RÉPUBLIQUE DU SÉNÉGAL

UN PEUPLE – UN BUT – UNE FOI

--

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR DE LA RECHERCHE ET DE L'INNOVATION

UNIVERSITÉ GASTON BERGER DE SAINT-LOUIS

U.F.R de Sciences Appliquées et de Technologie
Section d'Informatique

Mémoire | Rapport de stage de fin de cycle

Master 2 d'Informatique

Sujet : « Etude et Mise en Place d'un SOC avec Splunk. »

Présenté par

Ndeye Penda Fall

Pour l'obtention du

Master d'Informatique, option Réseaux, Sécurité et Systèmes Distribués

R2SD

Encadreur académique :	**Maitre de stage** :
Dr. Cherif Diallo	**Kalidou Sy**

Année Académique : 2016/2017 **N° ordre :**

Remerciements

Je tiens à remercier sincèrement mon encadreur à Atos Mr Kalidou Sy pour ses conseils, sa disponibilité et qui n'a ménagé aucun effort pour la réussite de ce stage.

Je remercie énormément mes parents et ma famille pour leurs soutiens, leurs conseils et leurs présences malgré la distance.

Je remercie notre professeur et encadreur Mr. Cherif Diallo pour ses conseils.

Je remercie aussi mes amis pour leurs conseils, leurs disponibilités et leurs compréhensions, particulièrement une qui saura se reconnaitre et sans oublier les familles Sène, Thiam et Lalyre pour leur accueil.

Mes remerciements vont aussi à tous les dirigeants et collaborateurs d'Atos qui ont facilité ces six mois de stage ainsi qu'à l'administration et le corps professoral de la section Informatique de l'UFR des Sciences Appliquées et de Technologies (SAT) de l'Université Gaston Berger de Saint-Louis.

Et finalement, je tiens à remercier tous ceux qui de près ou de loin ont contribués à l'élaboration de ce document par un conseil, une source ou autre, et particulièrement mes camarades de magistère.

Dédicaces

A mes parents,

ma famille et mes amis, …

Avant-propos

L'Université Gaston Berger de Saint-Louis du Sénégal est une université d'excellence et compte plusieurs UFR dont celle des Sciences Appliquées et de Technologies (SAT).

Cette UFR compte trois (3) sections à savoir : la section Informatique, la section Mathématique et la Section Physique.

Ces sections offrent des formations allant de licence 1 à la thèse en passant par le master 2.

C'est même dans le cadre de l'obtention de ce dernier diplôme cité que nous avons eu à effectuer des stages en entreprise pour obtenir à terme notre Master 2 en Réseaux, Sécurité et Systèmes Distribués (R2SD) de la section Informatique.

Table des matières

Remerciements 3
Dédicaces 4
Avant-propos 5
Tables des illustrations 9
Tables des tableaux 11
Liste des sigles et abréviations 12
Résumé 14
Introduction 15
CHAPITRE 1 : Généralités 16
1.1 Structure d'accueil 16
1.1.1 Historique 16
1.1.2 Domaines d'activité 17
1.1.3 Partenaires 17
1.2 Présentation du sujet 18
1.2.1 Contexte 18
1.2.2 Problématique 18
1.2.3 Objectifs 19
CHAPITRE 2 : SOC : Concepts et fondamentaux 20
2.1 Généralités 20
2.1.1 Définition 20
2.1.2 Objectifs 20
2.1.3 Types de SOC 21
2.2 Avantages et limites d'un SOC 21
2.2.1 Avantages 21
2.2.2 Limite : 22
2.3 Structure d'un SOC 22
2.3.1 Périmètre organisationnel 22
2.3.2 Services d'un SOC 22
2.3.3 Fonctionnement d'un SOC 24
2.3.4 Le mécanisme d'escalade 25
2.4 Technologies nécessaires 26
2.4.1 SIEM 26
2.4.2 Outils de gestion de la conformité 27
2.4.3 Outils d'analyse de la sécurité de renseignement sur le menaces (Threat Intelligence) 27

2.4.4 Outil de gestion des vulnérabilités et de tests de pénétration 27
CHAPITRE 3 : Conception d'un SOC 28
3.1 Les ressources humaines 28
3.1.1 Tiers 1 : Analystes de sécurité 28
3.1.2 Tiers 2 : Ingénieurs de sécurité 29
3.1.3 Tiers 3 : Experts sécurité 29
3.1.4 Tiers 4 : Manager du SOC 29
3.2 Cadrage fonctionnel et technique 29
3.2.1 Cadrage fonctionnel 29
3.3 Cadrage technique 33
3.4 Architecture fonctionnelle et technique 34
3.4.1 Architecture fonctionnelle 35
3.4.2 Architecture technique : 36
3.5 Conception détaillée 37
3.5.1 Cas d'utilisations 37
3.5.2 Exploitation des cas d'utilisation 38
3.5.3 Conception du module ATISE (Automatisation des Tests d'Intrusion et de Simulation d'Equipements) 40
CHAPITRE 4 : Implémentation 48
4.1 SIEM 48
4.1.1 Limites 48
4.1.2 Comparaison de quelques SIEM 49
4.2 Splunk 51
4.2.1 Généralités : 51
4.2.2 Architecture : 51
4.2.3 Catalogue de produits : 53
4.2.4 Apps et Add-on 54
4.3 Pratique 54
4.3.1 Architecture : 54
4.3.2 Activation du SSL 55
4.3.3 Définition de l'authentification à partir d'un annuaire externe 56
4.3.4 Mise en place du reverse proxy 58
4.3.5 Configuration des forwarders 58
4.3.6 Configuration du firewall : 60
4.3.7 Résultats 62
Conclusion 72

Annexe 1 : Installation et configuration de base de Splunk 74
Annexe 2 : Personnalisation des tableaux de bord et création d'applications 76
Création d'application : 76

Tables des illustrations

Figure 1: historique d'Atos (Atos, 2016) 16
Figure 2: Services d'un SOC 23
Figure 3: Structure de fonctionnement d'un SOC (Clusif, 2017) 25
Figure 4: Rôles et mécanisme d'escalade ((Mitre), 2014) 26
Figure 5: Processus de détection 30
Figure 6: Processus de qualification 31
Figure 7: Processus de gestion des incidents 32
Figure 8: Processus de supervision, de contrôle et d'administration 33
Figure 9: Fondamentaux d'un SOC 35
Figure 10: Workflow d'un SOC 36
Figure 11: Architecture technique d'un SOC 37
Figure 12: Diagramme cas d'utilisation ATISE 41
Figure 13: Diagramme de séquence lancer_campagne_test 42
Figure 14: Diagramme de séquence cas Gerer_privileges 44
Figure 15: Diagramme de séquence cas simuler_equipement 45
Figure 16: Diagramme de séquence cas comparer_tests 46
Figure 17: Architecture de Splunk (Splunk, Splunk Enterprise, s.d.) 52
Figure 18: Architecture de déploiement de Splunk (Splunk, Splunk Enterprise, s.d.) 53
Figure 19: Architecture d'implémentation 55
Figure 20: Page d'accueil Splunk après activation du SSL 56
Figure 21: Création d'utilisateurs 57
Figure 22: Activation de l'authentification LDAP 57
Figure 23: Serveur LDAP 58
Figure 24: Activation des modules proxy dans httpd.conf 58
Figure 25: Configuration du proxy dans httpd-vhost.conf 58
Figure 26: Configuration des forwarders : choix des forwarders 59
Figure 27: Répertoire à superviser 59
Figure 28: Paramétrage de la réception des données 60
Figure 29: Résumé des actions précédentes 60
Figure 30: Configuration du fichier de réception 61
Figure 31: Extrait du fichier de sauvegarde Iptables 61
Figure 32: Configuration de la rotation des logs 62
Figure 33: Configuration du forwarding 62
Figure 34: Application NetFilter Iptables for Splunk 62
Figure 35: Installation de Python for Scientific Computing 63
Figure 36: Installation ML Toolkit 63
Figure 37: Page d'accueil avec ML Toolkit installé 64
Figure 38: Apprentissage automatique 64
Figure 39: Cas d'utilisation ML-Toolkit 65
Figure 40: Listes des évènements reçus 66
Figure 41: Détection du ransomware 66
Figure 42: Requêtes permettant d'afficher les sites suspects 66
Figure 43: Détection du malware Trickbot 67
Figure 44: Détection des pics de trafic suspects 67
Figure 45: Amélioration de la détection d'un DDOS 68
Figure 46: Statistiques en rapport avec le flux DDOS 69

Figure 47: Requêtes SPL pour détecter les comportements aberrants 69
Figure 48: Requête de détection de vulnérabilités 70
Figure 49: Tableau de bord customisé avec d3js..... 70
Figure 50: Tableau de bord customisé avec d3js (2)..... 71
Figure 51: Tableau de bord customisé avec d3js..... 71
Figure 52: versions Splunk..... 74
Figure 53: Accueil Splunk..... 75
Figure 54: Ajout de l'application..... 77
Figure 55: Application visible dans la liste des applications..... 77
Figure 56: Page d'accueil de l'application 78
Figure 57: Nouveau tableau de bord 78
Figure 58: Ajout d'un panel au Dashboard..... 79
Figure 59: Requêtes pour le tableau de bord..... 79
Figure 60: Résultat 79

Tables des tableaux

Tableau 1: Descrition cas Lancer_campagne_test 42
Tableau 2: Description cas Gerer_privileges 44
Tableau 3: Description cas Simuler_equipement 45
Tableau 4: Description cas Comparer_tests 47

Liste des sigles et abréviations

Nous présentons dans ce tableau un ensemble de sigles et d'abréviations que nous allons utiliser dans le document.

Sigle ou abréviation	Signification
API	Application Programming Interface
ATISE	Automatisation des Tests et Simulation d'Equipements
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CISSP	Certified Information Systems Security Professional
CLI	Command Line Interface
GCFA	GIAC Certified Forensic Analyst
GCFE	GIAC Certified Forensic Examiner
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
GDC	Global Distribution Unit
HTTP	HyperText Transfer Protocol
IoC	Indicator of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technologie
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
ML	Machine Learning
MSSP	Management Security Service Provider
N1	Niveau 1
N2	Niveau 2
N3	Niveau 3
NOC	Network Operations Center
OIV	Organisation à Intérêt Vital
OT	Organisation technologie
PKI	Public Key Infrastructure
RSSI	Responsable Sécurité Système d'information
SI	Système d'Information
SaaS	Security as a Service
SAML	Security Assertion Markup Language
SEM	Security Event Management
SIEM	Security Incident & Event Management
SIM	Security Incident Management
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SPL	Search Processing Langage
SQL	Structured Query Language
SSI	Sécurité Système d'information
SSL	Secure Socket Layer
SSO	Single Sign One

URI	Uniform Resource Identifier
WMI	Windows Management Instrumentation
XML	eXtensible Markup Language

Résumé

Ce document est un mémoire de fin de cycle en vue de l'obtention du Diplôme de Master 2 Réseaux Sécurité et Systèmes Distribués. Il présente la réalisation d'un projet effectué dans le cadre d'un stage à Atos Sénégal portant sur l' « Etude et la mise en place d'un SOC (Security Operations Center) sur Splunk »

Plus que jamais, la numérisation des entreprises s'accélère. Dans ce contexte, les exemples d'attaques liés à internet déroulants de la transformation digitale sont de plus en plus nombreux. En effet, les risques de faille de sécurité ne cessent de s'intensifier, ce qui nous amène à penser à une approche rigoureuse de la Cybersécurité. Nous devons être en mesure de protéger les utilisateurs et les entreprises de la « Cyber-menace » en constante évolution.

Consciente de ces menaces, l'entreprise Atos Sénégal a décidé d'exploiter cette branche de la cybersécurité par l'étude et la mise en place d'un SOC sur un outil nommé Splunk pour plus de visibilité par rapport à ces menaces et pouvoir remédier aux éventuels incidents de sécurité qu'elles peuvent engager.

Pour ce faire on passera par :

- La mise en place d'une plateforme SOC qu'on aura à sécuriser,
- La définition des processus pour la mise en place du SOC,
- L'implémentation de quelques cas d'utilisation,
- Concevoir un module permettant l'automatisation des tests d'intrusion et la simulation de certains équipements.

Introduction

L'informatique, une science en pleine évolution, offre depuis ses débuts des avantages et vise à améliorer les conditions de vie des hommes.

L'automatisation de plusieurs tâches surtout dans les entreprises (industrialisation) permet d'optimiser l'utilisation des ressources, d'assurer un niveau de qualité et de réduire coûts et risques. On assiste à une transformation digitale où toutes les technologies et applications de l'entreprise sont intégrées à l'ensemble de ses activités et à la naissance des offres cloud et d'une nouvelle de développer et d'intégrer les applications (le devops).

Avec cette multitude d'applications de toutes sortes (gestion des paiements, gestion de accès et de l'authentification, etc.), la problématique du traitement et du stockage se fait sentir car les bases de données traditionnelles sont devenues impuissantes face à cette multitude de données, ainsi le big data vient en son heure et se propose de traiter ces données.

De plus monde est ainsi entré dans l'ère de « l'hyperconnectivité » ; où aussi bien les hommes que les entreprises sont connectés, communiquent et échangent entre eux. Et les données sont au cœur de cette révolution numérique. Elles ont acquis une valeur économique et stratégique majeure et sont aujourd'hui essentielles à la bonne marche de toute entreprise.

Ce pendant cette accessibilité des données constitue également des cibles potentielles. En effet la plupart des données et services de l'entreprise sont accessibles de l'extérieur ce qui a pour conséquence l'ouverture de l'entreprise à toutes sortes de menaces qui sont de plus en plus sophistiquées et pernicieuses. L'Internet, l'une des évolutions les plus innovantes et les plus adaptées de l'informatique, est insécure, il convient donc aux l'entreprises de protéger leur patrimoine.

C'est ainsi que des méthodes de sécurisation ont vu le jour (https, chiffrage, hachage, firewalling, etc.). Ce pendant ces méthodes ne permettent pas d'assurer une sécurité de bout en bout et les cyberattaques se font de plus récurrentes (Ransomware, spectre et Meltdown, etc.).

Vue tous ces aspects, toutes les entreprises devraient renforcer leur arsenal de sécurité et mettre en place un SOC (Security Operation Center) qui offre des capacités de réaction active et proactive.

Ainsi ce mémoire a pour but l'étude et la mise en place d'un SOC avec l'outil Splunk.

Dans un premier temps nous ferons une présentation générale de la structure d'accueil et du sujet.

Ensuite, nous allons faire étude de l'art de mettre en place un SOC avant de faire sa conception.

Nous allons terminerons enfin par son implémentation avec quelques cas pratiques.

CHAPITRE 1 : Généralités

1.1 Structure d'accueil

1.1.1 Historique

Atos est une entreprise de services numériques française qui fournit des services de payement électronique, de conseil, d'intégration de systèmes, d'infogérance, de Cloud, ainsi que des technologies de Big Data et Cybersécurité. Elle fut créée en 1997 et compte aujourd'hui environ 120 000 collaborateurs répartis dans 72 pays dont le Sénégal depuis 2014.

Son histoire est rythmée par des fusions / acquisitions dont l'acquisition de Bull, une société française fondée en 1930 et spécialisée dans l'informatique professionnelle exploitant notamment les brevets du norvégien Frederik Rosing Bull.

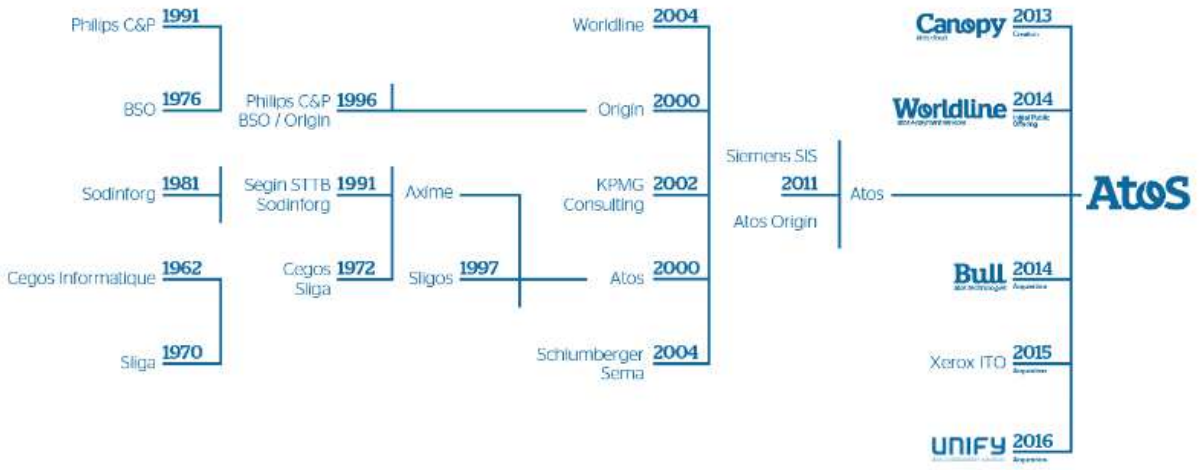


Figure 1: historique d'Atos (Atos, 2016)

Très récemment Atos a acquis Syntel qui est une entreprise américaine spécialisée dans le traitement des données particulièrement dans les domaines de la finance et de l'assurance. Cette dernière acquisition renforce la position d'Atos aux USA.

Atos exerce ses activités sous les noms de : Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify et Worldline et se représente ainsi autour de 5 marques d'expert :

- Atos est la marque principale du groupe, c'est sur elle que s'appuient les autres marques particulièrement en ce qui concerne l'identité et les valeurs fondamentales.
- Bull (Atos Technologie) : comme indiqué, c'est la marque technologique du groupe (logiciels et matériels). C'est le leader européen du calcul haute performance. C'est le bras armé d'Atos dans le big data et la sécurité.
- Canopy (Atos Cloud) : c'est la marque consacrée au Cloud. Canopy est un service intégrateur de services Cloud privé et public.
- Unify (Atos Collaboration solution) : c'est la marque dédiée aux solutions de communication unifiée, en temps réel. Vise à renforcer la collaboration sociale

et la transformation numérique des clients pour l'amélioration de leurs performances.

- ∞ Worldline (Atos e-payment services) : c'est le leader européen des services de transaction et de paiements.

1.1.2 Domaines d'activité

Atos s'illustre à travers plusieurs domaines d'activités, résultant de ses fusions/acquisitions, dont les principaux sont :

- ∞ Infogérance : Atos est spécialisée dans le secteur d'activité de l'infogérance qui est la gestion d'installations informatiques de ses clients (exploitation, optimisation, sécurisation).
- ∞ Conseil et intégration de systèmes : Le volet Atos Consulting, est un service de consultance qui prodigue des conseils à des entreprises demandant un accompagnement dans leurs transformations digitales. L'intégration de système consiste à la réunion au sein du même système de parties conçues séparément. Il y'a aussi l'intégration de services Cloud proposée par Atos Canopy.
- ∞ Worldline : couvre l'ensemble des chaines de valeur des paiements, gestion de transactions entre une entreprise, ses partenaires et ses clients. Worldline se concentre sur trois (3) piliers commerciaux à savoir : Merchant Services, Mobility et e-transactional services, Financial Services incluant equensWorldline
- ∞ Big Data et sécurité : Atos propose des solutions big data et sécurité à de nombreux clients, de même que des solutions de business intelligence qui permettent d'optimiser la prise de décision.

1.1.3 Partenaires

Atos s'est lié de partenariats stratégiques lui permettant d'offrir des solutions innovantes avec l'expertise nécessaire. Il s'agit principalement de :

- ∞ Google Cloud : un partenariat mondial pour fournir aux entreprises de nouvelles solutions sécurisées de Cloud Hybride, d'analyse de données et d'apprentissage automatique ainsi que d'environnement de travail connecté.
- ∞ SIEMENS : principal partenaire d'Atos, il s'illustre dans la conception d'équipements.
- ∞ DELL EMC : filiale de Dell Technologie, fournit l'infrastructure aux entreprises.
- ∞ VMWare : filiale de Dell Technologie, fournit des services Cloud et de développement de logiciels de virtualisation.
- ∞ RSA : pour assurer l'efficacité d'une stratégie de sécurité de nouvelle génération.
- ∞ CISCO : est un partenaire dans l'installation d'infrastructure réseau.
- ∞ ORACLE : pour l'implémentation et la gestion des bases de données ORACLE.
- ∞ Redhat : fournit des solutions sécurisées et de virtualisation.

Après cette brève présentation de la structure d'accueil nous allons à présent passer au sujet de notre étude.

1.2 Présentation du sujet

1.2.1 Contexte

La récurrence des attaques informatiques ces dernières années voire même ces derniers mois, est indéniable : c'est le cas de Ransomware qui a touché plusieurs grandes entreprises et structures par le monde, du Spectre MeltDown qui a récemment fait des ravages, etc. Et recrudescence des cyberattaques, n'est pas prête de s'estomper.

De plus l'ampleur, la fréquence et la coordination de ces attaques renseignent sur l'envergure des moyens techniques, humains mis en œuvre par leurs auteurs pour l'atteinte de leurs objectifs.

Certaines études ont montré qu'environ 1280 grandes entreprises rapportent une intrusion dans leurs systèmes chaque année. A cela s'ajoute le coût des fraudes informatiques et de télécommunications qui s'élevait à 10 milliards de dollars en 2009 aux USA.

D'après le Global Economic Crime Survey 2016, le taux de cybercriminalité reporté par les entreprises françaises a presque doublé en 2ans (environ 53% des entreprises affectées).

L'impact de ces attaques se fait sentir dans l'activité des entreprises touchées qui sont profondément perturbées voir même arrêtées, ce qui engendre des répercussions au plan financier, juridique, organisationnel, voir même la perte d'image de marque.

De plus avec la digitalisation, où toutes les infrastructures sont connectées à Internet, la menace de cyberattaques est omni présente.

Les lois et réglementations[1] en vigueur prescrivent aussi des exigences quant à la collecte et la conservation de données, principalement à caractère personnel, surtout pour les entreprises du secteur bancaire, de l'assurance et des entreprises à intérêt vital (défense, santé, fournisseurs d'eau, d'électricité, etc.).

Ainsi, aux vus des conséquences que peuvent avoir les cybermenaces (pertes financières, perte de l'image de marque, etc.) et de la nécessité d'être en adéquation avec les lois et règlementations, la responsabilité de la Direction de l'entreprise peut-être, de même, engagée au plus haut point.

Il est donc fondamental, pour les entreprises, de mettre en place des stratégies de sécurité plus adaptées et plus performantes. C'est en cela que la mise en place d'un SOC (Security Opération Center) est essentielle, surtout avec la pratique du Big Data et du traitement de données qui demandent un niveau de sécurité plus important.

1.2.2 Problématique

Le rôle de l'humain dans la gestion d'applications et de taches liées aux infrastructures IT n'est plus à exclure dans les sources de vulnérabilité. Ceci découlant d'erreurs susceptibles d'être commises par l'homme.

[1] Au Sénégal, la loi numéro 12, 2008 du 25 janvier 2008 sur la protection de données à caractère personnel traite en partie des conditions de protection minimales exigées pour tout traitement des données à caractère personnel, aux obligations qui pèsent sur le responsable du traitement de ces données et aux différentes sanctions prévues en cas de non-respect de la législation en vigueur.
En France, le RGPD (Règlement Général sur la protection des données) décrit un nouveau cadre règlementaire pour l'économie numérique.

Dans le domaine de la supervision de la SSI, (trois) 3 difficultés majeures sont rencontrées :

- La masse et la diversité des informations qui doivent être traitées ;
- L'identification des évènements qui précèdent les alertes de sécurité ;
- La communion des compétences requises pour un projet d'envergure.

Bien qu'il existe des logiciels (antivirus, firewall, etc.) et équipements de sécurité (sonde IDS/IPS, firewall, etc.), ces équipements sont utilisés de manière isolée et ne permettent pas d'avoir une vue d'ensemble du système d'information.

Ainsi le monitoring était essentiellement exécuté afin de notifier aux responsables de sécurité les différents incidents de sécurité. Cependant, depuis quelques temps, une nouvelle tendance s'est dessinée : la remédiation.

Face à la variété des applications, la diversité des sources d'informations et la recrudescence des cyberattaques, comment une entreprise peut se prémunir des dangers qui la guette dans le cyberespace ? Par quels moyens les équipes de sécurité pourront s'organiser pour une gestion efficiente de la sécurité, palier incontournable dans la confidentialité des données personnelles et la pérennité des applications ?

1.2.3 Objectifs

L'objectif visé consiste à mettre en place un système de sécurité centralisé utilisant le big data afin d'accroitre la protection des SI.

Ce système basé sur Splunk permettra :

- La centralisation des logs provenant de diverses sources : applications, serveurs, bases de données, équipements réseaux (routeurs, commutateurs, firewall, etc.), etc.
- L'analyse et le traitement de ces données en vue de déceler un comportement anormal
- La visualisation des données utiles sous forme de graphe pour une meilleure analyse

Ceci en vue de garantir le fonctionnement du SI et d'améliorer le temps de réaction face aux attaques.

Ces objectifs peuvent être subdivisés en plusieurs sous objectifs à savoir :

- L'installation de Splunk et la rédaction d'un guide de prise en main rapide,
- L'intégration de Splunk avec LDAP pour permettre l'authentification,
- La sécurisation de Splunk par reverse proxy,
- L'implémentation de quelques cas d'utilisation,
- La création d'un module permettant de simuler le fonctionnement de certains équipements et d'intégrer des outils de tests d'intrusion.

CHAPITRE 2 : SOC : Concepts et fondamentaux

2.1 Généralités

2.1.1 Définition

Tantôt définit comme un accompagnement quotidien composé d'hommes, de processus et de technologies, ou comme une équipe d'experts en sécurité chargée de surveiller, détecter, analyser et qualifier les évènements de sécurité ; un SOC fait partie de manière générale des dispositifs mis en place au sein de l'entreprise pour augmenter le niveau de sécurité de cette dernière.

Un SOC permet ainsi de répondre au besoin de supervision et de détection de l'entreprise par une surveillance en temps réel des données collectées et la levée d'alertes en cas d'incidents.

C'est un dispositif qui doit s'ajuster aux structures de l'organisation, toute organisation ayant déjà des éléments en place, des processus ou outils. Il doit enrichir le système global afin de contribuer à la finalité qui est de maintenir un niveau de sécurité propre à satisfaire les exigences en sécurité des parties intéressées de l'organisation et ce au meilleur coût.

2.1.2 Objectifs

Comme définit dans le chapitre précédent, un SOC est destiné aux structures souhaitant avoir une maîtrise de leur risque et augmenter le niveau de sécurité de leurs systèmes d'information tout en contrôlant le coût correspondant.

Ainsi, pour ce faire, l'objectif de l'organisation va être de répartir son effort sur les trois temps de la sécurité que sont la prévention, la détection et la réaction.

- La prévention : par la prise en charge partielle ou intégrale de la gestion des menaces et des vulnérabilités ;
- La détection : permettre ou améliorer la détection d'incidents en dotant de capacités à déceler toute attaque portant sur le périmètre du SI. Ces outils de monitoring et de détection s'appuient sur des outils de collecte complétés par des outils de corrélation dont les résultats seront traités par les analystes de sécurité et dont les paramètres sont enrichis par des experts élaborant de nouveaux scénarii de détection pertinents ;
- La réaction : fournir aux équipes d'investigation des informations pertinentes afin qu'ils puissent agir rapidement et plus efficacement ceci grâce à la capacité de prise en charge totale (périmètre, temporalité, impact, etc.) de l'attaque par le SOC.

Elle pourra également intégrer la problématique de conformité qui, en fonction des secteurs, peut fournir une incitation forte voire une obligation. En effet aujourd'hui plusieurs exigences réglementaires font directement ou indirectement référence à des mécanismes comme le SOC en vue de la protection des données en particulier les données personnelles surtout pour des organisations à intérêt vital (secteurs de la défense, de la santé, de l'énergie), les banques, assurances, etc.

D'autres missions peuvent aussi être confiées au SOC à savoir :

- La sensibilisation des utilisateurs ;
- L'expertise et conseils auprès des équipes informatiques ;
- Le pilotage de la mise en œuvre des correctifs de sécurité ;

En somme, un SOC doit permettre à l'entreprise de répondre à son objectif principal : garantir la continuité de ses activités métiers, en s'adaptant au mieux et au plus vite aux contraintes et risques liées à l'hyper-connectivité.

2.1.3 Types de SOC

On peut distinguer plusieurs types de SOC en fonction de la localisation (interne à l'entreprise, externe, ou hybride), des moyens humains, financiers et techniques.

