République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER

En
Informatique

Option
Administration et Sécurité des Réseaux

Thème

Mise en place d'une solution de sécurité SIEM avec Splunk cas d'étude : Entreprise Ifri

Présenté par : **Mlle.CHEURFA Sara**
Mlle.FERKAL Fatima

Soutenu le 07/07/2022 devant le jury composé de :

Président	**M. Redouane OUZEGANE**	**M.A.A**	**U. A. Mira Béjaia.**
Examinateur	**Mme. Nassima BOUADEM**	**M.C.B**	**U. A. Mira Béjaia.**
Promoteur	**M. Mohammed NAFI**	**M.C.B**	**U. A. Mira Béjaia.**

Année universitaire 2021/2022

Remerciements

*Nous remercions en premier lieu **ALLAH** le tous puissant de nous avoir illuminé et ouvert les portes de savoir, et de nous avoir donné la volonté et le courage d'élaborer ce travail.*

*Nous tenons à remercier spécialement notre promoteur **Mr. NAFI.M** pour avoir accepté de diriger ce travail, pour son aide, ses encouragements, ses précieux conseils, sa confiance, sa patience, tout au long de la réalisation de ce mémoire.*

Nous souhaitons formuler notre remerciements les plus affectueux à nous familles et surtout nous très chers parents et frères, qui ont toujours été là pour nous, leur confiance, leur amour nous porte et nous guide tous les jours. Sans oublier nous amies qui ont toujours encouragée au cours de la réalisation de notre travail.

Dédicace

Avant tout, je remercie le Dieu tout puissant, qui m'a donné la volonté, le courage et la patience et qui a guidé mes pas vers le droit chemin durant mes années d'études.

Je dédie ce travail

A mes ***très chers parents*** *qui ont été la source de ma réussite grâce à leurs prières et leurs encouragements, qui m'ont offert leur amour indéfectible et qui n'ont cessé de me donner le nécessaire à ma réussite.*
Toute ma gratitude pour leurs soutient tout
au long de mes études, que dieu les garde pour moi.

A mes très chers frères ***Massinissa et Ziri***

A ma très chère sœur ***Kamilia***

A mon très cher oncle ***Malek.B*** *et m'a très chère tante* ***Lyla.B***

Mes spéciales dédicaces à mes autres chères sœurs : Zahra, Houa et Cylia ,Yamina

A toi ma binôme Sara et ta famille.

A toute personne qui occupe une place dans mon cœur et à toute Personne qui m'ont aidé à achever ce niveau

Fatima.F

Dédicace

Avant tout, je remercie le Dieu tout puissant, qui m'a donné la volonté, le courage et la patience et qui a guidé mes pas vers le droit chemin durant mes années d'études.

Je dédie ce travail

A mes ***très chers parents*** *qui ont été la source de ma réussite grâce à leurs prières et leurs encouragements, qui m'ont offert leur amour indéfectible et qui n'ont cessé de me donner le nécessaire à ma réussite.*
Toute ma gratitude pour leurs soutient tout
au long de mes études, que dieu les garde pour moi.

A mes très chers frères ***Fateh ,Toufik et Samir***

A mes très chères sœurs ***Djehra , Naima et Soraya***

A mes très chéres ***Ryma , Maya , Sana , Mahdi***

Mes spéciales dédicaces à mes autres chères sœurs : Yasmine, Mina Soraya

A toi ma binôme Fatima et ta famille.

A toute personne qui occupe une place dans mon cœur et à toute Personne qui m'ont aidé à achever ce niveau

Sara.Ch

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

- **DMZ** **D**emilitarized **Z**one.
- **DoS** **D**enial **o**f **S**ervice.
- **ELK** **E**lasticsearch, **L**ogstash et **K**ibana.
- **HIDS** **H**ost-Based **I**ntrusion **D**étection **S**ystem.
- **HIPS** **H**ost-Based **I**ntrusion **P**revontion **S**ystem.
- **HWF** **H**eavy **W**eight **F**orwarder.
- **IDS** **I**ntrusion **D**étection **S**ystèm.
- **IP** **I**nternet **P**rotocol.
- **IPS** **I**ntrusions **P**revintion **S**ystem.
- **NIDS** **N**etwork-Based **I**ntrusions **D**étection **S**ystem.
- **NIPS** **N**etwork-Based **I**ntrusions **P**revontion **S**ystem.
- **OS** **O**perating **S**ystèm.
- **OSSIM** **O**pen **S**ource **S**écurity **I**nformation **M**anagement.
- **POC** **P**roof **O**f **C**oncept **.**
- **SEM** **S**écurity **E**vent **M**anagement .
- **SI** **S**ystèm **I**nformation.
- **SIEM** **S**écurity **I**nformations and **E**vent **M**anagement .
- **SIM** **S**écurity **I**nformations **M**anagement .
- **TCP** **T**ransmission **C**ontrol **P**rotocol.
- **UDP** **U**ser **D**atagram **P**rotocol.
- **UF** **U**niversal **F**orwarder.
- **VM** **V**irtual **M**achines. **V**irtual
- **VMI** **M**achine **I**nterface.
- **VPN** **V**irtual **P**rivate **n**etwork

Introduction générale

La sécurité informatique est devenue un enjeu important pour les entreprises. Les systèmes d'informations sont d'une importance primordiale, leur protection est donc une caractéristique nécessaire. De manière générale, la sécurité des systèmes d'information consiste à protéger les ressources de l'organisation afin qu'elles soient utilisées dans le contexte prévu. Cependant, de nouveaux problèmes émergents aujourd'hui autorisent les utilisateurs malveillants d'accéder à ces ressources et de lancer des attaques à partir de diverses sources.

Il est nécessaire pour une entreprise de développer des outils pour la surveillance proactive. Ces outils fournissent un système d'alerte immédiat dès qu'un dysfonctionnement ou une menace d'intrusion est détecté alors les problèmes potentiels sont identifiés avant qu'ils ne surviennent. Les utilisateurs reçoivent des informations concises leur permettant l'étude des incidents. L'évolutivité de l'infrastructure informatique est également prévue.

C'est dans ce cadre que s'inscrit notre travail, il consiste à la mise en place d'une solution SIEM(Security Information an Event Management) pour l'entreprise IFRI . Au cours de ce projet, nous allons nous intéresser à l'étude et la mise en place d'une solution Splunk.

Le présent mémoire est organisé de la façon suivante :
Le premier chapitre présente des généralités sur la sécurité informatique , allant de la généralité sur la sécurité réseau , en passant par ses caractéristiques et technique de parade aux attaques pour la bonne compréhension de ce concept. Nous allons également étudier l'importance de la sécurité informatique.

Le deuxième chapitre présente les solutions SIEM où les avantages et inconvénients ont été décrits.

Le troisième chapitre est consacré à la présentation de l'entreprise IFRI .

Le quatrième et dernier chapitre est consacré au déploiement de la solution SIEM choisie (SPLUNK) .Les différentes étapes à suivre pour la bonne installation et la configuration de cette dernière ont été exploités .

Chapitre 1

Généralités sur la sécurité informatique

1.1 Introduction

Les réseaux se développent en fonction de leurs caractéristiques et besoins, ils deviennent aujourd'hui une infrastructure indispensable dans tous les domaines de la vie. Cependant, les menaces et les attaques sur les réseaux prennent de nouvelles mises à jour représentant les pires ennemis de cette technologie de ces derniers . Pour cela, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

Dans ce chapitre nous allons faire une présentation générale de la sécurité informatique, ceci pour l'objectif de bien identifier le domaine d'étude.

1.2 Réseau informatique

Un réseau est un moyen permettant à des individus ou à des groupes de partager des ressources et des informations.
La technologie des réseaux informatiques est un ensemble d'ordinateur ou de périphérique reliés entre eux grâce à des lignes de communication et aussi à d'autre équipements qui permettent d'assurer la bonne circulation des données.

1.3 Sécurité informatique

Le système informatique doit être protégé contre toute violation ,vol des données et intrusion .Elle représente une partie essentielle dans l'entreprise qui nécessite une protection . La sécurité informatique consiste à assurer que les données sont uniquement utilisées dans le cadre prévu.
Les entreprises doivent comprendre comment adopter des solutions de sécurité intégrées dès la phase de conception.

1.4 Objectifs de sécurité

La sécurité est essentielle pour la protection de trois caractéristiques critiques des systèmes et de l'information qu'ils traitent et maintiennent, à savoir[1] :

- **Disponibilité :** assure que l'information et les systèmes soient accessibles et utilisables par les parties autorisées aux moments où elles en ont besoin.
- **Confidentialité :** assure que l'information soit protégée contre toute divulgation accidentelle ou malveillante aux parties non autorisées.
- **Intégrité :** assure que l'information et les systèmes soient protégés contre toute modification ou destruction accidentelle ou malveillante.

A côté de ces caractéristiques de bases nous rencontrons également les composantes suivantes :

- **Authentification :** assure l'identification d'un individu, d'une entité mais également l'origine de l'information ou encore d'une opération effectuée sur celle-ci.
- **Autorisation :** assure le contrôle du type d'activités ou d'informations qu'une personne ou entité est autorisée à effectuer ou accéder.
- **Non-répudiation ou irrévocabilité :** assure le fait qu'une personne ou entité ne puisse nier avoir effectué une activité. Dans le domaine du courriel, l'irrévocabilité est utilisée pour assurer que le destinataire ne pourra nier avoir reçu l'information, et assurer que l'expéditeur de la source de l'information ne peut nier avoir envoyé l'information.

1.5 Menaces

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant,qu'il soit interne ou externe à l'entreprise. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces derniers sont difficiles à réaliser.

- **Menaces graves :** Il s'agit de menaces classiques capables d'effectuer par elles-mêmes des actions destructrices et illégales (suppression et vol de données, pannes de réseau, etc.) au sein du système. Ces menaces incluent les logiciels traditionnellement connus sous le nom de Malware . Ce sont des vers, des virus et des chevaux de Troie.

- **Menaces mineures :** Ces menaces sont considérées comme moins dangereuses, mais peuvent être utilisées par des tiers pour effectuer des actions malveillantes. De plus, la présence de menaces même mineures dans le système démontre sa vulnérabilité. Les experts en sécurité informatique décrivent de telles menaces comme des logiciels "gris" (graywares) ou des "logiciels potentiellement non sollicités" (PUP - Programmes Potentiellement Indésirables), qui sont les types de logiciels suivants :adwares, dialers, canulars, riskwares et hacktools[2].

1.6 Attaques

Dans ce qui va suivre, nous présenterons les différents étapes et types d'attaques

1.6.1 Les étapes d'une attaque

Identification de la cible : Cette étape est indispensable à toute attaque organisée.Elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS...etc.

Le scanning : L'objectif est de compléter les informations réunies sur une cible visée.Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall...). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de perturber un réseau et entrainer la défaillance de certains systèmes. L'exploitation : Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, de services et applications ou des systèmes d'exploitation présents sur le réseau.

La progression : Il est temps pour l'attaquant de réaliser ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers root (administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces,...etc).

1.6.2 Les différents types d'attaques

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques-unes.

Le sniffing : Grâce à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que la carte reçoit et qui ne sont pas destinées. Si quelqu'un se connecte par telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblé.

L'IP spoofing : Cette attaque est difficile à mettre en oeuvre et nécessite une bonne connaissance du protocole TCP.Elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "spoofée". Cette attaque n'est intéressante que dans la mesure où la machine de confiance dont l'attaquant a pris l'identité peut accéder au serveur cible en tant que root.

Le DoS (Denial of Service) : Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Il en existe de plusieurs types comme le flooding", le smurf ou le débordement de tampon (buffer-overflow).

Les programmes cachés ou virus : Il existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un événement du système (appel d'une primitive, date spéciale). **L'ingénierie sociale (social engineering) :** Ce n'est pas vraiment une attaque informatique en soit, mais plutôt une

méthode consistant à se faire passer pour quelqu'un que l'on n'est pas afin de recueillir des informations confidentielles.

Le craquage de mots de passe : Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne) Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

1.6.3 les Différents cibles d'attaque

Une "attaque informatique" ou "cyberattaque" est un acte délibéré et malveillant qui utilise un réseau informatique pour endommager des informations ou ses processeurs. Cette dernière à plusieurs cibles[8](voir figure 1.1).

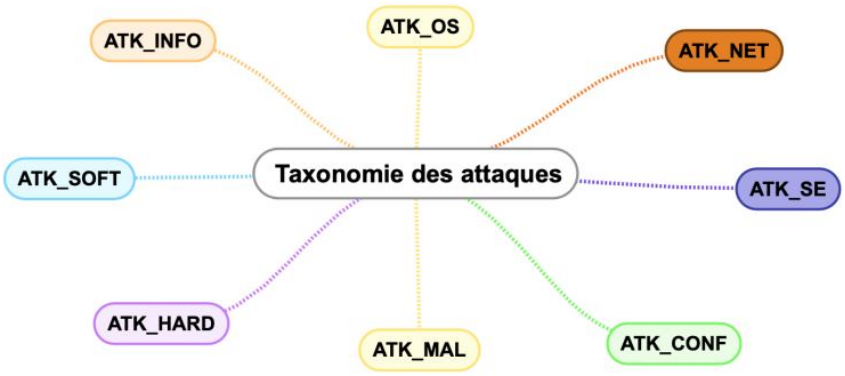

FIGURE 1.1 – Les différents cibles d'attaque [8]

Attaque sur les réseaux : De nombreux protocoles réseau ont historiquement été implémentés sans le concept de sécurité.Les éléments d'un système d'information est nécessaire pour cela il communique à travers plusieurs canaux configurés. Les canaux secrets sont des canaux de communication possibles, mais ils ne doivent pas être utilisés comme canaux de communication lors de la conception de système. Par conséquent, les canaux secrets peuvent envoyer des informations sans l'autorisation ou la connaissance du propriétaire de l'information ou de l'administrateur réseau.

Attaques sur les système d'exploitation : Les services de l'infrastructure étant fournis au-dessus du système d'exploitation, plusieurs attaques impliquent leur exploitation. Par conséquent, un système d'exploitation non maintenu ou obsolète en est souvent la principale raison. De plus, les vulnérabilités récemment découvertes mais non corrigées sont une tactique courante utilisée par les attaquants.

Attaques sur les applications et les logiciels :
Les applications présentent souvent des vulnérabilités qui peuvent être causées par une mauvaise exécution. Cette mise en œuvre inadéquate peut être causée par une négligence lors des étapes d'analyse et de conception de la sécurité, un manque de compétences/de sensibilité des développeurs, des problèmes de synchronisation et un manque de tests de sécurité pendant le développement ou la mise en œuvre. Les experts en sécurité découvrent de nombreuses vulnérabilités logicielles et des pirates .

1.7 Notion de politique de sécurité

La politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en oeuvre pour les assurer. La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation. Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.

Sa mise en oeuvre se fait selon les quatre étapes suivantes :

1. Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.

2. Elaborer des règles et des procédures à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés.

3. Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés

.

4. Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

1.8 Sécurité de l'infrastructure

— **Sécurité des accés** : Les politiques de sécurité d'accès doivent aussi répondre aux exigences légales. Ainsi les employés tout comme les invités doivent avoir des accès différenciés en fonction de leur rôle dans l'entreprise mais également de leur terminal

et de sa conformité.

— **Sécurité du réseau Intranet face à Internet** :Il s'agit d'un réseau informatique privé utilisé par les employés d'une entreprise (ou toute autre entité équivalente), et qui utilise les mêmes protocoles d'échange que sur Internet. L'Intranet se présente d'ailleurs sous la forme d'un site Web. Il permet aux collaborateurs d'échanger des documents et des informations dans un environnement sécurisé, dont l'accès est réservé à un groupe défini. En facilitant la vie professionnelle quotidienne, il représente ainsi l'infrastructure de base de la communication interne d'une organisation[3].

1.9 Techniques de parade aux attaques

La mise en oeuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité.
Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont les systèmes pare-feu. Néanmoins ce type de dispositif ne protège pas la confidentialité des données circulant sur le réseau.
Ainsi, la plupart du temps il est nécessaire de recourir à des applications implémentant des algorithmes cryptographiques permettant de garantir la confidentialité des échanges. La mise en place de tunnels sécurisés VPN (ainsi que d'autres dispositifs et mise en oeuvre cités ci-dessous) permet d'obtenir un niveau de sécurisation supplémentaire dans la mesure où l'ensemble de la communication est chiffré.

Pare-feu :
C'est un ensemble de composants matériels (physiques) et logiciels (logiques) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines du réseau.Il s'agit ainsi d'une passerelle filtrante.

Sans l'utilisation d'un pare-feu, les différents systèmes du sous-réseau s'exposent à des attaques venant de l'extérieur. Dans un environnement, sans firewall, la sécurité du réseau est basée sur la sécurité au niveau des hôtes et tous les hôtes doivent, dans un sens, coopérer pour atteindre un haut niveau uniforme de sécurité. Plus le sous-réseau est grand, moins il est facile de maintenir tous les hôtes au même niveau de sécurité. Lorsque les erreurs et les défaillances en sécurité deviennent courantes, les intrusions n'apparaiteront plus comme le résultat d'attaques complexes, mais à cause de simples erreurs de configuration et de choix de mots de passe inadéquats. Il suffirait alors qu'un des sytèmes hôtes soit compromis pour que tout le site devienne vulnérables[4].

Serveur Proxy :
Un serveur proxy est un système informatique situé entre le client qui demande un document Web et le serveur cible (un autre système informatique) qui sert le document. Dans sa forme la plus simple, un serveur proxy facilite la communication entre le client et le serveur cible sans modifier les demandes ou les réponses. Lorsque nous lançons une demande de ressource auprès du serveur cible, le serveur proxy détourne notre connexion et se présente comme un client auprès du serveur cible, demandant la ressource en notre nom.

Si une réponse est reçue, le serveur proxy nous la renvoie, donnant l'impression que nous avons communiquée avec le serveur [5].

DMZ(Zone démilitarisée) :
Dans les réseaux informatiques, une zone démilitarisée, ou DMZ, est un hôte informatique ou un petit réseau inséré comme une "zone neutre" entre le réseau privé d'une entreprise et le réseau public extérieur. La DMZ empêche les utilisateurs extérieurs d'avoir un accès direct à un serveur contenant des données de l'entreprise. Une DMZ est une approche optionnelle et plus sûre qu'un pare-feu et agit efficacement comme un serveur proxy [6].

Antivirus :
Un antivirus est un logiciel qui vise à offrir une meilleure protection que celle offerte par le système d'exploitation sous-jacent (tel que Windows ou Mac OS X). Dans la plupart des cas, il est utilisé comme une solution préventive. Cependant, lorsque cela échoue, le logiciel Antivirus est utilisé pour désinfecter les programmes infectés ou pour nettoyer complètement les logiciels malveillants du système d'exploitation.

Les logiciels antivirus utilisent diverses techniques pour identifier les logiciels malveillants, qui s'auto-protègent souvent et se cachent dans les profondeurs d'un système d'exploitation. Les logiciels malveillants avancés peuvent utiliser des fonctionnalités non documentées du système d'exploitation et des techniques obscures afin de persister et d'éviter d'être détectés. En raison de la grande surface d'attaque de nos jours, les logiciels antivirus sont conçus pour traiter toutes sortes de charges utiles malveillantes provenant de sources fiables et non fiables[7].

Les IPS(System de Prévention) et IDS(Détection d'intrusion) : Un ensemble complet de contre-mesures pour réduire les risques de sécurité informatique Conçu pour s'assurer que le périmètre de l'entreprise n'est pas affecté par Accès non autorisé oux données sensibles .
Objectif de ce mécanisme est d'alerter les administrateurs et les experts en sécurité si une personne, un programme ou un service tente d'accéder à une partie de l'infrastructure . A cette fin, IDS et IPS sont divisés en plusieurs catégories[8].

- Les IDS / IPS réseaux, aussi appelés NIDS / NIPS pour Network Intrusion Detection System, dont le but est de détecter d'éventuelles intrusions sur le réseau.

- Les IDS / IPS hôtes, aussi appelés HIDS / HIPS pour Host Intrusion Detection System dont l'objectif et de détecter les éventuelles intrusions sur différentes machines de l'infrastructure de l'entreprise.
- IDS hybride qui utilise les NIDS et HIDS pour avoir des alertes plus pertinentes. De plus ,ils permettent une meilleure détection d'attaque distribuée.

1.10 Conclusion

Le but de ce chapitre était d'introduire les principes fondamentaux liés à la sécurité informatique et des réseaux . Nous avons présenté la nécessité de le sécuriser. L'objectif est de bien définir le concept d'administration et la sécurité d'un réseau au sein d'une entreprise.

Chapitre 2

SIEM (Security Information and Event Management)

2.1 Introduction

Dans ce chapitre nous allons présenter le rôle et fonctionnement des SIEM. Nous allons ensuite citer quelques solution SIEM open source et propriétaire puis faire une comparaison entre ces solution .

2.2 Historique de SIEM

Dans la littérature informatique, le premier SIEM a été créé à la fin des années 1990 . Cependant, il ne portait pas ce nom à l'époque. Ce n'est qu'en 2005 que deux analystes de Gartner, Mark Nicolet et Amrit Williams, inventent l'acronyme qui sera la référence du marché de la cybersécurité. Les premiers SIEM offraient aux équipes informatiques une visibilité en temps réel pour gérer et centraliser de nombreuses alertes de sécurité afin de mieux comprendre certains événements indésirables du système d'information. La nouvelle génération SIEM peut gérer un nombre immense d'alertes et fournir des professionnels, des corrélations, des rapports et un tableau de bord beaucoup plus efficace. Avec ces nouveaux SIEM, les journaux d'événements (ou journaux) peuvent être conservés pendant de longues périodes, ce qui facilite les enquêtes post-attaque[9].

2.3 SIEM

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

SIEM est aussi connu comme système d'analyse de la sécurité (Big Data),système de renseignement sur les cybermenaces.

Le SIEM il est composé de deux concepts qui sont : SEM (gestion des événements de sécurité) et le SIM (gestion des informations de sécurité)

SEM :

Il traite les données des journaux et des événements des dispositifs de sécurité,, systèmes et applications en temps réel pour assurer la sécurité la surveillance, la corrélation des événements et les réponses aux incidents. SIEM soutient les activités de surveillance des menaces externes et internes de l'organisation de la sécurité informatique et améliore la gestion des incidents [10].

