



Université SAAD DAHLEB - Blida 1

Faculté des sciences, Département d'Informatique

Mémoire en vue de l'obtention du diplôme de

**MASTER**

Domaine : **Mathématique informatique**

Filière : **informatique**

Spécialité : **SSI**



---

## Déploiement et Intégration d'une Solution SIEM (Security Information and Event Management)

---



Réalisé par

**AZZOUZ Rania**

**GHERNOUG Yasmine**

*Soutenu le 22 / 06 / 2023 devant l'honorable jury :*

***Président : Mme.oukid Salyha***

***Encadreur : Mr. DJEMA Farid***

***Co-Encadreur : Mr. BAROUDE Hamza***

***Promotrice : Mme. BOUSTIA Narhimene***

***Examineur : Mme. ELBEY Fella***  
Année universitaire 2022 / 2023

## ***Remerciements***

*Nous remercions Dieu le tout puissant qui nous a donné la force, le courage, la santé et la volonté pour entamer et mener à bien ce travail.*

*Nous tenons à exprimer toute notre reconnaissance à notre encadreur **Mr. Farid DJEMA** pour sa grande participation et sa disponibilité. Nous tenons aussi à le remercier pour son soutien moral qui nous a aidé à bien travailler.*

*Nous tenons également à remercier notre enseignant-tuteur **Mme. Narhimene BOUSTIA** qui nous a fourni la chance d'enrichir nos connaissances.*

*Ainsi que **Mr. Hamza BAROUDE**, chef de projet SIEM, pour ses conseils et orientations qui nous ont beaucoup aidés.*

*Nous remercions également les membres du jury pour avoir fait l'honneur à nous d'examiner notre travail.*

*Nous dédions ce mémoire à nos parents, nos sœurs, mon mari, ma belle-famille qui nous ont soutenus tout au long de ces années et nous ont toujours encouragés à faire ce que nous souhaitions et à donner le meilleur.*

*Nos vifs remerciements à tous ceux qui nous ont aidées de près ou de loin pour la réalisation de ce modeste travail.*

## ملخص

في السنوات الأخيرة ، أصبح أمن أنظمة المعلومات تحديًا كبيرًا للشركات ، ولتحقيق هذا الأخير يتطلب رؤية عامة لأنظمة معلومات الشركة من خلال أدوات أو حلول مناسبة ، من بينها SIEM الذي يسمح بجمع وتطبيع وتخزين وتحليل المعلومات.

لقد صممنا ونفذنا كجزء من هذا العمل ، اختيارًا للحل وفقًا لاحتياجات شركة ICOSNET مما جعل من الممكن الحصول على رؤية عامة لنظام المعلومات الخاص بها ، لجمع وتوحيد ثم تخزين وتحليل السجلات الأولية من أنواع مختلفة من المعدات الأمنية ، وعرض لوحات المعلومات والتقارير وتلقي التنبيهات.

الكلمة الرئيسية: الأمن ، نظام المعلومات ، SIEM ، جمع ، توحيد ، تخزين ، تحليل. السجلات ، السجلات ، وعرض عام على IS ، معدات الأمان ، التصور ، لوحات المعلومات ، التقارير ، التنبيهات.

## Résumé

Depuis quelques années, la sécurité des systèmes d'information est devenue un grand défi pour les entreprises, et pour atteindre ce dernier il faut une visibilité globale sur les systèmes d'information de l'entreprise à travers des outils ou des solutions adéquates. Parmi ces outils, les systèmes de gestion des événements de sécurité (SIEM) permettent la collecte, la normalisation, le stockage et l'analyse des journaux d'événements.

Nous avons conçu et mis en œuvre dans le cadre de ce travail, un choix de solution conforme au besoin de l'entreprise ICOSNET qui a permis d'avoir une vue globale sur son système d'information, faire collecter, normaliser puis stocker et analyser les logs bruts qui viennent des différents types d'équipements de sécurité, avoir une visualisation sur les tableaux de bords et les rapports et recevoir les alertes.

Mot clé : sécurité, système d'information, SIEM, collecter, normaliser, stocker, analyser. Les logs, les journaux, vue globale sur SI, équipement de sécurité, visualisation, tableau de bords, rapport, les alertes.

## Abstract

Since a few years, the security of the information system became a great challenge for the companies, and to reach this last one it is necessary a global visibility on the information system of the company through tools or adequate solutions, among them there in the SIEM which allowed to collect, to normalize, to store and to analyze the logs.

We have designed and implemented in the framework of this work, a choice of solution in accordance with the need of the company ICOSNET which allowed to have a global view on its information system, to collect, normalize then store and analyze the raw logs come from these different types of security equipment, to have a visualization on the dashboards and the reports and to receive the alerts;

**Keyword:** security, information system, SIEM, collect, normalize, store, analyze. Logs, logs, global view on IS, security equipment, visualization, dashboard, report, alerts.

# Tables des matières

<b>Liste des figures</b>	3
<b>Liste des tableaux</b>	4
<b>Introduction générale</b>	5
<b>Chapitre 1. Généralités</b>	7
<b>Introduction</b>	7
1.	7
2.	8
3.1.	8
3.2.	8
3.2.1.	9
3.2.2.	9
3.3.	9
3.3.1.	9
3.3.2.	10
3.3.3.	10
3.3.4.	11
3.3.5.	12
3.3.6.	12
3.3.7.	12
3.	13
4.1	13
4.2	13
4.3	14
<b>Conclusion</b>	15
<b>Chapitre 2. Etude et Conception</b>	16
<b>Introduction</b>	16
1.	16
2.	16
3.	17
3.1	18
3.2	19
4.	19
4.1	22

<b>4.1.1 Cas d'utilisation 'Gérer les utilisateurs : ajouter un utilisateur'</b>	22
<b>4.1.2 Cas d'utilisation 'Gérer les utilisateurs : modifier un utilisateur'</b>	23
<b>4.1.3 Cas d'utilisation 'Gérer les utilisateurs : Supprimer un utilisateur'</b>	23
<b>4.1.4 Cas d'utilisation 'Gérer les utilisateurs : changer le mot de passe '</b>	24
<b>5.</b>	25
<b>6.</b>	26
<b>7.</b>	27
<b>Conclusion</b>	28
<b>Chapitre 3. Déploiement et Mise en service du SIEM LogPoint</b>	29
<b>1.</b>	29
<b>1.1.</b>	29
<b>1.2.</b>	30
<b>1.1.1.</b>	30
<b>1.1.2.</b>	30
<b>1.1.3.</b>	31
<b>2.</b>	32
<b>2.1.</b>	32
<b>2.2.</b>	33
<b>2.3.</b>	33
<b>3.</b>	34
<b>3.1</b>	34
<b>3.2</b>	42
<b>Conclusion</b>	43
<b>Conclusion générale</b>	44
<b>Abréviations</b>	45
<b>Bibliographie</b>	47

## Liste des figures

FIGURE 3.1 : LE MODELE MSSP	10
FIGURE 3.2 : TRIANGLE DE SOC.	10
FIGURE 3.3 : COMPOSANTS ET FONCTIONS D'UN SOC.	11
FIGURE 4.1 : ILLUSTRATION DES COMPOSANTS DU SIEM LOGPOINT.	16
FIGURE 1.1 : ILLUSTRATION DE L'ARCHITECTURE DE L'INFRASTRUCTURE IT.	18
FIGURE 5.1: DIAGRAMME DE NAVIGATION.	<b>Erreur ! Signet non défini.</b>
FIGURE 6.1 : LA LISTE DES REGLES PREDEFINIE.	29
FIGURE 6.2 : STRUCTURE DE TRAITEMENT D'INCIDENTS.	29
FIGURE 6.2 : INTERFACE SUIVI DES ALERTES ET INCIDENTS.	30
FIGURE 6.3 : INTERFACE ASSIGN USER.	30
FIGURE 1.1 : CONFIGURATION DE LA CONNEXION AU RESEAU	32
FIGURE 1.2 : PRISE D'ECRAN DE L'INTERFACE DE CONNEXION.	32
FIGURE 1.3 : AJOUTER UNE LICENCE.	32
FIGURE 1.4 : L'INTERFACE WEB LOGPOINT.	33
FIGURE 2.1 : PRISE D'ECRAN DES UTILISATEURS.	34
FIGURE 2.2 : LES GROUPES D'UTILISATEURS.	34
FIGURE 2.3 : LES GROUPES DE PERMISSION	35
FIGURE 2.4 : LES PERMISSIONS QUE L'ADMIN PEUT FAIRE.	35
FIGURE 2.5 : LES PERMISSIONS QUE L'OPERATEUR PEUT FAIRE.	36
FIGURE 3.1 : LES POLITIQUES CONFIGUREES.	36
FIGURE 3.2 : POLITIQUE DE NORMALISATION.	37
FIGURE 3.3 : POLITIQUE DE TRAITEMENT.	38
FIGURE 3.4 : POLITIQUE DE COLLECTE.	38
FIGURE 3.5 : LISTE DES ACTIFS INTEGRES.	39
FIGURE 3.6 : POLITIQUE DE NORMALISATION DE ROUTEUR.	39
FIGURE 3.7 : POLITIQUE DE TRAITEMENT DES ROUTEURS.	40
FIGURE 3.8 : POLITIQUE DE NORMALISATION DE SERVEUR.	41
FIGURE 3.9 : POLITIQUE DE TRAITEMENT DE SERVEUR.	41
FIGURE 3.10 : MIGRATION AGENT LOGPOINT.	41
FIGURE 3.11 : AJOUTE LE RECUPERATEUR DES LOGS	42
FIGURE 3.12 : CONFIGURATION DE SERVEUR DE TYPE LINUX.	42
FIGURE 3.13 : ARCHITECTURE DE SYSTEME.	<b>Erreur ! Signet non défini.</b>
FIGURE 3.14 : LES LOGS BRUTS COLLECTER.	44
FIGURE 3.15 : TABLEAU DE BORD.	45



## Liste des tableaux

TABLEAU 3.1 : DESCRIPTION TEXTUELLE DU -GESTION D'UTILISATEUR –	20
TABLEAU 3.2 : DESCRIPTION TEXTUELLE DU -GESTION DES LOGS -	20
TABLEAU 1.1 : DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : AJOUTER UN UTILISATEUR' –	24
TABLEAU 4.2 : DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : MODIFIER UN UTILISATEUR' -	25
TABLEAU 4.3 : DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : SUPPRIMER UN UTILISATEUR' -	25
TABLEAU 4.4 : DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : CHANGER LE MOT DE PASSE D'UTILISATEUR'-.	26
TABLEAU 1.1 : ENVIRONNEMENT DE TRAVAIL.	31
TABLEAU 1.2 : LA LISTE DES PORTS A OUVRIR.	33

# Introduction générale

De nos jours, la sécurité de données est devenue sans doute une des préoccupations majeures au cœur des entreprises quel que soit leur taille, leur secteur d'activité ou emplacement.

Selon le rapport d'IBM publié en 2022, le coût relatif aux violations de données dans le secteur de la santé s'élève à plus de 10 millions de dollars [1]. Par ailleurs, on estime que la cybercriminalité coûtera aux entreprises environ 10,5 trillions de dollars par an d'ici 2025[2].

La cybercriminalité se développe et s'organise davantage autour de modèles économiques connus. On constate l'émergence du *Ransomware-as-a-Service*, des attaques distribuées de déni de service (DDoS), l'utilisation de l'IA, etc., tous initiés et conduits de manière plus ciblée et intensive dans un but lucratif.

Les entreprises, en Algérie, ne font pas l'exception et ne sont plus à l'abri des alphas du numérique. Elles sont, désormais, amenées à se doter des outils adéquats face aux risques.

Le **SOC** (*Security Operations Center*), véritable tour de contrôle du **SI**, apporte la réponse en matière de défense. Son rôle consiste à surveiller, détecter, analyser et alerter.

Au cœur du SOC : le **SIEM** (*Security Information and Events Management*). Cet outil représente le véritable moteur du SOC en termes de collecte, corrélation et visualisation des événements.

**Icosnet Spa**, fournisseur de services Internet, a initié un projet de déploiement de l'outil SIEM LogPoint. Ce projet fournira des réponses particulières aux préoccupations de l'entreprise en matière de visibilité et de maîtriser les incidents de sécurité, à savoir :

- ✓ Gagner en visibilité par rapport aux milliers de logs et événements générés au niveau de l'infrastructure IT par les quelques centaines d'actifs (dispositifs de sécurité, équipements réseau, Serveurs, applications ...)
- ✓ Pouvoir effectuer une corrélation des multiples et différents événements, dont les relations, sont difficiles à percevoir et à identifier par les équipes sécurité ;
- ✓ Gagner en agilité quant à la détection et le traitement des incidents de sécurité, en automatisant les processus ;

- ✓ Renforcer les compétences des équipes de sécurité en vue de fournir un service qualitatif aux entreprises.

## Objectifs du travail

Dans le cadre de notre mémoire, notre travail consiste, principalement, à :

- Effectuer le déploiement et la configuration de l'outil SIEM,
- Implémenter les stratégies de détection et réponse aux incidents,
- Illustrer le fonctionnement du SIEM par des tableaux de bord et des indicateurs.

## Organisation du mémoire

Afin d'atteindre notre objectif, nous avons organisé notre mémoire autour de quatre chapitres qui abordent, chacun, un thème particulier :

-Dans le premier chapitre, nous présenterons l'organisme d'accueil, à savoir Icosnet Spa, ainsi que sa vision et sa démarche en termes de cybersécurité, nous illustrerons le concept SIEM et décrirons avec de plus amples détails les caractéristiques du SIEM LogPoint préconisé par l'entreprise.

-Le deuxième chapitre sera consacré à la conception du projet. Nous y trouverons les éléments d'architectures permettant une intégration optimale de la solution SIEM dans l'environnement alloué de l'entreprise.

-Le chapitre 3 sera consacré à l'installation du SIEM, sa configuration et mise en service.

Enfin, nous terminerons par une conclusion générale dans laquelle nous évaluerons, d'une part, notre travail et notre expérience à mener le projet de déploiement de l'outil SIEM et, d'autre part, l'impact perçu par l'intégration de cet outil dans l'environnement de l'entreprise.

Nous aborderons brièvement les futures étapes réservées à ce projet au niveau de l'entreprise.

# Chapitre 1. Généralités

## Introduction

Face à la cybercriminalité de plus en plus sophistiquée, la sécurité devient un enjeu de taille pour les entreprises. Pour faire face à cette menace croissante, il est nécessaire de basculer vers une approche qui privilégie l'utilisation d'outils de supervision avancés.

Nous allons illustrer les aspects relatifs à l'outil SIEM, la différence entre les solutions Open-source et commerciales ainsi que les principales caractéristiques de cet outil. Nous examinerons ensuite l'outil SIEM préconisé par l'entreprise Icosnet, à savoir, la solution SIEM LogPoint.

Aussi, nous mettrons en évidence les motivations de l'entreprise quant au choix de cette technologie.

- **83 %** des entreprises ont été victimes d'au moins une forme de cyberattaques,
- Toutes les **39 secondes** une entreprise est victime d'une cyberattaque,
- **30000** sites web sont piratés chaque jour,
- **45 %** des violations se sont produites dans le cloud,
- **277 jours** correspondent au délai moyen pour identifier et neutraliser une attaque de type « **ransomware** »,
- **29 jours** de réduction du temps de réponse pour les entreprises qui disposent de technologies de détection et de réponse. [1]

Aujourd'hui, la question ne se pose plus de savoir si une entreprise sera attaquée, mais quand et comment elle le sera. Les entreprises doivent donc mettre en place des mesures de sécurité efficaces pour y faire face et se remettre rapidement d'une attaque.