- SOC virtuel : pas d'installation dédiée, membres de l'équipe à temps partiel et ne sont actifs qu'en cas d'alerte ou d'incident critique.
- SOC dédié : pour ce type de SOC il existe une équipe et une installation dédiées et il entièrement interne à l'entreprise.
- SOC semi-dédié /cogéré : certains membres de l'équipe sont dédiés, d'autres sont semi-dédiés, il est cogéré lorsqu'une partie de la gestion du SOC est confiée à un MSSP.
- SOC de commande : coordonne d'autres SOC, fournit des renseignements sur les menaces, la connaissance de la situation et une expertise supplémentaire. Il est rarement directement impliqué dans les opérations au jour le jour.
- Centre d'opération SOC/NOC : installation dédiée avec une équipe dédiée effectuant non seulement non seulement de la sécurité mais également d'autres opérations informatiques critiques 24/7 dans la même installation afin de réduire les coûts.
- Fusion de SOC : c'est l'intégration des SOC traditionnels avec les nouvelles fonctions telles que l'intelligence des menaces, les fonctions de technologies opérationnelles et l'équipe d'intervention en cas d'incident informatique entre autres.
- SOC externalisé : un fournisseur construit et exploite le SOC avec une implication minimale (ou au mieux de supervision) de la part de l'organisation cliente.

2.2 Avantages et limites d'un SOC

2.2.1 Avantages

Un SOC a l'avantage de réduire le temps de détection, il permet d'identifier plus rapidement les menaces et dans la plupart des cas, permet de se remettre dans un délai raccourci d'une attaque par déni de service distribué (DDOS).

Sans les services d'un SOC, des attaques de cybers criminels peuvent rester cachées pendant une longue période car les entreprises ne disposent des compétences nécessaires pour détecter et répondre aux menaces en temps opportun. On peut toujours citer l'exemple de Yahoo qui a vu ses comptes piratés pendant de nombreuses années sans le savoir.

Ainsi, un SOC va permettre aux entreprises d'avoir une meilleure visibilité sur son environnement, disposer de compétences, de process et d'amélioration continue. Avec des attaques de plus en plus régulières, de nombreuses organisations recentrent leurs efforts de sécurité sur la prévention et la détection.

- Amélioration de la gestion des menaces :

Les entreprises déploient régulièrement diverses technologies de sécurité conçues pour prévenir et détecter les menaces, ainsi que pour renforcer et protéger les actifs. Pour une efficacité maximale, elles doivent être centralisées, normalisées, corrélées, et surveillées en temps réel, avec les ressources disponibles pour analyser et répondre aux activités et incidents suspects.

Les incidents sont souvent susceptibles de s'étendre sur plusieurs entités et cela nécessite donc des actions coordonnées pour réduire les risques. Un SOC répond parfaitement à toutes ces exigences.

Avec un SOC, les organisations bénéficieront ainsi d'une plus grande rapidité pour identifier des attaques et d'y remédier avant qu'elles ne causent des dommages.

- ∞ Maintien de sa conformité règlementaire :

Un SOC permet également de répondre aux exigences règlementaires en exigeant une surveillance de sécurité, une gestion des vulnérabilités ou une fonction de réponse aux incidents.

- ∞ Centralisation et consolidation des fonctions de sécurité :

La consolidation des fonctions de sécurité dans un SOC peut permettre de faire des économies, un partage des couts et des économies d'échelle, tout en maximisant l'expertise, les compétences et les ressources disponibles.

2.2.2 Limite :

Un SOC se doit d'intégrer tous les processus métiers de l'entreprise, tout doit être discuté en cela, sa mise en place est couteuse et chronophage.

De plus l'ensemble des règles et des bases de vulnérabilités et de tests permettant l'opérabilité du SOC doit être régulièrement mis à jour afin de garantir le bon fonctionnement de ce dernier.

Enfin le SOC étant constitué d'une équipe d'experts, il est souvent difficile d'abord de trouver les compétences nécessaires et ensuite de pouvoir les fidéliser.

2.3 Structure d'un SOC

2.3.1 Périmètre organisationnel

Sur le plan organisationnel, différents interlocuteurs doivent être identifiés au sein de l'entreprise. Il s'agit en général de :

- ∞ Le/les DSI
- ∞ Le/les RSSI
- ∞ Le/les responsables risques et audit
- ∞ Le/les architectes réseaux/système
- ∞ Le/les responsables du SOC
- ∞ Le/les responsables d'équipe opérationnelle
- ∞ Les analystes

2.3.2 Services d'un SOC

Un SOC c'est aussi un ensemble de services qui doit garantir l'atteinte des objectifs premiers à savoir : la prévention, la détection et la réaction.

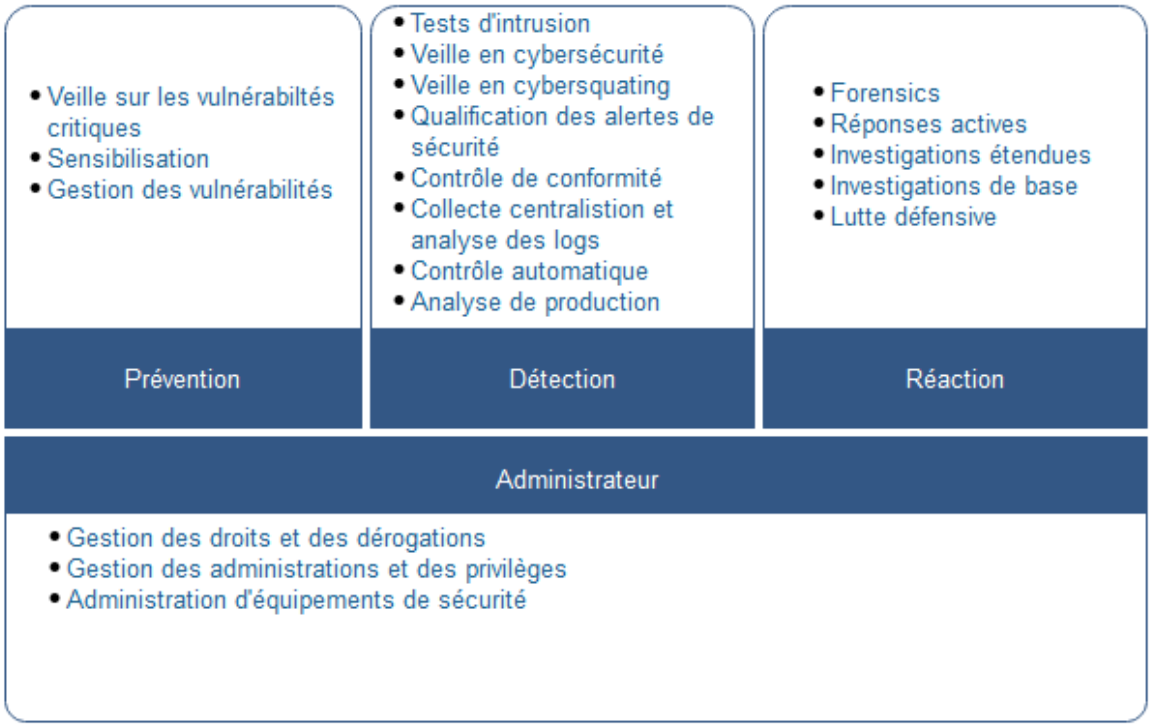


Figure 2: Services d'un SOC

2.3.2.1 La prévention

La prévention fait partie des fonctions que doit offrir un SOC. Cette prévention est faite par une combinaison des informations collectées et d'un certain nombre d'action et de processus notamment :

- La gestion de vulnérabilités : le SOC doit disposer d'informations à jour sur les vulnérabilités du SI afin de mettre à jour et d'adapter ses règles de sécurité. La gestion des vulnérabilités comprend la veille, la qualification, les préconisations puis le suivi du déploiement des patchs indiqués (Clusif, 2017).
- La sensibilisation : la sensibilisation reste un moyen incontournable en sécurité. En effet des actions de sensibilisation doivent être menées à l'endroit des utilisateurs du SI car la première menace en sécurité est l'utilisateur lui-même qui même par ignorance peut exposer le système à de nombreux risque.

2.3.2.2 La détection

Tout comme la prévention, la détection nécessite le traitement des informations issues des données collectées. L'implication directe des analystes de sécurité dans ce traitement est encore primordiale car permettant dans certains cas d'affirmer ou d'infirmer les incidents de sécurité et réduire ainsi les nombres de faux positifs et vrais négatifs. La fonction de détection passe par trois processus :

- La collecte et la qualification : Le SOC doit collecter des informations, des logs la plupart du temps, issus de l'infrastructure supervisée. Les données centralisées sont analysées pour permettre de faire ressortir de rapprochements et des corrélations qui peuvent mettre facilement en évidence d'éventuels incidents de sécurité.

- ∞ Le contrôle : l'efficience de la fonction de détection repose sur le contrôle régulier des outils et politiques mis en place. Ce contrôle permet de remonter au SOC les vulnérabilités et menaces potentiels mais aussi tout écart dans la politique de conformité en matière de sécurité. Le contrôle peut aussi passer par l'audit ou des tests d'intrusion afin de tester la résilience du système.
- ∞ La veille : La connaissance des menaces pesant sur l'organisation est primordiale pour le SOC. Cela lui permet d'affiner et d'optimiser les politiques de sécurité. Pour conserver l'image de l'entreprise, le SOC peut, par exemple, suivre l'enregistrement des noms de domaines proches de ceux de l'entreprise pour éviter le cybersquatting. Il peut surveiller les sites exposés et même aller plus loin en menant une surveillance dans le web profond afin d'être averti des potentiels menaces (threat intelligence).

2.3.2.3 La réaction

La fonction de réaction doit être bien définie pour permettre au SOC de bien réagir face à un incident de sécurité avéré, en coordonnant ou non avec le CSIRT. Il peut :

- ∞ Faire des investigations car disposant d'outils de détection, d'investigation lui permettant d'analyser des logs passés, des rapports de scans, des produits de sécurité, du forensiques, etc.
- ∞ Agir au moment de la détection par exemple en fermant un compte administrateur, en ajoutant ou activant une règle du pare-feu ou de l'IDS, etc.

A ces dernières fonctions, s'ajoutent les services relatifs à l'administration de sécurité qui est l'administration fonctionnelle des outils de sécurité avancés. Ce dernier volet peut contenir les services suivants :

- ∞ La gestion des droits et des dérogations
- ∞ La gestion des administrateurs et des privilèges
- ∞ L'administration des équipes de sécurité.

2.3.3 Fonctionnement d'un SOC

Le fonctionnement d'un SOC nécessite un certain nombre de fonctions adaptables en fonction des besoins de l'entreprise. Ces fonctions sont en général les suivantes (Clusif, 2017) :

- ∞ Le pilotage : ayant pour rôle de définir les objectifs et stratégie du SOC, ainsi que la validation des évolutions de ce dernier sur les plans technique, organisationnel et fonctionnel.
- ∞ La fonction opérationnelle : composée d'analystes, d'ingénieures, experts répartis en trois niveaux et sous la responsabilité d'un Manager. Le niveau gère les opérations d'analyse continue ainsi qu'un le traitement des incidents procédures. Le niveau 2 apporte une expertise complémentaire au niveau 1 ; le niveau 3 quand lui n'intervient qu'en cas d'alertes critiques non procédurées en renfort au niveau 2. Le mécanisme permettant de transférer la résolution d'un incident d'un niveau inférieur à un niveau supérieur s'appelle l'escalade (voir paragraphe suivant).
- ∞ La gestion et la maintenance des outils du SOC (SIEM, IDS/IPS, …) afin qu'ils soient opérationnels et prévenir de potentielles pannes.

- La consolidation et le reporting permettant le suivi des alertes traitées et des plans d'actions associés.
- La contextualisation servant d'interface avec les interlocuteurs appartenant aux autres services métier de l'entreprise comme la DSI.

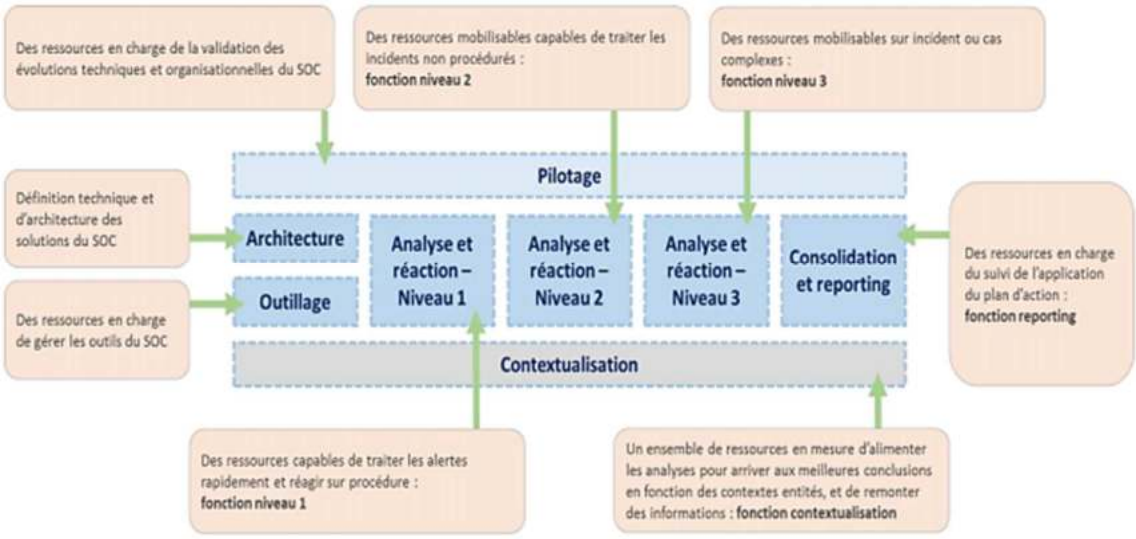


Figure 3: Structure de fonctionnement d'un SOC (Clusif, 2017)

2.3.4 Le mécanisme d'escalade

La figure suivante tirée de l'ouvrage *Ten Strategies of a World-Class Cybersecurity Operations Center* ((Mitre), 2014) résume les rôles opérationnels du SOC ainsi que le mécanisme d'escalade en cas d'incident.

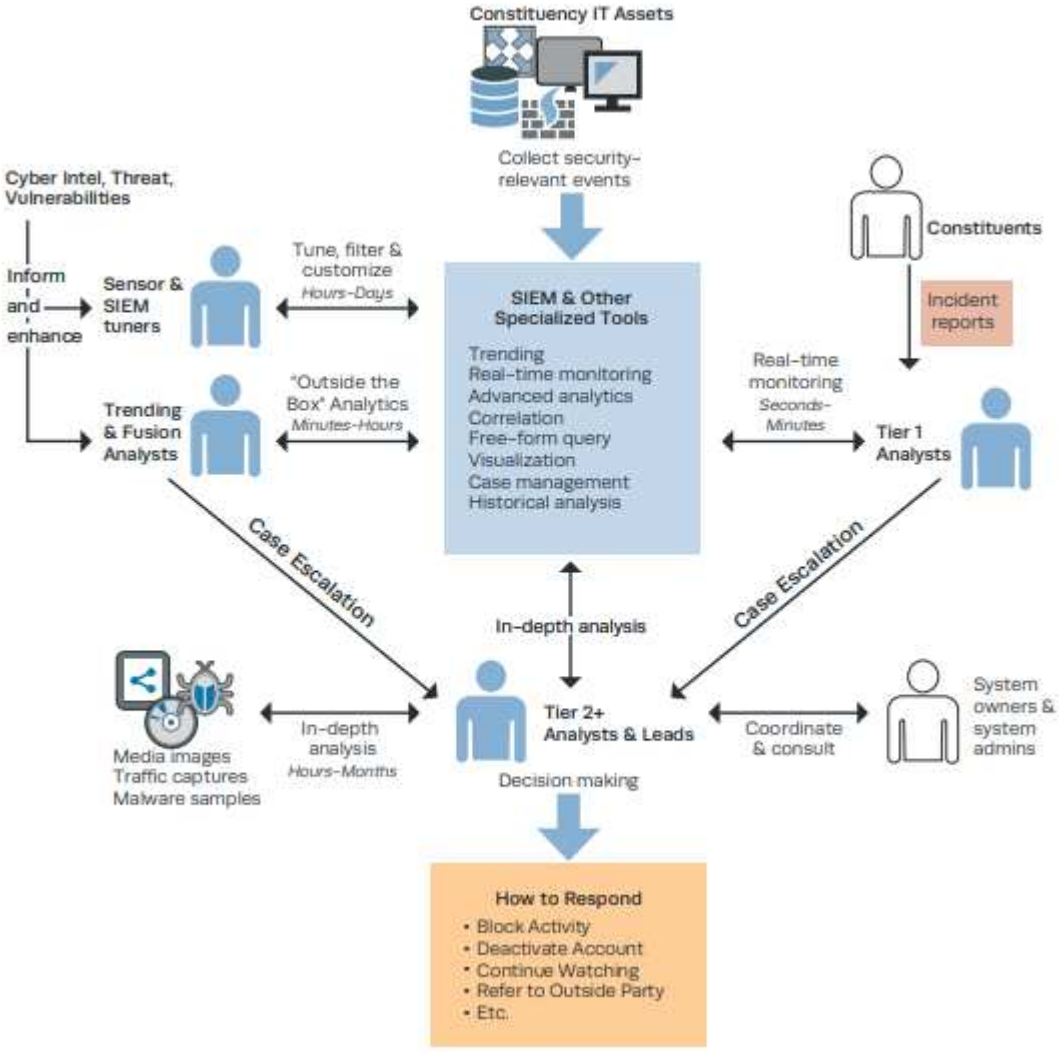


Figure 4: Rôles et mécanisme d'escalade ((Mitre), 2014)

2.4 Technologies nécessaires

Un SOC ne peut être mis en place sans un SIEM, en effet ce dernier constitue l'épine dorsale d'un SOC. Cependant, de nos jours, il existe d'autres technologies qui démontrent leur importance au niveau du SOC, il s'agit des technologies de gestion de la conformité, du threat intelligence, de gestion des vulnérabilités et d'analyse du comportement.

2.4.1 SIEM

2.4.1.1 Définition

La technologie SIEM assure la collecte, le regroupement, la normalisation et la conservation des logs adéquats, la collecte de données de contexte, l'analyse (y compris la corrélation et la hiérarchisation), la présentation (notamment la création de rapport et la visualisation), mais aussi les workflows et les contenus relatifs à la sécurité. Tous les cas pratiques d'utilisation de la technologie SIEM se concentrent sur la sécurité des informations, du réseau et des données mais aussi sur la conformité aux réglementations. ((Chuvakin)).

2.4.1.2 Fonctions d'un SIEM

Un bon SIEM doit proposer au moins les fonctions suivantes :

- La collecte des données de contexte et des logs
- La normalisation et la catégorisation
- La corrélation
- La notification et les alertes
- La hiérarchisation
- Les vues en temps réel
- La création de rapports
- Le workflow des rôles de sécurité

2.4.2 Outils de gestion de la conformité

Les solutions de gestion de la conformité permettent une solide gestion du cycle de vie des informations liées aux réglementations et aux produits/processus, ainsi qu'une gestion des politiques d'entreprise, de santé/sécurité et des procédures opérationnelles standard. Dans le cas d'un SOC, ces outils devront permettre :

- La vérification de la configuration de l'ensemble des systèmes et des équipements d'infrastructure.
- La conformité aux politiques de sécurité, la norme ISO27001 par exemple

2.4.3 Outils d'analyse de la sécurité de renseignement sur le menaces (Threat Intelligence)

Selon la définition du Gartner, la threat intelligence est « la connaissance fondée sur des preuves, y compris le contexte, les mécanismes, les indicateurs, les implications et des conseils concrets, concernant une menace nouvelle ou existante ou un risque pour les actifs d'une organisation qui peuvent être utilisés afin d'éclairer les décisions concernant la réponse du sujet à cette menace ou un danger. » (Moutaib, 2016). Elle permet ainsi de pouvoir réagir efficacement aux cyberattaques, de mettre l'entreprise dans une posture de vigilance et de lui fournir les atouts nécessaires pour endiguer l'impact des cyberattaques. Elle se base sur trois principes :

- Renseignements opérationnels : données techniques liées à des attaques pouvant affecter une entreprise en particulier,
- Renseignements tactiques : avec pour objectif de fournir aux équipes du SSI des prévisions méthodologiques contextualisées à six (6) mois et des
- Renseignements stratégiques : qui permettent aux entreprises de prévoir l'impact de la sécurité sur une partie « business ».

2.4.4 Outil de gestion des vulnérabilités et de tests de pénétration

Cet outil devra permettre d'effectuer entre autres opérations, des tests de vulnérabilité, l'audit des communications unifiées, la détection des points de terminaison et la détection des fuites de réseau, l'évaluation de la disponibilité, etc. La gestion des vulnérabilités et des tests de pénétration se définit sous forme de cycle car c'est un processus qui permet de tester la résilience du système et doit donc être répéter à des intervalles de temps réguliers ou à la demande.

CHAPITRE 3 : Conception d'un SOC

3.1 Les ressources humaines

La connaissance des fonctions principales d'un SOC, qui peuvent différer d'une organisation à une autre car les besoins n'étant pas souvent les mêmes, permet de déterminer la composition l'équipe SOC. Si dans certaines organisations où l'importance d'un SOC est reconnue, celui dispose des privilèges et des ressources adéquates permettant à son équipe d'inclure les compétences nécessaires pour bien fonctionner, dans d'autres organisations cependant, il existe une équipe par défaut qui essaie remplir ces rôles.

Les équipes SOC ont généralement des postes couvrant deux responsabilités de base à savoir : la maintenance et le management des outils de surveillance de la sécurité et la recherche des activités suspectes (Siemplify, 2017).

- ∞ Management et maintenance des outils de surveillance de la sécurité :

Il existe une panoplie d'outils de sécurité, cependant, sans une configuration appropriée, il est impossible de sécuriser et surveiller efficacement le système. Ainsi le rôle de l'équipe SOC est de gérer et mettre à jour régulièrement les différents outils utilisés ainsi que la collecte de données sur l'ensemble de l'infrastructure. Ces données sont par la suite transmises au SIEM avant d'être sujettes à l'analyse.

- ∞ Recherche d'activités suspectes :

Comme nous l'avons précisé tantôt, l'équipe SOC a recours à des outils (SIEM notamment) qu'elle doit gérer et surveiller. Ces derniers doivent lui permettre de pouvoir rechercher les activités suspectes et/ou potentiellement malveillantes sur l'étendue de l'infrastructure. La plupart de ces outils permettent de générer des alertes afin d'avertir l'équipe en cas de potentiels problèmes de sécurité et donner la possibilité à cette dernière de faire l'examen et la qualification de la menace. La combinaison d'outils et d'expertise appropriée sont les ingrédients nécessaires à la réussite d'une équipe SOC.

On note en général une segmentation des rôles en 4 niveaux ou tiers avec, pour chacun, des compétences et des responsabilités bien distinctes.

3.1.1 Tiers 1 : Analystes de sécurité

Ce sont des spécialistes du triage et sont les premiers à réagir en cas d'alerte pour en déterminer la pertinence et l'urgence. Ils peuvent répondre aux menaces si la pertinence de ces dernières est de leurs ressort et dans le cas contraire, générer un ticket d'incident à l'endroit des tiers de niveau 2. Ils peuvent gérer et configurer les outils de surveillance et faire des analyses ainsi que l'examen des rapports de vulnérabilités.

Les compétences sont requises des analystes de sécurité :

- ∞ Des compétences en administration système (Linux, Mac, Windows)
- ∞ Des connaissances en programmation (Python, Perl, Ruby, PHP, C, C#, Java, etc.),
- ∞ Des compétences en sécurité (CISSP, GCIA GCIH, etc.).

3.1.2 Tiers 2 : Ingénieurs de sécurité

Leur principal rôle est de répondre aux incidents de sécurité. Ils doivent, en plus des compétences des analystes de niveau 1, faire preuve d'obstination dans la recherche de causes et, pouvoir faire face au stress. Avoir été un ancien hacker serait un gros plus. Les analystes de niveau 2 ont aussi d'autres responsabilités à savoir :

- ∞ Examiner les fichiers de dérangement générés au niveau 1 ;
- ∞ Identifier les systèmes affectés en utilisant les renseignements sur les menaces émergentes ;
- ∞ Déterminer et recueillir les données des actifs (configurations, processus en cours, etc.) sur ces systèmes pour une analyse plus approfondie.
- ∞ Documenter les exigences, les procédures et les protocoles pour garantir que les autres utilisateurs disposent des ressources appropriées.

3.1.3 Tiers 3 : Experts sécurité

Ce sont des chasseurs de menaces et ils doivent être familiarisés à l'utilisation des outils de visualisation et de tests de pénétration (penteste) en plus des capacités des niveaux 1 et 2. Les experts de niveau 3 ont les responsabilités suivantes :

- ∞ Analyser les données de découverte d'actifs et d'évaluation des vulnérabilités ;
- ∞ Explorer des moyens d'identifier les menaces furtives qui peuvent être trouvé dans le réseau de l'entreprise sans qu'elles aient pu être détectées.
- ∞ Effectuer des tests de pénétration sur le système afin d'en vérifier la résilience et identifier les points faibles à corriger.
- ∞ Faire des recommandations pour l'optimisation des outils de surveillance en fonction des données de découverte des menaces.

3.1.4 Tiers 4 : Manager du SOC

Le SOC manager est le chef de l'exploitation du SOC. Il supervise l'activité du SOC et est chargé de définir les opérations de sécurité de l'organisation, le processus de recrutement, de formation, d'escalade et d'évaluation. Il gère l'élaboration et l'exécution des plans de communication de crise pour le RSSI et les autres parties prenantes. Il est chargé d'exécuter les rapports de conformité et prend en charge le processus d'audit et a le devoir de rendre compte au top management sur les performances du système. Le manager d'un SOC doit naturellement avoir du leadership et des capacités en communication sans oublier les connaissances sur les domaines de chacun des niveaux précédents.

3.2 Cadrage fonctionnel et technique

3.2.1 Cadrage fonctionnel

Le cadrage fonctionnel dépend des services qu'offre le SOC à l'entreprise. Ainsi en fonction de ces services, nous allons définir quelques processus notamment : le processus de détection, le processus de qualification, le processus de gestion des incidents, le processus supervision, de contrôle et d'administration, le processus de veille.

3.2.1.1 *Processus de détection*

Le processus de détection est axé sur les moyens de supervision des risques et la réception d'alerte. En effet c'est dans cette activité que les sorties provenant des dispositifs d'alertes, de la veille sécurité SI, des sollicitations des équipes externes ou help desk, les incidents provenant des dispositifs de supervision, sont examinées. Ainsi les analystes de niveau 1 procèdent d'abord à un filtrage/triage des évènements entrant afin d'évaluer leur pertinence. Dans le cas où les tiers de niveau 1 ne peuvent pas traiter l'alerte ou si l'alerte en est à sa première occurrence, ils font appel au niveau 2 (processus escalade). Le niveau 2 exécute le processus de qualification et le processus d'administration fonctionnelle du SOC pour mettre à jour les règles et les seuils de détection, amender les critères et seuils d'invocation du niveau 2.