SIM :

Il fournit la gestion des journaux , la collecte, la création des rapports et analyse les données des systèmes hôtes et des applications, des périphériques réseau et de sécurité.Il prend en charge les rapports de conformité réglementaire,la gestion interne des menaces et surveillance de l'accès aux ressources. SIM s'occupe l'utilisateur privilégié et les activités de surveillance de l'accès aux ressources , ainsi que les besoins des rapports de l'audit interne et les organismes de conformité [10].

Les SIEM utilisent des étapes de récupération, analyse et gestion de l'information,qui consiste la collecte, la normalisation, l'agrégation, la corrélation, le reporting et la réponse.

2.4 Rôle et Fonctionnement des SIEM

- **Rôle :**
  Les environnements informatiques sont de plus en plus distribués, complexes et difficiles à gérer.La taille et la complexité des entreprises augmentent de façon exponentielle. Les opérations informatiques sont souvent réparties entre différents groupes, tels que le centre d'exploitation du réseau, le centre d'exploitation de la sécurité, l'équipe des serveurs, l'équipe des postes de travail, etc.
  Chacun disposant de ses propres outils pour surveiller et répondre aux événements.Cela rend le partage de l'information et la collaboration difficiles lorsque des problèmes surviennent. Un SIEM peut rassembler les données de systèmes disparates dans un seul et même écran, ce qui permet une collaboration efficace entre les équipes dans les très grandes entreprises [11].

- **Fonctionnement des SIEM :**
  Examinons de plus près les principales fonctionnalités des solutions SIEM :
  - **l'agrégation :** L'agrégation des logs est le processus de regrouper plusieurs logs dans le même log selon des critères bien définis.Elle s'applique sur les logs du même type et elle facilite les vues du SIEM. L'agrégation a plusieurs avantages comme la réduction du nombre des logs dans le SIEM, l'accélération des opérations de recherche et la facilitation des tâches de surveillance. Cependant, la mauvaise implémentation des règles d'agrégation peut conduire à la perte des informations importantes. Cela facilite notamment le traitement de l'étape de corrélation, qui gère alors plus des évènements individuels mais des groupes d'évènements.

  - **Corrélation :** La corrélation correspond à l'analyse d'évènements selon certains critères. Ces critères sont généralement définis par des règles appelées règles de

corrélation. Le but de cette étape est d'établir des relations entre évènements, pour ensuite pouvoir créer des alertes de corrélations, des incidents de sécurités, des rapports d'activité.La corrélation se différencie sur plusieurs points :
-Auto-apprentissage et connaissances rapportées : Pour pouvoir fonctionner, les moteurs de corrélation ont besoin d'informations sur les systèmes et réseaux de l'infrastructure. Ces informations peuvent être collectées automatiquement et/ou saisies manuellement par un opérateur.
-Temps réel et données retardées : Dans certains cas, les événements bruts sont forgés et envoyés directement pour être corrélés en temps réel. Dans d'autres cas, les événements sont d'abord stockés, et envoyés après un premier traitement .Leur envoi peut être alors conditionné.
-Corrélation active et passive : La corrélation active a la possibilité de compléter les évènements reçus en recueillant des informations supplémentaires pour prendre des décisions. La corrélation passive est une corrélation qui ne peut pas interagir avec son environnement.Elle reçoit des évènements et prend des décisions.[9]

- **Les rapports :** Les rapports générés contiennent à la fois un résumé des alertes et un aperçu de la sécurité du système à instant T. SIEM peut également créer et générer des tableaux de bord et des rapports. Ainsi, différents acteurs administrateurs, utilisateurs peuvent connaître le SI (nombre d'attaques, nombre d'alertes par jour, etc.).
- **Tableaux de bord :** Les outils SIEM prennent les données des événements et les transforment en d'événements et les transforment en graphiques informatifs pour aider à voir les l'activité qui ne forme pas un modèle standard.[11]
- **Alertes :** Le SIEM fournit l'analyse automatisée des événements corrélés et la production d'alertes, afin de notifier les destinataires de problèmes immédiats.

Le schéma ci-dessous (figure 2.1) représente les fonctionnements d'un SIEM

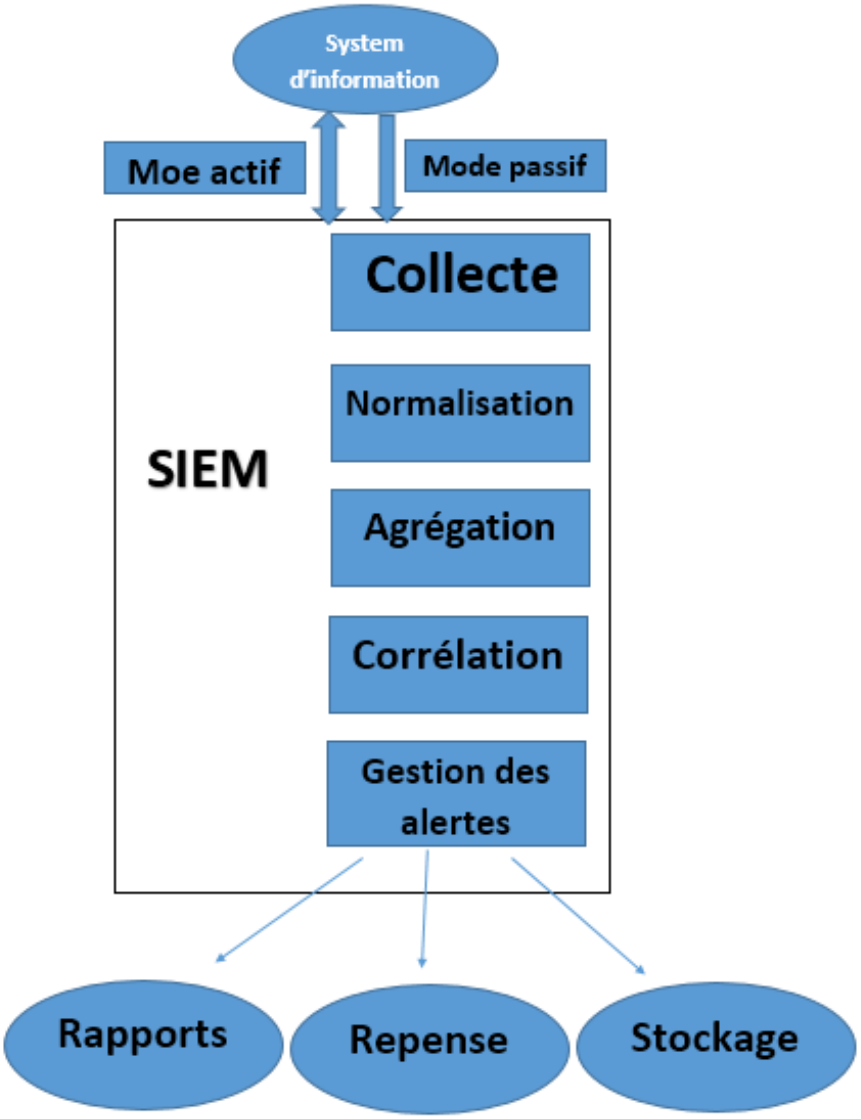

FIGURE 2.1 – Schéma de fonctionnement théorique d'un SIEM [9]

2.5 Modes de fonctionnement

Les équipements et logiciels de sécurité sont nombreux dans un système d'information, ils gèrent généralement de façon indépendante des informations de sécurité dites locales. Le principe de l'étape de collecte est de fournir au SIEM des données à traiter. Ces données peuvent être de nature diverse en fonction de l'équipement ou du logiciel, mais aussi être envoyées de manières tout à fait différentes. On distingue deux modes de fonctionnement [9] :

- **Mode actif :** Le SIEM possède un ou plusieurs agents déployés sur les équipements à superviser. Ces agents ont pour fonction de récupérer les informations des équipements et logiciels de sécurité et de les envoyer au SIEM. Un élément de sécurité qui a été conçu nativement pour être un agent du SIEM est appelé une sonde.

- **Mode passif :** Le SIEM est en écoute directe sur les équipements à superviser. Pour cette Méthode, c'est l'équipement ou le logiciel qui envoie des informations sans intermédiaire au SIEM.

2.6 Avantages et Inconvénients

SIEM présente et offre plusieurs avantages à tous les types d'organisations. Parmi ces avantages :

- La détection efficace des événements de sécurité .
- La prise des mesures défensives plus rapidement.
- La gestion des événements.
- Répond aux exigences de conformité d'une entreprise.
- Permet d'avoir une vue globale d'un réseau.

De plus, il permet aux organisations de gérer plus facilement la sécurité en filtrant de gros volumes de données de sécurité et en donnant la priorité aux alertes de sécurité générées par les logiciels.

Les SIEM peuvent également aider les organisations à répondre aux exigences de conformité en générant automatiquement des rapports qui incluent tous les incidents de sécurité enregistrés dans leurs sources. Sans cet outil, les entreprises devraient collecter manuellement les données des journaux et compiler les rapports.

Ils améliorent également la gestion des incidents en permettant aux équipes de sécurité de découvrir.

Cependant ,les SIEM présentent quelques inconvénients notamment :

- La configuration est parfois trop complexe .
- Les coûts de déploiement peuvent être élevés .
- De nombreuses alertes à surveiller .
- Non conçu pour identifier les vulnérabilités .
- Pas de détails sur la sensibilité des données .

Les outils SIEM dépendent généralement de règles pour analyser toutes les données enregistrées. Le problème, c'est que le réseau d'une entreprise génère un grand nombre d'alertes généralement 10 000 par jour qui peuvent être positives ou non. Difficile, dans ces conditions, d'identifier les attaques potentielles en raison du nombre de journaux non pertinents.

2.7 Quelques solutions SIEM

Il existe plusieurs solutions qui sont proposées par plusieurs en-têtés. Certaines sont payantes parce que elle sont propriétaires comme SPLUNK, SolarWinds, IBM QRadar, MCAfee et LogRhythme, d'autres sont libres ou gratuites(open Source) comme OSSIM, SIEMonster, Prelude, ELK et Graylog.
La figure 2.2 présente un schéma de classification des solutions SIEM selon la capacité d'exécution et l'intégralité de la vision.

FIGURE 2.2 – Classement des solutions SIEM en 2021[12].

Avant de déterminer la solution qui convient à notre projet,nous allons faire une brève présentations de certaines solutions,notamment IBM Qradar,MCAFee,ELK,LogRhythm,SPLUNK.

IBM QRadar : QRadar SIEM consolide les données d'événement de source de journal à partir de milliers de périphériques distribués et de points de terminaison d'application sur le réseau. Il effectue immédiatement des activités de normalisation et de corrélation sur les données brutes pour différencier les menaces réelles des faux positifs.

MCAFee : McAfee Enterprise Security Manager offre une visibilité en temps réel sur le monde extérieur (données sur les menaces, sources de réputation et statut de vulnérabilité) et une vue des systèmes, des données, des risques et des activités au sein de l'entreprise.

ELK(Elasticsearch Logstash Kibana) : Pile ELK (ELK Stack) est une collection de trois produits open-source : Elasticsearch, Logstash et Kibana. Ils sont tous développés, gérés et maintenus par la société Elastic. C'est une plateforme de gestion centralisée de logs qui intègre plusieurs technologies ensemble dans le but de permettre aux utilisateurs d'utiliser des données provenant de n'importe quelle source, quel que soit leur format, et de rechercher, analyser et visualiser ces données en temps réel.

LogRhythm : C'est une plate-forme d'entreprise qui associe de manière transparente, la gestion des journaux, la surveillance de l'intégrité des fichiers et l'analyse des machines, aux analyses d'hôte et de réseau, au sein d'une plate-forme unifiée de renseignements de sécurité. Il est conçu pour faire face à un paysage en constante évolution de menaces et de défis, avec une suite complète d'outils haute performance pour la sécurité, la conformité et les opérations .

SPLUNK : Logiciel pour suivre et analyser des données machine ,Splunk (produit) collecte, indexe et met en corrélation des données en temps réel dans des archives consultables, permettant la génération de graphiques, de rapports, d'alertes, de tableaux de bord et d'infographies.

2.8 Choix de la solution

Quelle que soit la solution SIEM solutions telles que choisir, la plate-forme doit disposer de certaines fonctionnalités de base telle que :

1) Gestion des journaux : collecte, normalisation et surveillance continue des fichiers journaux pour détecter les comportements anormaux.

2) Corrélation entre les événements : La capacité d'un SIEM à identifier les menaces qui peuvent exister sur un réseau sous différentes formes. Un SIEM peut comparer les activités suspectes d'un utilisateur donné sur le réseau et les identifier comme étant liées.

3) Identification des menaces : Avec une plateforme SIEM, on peut créer en continu des déclencheurs pour différentes alertes. et elle est compose d'une utilisation qualifiés améliorent la capacité à identifier les menaces et à réagir efficacement.

4) Rapports : C'est l'un des grands avantages de la construction d'un SIEM. Il est possible de créer des rapports personnalisés afin que la bonne personne ou le bon groupe de personnes sache toujours quand quelque chose ne va pas.

5) Réponse aux incidents :Le SIEM permet de collecter des informations sur les incidents potentiels. Si quelque chose de suspect se produit.

6) Renseignements sur les menaces : Une plate-forme SIEM solide comprend des capacités intégrées pour accéder aux données sur les menaces qui se produisent dans le monde, ainsi que la capacité de comprendre leur relation potentielle avec les événements se produisant sur le réseau.

2.9 ELK-VS-Splunk

D'après l'organisme d'accueil (Ifri) et leur besoin ,le département technique et infrastructures veut implémenter une parmi les deux solutions suivant : ELK ou bien SPLUNK. Pour cela nous allons faire une comparaison entre les deux.

Sr.Nom	Pile ELK	Splunk
1	Combinaison de 3 produits différents pour l'extraction, le stockage et l'analyse des données de journal	Il s'agit d'un produit unique comportant trois composants différents pour gérer les opérations de surveillance.
2	La conception du modèle de données et de l'index doit être finalisée en amont. Toute extraction de données doit être configurée dans Logstash bien avant. Chaque champ doit être défini dans la configuration	Toutes les données peuvent être extraites dynamiquement de la source et peuvent être analysées.
3	Les champs de données de la visualisation sont prédéfinis et ne peuvent pas être modifiés à la volée	De nouveaux champs de données peuvent être ajoutés de manière flexible à la volée pendant l'exécution.
4	Le critère des opérations de recherche est prédéfini	La recherche peut être effectuée à l'aide de n'importe quel champ de données.
5	A une grande base communautaire et beaucoup de soutien est disponible.	Dispose d'une bonne documentation et d'un formulaire bien informé pour l'assistance.
6	Les fonctions de gestion des utilisateurs ne sont pas si puissantes	L'administrateur a un bon contrôle en fournissant une autorisation au niveau du champ aux utilisateurs. Les utilisateurs peuvent configurer leur propre tableau de bord personnalisé.
7	Entièrement open source et gratuit	Les licences sont facturées en fonction de l'utilisation quotidienne. Facturé sur une base annuelle ou perpétuelle.
8	Certaines fonctionnalités d'ELK sont difficiles à configurer	Les configurations sont faciles à gérer.
9	A moins de fonctionnalités et d'avantages	A plus de fonctionnalités et d'avantages.
10	Pas d'investissement majeur dans la formation car la main-d'œuvre formée est disponible en abondance.	Les utilisateurs doivent investir une bonne somme dans la formation.

Tableau 2.1 – Tableau de comparaison de la pile ELK vs Splunk[13]

• Splunk offre une flexibilité riche en fonctionnement et conviviale, mais elle a un coût élevé. D'après la comparaison effectuée , splunk convient a tout les besoins de l'entreprise et simple à la mise en place.

2.10 Ecosystéme splunk

Splunk peut récupérée n'importe quelle source de données. soit sur le cloud ou sur des bases de données des systèmes d'exploitation des logs réseaux . un schéma explicatif est présente la figure 2.3 .
splunk est l'une des solutions les plus riches mais aussi des plus simples avec tout type d'environnement , aussi c'est une solution a travers laquelle on peut effectuer des recherches directement du monitoring ou de l'alertine, de faire du reporting et de l'analyse ou encore de pouvoir créer des tableaux de bord bien spécifiques.

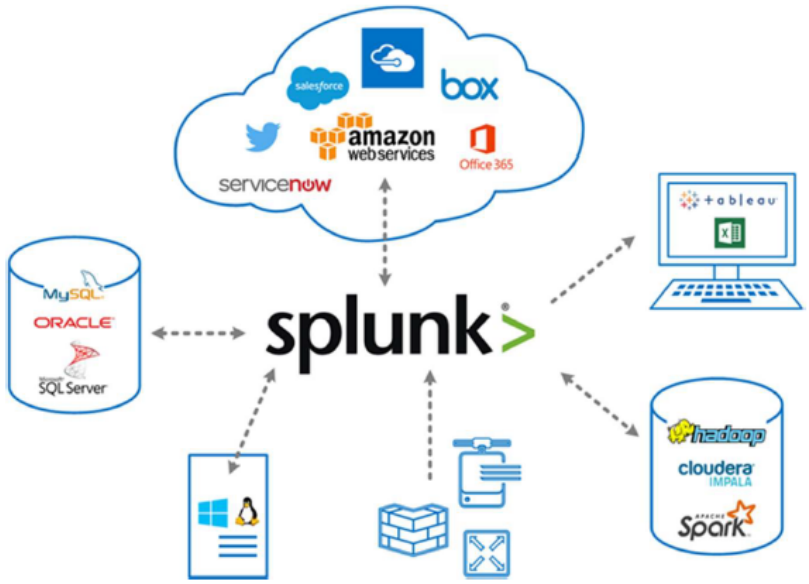

FIGURE 2.3 – Ecosystéme Splunk [20]

.

2.11 Fonctionnement de Splunk

Splunk offre essentiellement quatre fonctionnalités principales qui sont [14] :

- **Récupérer les données** : Il s'agit de la première phase d'embarquement des données. Il existe plusieurs méthodes pour faire entrer des données dans Splunk : il peut écouter le port, le point de terminaison d'API REST, le protocole de contrôle de transmission (TCP), le protocole de datagramme utilisateur (UDP), etc. ou utiliser une entrée scriptée.

- **Analyser** : La deuxième phase consiste à analyser l'entrée dans laquelle un morceau de données est décomposé en divers événements. La taille maximale des données dans le pipeline d'analyse est de 128 Mo. Dans la phase d'analyse syntaxique, vous pouvez extraire des champs par défaut, tels que le type de source et également extraire les horodatages des données, identifier la fin de la ligne et effectuer d'autres actions similaires. également masquer des données sensibles mais utiles. Par exemple, si les données proviennent d'une banque et comprennent les numéros de compte des

clients, le masquage des données est essentiel. Dans la phase d'analyse syntaxique, et appliquer des métadonnées personnalisées, si nécessaire.

- **Indexer** : Dans cette phase, l'événement est divisé en segments dans lesquels la recherche peut être effectuée. Les données sont écrites sur le disque et concevoir des structures de données d'indexation.

- **chercher** : Dans cette phase, les opérations de recherche sont effectuées sur les données d'indexation, et créer un objet de connaissance et effectuer n'importe quelle tâche, par exemple un rapport de vente mensuel. Les données d'entrée, l'analyseur syntaxique et l'indexeur se trouvent tous sur une machine autonome. En revanche, dans un environnement distribué, les données d'entrée sont analysées par l'indexeur ou le Forwarder (UF). le shéma 2.4 montre les principales fonctionnalités de splunk.

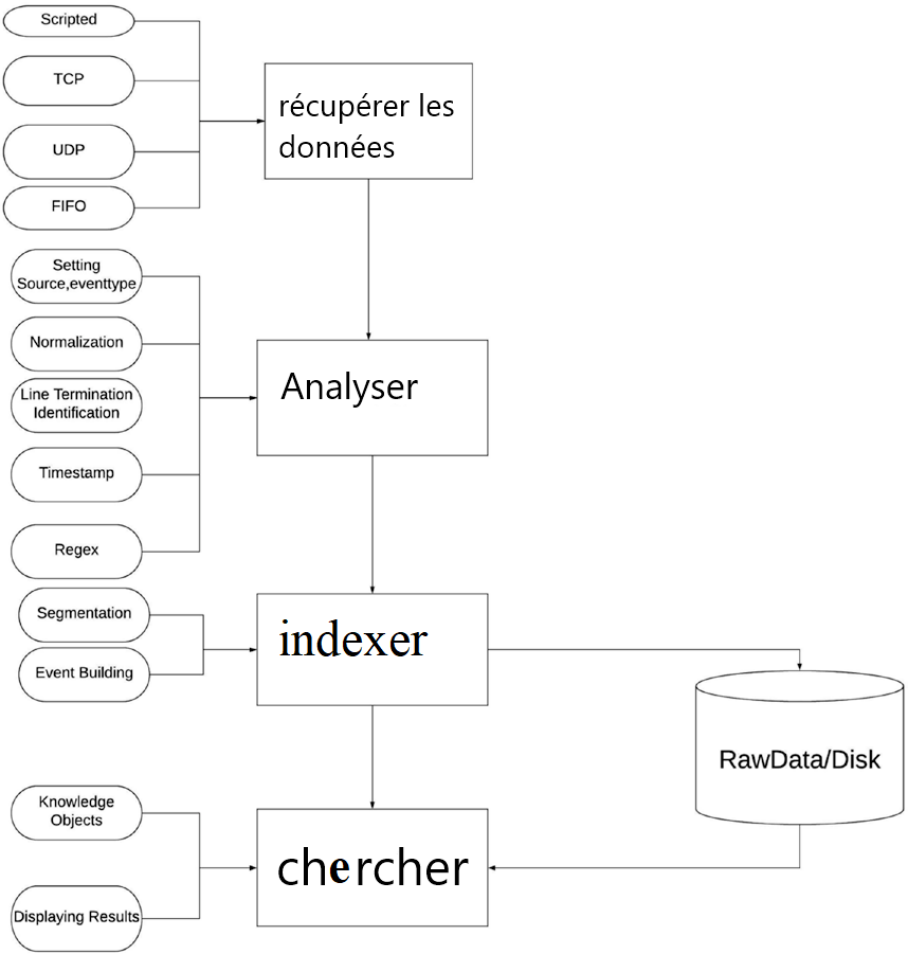

FIGURE 2.4 – Fonctionnalités de splunk[14]

2.12 Systéme de licence de splunk capacity planning

La licence Splunk détermine la limite de gestion des données. Chaque instance de Splunk Enterprise a besoin d'une licence qui spécifie les règles sur la quantité de données qu'elle peut indexer en une journée. Il existe différents types de licences Splunk.

