Sommaire :

Glossaire :

ACL	ACCESS CONTROL LIST
AD	Active Directory
API	Application Programming Interface
AWS	Amazon Web Service
BASH	Bourne-Again Shell
BDD	Behaviour-Driven Development
BI	Business Intelligent
BPM	Business Process Management
BYOD	Bring Your Own Divece
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Team
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DNS	Domain Name System
DOS	Denial of Service
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GDS	Greenbone Desktop Security
GED	Gestion Electronique des Documents
GSA	Greenbone Security Assistant
GUI	Graphical User Interface
GUN	GUN is Not Unix
HTML	Hypertext Maarkup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IOC	Indicator Of Compromise
IOT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
MISP	Malware Information Sgaring Plateform
MITM	Man In The Middle
MITRE	Massachussetts Institute of Technology Research Establishment
NIDS	Network Intrusion Detection System
NMS	Network Management System
NOSQL	Not only SQL

NVT	Network Vulnerability Test
OPENVAS	Open Vulnerability Assessment Scanner
OSSIM	Open Source Security Information and Event Management
OWASP	Open Web Application Security Project
PAP	Permissible Actions Protocol
PCA	Plan de Continuité d'Activité
PCIDSS	Payment Card Industry Data Security Standard
PDF	Portable Document Formant
PHP	Hypertext Preprocessor
PME	Petite et Moyenne Entreprise
POP3	Post Office Protocol
RRD	Round-Robin Database
RSE	Responsabilité Sociale des Entreprises
SI	System Information
SIEM	Security Information Event Management
SIRP	Security Incident Response Plateform
SLA	Service-level Agreement
SMS	Short Message Service
SMSI	Système de Management de la Sécurité l' Informations
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
SQL	Structured Query Language
SSH	Secure Shell
SSII	Société de Services et d'Ingénierie en Informatique
TIC	Technologie de l'Information et de la Communication
TLP	Traffic Light Protocol
URL	Unform Resource Locator
USB	Universal Serial Bus
VB	Visual Basic
VM	Virtual Machine
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language

Liste des figures :

Liste des Tableaux :

Résumé :

La cybersécurité est un vaste domaine peuplé de personnels spécialisés. Malgré leurs compétences, leur implication et la mise à disposition de ressources toujours plus conséquentes, il est impossible de garantir à 100% qu'une organisation est pleinement protégée contre les cyber-menaces.

Pour faire face à ces cyber-menaces les entreprises doivent faire recours à la détection et la réaction aux incidents de sécurité. Cela nécessite de mettre en place une équipe CERT / CSIRT dédiée à la gestion des incidents de sécurité. Avec l'aide d'outils appropriés cette équipe collectera l'ensemble des logs du SI et les alertes de sécurité. Elle se chargera de mener des investigations relatives à l'incident de sécurité. L'objectif est alors double : identifier la source de l'incident et appliquer les corrections nécessaires pour un retour en conditions de sécurité.

L'utilisation d'un outil de ticketing (TheHive) est indispensable pour garder une trace des incidents survenus sur le périmètre, des actions réalisées et pour permettre la rédaction de retours d'expérience qui pourront être présentés au management.

Abstract :

Cybersecurity is a vast field populated by specialized personnel. Despite their skills, their involvement and the provision of ever-increasing resources, it is impossible to guarantee 100% that an organization is fully protected against cyber threats.

To deal with these cyber threats, companies must resort to the detection and response to security incidents. This requires setting up a CERT / CSIRT team dedicated to the management of security incidents. With the help of appropriate tools, this team will collect all IS logs and security alerts. It will be responsible for investigating the security incident. The objective is therefore twofold: to identify the source of the incident and to apply the necessary corrections for a safe return.

The use of a ticketing tool (TheHive) is essential to keep track of incidents that have occurred on the perimeter, actions carried out and to allow the drafting of feedback that can be presented to management.

Introduction générale

Dans un monde ultra-connecté et où les actions de dématérialisation de processus et le nombre de transactions numériques explosent, les tentations d'utiliser frauduleusement les multiples points d'interconnexions avec l'extérieur, notamment les accès Internet, augmentent de jour en jour. Ainsi, les cyberattaques sont devenues non seulement plus nombreuses et diversifiées, mais aussi plus nuisibles et perturbatrices. Il est fondamental, ainsi, d'identifier et de comprendre les risques susceptibles d'affecter le système d'information et de développer l'agilité nécessaire pour faire face aux nouvelles menaces. De ce fait, la gestion des incidents de cybersécurité est devenue l'un des piliers de la sécurité des systèmes d'information. Cette activité complexe, requiert de nouvelles expertises et nécessite l'implication forte des responsables métiers et surtout du top management. C'est dans cette optique d'anticiper et de régler le plus rapidement possible ces incidents que nous nous sommes proposés de mettre en place une plateforme de gestion des incidents.

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. Dès lors qu'on a géré la sécurité, il est impératif de se mettre sur la défensive afin de pouvoir prévenir les éventuelles incidents de sécurité. C'est ainsi ; que nous allons articuler notre réflexion autour de ces questions :

- Comment centraliser la supervision d'un système d'information ?
- Comment détecter et corriger les incidents en cybersécurité ?
- Comment anticiper et répondre aux incidents de cybersécurité ?