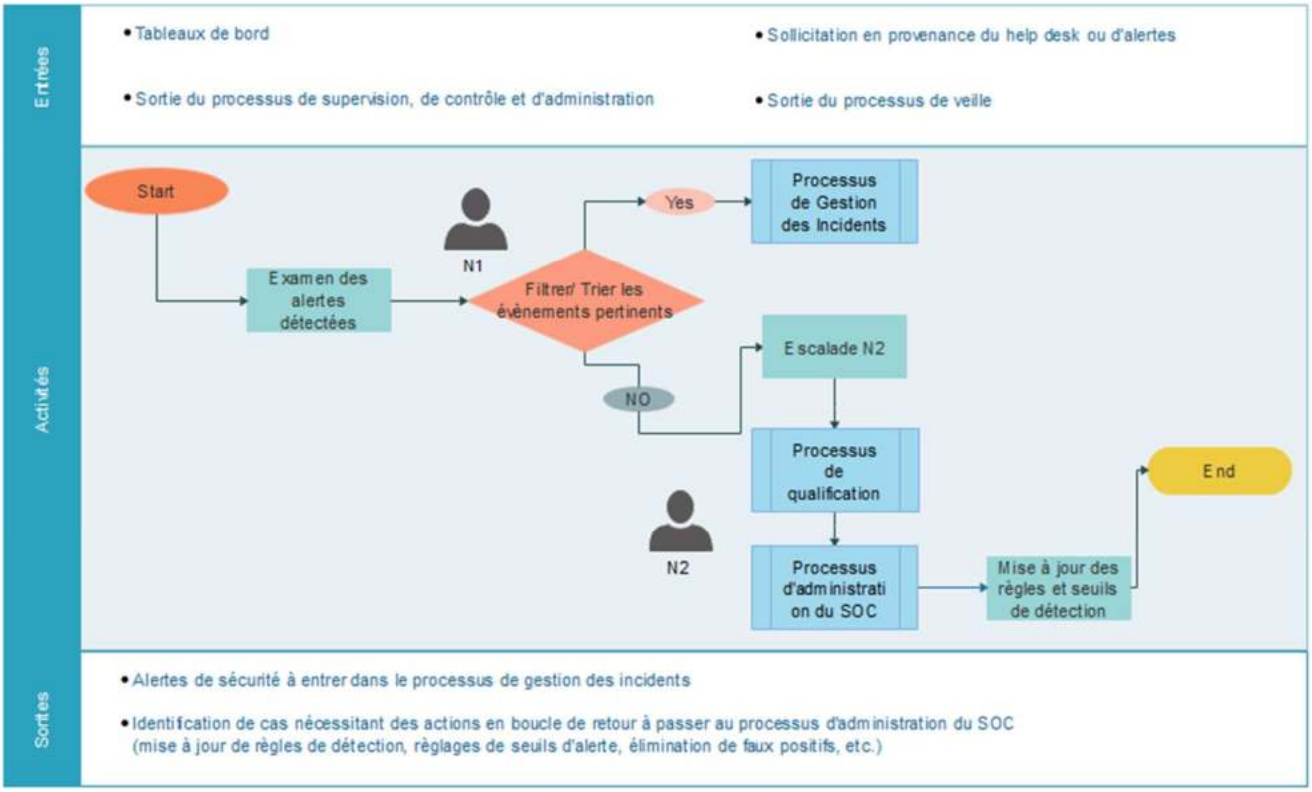


Figure 5: Processus de détection

3.2.1.2 *Processus de qualification*

L'ensemble des tâches de ce processus sont dévolues aux tiers de niveau 2 ; il inclut essentiellement :

- ∞ L'étude des alertes provenant du niveau 1
- ∞ L'enrichissement et la contextualisation de ces alertes
- ∞ La détermination de la véracité et de sévérité des incidents
- ∞ L'isolation et la description de faux positifs afin de les passer en entrée du processus d'administration du SOC

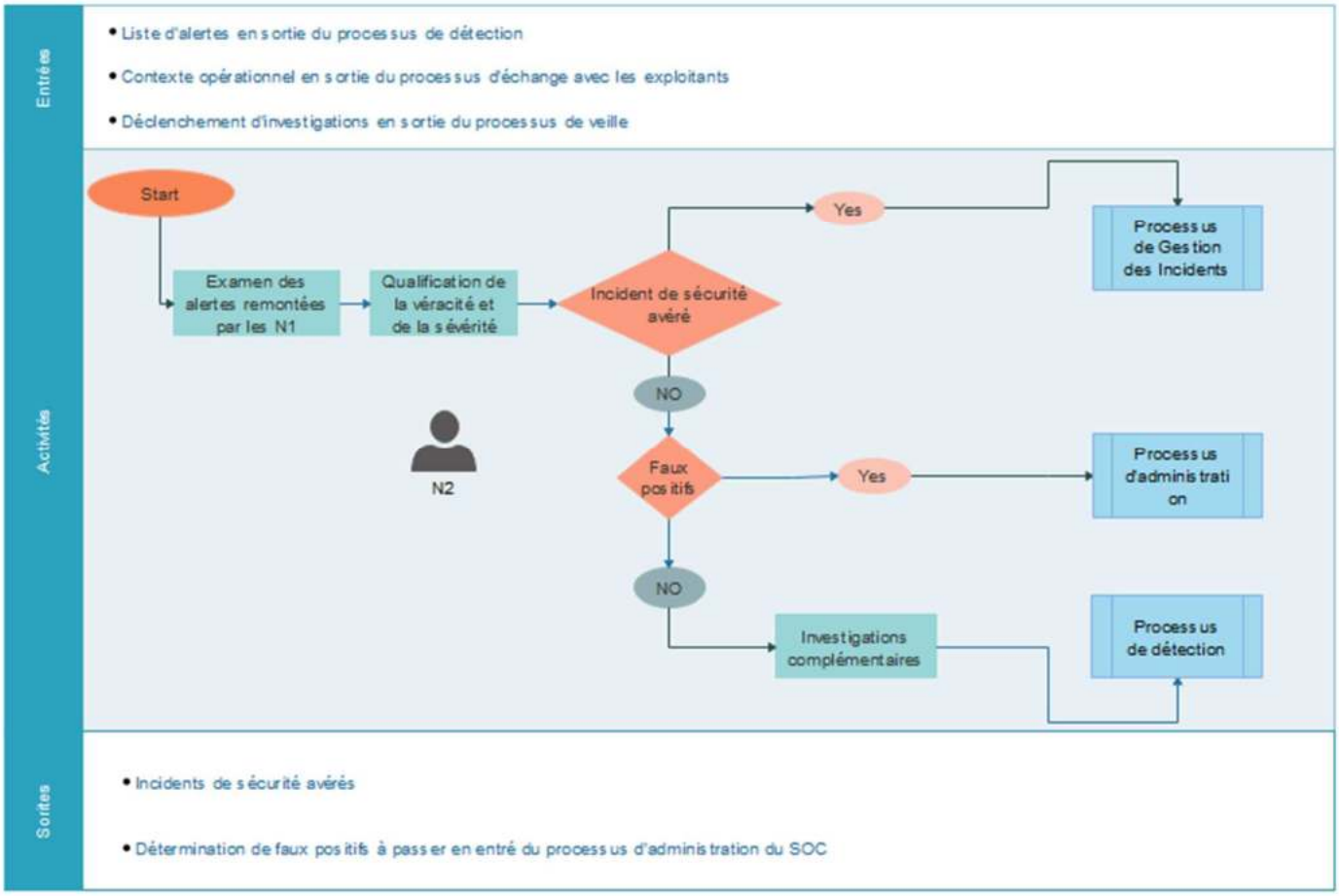


Figure 6: Processus de qualification

3.2.1.3 Processus de gestion des incidents

Les processus de détection, de qualification et de veille alimentent ce processus. Ainsi la gestion des incidents, est un processus où peuvent intervenir tous les membres de l'équipe SOC.

Il permet de définir le workflow de la gestion des incidents et peut se baser sur des référentiels (ITIL par exemple) ; et produit à la sortie, un retour d'expérience ainsi que l'amélioration des règles du SOC.

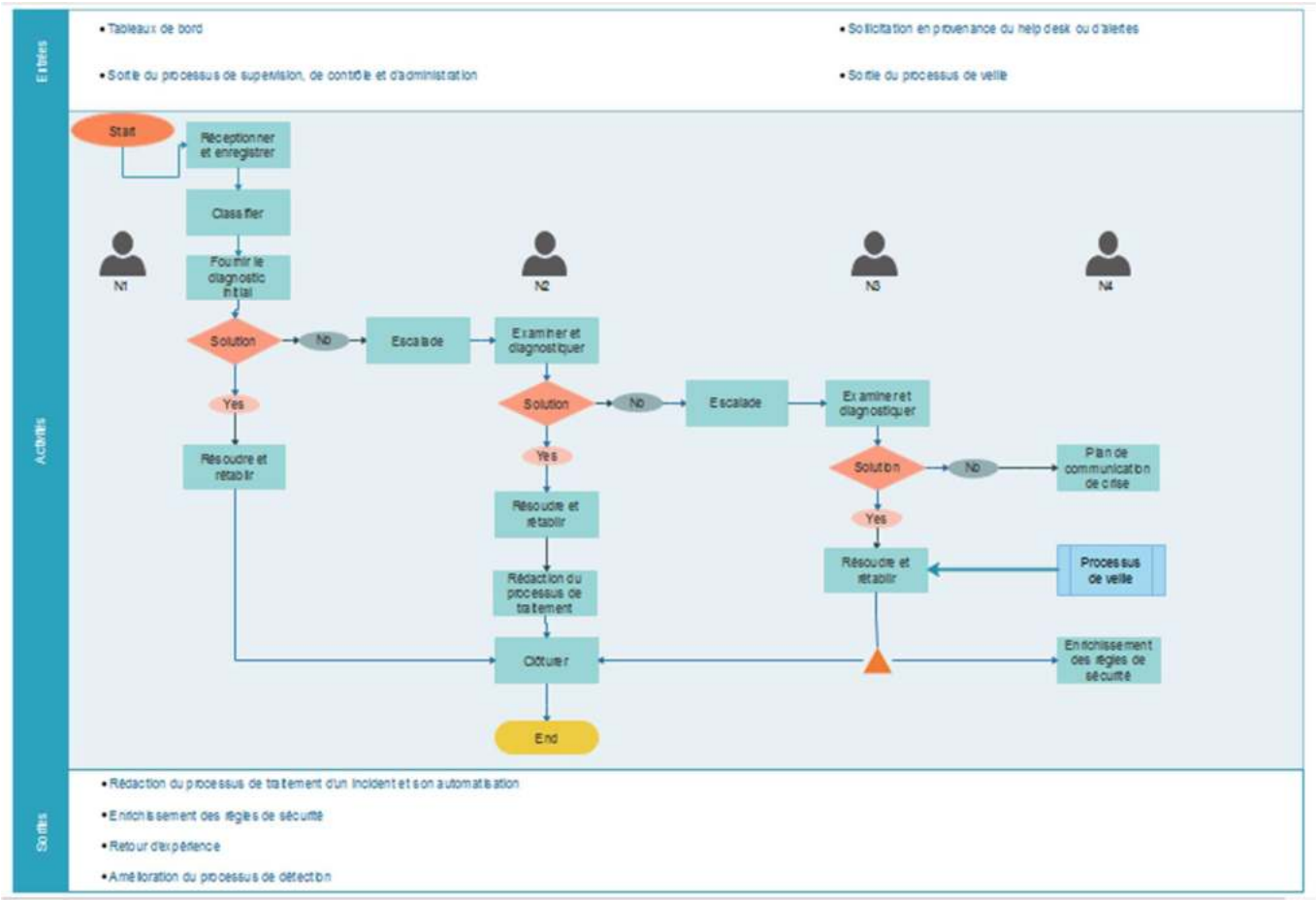


Figure 7: Processus de gestion des incidents

3.2.1.4 Processus de supervision, de contrôle et d'administration

Seul élément concerné par la supervision, le périmètre choisit du SI doit être supervisé en constance par les analystes.

La définition permet de mieux détecter et qualifier tout incident de sécurité. Ainsi, il est important, pour ne pas saturer la détection et la qualification, de contrôler les seuils définis dans ces règles.

L'administration du SOC permet, en général, l'amélioration continue des performances du SOC, et en particulier, l'optimisation des fonctions de détection et de qualification.

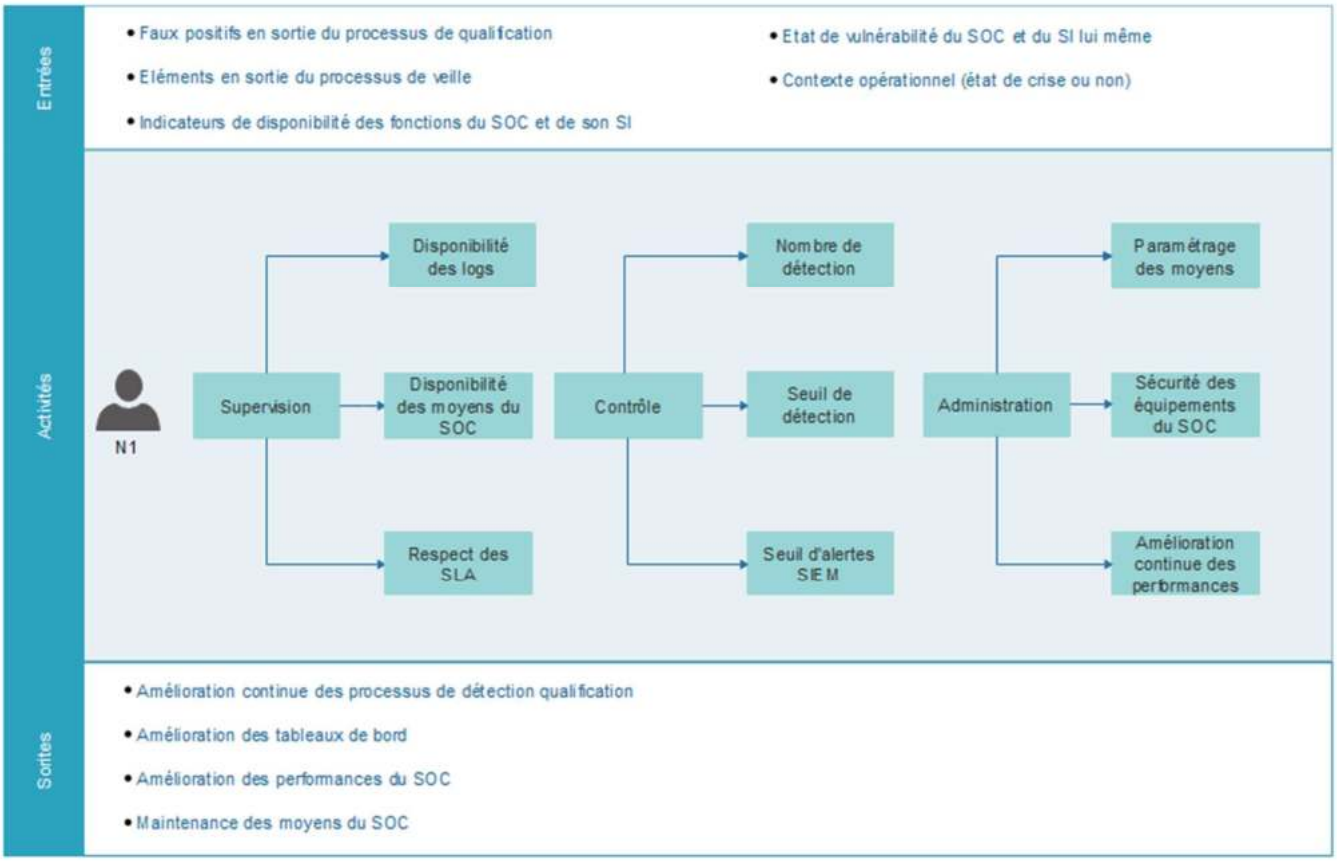


Figure 8: Processus de supervision, de contrôle et d'administration

3.2.1.5 Processus de veille

La veille est une fonction très importante dans un SOC car permettant de rester en alerte par rapport aux cybermenaces et vulnérabilités du SI. Ainsi elle incombe à tous les acteurs du SOC des analystes niveau 1 au manageur SOC.

Les principales tâches sont :

- La collecte et la synthèse des scénarios d'attaque, la collecte et la hiérarchisation des avis de sécurité ; rester informés des vulnérabilités des composants du SI supervisés. Ils doivent également s'assurer de l'efficacité des règles en fonction des nouvelles vulnérabilités et alertes.
- Le responsable du SOC agit dans le processus en supervisant la mise à jour de son équipe quant aux tendances d'évolution des menaces, des moyens de détection ainsi que de l'évolution du cadre règlementaire et des exigences métiers. Il doit également suivre des actions correctives ou préventives à moyen et long terme.

3.3 Cadrage technique

Le cadrage technique doit se concentrer sur le choix des outils en fonction des équipements à surveiller. La collecte de données et la supervision étant des opérations phares dans un SOC, il convient donc de les prendre en charge.

Différentes sources sont à l'origine de traces et d'évènements qui constituent les matières premières d'un SOC.

Parmi ces sources on peut distinguer les composants standards et de sécurité du système et les composants spécialisés.

Les composants standards du système sont des outils déjà mis en œuvre sur le SI indépendamment du SOC. Il s'agit entre autres de serveurs d'applications (serveurs Web, LDAP, etc.), de routeurs, etc. Ces derniers génèrent des logs bruts qu'il faut traiter avant que cela ne soit vraiment utilisable.

Les composants de sécurité du système sont les équipements tels que les firewalls (Iptables, PANDA, etc.), les antivirus, les scanneurs de vulnérabilité (Nessus), etc. qui fournissent des informations plus exploitables par le SOC.

Les composants spécialisés du SOC sont des équipements de sécurité qui génèrent des logs et des évènements de sécurité. Ce sont spécialement : les IDS, les outils de capture.

Ces différents équipements constituent une source d'évènements et de traces pour le SOC.

Le SOC doit aider à augmenter le niveau de sécurité du SI en cela, il est nécessaire dans un premier temps de sécuriser la plateforme ou la solution utilisée et d'activer l'authentification des utilisateurs (LDAP, Active Directory, etc.)

De plus pour éviter le nombre de faux positif ou de faux négatif, il est nécessaire de disposer d'une base de vulnérabilités et de faire des tests de pénétrations pour entrainer le SOC à mieux détecter et reconnaitre les attaques.

3.4 Architecture fonctionnelle et technique

Le type d'architecture dépend du type de SOC et de la taille de celui-ci. En effet dans la mise en place de l'architecture d'un SOC, il convient de prendre en compte aussi bien le périmètre c'est-à-dire identifier les équipements et services à prendre en compte, que les contraintes surtout celles inhérentes à l'entreprise.

La mise en place d'un SOC est chronophage et nécessite une quantité de travail importante pour produire des résultats, c'est pourquoi il est important de limiter sa couverture, dans un premier temps, afin d'avoir des résultats concluants rapidement (compétences, 2016).

De plus le choix des systèmes à intégrer est crucial c'est pourquoi dans notre étude, nous avons décidé d'intégrer des systèmes tels que les firewalls, les serveurs, les applications et autres systèmes sensibles.

Néanmoins, quel que soit le type choisi, un SOC est toujours constitué des trois éléments suivants : les ressources humaines, les processus et les moyens techniques et matériels.

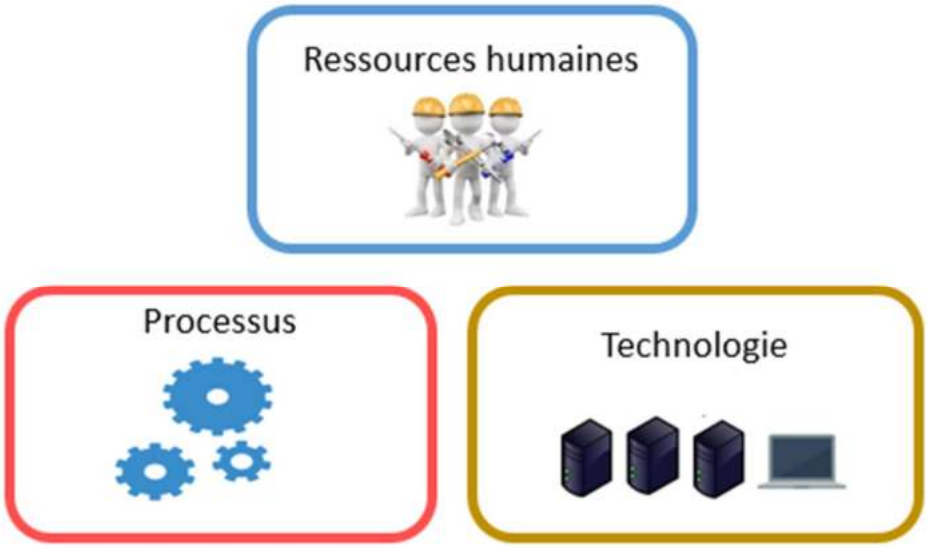


Figure 9: Fondamentaux d'un SOC

3.4.1 Architecture fonctionnelle

L'architecture fonctionnelle reprend les principales lignes du cadrage fonctionnel. En effet les différentes activités détaillées dans les principaux services et les différents rôles et outils vont constituer l'ossature de cette architecture.

Dans un premier temps le système fait du monitoring et de la corrélation des logs collectés et des évènements de sécurité issus du SI (log d'applications, serveurs, équipements réseaux). Les analystes de niveau 1 sont en charge de cette mission en plus des tests de vulnérabilité, de la détection et de la résolution d'incidents mineurs. Si l'incident relève d'un niveau supérieur, ils le retransmettent au niveau 2 où sont faites des analyses plus approfondies.

L'analyste de niveau 2, en plus de traiter les tickets transmis par le niveau 1, collecte et utilise les renseignements sur les menaces récentes ou en vogue et les captures de trafic afin de mieux traiter les incidents. Il dirige et détermine les plans d'assainissement et de reprise d'activité. Il peut consulter et assister dans certains cas le SOC Manager dans la prise de décision.

Les analystes de niveau 3 règlent, filtrent et personnalisent le système. Ils traitent les données de vulnérabilité et font des tests de vulnérabilité et d'intrusion afin de tester la résilience du système. Ils conseillent sur le choix des outils de surveillance de sécurité et déterminent les zones ayant une sécurité minimale. Le transfert de certains résultats aux analystes de tiers 2 permet à ces derniers de mieux réagir face aux incidents.

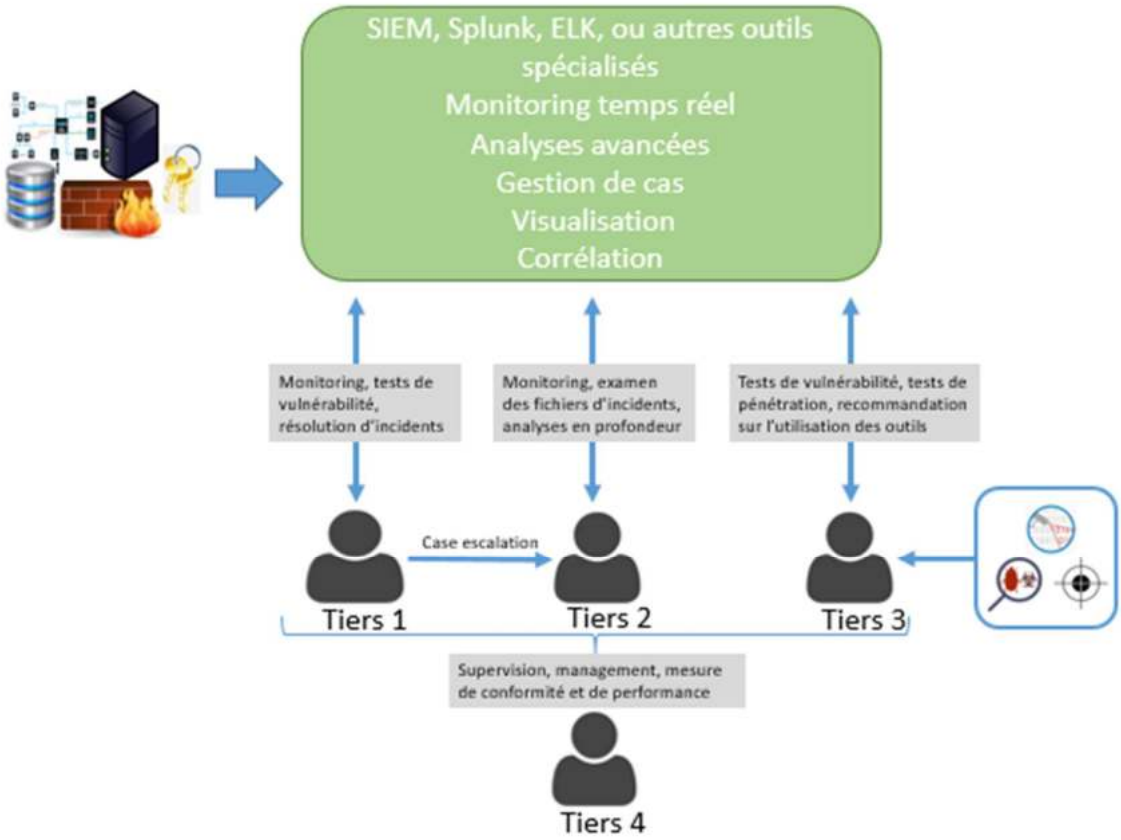


Figure 10: Workflow d'un SOC

3.4.2 Architecture technique :

L'architecture du SOC s'étend à toutes les couches du modèle TCP/IP. Ce pendant pour mieux faire ressortir l'architecture de déploiement adoptée, nous avons utilisé les couches suivantes :

- Application : représentant l'ensemble des applications de l'entreprise qui doivent être supervisées.
- La couche sécurité : contient le SIEM, ainsi que les autres outils nécessaires à la sécurité de la plateforme SOC et de l'entreprise à savoir : le serveur d'authentification, le proxy et les pares-feux.
- La couche réseau qui contient l'ensemble des équipements réseaux qui doivent être surveillés et fournir des logs. Il s'agit des routeurs, des commutateurs qui garantissent la connectivité.
- La couche physique regroupe les autres équipements de l'entreprise qui doivent aussi être supervisés à savoir : les serveurs, les machines du LAN, etc.

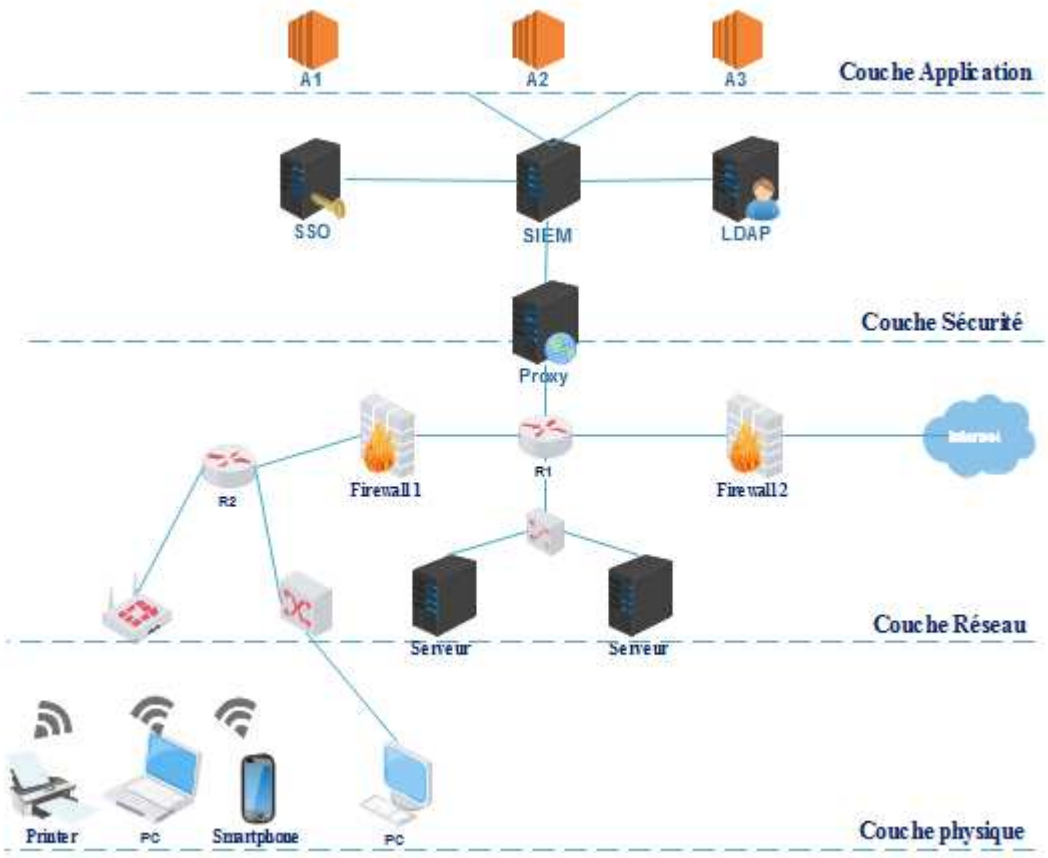


Figure 11: Architecture technique d'un SOC

3.5 Conception détaillée

3.5.1 Cas d'utilisations

Plusieurs cas d'utilisation peuvent être orchestrés. Ce pendant au vu de l'actualité des cyberattaques, où les ransomwares sont en vedette, des malwares qui sont omniprésents et de l'imprégnation forte dans l'internet des objets, nous avons senti le besoin de nous focaliser sur les trois cas d'utilisation suivants :

- Monitoring for suspicious connectivity: supervision des connections suspectes.
- Compromise and infected system tracking: malware detection: suivi des systèmes compromis ou infectés: detection de malware.
- Tracking for IoT devices Vulnerability : suivi des vulnérabilités des appareils IoT.

3.5.1.1 Supervision des connexions suspectes :

La connexion des réseaux d'entreprise et des réseaux publics constitue un véritable défi en matière de sécurité des informations, car les connexions donnant accès aux employés et aux clients peuvent également constituer une porte ouverte pour ceux qui souhaitent attaquer le réseau et ses applications.

Le trafic réseau sortant reste un point faible pour de nombreuses entreprises et constitue un vecteur d'attaque majeur.

La principale raison de verrouiller le trafic sortant de manière aussi sécurisée que le trafic entrant est sans aucun doute pour se préserver des attaques de Déni de Service Distribué (DDoS Distributed Deny of Service).

Une attaque par déni de service (DoS pour Denial of Service) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser (Définition Wikipédia).

Ainsi le but de cas d'utilisation est d'entrainer le SOC afin qu'il puisse détecter rapidement voire même prévenir une attaque par déni de service.

3.5.1.2 Détection de malware

Les attaques par malware, font partie des cyberattaques les plus répandues. Ces attaques deviennent de plus en plus pernicieuses. En effet il suffit juste de voir l'ampleur des attaques du Wannacry, du Petya ou même du NotPetya pour s'en convaincre.

Ainsi l'un des buts premiers d'un SOC est de pouvoir se prémunir de tels types attaques en fournissant un détecteur de logiciels malveillants qui tente de protéger le système en détectant les comportements malveillants. Le détecteur de logiciels malveillants doit utiliser des techniques d'apprentissage automatique pour la détection des logiciels malveillants.