Dans ce chapitre, nous fournirons un aperçu du paysage de la Cybersécurité et son impact sur les entreprises et comment la société Icosnet Spa se positionne dans cet environnement en tant que Fournisseur de Services de Sécurité.

## 1. Présentation de l'entreprise Icosnet

Créée en 1999, **Icosnet Spa** est un opérateur d'accès Internet, solutions de communication et hébergement Cloud. Icosnet Spa, considéré comme le seul fournisseur privé en Algérie, s'impose comme un fournisseur alternatif sur le marché de la convergence voix et données pour les PME/PMI, les grands comptes et les multinationales installées en Algérie.

Grâce à son capital humain pluridisciplinaire et motivé moyennant les 160 employés, Icosnet Spa a développé un patrimoine technique considérable caractérisé par 33 points de présences (**POP**), deux (02) data centers sur le territoire national, une variété de produits et services et un savoir-faire technique qualitatif.

Le positionnement et l'envergure actuels de l'entreprise lui permettent d'adresser des questions plus complexes et plus critiques dont la souveraineté numérique, l'hébergement Cloud La sécurité des données représente un défi tant pour les entreprises que pour l'écosystème des NTIC en Algérie.

**Icosnet Spa** est membre de l'Union internationale des télécommunications (**UIT**).

## 2. La protection des données au centre des préoccupations

### 3.1. La vision MSSP

Consciente des enjeux relatifs aux transformations numériques des entreprises, Icosnet se veut être un acteur majeur dans le domaine de la sécurité de l'information et la protection des données à travers une démarche capable de répondre efficacement aux aspirations des entreprises vis-à-vis des cyber risques.

**MSSP** (*Managed Security Service Provider*) représente un modèle de « Fournisseurs de Services » conçu pour gérer la totalité de la sécurité des entreprises en les protégeant contre toute vulnérabilité, menace ou attaque. Le modèle MSSP repose sur une expertise et des compétences avancées.



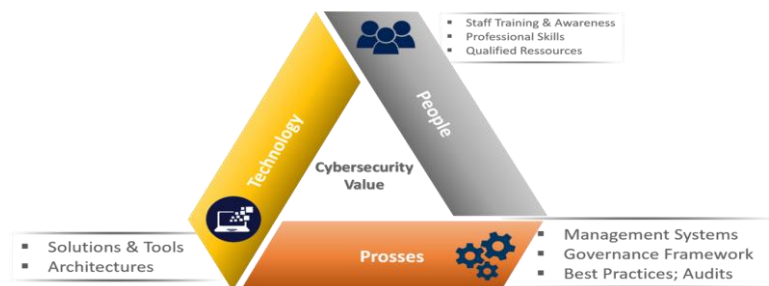
**FIGURE 3.1 :LE MODELE MSSP**

Pilier fondamental de sa vision stratégique en matière de Cybersécurité, **Icosnet** engage tous les moyens humains, technologiques et organisationnels nécessaires au déploiement, à terme, du modèle MSSP.

### 3.2. Le SOC

Un **SOC** (*Security Operations Center*) est un centre de commande pour les professionnels de la cybersécurité. Il permet à l'entreprise de surveiller en permanence la sécurité informatique de ses actifs IT, mais surtout, de réagir sans délai en cas d'attaque avérée ou suspectée.

Le SOC représente une entité opérationnelle combinant un personnel qualifié, des outils technologiques et des processus en mesure de gérer les différentes interactions et flux de traitement d'incidents.



**FIGURE 3.2 : TRIANGLE DE SOC.**

### 3.2.1. Fonctions et avantages d'un SOC

Le SOC surveille et analyse les données de sécurité générées au niveau de l'ensemble de l'infrastructure IT de l'entreprise, en allant des serveurs et des applications jusqu'aux périphériques réseau et de sécurité.

Le SOC répond aux fonctions vitales suivantes :

- La Surveillance continue et triage des événements de sécurité,
- La Gestion des incidents et amélioration des temps de réponse, notamment, la détection des intrusions et l'analyse des menaces,
- La Détection et gestion des vulnérabilités des actifs matériels et logiciels,
- La Réduction des coûts associés aux incidents de sécurité,
- Le Développement de données et d'indicateurs pour le Reporting et la gestion de la conformité.

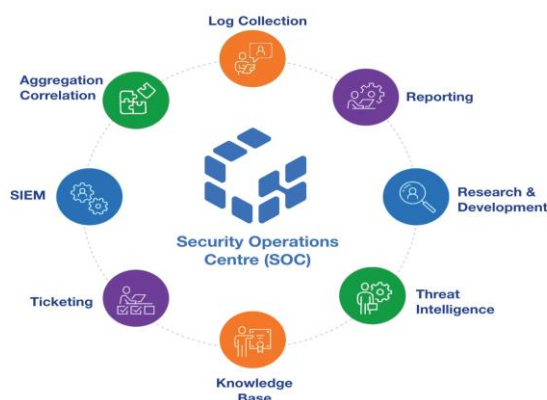


FIGURE 3.3 : COMPOSANTS ET FONCTIONS D'UN SOC.

### 3.2.2. Défis relatifs à la mise en place d'un SOC

La surveillance continue du SOC fournit un avantage significatif en réduisant l'écart entre le moment correspondant à la tentative d'intrusion et celui de la détection, permettant ainsi aux entreprises de bénéficier d'une précieuse proactivité face aux risques.

La mise en place et le maintien d'un SOC nécessitent du temps, des ressources humaines qualifiées et des ressources financières conséquentes. Ces facteurs peuvent rendre la mise en place d'un SOC inaccessible pour certaines entreprises.

Compte tenu des capacités, parfois limitées, des entreprises à appréhender les cyber risques, Icosnet s'est inscrite comme objectif de mettre en place un SOC qui permettra aux entreprises de bénéficier, sans engager d'importants investissements, des services du SOC en mode managé.

## 3.3. Au cœur du SOC : LE SIEM

### 3.3.1. Historique du SIEM

L'institut des normes et de la technologie des États-Unis **NIST** définit une solution **SIEM** (*Security Information and Event Management*) comme « Une application qui offre la possibilité de recueillir des

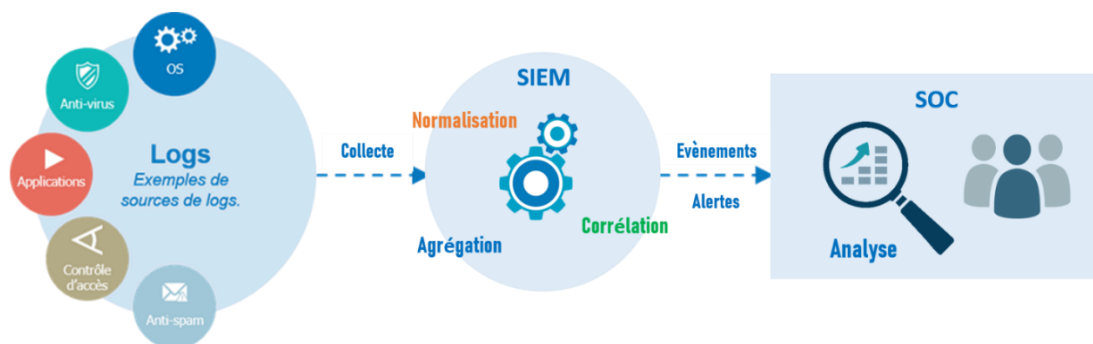
données de sécurité à partir des composants d'un système d'information et de présenter ces données sous forme d'informations exploitables via une interface unique » [4].

**Mark Nicolett** et **Amrit Williams** de **Gartner** ont été les premiers à nommer la solution SIEM en 2005[4]. A l'origine, deux types de solutions distinctes géraient les données de sécurité : le **SIM** qui se concentre sur la collecte et la gestion des logs et le **SEM** [5] qui se charge de l'analyse et du signalement en temps réel.

Les deux analystes ont constaté l'étroite complémentarité des deux outils et ont jugé plus pertinent de les combiner pour mieux piloter la sécurité, d'où l'émergence de la notion du SIEM.

### 3.3.2. Définition d'un SIEM

Le SIEM, véritable moteur du SOC, permet de fournir une vue complète et centralisée de la posture de sécurité d'une infrastructure IT et fournit aux professionnels de la cybersécurité un aperçu de tous les événements et activités au sein de cette infrastructure.



**Figure 3.4 : DÉFINITION D'UN SIEM [5]**

Les technologies SIEM varient en envergure : les plus basiques assurent la gestion des logs et génèrent des alertes, quand d'autres combinent de puissants moteurs d'analyse et intègrent des technologies avancées telles que le **SOAR** (*Security Orchestration, Automation, and Response*) pour automatiser la réponse aux menaces et l'**UEBA** (*User and Entity Behavior Analytics*) qui permet la détection des menaces sur une base comportementale. Certains SIEM, de nouvelle génération, proposent également des modules de *machine Learning* qui disposent d'algorithmes d'apprentissage capables d'automatiser les processus de prise de décision et de réponse en fonction des données collectées.

### 3.3.3. Les apports d'une solution SIEM

Les solutions SIEM représentent de véritables atouts pour les entreprises et apportent une valeur ajoutée significative aux entreprises à travers les multiples valeurs qu'elles intègrent [6]:

- **Reconnaissance avancée des menaces en temps réel**

La surveillance active permanente (24/7) gère l'ensemble de l'infrastructure et réduit considérablement le délai nécessaire pour identifier les menaces et vulnérabilités potentielles du réseau et y répondre.

- **Détection des menaces avancées et inconnues**

Se basant sur des flux intégrés de renseignements sur les menaces, les solutions SIEM peuvent atténuer avec succès un ensemble important de failles de sécurité, dont les attaques par **hameçonnage**, les injections **SQL** et l'exfiltration de données.

- **Surveillance des applications et des utilisateurs**

Les solutions SIEM suivent toutes les activités du réseau de tous les utilisateurs, appareils et applications, améliorant considérablement la transparence dans l'ensemble de l'infrastructure en détectant les menaces, quelle que soit l'origine des accès aux actifs de l'entreprise.

- **Réalisation d'investigations numériques**

Les solutions SIEM permettent aux organisations de collecter et d'analyser efficacement les données de logs et recréer des incidents antérieurs ou en analyser de nouveaux pour enquêter sur les activités suspectes et mettre en œuvre des processus de sécurité plus efficaces.

- **Automatisation basée sur l'IA**

Les solutions SIEM de nouvelle génération intègrent de puissantes fonctionnalités d'orchestration, d'automatisation et de réponse (SOAR). D'autre part, grâce à un apprentissage automatique en profondeur, elles peuvent identifier des menaces et répondre aux incidents en moins de temps.

- **Amélioration de l'efficacité organisationnelle**

En optimisant la visibilité des environnements informatiques, la technologie SIEM peut être un élément essentiel pour améliorer l'efficacité entre les différents services. Les équipes peuvent communiquer et collaborer efficacement lorsqu'elles répondent aux événements et incidents de sécurité.

- **Audit de conformité réglementaire**

L'automatisation avancée permet de rationaliser la collecte et l'analyse des journaux système et des événements de sécurité, et de centraliser l'audit et le reporting de conformité de l'ensemble de l'infrastructure de l'entreprise.

### **3.3.4. Solutions SIEM Open-source**

Un logiciel Open-source est un logiciel développé et géré dans le cadre d'une collaboration ouverte et mis à disposition, généralement, gratuitement pour que chacun puisse l'utiliser, l'examiner, le modifier et le redistribuer comme il le souhaite[7].

Du fait des coûts élevés des outils propriétaires, qui s'avèrent au-delà des capacités des entreprises, ces dernières s'orientent vers les solutions SIEM Open-source espérant trouver refuge contre les menaces et les risques qu'elles encourent.

Cependant, si l'open source permet aux entreprises d'économiser sur les coûts de licence ( Licence), il entraîne en contrepartie des coûts cachés liés à la gestion des développements, à l'intégration des solutions et, plus particulièrement, à la qualité du support aux utilisateurs finaux en cas de panne ou de dysfonctionnement du service.



Plusieurs solutions SIEM Open-source sont disponibles, dont : **ELK Stack**, **Vazduh** et **Ossec**.

### 3.3.5. Solutions SIEM propriétaires

Une solution propriétaire, dite commerciale ou payante, appartient à la personne morale ou physique l'ayant conçue et développée. Contrairement à un logiciel Open-source, son code n'est pas accessible, modifiable ou distribué sans autorisation formelle de son éditeur [8].

Utiliser une solution SIEM propriétaire revient à établir une relation commerciale avec le prestataire. L'acquisition du logiciel est, généralement, accompagnée par une prestation de service de support technique, droit aux mises à jour et développements spécifiques.

L'acquisition et l'exploitation d'une solution SIEM propriétaire engage souvent un budget conséquent. Cependant, le **TTM** reste élevé comparé à un déploiement Open-source. L'avantage majeur pour le fournisseur de services est sans doute sa capacité à honorer ses engagements de disponibilité et continuité de service vis-à-vis des utilisateurs.

Par ailleurs, les équipes de sécurité bénéficiant du support de l'Éditeur focalisent leurs efforts sur le traitement et la réponse aux incidents plutôt que les questions de développement (cas Open-source).

Parmi les solutions SIEM propriétaires, on y trouve : **IBM QRadar**, **Splunk**, **LogPoint** et **LogRhythm**.

### 3.3.6. Quels modes de déploiement pour le SIEM

Historiquement, le SIEM traîne l'image d'une solution coûteuse en matière d'investissements. D'autre part, la complexité des menaces cybers est telle aujourd'hui que le déploiement d'une telle solution au sein de l'entreprise nécessite des compétences internes qui s'avèrent souvent onéreuses et volatiles.

Toutes ces conditions font que bon nombre des entreprises s'orientent, de plus en plus, vers des modèles de sous-traitance et service managé disponible sur le Cloud sous forme de SIEM-as-a-Service (ou SOC-as-a-Service). La sécurité du SI est ainsi garantie à moindre coût.

### 3.3.7. Critères de choix de la solution SIEM

Le personnel de sécurité a tout intérêt à étudier les capacités des différents systèmes SIEM disponibles pour identifier celui qui répond le mieux aux besoins de son entreprise.

Pour Icosnet, le choix de la solution SIEM répond à des spécifications particulières correspondantes au contexte de l'entreprise en tant que fournisseur de services. On distingue :

- **Les coûts de la solution :** Les coûts relatifs au déploiement, au fonctionnement et au maintien de la solution doivent être clairement identifiés et quantifiés :
  - Les coûts d'acquisition et les coûts récurrents relatifs au support technique et aux licences,
  - Les coûts associés à l'extension de la solution : volume des données, nombre d'actifs et nombres d'utilisateurs,
  - Les coûts de formations et développements spécifiques.
- **Le Support Technique :** La qualité de service et l'accompagnement de l'éditeur le long du cycle de vie du produit (projet, exploitation, développement, etc.) est un élément décisif. Le

support doit être réactif et performant permettant de garantir une continuité de service sans faille.

- **La prise en charge des sources de logs :** La solution SIEM doit être en mesure d'ingérer toutes les sources de données dont dispose l'entreprise (équipements de sécurité, équipements réseaux, les serveurs et applications d'hébergement, etc.).
- **La flexibilité :** La volumétrie des données produites par l'infrastructure IT ne cesse d'augmenter. Une telle tendance exige que la solution SIEM soit d'une grande flexibilité et capable d'adapter sa capacité et son architecture à toute sollicitation de charge.
- **L'ergonomie de la solution :** La solution doit disposer d'interfaces ergonomiques : des tableaux de bords (Widgets) et un Reporting complet permettant aux différents utilisateurs d'assimiler rapidement et clairement la posture en sécurité.
- **L'évolutivité :** Face à la sophistication croissante des cyberattaques, le SIEM doit garantir un taux de détection élevé (tends vers 100%). Il doit donc intégrer les nouvelles techniques de détection telles que le SOAR, l'UEBA et l'AI.
- **La conformité réglementaire :** Les exigences réglementaires de conformité vis-à-vis de certaines normes et textes loi, comme la protection des données à caractère personnelles, présentent aussi un critère à ne pas négliger.