Licence Splunk Entreprise : La licence "standard" de Splunk Enterprise spécifie le type de données qui sont indexées, disponibles à l'achat ou configurées.

Licence No-Enforcement : La licence Splunk Enterprise standard a un volume maximum d'indexation par jour,avec lequel l'entreprise reçoit un avertissement de violation s'il dépasse. plus de cinq avertissements en un mois. Cela peut entraîner la désactivation de la tête de recherche Splunk. Cependant, dans le cas d'un système sans application.

Licence d'essai Enterprise : Licence d'essai Enterprise permet une indexation maximale de 500 Mo/jour. Elle expire après 60 jours, et il sera demandé de passer à la licence standard Splunk Enterprise ou la licence gratuite.

Licence d'essai de vente : La licence d'essai Enterprise expire après 60 jours et offre une capacité d'indexation de 500 Mo/jour. Si un projet nécessite une capacité d'indexation supérieure à 500 Mo/jour,il est possible d'utiliser la licence d'essai. En contactons directement l'équipe commerciale de Splunk pour obtenir une licence.

Licences Splunk pour l'IoT industriel : Splunk propose une licence spéciale pour l'IoT industriel qui donne accès à des ensembles d'applications spécifiquement conçues.

Licence Forwarder : La licence Forwarder permet le transfert d'un nombre illimité de données. Contrairement à une licence gratuite, elle permet l'authentification et p as nécessaire d'acheter une licence supplémentaire car elle est incluse dans Splunk.

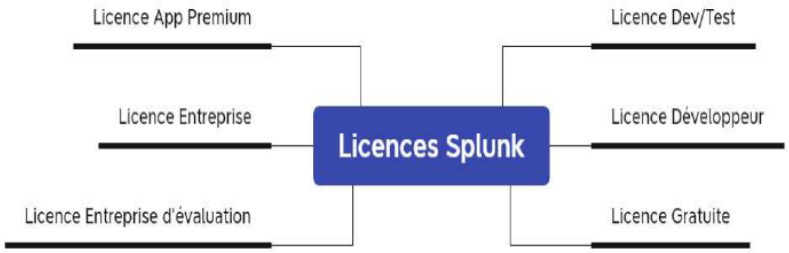

FIGURE 2.5 – Systéme de license de splunk capacity planning [21]

2.13 Principaux composants de splunk

Forwarder

Ce sont les agents collecteurs de logs , installés sur les systèmes d'exploitation Unix et Windows, le forwarder universel collecte et envoie les données de la machine aux indexeurs pour un traitement et un stockage ultérieurs.
Les forwarder assurent une collecte fiable et sécurise des données provenant de sources distantes et les transmets à Splunk pour indexation et consolidation. Ils peuvent évoluer jusqu'à des dizaines de milliers de systèmes distants.

Il existe deux types de forwarder Splunk, qui sont :

- **Forwarder Universel (UF) :** un agent Splunk installé sur un système non-Splunk pour collecter les données localement, mais ne peut ni analyser ni indexer les données.
- **Heavy Weight Forwarder(HWF) :**instance complète de splunk avec les fonctionnalités avancées.Fonctionne généralement comme un collecteur distant, un transitaire intermédiaire et éventuellement un filtre car il analyse les données.

Indexeur

L'indexeur est le processus central de Splunk qui transforme les données brutes en événements interrogeables et les stocke dans des index. Pendant l'indexation, l'indexeur décompose les données brutes en événements, extrait l'horodatage (et quelques autres méta-champs) et écrit les données sur le disque,c'est également le processus qui recherche et récupère les données indexées. Dans les systèmes Unix le processus d'indexation est nommé splunkd. Dans un environnement distribué, l'indexeur est également appelé search peer (pair de recherche). De nombreux indexeurs sont regroupés dans un cluster, et les données sont répliquées entre les membres du cluster[15].

Search head

La tête de recherche gère les recherches effectuées par les utilisateurs. Il s'agit d'un processus Splunk Enterprise qui utilise l'architecture map-reduce. Il distribue les requêtes de recherche (la phase map de map-reduce) à un groupe d'indexeurs (également connus sous le nom de pairs de recherche) où les recherches sont exécutées.
La tête de recherche reçoit les résultats de la recherche et les fusionne (la phase de réduction de map-reduce) pour les envoyer à l'indexeur, avant de renvoyer les résultats à l'utilisateur. Les têtes de recherche peuvent également être regroupées dans un cluster de têtes de recherche. Les grappes de têtes de recherche assurent une haute disponibilité et un l'équilibrage de la charge. Ils permettent également de contrôler l'accès aux données indexées. Généralement lorsque une connexion à l'interface Web de Splunk.[15].

2.14 Mode déploiement splunk

Déploiement standalone

Le déploiement se fait sur une seule instance de Splunk. Ce type de déploiement n'est jamais utilisé en pro Il est utilisé pour des POC (Proof Of Concept) ou de la formation . Un usage personnel est préconisé [16].
comme nous le voyons sur la figure 2.6

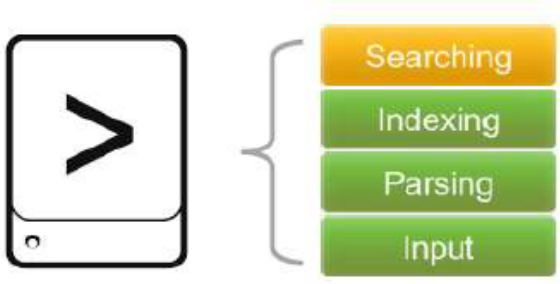

FIGURE 2.6 – Déploiement standalone [21]

Déploiement Basique

Les Forwarders assurent la collecte fiable et sécurisée de données provenant de sources diverses puis les livrent à Splunk Enterprise pour les analyser . Ce type de déploiement est similaire à la configuration d'un déploiement standalone la différence réside dans le fait qu'il y a des forwarders qui vont aller chercher des information à travers le réseau .Les forwarders envoient automatiquement des données basées sur fichier de toutes sortes à l'indexeur Splunk. comme elle le présente la figures 2.7

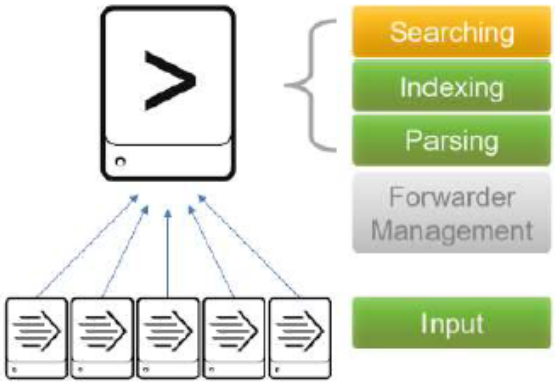

FIGURE 2.7 – Déploiement Basique (Forwarders) [21]

Déploiement multi instances

La gestion de la recherche et l'indexation sont réparties sur plusieurs machines. Dans un déploiement distribué typique, chaque instance de Splunk Enterprise effectue une tâche spécialisée et réside sur l'un des trois niveaux de traitement correspondant aux principales fonctions de traitement (voir la figures 2.8)

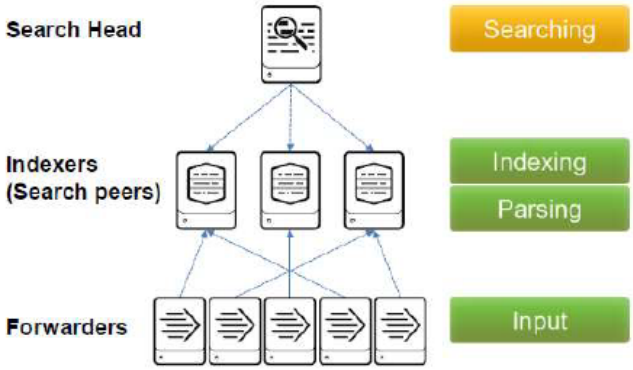

FIGURE 2.8 – Déploiement Multi-instance [21]

Déploiement capacité croissante

Permet de desservir plus d'utilisateurs pour augmenter la capacité de recherche et d'ajout d'un cluster de têtes de recherche.Un Deployeur est utilisé pour gérer et distribuer les applications aux membres du cluster de têtes de recherche(figure 2.9).

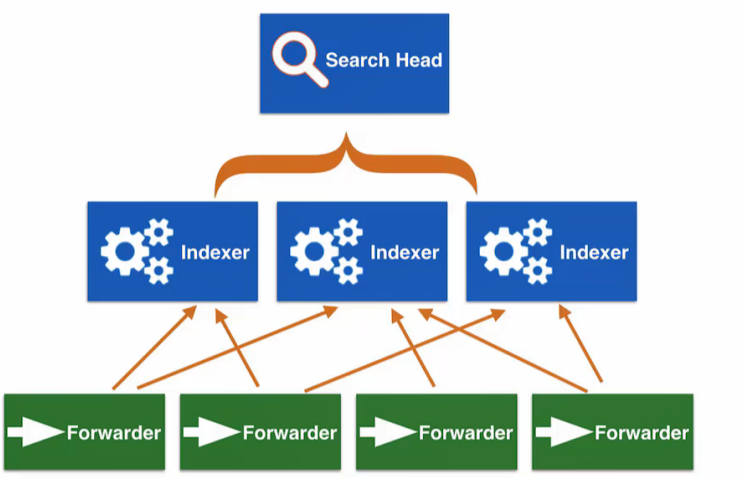

FIGURE 2.9 – Déploiement de capacite croissante [21]

Déploiement index cluster

- Clusters d'index des fonctionnalités comme Configurés pour répliquer les données,prévenir la perte de données, Favoriser la disponibilité, Gestion de plusieurs indexeurs.
- Clusters d'index non répliqués. Comme fonctionnalité Offre une gestion simplifiée et Ne fournissent pas de disponibilité ou de récupération des données. figure 2.10

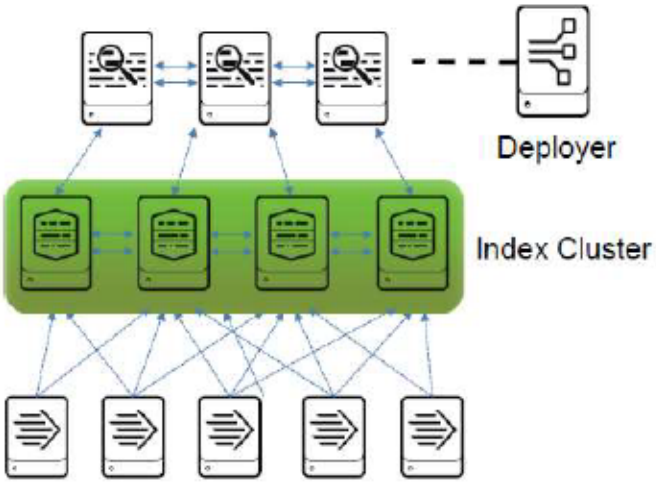

FIGURE 2.10 – Déploiment-index cluster [21]

2.15 Conclusion

Dans ce second chapitre, nous avons présenté le fonctionnement et le rôle de SIEM ainsi des solutions qui permettent la gestion centralisée des fichiers journaux et les outils qui permettent de la déployer. Après une étude comparative, nous avons opté pour la solution SPLUNK qui selon l'étude, serait le meilleur choix pour concevoir un outil SIEM flexible qui répond aux besoins de lentreprise .

Chapitre 3

Présentation de l'organisme d'accueil

3.1 Introduction

Ce chapitre est consacré sûr la présentation de l'organisme d'accueil qui nous a accueilli dans le cadre de notre stage de fin de cycle. Nous allons faire une mise en place d'une solution SIEM pour assurer la sécurité informatique au sein de GROUPE IFRI.

3.2 Groupe IFRI

La Groupe IFRI est une société à caractère industriel.Elle est spécialisée dans la production des minérales et des boissons diverses, Elle contribue au développement du secteur agroalimentaire à l'échelle nationale.

Cette société est créée par les fonds propres de M. IBRAHIM Laid en 1986.Elle était nommée «LIMONADERIE IBRAHIM » spécialisée dans la production de boissons gazeuses en emballage en verre.

Depuis la date de sa création, l'organisation a capitalisé une expérience dans le domaine des boissons, ce n'est que dix ans plus tard, en 1996, que l'entreprise hérite un statut juridique de SNC (Société Non Collective) puis le statut de la SARL (Société à Responsabilité Limitée) composée de plusieurs associés .

À cette dernière date, la marque « IFRI » est connue et exploitée dans le monde industriel. Ce fut le point de départ de la première unité de fabrication d'eau minérale naturelle en Algérie sous un emballage en bouteilles en polyéthylène téréphtalate (PET). Plus de vingt (20) millions de bouteilles ont été commercialisées sur l'ensemble du territoire national dans la même année. Ce chiffre atteint 48 millions d'unités en1999, puis 252 millions de litres en 2004. La production franchi le cap des 541378351 millions de litres dans toutes les gammes des produits IFRI en 2012.

3.3 Missions d'IFRI

L'entreprise IFRI a pour mission essentielle la production et la commercialisation des produits agroalimentaires.Elle est spécialisée dans la production d'eau minérale et de boissons diverses

en emballage en verre et PET.

La finalité de l'entreprise est d'être leader dans le domaine des eaux minérales tout en renforçant progressivement ses positions dans le segment des boissons diverses et de développer ses capacités à l'international.

Le GROUPE IFRI présentent à l'échelle nationale et internationale.Nationale dans un esprit de proximité du consommateur, le produit IFRI figure sur tout le territoire national.Et à l'échelle internationale L'établissement IFRI se lance dans la conquête du marché mondial, grâce à la stratégie du groupe en matière de développement des exportations par sa gamme élargie de boissons.

3.4 Répartition géographique

La group IFRI est réparti sur deux sites qui sont :
Site IGHZER AMOKRANE
L'activité principale et la direction de Groupe IFRI sont situées, dans la commune d'IGHZER – AMOKRANE, Daïra IFRI OUZELLAGUEN dans la wilaya de Bejaia. Elle est implantée à l'entrée-Est de la vallée de la Soummam dans la zone « AHRIK IGHZER AMOKRANE », en contre bas du massif montagneux de Djurdjura qui constitue son réservoir naturel d'eau.
Site Zone activité TAHARACHT AKBOU
L'activité secondaire de production de JUS IFRUIT est implantée à la Zone TAHARACHT a AKBOU sur un site de 20 HA destiné à recevoir les projets d'extension dans la gamme soda, jus.... etc.

3.5 Organigramme de l'organisation globale

La société travaille 24/24 heures avec des lignes de production automatisées et équipées des systèmes de contrôle de qualité de dernière génération dans toutes les unités et étapes de la production. Grâce aux options technologiques qui ont prévalu lors du choix des équipements de production et de contrôle, IFRI accroît sans cesse ses capacités. Elle veille au respect des normes d'hygiènes, de sécurité et environnementales et de qualité les plus strictes afin de diversifier sa gamme de production. Le groupe IFRI a diversifié ses filières, il est composé de quatre sociétés.

- **IFRI :** qui a pour mission de produire une gamme diversifiée de boissons (eauminérale naturelle, eau minérale gazéifiée, les sodas, les boissons fruitées, les boissons fruitées au lait).

- **GENERAL PLAST(GP) :** créée en 1999, l'entreprise GP c'est spécialisée dans la fabrication de la préforme en PET (Polyéthylène Téréphtalate) et bouchon en PEHD (Polyéthylène Haute Densité).

- **BEJAIA LOGISQTIQUE(BL) :** fondée en 2008,cette SARL BEJAIA LOGISTIQUE(BL) est la référence dans le domaine du transport routier. Son activité est étendue dans le transport public de marchandises, location d'engins et matériels pour bâtiments, travaux publics et manutention, location de véhicules avec ou sans chauffeur et dans le transport des produits pétroliers.

- **HUILERIE OUZELLAGUEN :** lancée en 2008 avec la création de la filiale oléicole dénommée SARL Huileries Ouzellaguen,spécialisée dans la transformation (trituration) d'olives et mise en bouteille d'huile d'olive extra vierge.Le produit est commercialisé sous le nom de Numidia.

La figure 3.1 présente l'organigramme de l'entreprise IFRI

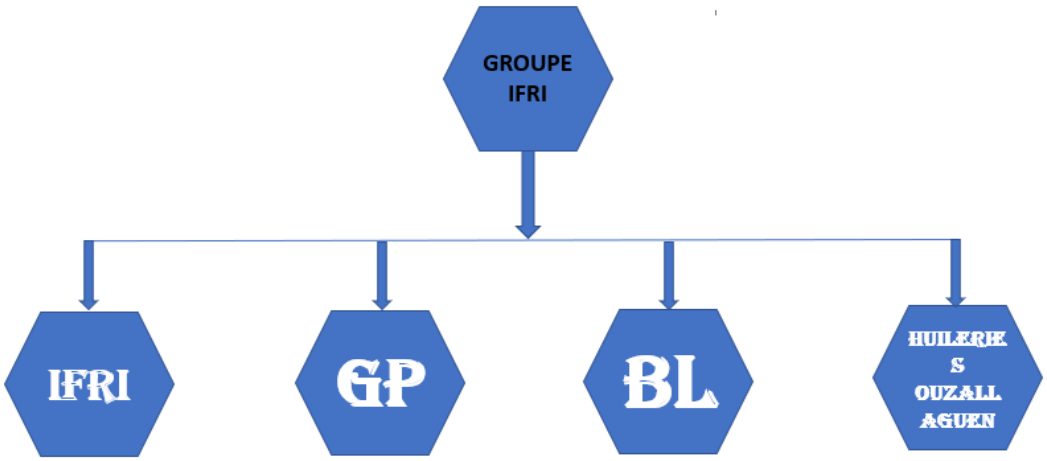

FIGURE 3.1 – Organigramme de l'entreprise IFRI.

3.6 Organisation de groupe IFRI

La structure organisationnelle des différentes fonctions de l'entreprise est présentée dans la figure 3.2 Nous avons effectué nôtre stage au sein de entrepris IFRI au département technique et infrastructures.

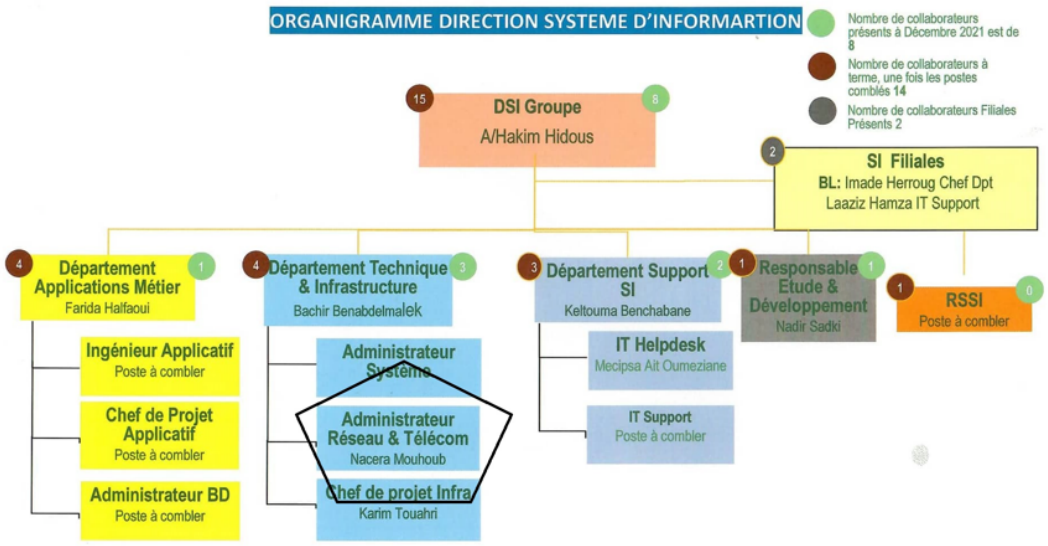

FIGURE 3.2 – Organigramme de l'entreprise IFRI.

3.7 Architecture du réseau informatique

Présentation de réseau

Le réseau de groupe est reparti sur quatre sites reliés par la fibre optique. Il est constitué de plusieurs équipements, des Switch, des routeurs, des firewalls, pour la plupart des marques hétérogène (hp, alcatel, cisco, dlink....Etc) la figur 3.3 montre l'infrastructure réseau de l'entreprise.