Pour répondre à toutes ces questions nous nous sommes fixés comme objectif générale la mise en place d'un CERT (Computer Emergency Response Team)

Nos objectifs secondaires sont :

- Parler de l'organisation et du management d'un CERT
- Rappeler les objectifs de la sécurité informatique
- Faire une étude comparative des différentes solutions afin de déterminer les plus adaptent à notre projet

- Avoir une vue sur l'ensemble du système d'information afin de pouvoir répondre aux incidents

La protection d'un système d'information (SI) en plaçant uniquement des pare-feu à ses frontières ne suffit plus. Ce qui gère la sécurité sont appelés aujourd'hui à pouvoir anticiper les attaques informatiques, minimiser leurs impacts et avoir un retour rapide à la normale. C'est dans cette perspective que nous avons choisi de mettre en place un CERT (Computer Emergency Response Team)

L'accomplissement de ces objectifs nous conduit à l'hypothèse à laquelle un CERT peut-il empêcher une attaque informatique ?

Pour bien élaborer notre recherche scientifique nous nous sommes éventuellement basés sur la recherche documentaire à travers les sites internet, les différents mémoires lus et les ouvrages scientifiques.

Dans l'optique de mener à bien notre travail, nous allons effectuer une étude et mise en place de notre projet en suivant ce plan :

- ✓ Une Première Partie titrée Cadre méthodologique et Théorique où nous allons expliquer la pertinence du sujet, ainsi que la problématique et les objectifs. Par la même occasion nous allons parler de la sécurité informatique et la cybersécurité.
- ✓ Une Deuxième Partie dans laquelle nous ferons l'Etude conceptuelle sur du management et de l'organisation d'un CERT et aussi l'étude des solutions à déployer.
- ✓ Enfin une Troisième et dernière Partie, dans laquelle nous parlerons de l'implémentation des solutions choisies et les tests de fonctionnement.

Partie I : Cadre Méthodologique et Théorique

Chapitre 1 : Cadre Méthodologique

1.1 Présentation de NEUROTECH :

L'entreprise Neurotech est une Société de Services et d'Ingénierie en Informatique (SSII) qui s'est également développée dans le secteur des télécommunications. Elle a été fondée par M. Abdoulaye MBAYE qui est actuellement le Président Directeur Générale de la structure. Elle forme chaque année ses ingénieurs sur différentes solutions informatiques afin d'évoluer et d'être toujours compétitive face à la concurrence actuelle du marché qui ne cesse de croître. Elle a collaboré avec des dizaines d'entreprises et s'est fait une considération favorable, largement répandu dans le public, grâce à ses prestations de qualité et une implémentation de solutions optimisées pour le développement des systèmes d'informations des entreprises.

✓ Histoire de NEUROTECH

NEUROTECH est une société anonyme crée en Octobre 2003 à Dakar (Sénégal) avec un capital actuel de 142.860.000 FCFA et affiche cinq (05) milliards de chiffres d'affaires. Le siège social de l'entreprise se trouve au quartier du Point-E vers le rondpoint de l'Université Cheikh Anta DIOP.

Elle possède également une filiale à Bamako (Mali) ainsi que des bureaux à Abidjan (Côte d'Ivoire), à Ouagadougou (Burkina), à Cotonou (Bénin) et à Lomé (Togo).

NEUROTECH, c'est avant tout une aventure humaine, une réussite sénégalaise, la réussite d'hommes et de femmes qui ont cru en leur rêve, celui d'ériger l'expertise locale au rang de modèle.

De 3 à 15, puis à 90 collaborateurs de nos jours (2020) dont soixante (60) ingénieurs et techniciens, Neurotech a également développé un portefeuille d'activités large, et parallèlement, construit des processus alignés sur les standards internationaux.

Le Credo de Neurotech est de développer une technologie intelligente, agile, capable de se réinventer et de s'adapter au marché. Un Credo qui s'applique également à l'organisation qui depuis le départ, continue de s'épanouir et de se développer.

✓ Organigramme de NEUROTECH

Un schéma ci-dessus illustre l'organisation simplifiée de Neurotech

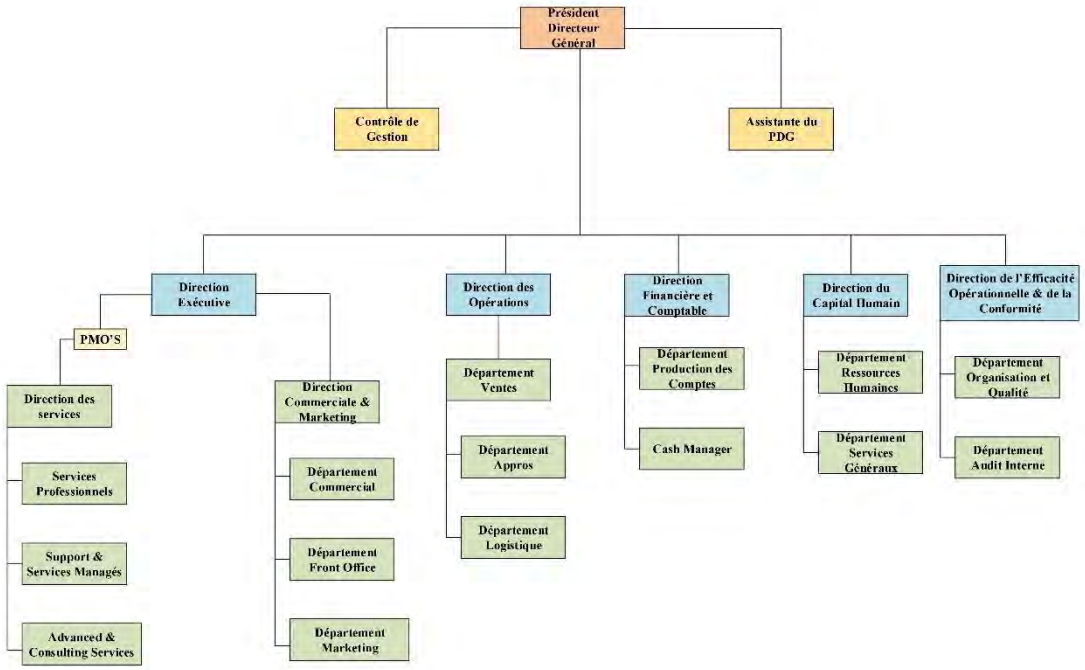


Figure 1:Organigramme de Neurotech

Les Métiers :

L'activité de Neurotech est segmentée en Départements de domaines d'activités différents regroupant des compétences spécifiques.