### 3. La solution SIEM LogPoint

Suite à une étude comparative basée sur les critères de choix susmentionnés, Icosnet s'est orientée vers le SIEM LogPoint. Ce choix a été renforcé par les références de l'Éditeur ainsi qu'à travers les multiples échanges et discussions prometteuses en termes de collaboration et partenariat stratégique.

#### 4.1 Présentation de LogPoint

Log Point est considéré comme l'un des principaux fournisseurs de SIEM en Europe. L'entreprise est basée à Copenhague, au Danemark et dispose de bureaux dans le monde entier. LogPoint propose des technologies avancées et convergentes qui détectent efficacement les menaces, minimise les faux positifs et répond aux risques de manière autonome et efficace... Aujourd'hui, plus de 1000 organisations font confiance à LogPoint »[9].

#### 4.2 Caractéristiques clés du SIEM LogPoint

LogPoint permet de collecter n'importe quel type de logs. Il s'appuie sur un stockage de fichiers plats et une indexation des informations dans un environnement Big data. Cela permet de traiter un volume d'information sans limite et une performance en temps de réponse avancée. Log Point se distingue par :

- **La capacité à traiter les données brutes** : Grâce à sa grande capacité de normalisation, Log Point permet de traduire les données brutes en informations exploitables.
- **La gestion des coûts** : Le modèle de Licence repose sur le nombre des nœuds (ou adresses IP) et non pas sur le volume des données traitées qui augmente sans cesse.
- **La prise en charge du Framework MITRE ATTACK** : Le *Framework ATTACK* propose des tactiques et des techniques efficaces et renforce les dispositifs de défense contre les menaces.
- **La conformité au standard EAL3+** : LogPoint dispose de la certification EAL 3+. Elle est exigée par l'OTAN et les organisations aux infrastructures critiques comme l'armée, les agences de renseignement, les entreprises de services publics et les télécoms [10].
- **L'intégration du composant SOAR** : SOAR fait référence aux mécanismes qui combinent l'analyse des menaces et l'automatisation des processus de résolution des incidents [11].
- **L'intégration de l'UEBA** : L'UEBA est une technologie de cybersécurité créée par le Gartner. Elle utilise des algorithmes d'apprentissage automatique qui observent et détectent les comportements inhabituels des personnes ou des actifs.

### 4.3 Composants du SIEM LogPoint

La solution LogPoint s'articule autour de trois fonctions principales :

- **La Collection des journaux** : LogPoint s'appuie sur Syslog pour collecter les messages de journalisation et des événements système. Les journaux envoyés depuis le périphérique source sont reçus par le « Collecteur » qui gère le stockage des logs.

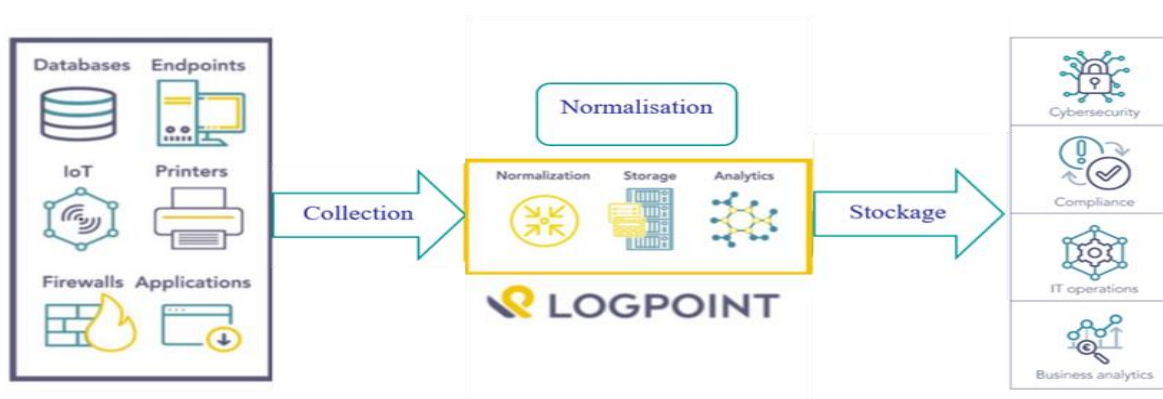


FIGURE 4.1 : ILLUSTRATION DES COMPOSANTS DU SIEM LOGPOINT.

- **La Normalisation** : Une fois les journaux collectés, la phase de normalisation commence. Cela signifie que les logs bruts dans différents formats sont traduits dans un seul "langage". Les

données sont doublement indexées pour améliorer les capacités de recherche et de récupération des données.

- **Le Stockage et l'indexation** : Une fois la normalisation effectuée, l'information est stockée et indexée permettant ainsi d'effectuer des corrélations et de construire des tableaux de bord, de créer des alertes, de définir des incidents ou d'établir des rapports, ils vont permettre aussi de définir des actions automatisées sur des outils tiers.

## Conclusion

Dans ce chapitre, nous avons présenté l'entreprise Icosnet Spa et sa vision de la gestion de la sécurité pour les entreprises, axée sur les services de sécurité managés. Une des étapes clés de cette stratégie est le déploiement d'un dispositif SIEM, qui fera l'objet de notre étude et des prochains chapitres.

D'autre part, nous avons passé en revue les principales caractéristiques des solutions SIEM. Nous avons mis en évidence les critères de choix de l'entreprise qui l'ont conduite à choisir LogPoint comme solution SIEM.

Enfin, nous avons passé en revue les principales caractéristiques de LogPoint.

# Chapitre 2. Etude et Conception

## Introduction

Dans le chapitre précédent, nous avons présenté le contexte général du travail ainsi que les notions de bases liées à notre sujet.

Après avoir défini le cadre de notre solution, nous nous orientons à travers le présent chapitre, vers la conception de notre système.

Nous allons commencer par détailler l'architecture de notre solution :

## 1. Architecture de l'infrastructure IT

Le schéma ci-après fournit une vue macro (*High Level*) de l'architecture de l'entreprise. Le SIEM sera implémenté de manière à superviser et contrôler les points les plus sensibles de l'infrastructure.

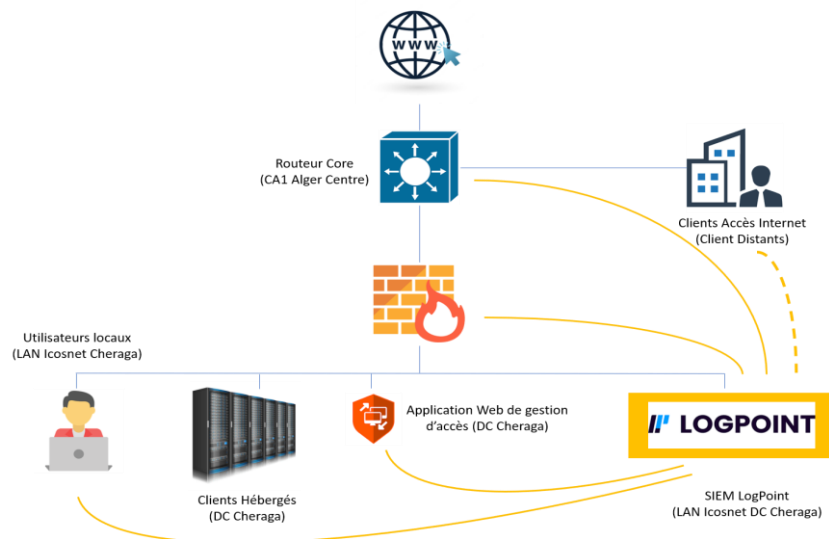


FIGURE 1.1 : ILLUSTRATION DE L'ARCHITECTURE DE L'INFRASTRUCTURE IT.

## 2. Etablissement des sources de données

Sur recommandation de l'équipe du projet, le déploiement sera effectué à travers des phases distinctes permettant d'évaluer et contrôler l'implémentation du SIEM au niveau ressources, charge, maîtrise, etc.

Pour notre part, le travail sera limité à l'implémentation de certaines ressources représentatives des différents types d'actifs présents au sein de l'infrastructure IT, à savoir :

- **Pare-feu Principal (Firewall Core) :**

Le Firewall *Core* représente le point névralgique des communications de l'entreprise. Cet équipement gère l'ensemble de la sécurité du Système d'Information ainsi que du *Data Center* où sont hébergés les Clients et les applications Cloud.

Tous les flux de communication internes et externes transitent à travers ce point. Il convient donc de superviser de très près le trafic acheminé de et vers les différentes sources et destinations du réseau. Cependant, et comme illustré sur la Figure 1.1 , le trafic relatif aux Clients accès n'est pas acheminé à travers ce point.

- **Routeur Principale (Core) :** Le Routeur Core est déployé au niveau périphérique du réseau de l'entreprise. En effet, et comme son nom l'indique, ce dernier gère le routage et les communications Internet de tous les Clients de l'entreprise (en tant que fournisseur de service d'accès Internet), quel que soit leurs emplacements.

Ainsi, la partie du flux non inspectée par le Firewall Principale passe par le Routeur Core. Il convient donc de superviser cet équipement afin de maîtriser les menaces sur l'ensemble du réseau WAN.

- **Application web gestion d'accès professionnelle :**

Application web gestion d'accès professionnelle représente un échantillon des catégories d'applications hébergées sur le Cloud de l'entreprise. Elle illustre les différentes couches et différents usages associés aux applications Web, données sensibles, accès à distance, utilisateurs à privilèges, etc.

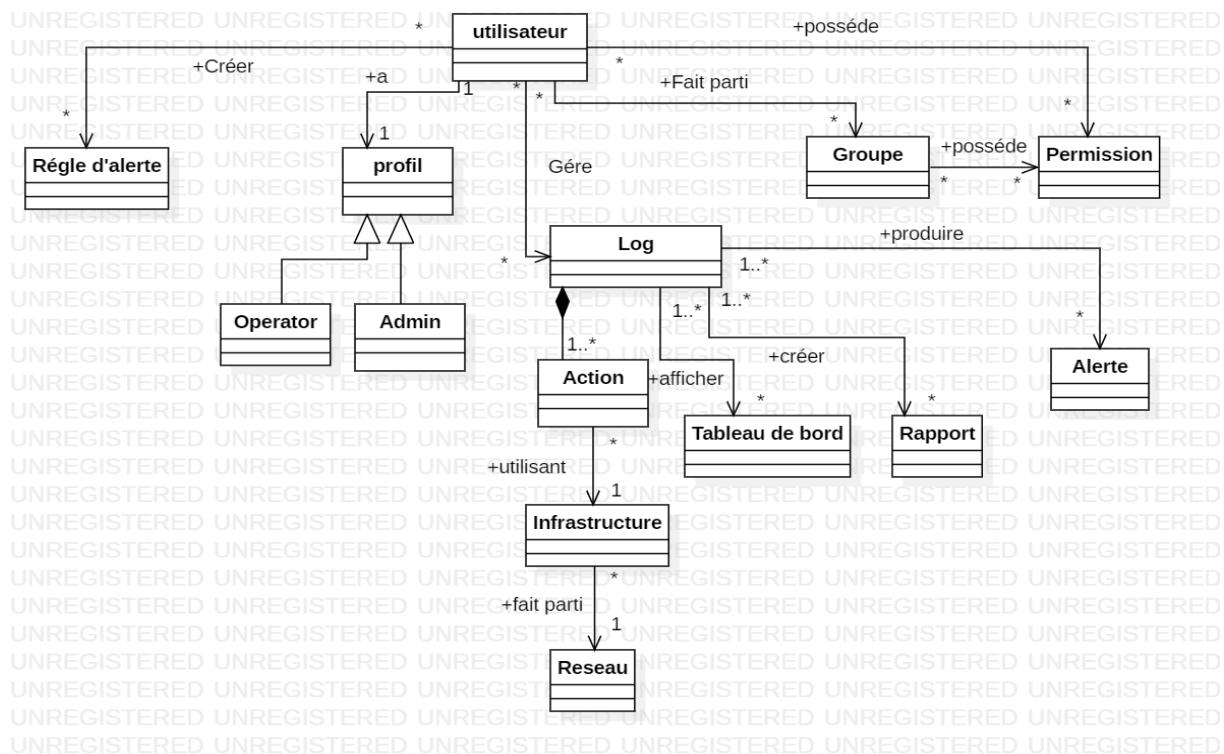
Cette application permet donc de reproduire une grande catégorie de violations de données ou accès non autorisés, ce qui doit être supervisé et contrôlé par le SIEM.

### 3. Diagramme de classe :

Dans cette partie, nous allons présenter le diagramme de classe global de notre système (comprenant uniquement les classes et les relations) pour illustrer les entités qui constituent le système, afficher les relations entre les entités et décrire le rôle de ces entités. Nous allons par la suite détailler ce diagramme en montrant quelques descriptions textuelles :

- Gestion d'utilisateurs
- Gestion des logs

Le diagramme de classe de notre système est représenté par la **figure 3.1**.



**Figure 3.1** : Diagramme de classe de système LOGPOINT.

Les tableaux suivants montrent la description textuelle de quelques classes utilisées dans le diagramme de classe :

### 3.1 Gestion d'utilisateurs

Le tableau suivant décrit comment l'utilisateur de notre système peut gérer les utilisateurs .

Classe	Description
<b>Utilisateur</b>	Cette classe représente l'utilisateur de notre système qui se caractérise par un nom, prénom, email, nom d'utilisateur, mot de passe chaque utilisateur fait partie d'un ou plusieurs groupes, et il est possédé des permissions. L'utilisateur peut jouer le rôle d'administrateur ou opérateur.
<b>Groupe</b>	Cette classe représente les groupes de permission auxquels appartient l'utilisateur et créés par l'administrateur. Chaque groupe est identifié par un nom, une description et l'objet de permission.

<b>Permission</b>	Cette classe représente les permissions liées au système. Chaque permission est caractérisée par un id, un nom et une description.
<b>Règle d’alerte</b>	Cette classe représente les règles d’alerte créées par l’utilisateur du système, Il est identifié par un id, un nom, une description, son état (utilisé ou non).

**TABLEAU 3.1 :** Description textuelle du -Gestion d'utilisateur –

### 3.2 Gestion des logs

Le tableau suivant décrit la gestion des logs.

<b>Classe</b>	<b>Description</b>
<b>Log</b>	Cette classe représente les logs de notre système.
<b>Action</b>	Cette classe représente une action effectuée par les utilisateurs dans les infrastructures.
<b>Infrastructure</b>	Cette classe représente les actifs d’où proviennent les logs situés dans un réseau, Chaque actif est caractérisé par un id, un nom et une adresse IP.
<b>Réseau</b>	Cette classe représente le réseau où les utilisateurs d’infrastructures font leurs actions. Il est identifié par un id, un nom et une adresse.
<b>Tableau de bord</b>	Il représente l’ensemble d’affichage de détails des logs .
<b>Alerte</b>	Elle représente les alertes potentielles qui menacent d’arriver

**TABLEAU 3.2 :** DESCRIPTION TEXTUELLE DU -GESTION DES LOGS -

## 4. Diagramme de cas d’utilisation (use case)

Le diagramme de cas d’utilisation représente un ensemble d’action qui est réalisé par le système et qui renvoie un résultat observable qui est outil pour l’acteur. Il permet de décrire les fonctionnalités du système, sans préciser comment elles seront implémentées.