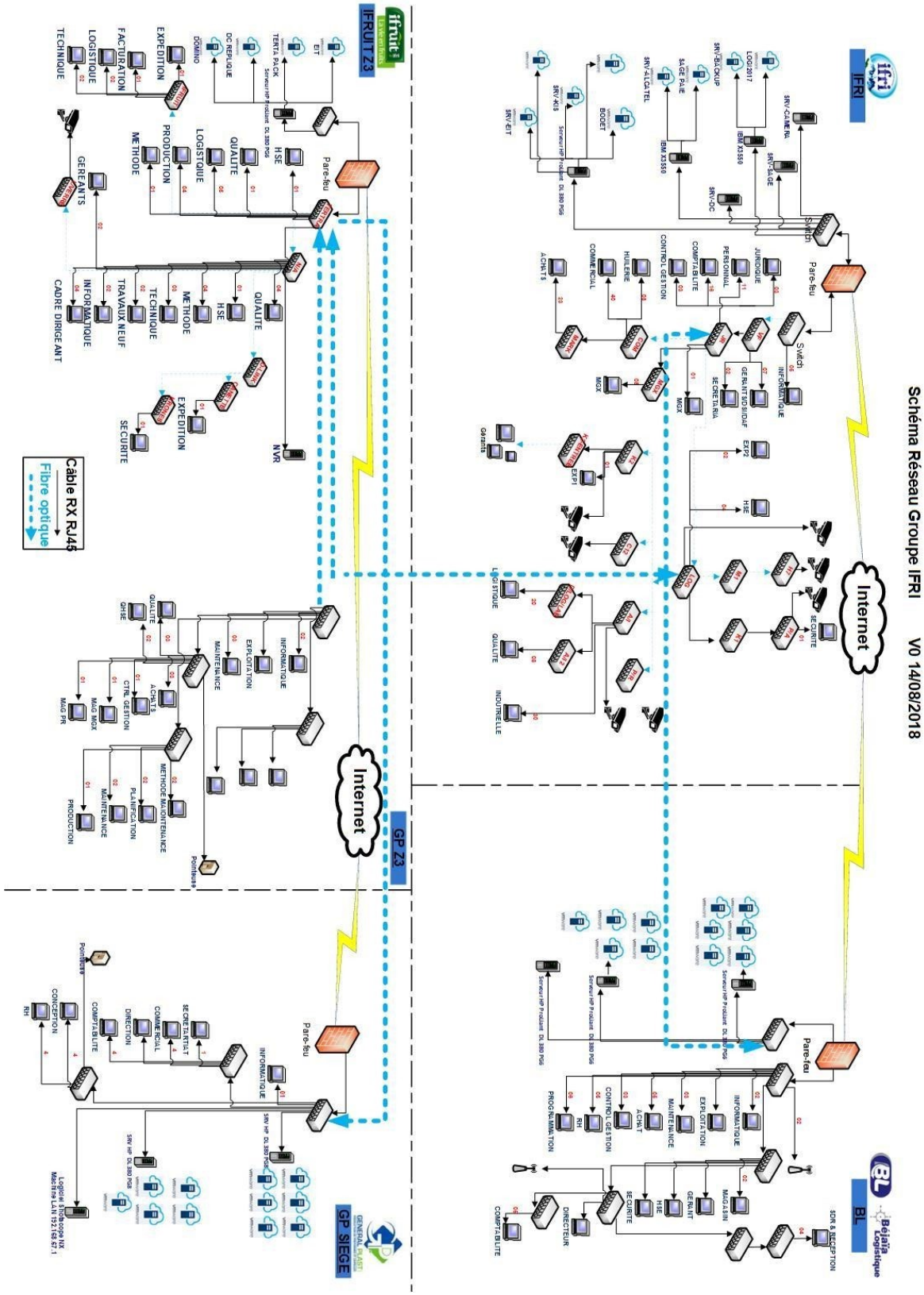

FIGURE 3.3 – Architecture réseau de l'entreprise IFRI

Parc informatique
La on citon les équipements les systèmes utilisés au sien de l'organisme IFRI .

Equipments et Matériel	Marque	Quantité
PC de bureau	Dell , HP	250
Laptop	Acer , HP, DEell	150
Imprimantes	Canon , HP , Epson	80
Serveurs	Dell , HP , Fujitsu	15
Pointage	Bodet	10
Virtualisatio	Vmware , Nutanix	50 Sv
Switchs	HP ,Télésystem , Cisco , Alcatel	50
Point d'accés Wif	D'link , Cisco	30
routeur	Cisco	4

Tableau 3.1 – Equipments et Matériel.

- **ERP et Système d'information** :ils on utilisé sage 3,sage 100,sage 7 ,Logistrace,Bodet ,ATEIS ,Dimon Maint et pour les pare-feu ils on utilisé Pfsense ,Sophos et Kaspersky

3.8 Problématique et solution proposées

Suite au confinement, l'intégration du télétravail dans les usages obligent les entreprises à repenser leur approche de la cyber sécurité. Le poste de travail du collaborateur se trouve désormais de plus en plus souvent en dehors de l'entreprise . C'est d'ailleurs une nécessité pour assurer la continuité de l'activité en cas de crise.

A cette réalité, l'entreprise IFRI , a évidemment besoin de sécuriser leur réseau, pour protéger leur confidentialité, pour cela, ils implémentent typiquement des IDS, des IPS, des pare-feu, et des technologies similaires, dans un effort pour atténuer les risques. Ils oublient souvent une étape importante la gestion des journaux. Mais comme les journaux enregistrent toute action prise sur un réseau, sont générés tout type de dispositif , leur volume risque d'être très important, au point où il devient très difficile de les gérer et donc, de les exploiter facilement.

De tous ces problèmes, le besoin d'une solution sécurité qui automatise l'exploitation des logs tout en fournissant plus de visibilité sur le système, et est né. Et le SIEM est la réponse à ce besoin. Notre application de supervision doit offrir donc plus de simplicité d'utilisation, plus d'efficacité mais aussi plus de visibilité, elle devra non seulement tenir compte des problèmes actuels mais également être capable d'évoluer facilement et efficacement au rythme des besoins.

A la fin de notre travail, nous devons mettre en place une solution qui permet :
- Monitoring en temps-réel.
- Créer et envoyer une notification d'alerte.
- créer des tableau de bord.

- Identifier les problèmes de sécurité dès que possible.
- centraliser,analyser et visualiser les sources de données pour vérifier les menace.

3.9 Conclusion

Ce chapitre fait l'objet de la présentation de l'entreprise et son environnement.L'étude du système réseau de l'entreprise est une étape primordiale pour protéger et faire face aux problèmes et menaces liés à la surveillance du réseau informatique dont le GROUPE IFRI . Le chapitre suivant sera consacré sur l'implémentation de logiciel SPLUNK tout en expliquant les différents cas d'utilisation qu'on y trouve : récupérations des données, créations des visualisations ,des tableaux de bord et des alertes.

Chapitre 4

Mise en place de la solution proposée

4.1 Introduction

L'objectif principal de cette phase est de mettre en place la solution décrite dans le chapitre précédent aprés la conception de l'architecture adoptée. Pour ce faire, nous allons d'abord spécifier l'environnement de développement et définir les exigences pour le développement de Splunk entreprise. Nous décrirons ensuite les différentes étapes d'installation des outils utilisés et leur mise en œuvre. Enfin, nous montrerons les différentes interfaces à travers des tests pour vérifier l'efficacité et le bon fonctionnement de notre solution.

4.2 Présentation de l'environnement de travail

Dans cette section, nous allons présenter l'environnement de développement qui est constitué de deux parties, nommées environnement matériel et environnement logiciel.

Environnement matériel

Nous avons utilisé un ordinateur portable qui a les caractéristiques mentionner dans le tableau

Processeur	Inlel(R) Core(TM) i7-7500u CPU @ 2.70GHz 2.90 GHz
Mémoire RAM	16,00GO
Type du Système	Système d'exploitation 64bits
Système d'exploitation	Windows 10
type de disque	HDD de 1 tb et SSD de 500 gb

Tableau 4.1 – Caractéristiques techniques

Environnement logiciel

- **GNS3 :** Gns3 est un émulateur d'équipement Cisco. Avec cet outil, nous pouvons charger un vrai Cisco IOS (Internetwork operating system) et l'utiliser pour une simulation complète sur un seul ordinateur. Il permet aux machines virtuelles de se connecter aux hyperviseurs Vmware ou Virtualbox et est utilisé par les ingénieurs réseaux du monde entier pour émuler, configurer, tester et dépanner les réseaux

virtuels et réels. Cela signifie que nous pouvons concevoir des réseaux simples et complexes et les simuler virtuellement. Il s'agit d'un logiciel gratuit qui s'exécute sur plusieurs plate-formes telles que Windows, Linux et MacOS. GNS3 est valide Cisco IOS, Juniper, MikroTik, Arista, Vyatta Net. réel.

- **VMware Workstation :** VMware Workstation est basé sur une virtualisation complète. Par conséquent, il est compatible avec la plupart des systèmes d'exploitation sans avoir besoin d'exigences matérielles particulières. VMware Workstation 6 prend également en charge la para-virtualisation lorsque les systèmes Linux invités utilisent un noyau étendu avec des fonctionnalités VMware VMI (Virtual Maching Interface). Cela améliorera les performances de Virtualisation [17].

- **Sophos :** Est un fabricant de matériel et de logiciels dans le domaine de la cybersécurité, dont parmi ses principaux produits XG firewall, anti-virus, anti-spyware, anti-spam, Contrôle d'accès au réseau, logiciel de cryptographie et prévention des pertes de données pour les appareils, serveurs pour la protection des e-mails et filtre pour les passerelles réseau [18].

- **Pfsense :** PfSense est une distribution open source de pare-feu basée sur FreeBSD qui fournit une plateforme de routage et de pare-feu flexible et puissante. La polyvalence de pfSense nous offre un large éventail d'options de configuration qui, par rapport à d'autres offres, rend la détermination des exigences un peu plus difficile et beaucoup plus importante.

- **Ubuntu :** Ubuntu est une distribution de Linux plus conviviale avec l'utilisateur , la distribution bureautique Ubuntu. Sa facilité d'installation et ses mécanismes de mise à jour montrent un haut niveau de maturation et de simplification, similaire à des produits de la concurrence du monde propriétaire, est bien connue en termes de sécurité et optimisation de ressources. [19]

4.3 Architecture adoptée

Notre architecture est composée de quatre (4) site . Nous avons installé tous les équipements nécessaires au niveau de chaque site .Après l'installation et la configuration de toute les équipes et le bon fonctionnement de architecture nous avons commencé la mise en place de la solutions splunk.
Sur le serveur Windows 10 qui ce trouve au niveau de site Ifri nous avons installé notre application Splunk Entreprise pour puisse récupérer les logos.Au niveau de sites Z3 et GP on à installé universel Forwarder sur deux (2) machine Ubuntu et Windows serveur 2022 (les deux machine sont considérée comme des machines clients).

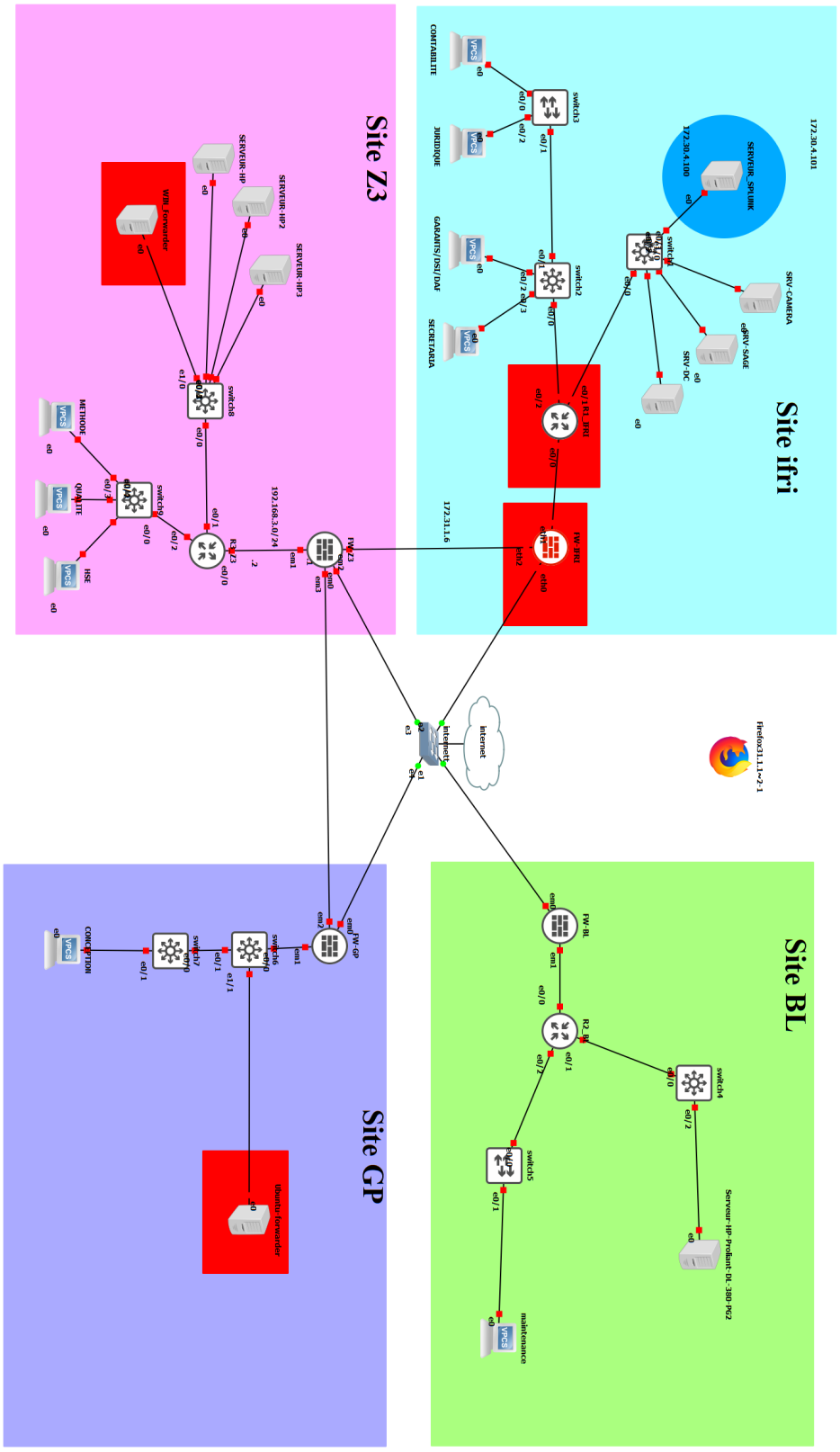

FIGURE 4.1 – Architecture adoptée

4.4 Tableaux d'adressage

Ces tableaux présentés les tableaux d'adressage pour chaque équipement de chaque site.

Site IFRI

	Interfaces	Adresses /Masques	Descriptions	Pasreils
Sophos	Eth0	wan	FW_IFRI->internet	
	Eth1	192.168.2.0/24	FW_IFRI->R1_IFRI	192.168.2.1
	Eth2	172.31.1.4/31	FW_IFRI->FW_Z3	172.31.1.1
R1_IFRI	e0/0	192.168.2.0/24	R1_IFRI->FW_IFRI	192.168.2.1
	e0/1	172.30.4.0/24	R1_IFRI->switch1	172.30.4.1
	e0/2	172.30.3.0/24	R1_IFRI->switch2	172.30.3.1
Switch1	e0/0	DHCP	switch1->R1_IFRI	172.30.4.1
	e0/1	DHCP	SRV-DC	172.30.4.1
	e0/2	DHCP	SRV-SAGE	172.30.4.1
	e0/3	DHCP	SRV-CAMERA	172.30.4.1
	e1/0	172.30.4.100/24	SERVEUR_SPLUNK	172.30.4.1
Switch2	e0/0	DHCP	switch1> R1_IFRI	172.30.3.1
	e0/1	DHCP	Switch2->switch3	172.30.3.1
	e0/2	DHCP	GARANTS/DSI/DAF	172.30.3.1
	e0/3	DHCP	GARANTS/DSI/DAF	172.30.3.1
Switch3	e0/0	DHCP	COMTABILITE	172.30.3.1
	e0/1	DHCP	Switch2->switch3	172.30.3.1
	e0/2	DHCP	JURIDIQUE	172.30.3.1

Tableau 4.2 – Adressage de site IFRI

Site Z3

	Interfaces	Adresse /Masque	Descriptions	Pasreil
Pfsense	em0	wan		
	Em1	192.168.3.0/24	FW_Z3->R3_Z3	192.168.3.1
	Em2	172.31.1.4/31	FW_Z3->FW-IFRI	172.31.1.1
	Em3	172.31.1.0/30	FW_Z3->FW-GP	172.31.1.1
R3_Z3	e0/0	192.168.3.0/24	R2_Z3->FW_IFRI	192.168.2.1
	e0/1	172.30.2.0/24	R2_Z3->switch8	172.30.4.1
	e0/2	172.30.1.0/24	R2_Z3->switch9	172.30.3.1
Switch8	e0/0	DHCP	Switch8->R3_Z3	172.30.2.1
	e0/1	DHCP	SERVEUR-HP2	172.30.2.1
	e0/2	DHCP	SERVEUR-HP	172.30.2.1
	e0/3	DHCP	SERVEUR-HP3	172.30.2.1
	e1/0	172.30.3.100/24	WIN_Forwarder	172.30.2.1
Switch9	e0/0	DHCP	Switch9> R3_Z3	172.30.1.1
	e0/1	DHCP	HSE	172.30.1.1
	e0/2	DHCP	QUALITE	172.30.1.1
	e0/3	DHCP	METHODE	172.30.1.1

Tableau 4.3 – Adressage de site Z3

Site BL

	Interfaces	Adresse /Masque	Descriptions	Pasreil
Pfsense	em0	wan	FW_BL->internet	
	Em1	192.168.1.0/24	FW_BL->R2_BL	192.168.1.1
R2_BL	e0/0	192.168.1.0/24	R2_BL->FW_BL	192.168.1.1
	e0/1	172.30.5.0/24	R2_Z3->switch4	172.30.5.1
	e0/2	172.30.6.0/24	R2_Z3->switch5	172.30.6.1
Switch4	e0/0	DHCP	Switch4->R2_BL	172.30.5.1
	e0/1	DHCP	Proliant-DL-380-PG2	172.30.5.1
Switch5	e0/0	DHCP	Switch5> R2_BL	172.30.6.1
	e0/1	DHCP	maintenance	172.30.6.1

Tableau 4.4 – Adressage de site BL

Site GP

	Interfaces	Adresse /Masque	Descriptions	Pasreil
Pfsense	em0	wan	FW_GP->internet	
	em1	172.30.7.0/24	FW_GP->switch6	192.168.7.1
	em2	172.31.1.0/30	FW_GP->FW_Z3	172.31.1.1
Switch6	e0/0	DHCP	Switch6-> FW_GP	172.30.7.1
	e0/1	DHCP	Switch6_switch7	172.30.7.1
	E1/1	172.30.7.100/24	Ubuntu_forwarder	172.30.7.1
Switch7	e0/0	172.30.7.0	Switch7> switch6	172.30.7.1
	e0/1	DHCP	CONCEPTION	172.30.7.1

Tableau 4.5 – Adressage de site GP

4.5 Installation des logiciels

Installation de GNS3

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes illustrées dans la figure 4.2.

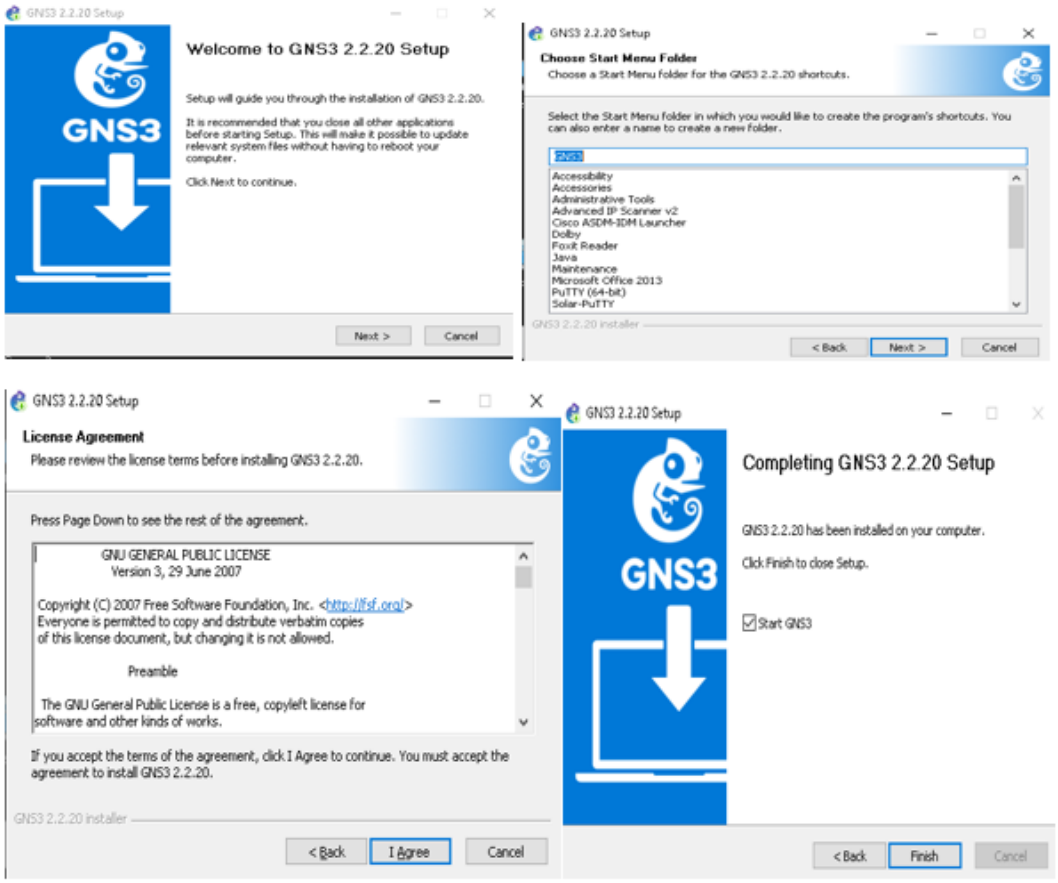

FIGURE 4.2 – Installation de GNS3

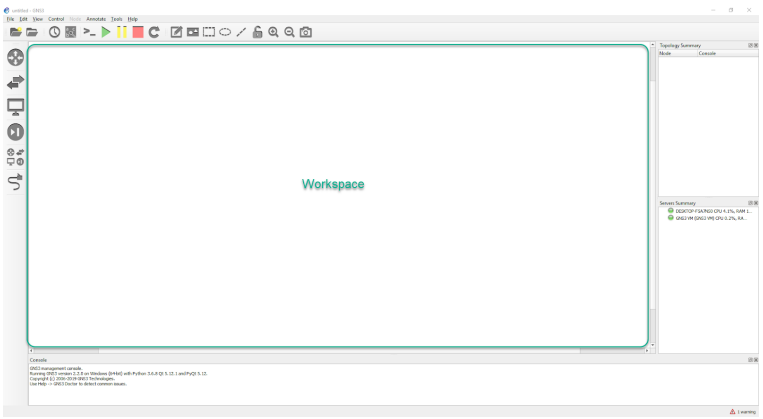

FIGURE 4.3 – Interface de GNS3

Installation k de VMware Worstation

Afin de créer les machines utilisateurs virtuelles au sein du même ordianteur, nous sommes appelés à installer VMware Workstation en suivant les étapes indiqué dans la figure 4.4 et la configuration on suivant les étapes comme la figure 4.5 :