✓ Département Gestion Electronique de Bâtiment (GEB)

La qualité et l'expertise constituent les maîtres-mots de cette activité qui donne toute la fiabilité du système d'informations. L'expertise de Neurotech touche à tous les domaines du câblage informatique, électrique et apporte également des solutions de wifi, vidéosurveillance et d'urbanisation de Datacenter. Elle touche également les domaines des onduleurs de puissance, la domotique, les ponts radio (FH), l'IoT, le contrôle d'accès et la sécurité physique et la surveillance environnementale des salles serveurs.

✓ Le Département Entreprise Network

Le réseau est au cœur de tout système d'informations. Le savoir-faire de Neurotech dans le domaine de l'infrastructure réseau permet de bénéficier d'une solution réseau complète, modulable et parfaitement dimensionnée aux besoins d'une entreprise. Neurotech apporte des solutions de communications unifiées avec une panoplie de services à valeur ajoutée tout en optimisant les liens WAN (gestion de la bande passante, mutualisation de liaisons télécoms).

✓ Le Département Datacenter & Stockage

De la virtualisation à la sauvegarde, la réduction des coûts d'investissement des clients dans les infrastructures Datacenter est assurée par Neurotech et aucune place n'est laissée à l'improvisation. La réplication améliore la fiabilité, la tolérance aux pannes et la disponibilité d'un système d'informations via un plan de reprise d'activités sur mesure. Le Groupe Neurotech relève avec ses clients le défi de la migration de son infrastructure vers le cloud.

✓ Le Département Sécurité & Optimisation de Performance

L'objectif de Neurotech dans ce département est de réguler et sécuriser au maximum le réseau de ses clients. Il s'engage à optimiser les performances de leur infrastructure en protégeant l'entreprise des risques d'intrusion et de piratage.

De la sécurité périmétrique à la gestion des vulnérabilités, les données sont protégées et sont conformées aux standards internationaux (PCIDSS, ISO27001, etc…). Du firewall applicatif à la gestion du DNS, Neurotech apporte des solutions sur mesure.

✓ Le Département Cloud Client Computing

Neurotech s'adapte en permanence aux changements inhérents à l'adoption de nouvelles technologies. Aujourd'hui, la gestion de l'utilisateur doit prendre en compte la diversité de terminaux que celui-ci utilise (tablette, PC, smartphone). Il s'appuie sur la technologie du cloud pour gérer les utilisateurs de ses clients ainsi que de leurs accès.

✓ Le Département Cloud Information & Content Management

Neurotech se positionne également sur la gestion de l'information.

- **Le Business Intelligent (BI)** offre des outils puissants d'aide à la décision qui permettent de mieux piloter une entreprise et ainsi d'accroitre sa compétitivité.

- **La Gestion Électronique des Documents (GED)** est une solution qui permet de dématérialiser l'activité d'une entreprise et d'améliorer l'accès aux documents pour collaborer plus facilement.
- **Le Business Process Management (BPM)** améliore la performance d'une entreprise en optimisant ses processus.
- **Les solutions CRM (Customer Relationship Management)** permettent la gestion de la relation client.
- **Les ERP (Enterprise Resource Planning)** sont des progiciels de gestion intégrée pour la prise en charge des processus métiers.

✓ La démarche qualité

Neurotech est une entreprise engagée dans une démarche qualité sanctionnée par un certificat ISO 9001 V2015. Cet engagement se matérialise par une politique qui guide toutes ses actions et un système de management qui est évalué régulièrement pour veiller à la performance de l'entreprise. La finalité d'une telle démarche est d'atteindre les objectifs décrits dans sa politique à savoir :

- Être une entreprise performante (rentable, clients satisfaits, bonne organisation)
- Être un employeur de choix (créer un cadre d'épanouissement et de développement personnel pour ses collaborateurs).

Neurotech nourrit le projet ambitieux de demeurer un champion au Sénégal dans l'innovation et la qualité de services et d'être résolument tournée vers son développement en Afrique de l'Ouest et du Centre.

✓ Les organes de décision

• Le Conseil d'administration

Il est composé de cinq (05) membres dont l'Administrateur Général. Ce conseil est compétent pour toutes les décisions stratégiques et pour la validation du budget annuel.

• Le Comité de Direction

Il a une compétence générale sur les questions relatives à l'organisation, le pilotage de l'activité et le reporting. Il est également compétent sur les mesures pouvant affecter les Ressources Humaines (structure des effectifs, durée de travail, conditions d'emploi et de formation). Il regroupe l'Administrateur Général et les Directeurs.

- **Le Comité Exécutif**

C'est un organe de partages et de réflexions sur le management opérationnel et l'exécution de la stratégie.

✓ La Responsabilité Sociétale de Neurotech

- **L'engagement RSE de Neurotech**

Initié par la Direction Générale, la RSE de Neurotech vise à rétablir, unifier et raffermir les liens cordiaux entre les membres du personnel dans un cadre propice à une collaboration agréable. Son caractère transversal lui a donné la possibilité de s'appliquer et de faire observer à ses parties prenantes une conformité aux principes du Global Compact dont elle est signataire.

En effet, un document de communication sur les progrès (COP) publié chaque année sur le site www.unglobalcompact.org décrit l'ensemble des actions menées, des projets entrepris pour appliquer et faire appliquer les 10 principes de Global Compact qui gravitent autour des Droits de l'Homme, de la lutte contre la corruption, des Normes Internationales du Travail et de la Protection de l'Environnement dans sa sphère d'influence.