Dans le cas de notre système, nous avons identifié principalement deux acteurs

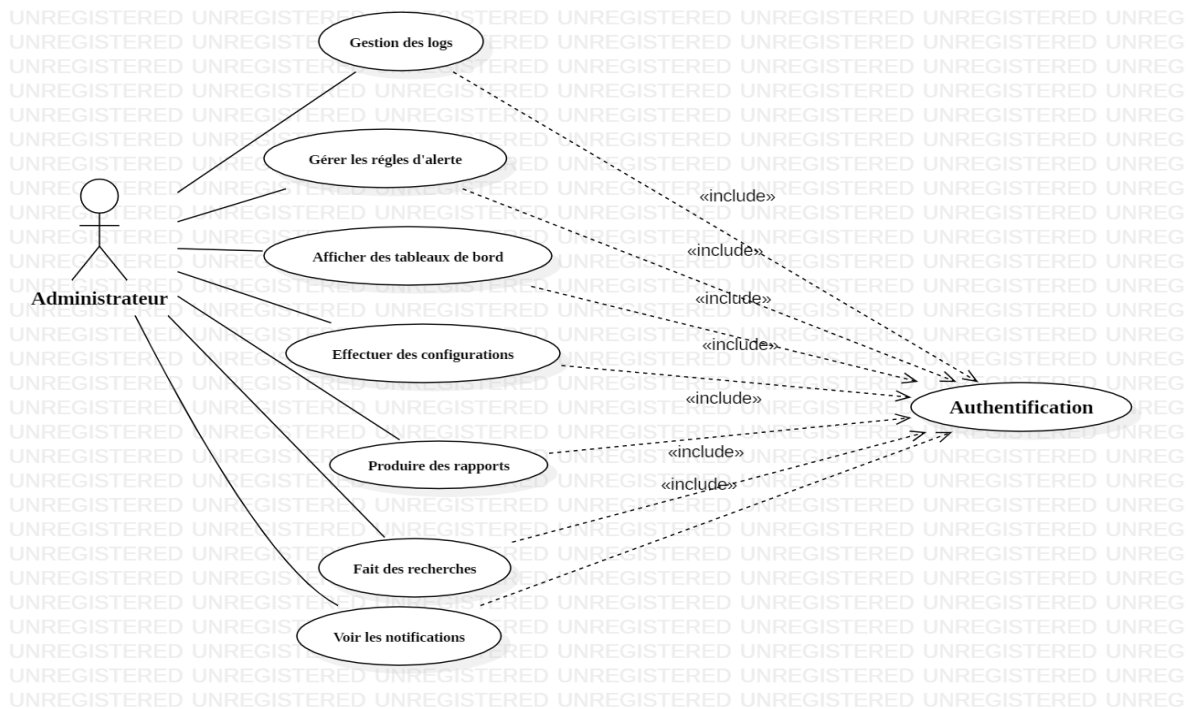
**Administrateur :**

- La Gestion des logs



- Gérer les règles d’alerte
- Afficher des tableaux de bord
- Effectuer des configurations
- Produire des rapports
- Fait des recherches
- Voir les notifications

La figure 4.1 représente le diagramme de cas d’utilisation associé à l'administrateur.

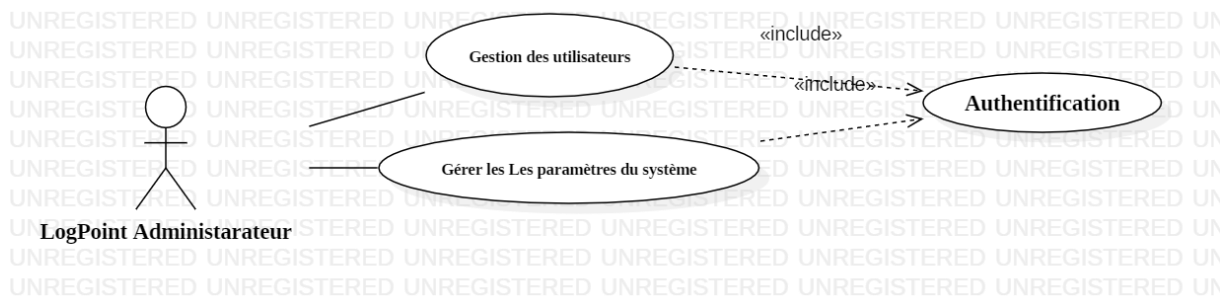


**Figure 4.1 :** diagramme de cas d’utilisation associé à l'administrateur.

### LogPoint Administrateur

- Gestion d’utilisateurs
- Gérer les paramètres du système

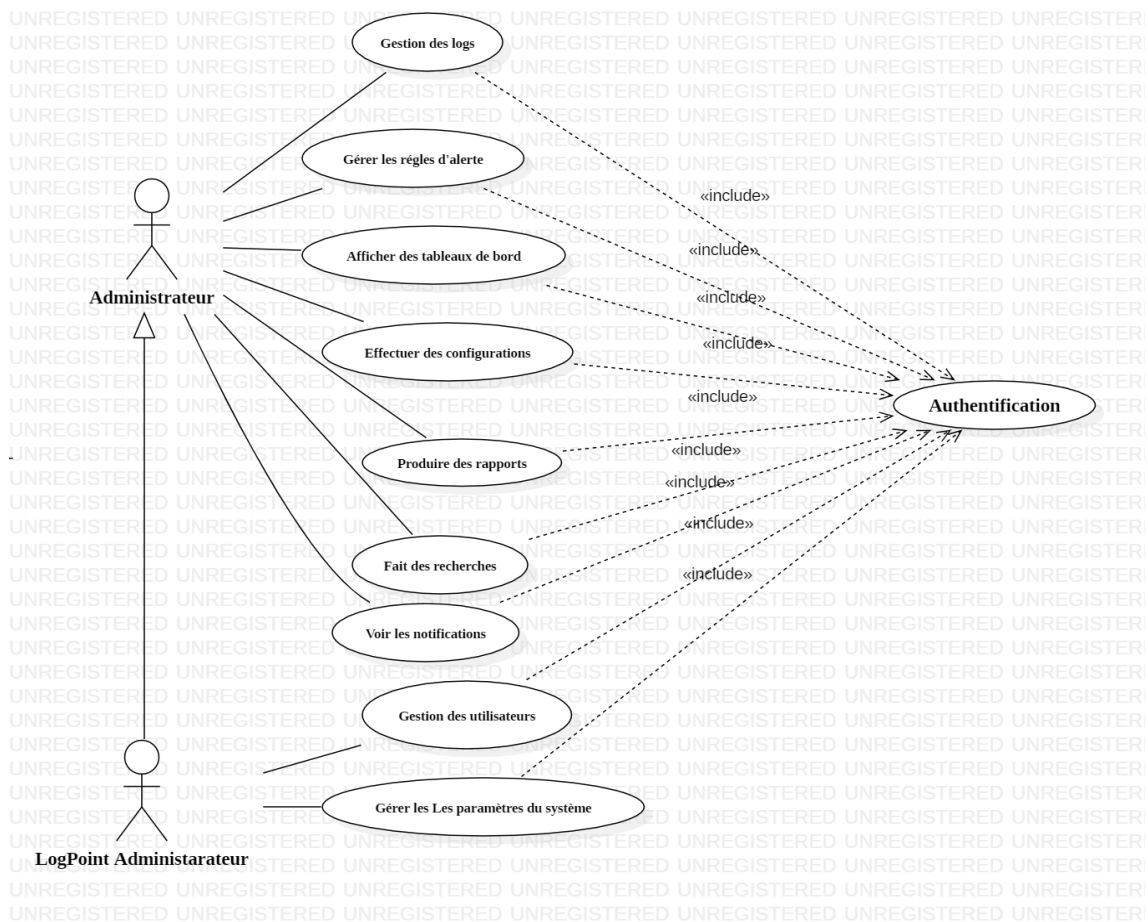
La figure 4.2 représente le diagramme de cas d’utilisation associé au LogPoint administrateur.



**Figure 4.2 :** Diagramme de cas d'utilisation associé au LogPoint administrateur.

Le LogPoint administrateur a les mêmes cas d'utilisation que l'administrateur, il existe donc une relation des spécialisations entre les deux acteurs.

La figure 4.3 représente le diagramme de cas d'utilisation globale de notre système qui rassemble tous les cas d'utilisations précédemment identifiées.



**Figure 4.3 :** diagramme de cas d'utilisation global de notre système.

## 4.1 Cas d'utilisation détaillé 'gestion des utilisateurs'

Dans cette section, nous allons décrire de façon détaillée un cas d'utilisation identifié précédemment en recensant de façon textuelle toutes les interactions entre les acteurs et le système afin de mieux comprendre le fonctionnement du système.

La figure 4.4 représente le cas d'utilisation "gestion des utilisateurs" qui montre la possibilité d'administrateur à gérer les groupes de permission et la consultation des listes d'utilisateurs et les groupes d'utilisateurs, après la consultation des utilisateurs peut ajouter ou supprimer ou bien modifier et même changer le mot de passe d'utilisateur, il fait la même avec les groupes d'utilisateurs.

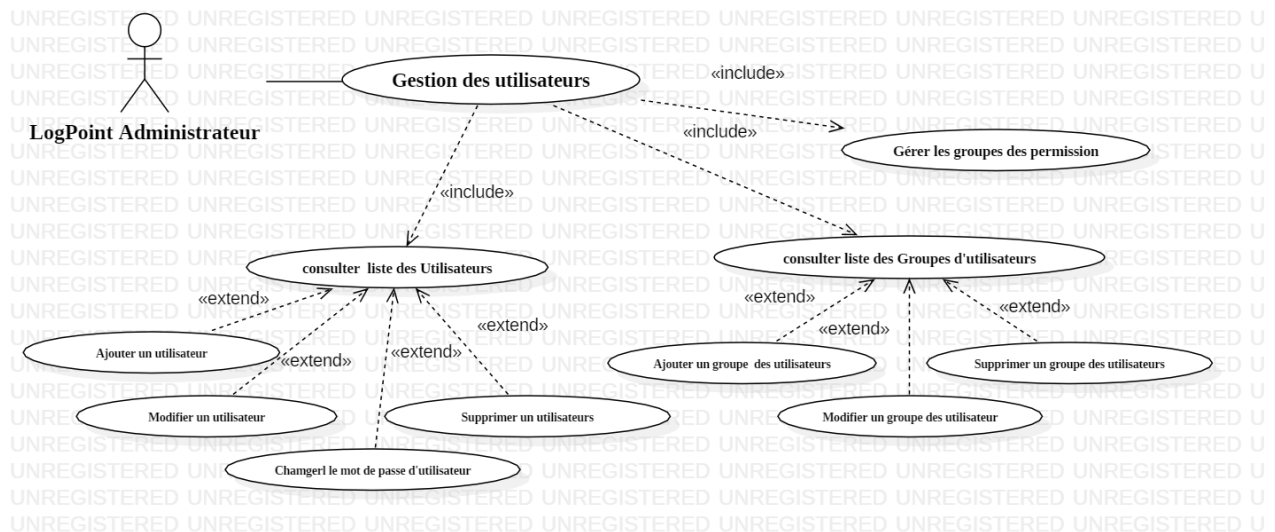


Figure 4.4 : le cas d'utilisation ' gestion des utilisateurs'.

### 4.1.1 Cas d'utilisation 'Gérer les utilisateurs : ajouter un utilisateur'

Ce use-case montre comment l'administrateur peut ajouter un utilisateur.

<b>Cas d'utilisation</b>	Ajouter un utilisateur.
<b>Résumé</b>	L'acteur ajoutait un nouvel utilisateur.
<b>Acteur</b>	LogPoint L'administrateur.
<b>Pré condition</b>	-L'acteur doit introduire des informations valides pour ajouter un utilisateur.
<b>Scénario nominal</b>	<ol style="list-style-type: none"> <li>1. L'acteur demande le formulaire d'ajout.</li> <li>2. L'acteur remplit le formulaire d'ajout.</li> <li>3. L'acteur valide et envoie le formulaire.</li> <li>4. Le système crée un utilisateur et renvoie un message confirmant l'action.</li> </ol>

<b>Scénario alternatif</b>	<ol style="list-style-type: none"> <li>1. Utilisateur existant.</li> <li>2. Les informations de l'utilisateur sont invalides.</li> <li>3. Un champ manque dans la saisie.</li> </ol>
<b>Post condition</b>	Un nouvel utilisateur est ajouté à la liste.

**TABLEAU 1.1 :** LA DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : AJOUTER UN UTILISATEUR' –

#### 4.1.2 Cas d'utilisation 'Gérer les utilisateurs : modifier un utilisateur'

Ce use-case explique comment se fait la mise à jour des informations des utilisateurs.

<b>Cas d'utilisation</b>	Modifier un utilisateur.
<b>Résumé</b>	L'acteur met à jour les informations de l'utilisateur.
<b>Acteur</b>	LogPoint administrateur.
<b>Pré condition</b>	-L'acteur doit introduire des informations valides pour la modification d'un utilisateur. -Utilisateur existant
<b>Scénario nominal</b>	<ol style="list-style-type: none"> <li>1. L'acteur demande le formulaire de modification.</li> <li>2. L'acteur met à jour les informations.</li> <li>3. L'acteur confirme la modification et envoie le formulaire.</li> <li>4. Le système valide les modifications et renvoie un message confirmant l'action.</li> </ol>
<b>Scénario alternatif</b>	<ol style="list-style-type: none"> <li>1. Les informations de l'utilisateur sont invalides.</li> <li>2. Un champ manque dans la saisie.</li> </ol>
<b>Post condition</b>	L'utilisateur possède de nouvelles informations.

**TABLEAU 4.2 :** LA DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : MODIFIER UN UTILISATEUR' -

#### 4.1.3 Cas d'utilisation 'Gérer les utilisateurs : Supprimer un utilisateur'

Ce use-case explique la suppression des utilisateurs .

<b>Cas d'utilisation</b>	Supprimer un utilisateur.
<b>Résumé</b>	L'acteur supprime un utilisateur.
<b>Acteur</b>	LogPoint administrateur.
<b>Pré condition</b>	-Utilisateur existant
<b>Scénario nominal</b>	<ol style="list-style-type: none"> <li>1. L'acteur demande l'action de suppression.</li> <li>2. L'acteur valide l'action de suppression.</li> <li>3. Le système renvoie un message confirmant l'action.</li> </ol>
<b>Post condition</b>	Un utilisateur supprimé.