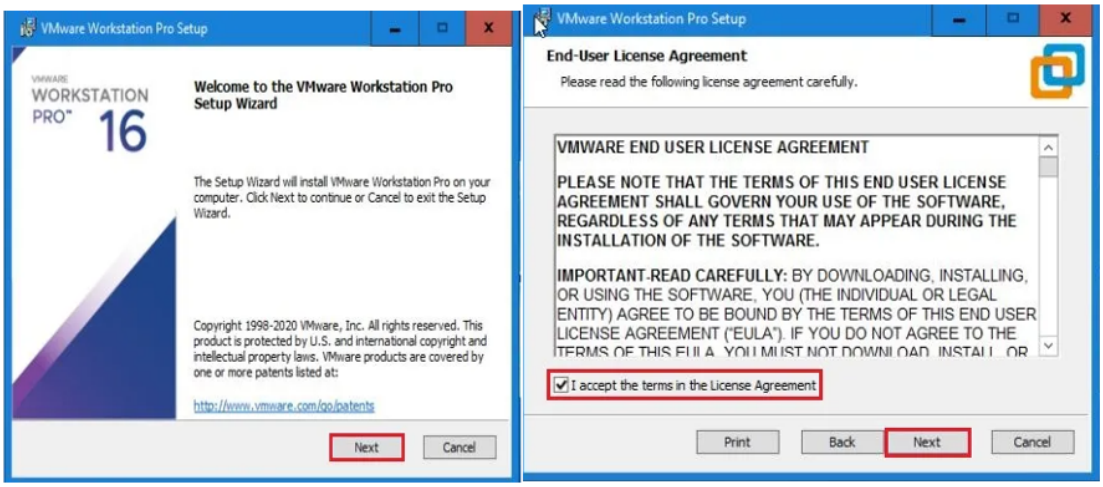

FIGURE 4.4 – Installation VMware Workstation

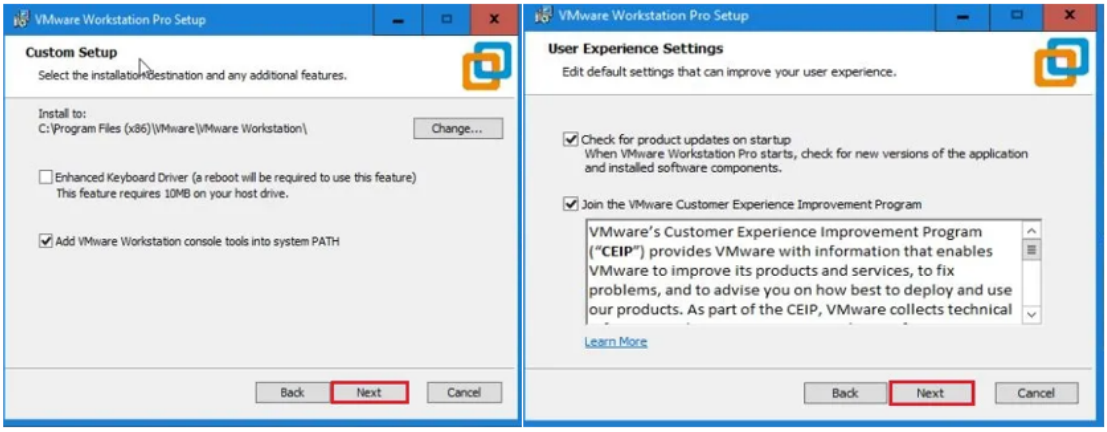

FIGURE 4.5 – Configuration VMware Workstation

4.6 Création des machines et serveur virtuelles

Installation du Windows 10

Nous avons créé une machine après avoir ajouté l'image de Windows 10 sur VMware avec les caractéristiques cités dans la figure 4.6 :

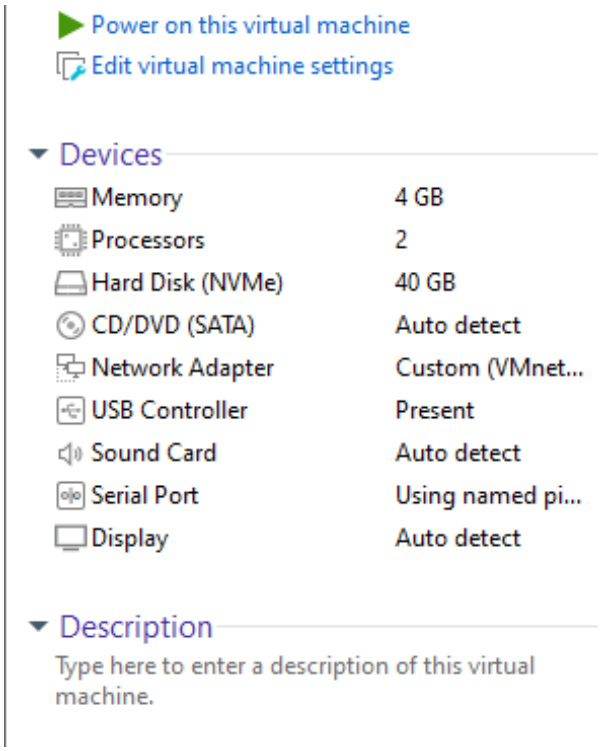

FIGURE 4.6 – Caractéristiques de win10

Installation de Windows Server 2022

Dans cette partie, nous allons voir les différentes étapes d'installations de Windows Server 2022 comme le montre la figure 4.7

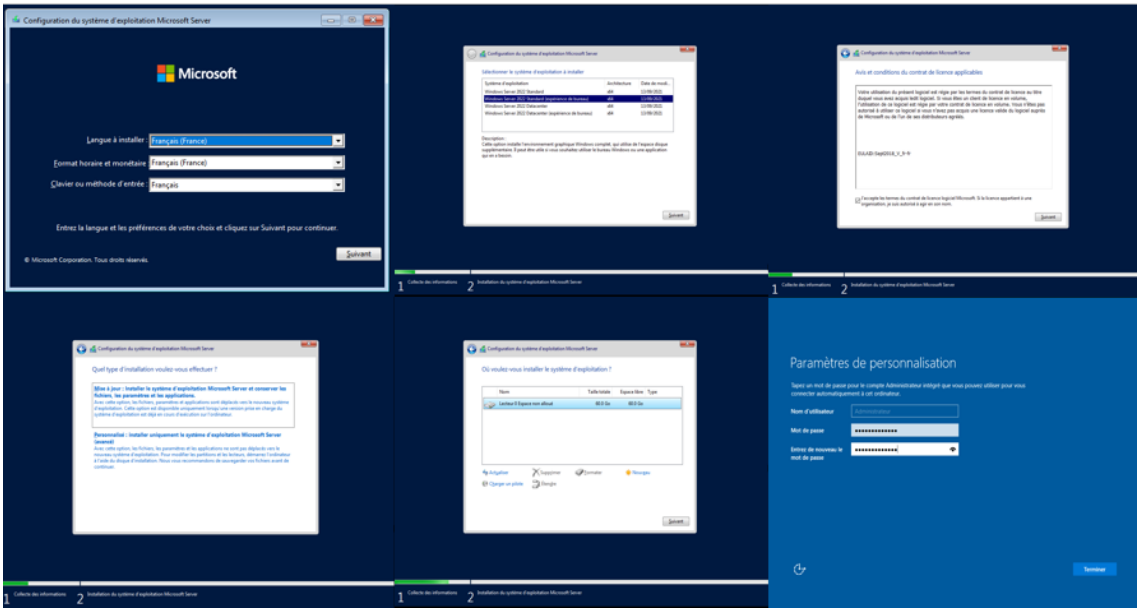

FIGURE 4.7 – Installation de Windows server 2022

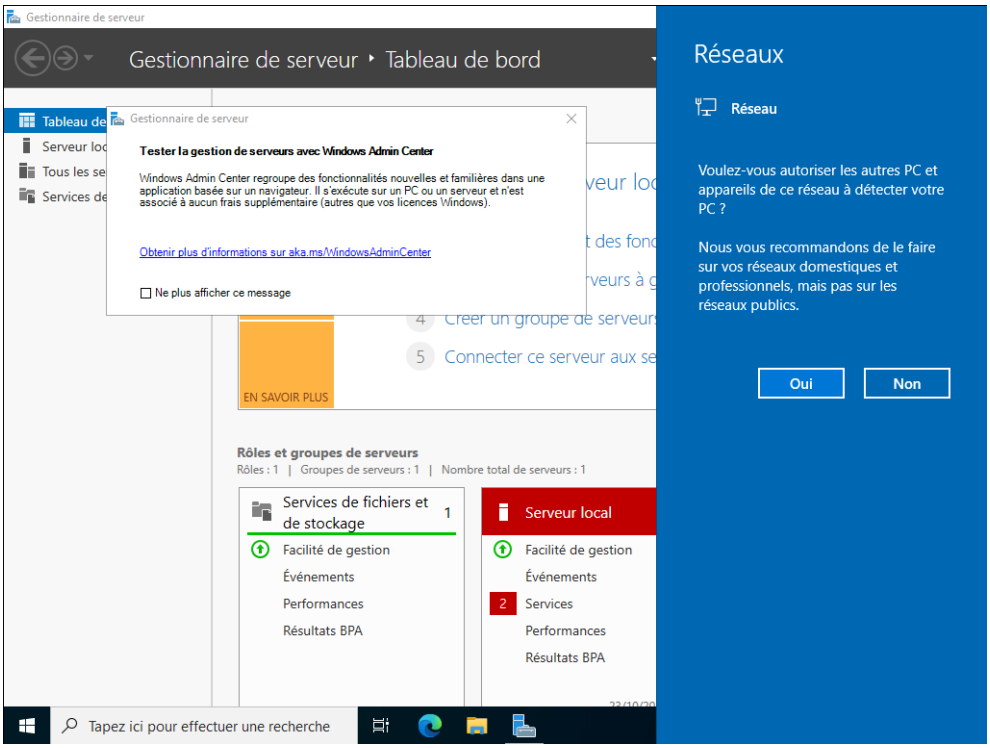

FIGURE 4.8 – Fin d'nstallation de Windows server 2022

Installation de l'Active Directory

Il sécurise gratuitement de nombreux services accessibles uniquement depuis les ordinateurs de l'entreprise. Les étapes sont les suivantes :

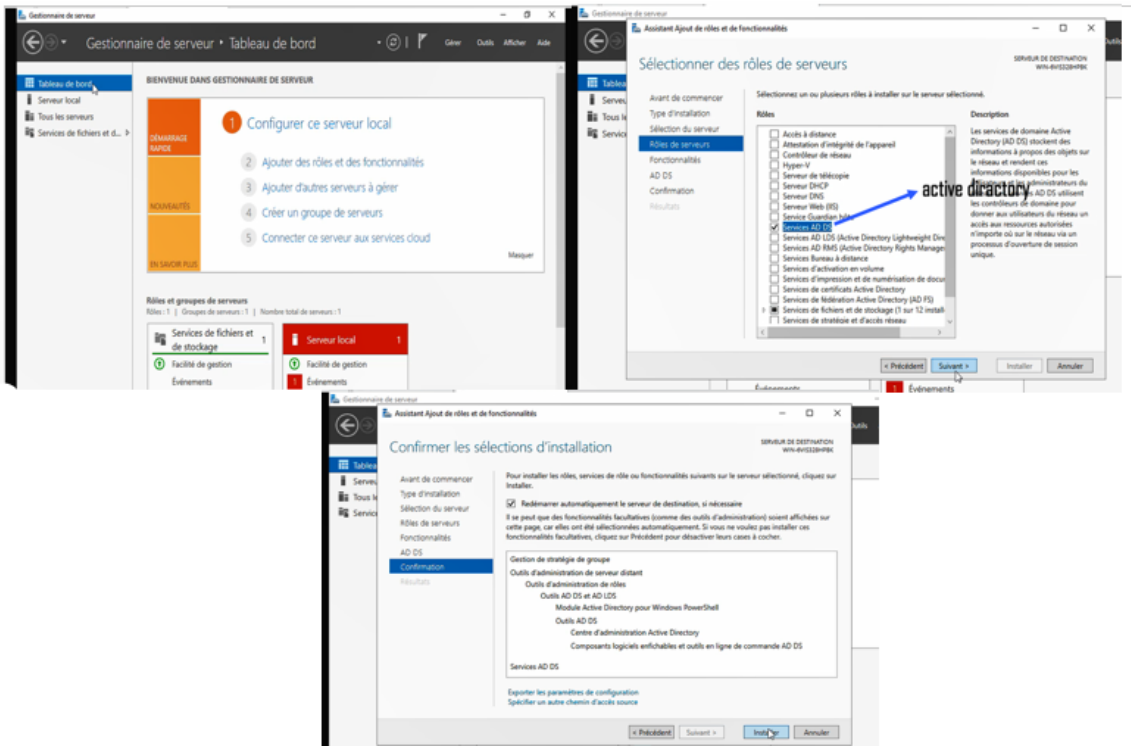

FIGURE 4.9 – Installation de Active Directory

4.7 Installation et configuration des firewalls

Installation de pfSense

Pour installer pfSense, nous avons suivi les étapes suivantes :

- Démarrer la VM et accepter la licence
- Installer pfSense
- Redémarer pfSense

Comme nous le voyons sur les figures 4.10 et 4.11

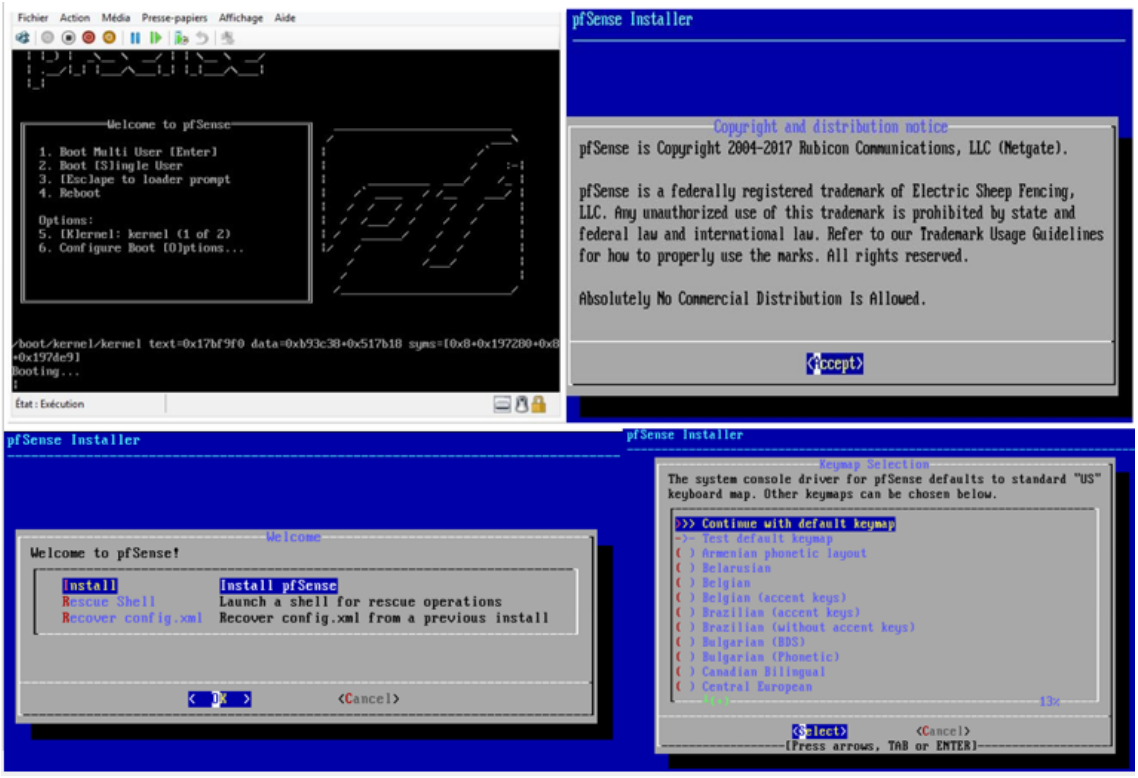

FIGURE 4.10 – Installation de pfSense

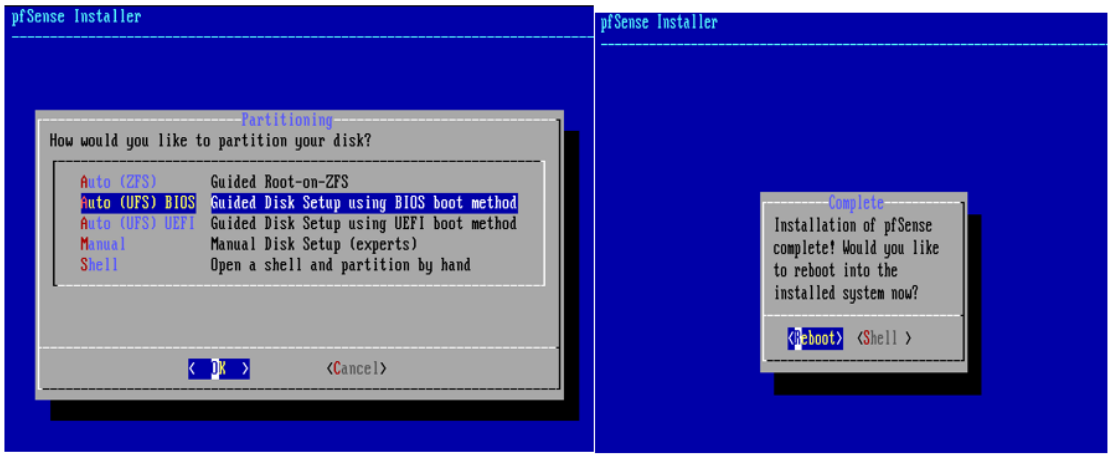

FIGURE 4.11 – Fin d'installation de pfSense

Configuration de Pfsense

Cette étape consiste à configurer le pare-feu pfSense que nous avons déjà installé où la configuration de la page d'authentification est nécessaire.
Tout d'abord, il faut se rendre sur le site du pare-feu et insérer quelques information sur l'entreprise suivi du mot de passe avec lequel accédera l'administrateur à Pfsense comme elles les prisent les figures 4.12 et 4.13

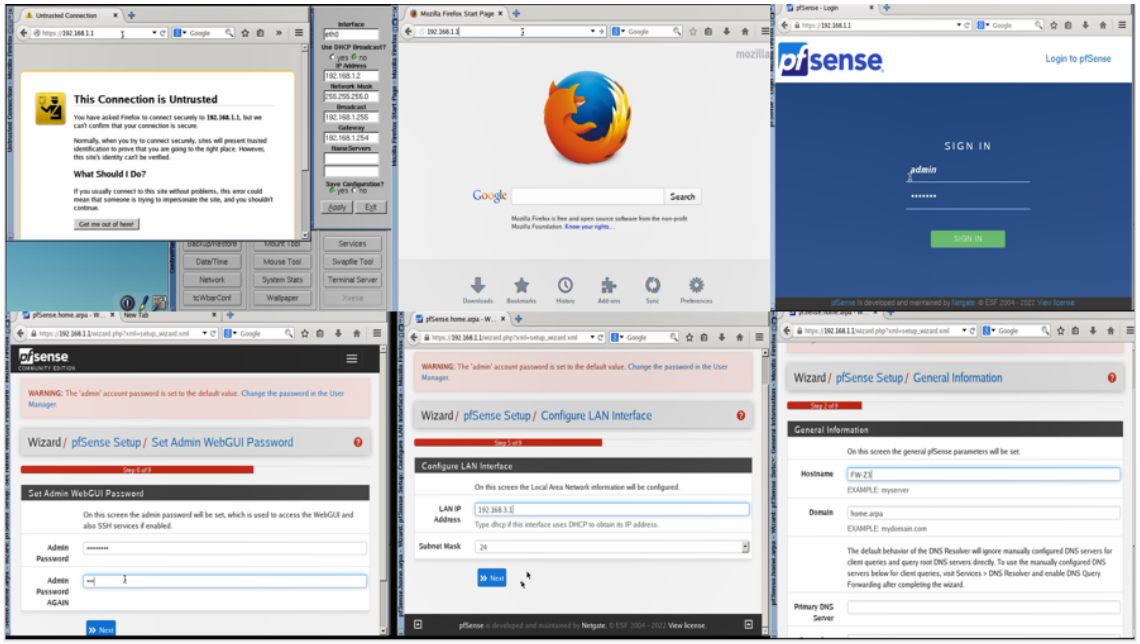

FIGURE 4.12 – Création du compte Pfsense

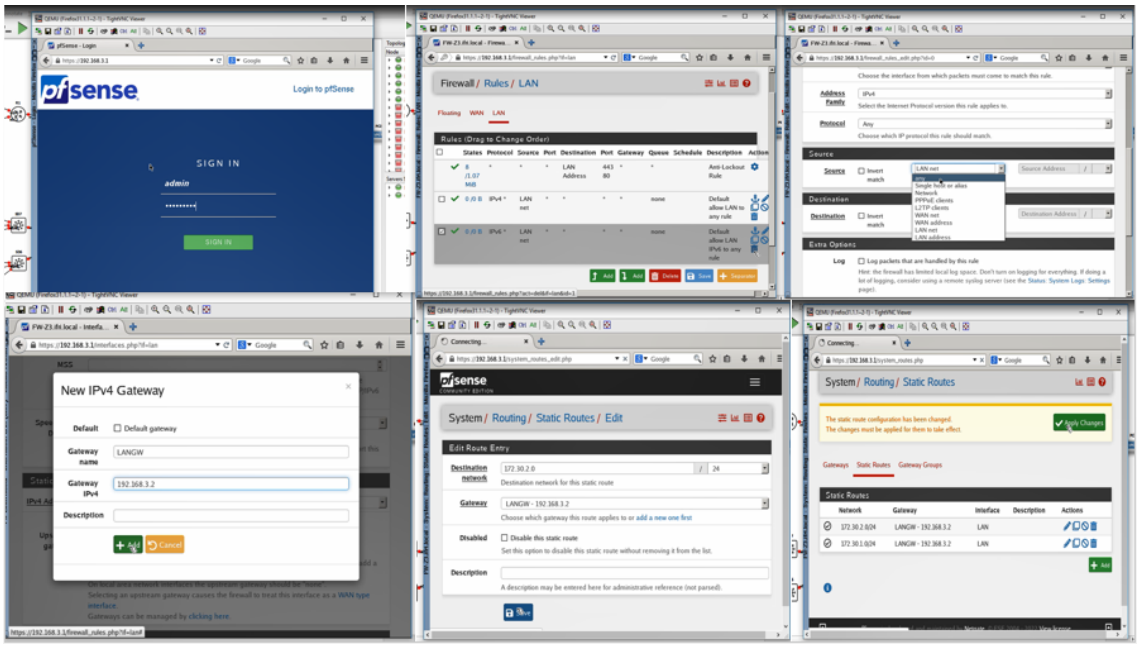

FIGURE 4.13 – Configuration de Pfsense

Installation de Sophos Les étapes d'installation de Sophos sont regroupées dans la figure 4.14.