Afin de répondre au mieux aux préoccupations de chaque membre du personnel, le comité RSE de Neurotech se subdivise en cinq (05) entités. Ceux-ci doivent ainsi servir de cadre d'échanges, d'épanouissement et d'innovation.

Pour ce faire, l'observation des règles de bienséance, l'application de ces règles, l'application des règles fondamentales d'hygiène et de sécurité sont de rigueur dans l'exécution de toutes les activités à mener en groupe ou individuellement.

Ces différents comités sont présentés ci-dessous.

✓ Les Comités RSE

- **Human Cloud**

Ce comité veille au rapprochement et à la cohésion du groupe. Un véritable esprit d'entreprise se fait sentir à travers les actions et les activités qu'elle aura à mener.

- **Hygiène Santé et Sécurité au Travail**

Comme son nom l'indique, ce comité anticipe sur les risques liés au non-respect des normes d'hygiène, de santé et de sécurité pour les travailleurs. Ce comité a un caractère réglementaire et met en place des actions à la mesure de l'entreprise, de son cadre et de son quotidien.

- **Développement Durable**

L'objectif de ce comité repose sur trois (03) piliers : Les projets devront être économiquement efficaces, socialement équitables et écologiquement viables.

- **Sport**

L'objectif du comité sport est d'inciter le personnel à adopter une meilleure qualité de vie à travers la pratique régulière d'une ou plusieurs disciplines sportives.

- **Relations Publique et Partenariats**

Il est question pour ce comité de donner vie à ses relations de partenariat à travers une animation soutenue de chacune d'entre elles. Un portefeuille diversifié d'activités est le gage d'un impact apprécié par ses partenaires.

1.2 Contexte du sujet

Avec la forte évolution des nouvelles technologies et la capacité de traitement des données par les systèmes informations, les attaques informatiques sont devenues plus fréquent. Aucune entreprise ne peut affirmer maîtriser son système d'information à 100% encore moins sa sécurité. Aujourd'hui la question à se pose n'est plus quand est-ce qu'ont été victimes d'une cyber-attaque, mais plutôt s'interroger depuis quand, comment et pourquoi notre système d'information a été compromis.

1.3 Problématique

L'époque où on pouvait protéger un système d'information (SI) uniquement en plaçant des pare-feu à ses frontières est bel et bien révolue. Avec l'arrivée du BYOD, l'heure est à l'ouverture des SI. Un impératif pour permettre une meilleure collaboration entre les équipes, tant en interne qu'avec les partenaires de l'entreprise. Mais aussi une opportunité pour les pirates qui en profitent pour s'infiltrer sur les serveurs pour dérober des informations ou se servir des machines comme relai (via un réseau de botnet) pour des attaques plus vaste. Les

systèmes d'informations se sont ouverts vers l'extérieur et aujourd'hui la question n'est plus de savoir si on sera attaqué mais quand. Il faut revoir notre approche quant aux systèmes de défense et d'alerte en alliant les équipements de sécurité ainsi qu'à l'analyse des informations générés par ces derniers nous menant à une analyse prédictive des événements du système d'information. Par conséquent il est impératif de mettre en place un système de gestion des incidents permettant de détecter et de résoudre les incidents le plus rapidement possible.

1.4 Objectif du sujet

Suite à une contextualisation du sujet et une problématique bien posée le besoin de mettre en place une plateforme de gestion des incidents de cybersécurité se fait sentir. Pour ce faire nos objectifs sont les suivantes ;

- Définir le rôle que joue un CERT
- Faire une étude des différents outils
- Proposer un outil de sonde d'analyse détaillée de trafic réseau
- Proposer un outil de découverte et mesure de la disponibilité des services réseau
- Proposer un outil de gestion intégrée des vulnérabilités
- Proposer un outil de centralisation et d'analyse des évènements
- Proposer un outil de gestion des incidents de sécurité
- Proposer un outil de protection des applications web contre les cyberattaques

1.5 Pertinence du sujet :

De nos jours, les entreprises peuvent être victimes d'attaques sur plusieurs fronts, comme jamais auparavant. Chaque application constitue une nouvelle ouverture par laquelle les attaquants peuvent tenter d'accéder aux précieux renseignements de l'entreprise. Pour une entreprise, la question n'est pas de savoir si elle sera visée par une cyberattaque mais plutôt quand. Et c'est à cet instant qu'il faut se préparer en investissant dans la détection et la réaction à une attaque informatique.

1.6 Délimitation du sujet :

Pour mener à bien l'élaboration de ce document, nous avons jugé nécessaire de circonscrire aussi bien dans l'espace que dans le temps son champ d'investigation. Notre travail se limite dans une architecture virtuelle basé sur des outils de simulations ou d'émulations. Dans cette

perspective, nous visons à reproduire une plateforme de gestion des incidents qui pourrait être implanté à NEUROTECH.

Chapitre 2 : cadre théorique : Sécurité informatique et cybersécurité

2.1. Objectif de sécurité

La cybersécurité concerne la sécurité informatique, celle de l'information et la sécurité des réseaux, des environnements connectés à Internet. La sécurité des systèmes accessibles via le cyberspace peut être mise en défaut, entre autres, par des cyberattaques. Ainsi, du fait de l'usage extensif d'internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveau d'importance variable, peuvent affecter les individus, les organisations ou les Etats.