**TABLEAU 4.3 : LA DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : SUPPRIMER UN UTILISATEUR' -**

#### 4.1.4 Cas d'utilisation 'Gérer les utilisateurs : changer le mot de passe '

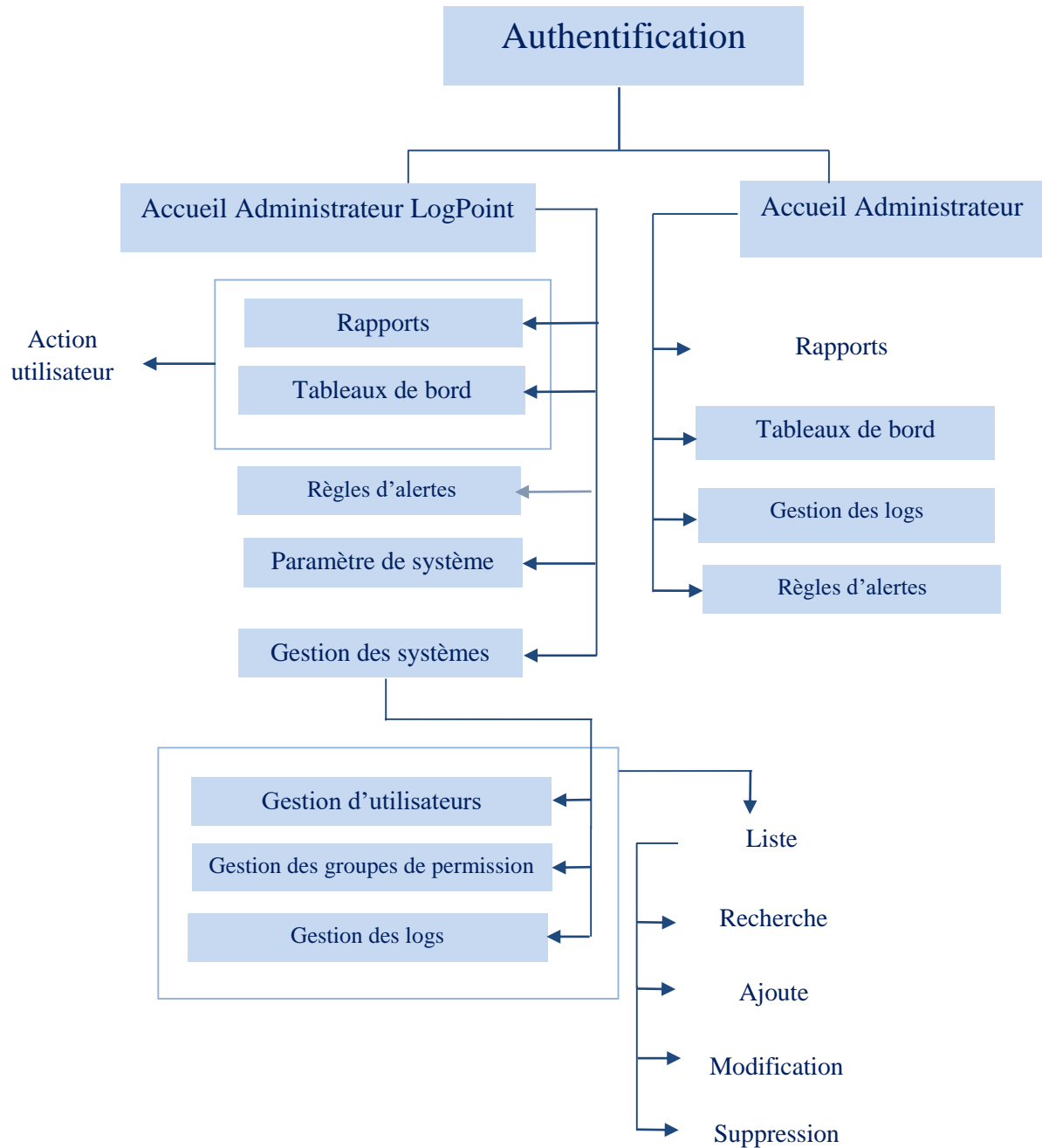
Ce use-case montre comment l'administrateur peut changer le mot de passe d'utilisateur.

<b>Cas d'utilisation</b>	Changer le mot de passe d'utilisateur.
<b>Résumé</b>	L'acteur change le mot de passe d'utilisateur.
<b>Acteur</b>	LogPoint L'administrateur.
<b>Pré condition</b>	-Utilisateur existant -L'acteur doit donner un mot de passe valide.
<b>Scénario nominal</b>	<ol style="list-style-type: none"> <li>1. L'acteur demande le formulaire de modification de mot de passe.</li> <li>2. L'acteur remplit le formulaire de modification.</li> <li>3. L'acteur valide et envoie le formulaire.</li> <li>4. Le système change le mot de passe et renvoie un message confirmant l'action.</li> </ol>
<b>Scénario alternatif</b>	<ol style="list-style-type: none"> <li>1. Le mot de passe ne change pas.</li> <li>2. Mot de passe invalide.</li> <li>3. Un champ manque dans la saisie.</li> </ol>
<b>Post condition</b>	Mot de passe changé pour un utilisateur.

**TABLEAU 4.4 : LA DESCRIPTION TEXTUELLE DU - CAS D'UTILISATION 'GERER LES UTILISATEURS : CHANGER LE MOT DE PASSE D'UTILISATEUR' -.**

## 5. Diagramme de navigation

La figure 5.1 représente un diagramme de navigation de notre SIEM LogPoint et donne une vision globale sur notre système et la relation entre ses différentes interfaces.



## 6. Utilisateurs, rôles et responsabilités

Nous avons déjà évoqué l'importance de la ressource humaine quant à la réussite du projet SIEM (ou SOC). En effet, les compétences en termes de sécurité, la maîtrise du fonctionnement de la solution SIEM et la maîtrise des processus de traitement et réponses aux incidents ne peuvent être dissociées du projet global relatif à une implémentation réussie du SIEM.

A cet effet, nous avons convenu de fournir un bref aperçu du personnel de sécurité amené à prendre en charge le dispositif SIEM de manière opérationnelle et effective.

- **Opérateurs de supervision (tier-1)**

Le rôle des opérateurs (tiers-1) consiste à superviser tous les événements de sécurité du SI : les menaces externes et internes, les vulnérabilités sur les actifs, les infections des *Endpoint*, les accès non autorisés, etc., constatés sur les tableaux de bord et les indicateurs du SIEM en vue d'effectuer un premier diagnostic et aiguiller par la suite les incidents avérés. Ils assurent ainsi un niveau élémentaire dans le processus de traitement des incidents.

Si l'opérateur constate qu'une alerte ou un événement suscite plus d'attention et d'analyse, ce dernier est escaladé au personnel tiers-2, à travers un ticket, selon la procédure de gestion d'incidents.

- **Analyste tier-2**

L'analyste tier-2 correspond au personnel de sécurité de l'entreprise. Son rôle principal et spécifique est de répondre aux incidents de sécurité. Pour ce faire, il analyse et enquête en profondeur sur les menaces signalées ou constatées. Il neutralise ensuite ces menaces et résout les problèmes en apportant l'assistance nécessaire aux équipes métiers, selon le périmètre impacté. Le personnel de sécurité tier-2 prend en charge, à la fois, les incidents remontés par l'équipe de supervision mais aussi les alertes reçues directement par le système correspondant au niveau de sévérité alloué à ce dernier.

Le personnel tier-2 prend en charge l'amélioration des processus de traitement d'incidents et affine et ajuste constamment les règles de détection et de sécurité du SIEM en maintenant une veille constante de l'environnement dans lequel évolue l'entreprise et ses métiers.

- **Analyste tier-3 (expertise)**

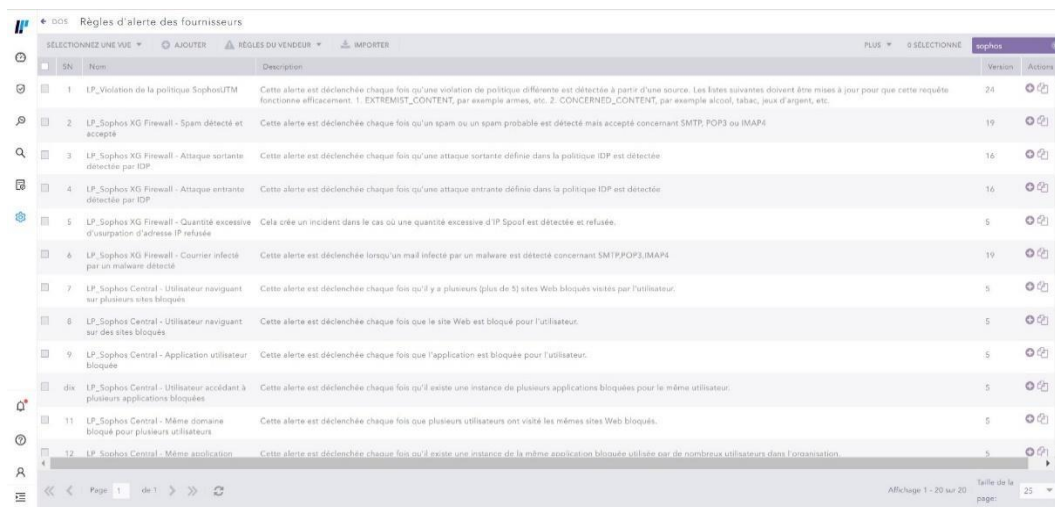
Dans le cas où l'incident s'avère complexe, critique ou large et dépasse les capacités ou les compétences du personnel tier-2, ce dernier peut avoir recours à des experts internes (autres compétences internes de l'entreprise) ou externes (sous-traitants, consultants, etc.) pour lui apporter une assistance supplémentaire permettant de traiter l'incident avec les moindres coûts/impact et délais.

En raison de la complexité et de la sophistication de plus en plus élevées des menaces, l'entreprise entretient, globalement, des relations avec des partenaires et des experts en matière de sécurité, ce qui permet de fédérer les efforts contre les risques et les cyber-menaces.

## 7. Traitement des incidents

Tout d'abord, pour être en mesure de gérer des alertes et des incidents, nous devons disposer de règles déterminant l'origine de ces alertes, appelées les règles d'alerte. À notre niveau de conception, nous n'avons pas besoin de créer de nouvelles règles, car il existe déjà une liste de règles prédéfinies dans l'application. Par exemple, la règle 'LP Connexion réseau à un serveur suspect' déclenche une alerte de pare-feu Sophos à chaque fois qu'elle détecte une communication entre les hôtes et les domaines mentionnés dans la liste de la requête de cette règle. De même, la règle 'Erreurs HTTP excessives LP Défaut' déclenche une alerte chaque fois que 20 erreurs HTTP sont détectées par le pare-feu.

Voici une figure montre la liste des règles prédéfinies pour le déclenchement d'une alerte à partir du pare-feu Sophos.



SN	Nom	Description	Version	Actions
1	IP_Violation de la politique SophosJTM	Cette alerte est déclenchée chaque fois qu'une violation de politique d'filtrage est détectée à partir d'une source. Les listes suivantes doivent être mises à jour pour que cette requête fonctionne efficacement. 1. EXTREMIST_CONTENT, par exemple armes, etc. 2. CONCERNED_CONTENT, par exemple alcool, tabac, jeux d'argent, etc.	24	
2	IP_Sophos XG Firewall - Spam détecté et accepté	Cette alerte est déclenchée chaque fois qu'un spam ou un spam probable est détecté mais accepté concernant SMTP, POP3 ou IMAP4	19	
3	IP_Sophos XG Firewall - Attaque sortante détectée par IDP	Cette alerte est déclenchée chaque fois qu'une attaque sortante définie dans la politique IDP est détectée.	16	
4	IP_Sophos XG Firewall - Attaque entrante détectée par IDP	Cette alerte est déclenchée chaque fois qu'une attaque entrante définie dans la politique IDP est détectée.	16	
5	IP_Sophos XG Firewall - Quantité excessive d'usurpation d'adresse IP relâchée	Cela crée un incident dans le cas où une quantité excessive d'IP Spoof est détectée et relâchée.	5	
6	IP_Sophos XG Firewall - Courrier infecté par un malware détecté	Cette alerte est déclenchée lorsqu'un mail infecté par un malware est détecté concernant SMTP,POP3,IMAP4	19	
7	IP_Sophos Central - Utilisateur navigant sur plusieurs sites bloqués	Cette alerte est déclenchée chaque fois qu'il y a plusieurs (plus de 5) sites Web bloqués visités par l'utilisateur.	5	
8	IP_Sophos Central - Utilisateur navigant sur des sites bloqués	Cette alerte est déclenchée chaque fois que le site Web est bloqué pour l'utilisateur.	5	
9	IP_Sophos Central - Application utilisateur bloquée	Cette alerte est déclenchée chaque fois que l'application est bloquée pour l'utilisateur.	5	
dix	IP_Sophos Central - Utilisateur accidenté à plusieurs applications bloquées	Cette alerte est déclenchée chaque fois qu'il existe une instance de plusieurs applications bloquées pour le même utilisateur.	5	
11	IP_Sophos Central - Même domaine bloqué pour plusieurs utilisateurs	Cette alerte est déclenchée chaque fois que plusieurs utilisateurs ont visité les mêmes sites Web bloqués.	5	
12	IP_Sophos Central - Même application	Cette alerte est déclenchée chaque fois qu'il existe une instance de la même application bloquée utilisée par de nombreux utilisateurs dans l'organisation.	5	

Figure 6.1 : La liste des règles prédéfinie.

Le délai entre la détection d'une menace et la réponse à celle-ci doit être le plus réduit possible. En effet, l'impact d'une attaque ou d'une vulnérabilité sur le SI est étroitement lié à la rapidité de s'exécuter.

LogPoint fournit une structure complète qui intègre les rôles des différents utilisateurs qui interagissent, soit de manière directe avec le SIEM tels que les administrateurs de la solution, soit les analystes de sécurité, les opérateurs de supervision et les correspondants de sécurité relatifs aux différents métiers de l'entreprise.



Incident User Groups		
+ ADD		
<input type="checkbox"/>	S.N.	Name
<input type="checkbox"/>	1	User Account Administrator
<input type="checkbox"/>	2	LogPoint Administrator
<input type="checkbox"/>	3	Suppervion

**Figure 6.2 :** La structure de traitement d'incidents.

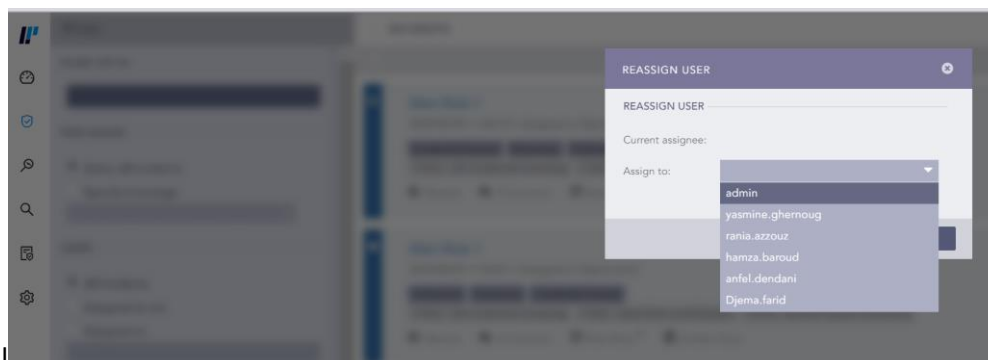
- **Suivi des alertes et incidents**

Comme évoqué plus haut, les opérateurs de supervision ont, comme première tâche, de superviser les événements et les alertes de sécurité. Ils doivent disposer, à la fois d'un accès aux tableaux de bords du SIEM, mais aussi à l'interface de gestion d'incidents qui leur permettent de créer un ticket, l'escalader, effectuer son suivi et sa résolution ainsi que sa documentation en vue de futurs usages.

The screenshot shows the 'INCIDENTS' management interface. On the left is a 'Filter' sidebar with sections for NAME (OR ID), TIME RANGE (with radio buttons for 'Select all incidents' and 'Specify timerange'), USERS (with radio buttons for 'All Incidents', 'Assigned to me', and 'Assigned to'), RISK (with checkboxes for Critical, High, Medium, and Low), and ATTACK CATEGORY. The main area displays a list of incidents under the heading 'INCIDENTS'. Three incident cards are visible, each titled 'Alert Rule 1' and assigned to 'Djema.farid'. The first card is dated 2023/05/25 11:44:10 and has tags for 'Credential Access', 'Discovery', and 'Collection'. The second card is dated 2023/05/25 11:44:01 and has tags for 'Collection', 'Discovery', and 'Credential Access'. The third card is dated 2023/05/25 11:43:02 and is marked as 'Resolved'. Each card includes a list of T1003-T1018 tags, a 'Resolve' button, a comment count, and options for 'View Data' and 'Incident Data'.

**Figure 6.2 :** L'interface Suivi des alertes et incidents.

En cas de besoin, l'alerte est transférée au niveau du support adéquat selon l'arborescence des ressources et la procédure de traitement des incidents.