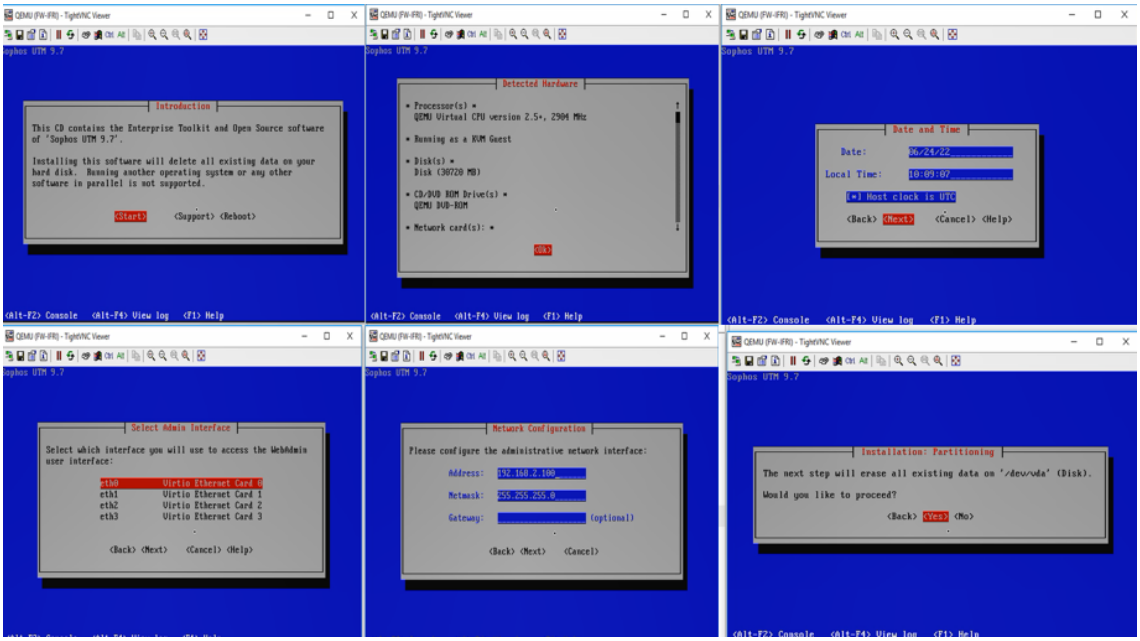

FIGURE 4.14 – Installation de Sophos

Configuration de Sophos

L'étape suivante consiste à configurer un pare-feu Sophos déjà installé ou à configurer une page d'authentification. Tout d'abord, vous devez vous rendre sur la page du pare-feu. Saisissez les informations sur l'entreprise suivies du mot de passe permettant à l'administrateur d'accéder à Sophos. Tout les étapes sont clairement présenté dans les figures 4.15 et 4.16

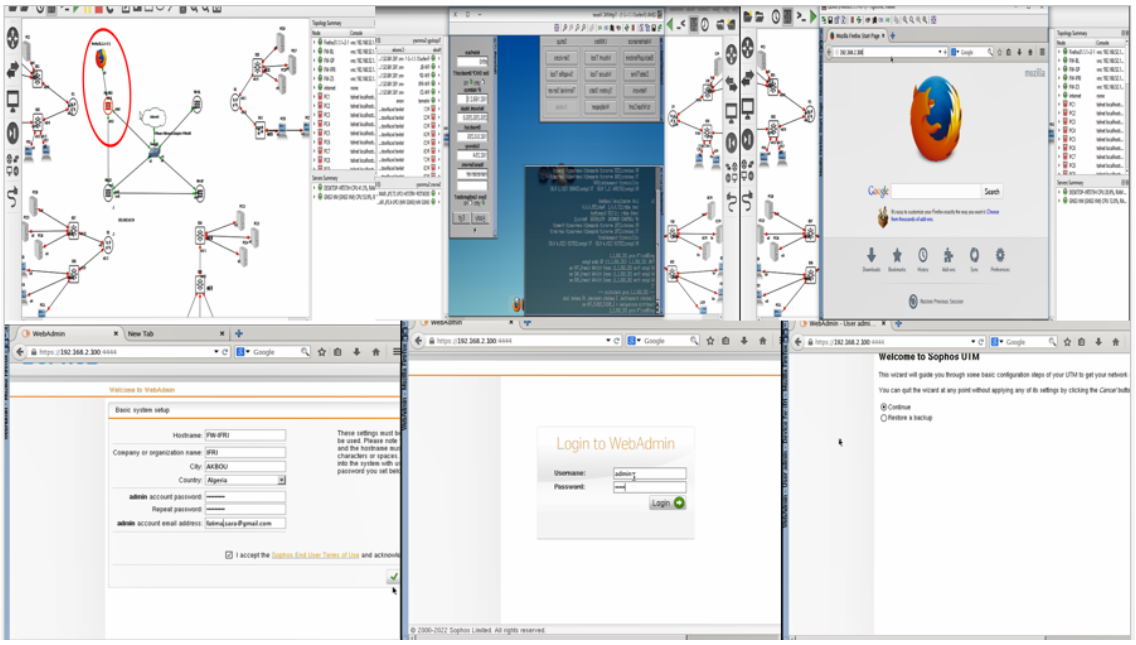

FIGURE 4.15 – Création de compte Sophos

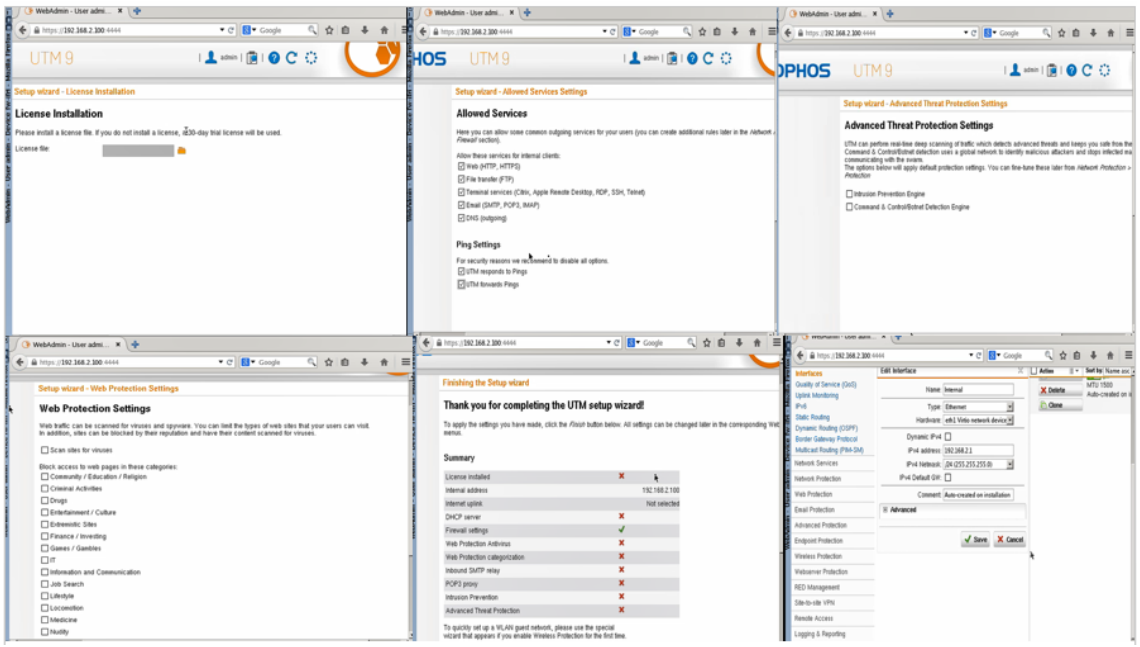

FIGURE 4.16 – Configuration de Sophos

4.8 Mise en œuvre de la solution

4.8.1 Installation Splunk entreprise

Installation sous Windows serveur

Afin d'installer Splunk sur un serveur Windows 10, nous avons :

- créé un compte et téléchargé le programme d'installation de Splunk à partir de la page officielle "Splunk.com". Le programme d'installation de Windows est un fichier MSI.
- double-cliqué sur le fichier splunk.msi pour démarrer l'installation. Le programme s'exécute et affiche le panneau du programme d'installation de Splunk Enterprise .
- Avant de cliquer sur "suivant", il faut d'abord cocher la case "Cochez cette case pour accepter le contrat de licence". Cela active les boutons "Personnaliser l'installation" et "Suivant" comme illustré dans la figure 4.17

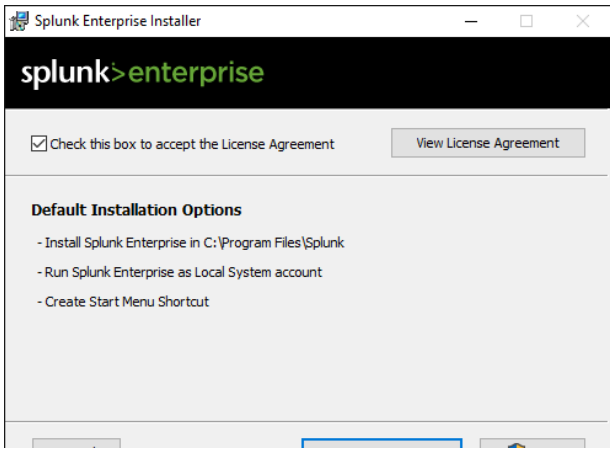

FIGURE 4.17 – Installer splunk

Le programme d'installation affiche le panneau "Informations de connexion", nous spécifions un nom d'utilisateur et un mot de passe avant de cliquer sur "suivant ".Figure 4.18

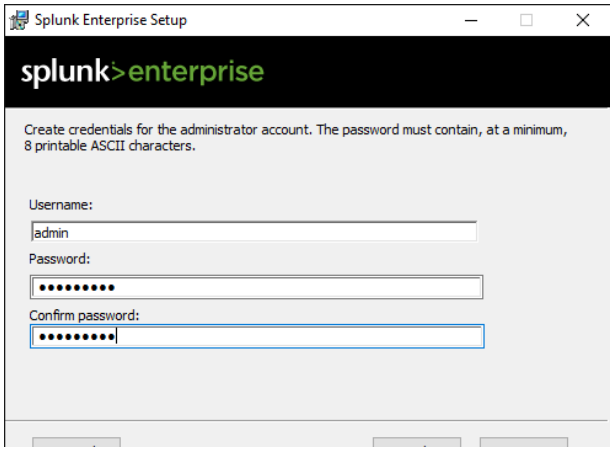

FIGURE 4.18 – Création d'un compte administrateur

Ces informations seront utilisées ultérieurement pour accéder à la plate-forme SPLUNK une fois l'installation terminée.figure 4.19

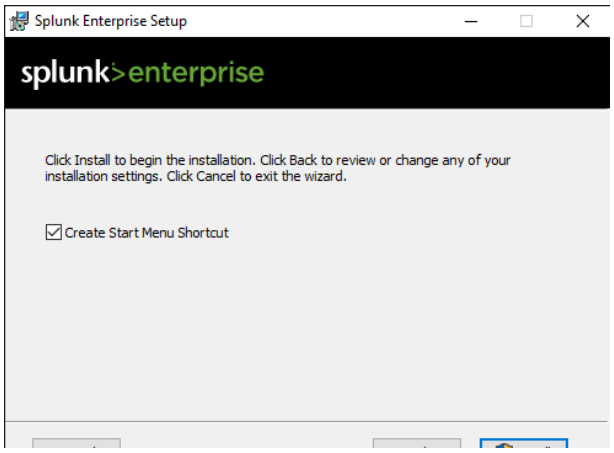

FIGURE 4.19 – panneau récapitulatif de l'installation.

— Cliquons sur "Installer" pour procéder à l'installation. Le programme s'exécute, installe le logiciel et affiche la fenêtre Installation terminée.
— Enfin, cliqué sur terminer. Splunk Enterprise démarre et se lance dans un navigateur.Figure

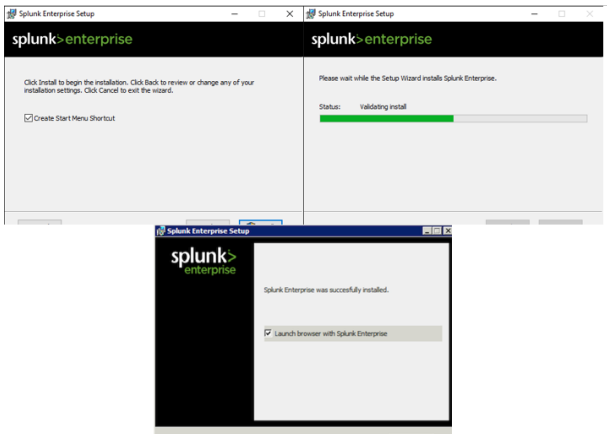

FIGURE 4.20 – Étape d'instalation de splunk

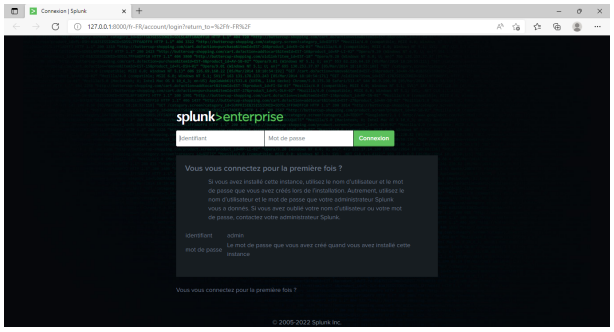

FIGURE 4.21 – Interface utilisateur de splunk

Un nom d'utilisateur et un mot de passe sont requis pour accéder à l'interface de Splunk. La capture d'écran 4.22 montre la page d'accueil de Splunk Enterprise.

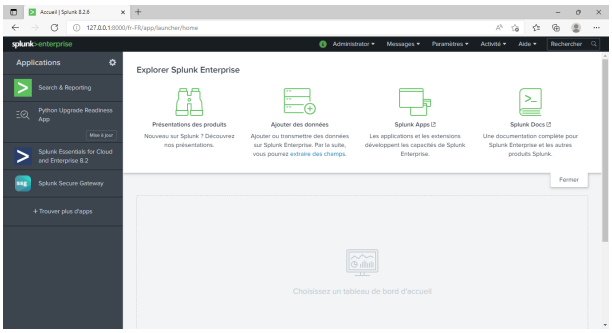

FIGURE 4.22 – L'interface de Splunk

Installation sous Linux

Il faut d'abord créer un compte Splunk et télécharger le logiciel Splunk Free sur leur site officiel en suivant le lien indiqué sur la figure 4.23

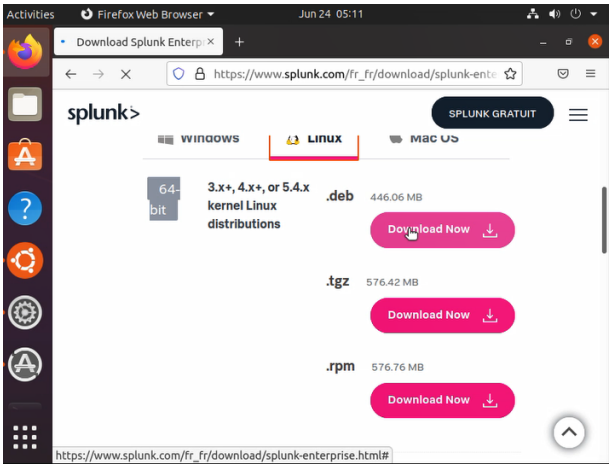

FIGURE 4.23 – Fichier à télécharger

Une fois le fichier téléchargé, nous avons exécuté la commande "sudo dpkg" pour installer le serveur Splunk, comme illustré sur la figure 4.24

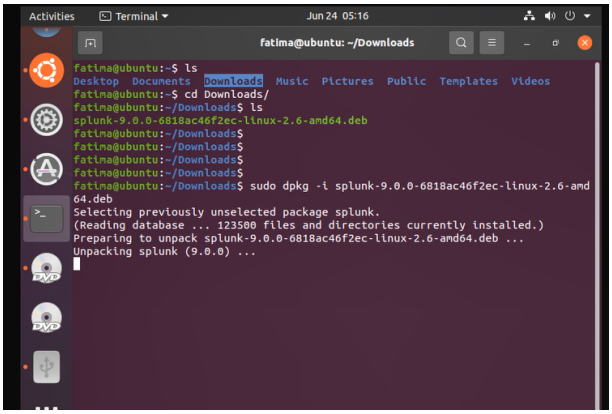

FIGURE 4.24 – Installer le serveur Splunk

L'exécutable de Splunk est lancé avec les arguments ci-dessous.

Le service Splunk est ensuite redémarré avec la commande "restart", puis un nom et un mot de passe sont donnés à Splunk.

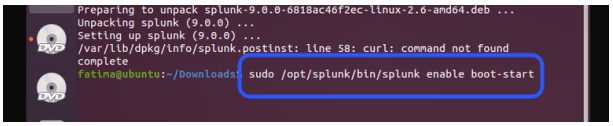

FIGURE 4.25 – Installation

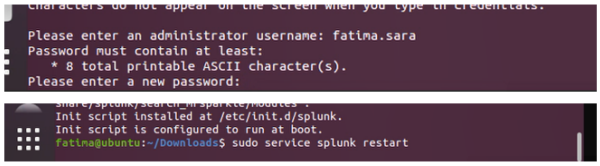

FIGURE 4.26 – Installation

Depuis le navigateur, Splunk est accessible à l'adresse 172.0.0.1 :8000. L'interface d'authentification représentée par la figure 4.27 s'affichera.

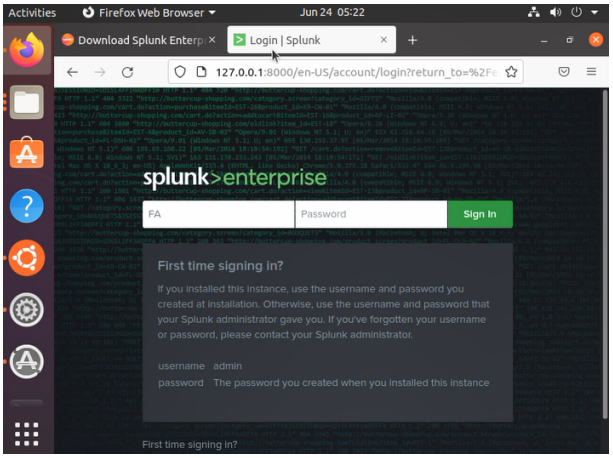

FIGURE 4.27 – Fin de l'installation

4.8.2 Récupération des logs

Pour collecter les fichiers logs depuis un ordinateur distant, il faut configurer l'expéditeur et le destinataire. Ce dernier est une instance Splunk qui reçoit les données.

La récupération des données sur Windows Server 2022 se fait en suivant les trois étapes suivantes :

a) **Autoriser la réception via la console Web :** Pour configurer la transmission, comme illustré sur la figure 4.28, nous avons :
- cliqué sur "Paramètres" et sélectionné "Transmission et réception".
- sélectionné "Configurer la transmission" et cliqué sur "Ajouter nouveau".
- introduit le nom d'hôte ou l'adresse IP du serveur de déploiement et le port 9997.

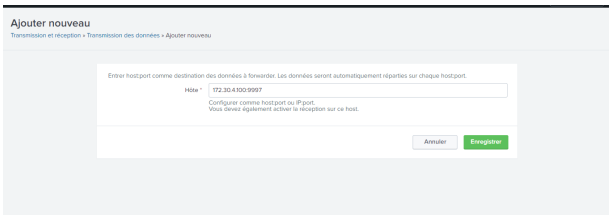

FIGURE 4.28 – Configuration de Splunk Heavyweight Forwarder

Pour configurer la réception, comme le montre la figure 4.29, nous avons :

- cliqué sur "Paramètres" et sélectionné "Transmission et réception".
- sélectionné "Configurer la réception" puis cliqué sur "Ajouter nouveau".
- tapé 9997 Dans le champs "Écouter ce port". Si nous utilisons un port différent, nous devons le spécifié au niveau du forwarder.

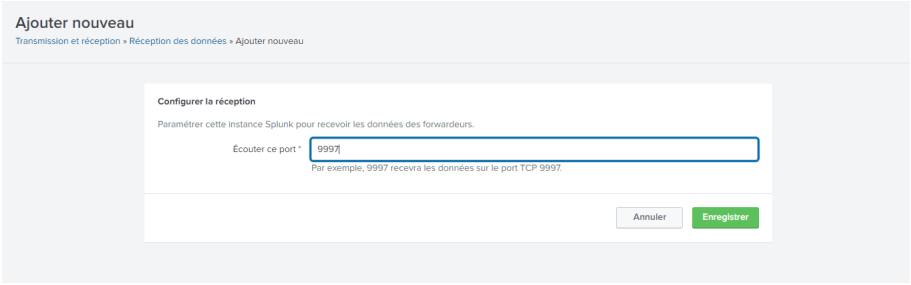

FIGURE 4.29 – Configurer la réception sur l'indexeur Splunk

b) **Configurer splunk universal forwarder :**
Le moyen le plus efficace de collecter les données à partir d'une machine distante est d'installer les redirecteurs universels, appelés Universal Forwarders . Pour ce faire, nous avons téléchargé l'image du forwarder et lancé le fichier MSI Universal Forwarder en acceptant le contrat de licence et en cliquant sur Suivant.