3.5.1.3 Suivi des vulnérabilités dans l'Internet des objets

L'émergence de nombreux fabricants produisant des appareils pour l'internet des objets (IoT) a suscité de nouvelles préoccupations en matière de sécurité.

De nombreux périphériques IoT présentent des failles de sécurité les rendant vulnérables aux attaques et les fabricants ont des difficultés à fournir des correctifs de sécurité appropriés à leurs produits en temps opportun et de manière convenable.

Fournir un système visant à protéger le réseau de l'utilisateur contre les périphériques vulnérables.

Le système devra identifier automatiquement les périphériques vulnérables lorsqu'ils sont introduits pour la première fois sur le réseau.

3.5.2 Exploitation des cas d'utilisation

Etudier ces cas d'utilisation et en général un cas d'utilisation en sécurité nécessite des logs intéressants en sécurité. De plus la politique de sécurité de la structure d'accueil ne nous permettant pas de prendre les logs de production, nous nous sommes tournés vers des sites proposant des logs en sécurité. Ainsi les sites comme SecRepo et MawareAnalysis, entre autres, proposent un ensemble varié de logs de sécurité.

Aussi quelque que soit le cas d'utilisation, l'exploitation comporte généralement 3 grandes parties :

- ∞ Exploitation des journaux
- ∞ Définition des règles
- ∞ Détection et affinage

3.5.2.1 Exploitation des logs

L'exploitation débute par l'identification des équipements et applications capables de fournir des logs pertinents en rapport avec le cas d'utilisation. Ceci peut résulter de la description et d'un examen du cas d'utilisation. Cette activité peut être sautée dans le cas où le cas d'utilisation est documenté mais il est toujours bien de répéter ces activités pour s'assurer que tous les journaux sont identifiés.

Ensuite il convient de trouver les évènements pertinents dans ces logs. Un fichier de logs peut contenir plusieurs évènements n'ayant pas tous forcement de relation avec le cas d'utilisation donc il est important de bien comprendre aussi bien le cas d'utilisation que la source des logs et de faire si nécessaire des tests.

De plus il faut vérifier les configurations des journalisations pour être sûr d'enregistrer les bons journaux. Il faut garder à l'esprit que l'activation de l'audit ou la modification des configurations peut avoir un impact sur les performances, d'où la nécessité de faire des tests.

Les trois étapes faites, il reste à configurer l'intégration des journaux sur le système de gestion des évènements. Certains journaux peuvent être directement envoyés au gestionnaire d'évènements (via socket, REST client, etc.) c'est le cas du répertoire syslog dans les distributions Unix. Cependant d'autres nécessitent des connecteurs spécialisés intégrés au système de gestion comme pour le cas des journaux Windows afin d'en faciliter l'ingestion.

3.5.2.2 Définition des règles

3.5.2.2.1 Règles par défaut

Ce sont un ensemble de règles déjà définies dans le système de gestion des logs. Cependant, selon les cas d'utilisation choisis, il ne faut prendre en compte que les règles pouvant déclencher le cas d'utilisation et veiller à comprendre leur fonctionnement. Les tester pour voir quelles activités déclenchent la règle, relever les faux positifs et si besoin les personnaliser.

3.5.2.2.2 Règles personnalisées

Dans le cas où il n'existe pas de règles par défaut permettant de déclencher le cas d'utilisation, où que des règles existantes peuvent le déclencher mais avec un nombre élevé de faux positifs ; il faut penser à écrire ses propres règles ou à personnaliser les règles existantes. Les règles personnalisées sont plus adaptées à l'organisation et ont plus de succès dans la détection du risque décrit. Cependant il est nécessaire de bien comprendre comment se fait la rédaction des règles. Afin de tester l'efficacité des règles personnalisées, une surveillance doit être faite dans le but de vérifier si elles produisent bien les résultats souhaités, et même aller jusqu'à simuler l'activité pouvant la déclencher pour arriver à des résultats concluants.

Les règles personnalisées doivent fournir les résultats souhaités exacts, dans le cas contraire il faut voir comment les améliorer. Une fois mises-à-jour, les tester à nouveau jusqu'à obtenir le résultat escompté et réduire au maximum les faux positifs.

Que ce soit pour les règles personnalisées comme pour les règles par défaut, les processus de triage, pour définir la manière de traiter les alertes déclenchées, doivent être définis. Cela permettra de déterminer si l'alerte est valide et si elle est critique. D'abord il faut vérifier si les processus de triage existants s'appliquent à ces nouvelles règles. S'il n'y a pas de processus de triage applicable, sa création est nécessaire. L'objectifs étant et minimiser le nombre de processus de tri différents tout en garantissant des processus de triage suffisants pour gérer les alertes générées par les règles.

Il faut aussi former le reste de l'équipe de détection de sécurité sur les règles, leur fonctionnement et le processus de triage et de gestion à utiliser lorsqu'elles alertent sur l'activité.

3.5.2.3 Détection et ajustement

Les cas d'utilisation vont d'une règle unique à plusieurs règles. Il est important de surveiller et d'évaluer la qualité des règles activées ainsi que leur couverture. Malgré le nombre très réduit de modèles ou de méthode de mesure en profondeur les mécanismes de détection, il faut en choisir un et l'adopter.

L'ajustement des règles à l'environnement de l'organisation est un processus continu car l'organisation est en continuelle mutation (ajouts de nouveaux serveurs, changement de pare-feu, etc.). Ces changements auront un impact sur le système de gestion des évènements en effet, un simple changement de configuration peut rendre une règle inefficace. Ils peuvent ainsi conduire à de nouveaux faux positifs affectant ainsi la capacité de détection. De ce fait, il faut mettre à jour les règles et veiller à ce qu'elles s'adaptent aux mutations ; le tout dans le but de d'améliorer continuellement la capacité de détection. La principale source d'informations à prendre en compte dans l'amélioration est le résultat des tris et de la réponse aux alertes. Ainsi après chaque alerte ou incident de sécurité validé, il faut se poser la question de savoir que peut-on encore modifier pour améliorer la détection ? Il est aussi impératif d'examiner périodiquement les évènements corrélés dans le système de gestion des évènements voir vérifier s'il y'a un changement léger ou radical. Cela est particulièrement vrai pour les règles personnalisées.

3.5.3 Conception du module ATISE (Automatisation des Tests d'Intrusion et de Simulation d'Equipements)

Durant notre étude, nous avons rencontré plusieurs difficultés notamment l'accès à des données de sécurité intéressantes qui constitue un problème commun dans toutes les études en sécurité informatique. De plus la plupart des outils utilisés, les SIEM par exemple, ne propose pas des fonctionnalités pouvant tester la résilience du système. C'est pourquoi nous avons pensé qu'il serait intéressant à partir de notre outil central de pouvoir lancer des tests d'intrusion et de simuler le fonctionnement de certains équipements grâce à un certain nombre de logs disponibles. Ce module nommé ATISE pour Automatisation des Tests d'Intrusion et de Simulation d'Equipements permettra ainsi de :

- ∞ Mesurer l'efficacité des stratégies développées pour le SOC
- ∞ Offrir au niveau 3, la possibilité d'implémenter des maquettes avant la mise en production
- ∞ Obtenir des rapports complets sur la vulnérabilité du SOC.

3.5.3.1 Fonctionnalités du module

Comme nous l'avons énoncé plus tôt, ce module devra avoir les fonctionnalités suivantes :

- ∞ Simuler un équipement (routeur, firewall, serveur, etc.)
- ∞ Lancer des campagnes de tests d'intrusion

- ∞ Comparer les résultats des différents tests
- ∞ Définir des privilèges suivant le type d'utilisateur en fonction de leurs rôles.

3.5.3.2 Les utilisateurs

L'exécution de tests d'intrusion étant de l'apanage des spécialistes du niveau 3, ces derniers seront les principaux utilisateurs de ce module. En effet responsables de la veille sur les nouvelles menaces et vulnérabilités, ces derniers ont souvent recourt à des tests pour évaluer la résilience du système afin mettre à jour au besoin les configurations de sécurité et ainsi optimisé la sécurité du système d'information.

Le SOC Manager aussi trouvera son intérêt dans ce module. En effet les rapports sur l'efficacité des stratégies développées obtenu à partir des statistiques sur les tests facilitent à l'administrateur du SOC les tâches d'audit et de mesure des performances.

3.5.3.3 Diagrammes

3.5.3.3.1 Diagramme de cas d'utilisation

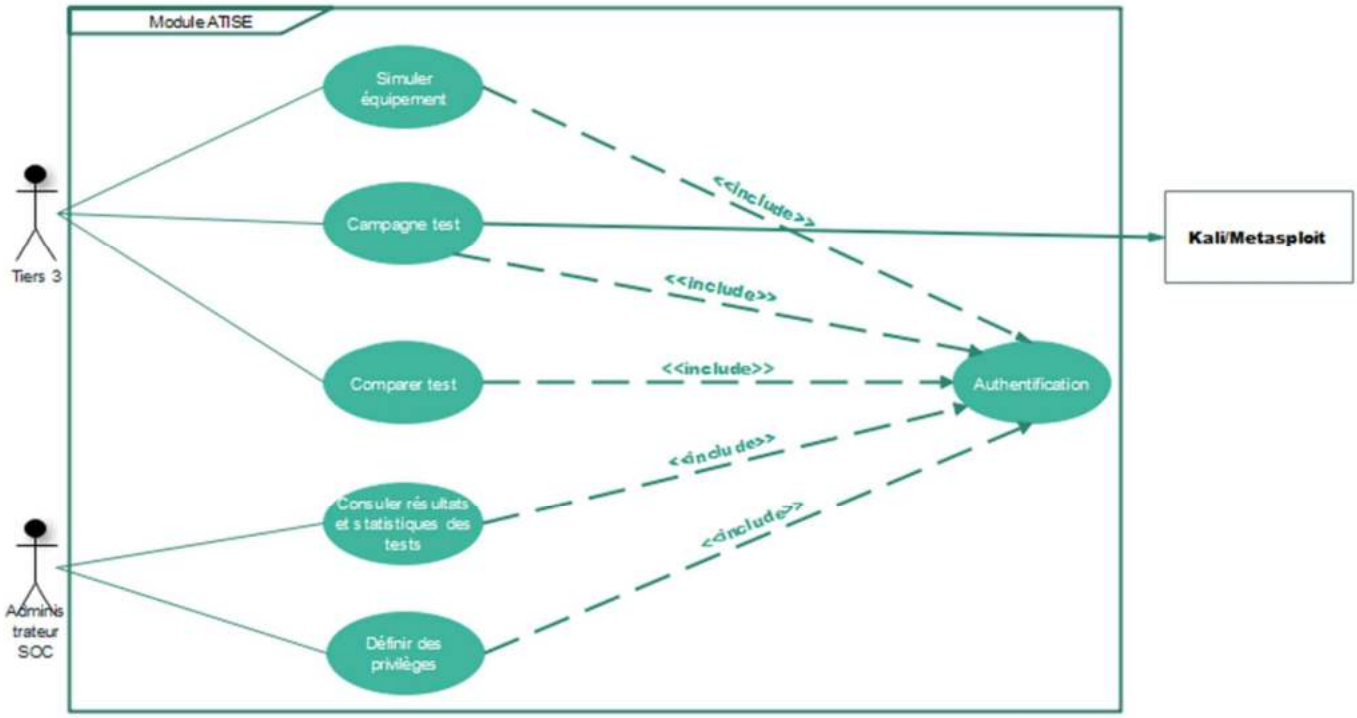


Figure 12: Diagramme cas d'utilisation ATISE

3.5.3.3.2 Diagrammes de séquence :

3.5.3.3.2.1 Cas lancer campagne test :

- ∞ Diagramme de séquence

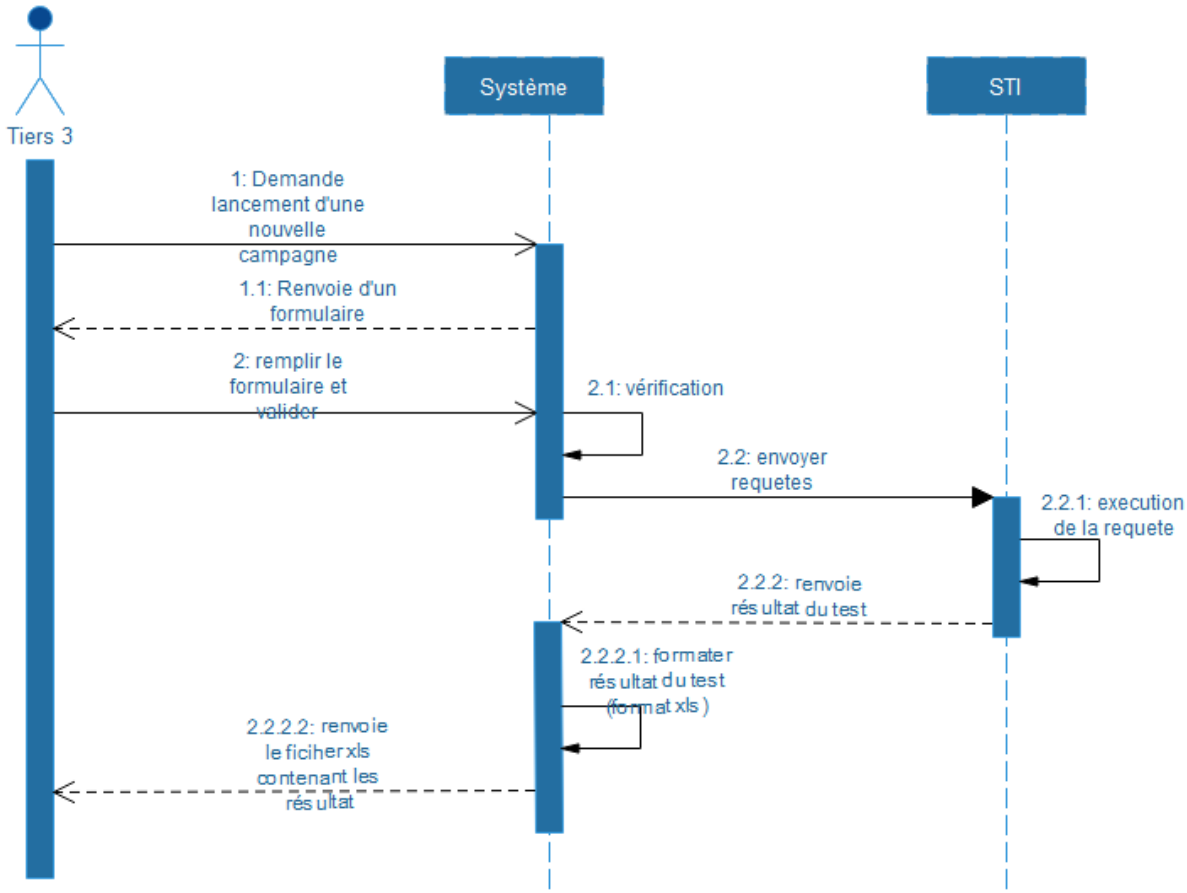


Figure 13: Diagramme de séquence lancer_campagne_test

∞ Description textuelle

Tableau 1: Description cas Lancer_campagne_test

Titre	Lancer_campagne_test
Description	
Acteurs	Tiers niveau 3
Précondition	L'utilisateur a accès à la plateforme et dispose des privilèges nécessaires
Scénario nominal	1. L'administrateur clique sur le menu de lancement d'une nouvelle campagne test 2. Le système lui renvoie un formulaire à remplir 3. Le tiers 3 remplit le formulaire et le valide 4. Le système vérifie la fiabilité des données soumises 5. Le système envoie les requêtes nécessaires au serveur de test d'intrusion 6. Le serveur de test d'intrusion exécute les requêtes

	7. Le serveur de test d'intrusion renvoie les résultats de tests au système 8. Le système formate les résultats au format xlsx 9. Le système renvoie le fichier xlsx contenant les résultats à l'utilisateur 10. Le système retourne l'utilisateur sur la liste des tests
Scénario alternatif	Etape 4 : Les données soumises par l'utilisateur ne sont pas valides. Le système renvoie un message d'erreur à l'utilisateur. Le scénario nominal reprend à l'étape 2
Post condition	Etape 5 : Le système ne parvient pas à joindre le serveur de test d'intrusion. Le système génère des erreurs pour l'utilisateur et met fin à la campagne de test

3.5.3.3.2.2 Cas gérer privilèges :

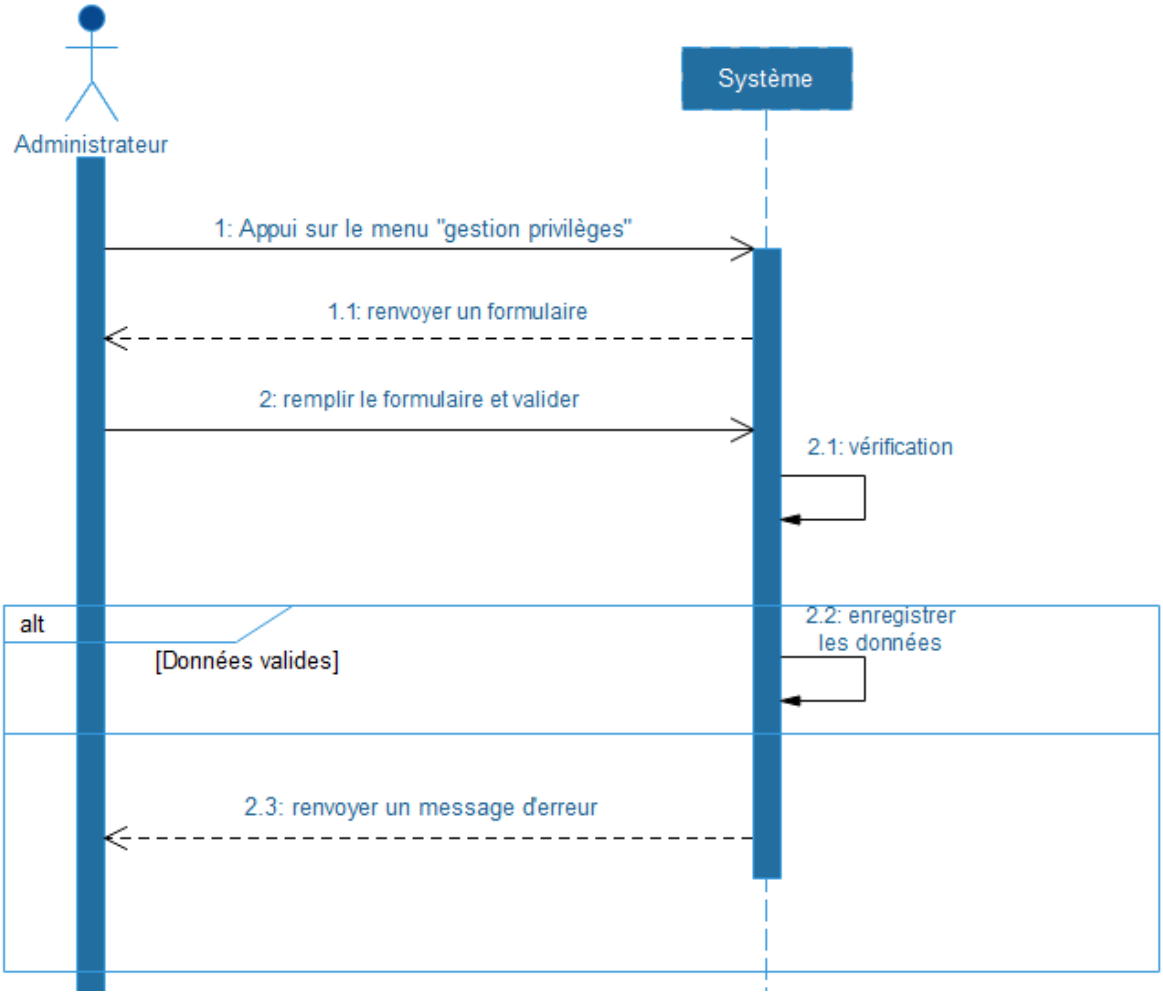


Figure 14: Diagramme de séquence cas Gerer_privileges

Description textuelle :

Tableau 2: Description cas Gerer_privileges

Titre	Gerer_privileges
Description	
Acteurs	Administrateur
Précondition	L'utilisateur a accès à la plateforme et dispose des privilèges nécessaires
Scénario nominal	1. L'administrateur clique sur le menu de gestion des privilèges. 2. Le système lui renvoie un formulaire à remplir 3. L'administrateur remplit le formulaire et le valide 4. Le système vérifie la fiabilité des données soumises 5. Le système enregistre les modifications

Scénario alternatif	Etape 4 : Les données soumises par l'utilisateur ne sont pas valides. Le système renvoie un message d'erreur à l'utilisateur. Le scénario nominal reprend à l'étape 2
Post condition	Les utilisateurs autorisés peuvent utiliser le module

3.5.3.3.2.3 Cas simuler équipement :

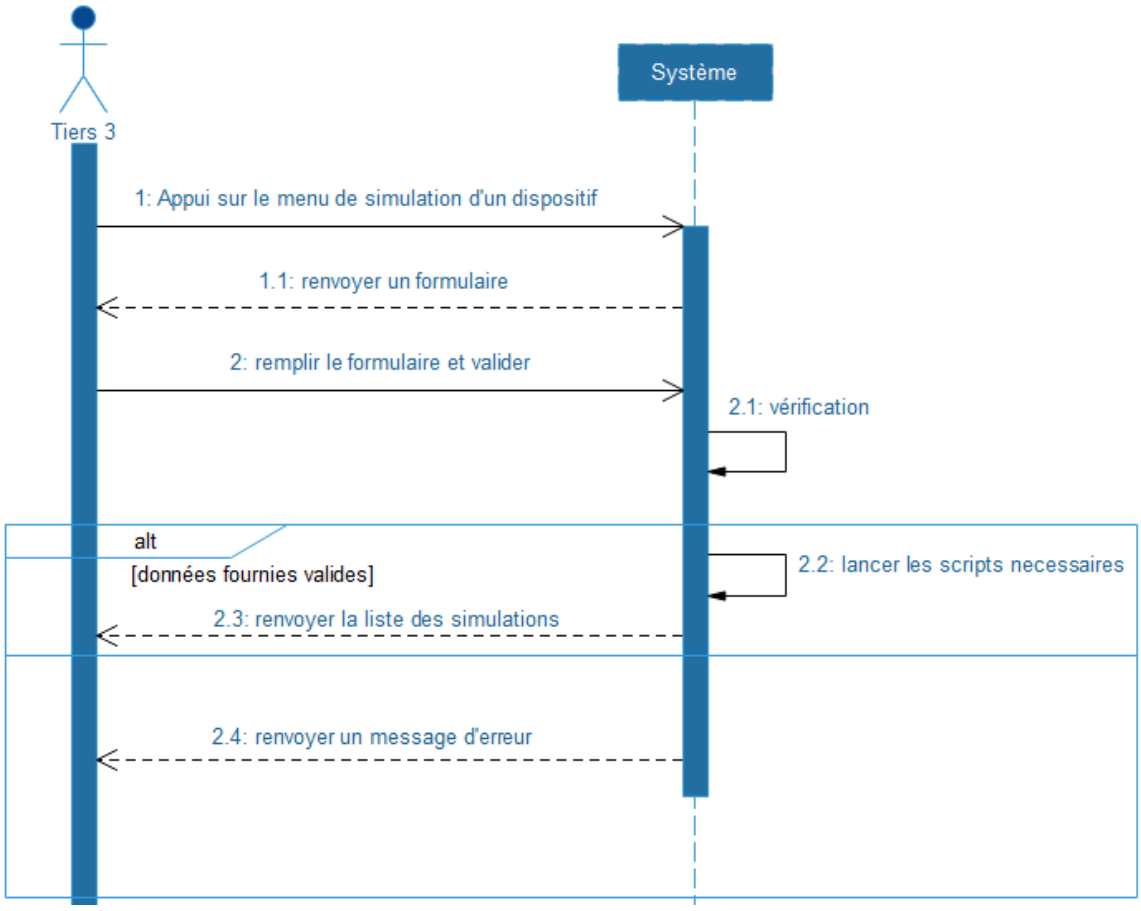


Figure 15: Diagramme de séquence cas simuler_equipement

Description textuelle :

Tableau 3: Description cas Simuler_equipement

Titre	Simuler_equipement
Description	
Acteurs	Tiers niveau 3
Précondition	L'utilisateur a accès à la plateforme et dispose des privilèges nécessaires
Scénario nominal	1. L'utilisateur clique sur le menu de de simulation d'un dispostif

	2. Le système lui renvoie un formulaire à remplir 3. Le tiers 3 remplit le formulaire et le valide 4. Le système vérifie la fiabilité des données soumises 5. Le système lance les scripts nécessaires pour les streaming des logs en temps réel. 6. Le système retourne l'utilisateur sur la liste des simulations.
Scénario alternatif	Etape 4 : Les données soumises par l'utilisateur ne sont pas valides. Le système renvoie un message d'erreur à l'utilisateur. Le scénario nominal reprend à l'étape 2 Etape 5 : l'exécution des scripts a échoué. Le système renvoie un message d'erreur à l'utilisateur et met fin à l'opération
Post condition	

3.5.3.3.2.4 Cas comparer test :

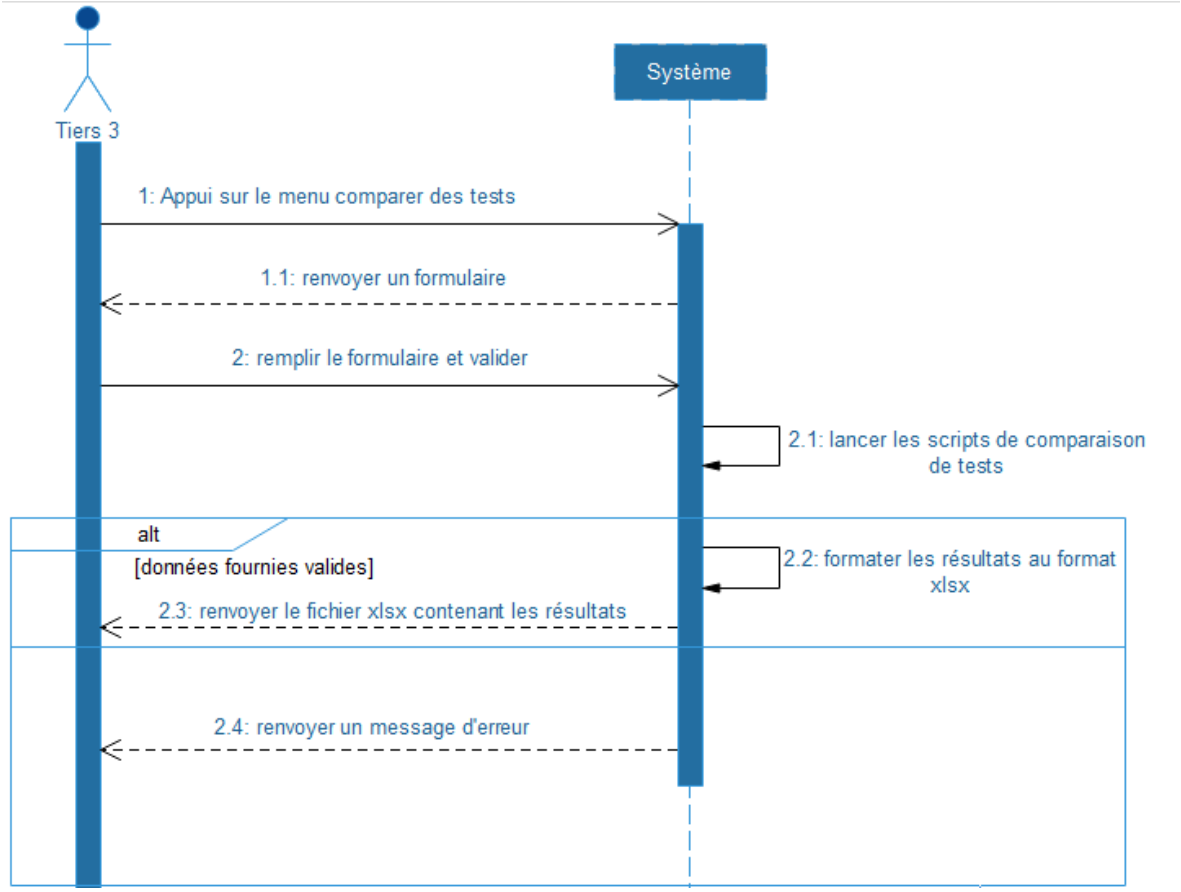


Figure 16: Diagramme de séquence cas comparer_tests

Description textuelle :

Tableau 4: Description cas Comparer_tests

Titre	Comparer_tests
Description	
Acteurs	Tiers niveau 3
Précondition	L'utilisateur a accès à la plateforme et dispose des privilèges nécessaires
Scénario nominal	1. L'administrateur clique sur le menu de comparaison de tests 2. Le système lui renvoie un formulaire à remplir 3. Le tiers 3 remplit le formulaire et le valide 4. Le système vérifie la fiabilité des données soumises 5. Le système lance les scripts de comparaison des tests. 6. Le système formate les résultats au format xlsx. 7. Le système renvoie le fichier xlsx contenant les résultats à l'utilisateur
Scénario alternatif	Etape 4 : Les données soumises par l'utilisateur ne sont pas valides. Le système renvoie un message d'erreur à l'utilisateur. Le scénario nominal reprend à l'étape 2. Etape 5 : l'exécution des scripts a échoué. Le système renvoie un message d'erreur à l'utilisateur et met fin à l'opération
Post condition	

CHAPITRE 4 : Implémentation

4.1 SIEM

Les SIEM sont le centre des architectures SOC cependant les possibilités offertes par les SIEM traditionnels présentent certaines limites.