**Figure 6.3:** L'interface Reassign user.

## Conclusion

Le chapitre conception nous a permis d'identifier l'environnement nécessaire au déploiement du SIEM en termes d'architecture, sources de logs, utilisateurs et processus de fonctionnement.

Nous avons pu découvrir l'avantage de la planification et de la prise en charge des différents éléments qui impactent de la réussite du cycle de vie du produit SIEM sur ces deux principales phases : la phase projet et la phase exploitation.

# Chapitre 3. Déploiement et Mise en service du SIEM LogPoint

## 1. Implémentation de la Solution

### 1.1. Environnement de travail

Pour effectuer l'installation de LogPoint en milieu de production, nous avons recommandé d'utiliser du matériel représentatif de notre environnement de production. Ce matériel doit respecter ou dépasser les spécifications de capacité recommandées ci-dessous :

<b>CPU</b>	Minimum Quad-core
<b>Mémoire RAM</b>	Minimum 8 GB
<b>Disque</b>	Minimum 150 GB

**TABEAU 1.1 :** L'ENVIRONNEMENT DE TRAVAIL.

## 1.2. Déploiement, configuration et mise en service

### 1.1.1. Installation de LogPoint

1. Nous avons démarré le système avec la version LogPoint ISO v7.2.1 sur l'environnement virtuel VMWARE. Tout d'abord, nous avons demandé au fournisseur LogPoint de nous fournir une plateforme qui réponde à nos besoins d'intégrer un nombre limité d'actifs. Après avoir reçu de fichier d'installation, nous avons téléchargé sur une interface virtuelle SEV NSX au niveau du DATA-CENTER de l'entreprise, puis nous avons choisi l'interface réseau à configurer pour donner l'accès à cette application à partir du réseau local en effectuant l'étape suivante pour enfin lancer l'installation
2. Ensuite, nous avons configuré le **Sous-réseau**, l'**Adresse**, la **Passerelle**, le **Nom de serveur** et le **Domaine de recherche**.

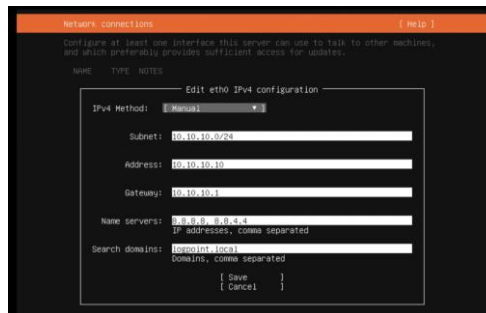
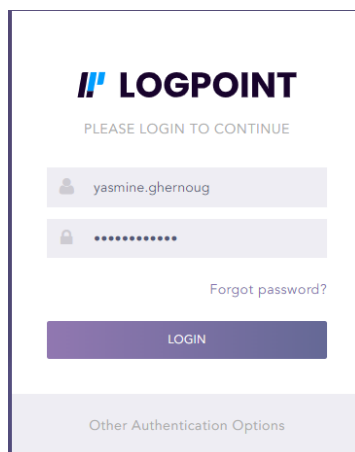


Figure 1.1 : La configuration de la connexion au réseau

### 1.1.2. Accès à l'interface Web LogPoint

Une fois l'installation terminée, nous avons utilisé les informations d'authentification pour accéder à l'interface utilisateur de LogPoint à partir du réseau local, nous avons exploité la commande **ifconfig** qui affiche l'adresse IP de la machine installée. Ensuite, nous avons modifié et saisi les nouvelles informations d'identification ( nom d'utilisateur et mot de passe modifiés ) comme il est montré sur la figure 1.2 ci-dessous.



**Figure 1.2 :** Capture d'écran de l'interface de connexion.

- Nous avons besoin d'une licence LogPoint valide pour l'utiliser, La licence contient les détails du produit acheté, le nombre de sources des logs qu'il peut gérer et sa date d'expiration.

### 1.1.3. Application de la licence

Nous avons téléchargé la **clé de licence** fournie par le fournisseur lui-même, ensuite nous avons reçu et ajouté la licence.



**Figure 1.3 :** L'ajout une licence.

Pour synchroniser les paramètres de temps dans le système, nous avons activé le serveur NTP qui est responsable d'égalité de temps entre le reçu de log et le temps d'alerte au cas d'une action anormale.

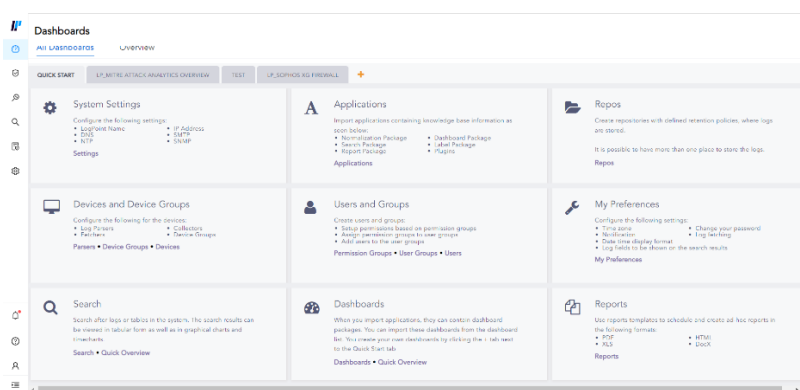
Voici la liste des ports à ouvrir selon l'architecture utilisée

Port/protocole	RAISON
<b>20 &amp; 21</b>	Collecteur FTP et récupérateur
<b>22</b>	Connexion SSH ET SCP récupérateur
<b>80 &amp; 443</b>	HTTP connexion
<b>123</b>	NTP
<b>161 &amp; 162</b>	SNMP caractéristiques
<b>389</b>	LDAP source d'enrichissement
<b>514 &amp; 6514 (SSL)</b>	Syslog collector
<b>1193 and 1194</b>	Connection entre les machines LogPoint

<b>1311</b>	Fonctions consolidées pour la gestion des serveurs locaux et en réseau
<b>6161 &amp; 6162 (SSL)</b>	Snare collecteur
<b>6343</b>	SFlow collecteur
<b>6379</b>	Redis
<b>9001</b>	Netflow collecteur
<b>18000</b>	Serveur web
<b>27017</b>	Base de données
<b>6400, 6900-7099</b>	LogPoint Collecteur

**TABLEAU 1.2 : LA LISTE DES PORTS A OUVRIR.**

Voici l'Interface Web LogPoint figure 1.4 :



**Figure 1.4 : L'interface Web LogPoint.**

Avec l'interface web, nous avons pu effectuer les configurations nécessaires au bon fonctionnement du système, telles que la configuration des paramètres du système pour les mises à jour, l'ajout ou le renouvellement des licences, la configuration des applications pour le rapiéçage des logs, la configuration des utilisateurs pour l'analyse et l'alerte des actions anormales dans le système d'information de l'entreprise, les use cases, etc.

## 2. Configuration des utilisateurs

### 2.1. Création des utilisateurs

Il existe déjà l'utilisateur admin de l'application qui est responsable d'intégrer les actifs, faire les mises à jour, ajouter les règles d'alerte qui sont responsables de détecter toute action anormale. Nous avons créé des nouveaux utilisateurs et les avons ajoutés dans un groupe d'utilisateurs des administrateurs, puis les activer et enfin modifier leurs mots de passe (voir figure 2.1).

S.N.	Username	Name	Email	User Group	Last Login	Actions
1	anfel.dendani	Anfel Dendani	anfel.dendani@icosnet.com	LogPoint Administrator	2023/05/23 14:57:02	[Icons]
2	hamza.baroud	Hamza Baroud	hamza.baroud@icosnet.com	LogPoint Administrator	2023/05/24 17:41:08	[Icons]
3	rania.azzouz	rania azzouz	azzouzeria91@gmail.com	LogPoint Administrator		[Icons]
4	yasmine.ghernoug	yasmine ghernoug	ghernougyasmine09@gmail.com	LogPoint Administrator	2023/05/25 10:02:45	[Icons]
5	admin	Admin Admin	admin@logpoint.local	LogPoint Administrator	2023/05/21 10:21:07	[Icons]

**Figure 2.1** : prise d'écran des utilisateurs.

## 2.2. Création groupes d'utilisateurs

Il existe deux groupes d'utilisateurs (voir figure 2.2) par défaut **LogPoint Administrateur** qui a les privilèges élevés et **User Account Administrateur** qui possède l'accès à tous les privilèges à part les paramètres du système. Nous avons ajouté un autre groupe qui s'appelle **Supervision** dont le but est de faire l'agent au niveau des logs c'est-à-dire il ne possède l'accès qu'à la lecture des logs collectés.

S.N.	Name	Description	Actions
1	Suppervion	Suppervion Agent	[Icons]
2	User Account Administrator	The user group has all permissions except the system related permissions that the LogPoint Administrators group has.	[Icons]
3	LogPoint Administrator	This user group is highly privileged user group. The users within this group has access to the most restricted system related areas- System Settings, LogPoint License, Software Updates, Security Updates, Application Installation and Backup/Restore.	[Icons]

**Figure 2.2** : Les groupes d'utilisateurs.

## 2.3. Configuration des groupes de permissions :

Il existe deux groupes de permissions qui sont le groupe operator et groupe admin, ces groupes nous permettent de contrôler les niveaux d'accès des utilisateurs. Étant donné le nombre limité d'utilisateurs créés, nous pouvons choisir de gérer les accès des utilisateurs un par un. Par conséquent, il n'est pas nécessaire de les ajouter à ces deux groupes(voir figure 2.3).

S.N.	Name	Description	Actions
1	operator	Operator	[Icons]
2	admin	Administrator	[Icons]

**Figure 2.3** : Les groupes de permission

- **Autorisation admin :**

La figure 2.4 montre les trois permissions de l'utilisateur admin : lire les logs, les notifications et tous les éléments affichés sur la plate-forme, et créer et supprimer les utilisateurs ....

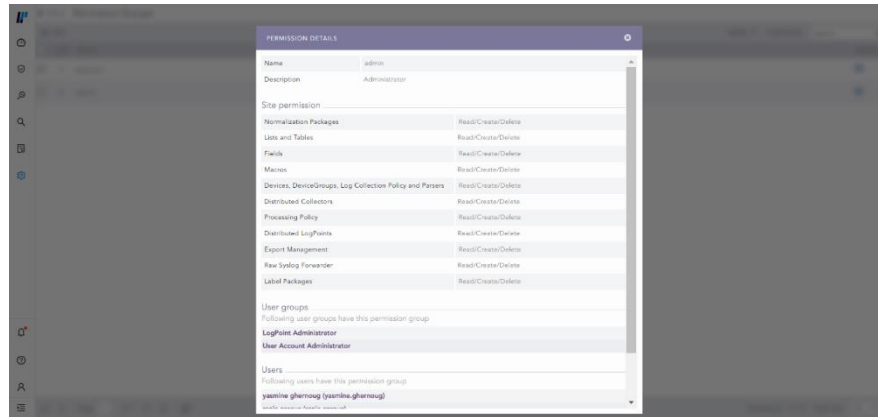


Figure 2.4 : Les permissions que l’admin peut faire.

- **Autorisation par opérateur**

Qui a uniquement accès à la lecture des logs affichés sur l'application.

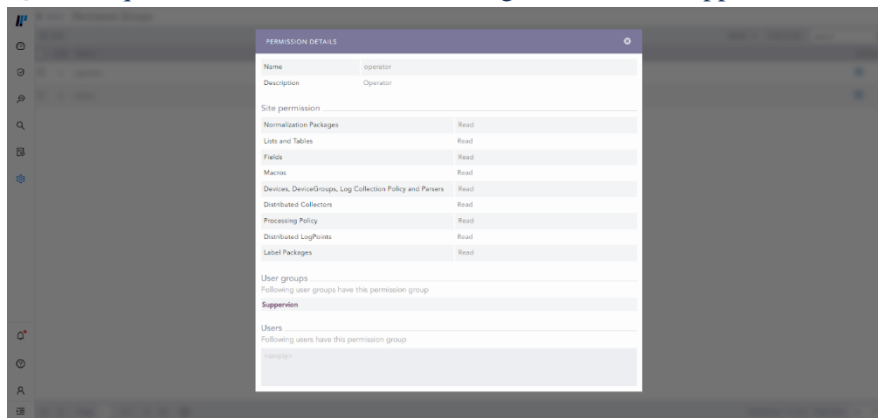


Figure 2.5 : Les permissions que l’opérateur peut faire.

## 3. Intégration et mise en production

### 3.1 Implémentation des sources de logs

Selon un diagnostic général fait au niveau du département de sécurité de l’entreprise, nous avons identifié quelques actifs critiques à intégrer en priorité.

Nous avons choisi ces trois équipements (le pare-feu SOPHOS, Routeur PE1 CA1 Alger et un serveur d’authentification beyondtrust) afin de toucher tous les aspects de sécurité au niveau du département.

Avant d’entamer l’intégration des actifs, nous devons faire des configurations sur certaines politiques afin de recevoir les logs des actifs comme montré sur la figure 3.1.

1. **Repos**
2. **Politique de routage**
3. **Politique de normalisation**
4. **Politique d’enrichissement**
5. **Politique de traitement**

- 6. La configuration des collecteurs distribués
- 7. Configuration des *parsers* ou les Analyseurs
- 8. Politique de collecte
- 9. Intégration des actifs

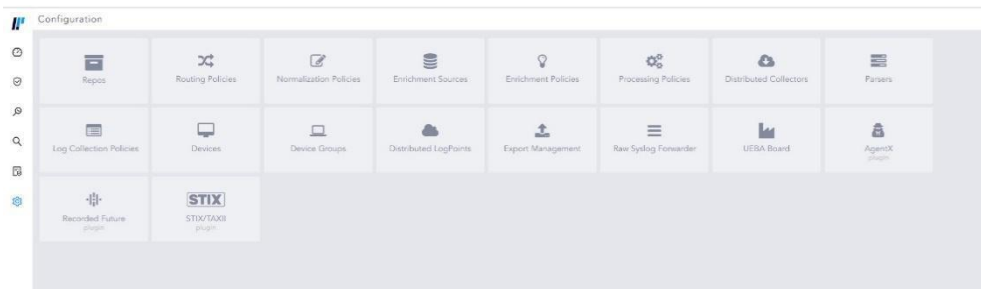


Figure 3.1 : Les politiques à configurer.

- **Le pare-feu SOPHOS :**

- 1. REPOS

On commence par la configuration des REPOS où les dépôts ou les logs devraient être stockés, nous avons opté sur le dépôt par défaut à cause de l'espace de stockage qui était limité.

- 2. Politique de routage

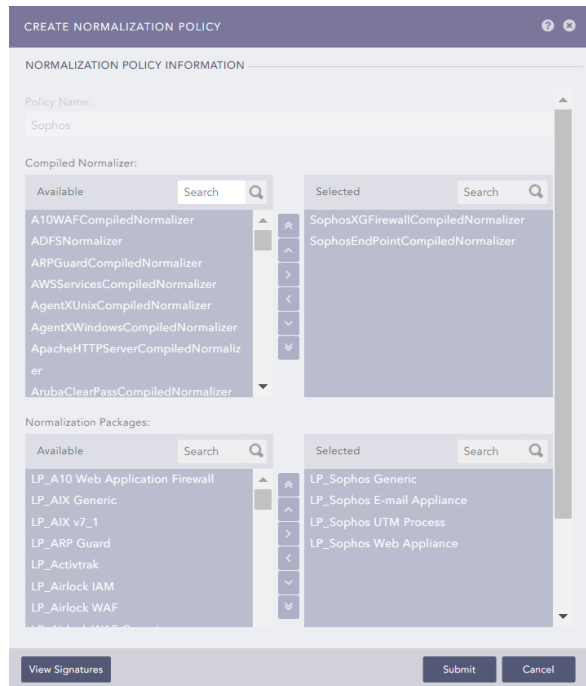
Qui dirigent les journaux générés par le pare-feu pour qu'ils soient stockés au niveau des dépôts (REPOS) par défaut.