La notion de sécurité informatique fait référence à des propriétés d'un système informatique qui s'expriment en termes de disponibilité, d'intégrité et de confidentialité. Ces critères de base sont réalisés par la mise en œuvre de fonctions et services de sécurité, tels que ceux contrôle d'accès ou de détection d'incidents par exemple. Des services de sécurité liés à l'authentification ou encore à la non-répudiation, à l'imputabilité, ou à la traçabilité contribuent à protéger des infrastructures numériques

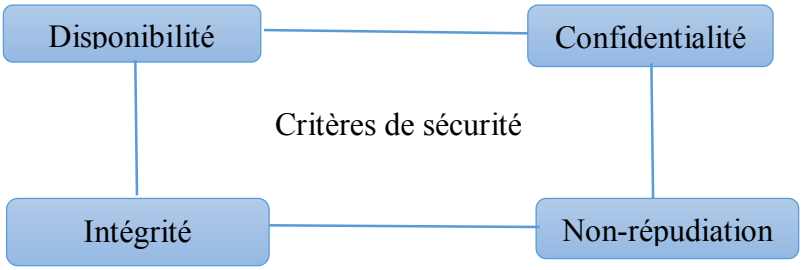


Figure 2:Critère de sécurité

- ✓ **Disponibilité :**

La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service détermine la capacité d'une ressource à être utilisée. Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit.

La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié et une certaine redondance ainsi que par une gestion opérationnelle et une maintenance efficaces des ressources. Un service nominal doit être assuré avec le minimum d'interruption, il doit respecter les clauses de l'engagement de service établies sur des indicateurs dédiés à la mesure de la continuité de service. Des pertes ou destruction de données, donc une indisponibilité de celles-ci, sont possible si les procédures de sauvegarde et de restitution ainsi que les supports de mémorisation associés ne sont pas gérés correctement ou il y a malveillance. Une politique de sauvegarde ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité, supportable par l'entreprise doivent être préalablement établis pour que la mise en œuvre des mesures technique soit efficient.

- ✓ **Intégrité :**

Le critère d'intégrité des ressources physiques et logiques (équipement, données, traitement, transaction, services) est relatif au fait qu'elles sont demeurées intactes, qu'elles n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires tant de manière intentionnelle, qu'accidentelle. Préserver l'intégrité des ressources et s'assurer que les ressources sont intègres sont l'objet de mesures de sécurité. Ainsi, se prémunir contre l'altération des données et avoir la certitude qu'elles n'ont pas été modifiées collabore à la qualité des prises de décision basées sur celles-ci

- ✓ **Confidentialité :**

La notion de confidentialité est liée au maintien du secret, elle est réalisée par la protection des données contre une divulgation non autorisée. Il existe deux types d'action complémentaires permettant d'assurer la confidentialité des données :

- Limiter et contrôler leurs accès afin que seules les habilitées à les lire ou à les modifier puissent le faire ;
- Les rendre inintelligible en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

- ✓ **Authentification :**

L'authentification permet de vérifier l'identité d'une entité afin de s'assurer de son authenticité. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une

information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique.

- ✓ **Non-répudiation :**

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité.

2.2. Domaines d'application

Toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité informatique. En fonction de son domaine d'application, celle-ci peut se décliner en :

- ✓ **Sécurité matérielle, physique et environnementale :**

La sécurité matérielle, physique et environnementale concerne tous les aspects liés à la sécurité des composantes, équipements et systèmes de l'environnement dans lequel ils se situent. Sans vouloir être exhaustif, nous retiendrons que la sécurité physique repose essentiellement sur :

- La fiabilité des matériaux (éléments matériels constitutifs des systèmes) et usage d'équipement qui possèdent un bon degré de sûreté de fonctionnement, de fiabilité et de robustesse ;
- Protection des sources énergétique et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- La redondance physique des infrastructures et des sources énergétiques ;
- Le plan de maintenance préventive.

- ✓ **Sécurité logique, sécurité applicative et sécurité de l'information :**

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle s'appuie généralement sur :

- La qualité de développement des logiciels et des tests de sécurité ;
- Une mise en œuvre adéquate de la cryptographie pour assurer intégrité et confidentialité ;
- Des procédures de contrôle d'accès logique et d'authentification ;

- Des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents.

✓ **Sécurité de l'exploitation :**

La sécurité de l'exploitation doit permettre un bon fonctionnement opérationnel des systèmes informatiques et des réseaux de télécommunication. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour. Les points clés de la sécurité de l'exploitation sont les suivantes :

- Gestion du parc informatique ;
- Gestion des configurations et des mises à jour ;
- Gestion des incidents et suivi jusqu'à leur résolution ;
- Gestion des performances ;
- Gestion des sauvegardes, des secours et de la continuité ;
- Gestion de la maintenance et des contrats de maintenance ;
- Gestion des logs et des fichiers de journalisation.

✓ **Sécurité des réseaux de télécommunication :**

La sécurité des télécommunications consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler). Cela s'appuie sur des mesures architecturales adaptées, l'usage de plate-forme matérielles et logicielles sécurisées et une gestion de réseau de qualité.

✓ **Cybersécurité**

L'objet de la cybersécurité est de maîtriser les risques liés à l'usage du numérique et du cyberspace. Cela concerne toutes les infrastructures, tous les systèmes d'information, services et données ainsi que tous les acteurs qui dépendent du numérique. Désormais, toutes les activités de la société intègrent un élément de traitement informatisé dont il faut assurer le bon fonctionnement, la cohérence, la sûreté de fonctionnement, la fiabilité, la sécurité et la résilience.

2.3. Politique de sécurité

L'information s'impose comme un capital des plus précieux pour l'entreprise. Le système d'information, constituer des moyens informatiques, est essentiel à l'activité de l'entreprise. L'utilisation inappropriée du SI, ou son mal fonctionnement peuvent menacer l'existence de l'entreprise. En analysant et définissant les risques, l'on peut construire une politique de sécurité du SI, définissant le cadre d'utilisation des moyens informatiques.