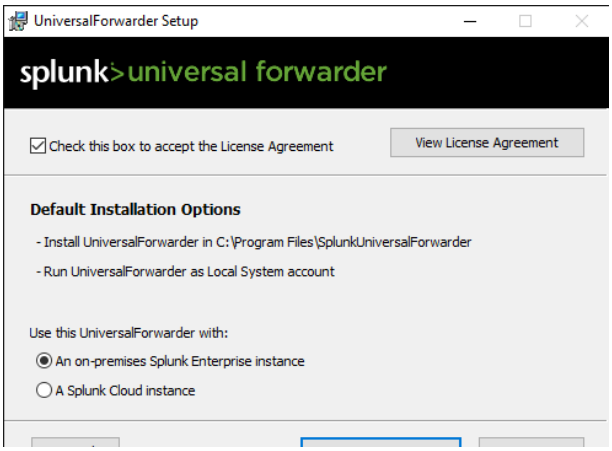

FIGURE 4.30 – Installer Splunk universal forwarder

Nous avons ensuite entré les informations demandées, comme dans la figure 4.31 pour créer un compte administrateur.

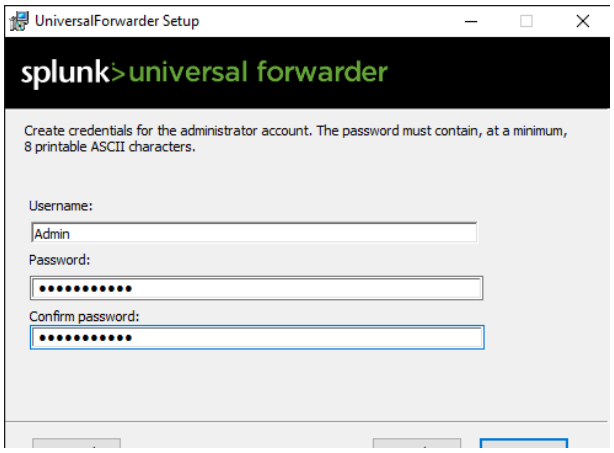

FIGURE 4.31 – Création d'un compte d'administrateur

Pour spécifier le serveur de déploiement, nous avons indiqué le nom du serveur Splunk ou son adresse ip. Par contre, le port est laissé à sa valeur par défaut comme nous voyons dans la figures 4.32

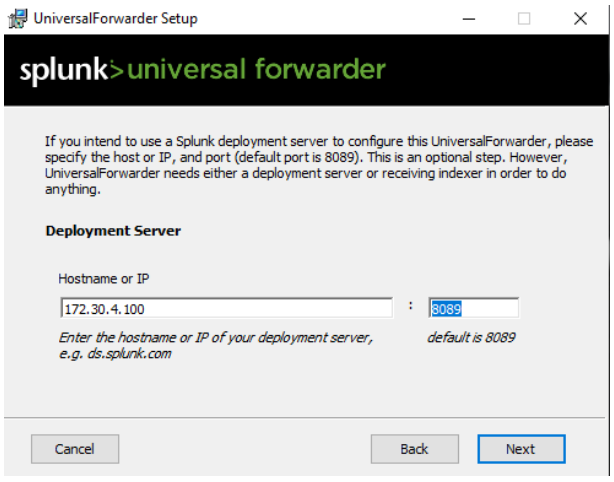

FIGURE 4.32 – Configurer déploiyment server

Pour spécifier l'indexeur Splunk, nous avons donné le nom ou l'adresse ip du serveur Splunk. Encore une fois, le port reste à sa valeur par défaut.Figure 4.33

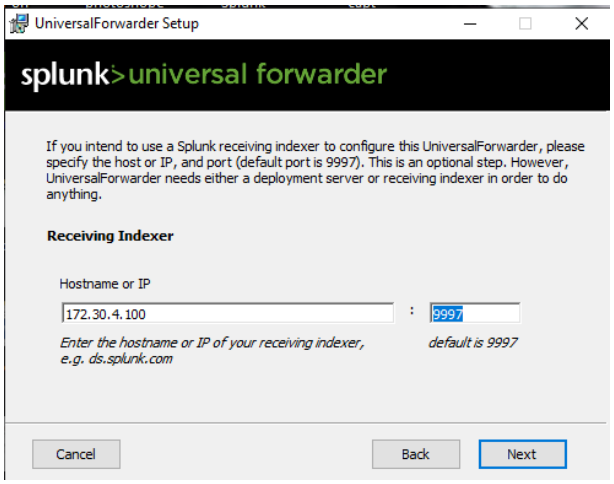

FIGURE 4.33 – Configurer l'écoute sur l'indexeur

Maintenant que l'installation de splunk universel forwerder est términée, la connectivité entre la machine distante (cliente) et le serveur splunk est assurée.

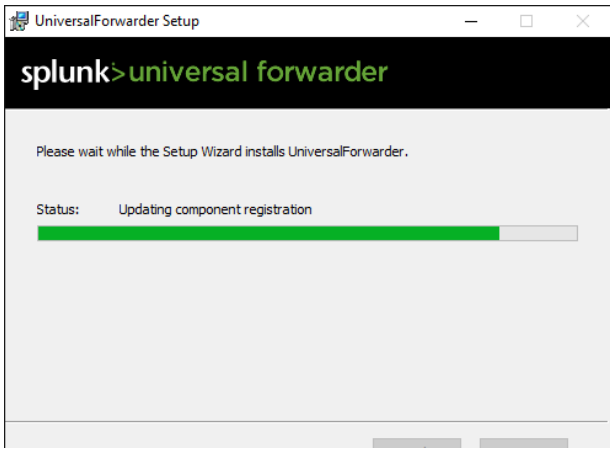

FIGURE 4.34 – Fin de l'instalation

c) **Collecte des logs**

Pour collecter les données journaux, nous avons sélectionné "Ajouter des données" dans "Paramètres", puis cliqué sur "Transmettre", comme représenté sur la figure 4.35

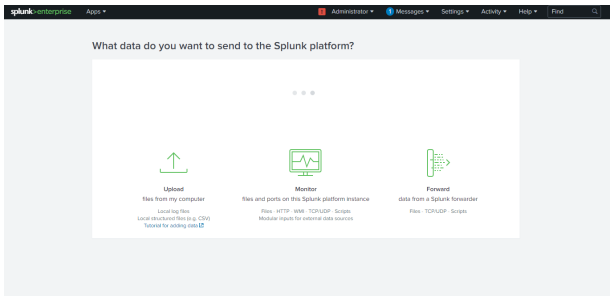

FIGURE 4.35 – Forward

Parmi la liste des machines clientes qui s'affichent, nous avons choisi celles dont nous voulions récupérer les logs, puis spécifié le nom de la classe serveur qui regroupe plusieurs hôtes, et enfin cliqué sur Suivant pour continuer la configuration comme elle le présent la figure 4.36

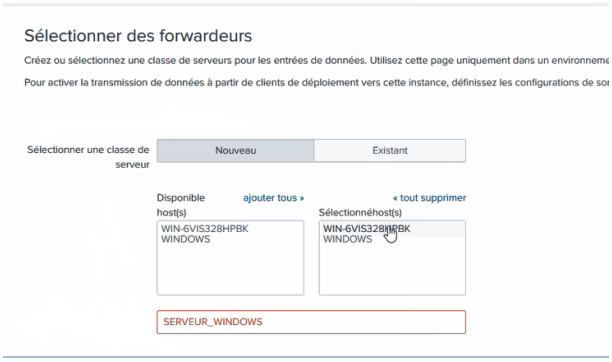

FIGURE 4.36 – Classe serveur

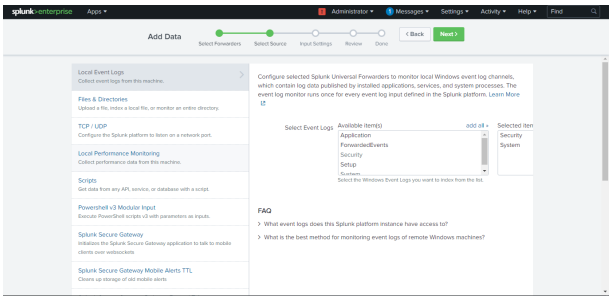

FIGURE 4.37 – Sélection des logs d'événements

Nous avons sélectionné un index pour organiser le stockage des données. Nous pouvons en créer autant que nous souhaitons pour diffèrent type de sources telles que Windows, Linux, Switchs et Firewall comme cité dans la figure 4.38

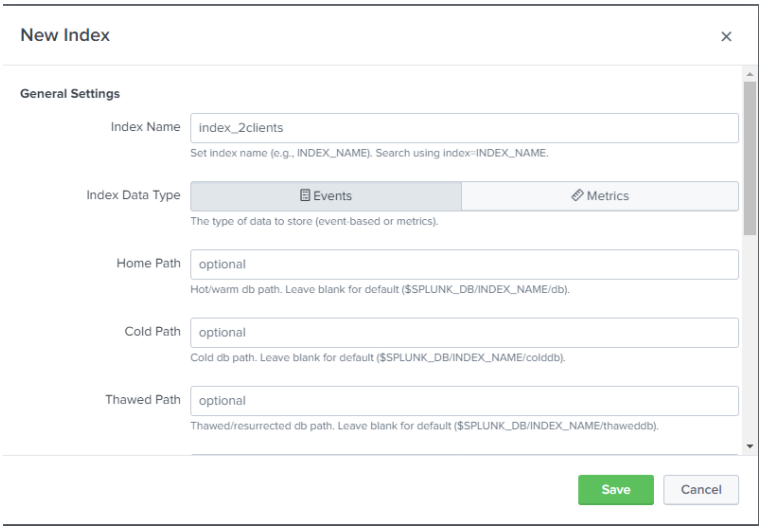

FIGURE 4.38 – Création d'un index

Le résumé des paramètres d'entrée s'affiche. En cliquant sur "Lancer la recherche", des logs devraient apparaître dans Splunk. Dans le cas contraire, nous devons redémarrer splunk pour que les modifications prennent effet comme la figure 4.39

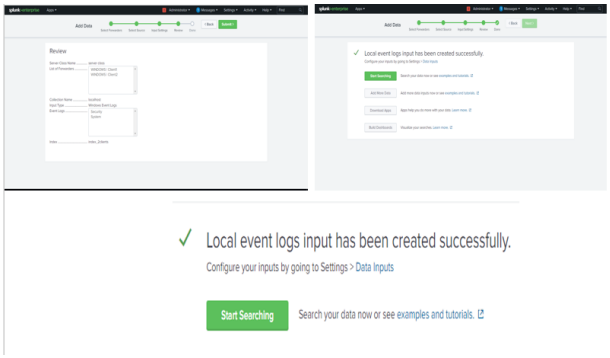

FIGURE 4.39 – Recherche des logs

Une fois les logs s'affichent dans Splunk, nous pouvons effectuer des traitements dessus.comme nous le voyons dans la figure 4.40

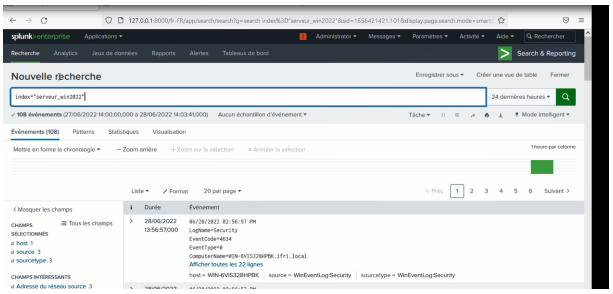

FIGURE 4.40 – Exporté des logs

4.8.3 Récupération des syslogs

Dans cette étape nous avons récupéré les logs d'un routeur cisco, pour cela nous avons suivie quatre étapes :

a) **Configuration le routeur pour l'envoi de syslog :**

— Nous avons effectué un choix de net de la machine splunk et effectue le port UDP 514 qui est le port par défaut.
— Nous avons aussi activé l'utilisation d'un mot de passe. figure 4.41

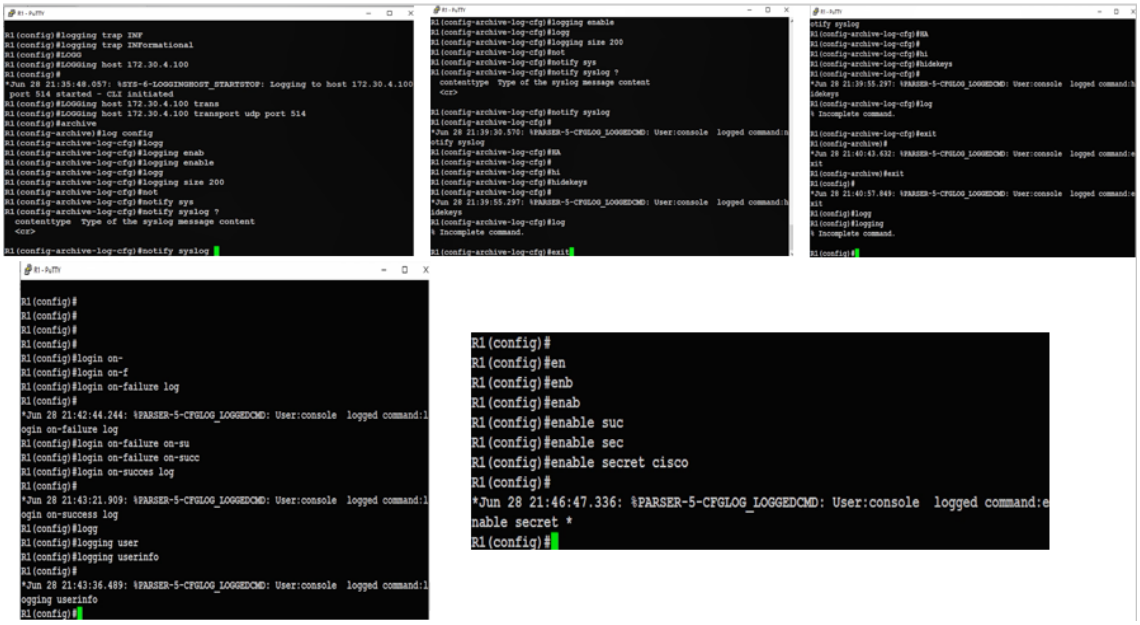

FIGURE 4.41 – L'indexation des Syslogs

b) **Créer une règle pour le trafic entrant**

Pour autoriser le trafic réseau entrant, nous avons utilisé le nœud pare-feu Windows et nous avons créé une règle entrante selon les étapes suivantes :

- Dans Paramètres avancés , nous avons cliqué sur "Règles entrantes" . Dans le volet Actions à droite,nous avons cliqué sur "Nouvelle règle".
- Nous avons coché sur "Ports locaux spécifiques" et effectué le port 514 et cliqué sur Suivant.
- Dans la page "Nom", nous avons saisi un nom et une description pour la règle créée, puis cliqué sur "Terminer".

c) **Cisco Networks Add-on for Splunk Enterprise**

C'est une application qui s'exécute sur la plate-forme Splunk et fournit des fonctionnalités spécifiques ,elle permet à l'administrateur du logiciel Splunk de mapper les événements des dispositifs Cisco.

Nous avons suivi ces étapes pour installer add-on cisco Cisco Network :

- Nous avons téléchargé add-on cisco Cisco Network depuis Splunkbase .
- Nous avons Installé l'application à partir du fichier .

d) **Configuration de la réception des Syslog sur Splunk**

Les syslogs d'un routeur par défaut écoutent sur le port 514,nous avons donc configuré Splunk afin qu'il récupère les syslogs d'un routeur Cisco

Voici les étape à suivre :

- Sur l'interface Web de Splunk, nous avons cliqué sur Paramètres, puis sur "Entrée des données".
- Sur la ligne UDP, nous avons cliqué sur "Ajouter nouveau".
- Nous avons sélectionné "Syslog UDP" et le port 514,Puis sélectionné un type de source.
- Dans Index, nous avons cliqué sur "Créer un nouvel Index" pour créer un index spécifique .

figure4.42

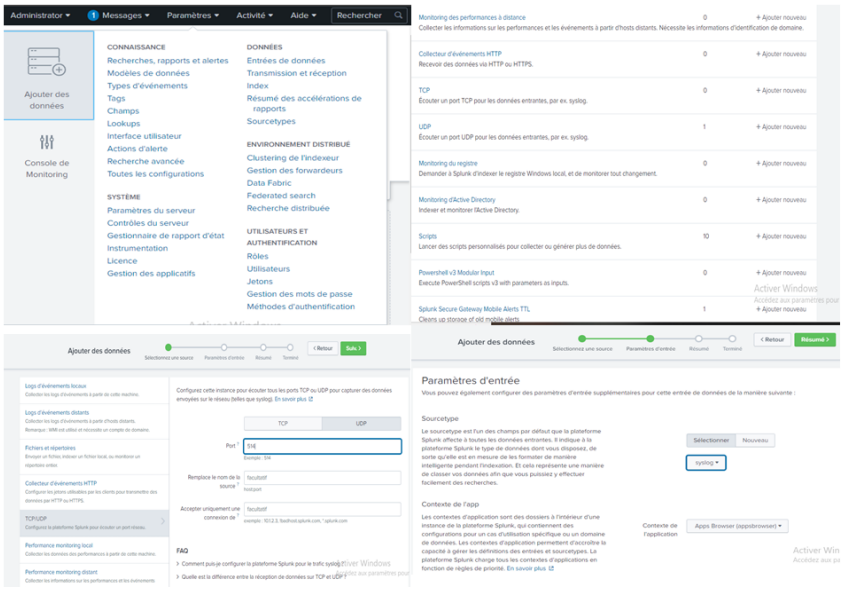

FIGURE 4.42 – Exporté des Syslogs

Le résumé des paramètres d'entrée s'affiche 4.43

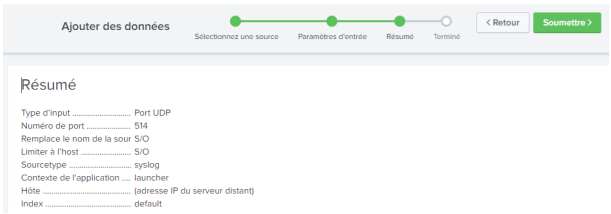

FIGURE 4.43 – Résumer des paramètres des logs

Nous avons cliqué sur "Lancer la recherche", les logs doivent déjà arriver dans Splunk. 4.44

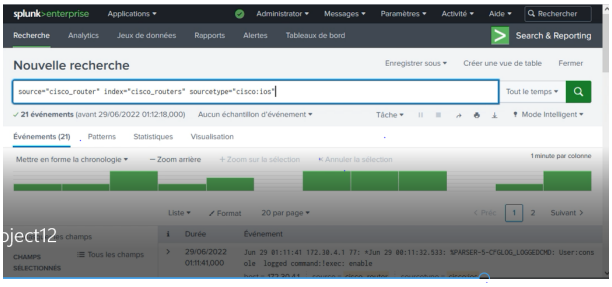

FIGURE 4.44 – Les logs de router

4.8.4 Récupération des logs d'un parfeu sophos

Nous devons créer une nouvelle entrée de données pour Sophos UTM. Pour cela nous devons créer un nouveau port TCP 8514.

Sur Splunk,nous avons également créé un nouveau type de source et un nouveau index pour ces données transmet-Sophos UTM.Figure 4.45

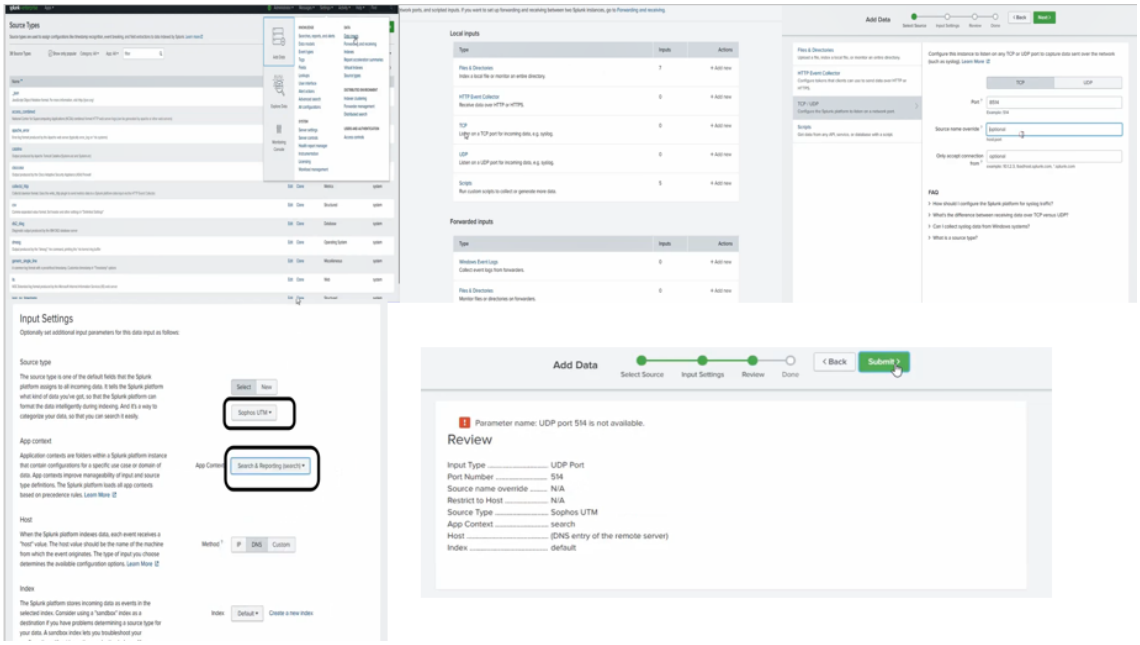

FIGURE 4.45 – Résumer des parametre des logs

Dans la page de configuration de syslog distant, nous avons défini un nouveau port tcp 8514 pour le serveur Splunk distant. Sophos UTM et transmit tous les journaux système au port distant 8514.figure4.46