Bien qu'étant la pierre angulaire d'un SOC, le SIEM a besoin de solutions complémentaires pour avoir une vision d'ensemble des faiblesses d'un SI et des évènements s'y produisant.

4.1.1 Limites

Les fonctions de collecte, centralisation et d'analyse des traces générées par les systèmes d'information, désignées par Security Information and Events Management SIEM, constituent la brique fondamentale des SOC « historiques ». Ce SIEM, si essentiel dans la supervision de sécurité, devient aujourd'hui la faiblesse du SOC.

En effet les SIEM traditionnels présentent certaines limites surtout en termes de performances qui nécessitent de limiter le périmètre du système d'information à superviser. Le talon d'Achille d'un SIEM est sa performance qui se matérialise en nombre d'évènements traités à la seconde. Cette limite structure les choix du (des) périmètre(s) à superviser : afin de « préserver » les performances du SIEM des choix doivent être pris. La majorité des implémentations d'un SIEM favorise la supervision des points d'entrée et de sortie du système d'information (principalement les pares feux) et les interconnexions du réseau (proxy et reverse proxy) et, lorsqu'elles sont activées dans les pares feux ou déployées dans les réseaux internes, des sondes de détection d'intrusion. Ces périmètres limités de supervision permettent de mettre en œuvre un faible nombre de scénarios d'attaque à superviser. Par ailleurs, les scénarios d'attaque supervisés adressent les scénarios connus et documentés. Des scénarios qui ne permettent pas systématiquement les attaques furtives ou de niveau étatique (Noé & Loureiro, 2017) (Khémissa, 2018).

Le rôle d'un SIEM est d'exploiter les logs. Sur le plan temporel, le SIEM va donc pouvoir avoir un impact sur les phases de Détection/Réaction et d'Investigation. Mais sans source d'information complémentaire, il sera peu utile sur la phase de Prévention/Protection. Un SIEM n'est qu'un outil d'analyse de logs. Sa capacité est limitée aux informations fournies dans les logs. De fait, il ne sera pas en mesure de détecter des incidents ne laissant pas de traces sur les équipements dont les logs sont collectés. Cela rend relativement inutile pour détecter un problème sur un système d'exploitation ou pour diagnostiquer l'impact d'un incident sur un système (telles une intrusion, l'installation de rootkit, l'altération du système ou des applications, …).

Bien qu'étant la pierre angulaire d'un SOC, le SIEM a besoin de solutions complémentaires pour avoir une vision d'ensemble des faiblesses d'un SI et des évènements s'y produisant.

Les principaux outils sont les solutions de contrôles de conformité en continue, de vulnérabilités et d'intégrité. Ces solutions permettent de fournir des informations sur les brèches utilisables par un attaquant, et suivent et tracent en profondeur les variations des systèmes ou les signes d'actions potentiellement illicites.

4.1.2 Comparaison de quelques SIEM

4.1.2.1 IBMQRadar

IBMQRaadar est une plateforme de gestion de la sécurité réseau. Il permet l'analyse et la corrélation de logs, de l'activité réseau. C'est une solution propriétaire existant sous Cloud, en software ou sous forme matérielle délivrée par IBM.

Il permet selon le forfait d'indexer jusqu'à un million d'évènements par seconde, de faire de l'analyse comportementale (UBA) ainsi que du forensique.

	Splunk	IBMQRadar
Cas d'utilisation	Industries hautement règlementées	Entreprises et entreprises régulées (réglementées ??)
Mesures	Plusieurs pétaoctets de données par jour	Plus de 400 sources, jusqu'à 1 million d'évènements par seconde
Intelligence	Intégration avec Splunk UBA et Machine Learning Toolkit	UBA, forensiques, inspection de paquets, intégration avec Watson
Livraison	Logiciel ou sur Cloud	Cloud ou matériel, logiciel ou application virtuelle
Cout	Basé sur le maximum de données indexées par jour. Commence à $1800/GO/jour	Cloud à partir de $800/mois. Sur site à $10400

4.1.2.2 Elastic Stack

Elastic Stack est une plateforme permettant l'analyse et la gestion des logs. Il permet d'indexer et de stocker des documents et offre ensuite la possibilité de faire des analyses et des requêtes sur ces derniers. C'est une suite logicielle essentiellement composée d'Elasticsearch, Logstash, Kibana et récemment, de Beats.

Elasticsearch est un moteur d'indexation, d'analyse et de recherche des données, c'est grâce à son succès que la société Elastic s'est fait connaître. Il offre une plateforme de recherche évolutive basée sur Lucene (Apache Lucene).

Logstash, quant à lui, est un outil de collecte de données issues de bases de données, d'applications web, de services, etc. qui à l'issue de cette ingestion, les transforme avant de les envoyer vers la base de données Elasticsearch.

Comme alternative à Logstash avec ses longues périodes de démarrage, Beats permet de collecter et d'expédier différents types de données dans Elasticsearch ou même à Logstash pour des traitements supplémentaires. C'est un ensemble d'outils légers de collecte de logs : Filebeat pour les fichiers logs, Metricbeat pour les indicateurs, Packetbeat pour les données réseau, Winlogbeat pour les logs provenant de systèmes d'exploitation Windows, Auditbeat pour les données d'audit et Heartbeat pour la surveillance de la disponibilité.

Enfin Kibana, qui constitue l'interface utilisateur permettant de visualiser les données indexées dans Elasticsearch. De plus il offre la possibilité de paramétrer toute la suite Elastic.

	Splunk	Elastic Stack

Installation	Très simple d'installation : création d'un compte utilisateur et récupération du fichier adéquat sur le site officiel	Installation simple mais un peu plus complexe que celle de Splunk
Configuration	Configuration simple via l'interface web	Configuration complexe dû à la complexité de configuration de logstash nécessitant la connaissance de certains langages de script
Recherche	Utilisation basique : simple et prédictif. Utilisation du SPL (Splunk Search Processing Langage) pour des requêtes avancées.	Utilisation basique : simple et prédictif. Utilisation d'un langage proche de Lucene pour des recherches avancées
Graphiques	Graphes crées depuis la recherche grâce aux champs disponibles	Graphes crées depuis la recherche et depuis le menu visualise grâce à des filtres, nécessites en contrepartie une bonne configuration de Logstash.
Dashboard	Possibilité de placer des Dashboard à l'accueil. Dashboard cependant non interactif. Les barres de temps et de recherche non disponibles par défaut. Reconfiguration possible (en XML) pour adapter le Dashboard à la visualisation mais peut devenir rapidement contraignant.	Dashboard facile à créer et à modifier ; interactifs par défaut et ajustés en fonction de la recherche ou de la plage horaire sélectionnée. Barre de recherche et de temps disponibles par défaut.
Alertes	Nécessite la version Splunk Entreprise	Nécessite le X-Pack donc un abonnement
Identification et gestion des utilisateurs	Requiert la version Entreprise pour la création des utilisateurs et la gestion des rôles. Possibilité d'intégration avec Active Directory ou LDAP	Requiert le X-Pack pour l'identification et la gestion des utilisateurs
Couts	Version Entreprise par GO de données indexées par jour ; nécessaire pour bénéficier des alertes, de la gestion des utilisateurs, du support Version gratuite limitée à 500Mo de logs par jour	Open source Requiert l'achat d'une licence pour bénéficier de toutes les fonctionnalités : identification et gestion des utilisateurs, les alertes, le support, etc.

4.2 Splunk

4.2.1 Généralités :

Splunk surveille et analyse les données machine de tous les types de source pour délivrer l'Intelligence Opérationnelle nécessaire pour optimiser les performances de l'informatique, de la sécurité et des fonctions de l'entreprise (Splunk, Splunk Enterprise, s.d.).

Il permet de chercher, d'analyser et de visualiser des données générées ou collectées sur différents dispositifs en allant des applications simples aux capteurs. Sa compatibilité avec la plupart des types de données (csv, ZIP, log4j, Catalina, pcap, XML, syslog, etc.) et sa capacité à traiter les données en temps réel constituent ses principaux atouts.

Splunk dispose d'une capacité de stockage et d'analyse de larges volumes de données ce qui combinée avec ses fonctionnalités de visualisation (tableaux de bord, pivot, etc.) en font aujourd'hui un outil majeur du Big Data. De plus grâce à ses fonctions d'analyses intuitives, au Machine Learning, à ses applications prêtes à l'emploi et à ses API ouvertes, Splunk est une plateforme flexible capable aussi bien de traiter des scénarios d'utilisation spécifiques que d'être la colonne vertébrale des analyses de toutes l'entreprise.

Splunk utilise un langage propriétaire le SPL (Search Processing Language) qui allie la syntaxe pipeline des systèmes Unix avec le meilleur du SQL. Ce langage permet de :

- ∞ D'accéder à toutes les données dans leur format d'origine
- ∞ Optimiser les données pour extraire des évènements chronologiques
- ∞ Utiliser le même langage pour la visualisation.

4.2.2 Architecture :

L'architecture de Splunk peut être résumée, de façon simplifiée, en 3 composantes :

- ∞ Le CLI : qui est une ligne de commande qui permet de saisir un certain nombre de commandes disponibles permettant notamment de faire la configuration des produits.
- ∞ L'interface web : c'est une interface graphique simple et très intuitive qui permet de faciliter la plupart des configurations. Cette interface écrite en Python et en Ajax permet surtout d'effectuer des recherches et d'afficher les résultats.
- ∞ Et le moteur de Splunk qui est un daemon en C++ qui permet de faire toutes les fonctions d'analyse, de collecte, d'indexation, de reporting, de monitoring, etc. Les API qu'elle fournit sont accessibles grâce aux services web REST ce qui lui vaut d'être compatible avec n'importe quel framework web.

Ces trois composantes sont reposent sur une base de données, inspirée de Google File System (GFS), propriétaire et distribuée où sont stockées les données sous forme d'indexes d'où le nom de « data store » ou magasin de données (Duval, 2016).

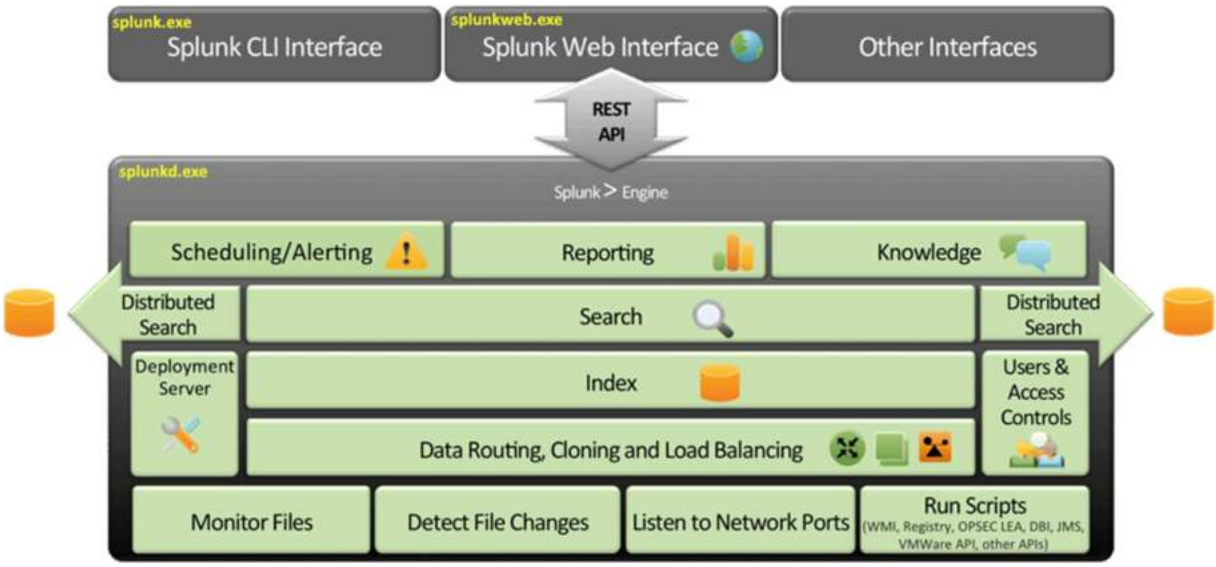


Figure 17: Architecture de Splunk (Splunk, Splunk Enterprise, s.d.)

L'implémentation distribuée de Splunk fait ressortir trois composantes fondamentales à savoir :

- ∞ Les Search Head : ce sont les nœuds maîtres, ils exécutent les recherches sur les magasins de données et disposent des interfaces CLI et Web.
- ∞ Les Indexers : ils exécutent le daemon Splunk. Ils font l'analyse, l'indexation et la préparation au stockage des données reçues. C'est lors de l'indexation que les données sont transformées en évènements plus exploitables. Les indexeurs constituent les nœuds esclaves de l'architecture.
- ∞ Les Forwarders : ou collecteurs de logs sont des agents très peu gourmands en ressources installés au plus proche des sources de données. Ils sont chargés de collecter et de transférer les données aux Indexers.

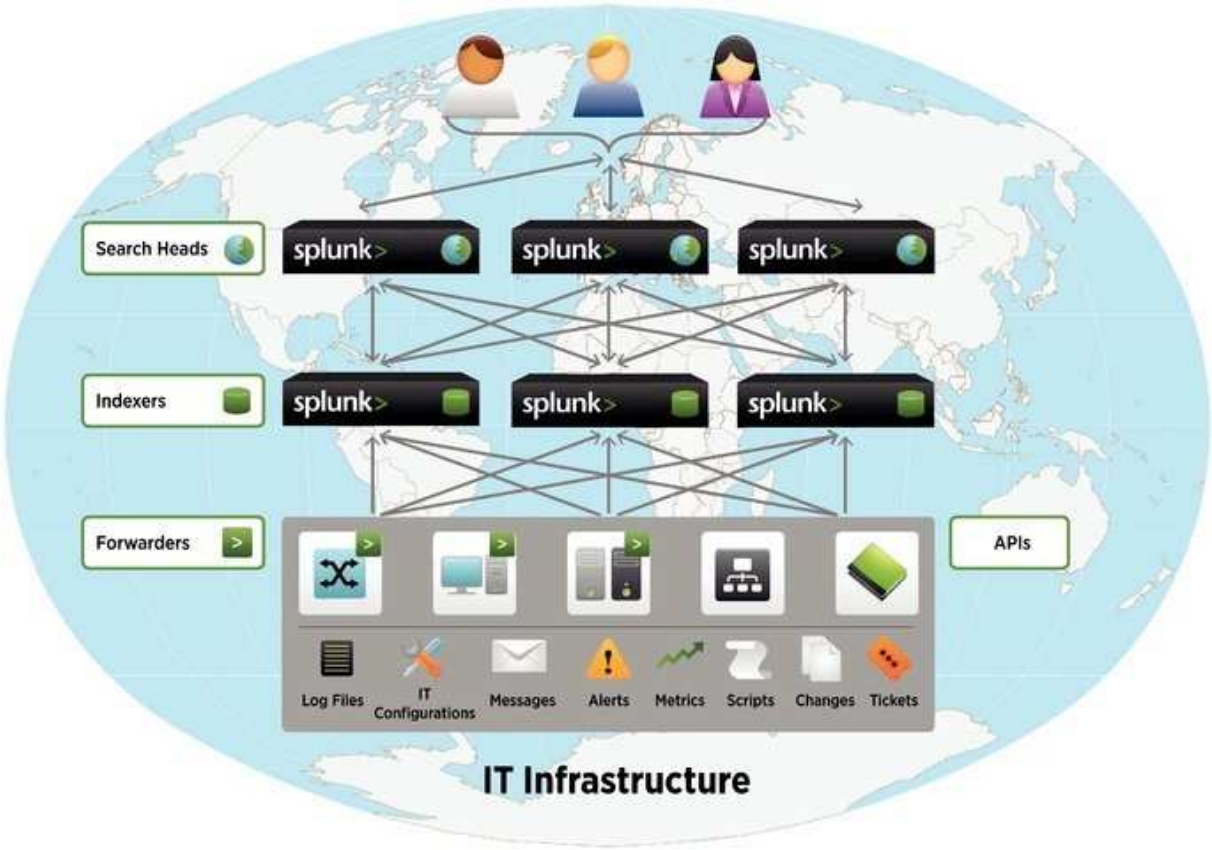


Figure 18: Architecture de déploiement de Splunk (Splunk, Splunk Enterprise, s.d.)

Cette répartition démontre la souplesse de l'architecture Splunk qui constitue l'un de ses plus grands atouts.

4.2.3 Catalogue de produits :

Splunk offre plusieurs produits complémentaires visant des besoins différents et des solutions ciblées.

- Splunk Enterprise : produit « on premises » de Splunk, c'est leur produit phare. Il s'illustre par la facilité de son déploiement, la possibilité d'implémenter des architectures distribuées sans oublier son évolutivité.
- Splunk Cloud : offre l'accès aux fonctionnalités de Splunk à travers le Cloud. C'est la version SaaS (SOC/Security As A Service) de Splunk.
- Splunk Light : dédié aux petits environnements informatiques, Splunk Light est une option pour les PME/TPE. C'est une version du moteur Splunk destinée à être déployée sur un serveur unique et à être utilisée par 5 utilisateurs maximum.
- Splunk Enterprise Security : c'est la solution la plus adoptées comme base d'un SOC. En effet cette solution est l'un des plus puissants SIEM du marché, car en plus d'offrir une vue globale de l'infrastructure, elle dispose de cas d'utilisation prédéfinis (détection d'une attaque par force brute, injection SQL, etc.).
- Splunk IT Service Intelligence : destiné à la gestion d'une infrastructure physique comme Cloud. Automatise un certain nombre de tâches classiques de l'IT.
- Splunk User Behaviour Analytics : comme son nom l'indique, il permet l'analyse comportementale pour une détection plus rapide des menaces.

Splunk propose ainsi une large gamme de services qui peuvent être combinés pour obtenir des résultats optimaux.

4.2.4 Apps et Add-on

Le daemon Splunk offre de services accessibles en REST, facilitant ainsi l'extension de la plateforme. Deux mécanismes d'extension sont offerts par Splunk :

- ∞ Les Apps : ce sont des applications disposant d'interfaces utilisateurs. Par exemple le trio de solutions Premium exposé plus haut à savoir Splunk ES, ITSI et UBA sont des applications Splunk. Les applications peuvent faire appel à des Add-Ons qui sont soit intégrés directement à l'application donc l'installation de l'application suffit pour son utilisation, soit ces Add-Ons doivent sont des prés-requis et donc doivent être installés par l'utilisateur avant de pouvoir utiliser l'application.
- ∞ Les Add-Ons : sont des briques de logiciel destinées à enrichir les fonctionnalités de base de Splunk ou d'applications Splunk. Il existe de nombreux Add-Ons pour Windows, Unix, Linux, AWS, etc. Ils ne disposent pas d'interface utilisateur et permettent de customiser la collecte, l'analyse, l'enrichissement du moteur de recherche ou même de fournir des macros.

Pour faciliter la publication et la recherche d'Apps et d'Add-Ons, Splunk a mis à disposition la Splunkbase qui est l'homologue de PlayStore ou AppStore mais destinée uniquement aux extensions Splunk.

Splunkbase permet aussi aux fournisseurs de logiciels et d'équipements de fournir des connecteurs garantissant la compatibilité et facilitant l'intégration de leurs produits avec Splunk.

4.3 Pratique

4.3.1 Architecture :

Les procédures de sécurité d'Atos ne permettent pas d'avoir accès à leurs équipements et serveurs pour une première étude, c'est pourquoi, pour un début, nous avons fait l'implémentation sur GNS 3, un émulateur d'équipements réseaux.

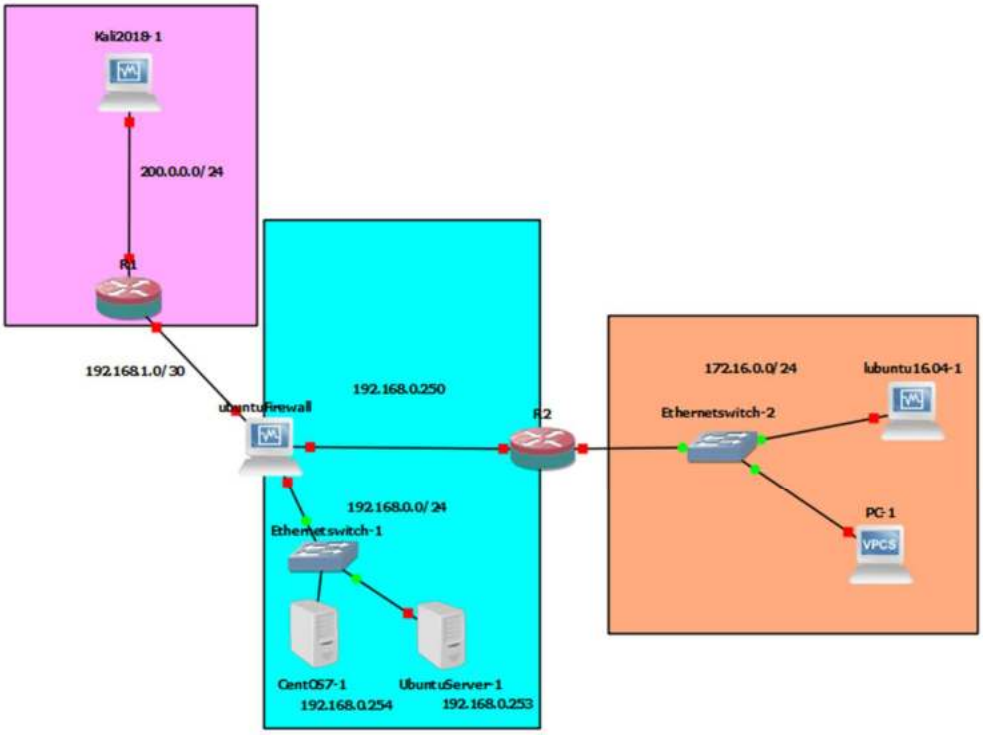


Figure 19: Architecture d'implémentation

4.3.2 Activation du SSL

Pour utiliser Splunk en tant SIEM il faut d'abord le sécuriser lui-même. En activant dans un premier temps le SSL et en générant des certificats.

L'activation du SSL se fait sur la plateforme web accessible sur le port 8000 (par défaut) de la machine hébergeant Splunk (voir installation de Splunk en annexe).

Après l'activation du SSL, il reste à générer les certificats. Vu que nous sommes en stade d'expérimentation, nous avons utilisé OpenSSL pour générer nos propres certificats auto signés.

Ainsi on peut voir maintenant qu'on accède au site de manière sécurisée (https).

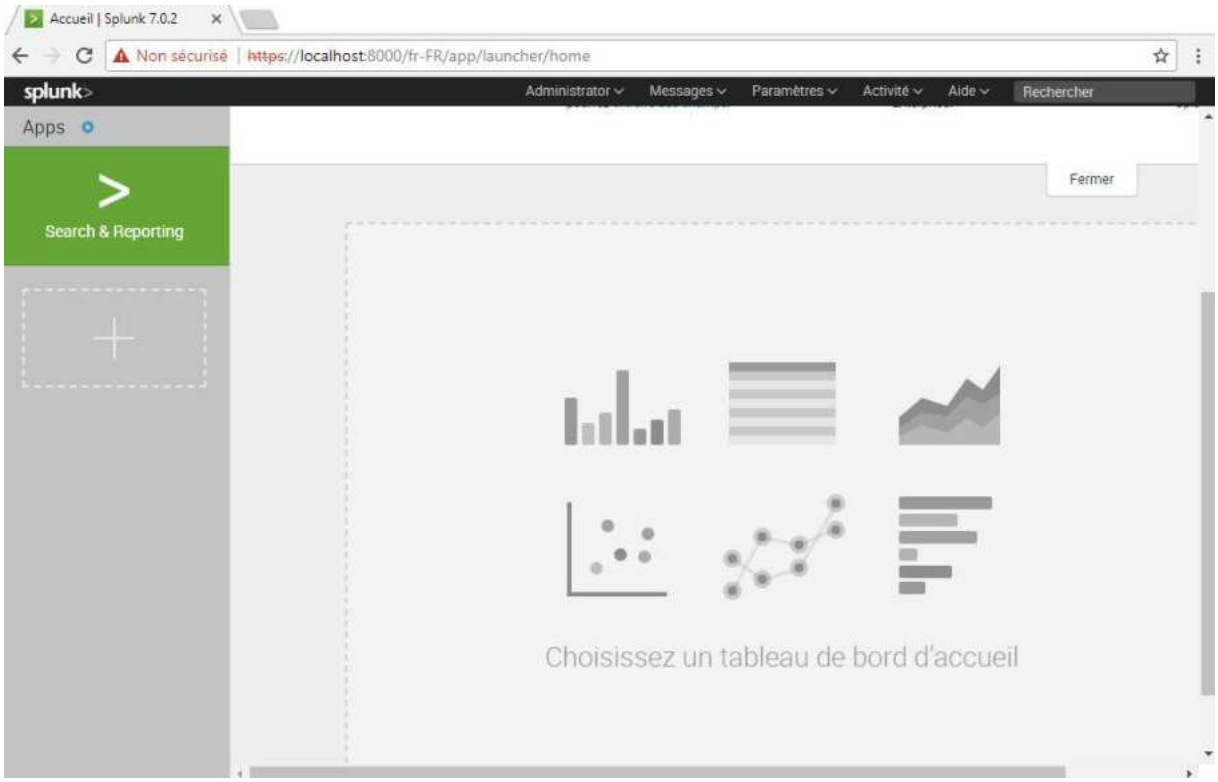
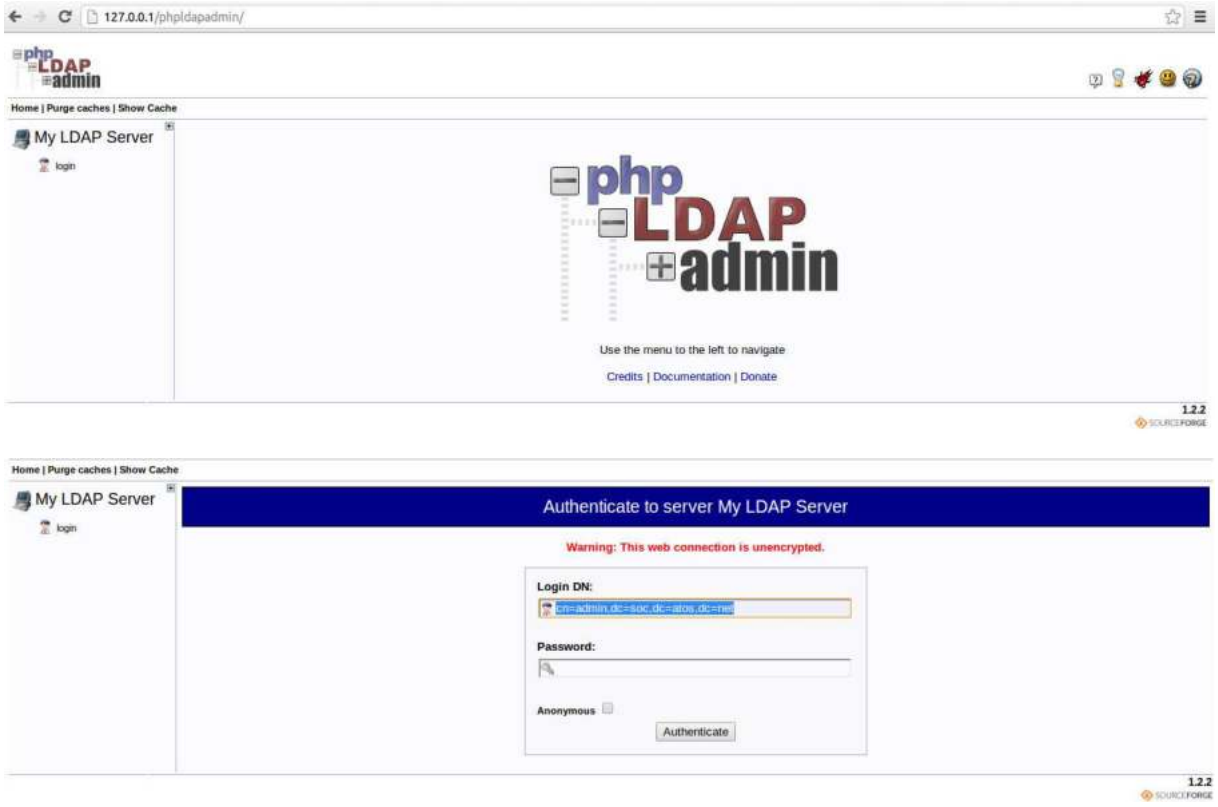


Figure 20: Page d'accueil Splunk après activation du SSL

4.3.3 Définition de l'authentification à partir d'un annuaire externe

Ensuite nous avons défini un annuaire ldap pour spécifier les utilisateurs pouvant s'y connecter. Après l'installation de LDAP, nous avons défini quelques utilisateurs pour tester l'authentification.