- 3. Politique de normalisation

Ce sont des règles prédéfinies pour chaque type d'actif, ayant pour objectif d'unifier le format des journaux bruts reçus de diverses sources, comme illustré dans la figure 3.2. Par exemple, la règle de normalisation pour le pare-feu Sophos, 'Sophos Endpoint Compiled', a pour mission d'unifier les journaux reçus de la source Endpoint, permettant ainsi à l'analyste d'analyser et de déduire les alertes provenant de cette source. De même, d'autres règles ont été établies, mais elles ne sont pas compilées, car ce pare-feu ne reçoit pas de journaux provenant d'autres sources que ces deux mentionnées.

En ce qui concerne le package de normalisation, il s'agit de différents ensembles de politiques. Ainsi, chaque ensemble de règles similaires est regroupé au sein du même ensemble."





**Figure 3.2 :** La politique de normalisation.

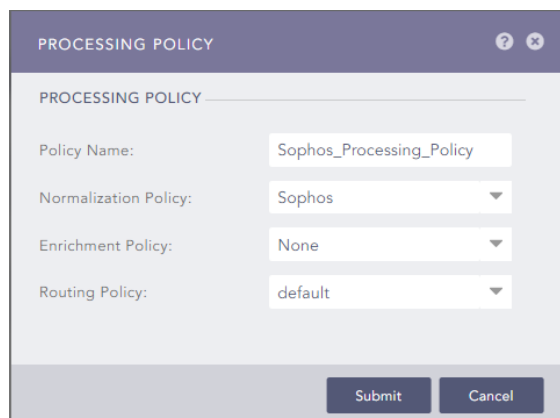
Configuration des sources d'enrichissement, c'est-à-dire les racines d'où viennent les logs comme l'UEBA qui aide à détecter les comportements anormaux et déclenche une alerte. Dans notre cas, l'entreprise ne possède pas cette technique, nous n'avons donc pas besoin de la configurer.

#### **4. Politique d'enrichissement**

Ces informations détaillées sont ajoutées à chaque log dans le but d'éviter toute confusion entre les journaux qui sont vraiment similaires. Elles permettent à l'analyste d'analyser ces journaux et de détecter les actions anormales. Nous n'avons pas configuré cette politique car nous ne recevons des logs que de trois actifs intégrés.

#### **5. Politique de traitement**

Cette politique regroupe les deux politiques précédentes en stockant ces deux dernières dans un modèle de politique de traitement, afin de ne pas avoir à refaire le travail chaque fois que nous devons configurer le même type d'actifs.



**Figure 3.3 :** La Politique de traitement.

### 6. La configuration des collecteurs distribués

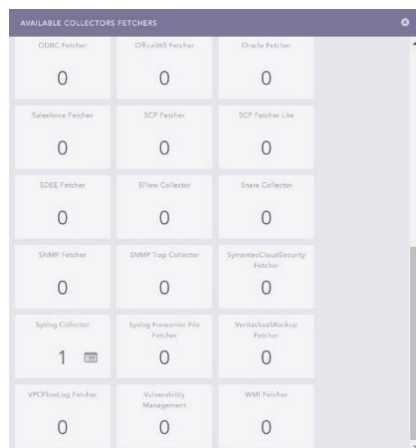
Qui sont dispatchés dans chaque application logpoint déployée et distribuées dans un territoire disant national pour centraliser les logs dans une application principale quelque part dans les réseaux des entreprises de même territoire, Cette configuration n'a pas été faite car nous avons déployé une seule application dans le réseau d'entreprises ICOSNET Alger.

### 7. Configuration des parsers ou les Analyseurs

Pour analyser les données entrantes et en extraire chaque message de journal.

### 8. Politique de collecte

Ce sont des collecteurs et les récupérateurs des logs à partir des différentes sources, nous avons configuré le collecteur SYSLOG qui est responsable de collecter les logs d'après le pare-feu Sophos qui est du type actif système d'où le SYSLOG est responsable de la collection des logs ce type d'actif.



**Figure 3.4 :** La politique de collecte.

### 9. Intégration de pare-feu Sophos

Après toute une procédure des configurations, là où nous avons intégré le pare-feu Sophos dans la plateforme et nous avons commencé à recevoir ces logs, voici la figure 3.4 montre le pare-feu intégré dans LogPoint et la date des derniers logs reçus avant cette prise d'écran.

S/N	Name	Address	Device Group	Log Collection Policy	Last Log Received	Actions
1	localhost	127.0.0.1,::1	linux		2023/05/26 09:53:01	
2	Beyondtrust	10.250.13.2	linux		N/A	
3	Jumpsta_Srv_Windows	192.168.101.179	windows	Windows_Log_Collection_Policy	2023/05/26 09:50:56	
4	sophos_Firewall	10.250.13.17	Firewall	Sophos_policy_Firewal	2023/05/26 09:57:52	
5	Router_PE1_CA1_Alger	172.31.1.203	Routers_Switch	Router_Log_Policy	2023/05/26 09:42:04	

**Figure 3.5 :** La Liste des actifs intégrés.

▪ **Routeur Router\_PE1\_CA1\_alger :**

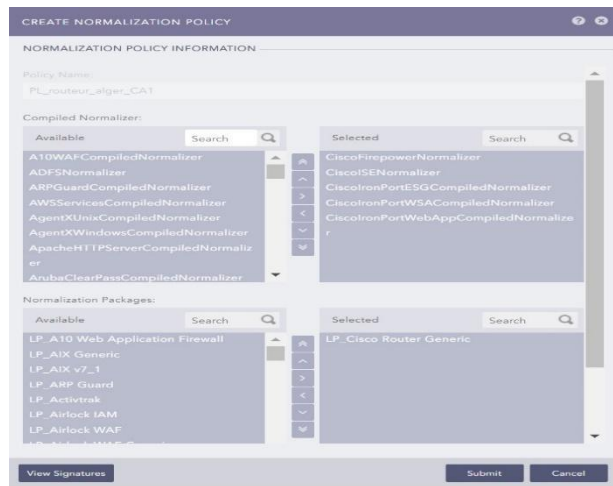
D’après le premier actif intégré : le Sophos, nous avons appris que nous avons quatre politiques principales à configurer chaque fois avant d’intégrer un actif de type système comme le routeur et le pare-feu et les autres configurations reste toujours les mêmes pour tous les autres actifs de même type, ce niveau nous sommes passé directement à ces trois politiques suivant les étapes mentionnées ci-dessous.

**1. Politique de routage**

Qui conduisent les logs générés d’après le routeur pour que ce stock au niveau des dépôts (repos) par défaut.

**2. Politique de normalisation**

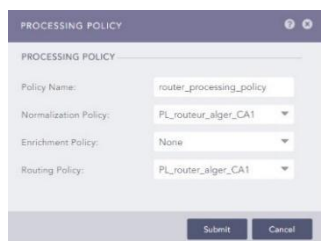
Voici la figure ci-dessous montre la politique de normalisation faite pour le routeur Cisco, dont chaque règle est responsable d’unifier le format des logs reçus de chaque port sélectionné comme il est mentionné.



**Figure 3.6 :** La politique de normalisation de routeur.

**3. Politique de traitement**

Une politique qui regroupe les deux derniers politiques et les fusionne pour le même type d’actif à intégrer plus tard.



**Figure 3.7 :** La politique de traitement des routeurs.

#### **4. Politique de collecte**

En dernier nous avons configuré la politique de collecte de routeurs pour qu'il puisse collecter et récupérer les journaux d'après cet appareil de type système, De cela il a besoin d'un collecteur SYSLOG commence le pare-feu Sophos (**figure 3.4**).

- Enfin nous avons pu intégrer le routeur dans la plate-forme pour recevoir des logs d'après eux. La figure 3.4 Ci-dessus montre le routeur intégré dans LogPoint et la date des derniers logs reçus avant la prise d'écran.

##### **▪ Serveur d'authentification beyondtrust**

Ce serveur permet de donner l'accès des serveurs aux utilisateurs sans donner le mot de passe pour accéder et en même temps un outil qui aide à surveiller les événements que l'utilisateur peut faire dans ces serveurs. Ce type d'actif a deux dispositifs à intégrer, un serveur du type Windows qui est responsable de l'accès au serveur et un autre serveur de type Linux, responsable de la configuration de l'accès de ces utilisateurs.

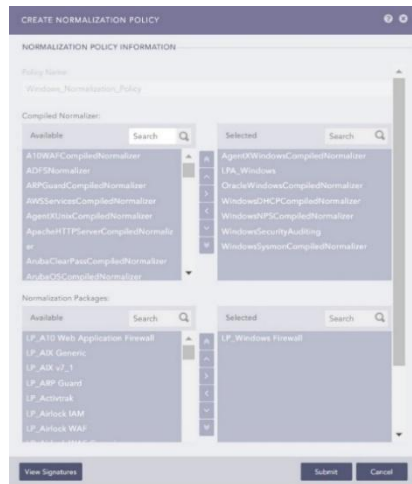
- Nous avons commencé la configuration de serveur de type Windows et, comme mentionné plus tôt, nous avons quatre configurations principales à réaliser à chaque intégration d'un nouvel actif. Aussi, la configuration des autres politiques reste la même.

#### **1. Politique de routage**

Qui dirigent les journaux générés par le pare-feu pour qu'ils soient stockés au niveau des dépôts (REPOS) par défaut.

#### **2. Politique de normalisation**

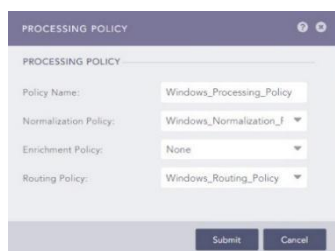
Ce sont des règles compilées afin d'unifier chaque type des journaux reçus depuis un port sélectionné pour la réception des logs, la figure ci-dessous montre les règles compilées pour ce serveur.



**Figure 3.8 :** La Politique de normalisation de serveur.

### 3. Politique de traitement

Nous avons configuré la politique de traitement pour ce serveur de manière à le maintenir comme un modèle, de sorte que l'intégration des autres actifs de même type ne nécessite pas de parcours de configuration complet.

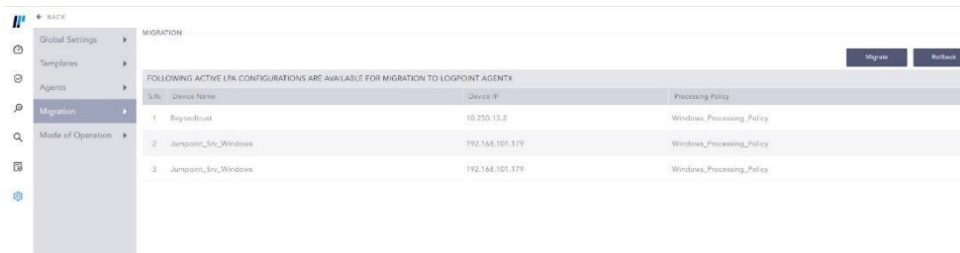


**Figure 3.9 :** La politique de traitement de serveur.

### 4. Politique de collecte

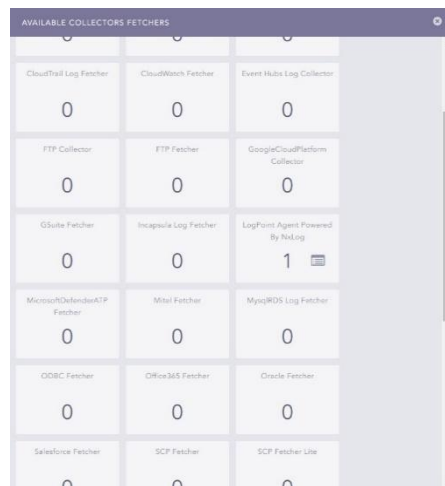
La politique de collecte de serveur qui est un actif du type WINDOWS et non pas de type système comme les deux derniers actifs intégrés déjà, De cela il a besoin d'un agent de LogPoint s'appelle **AgentX** qui fait collecter et récupérer les logs et les envoyés vers LogPoint comme il figure sur la figure 3.10.

- ✓ Tout d'abord nous avons installé l'**agentx** LogPoint depuis le site officiel de Log Point.
- ✓ Ensuite, nous avons fait migrer cet agent juste après son activation vers la plate-forme.



**Figure 3.10 : La Migration Agent logPoint.**

- ✓ Nous avons ajouté le récupérateur des logs, représenté par l'agent du nom de « LogPoint Agent Powered by NxLog » qui récupère les journaux du serveur WINDOWS et les envoie à l'application Log Point.



**Figure 3.11 : L' Ajout du récupérateur des logs**

- Deuxièmement, nous avons configuré le serveur Linux de type système donc nous avons utilisé une procédure de configuration similaire au routeur Cisco ou au pare-feu Sophos. Et voici les résultats dans la figure 3.12.



**Figure 3.12 : La configuration de serveur de type linux.**

En fin, nous avons intégré les deux serveurs **Beyondtrust Linux** et **Windows** au sein de la plateforme LogPoint. La **figure 3.5** montre le serveur beyondtrust intégré dans LogPoint et la date des derniers logs reçus avant la capture d'écran.

## 3.2 Architecture du système (Traitement des logs)

Dans cette partie, nous allons présenter l'architecture générale du système qui se base sur :

1. La collection des logs à partir des sources de données.
2. La normalisation des logs collectés
3. Le stockage des logs normalisés dans une base donnée.
4. Les logs stockés ils vont ensuite indexer pour pouvoir être recherchés
5. La construction des tableaux de bord à partir de les données stockées
6. La Corrélation

Cette partie décrit chaque composante de cette architecture :

- **Logs source**

C'est la première partie de l'architecture, l'emplacement local qui envoie les logs.

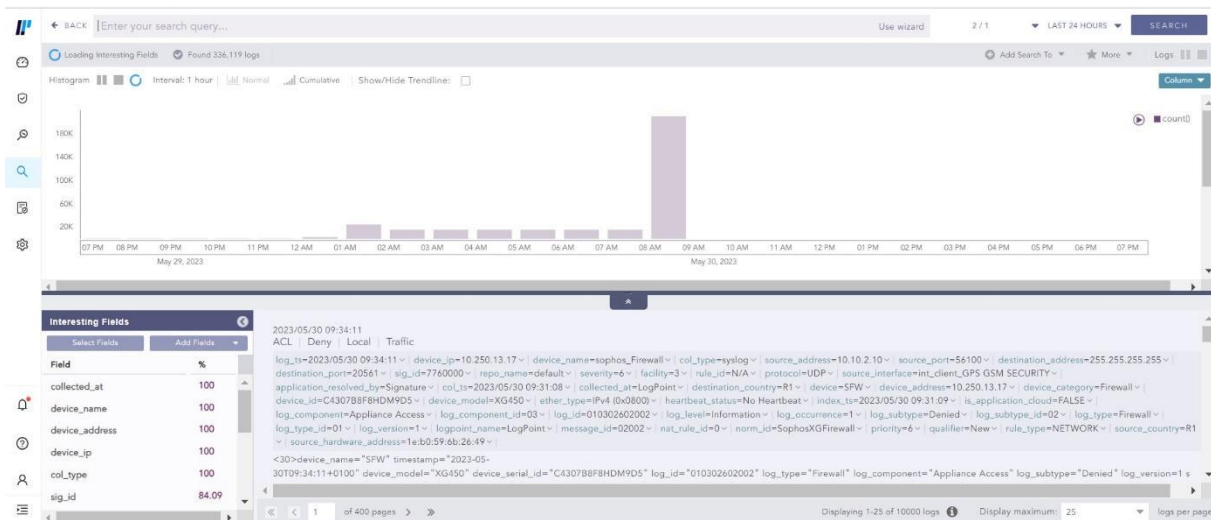
- **La Collection des journaux :**

La disponibilité de la couche de collecte nécessite l'utilisation d'agents LogPoint ou de collecteur connecté au même backend en mode actif-actif. Un équilibreur de charge tierce est requis pour distribuer les flux de l'appareil (SYSLOG) au collecteur.

