, "Comment réussir le déploiement d'un soc." https://clusif.fr/wp-content/uploads/2017/03/clusif-2017-deploiement-soc_vf.pdf, 2017. 22/04/2023.

[49] Guardia Cybersecurity School, "Responsable du soc : fiche métier avec les missions, la formation...."

[50] manageengine, "Security operations center(soc) :the what, why, and how." https://download.manageengine.com/log-management/security-operations-center/security-operations-center.pdf. 22/04/2023.

[51] Higher Education Information Security Council (HEISC), "Security operations center (soc) case study : Heisc working group paper." https://library.educause.edu/-/media/files/library/2019/6/HEISCsoc.pdf, 2019. Consulté le 14 mars 2023.

[52] Graylog, "Log formats : A complete guide." https://fiches-pratiques.silicon.fr/Thematique/cybersecurite-1338/FichePratique/Tout-savoir-SOC-centre-operations-securite-365816.htm. Consulté le 25 avril 2023.

[53] P. A. Networks, “What is a security operations center (soc)? - cyberpedia - palo alto networks.” https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc. Consulté le 29 avril 2023.

[54] kaspersky, “Faire vivre un soc :mÉthodologie et conseils.” https://media.kaspersky.com/fr/business-security/enterprise/Faire-vivre-un-SOC_Methodologie-et-conseils.pdf, 2016. Consulté le 20 mai 2023.

[55] CIGREF, “Réagir à une cyberattaque massive.” = https ://www.calameo.com/cigref/read/005869235d0f464ed5a22, 2023. Consulté le 29 mars 2023.

Résumé

Ce travail s'inscrit dans le cadre du projet de fin d'études à l'Université Abderrahmane Mira - Bejaïa en vue de l'obtention du diplôme de Master en Administration et Sécurité des Réseaux Informatiques.

Ce mémoire traite des principes fondamentaux du SIEM (Security Information and Event Management) et du SOC (Security Operations Center), explore les différentes technologies et solutions de sécurité disponibles, et propose une approche pratique pour mettre en œuvre une solution SIEM efficace.

En résultat, nous avons réussi à implémenter avec succès un système de gestion des informations et des événements de sécurité informatique en utilisant la plateforme SPLUNK. Cette solution garantit une protection optimale des infrastructures informatiques des entreprises contre les cyberattaques et tout type de menace, réduisant ainsi le risque à un niveau proche de 0%. Dans ce mémoire, nous détaillons la démarche d'implémentation en expliquant en détail les concepts, la logique et les outils utilisés tout au long du processus.

Mots clés : Log,SIEM,SIM,SEM,SOC,Splunk.

Abstract

This work is part of the end-of-study project at Abderrahmane Mira University - Bejaïa to obtain the Master's Degree in Administration and Computer Network Security.

This thesis discusses the fundamental principles of SIEM (Security Information and Event Management) and SOC (Security Operations Center), explores the different security technologies and solutions available, and offers a practical approach to implementing an effective SIEM solution.

As a result, we managed to successfully implement a computer security information and event management system, using the SPLUNK platform. This solution guarantees optimal protection of companies' IT infrastructures against cyberattacks and any type of threat, thus reducing the risk to a level close to 0%. In this thesis, we detail the implementation process, explaining in detail the concepts, the logic and the tools used throughout the process.

Keywords : Log,SIEM,SIM,SEM,SOC,Splunk.