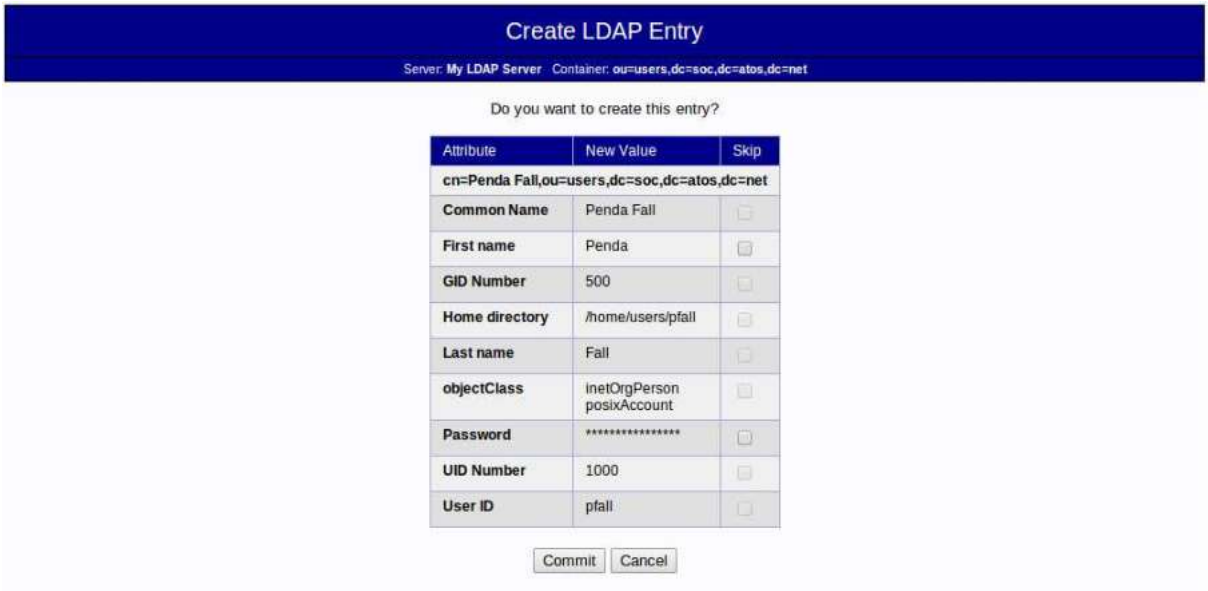


Figure 21: Création d'utilisateurs

Splunk prend en charge différents types d'authentification en allant de la native à l'externe avec :

- ∞ LDAP pour l'authentification d'utilisateurs disposant d'une entrée dans un annuaire LDAP ;
- ∞ SAML (Security Assertion Markup Language) qui est un standard qui permet la fédération de l'authentification dont le mécanisme de permettre à l'utilisateur d'accéder à tout serveur en partenariat avec le fournisseur IdP (Identity Provider) auprès duquel il se connecte.

Dans notre cas, vu qu'on utilise un annuaire OpenLDAP, nous avons coché le type d'authentification LDAP.

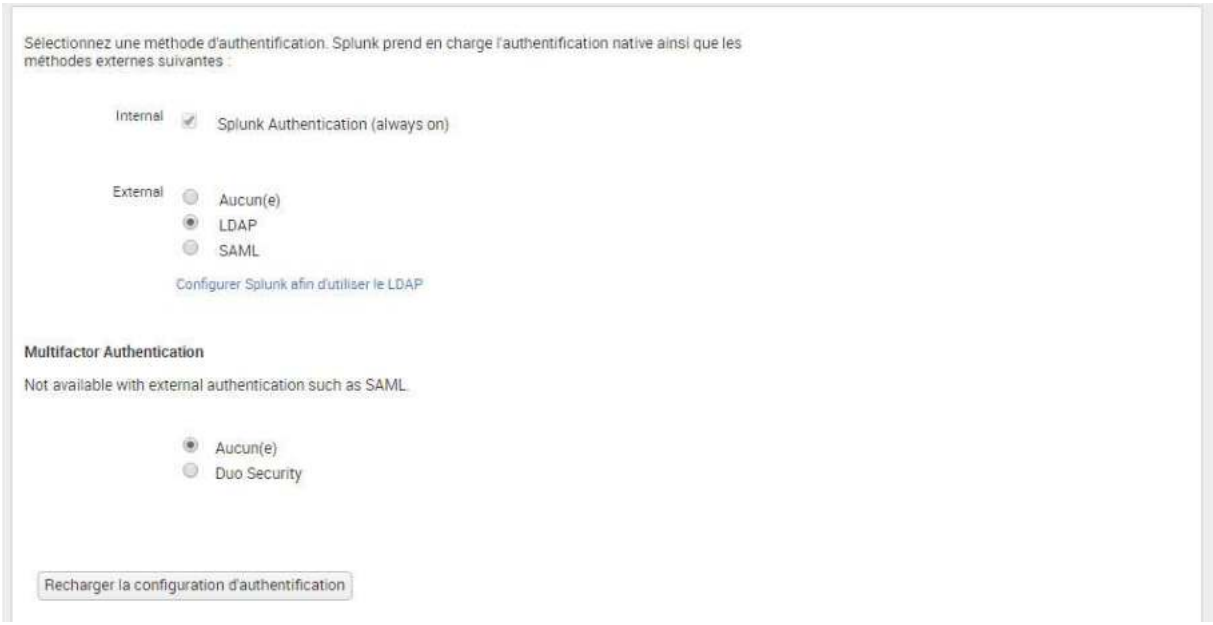


Figure 22: Activation de l'authentification LDAP

Après la configuration, dans la liste des stratégies, on peut voir notre nouvelle stratégie avec sa priorité.



Figure 23: Serveur LDAP

4.3.4 Mise en place du reverse proxy

Nous avons configuré Apache pour qu'il accepte le proxying. D'abord il a fallu charger les modules proxy en enlevant les commentaires dans le fichier de configuration httpd.conf.

```
#LoadModule buffer_module modules/mod_buffer.so
LoadModule cache_module modules/mod_cache.so
LoadModule cache_disk_module modules/mod_cache_disk.so
LoadModule cache_socache_module modules/mod_cache_socache.so
#LoadModule cern_meta_module modules/mod_cern_meta.so
LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
```

Figure 24: Activation des modules proxy dans httpd.conf

Ensuite dans le fichier httpd-vhost.conf, la clause qui permet de spécifier à Apache ce qu'il faut faire lorsque le module proxy est chargé.

```
 ServerName soc.atos.net
  ServerAlias soc.atos.net
  SSLEngine on
  Redirect / https://soc.atos.net:8000/
  SSLCertificateFile "C:/Program Files/Splunk/etc/auth/mycerts/mySplunkWebCertificate.pem"
  SSLCertificateKeyFile "C:/Program Files/Splunk/etc/auth/mycerts/mySplunkWebPrivateKey.key"
  <IfModule mod_proxy.so>
        ProxyPass / https://192.168.0.253:8000/ retry=0
        ProxyPassReverse / https://1192.168.0.253:8000/
    </IfModule>
</VirtualHost>
```

Figure 25: Configuration du proxy dans httpd-vhost.conf

4.3.5 Configuration des forwarders

Comme nous l'avons signalé plus haut, il existe une licence Splunk Forwarder qui permet de collecter les données sur une machine distante et de les renvoyer à l'instance principale qui est le search head.

Ainsi nous avons installé Splunk Forwarder sur deux machines l'une sous Linux et l'autre sous Windows. Pour que la communication puisse passer il faut activer la réception sur l'instance principale (CentOS Splunk) et la transmission sur les forwarders. L'activation peut se faire

grâce à l'interface graphique sur l'instance Enterprise uniquement car les forwarders ne disposent pas d'interface graphique ou grâce aux fichiers de configuration *input.conf* et *output.conf* respectivement dans l'instance Enterprise et l'instance Forwarder.

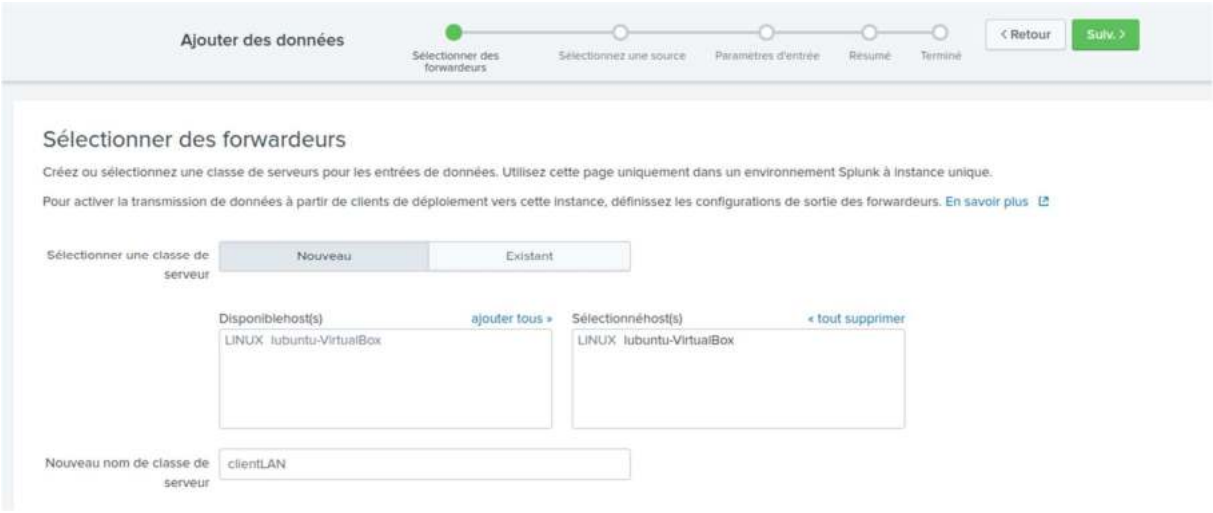


Figure 26: Configuration des forwarders : choix des forwarders

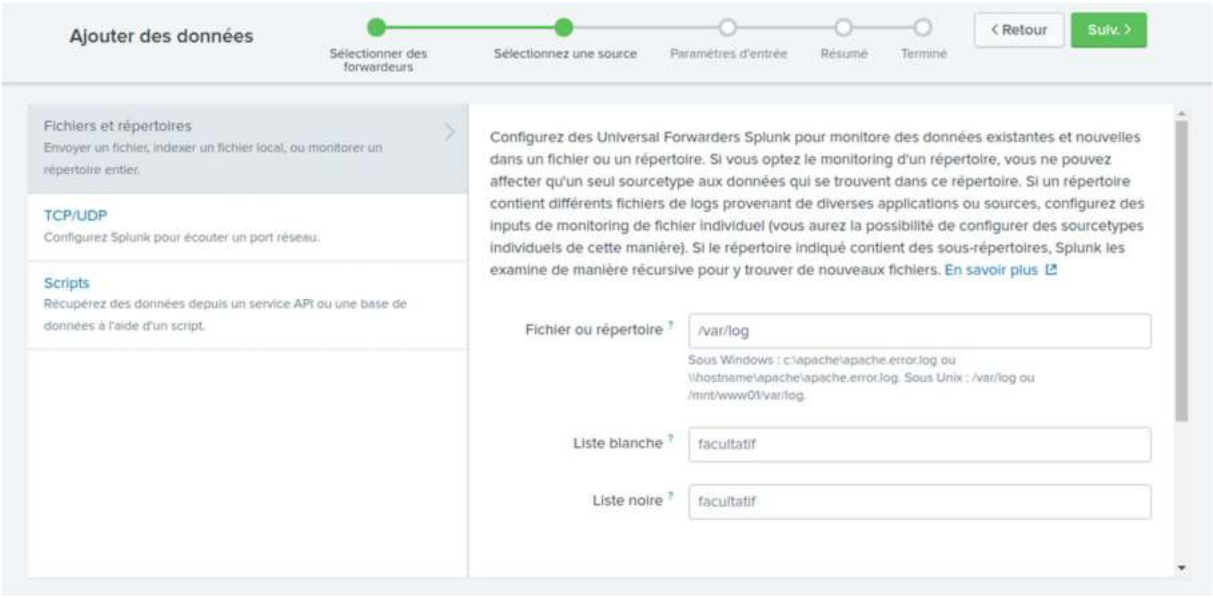


Figure 27: Répertoire à superviser

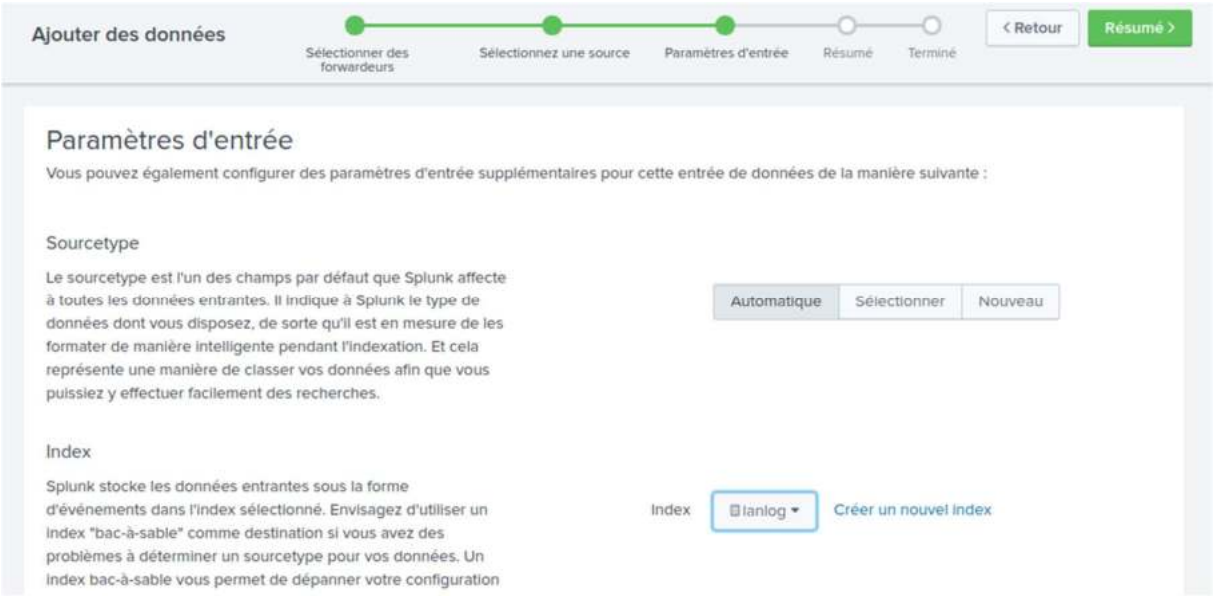


Figure 28: Paramétrage de la réception des données

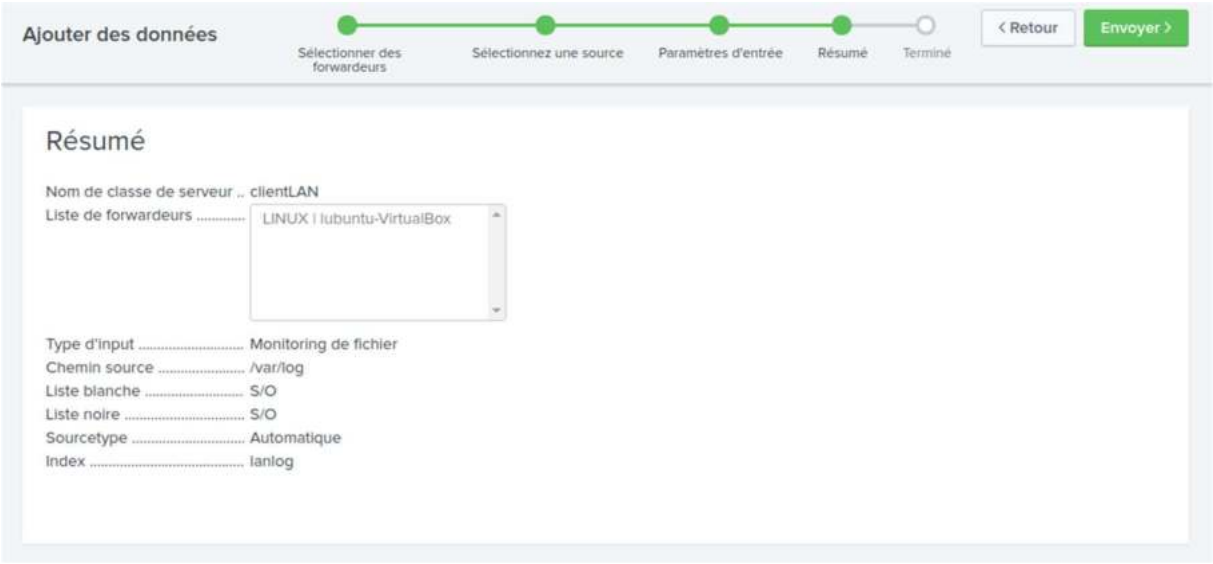


Figure 29: Résumé des actions précédentes

4.3.6 Configuration du firewall :

Un pare-feu représente l'élément incontournable dans une architecture de sécurité et l'équipement de sécurité par excellence dans un réseau informatique. Il dispose de différents mécanismes de filtrage comme : le filtrage de paquets, l'implémentation de proxys applicatifs, les passerelles de niveau circuit ou même l'inspection de paquets. Les pares-feux sont configurés pour satisfaire la politique de sécurité. Dans les distributions Linux, Netfilter/Iptables est la référence en matière de firewall. Netfilter est un framework implémenté dans les distributions Linux depuis le noyau 2.4 et Iptables est l'interface en ligne de commande permettant de le gérer.

Nous allons donc configurer Iptables sur un routeur Linux afin de filtrer les différents flux dans le réseau.

D'abord nous avons créé un fichier iptables.conf dans lequel on spécifie le fichier dans lequel les logs iptables seront stockés car par défaut, iptables se sert du fichier générique /var/log/syslog.

```
 GNU nano 2.9.3                          /etc/rsyslog.d/iptables.conf

:msg,contains,"ACTIONS=" /var/log/iptables.log
& stop
```

Figure 30: Configuration du fichier de réception

Ensuite nous avons défini un ensemble de règles dans le fichier /etc/iptables/iptables.v4 qui est le fichier de configuration créé à l'installation de iptables-persistent. Iptables-persistent permet de sauvegarder les règles dans un fichier et de pouvoir les restaurer au démarrage de la machine.

```
:FROM-Lan - [0:0]
:FORM-DMZ - [0:0]
###

-A LOG-INPUT -j LOG --log-prefix "IPTables-REJECT-INPUT: "
-A LOG-FORWARD -j LOG --log-prefix "IPTables-REJECT-FORWARD: "
-A LOG-Externe-TO-Lan -j LOG --log-prefix "IPTables-REJECT-Extieur-TO-LAN: "
-A LOG-Lan-TO-Exterieur -j LOG --log-prefix "IPTables-REJECT-Lan-TO-Externe: "
###

-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m limit --limit 2/sec -j ACCEPT
-A INPUT -d 192.168.0.254 -p tcp --dport 22 -j accept -m comment --comment "Access to the SSH inter
-A INPUT -m limit --limit 2/sec -j LOG-INPUT
-A INPUT -m limit --limit 2/sec -j LOG-INPUT
-A INPUT -j REJECT --reject-with icmp-port-unreachable
###

-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i enp0s3 -o enp0s8 -s 192.168.0.0/24 -j TO-Exterieur
-A FORWARD -i enp0s9 -o enp0s8 -s 172.16.0.0/24 -j TO-Exterieur

-A FORWARD -o enp0s0 -d 192.168.0.0/24 -j TO-DMZ
-A FORWARD -o enp0s9 -d 172.16.0.0/24 -j TO-Lan

-A FORWARD -i enp0s3 -s 192.168.0.0/24 -j FROM-DMZ
-A FORWARD -i enp0s9 -s 172.16.0.0/24 -j FROM-Lan

-A FORWARD -i enp0s9 -s 172.16.0.0/24 -o enp0s3 -d 192.168.0.0/24 -j Lan-TO-DMZ

-A FORWARD -i enp0s3 -o enp0s3 -j ACCEPT
```

Figure 31: Extrait du fichier de sauvegarde Iptables

Les logs Iptables peuvent rapidement être volumineux c'est pourquoi, il est important de configurer la rotation des logs qui permet d'archiver les anciens logs.

```
 GNU nano 2.9.3                  /etc/logrotate.d/iptables                Modified

/var/log/iptables.log
{
 rotate 7
 daily
 missingok
 notifempty
 delaycompress
 compress
 postrotate
    invoke-rc.d rsyslog reload > /dev/null
 endscript
}
```

Figure 32: Configuration de la rotation des logs

Enfin nous avons configuré le forwarder pour qu'il envoie les données Iptables sur le serveur Splunk afin que les logs puissent être traités dans une application dédiée installée dans le serveur Splunk.

```
root@ubuntuserver:/opt/splunkforwarder# bin/splunk add forward-server 192.168.0.250:9997
Your session is invalid.  Please login.
Splunk username: admin
Password:
Added forwarding to: 192.168.0.250:9997.
root@ubuntuserver:/opt/splunkforwarder#
```

Figure 33: Configuration du forwarding

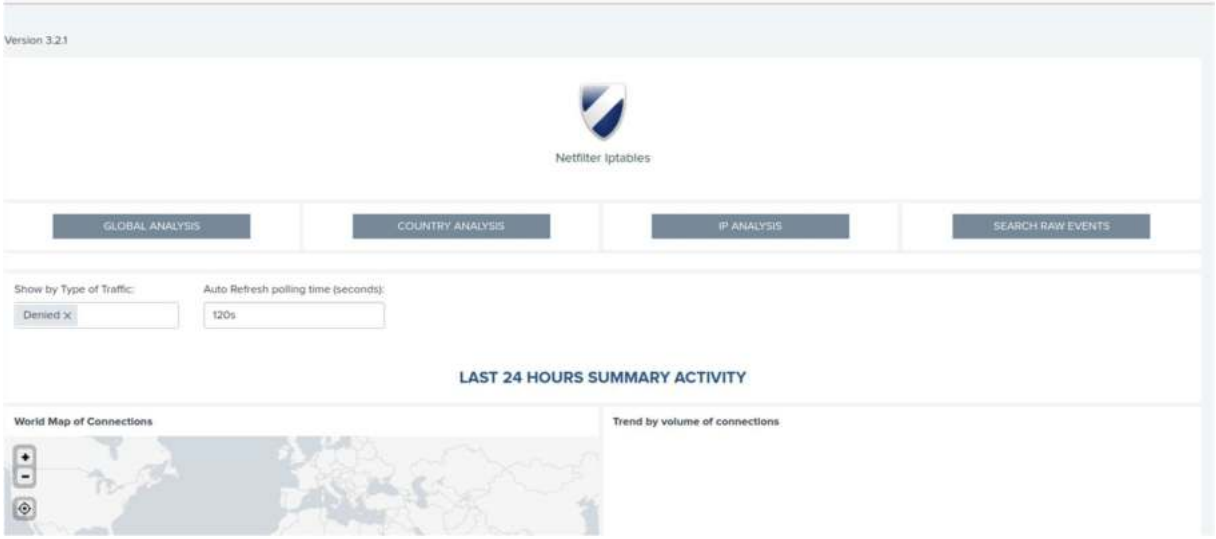


Figure 34: Application NetFilter Iptables for Splunk

4.3.7 Résultats

4.3.7.1 Implémentation des cas d'utilisation

Dans l'implémentation des cas d'utilisation, nous avons eu à installer Machine Learning Toolkit (ML Toolkit) qui est une application Splunk qui permet d'ajouter de nouvelles commandes SPL et des visualisations permettant d'utiliser une variété de concepts du Machine Learning. Splunk MLToolkit comprend des méthodes d'analyse de données, notamment des algorithmes tels que la détection de régression, d'anomalies et de valeurs aberrantes. Celles-ci sont essentielles pour comprendre, modéliser et détecter les tendances dans des données qui ne sont pas facilement

identifiables par observation. ML Toolkit permet également la visualisation personnalisée et des exemples de jeux de données pour s'exercer aux commandes SPL (Splunk Processing

Language). Il fournit également un assistant pour créer un modèle d'analyse des données, ce qui permet de démarrer plus rapidement avec Machine Learning.

L'installation de ML Toolkit peut se faire directement à partir de Splunkweb pour un serveur ayant accès à Internet ou à partir du fichier correspondant téléchargé depuis Splunkbase. Le ML Toolkit a comme prés requis l'installation du Add-on Python for Scientific Computing donc on a d'abord installé ce dernier. A noter que l'installation des Apps Splunk et des Add-Ons se fait de la même façon.

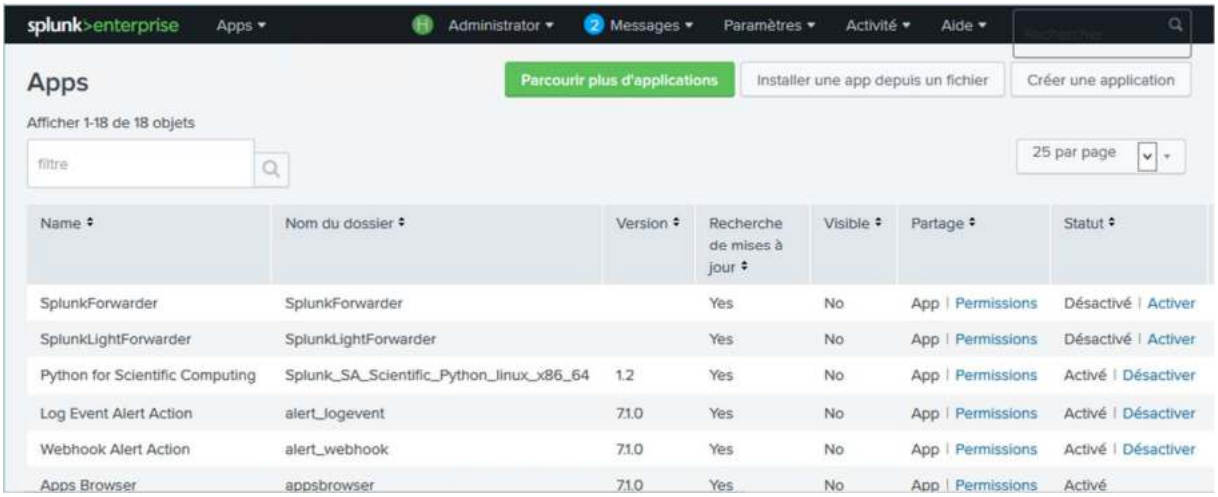


Figure 35: Installation de Python for Scientific Computing

Une fois le add-on Python for Scientific Computing installé, on peut installer le ML Toolkit. Dans notre cas, nous avons choisi l'option d'installation depuis un fichier.



Figure 36: Installation ML Toolkit

Après l'installation ML Toolkit, on peut voir l'icône de l'application sur la barre des applications sur la page d'accueil de Splunk.

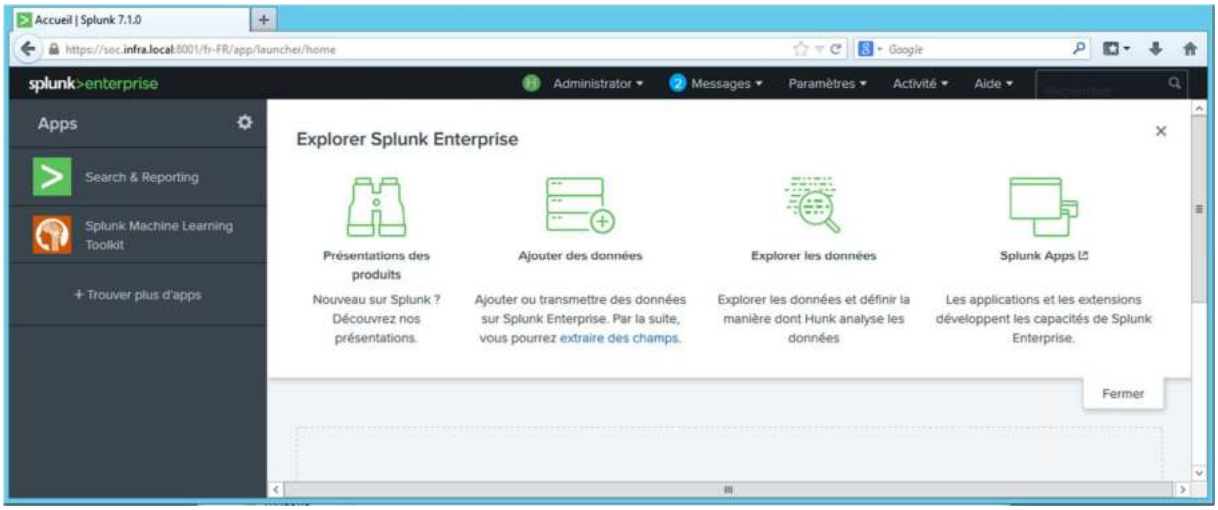


Figure 37: Page d'accueil avec ML Toolkit installé

Avec ML Toolkit, il est possible d'exécuter des entrainements automatiques c'est-à-dire, avec une entrée de données, le système va planifier l'exécution des requêtes pour une période de temps déterminée. Ce mécanisme permet d'aiguiser la capacité de détection du système.