La politique de sécurité informatique fixe les principes visant à garantir la protection des ressources informatiques et de télécommunications en tenant compte des intérêts de l'entreprise et de la protection des utilisateurs. Les ressources informatiques et de télécommunications doivent être protégées afin de garantir confidentialité, intégrité et disponibilité des informations qu'elles traitent, dans le respect de la législation en vigueur.

L'entreprise doit se doter d'une organisation et d'une politique de sécurité du système d'information. Cette politique doit ensuite se décliner en un plan d'actions à plusieurs volets : mesure organisationnelles, mesure technique, mesure sociale liées aux ressources humaines, aspects juridiques. L'organisation quotidienne de la sécurité doit poursuivre les efforts réalisés en amont en dotant l'entreprise d'outils de mesure et de pilotage des actions de sécurité.

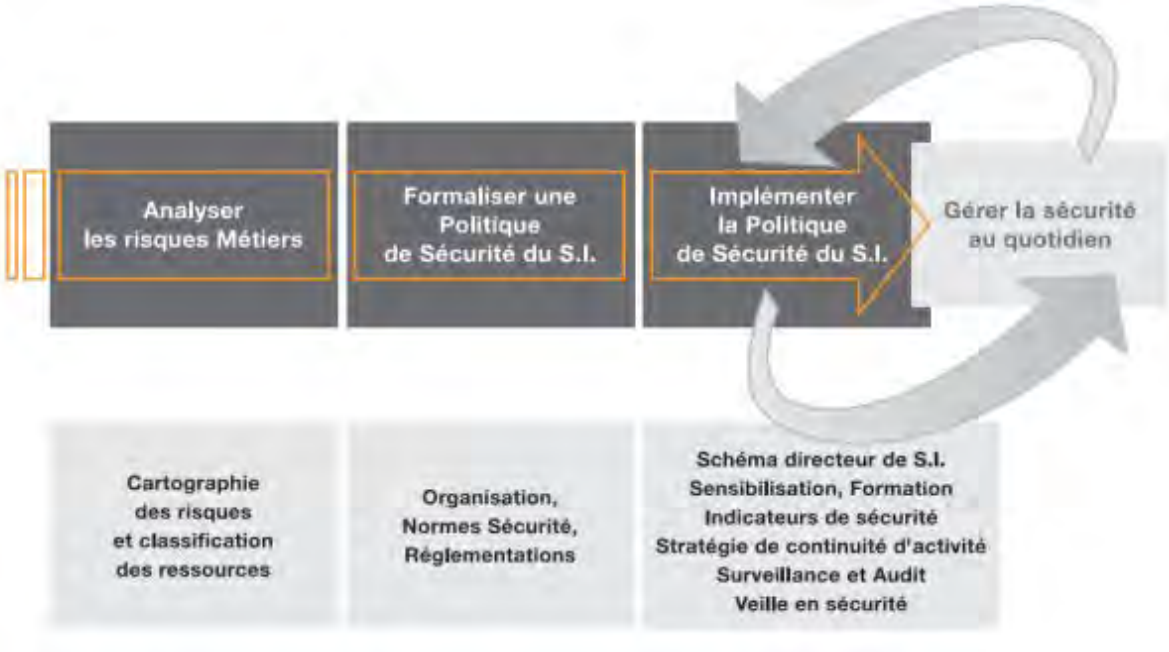


Figure 3:Démarche globale de protection du SI

La gestion de la sécurité s'organise autour de quatre missions majeures :

- ✓ **Etudes et standards de sécurité**

L'objectif principale consiste à rédiger la politique de sécurité ou le plan de continuité d'activité, puis à les décliner dans les processus projets et exploitation. Cela permet de transformer les concepts et les directives en réalisations concrètes sur le système d'information. Cette fonction couvre à la fois les impératifs de « prévention » et « défense ».

- ✓ **Contrôle de la sécurité**

Elle regroupe l'ensemble des actions permettant de mesurer le niveau de sécurité de tout ou une partie du système d'information : identifications objective et exhaustive des menaces, évaluation de l'efficacité des mesures de protection, suivi des procédures correctrices (mise en conformité). Elle répond ainsi à l'objectif de « contrôle ».

- ✓ **Administration de la sécurité**

Cette fonction englobe des actions qui visent la mise en œuvre, la surveillance et l'application des règles de sécurité aux systèmes d'information. Elle couvre les aspects techniques des objectifs de prévention, de défense et de détection. Ainsi les actions de configuration permettent de maintenir les composantes du système d'information à un niveau optimal de sécurité. Les actions de supervision permettent quant à elles de détecter tout évènement anormal identifier et d'initier les actions correctrices.

- ✓ **Pilotage de la sécurité**

Cette fonction couvre tous les objectifs de sécurité et joue un rôle central dans le dispositif de gestion de la sécurité. Elle représente la « tour de contrôle » en termes de coordination et d'homogénéité des actions de sécurité au quotidien, de manière proactive et réactive 'veille de sécurité, solutions réactives). Elle permet de suivre le niveau de sécurité interne et externe (reporting, tableaux de bords) et d'apporter des réponses efficaces aux nouvelles menaces (gestion de crises).