-SYSLOG : Syslog est l'abréviation de **System Logging Protocole** (protocole de journalisation du système). Il s'agit d'un protocole standard utilisé pour envoyer des messages de journalisation ou d'événements système à un serveur spécifique, appelé **serveur Syslog**. Il est principalement utilisé pour collecter les journaux de divers périphériques à partir de plusieurs machines différentes dans un emplacement central pour la surveillance et l'examen [12].

Par conséquent, les journaux envoyés depuis le périphérique source sont toujours reçus par Collector LogPoint. De plus, le collecteur gère nativement le stockage temporaire des logs sur disque (buffering) en cas de perte de connexion avec le backend. Une fois cette connexion rétablie, le collecteur enverra automatiquement les journaux temporairement stockés en parallèle avec les journaux arrivant au fil du temps.

Voici une figure qui montre les journaux collectés soit de pare-feu Sophos ou bien de routeur Router-PE1-CA1-alger ou bien de serveur **beyondtrust**.



**Figure 3.14** : les logs bruts collectés.

La figure ci-dessus montre des logs bruts collectés de pare-feu 24h avant la capture d'écran montrant toutes les informations nécessaires (l'adresse IP, le port, le protocole ...)

- **Normalisation des données de logs :**

Une fois les journaux collectés, la phase de normalisation commence. Cela signifie que les logs bruts dans différents formats sont traduits dans un seul "langage" Log point. Par exemple, l'adresse IP et l'adresse source etc. d'un appareil sont des informations transformées. LogPoint utilise une taxonomie globale. Les informations contenues dans les messages sont traduites dans une seule langue, par exemple les noms d'utilisateur sont toujours appelés noms d'utilisateur ....

Une fois les données normalisées, le texte brut des logs est stocké dans la base documentaire parallèlement à la normalisation. Les données sont ensuite doublement indexées pour améliorer les capacités de recherche et de récupération des données. Les données sont stockées dans un ou plusieurs référentiels : chaque référentiel peut avoir sa propre durée de conservation des données et des droits d'utilisateur spécifiques associés. Les données peuvent être librement déplacées entre les référentiels. Un référentiel peut également être une entité externe telle qu'un NAS/SAN/sauvegarde qui permet aux clients de mettre en œuvre une stratégie de gestion de la durée de vie. Les données brutes du journal sont modifiées selon un rapport minimum, Cela signifie que les clients n'ont plus besoin du même espace de stockage qu'auparavant.

L'étape de normalisation faite derrière l'écran en appliquant la politique de normalisation qui sont des package prédéfinie pour chaque type de périphérique est montré ci-dessus dans la politique de normalisation pour chaque actif intégré.

- **Stockage :**

Une fois que la machine de la normalisation a fait son travail, l'information doit être stockée. Les logs sont stockés sur un politique de stockage que définis par l'analyste, il peut décider de stocker les logs dans un endroit donné qu'on appellera repose history ou repos pour simplifier avec une période de rétention de 30 jours puis ensuite décider de migrer les données vers une zone où le stockage est moins



critique et enfin garder ces données pendant 365 jours pour se conformer à une durée légale de stockage pour ce type de log. Une fois les logs stockés, ils vont ensuite indexer pour pouvoir être rechercher, c'est la quatrième étape.

Cette indexation et ces résultats vont ensuite nous permettre de faire des corrélations (la liaison entre les événements) de construire des tableaux de bord, d'établir des rapports, ils vont permettre aussi de définir des actions automatisées sur des outils tiers.

Voici une figure de tableau de bord générée pour les journaux du pare-feu. Ces tableaux montrent, par exemple, les dix types de trafic générés à chaque fois par Sophos. Par exemple, la couleur mauve dans le tableau des dix premiers journaux du sous-type de trafic attribué signifie que ce sont des journaux autorisés par Sophos, tandis que l'orange indique des journaux non autorisés. Chaque couleur a une signification. Pour un autre exemple, le tableau de bord des dix premières sources de journaux arrivés dans Sophos affiche chaque couleur en fonction de l'adresse IP de la source du journal. Nous avons également le tableau de bord des dix premiers ports de destination autorisés pour le trafic, les dix principaux composants responsables de la journalisation pour le pare-feu Sophos, ainsi que les tendances des événements dans le pare-feu.

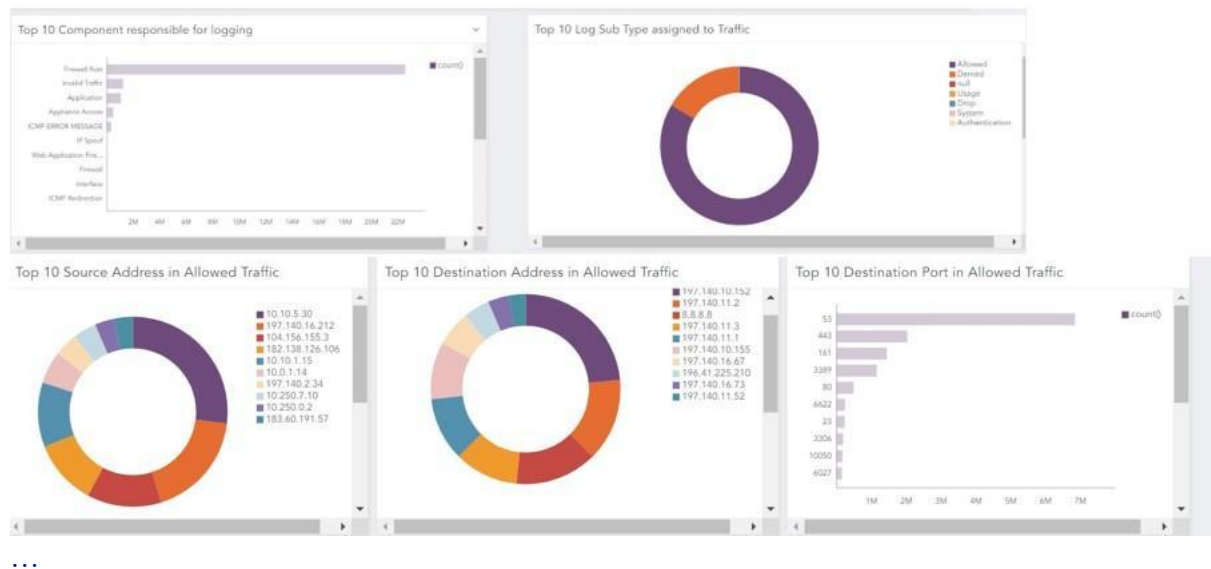


Figure 3.15 : un tableau de bord.

## Conclusion

L'installation et la configuration de base du SIEM LogPoint se sont déroulées sans encombre et dans un délai réduit. Lors de l'implémentation des différents éléments nécessaires au fonctionnement de la solution, nous avons eu recours au support Technique LogPoint qui a été réactif et qui nous a orientés aussitôt vers la bonne piste.

Nous avons particulièrement noté la simplicité du déploiement et la facilité d'intégration de la solution LogPoint dans l'environnement de l'entreprise.

# Conclusion générale

Ce projet de fin d'études consiste à déployer et intégrer une solution SIEM commercial dans le but d'avoir une visibilité globale sur le système d'information de l'entreprise et pour aussi construire une plateforme solide pour son futur projet, qui intégrera le SOC avec le SIEM comme unité centrale de fonctionnement.

À la fin de ce travail, nous pouvons affirmer que nous avons relevé le défi principal de ce projet. Nous avons réussi à créer une application permettant de collecter, normaliser, stocker et analyser les journaux, tout en générant des alertes en fonction des conditions établies, appelées les règles d'alerte, pour détecter les actions anormales. Nous avons initialement utilisé des règles prédéfinies, mais il est possible d'en créer de nouvelles ultérieurement en fonction des besoins de l'entreprise."

L'installation d'un SIEM au cœur de l'infrastructure de l'ISP a constitué un défi pour notre binôme sur plusieurs plans. Le SIEM LogPoint est à la pointe de la technologie, il était donc question d'être au même diapason par rapport à sa philosophie de fonctionnement. D'autre part, le domaine de la cybersécurité était jusqu'à présent principalement théorique pour nous, mais nous avons désormais véritablement plongé dans ce domaine

Le travail effectué, aussi réduit que soit le périmètre traité dans le cadre du mémoire, a néanmoins permis à l'entreprise de répondre à ses problématiques et besoins en termes de visibilité et de maîtrise des événements de sécurité dans son réseau et son infrastructure IT.

Nous avons constaté les avantages d'une solution propriétaire à travers la simplicité de déploiement et la disponibilité du support technique de l'éditeur.

Enfin, le projet SIEM se poursuivra au sein de l'entreprise, et nous sommes convaincus que de nombreuses améliorations seront apportées à l'avenir.

## Abréviations

<b>Abréviation</b>	<b>Description</b>
<b>SIEM</b>	<b>S</b> écurité d' <b>I</b> nformation et <b>E</b> vènement <b>M</b> anagement
<b>SI</b>	<b>S</b> ystème <b>I</b> nformation
<b>MSSP</b>	<b>M</b> anager <b>S</b> ecurity <b>P</b> rovider
<b>SOC</b>	<b>S</b> ecurity <b>O</b> peration <b>C</b> enter
<b>SIM</b>	<b>S</b> écurité <b>I</b> nformation <b>M</b> anagement
<b>SEM</b>	<b>S</b> écurité <b>É</b> vènement <b>M</b> anagement
<b>POP</b>	<b>P</b> oint <b>O</b> f <b>P</b> resence
<b>UIT</b>	<b>I</b> nternational <b>T</b> elecommunication <b>U</b> nion
<b>AI</b>	<b>A</b> rtificial <b>I</b> ntelligence
<b>TTV</b>	<b>T</b> ime <b>T</b> o <b>V</b> alue
<b>ELK</b>	<b>E</b> lasticsearch <b>L</b> ogstash <b>K</b> ibana
<b>EPS</b>	<b>E</b> vents <b>P</b> er <b>S</b> econd
<b>UEBA</b>	<b>U</b> ser and <b>E</b> ntity <b>B</b> ehavior <b>A</b> nalytics
<b>SOAR</b>	<b>S</b> ecurity <b>O</b> rchestration <b>A</b> utomation and <b>R</b> esponse
<b>EAL3+</b>	<b>E</b> valuation <b>A</b> ssurance <b>L</b> evel
<b>SAAS</b>	<b>S</b> oftware <b>a</b> s <b>a</b> <b>S</b> ervice
<b>NAS</b>	<b>N</b> etwork <b>A</b> ttached <b>S</b> torage
<b>SAN</b>	<b>S</b> torage <b>A</b> rea <b>N</b> etwork
<b>VPN</b>	<b>V</b> irtual <b>p</b> rivate <b>N</b> etwork
<b>WAF</b>	<b>W</b> eb <b>A</b> pplication <b>F</b> irewall
<b>IPS</b>	<b>I</b> ntrusion <b>P</b> revention <b>S</b> ystems
<b>IDS</b>	<b>I</b> ntrusion <b>D</b> etection <b>S</b> ystems
<b>DDOS</b>	<b>D</b> istributed <b>D</b> enial- <b>o</b> f- <b>S</b> ervice
<b>HTTP</b>	<b>H</b> ypertext <b>T</b> ransfer <b>P</b> rotocol
<b>HTTPS</b>	<b>H</b> ypertext <b>T</b> ransfer <b>P</b> rotocol <b>S</b> ecure

<b>DHCP</b>	<b>D</b> ynamic <b>H</b> ost <b>C</b> onfiguration <b>P</b> rotocol
<b>NTP</b>	<b>N</b> etwork <b>T</b> ime <b>P</b> rotocol
<b>SMTP</b>	<b>S</b> imple <b>M</b> ail <b>T</b> ransfer <b>P</b> rotocol
<b>PME</b>	<b>P</b> etite <b>M</b> oyenne <b>E</b> ntreprise
<b>IT</b>	<b>I</b> nfrastructure
<b>NIST</b>	<b>N</b> ational <b>I</b> nstitute of <b>S</b> tandards
<b>SQL</b>	<b>S</b> tructured <b>Q</b> uery <b>L</b> anguage
<b>TTM</b>	<b>T</b> ime <b>T</b> o <b>M</b> arket
<b>WAN</b>	<b>W</b> ide <b>A</b> rea <b>N</b> etwork
<b>CPU</b>	<b>C</b> entral <b>P</b> rocessing <b>U</b> nit
<b>RAM</b>	<b>R</b> andom <b>A</b> ccess <b>M</b> emory
<b>GB</b>	<b>G</b> igabyte
<b>FTP</b>	<b>F</b> ile <b>T</b> ransfer <b>P</b> rotocol
<b>SSH</b>	<b>S</b> ecure <b>S</b> ocket <b>S</b> hell
<b>LDAP</b>	<b>L</b> ightweight <b>D</b> irectory <b>A</b> ccess <b>P</b> rotocol
<b>SSL</b>	<b>S</b> ecure <b>S</b> ocket <b>L</b> ayer

# Bibliographie

- [1] « Coût d'une violation de données en 2022 - France | IBM ». <https://www.ibm.com/fr-fr/reports/data-breach>.
- [2] « Cybercrime To Cost The World \$10.5 Trillion Annually By 2025 ». <https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021/>.
- [3] « Accueil », *ICOSNET*. <https://icosnet.com.dz/entreprise/>.
- [4] Avira, « Qu'est-ce qu'une solution SIEM ? Définition et explications | Avira », *Avira Blog*, 9 février 2023. <https://www.avira.com/fr/blog/votre-guide-pour-debuter-gestion-des-informations-et-des-evenements-de-securite-siem>.
- [5] « Memoire Online - Etude et mise en place d'un SIEM (security information and event management) open source: cas de « Bankevi groupe » - Essen Obed KUAOVI KOKO », *Memoire Online*. <https://www.memoireonline.com/07/21/11983/Etude-et-mise-en-place-dun-SIEM-security-information-and-event-management-open-source-cas-de-.html>.
- [6] « Qu'est-ce que la gestion des événements et des informations de sécurité (SIEM) ? | IBM ». <https://www.ibm.com/fr-fr/topics/siem>.
- [7] « What is open source software? | IBM ». <https://www.ibm.com/fr-fr/topics/open-source>.
- [8] SG-Software, « Une solution Open Source ou propriétaire pour votre entreprise? », <https://sg-software.dz/>. <https://www.sg-software.dz/Articles/Une-solution-Open-Source-ou-propri%C3%A9taire-pour-votre-entreprise->.
- [9] M. Dalgaard, « À propos de nous », *Logpoint*. <https://www.logpoint.com/fr/a-propos-de-nous/>.
- [10] M. Dalgaard, « Pourquoi choisir Logpoint ? », *Logpoint*. <https://www.logpoint.com/fr/pourquoi-choisir-logpoint/>.
- [11] « SOAR - Recherche Google ». <https://www.google.com/search?q=SOAR&oq=SOAR&aqs=chrome..69i57j0i27112.1843j0j7&sourceid=chrome&ie=UTF-8>.
- [12] « Syslog - Definition and Details ». <https://www.paessler.com/it-explained/syslog>.