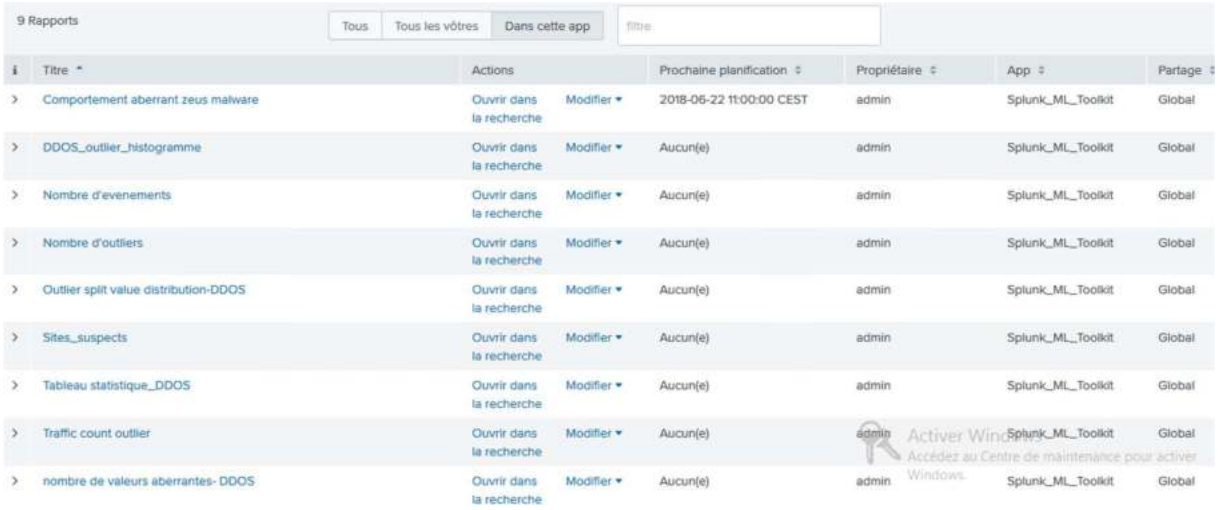


Figure 38: Apprentissage automatique

Le Splunk Machine Learning Toolkit offre plusieurs cas d'utilisation d'analytiques qui peuvent être testés, et customisés pour convenir aux besoins.

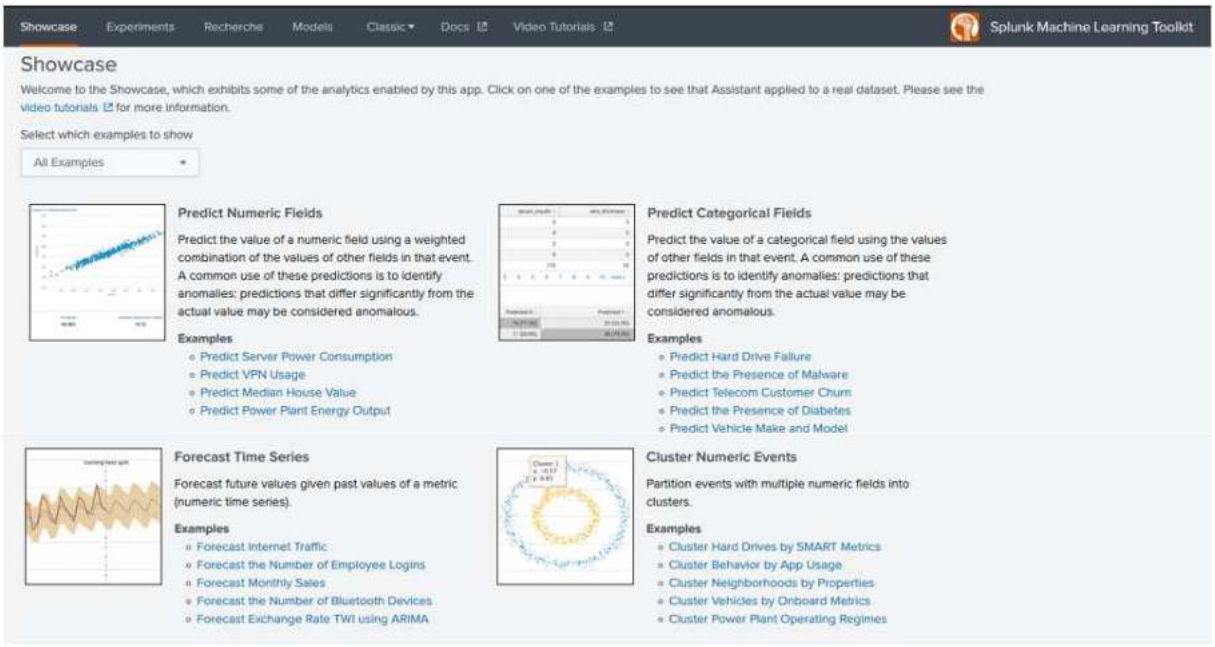


Figure 39: Cas d'utilisation ML-Toolkit

C'est sur ces cas que l'on va se baser dans la suite pour l'implémentation de nos cas d'utilisation.

∞ Malware détection

Pour ce premier cas d'utilisation, nous avons pris deux fichiers logs : le premier est un fichier contenant les logs d'un malware Grandsoft EK et le second fichier contient les logs d'un malware le Trickbot.

Faire ingérer ces logs au système lui a permis de détecter un comportement anormal mais il fallait savoir de quels types de malware il s'agit.

Grandsoft EK qui est un kit d'exploitation qui permet d'utiliser différents types de malware dont Zeus-Panda Banker qui à l'origine est un cheval de Troie qui cherche à récupérer des informations bancaires. Son fonctionnement étant qu'après infection de l'hôte qui peut se faire via une pièce jointe contenu dans un mail douteux ou lien douteux, le malware s'installe sur la machine hôte et commence à se connecter au serveur avec des noms un peu inhabituels et des domaines bidons (.xyz). Ainsi pour détecter la présence de ce malware grâce à Splunk, il fallait d'abord trouver tous les comportements inhabituels et ensuite voir si dans ces comportements il existe des connexions vers des serveurs avec des noms douteux. C'est ainsi que nous avons

pu détecter trois sites aux noms douteux avec qui la machine a commencé à communiquer et ainsi confirmer la présence du malware.

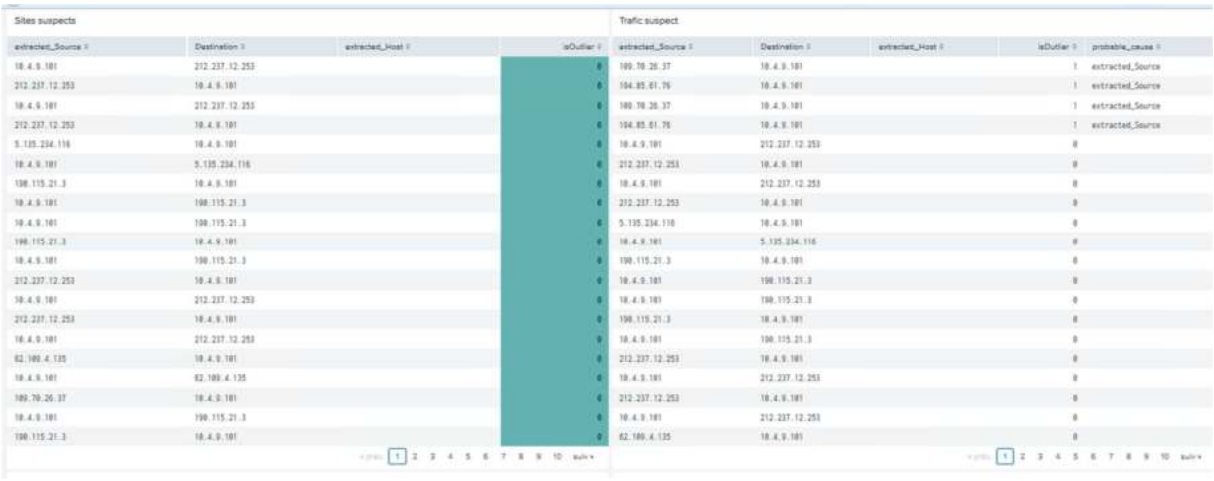


Figure 40: Listes des évènements reçus

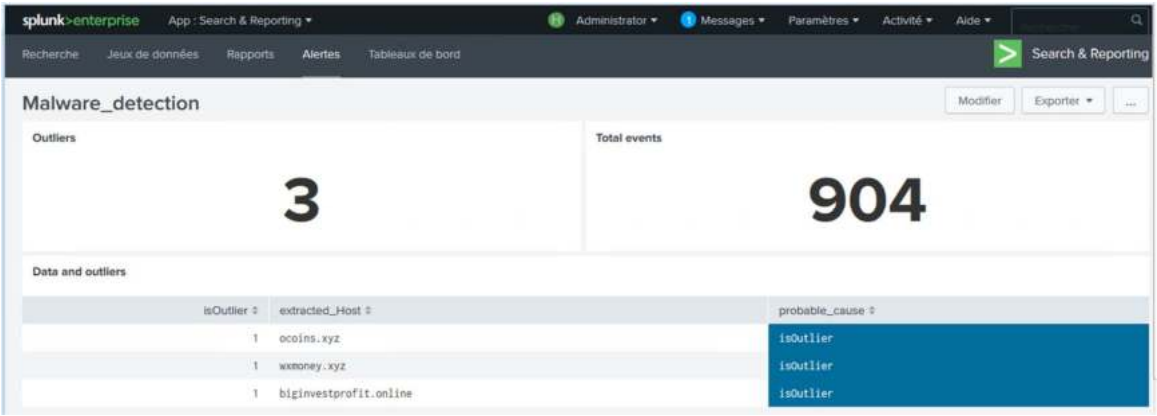


Figure 41: Détection du ransomware

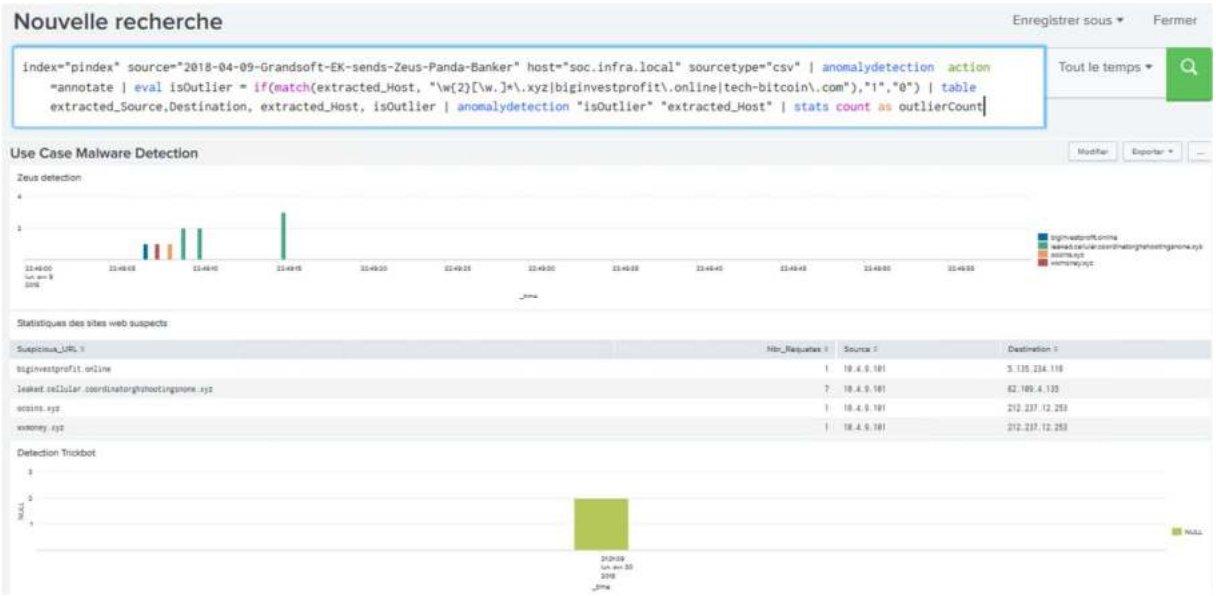


Figure 42: Requêtes permettant d'afficher les sites suspects

Le Trickbot est un cheval de Troie bancaire qui vole les identifiants de connexion de sites bancaires ciblés. Il s'attaque aux systèmes d'exploitation Windows 32 et utilise le protocole Samba et crée des exécutables dans le répertoire Windows.

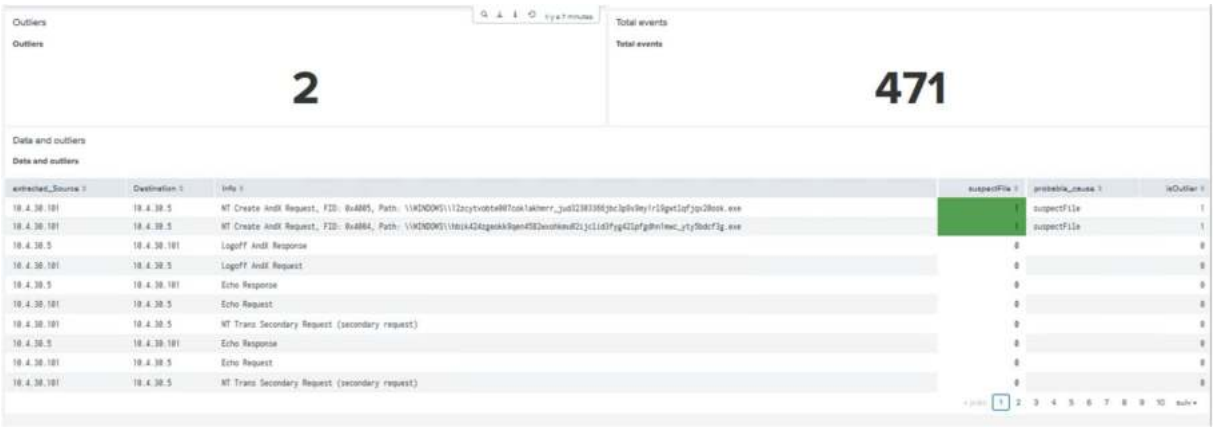


Figure 43: Détection du malware Trickbot

∞ Suspicious connectivity

La détection des DDOS se fait lorsqu'un nombre élevé de connexions est détecté. Plusieurs machines commencent à envoyer des requêtes à la même machine avec des intervalles très courts. Ainsi après avoir fait ingérer les logs d'un fichier DDOS à Splunk, ce dernier a détecté des pics de trafics pendant un temps relativement court.

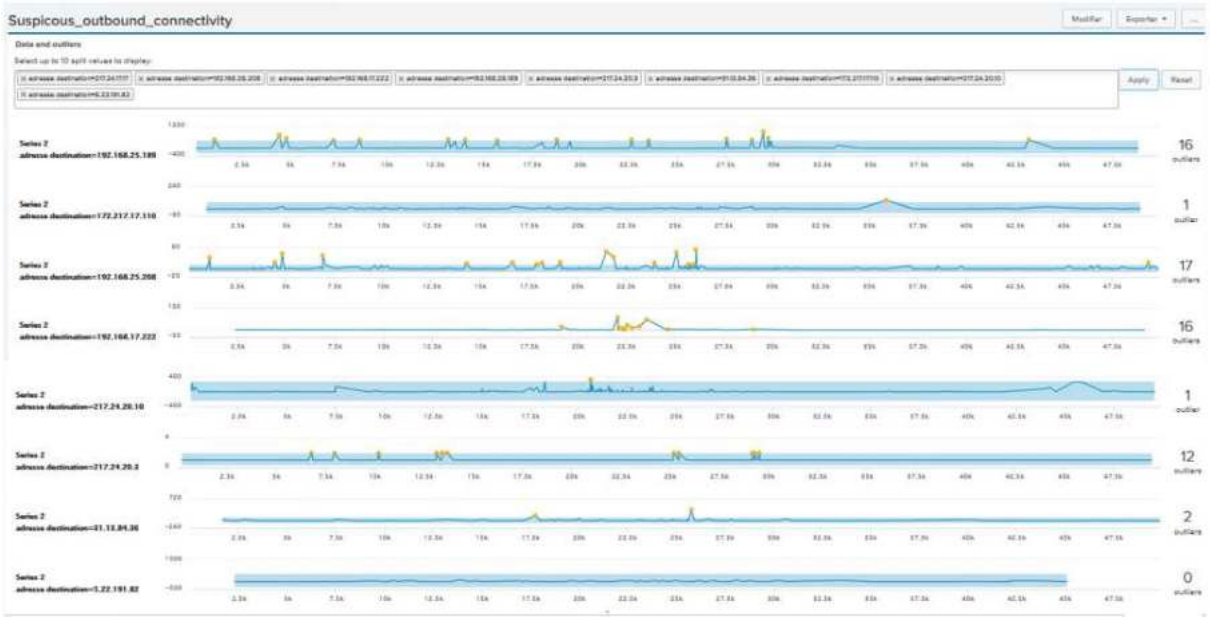


Figure 44: Détection des pics de trafic suspects

Pour améliorer la détection, nous avons ajouté d'autres paramètres et utiliser le Machine Learning. C'est ainsi que certaines sources ont pu être enlevées et la détection est devenue plus précise. Ces sources étant détectées leurs blocage devient aisé.



Figure 45: Amélioration de la détection d'un DDOS

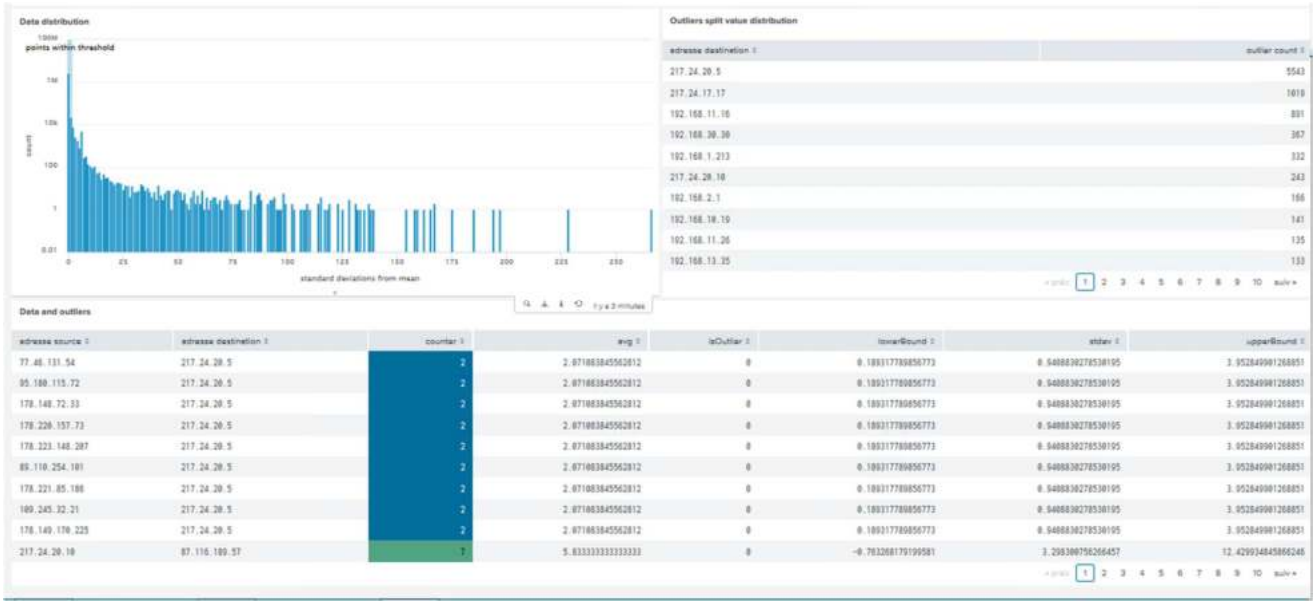


Figure 46: Statistiques en rapport avec le flux DDOS

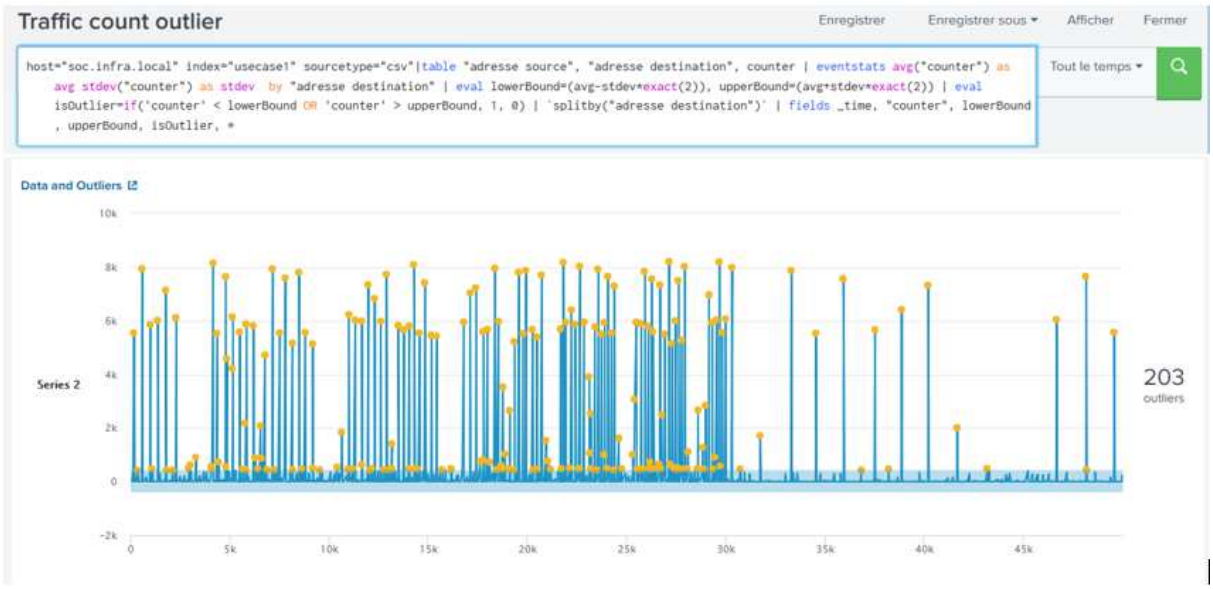


Figure 47: Requêtes SPL pour détecter les comportements aberrants

∞ IoT vulnerability

Ce cas d'utilisation fait partie des plus difficiles à cause des difficultés rencontrées déjà pour obtenir des logs et ensuite parce que la plupart des logs obtenus ne sont pas réellement intéressants. Ainsi nous avons juste pu démontrer que des informations d'authentification circulent en clair sur le réseau.



Figure 48: Requête de détection de vulnérabilités

Ces différents cas d'utilisation montrent l'importance de disposer d'un SOC pour se prémunir des cyberattaques.

4.3.7.2 Customisation des tableaux de bord

Splunk offre plusieurs types de diagrammes de base qui, la plupart du temps, suffisent comme tableau de bord. Toutefois, dans certains cas il serait plus pratique de disposer de diagrammes particuliers ou d'une disposition particulière qui siéent mieux au besoin.

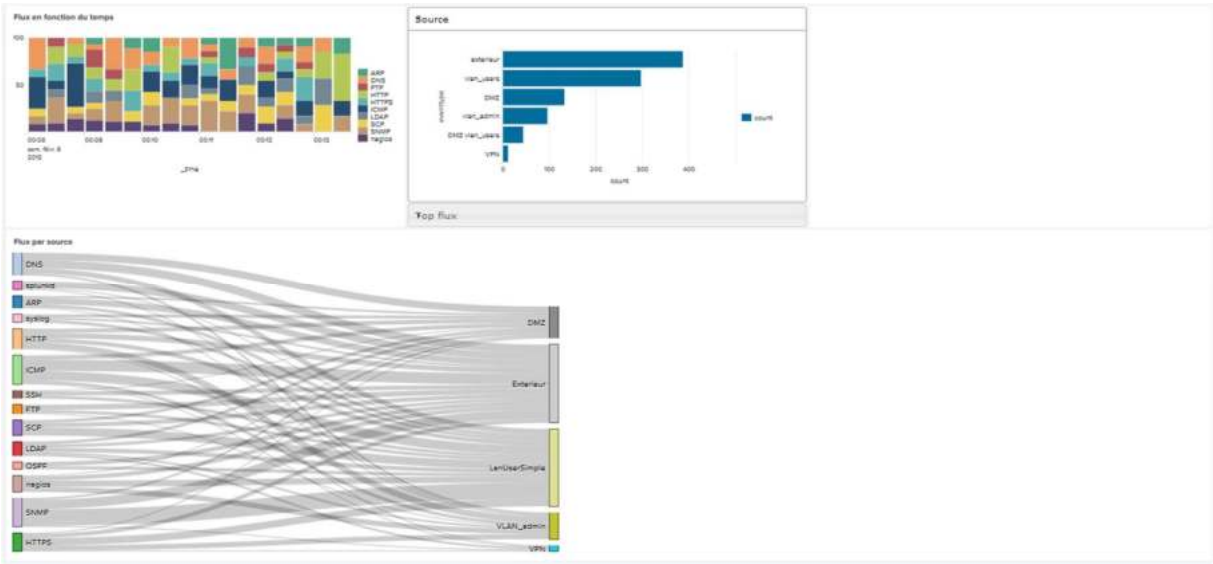


Figure 49: Tableau de bord customisé avec d3js

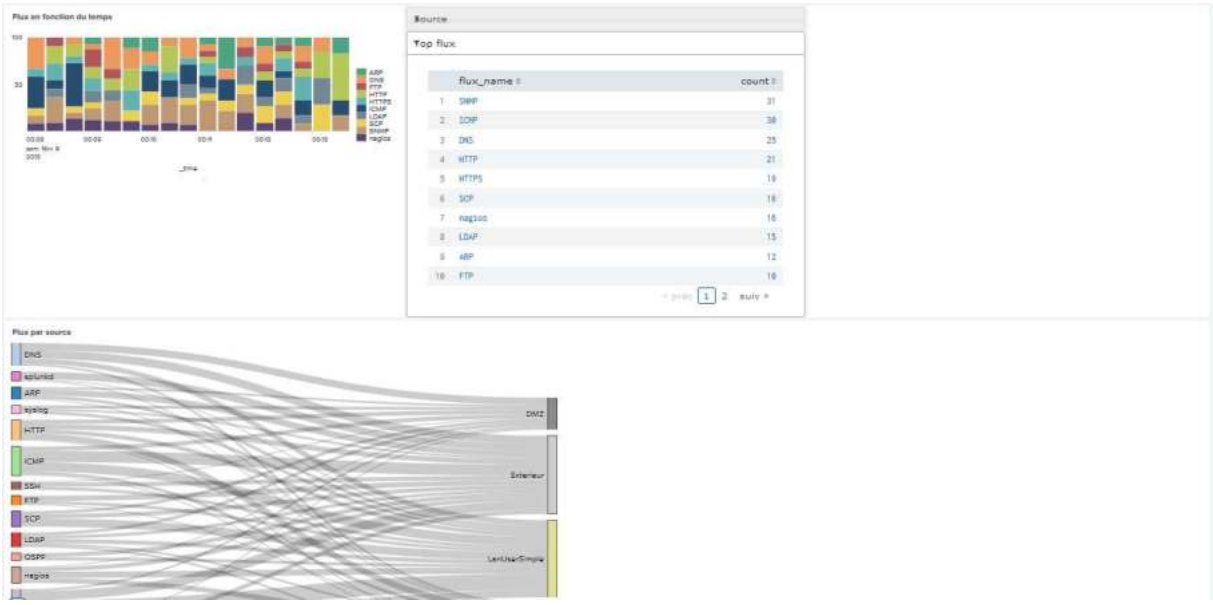


Figure 50: Tableau de bord customisé avec d3js (2)

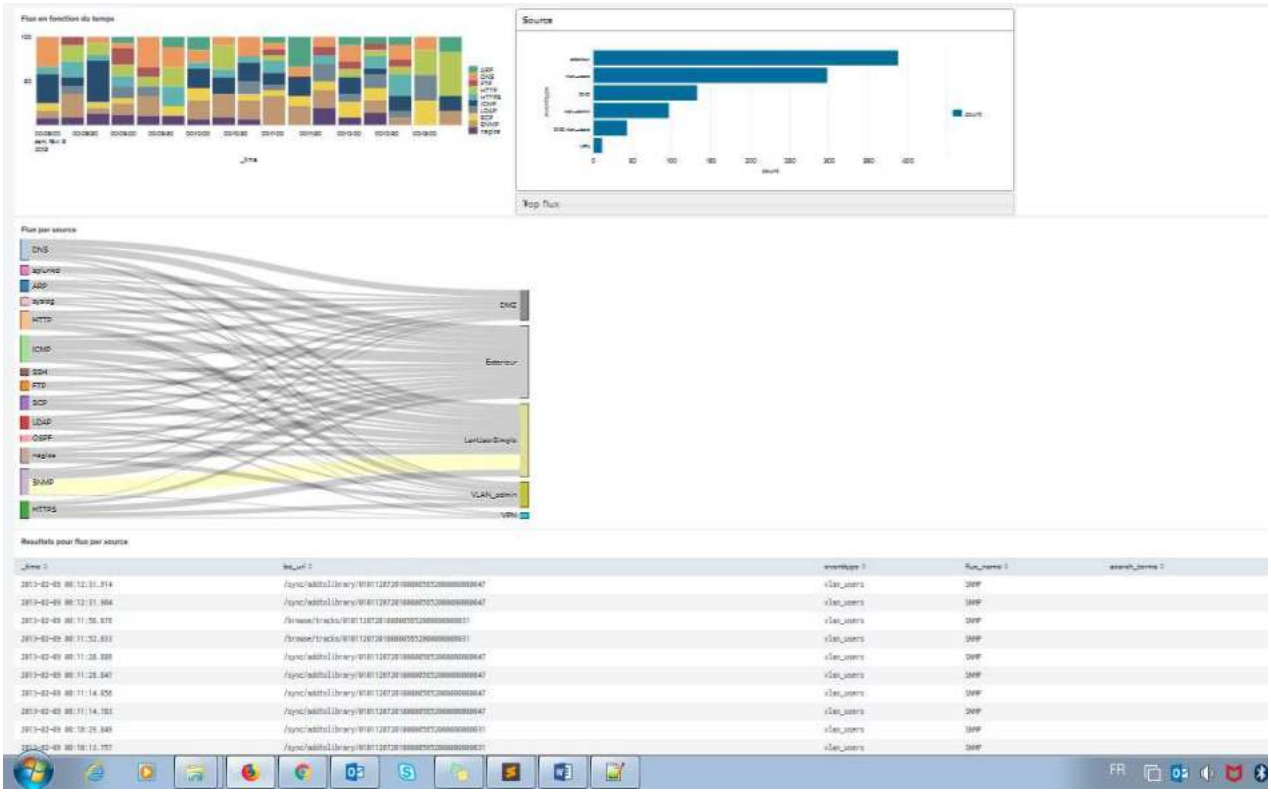


Figure 51: Tableau de bord customisé avec d3js (3)

Conclusion

Le SOC assure la supervision des systèmes d'information de l'entreprise. C'est un outil composé des processus, de technologies ainsi que de compétences diverses et nécessite une implication à tous les niveaux de l'entreprise.