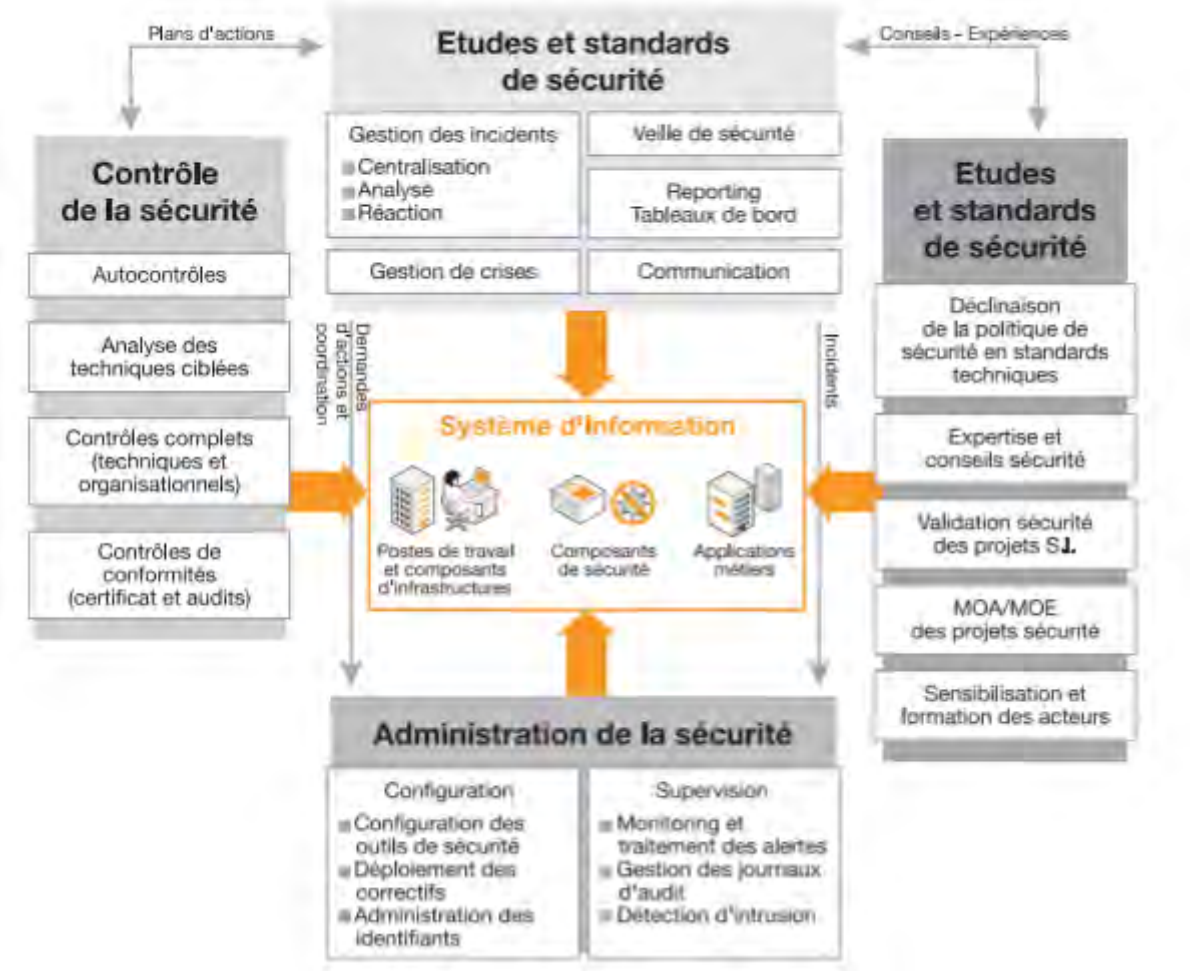


Figure 4: Vue d'ensemble des fonctions de la gestion de la sécurité

Ces différentes fonctions s'exercent sur l'ensemble des composantes du système d'information des postes de travail aux application métiers en passant par les composantes d'infrastructure et de sécurité. Ces fonctions interagissent très fortement entre elles. Analysons de plus près la fonction de pilotage de la sécurité.

La fonction de pilotage de la sécurité constitue un point de centralisation de l'ensemble des évènements de sécurité survenant sur le système d'information. Ces évènements comprennent :

- Le recensement des menaces externes, grâce à une veille de sécurité active ;
- La détection des évènements et incidents dans le cadre des actions de supervision ;
- La compilation des résultats des différentes actions de contrôle.

Chaque évènement remonté à la fonction de pilotage doit faire l'objet d'une évaluation, via une analyse de risques. Selon les risques encouru un niveau de priorité sera affecté au traitement de chaque évènement. Une telle analyse nécessite une connaissance précise de la

criticité et du niveau de vulnérabilité de chaque composant du système d'information. Les actions à mener pour limiter les menaces ou pour traiter les incidents sont ensuite identifiées :

- De manière proactive : mise à jour des logiciels antivirus, surveillance de l'activité du réseau, déploiement des correctifs ;
- En cas d'incident : déconnexion des ressources critiques, fermeture des ports de réseaux, isolation des réseaux locaux

La fonction de pilotage assure le suivi de la réalisation de ces actions afin de maîtriser les risques. La constitution d'une cellule de gestion de crise peut être décidée pour traiter les incidents les plus critiques. Elle s'appuie généralement sur les structures et les processus existants (déclenchement et pilotage de plan de reprise d'activité, mobilisation de la cellule de communication au sein de l'entreprise…). Le pilotage de la sécurité inscrit la gestion de la sécurité dans une boucle d'amélioration continue.

Figure 5: Boucle d'amélioration continue

Reporting et tableaux de bord sont au cœur de la boucle d'amélioration continue grâce aux indicateurs (fonctionnels, stratégiques et opérationnels) qui alimentent le système de pilotage. Leur analyse permet de maîtriser les risques dans le temps, en fonction des objectifs définis. Les tableaux de bord constituent ainsi un instrument de mesure de la qualité du dispositif de gestion de sécurité. Ils sont aussi des outils de sensibilisation et de communication puissants.