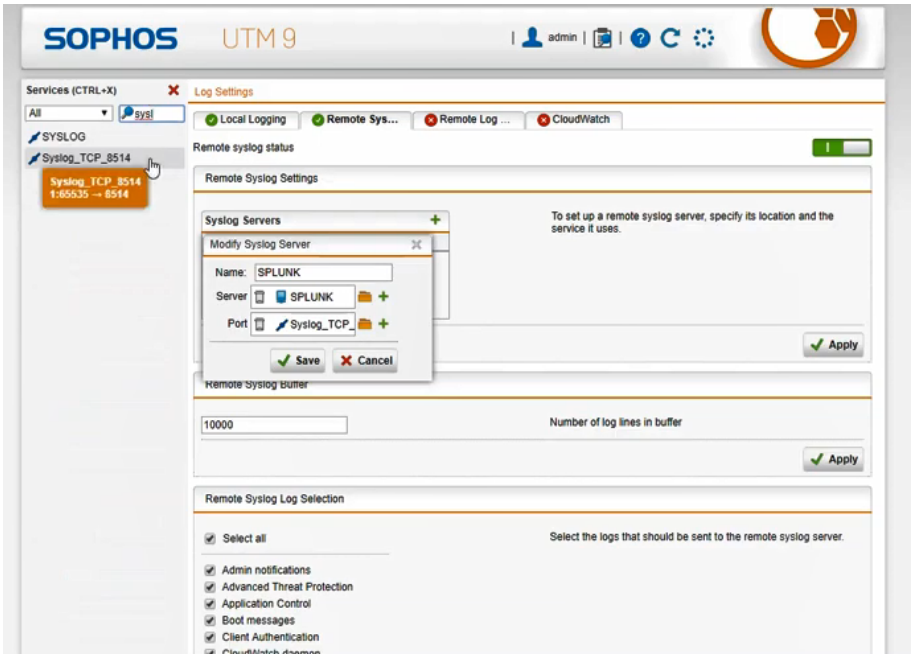

FIGURE 4.46 – Configuration Sophos

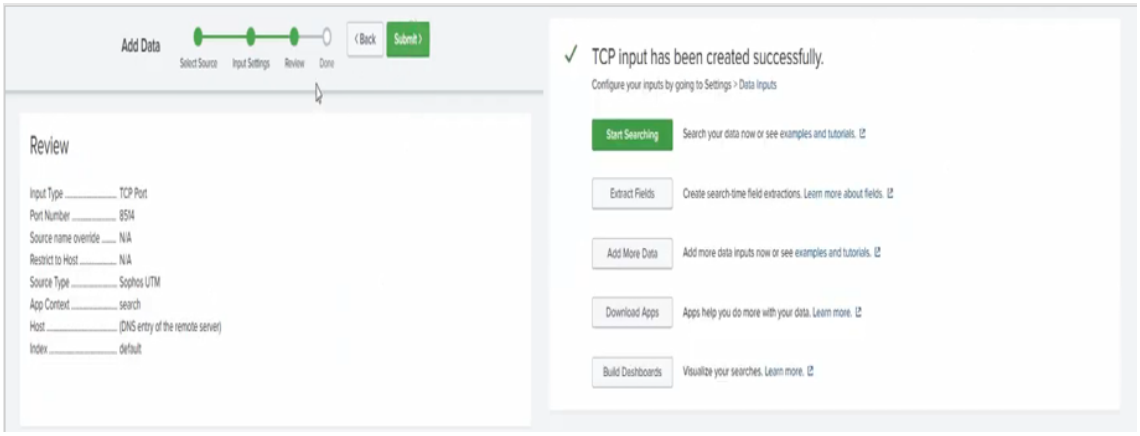

FIGURE 4.47 – Recherche des logs

Grâce à la recherche Figure 4.47, les journaux système d'UTM sont maintenant disponibles.Figure 4.48

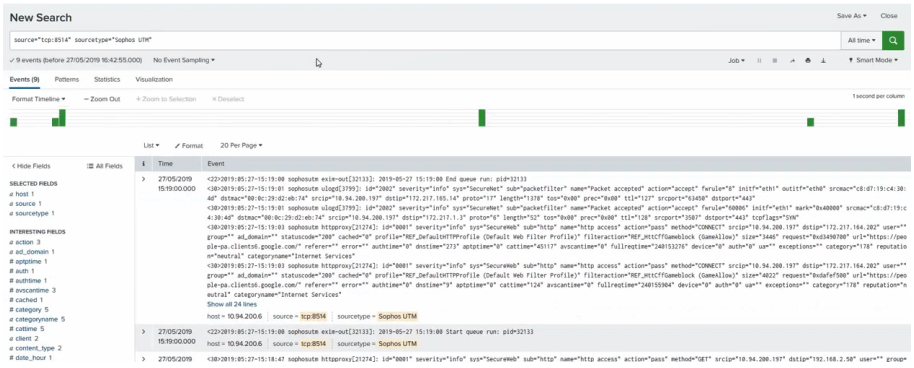

FIGURE 4.48 – Les logs de Sophos

4.8.5 Supervision

Les visualisations facilitent l'analyse et l'interrogation des données au cours des investigations et au sein des tableaux de bord et des rapports. Une bonne représentation graphique facilite considérablement l'interprétation des résultats d'analyse de vos données les plus complexes.

Création des tableux de bord

Nous avons ajouté nos résultats de recherche sous forme de volet à un nouveau tableau de bord ou à un tableau de bord existant, puis nous l'avons personnalisé.

— Dans Splunk, nous avons cliqué sur l'"app Search reporting".

— Dans l'onglet Recherche, nous avons saisi une recherche qui renverra les résultats que nous voulions afficher dans un tableau de bord.

exemple :

- SourceType="linux-secur" host=sevreur-linux source="linux-s-30DAY.log"|top ip Source limite=10
- SourceType="linux-secur" host=sevreur-linux source="linux-s-30DAY.log" |top stats cont (IPsource)

Nous avons choisi le volet du tableau de bord dans le menu contextuel.

— Nous avons effectué l'une des opérations suivantes :

- Nous avons séléctionné "Nouvea"u et configuré les réglages de notre tableau de bord.
- Nous avons séléctionné "existant" ,puis sélectionnez un tableau de bord existant.

— nous avons cliqué sur "Enregistrer".

— Nous avons sélectionné "View Dashboard" pour afficher nos données dans le tableau de bord. figure 4.49

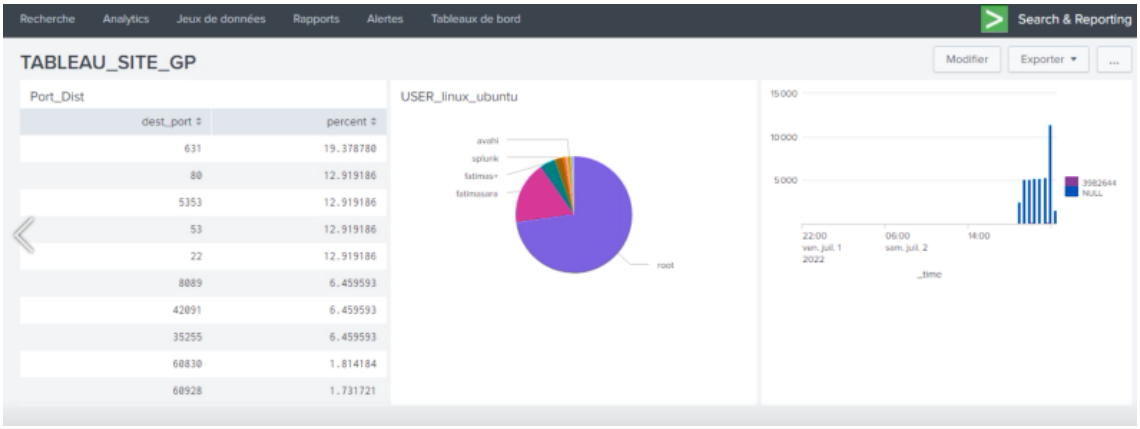

FIGURE 4.49 – Tableu de bord

4.8.6 Création des alertes

Nous avons utilisée les alertes pour surveiller et répondre à des événements spécifiques. Les alertes se déclenchent lorsque les seuils d'alerte définis pour une métrique sur une entité ou un groupe répondent à des conditions spécifiques. Voici les étapes pour créer une alerte dans splunk : Dans la page Recherche, nous avons entré la chaîne de recherche . et sélectionnée les trois différents modes disponibles : mode rapide, mode intelligent et mode verbeux. figure4.50

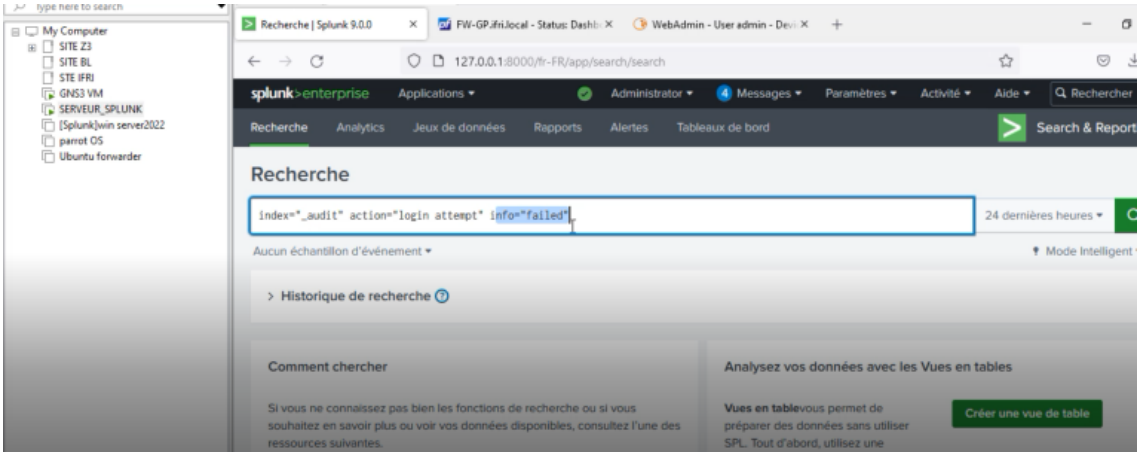

FIGURE 4.50 – Requete de recherche

Pour créer une alerte, nous avons sélectionné Enregistrer sous, puis sélectionnez Alerte . L'écran suivant s'affichera dans lequel nous pouvons entrer des détails supplémentaires.figure 4.51

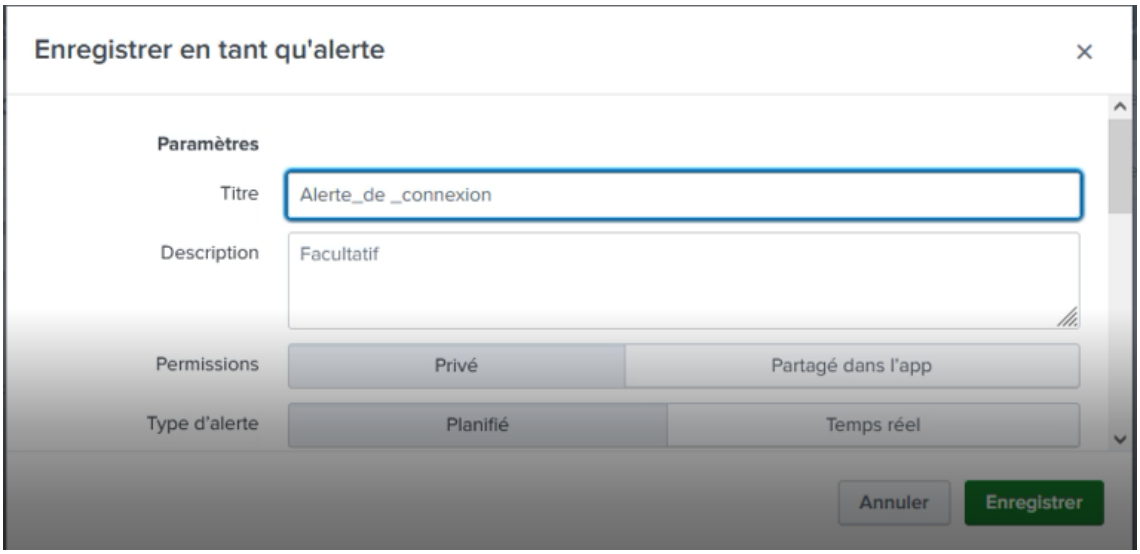

FIGURE 4.51 – Requete de recherche fu1

Limitation : nous avons utilisé la limitation pour supprimer le déclenchement d'une alerte pendant une période spécifique.
Actions de déclenchement : il s'agit de la section qui détermine la manière dont les utilisateurs sont informés de cette alerte. dans l'objet et le corps de l'e-mail pour ajouter de la spécificité à l'alerte. Par exemple, les champs objet et corps sont préremplis avec du texte qui utilise le jeton *name* ,Une fois que nous avons enregistrée l'alerte, nous avons verrez ce qui suit où nous pouvons apporté des modifications aux autorisations .figure4.52

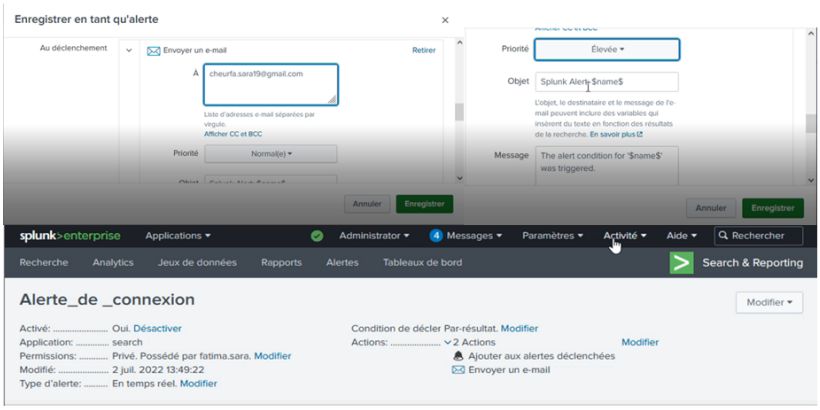

FIGURE 4.52 – Requete de recherche

4.9 Conclusion

Ce dernier chapitre nous à permis d'effectué une installation et configuration de touts équipements permettant un bon fonctionnement de notre solution **«SPLUNK»** avec le imulateur GNS3. Nous avons fait les différents étapes de récupérations des logos et des Syslog dans différents équipements et les analyses avec des tableaux de bord et des graphes.

Conclusion et perspectives

et m'a très chère tant

Pour un grand nombre d'entreprises, la pandémie du covid 19 a pu être l'occasion d'accélérer leur transition et d'approfondir leur fait de route numérique ce qui a été le cas pour le groupe IFRI qui nous a accueilli dans son organisme pour mener à point une mise en place d'une solution SIEM afin de réaliser ce travail, nous avons d'abord présenter un large panorama sur les dispositifs de sécurité à savoir les Parfeu et leur fonctionnement, les systèmes de détection IDS d'intrusion, les IPS ainsi qu'une principale solution SIEM.

Lors de notre stage au sein de l'entreprise, nous avons constaté que les données sont l'un des actifs le plus sous-utilisé et sous-évalué de toute l'organisation du réseau, alors qu'elles contiennent de puissantes informations commerciales et opérationnelles qui peuvent nous aider à diagnostiquer les problèmes de service et à détecter tout type de menace ou d'attaque.

Pour atténuer les risques liés à la sécurité engendrée par une croissance de données massives, la direction de l'entreprise IFRI nous a proposé l'intégration dans la structure de leur réseau d'un système basé sur l'intelligence opérationnelle. Notre choix c'est porter sur la solution SPLUNK entreprise qui s'est avéré très concluante en matière d'observabilité et d'adaptation aux besoins de l'entreprise. Ces résultats générant de précieuses investigations et de réponses rapides pour les alertes quotidiennes ont été visualisés grâce à une simulation effectuée sur l'émulateur GNS3.

D'une façon générale ce projet nous a été très bénéfique car nous avons enrichi nos connaissances sur les deux plans : théorique et pratique, et nous pouvons dire que les objectifs fixés au début ont été atteints. Mais cette évolution s'accompagne de nouveaux défis avec l'adoption généralisée des services Cloud, nous faisons de l'observabilité un nouveau champ de bataille de l'expérience client.

De ce fait, notre perspective est de se projeter sur des outils tel que SPLUNK observabilité et SPLUNK Cloud car plus le volume de données augmente, plus nos systèmes sont observables et moins ils peuvent être traités par des êtres humains sans l'assistance de l'intelligence artificielle.

Bibliographie

[1] Didier Godart. *Sécurité informatique : risques, stratégies et solutions : échec au cyber-roi.* Edipro, 2002 , Consulté le 10 mai 2022.

[2] https ://download.geo.drweb.com/pub/drweb/unix/doc/html/controlcenter/fr/dw-8-app-a-threat-types.htm , consulté le 7 juin 2022.

[3] https ://www.mozzaik365.com , Consulté le 20 juin 2022.

[4] Mme Nadia Nouali-Taboudjemat. Les firewalls comme solution aux problèmes de sécurité. In *Revue d'Information Scientifique et Technique (Rist)*, volume 9, pages 01–12. CERIST, 1999, Consulté le 27 mai 2022.

[5] *Squid Proxy Server 3.1 : guide du débutant.* 2011, Consulté le 3 juin 2022.

[6] *Construire des DMZ pour les réseaux d'entreprise.* Syngress Publishing, 2003, Consulté le 15 juin 2022.

[7] Elias Koret, Joxean et Bachaalany. *Le manuel du hacker antivirus.* 2015, Consulté le 15 juin 2022.

[8] DES ENTREPRISES DU CÔTÉ. Petites entreprises et sécurité informatique : un mariage de raison ?, consulté le 28 mai 2022.

[9] N Cherriere, G Montassier, R Picard, and E Thuiller. Les siem (security information and event management) : Gestion de la sécurité centralisée , consulté le 22 juin 2022.

[10] Mark Nicolett and Kelly M Kavanagh. Magic quadrant for security information and event management. *Gartner RAS Core Reasearch Note (May 2009)*, 2011, Consulté le 14 juin 2022.

[11] Eva Kostrecová and H Bınová. Research paper security information and event management. *Management*, 4(2), 2015, Consulté le 9 juin 2022.

[12] John Collins Kelly Kavanagh, Toby Bussa. Magic quadrant for security information and event management. *Gartner Group Research Note*, 2021, Consulté le 25 juin 2022.

[13] https ://www.educba.com/elk-stack-vs-splunk , consulté le 8 juin 2022.

[14] Deep Mehta. Splunk certified study guide , consulté le 26 mai 2022.

[15] Karun Subramanian. *Practical Splunk Search Processing Language : A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome*. Springer, 2020 , Consulté le 11 juin 2022.

[16] https ://splunkbase.splunk.com/app/742 , consulté le 13 juin 2022.

[17] Michael Kofler. *Linux : Installation, configuration et applications*. Pearson Education France, 2008 , Consulté le 10 juin 2022.

[18] Marcelo PUNTEL. Análise e aplicação de um modelo de política de acesso à internet em ambiente corporativo com sophos xg firewall. 2019 , Consulté le 25 juin 2022.

[19] IAE GUSTAVE EIFFEL. Le succès d'ubuntu : Un cas d'avantage concurrentiel dynamique dans l'open source , consulté le 16 juin 2022.

[20] https ://discoveredintelligence.ca , consulté le 10 juin 2022.

[21] https ://www.alphorm.com , consulté le 3 juin 2022.

Résumé

La supervision de la sécurité des systèmes d'information présente un grand défi pour les grandes entreprises, elle est considérée comme un pilier essentiel pour assurer la sécurité de tous les composants du système d'information afin de détecter les failles et les violations de sécurité et y remédier à eux. Parmi les parties analysées dans ces entreprises, on trouve ce qu'on appelle les fichiers Journaux, ces derniers sont construits et enregistrés avec un format spécial par de chaque équipement, système ou composant du SI en général. Ces fichiers aident à suivre les activités des utilisateurs dans le SI, ce qui permet de détecter et suivre les comportements suspects qui viole la politique de sécurité d'une façon ou d'une autre. Le suivi et l'analyse de ces événements est fait dans la plupart du temps par une équipe de sécurité. Cette tâche est une tâche difficile, du fait que le suivi des évènements doit être fait d'une manière enchainée sans négliger ou oublier aucun d'eux, surtout si cette surveillance concerne une activité critique. Dans ce projet, on va proposer une solution pour l'analyse des enregistrements data et sécurité en format de fichiers et logs en temps réel du SI « IFRI », et ceci en les récupérant à partir du serveur Splunk, les enrichir en utilisant différentes méthodes, cela sera suivi par leur indexation et stockage, afin qu'ils soient analysés par le système et contrôlés d'une manière simplifiée par l'équipe de sécurité. Cette solution va permettre une analyse dynamique de ces événements selon des règles construites et stockées par cette équipe, ce qui va aider majoritairement dans la facilitation de la supervision de la sécurité du système en offrant la possibilité de la recherche rapide et la filtration de ces évènements. A la fin de chaque analyse, un ensemble des alertes peut être ajouté et affiché dans le tableau de bord de ce système. La solution est mise en couvre en la présentant à travers une interface d'une application web qui respecte les règles d'interface Homme Machine (IHM) et les critères de sécurité des application web .

Mots clés : SIEM, fichier log, événement, supervision, SI, détection, analyse d'événements, indexation, alerte, tableau de bord, recherche et filtrage, Splunk.

Abstract

The supervision of the security of the information systems presents a great challenge for large companies, it is considered an essential pillar to ensure the security of all the components of the information system in order to detect the flaws and security violations and remedy them to them. Among the parts analyzed in these companies, we find the so-called Log Files, which are built and recorded with a special format by each equipment, system or component of the IS in general. These files help to follow the activities of users in the IS, which allows to detect and follow suspicious behaviors that violate the security policy in one way or another. The monitoring and analysis of these events is done in most cases by a security team. This is a difficult task, since the monitoring of events must be done in a chained way without neglecting or forgetting any of them, especially if this monitoring concerns a critical activity. In this project, we will propose a solution for the analysis of data and security records in file format and logs in real time of the IS "IFRI", by retrieving them from the Splunk server, enriching them using different methods, followed by their indexing and storage, so that they can be analyzed by the system and controlled in a simplified way by the security team. This solution will allow a dynamic analysis of these events according to rules built and stored by this team, which will help mainly in facilitating the supervision of the security of the system by offering the possibility of quick search and filtration of these events. At the end of each analysis, a set of alerts can be added and displayed in the dashboard of this system. The solution is covered by presenting it through a web application interface that respects the rules of Human Machine Interface (HMI) and the security criteria of web applications.

Keywords: SIEM, log file, event, supervision, IS, detection, event analysis, indexing, alert, dashboard, search and filtering, Splunk.