Durant cette étude, l'importance de la mise en place d'un SOC aussi bien par les entreprises tierces que par les OIV, a été démontrée surtout en cette période où celles-ci sont exposées sur Internet, que l'échange et l'accessibilité des données sont une nécessité à leur bon fonctionnement et que la sécurisation de ces données une obligation sur le plan juridique.

Splunk étant l'outil choisi pour la mise en place d'un SOC, nous avons dû faire des études sur ce dernier et essayer de comprendre son fonctionnement avant d'implémenter quelques cas d'utilisation sur des menaces récurrentes.

Cette mise en place d'un SOC avec Splunk, nous a permis de voir l'importance de disposer d'outils de simulation pour tester la résilience de l'infrastructure et ajuster les règles de sécurité que l'on va essayer d'implémenter dans la suite.

Les résultats obtenus à l'issu de stage ont permis à Atos Sénégal de disposer des moyens nécessaires pour mettre en place leur propre SOC, et des études de faisabilités sont en train d'être menées pour la mise en place d'un tel système.

Bibliographies

(Mitre), C. Z. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center.* Mitre.

Atos. (2016). *Atos-Presentation Corporate 2016.*

Chuvakin, D. A. (s.d.). *The complete guide to log and event management* . NetIQ.

Clusif. (2017). *Comment réussir le déploiement d'un SOC.*

compétences, F. d. (2016). *Supervision de la Sécurité du Système d'Information dans les secteurs Banques et Assurances: Le Security Operation Center-SOC.*

Duval, L. (2016, Juillet). *Tout-ce-quil-faut-savoir-sur-Splunk.* Récupéré sur www.lemagit.fr: https://www.lemagit.fr/essentialguide/Tout-ce-quil-faut-savoir-sur-Splunk

Khémissa, S. (2018, Février 2018). *Supervision-de-securite-des-systemes-dinformation-les-limites-du-modele-actuel.* Récupéré sur cybersecurite-hq.fr: http://cybersecurite-hq.fr/2018/02/supervision-de-securite-des-systemes-dinformation-les-limites-du-modele-actuel/

Moutaib, A. (2016, Fevrier 2016). *La-threat-intelligence-une-nouvelle-arme-contre-les-cyber-menaces.* Récupéré sur www.lecercle.biz: https://www.lecercle.biz/Le-Cercle-publications/La-threat-intelligence-une-nouvelle-arme-contre-les-cyber-menaces

Noé, L., & Loureiro, S. (2017, Décembre). *Un SOC ne peut pas uiquement s'appuyer sur un SIEM.* Récupéré sur www.globalsecuritymag.fr: http://www.globalsecuritymag.fr/Un-SOC-efficace-ne-peut-pas,20171219,75852.html

Siemplify. (2017, Septembre 20). *Understanding-the-soc-team-roles-and-responsibilities.* Récupéré sur www.siemplify.co: https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities

Splunk. (s.d.). *search-processing-language.* Récupéré sur /www.splunk.com: https://www.splunk.com/fr_fr/resources/search-processing-language.html

Splunk. (s.d.). *Splunk Enterprise*. Récupéré sur www.splunk.com: https://www.splunk.com/fr_fr/products/splunk-enterprise.html

Annexe 1 : Installation et configuration de base de Splunk

Pour l'installation de Splunk il faut se rendre sur le site de l'éditeur (https://www.splunk.com/fr_fr/download.html) et télécharger la version Splunk adaptée au système d'exploitation du serveur qui va l'héberger. A noter que Splunk Enterprise n'est pas supporté par les systèmes d'exploitation 32bits et qu'il faut disposer d'un compte sur Splunk pour pouvoir télécharger aussi bien le logiciel que les applications et les addons.

Dans notre cas nous avons vu que nous utilisons un serveur centOS 7 64bit pour héberger Splunk, nous avons téléchargé la version rpm de Splunk Enterprise.

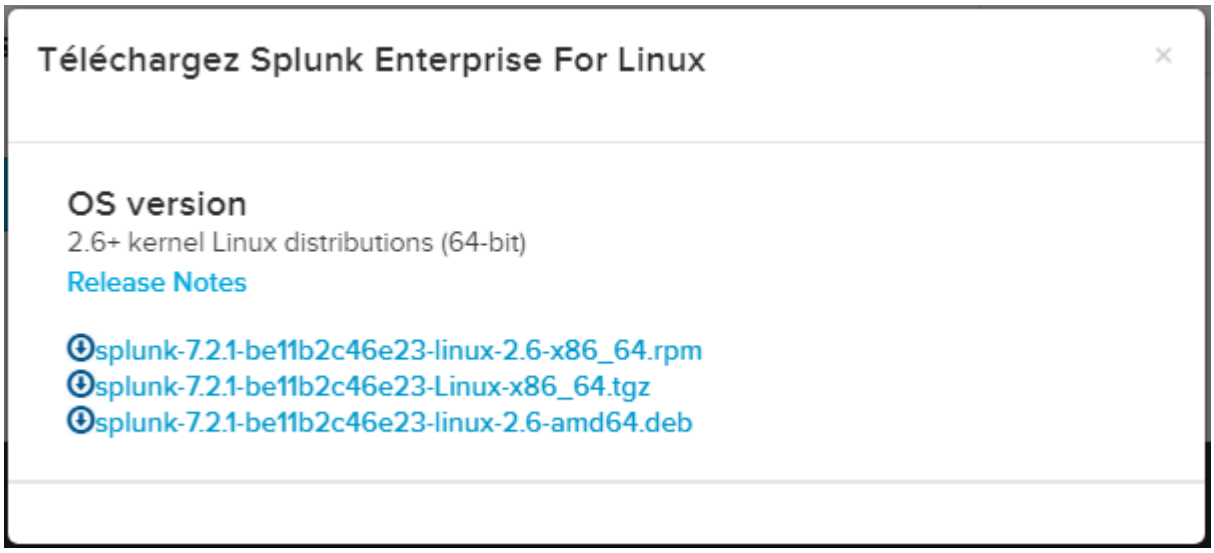


Figure 52: versions Splunk

Il est possible aussi de le télécharger avec la commande wget :

```
wget -O splunk-7.1.2-a0c72a66db66-linux-2.6-x86_64.rpm 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.1.2&product=splunk&filename=splunk-7.1.2-a0c72a66db66-linux-2.6-x86_64.rpm&wget=true'
```

La version téléchargée est une version d'essai de 60 jours avec la possibilité d'indexer jusqu'à 500 Mo par jour.

Pour lancer l'installation, il faut taper la commande suivante :

```
# rpm -i splunk-7.1.2-a0c72a66db66-linux-2.6-x86_64.rpm
```

Splunk est installé par défaut dans le répertoire /opt et pour le lancer il suffit d'entrer la commande :

```
# /opt/splunk/bin/./splunk start
```

Il est demandé d'entrer le mot de passe du compte administrateur. Si l'installation e passe normalement, une clé RSA privée est créée et à partir de ce moment, l'interface web de Splunk est accessible à l'adresse de la machine hôte de Splunk sur le port 8000 qui est le port par défaut (http://@ipmachinesplunk:8000). Par défaut l'application Search est installée

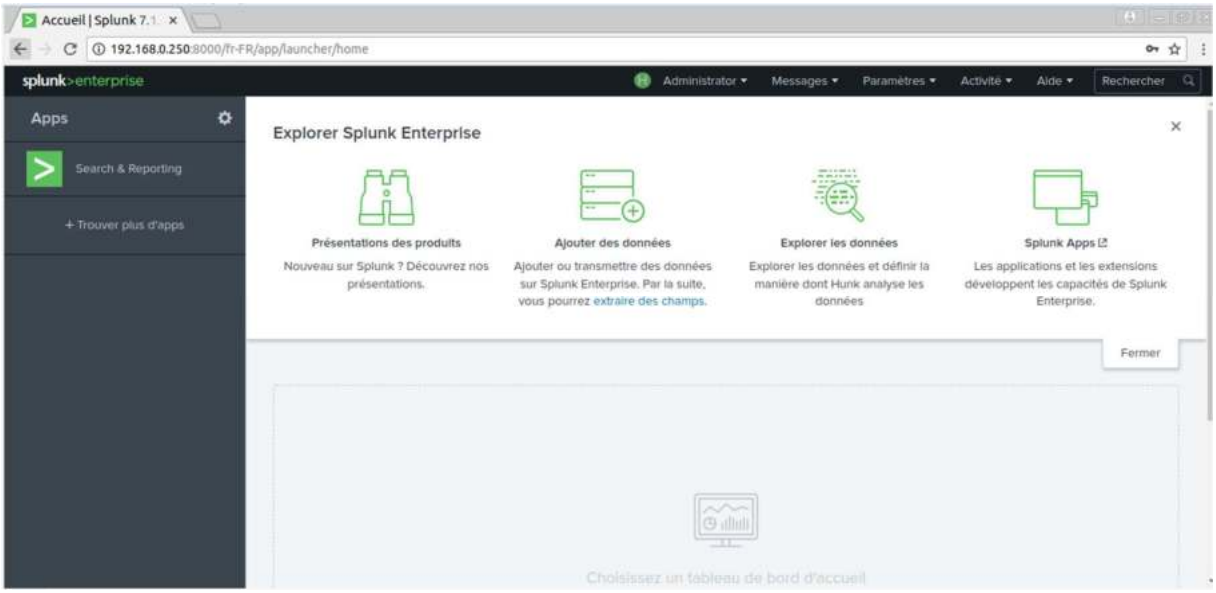


Figure 53: Accueil Splunk

Annexe 2 : Personnalisation des tableaux de bord et création d'applications

Splunk offre la possibilité de personnaliser les tableaux de bord et de créer ses propres applications.

Les tableaux de bord sont liés aux applications à partir d'où ils sont créés et peuvent être modifiés via l'éditeur de tableaux de bord disponible sur l'interface graphique mais cette dernière offre des possibilités limitées. Pour mieux personnaliser les tableaux de bord il faut éditer les fichiers sources de ces derniers généralement localisés dans ***%Repertoire d'installation_de_Splunk%/etc/apps/nomApplication/local/data/ui/***. Les tableaux de bord créés par défaut sont au format XML dans ce cas le fichier se trouve dans le répertoire ***views*** contenu dans le répertoire ***ui***. Et au cas où on souhaite ajouter du Jquerry ou de l'Angular, voir d'autres librairies de graphisme (chartjs, d3js, etc.) il faudrait d'abord convertir le tableau du format XML au format HTML et dans ce cas les fichiers se trouvent dans un nouveau répertoire (***html***) créé toujours dans le répertoire ***ui***.

Pour personnaliser les tableaux de bord HTML (tableaux de bord convertis de Simple XML en HTML) on utilise du JavaScript et le SplunkJS Stack. Le tableau de bord converti utilise SplunkJS Stack pour générer le code sous-jacent. Chaque visualisation XML simple est convertie en un gestionnaire de recherche et en une vue Splunk, avec un wrapper autour de la vue qui inclut une implémentation de panneau. Toute personnalisation du tableau de bord doit être effectuée à l'aide de JavaScript.

Création d'application :

Splunk permet de créer ses propres applications facilement depuis l'interface web. L'intérêt de pouvoir intégrer ses propres applications dans Splunk réside dans la possibilité de pouvoir les adapter selon les besoins du moment.

Dans l'interface web choisir l'option ajouter une nouvelle application et renseigner dans le formulaire le nom, la description (optionnelle), le nom du dossier dans le répertoire standard où sont localisés les fichiers de configuration des applications (repertoire_installation_splunk/etc/apps), ainsi que le modèle à utiliser pour que Splunk génère le squelette de l'application.

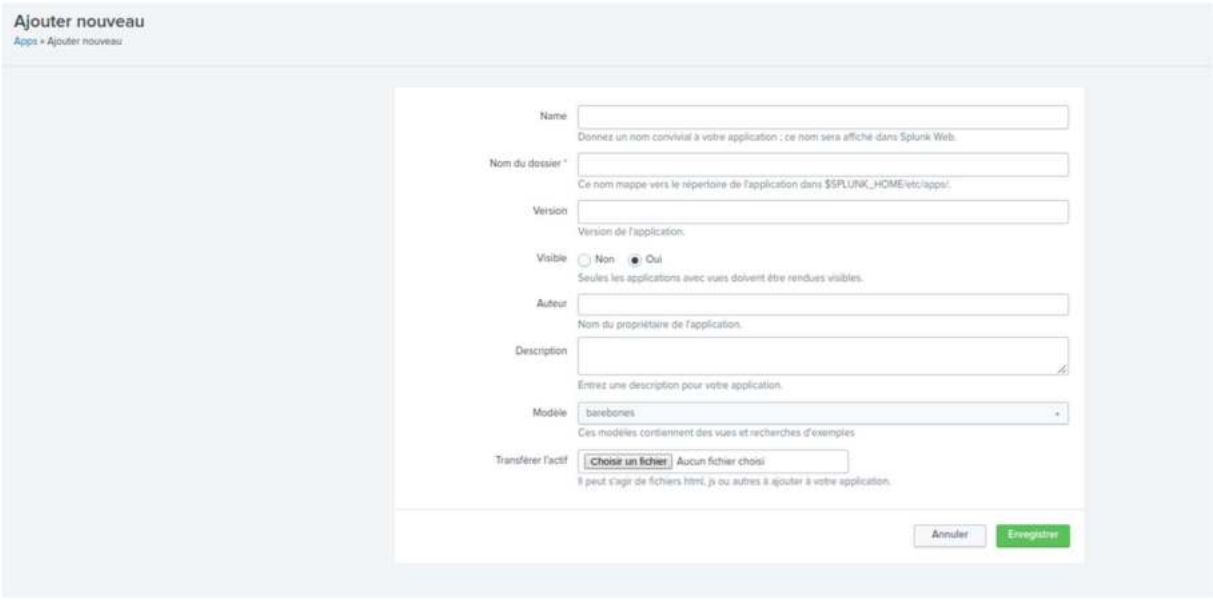


Figure 54: Ajout de l'application

Name	Nom du dossier	Version	Recherche de mises à jour	Visible	Partage	Statut	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Désactivé | Activer	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Désactivé | Activer	
Log Event Alert Action	alert_logevent	7.1.1	Yes	No	App | Permissions	Activé | Désactiver	Modifier les propriétés | Afficher les objets
Webhook Alert Action	alert_webhook	7.1.1	Yes	No	App | Permissions	Activé | Désactiver	Modifier les propriétés | Afficher les objets
Apps Browser	appsbrowser	7.1.1	Yes	No	App | Permissions	Activé	Modifier les propriétés | Afficher les objets
framework	framework		Yes	No	App | Permissions	Activé | Désactiver	Modifier les propriétés | Afficher les objets
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Désactivé | Activer	
introspection_generator_addon	introspection_generator_addon	7.1.1	Yes	No	App | Permissions	Activé | Désactiver	Modifier les propriétés | Afficher les objets
Home	launcher		Yes	Yes	App | Permissions	Activé	Lancer l'app | Modifier les propriétés | Afficher les
learned	learned		Yes	No	App | Permissions	Activé | Désactiver	Modifier les propriétés | Afficher les objets
legacy	legacy		Yes	No	App | Permissions	Désactivé | Activer	
myApp	myApp1	None	Yes	Yes	App | Permissions	Activé | Désactiver	Lancer l'app | Modifier les propriétés | Afficher les
sample data	sample_app		Yes	No	App | Permissions	Désactivé | Activer	

Figure 55: Application visible dans la liste des applications

Après la création de l'application, la page d'accueil de l'application est vide. Il faut donc ajouter un tableau de bord.

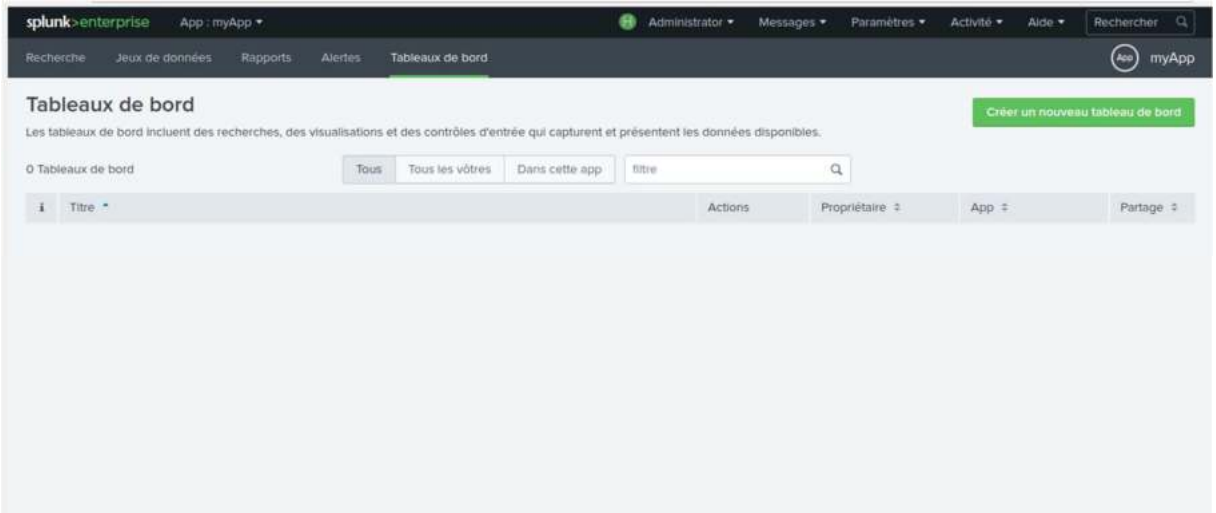


Figure 56: Page d'accueil de l'application

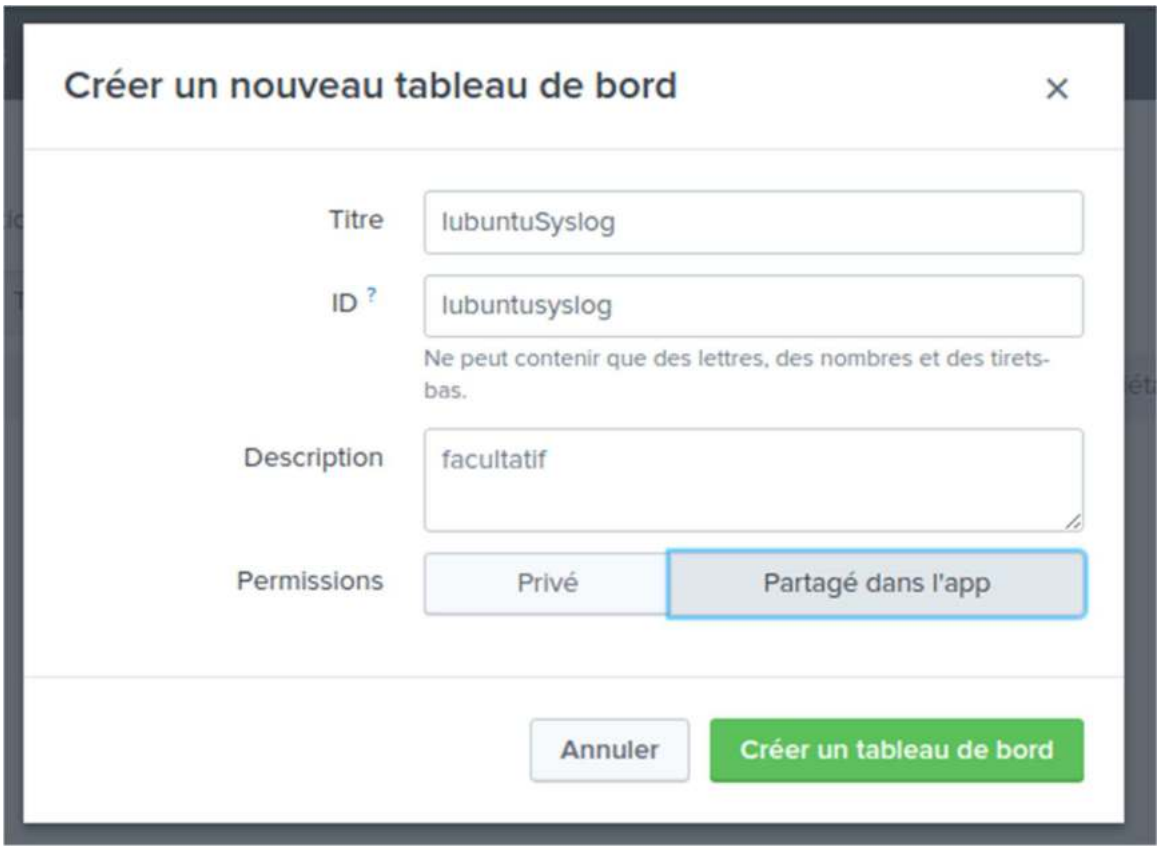


Figure 57: Nouveau tableau de bord

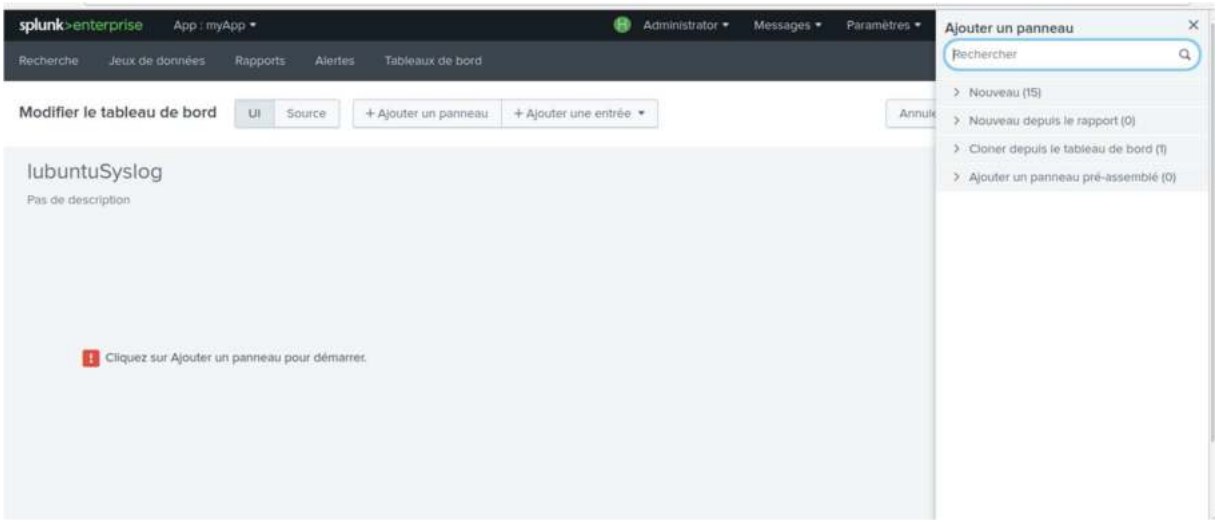


Figure 58: Ajout d'un panel au Dashboard

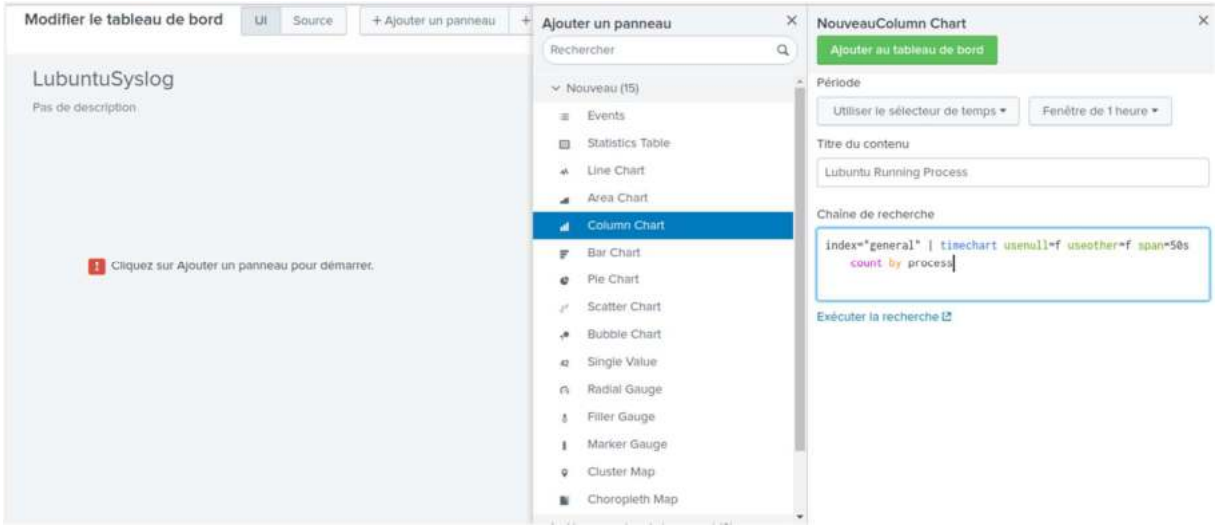


Figure 59: Requêtes pour le tableau de bord

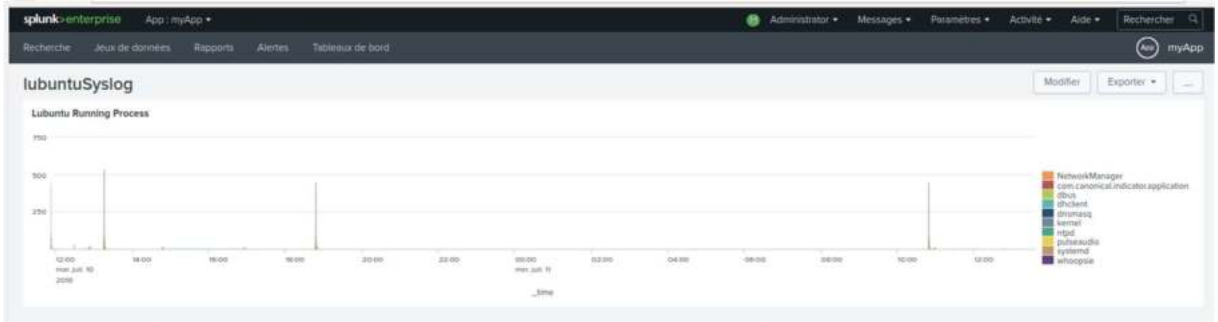


Figure 60: Résultat