2.4. Gestion de la sécurité du SI

Pour maîtriser la sécurité de façon permanente, plusieurs objectifs doivent être remplis. Détection : surveiller pour faire face aux nouvelles menaces il s'agit d'analyser les mesures capables de limiter la probabilité qu'un incident de sécurité ne se produise. Une veille sur les points de vulnérabilité devient indispensable pour identifier, analyser les nouvelles menaces puis décider des actions correctrices à effectuer.

- ✓ **Détection :** surveiller l'état de santé du SI

La détection d'une attaque est une information cruciale. En effet, ignorer une attaque interdit tout déclenchement rapide des mesures de défense destinées à limiter les dégâts. La sophistication des techniques d'attaques, exige de disposer des moyens permettant de signaler rapidement toute anomalie du système d'information et de stopper ainsi toute tentative d'intrusion.

- ✓ **Réaction :** définir un plan de secours

Cet objectif consiste à définir les actions à suivre lorsqu'un incident survient, afin de minimiser son impact. L'élaboration d'un PCA permet de garantir la survie du SI. Ses caractéristiques premières sont rapidité et cohérence des actions. La rapidité est essentielle pour limiter les impacts et répondre face à la vitesse de propagation d'une attaque. La cohérence permet d'intervenir de manière complète homogène sur l'ensemble du périmètre du système d'information. Il convient cependant de rappeler que le niveau de sécurité du système d'information demeure toujours équivalent à celui du maillon le plus faible. Le PCA doit donc garantir une coordination générale des actions telle que la mobilisation de la structure de gestion de crise ou l'activation des procédures d'escalade pour répondre efficacement aux incidents.

- ✓ **Contrôle :** adapter en permanence les processus et les moyens de sécurité

Au cours du temps, risque et besoins évoluent. Il convient donc de contrôler régulièrement la pertinence de la politique de sécurité et de surveiller en permanence les processus et les systèmes de sécurité. Une démarche de pilotage des actions de sécurisation, contrôlée par des indicateurs quantitatifs, permet sa mise en œuvre. Ces indicateurs permettent de fournir à la Direction Générale une mesure sur le niveau de sécurité global du système d'information.

Leur incrémentation dans des tableaux de bord aide à apprécier l'efficacité des processus de sécurité et à discerner des vecteurs d'ajustement. Ils doivent refléter l'activité liée aux enjeux Business.

La gestion de la sécurité constitue une solution efficace pour atteindre ces objectifs. Cette organisation est nécessaire, et on perçoit aisément les limites d'une démarche « artisanale » dans le domaine. Chaque entreprise doit s'organiser et se doter progressivement d'un centre de pilotage pérenne. Ce travail d'organisation doit permettre de maîtriser les coûts générés par la gestion de la sécurité, en optimisant les ressources et les procédures de gestion de risques.

2.5. Audit de la sécurité

L'objectif principale d'un audit de sécurité est d'évaluer avec précision la capacité du système d'information à résister aux attaques informatiques, à identifier les failles et appliquer les actions correctives nécessaires avant qu'il ne soit trop tard. Identifier les forces et les faiblesses du SI, permet d'obtenir une vision complète et réaliste de la capacité de l'infrastructure analysée à résister aux attaques de tous types et de toutes origines, en développant les axes de progression préalablement identifiées.

Un audit de sécurité SI peut être réalisé pour répondre à des besoins différents, notamment :

Evaluer le niveau de maturité du SI en terme de sécurité suite à la demande du commanditaire d'audit

- Vérifier l'efficacité de la politique de sécurité du SI mise en place ;
- Tester la sécurité d'un nouvel élément installer dans le SI ;
- Analyser et réagir suite à une attaque ;
- Tester la résistance du SI par la simulation des attaques dans des conditions réelles ;
- Se certifier (par exemple ISO 27001)

Une mission d'audit de sécurité ne permet que de trouver les vulnérabilités liées au SI et de proposer des actions correctives à travers un ensemble de vérifications et de contrôles. A l'issue de la mission, le prestataire d'audit livre un rapport détaillé pour mettre en évidence les écarts et les non-conformités trouvés. Un plan d'action contenant les mesures à mettre en œuvre par priorité est établi, partagé et validé par l'organisme audité

2.5.1. Audit de sécurité de système d'information

L'audit de sécurité du système d'information représente une vue à un instant précis de tout ou partie du système d'information (SI), permettant de comparer l'état du SI à un référentiel existant. L'audit répertorie d'une part les points forts, mais surtout les points faibles (vulnérabilités) de tout ou partie du système, l'auditeur détermine ainsi une série de recommandations pour supprimer les vulnérabilités découvertes. L'audit est généralement réalisé conjointement à une analyse de risques, et par rapport au référentiel. Le référentiel est généralement constitué de :

- La politique de sécurité du système d'information (nommée PSSI) ;
- La base documentaire du SI ;
- La réglementation propre à l'entreprise selon son domaine d'activité ;
- Les textes de loi ;
- Les documents de référence dans le domaine de la sécurité de l'informatique.

✓ **Approche générale**

Un audit des systèmes d'information, se fait selon un schéma en trois phases :

1) Définition précise du plan de travail, récolte d'information, recherche de schématisation des processus métiers et/ou informatiques à apprécier, définition des rôles et responsabilités, analyse des forces – faiblesse ;
2) Analyse des processus importants, définition des risques, évaluation préliminaire des risques, de l'efficacité des contrôles ;
3) Tests des contrôles, un audit des systèmes d'information ne concerne pas nécessairement la sécurité. En effet, il peut servir à évaluer des aspects stratégiques ou de qualité des systèmes d'information. Par exemple, répondre à la question suivante : Est-ce que les systèmes information de l'entreprise répondent efficacement aux besoins des services métiers.

✓ **Audit de l'infrastructure informatique**

1) **Mission :**

Evaluer les risques des systèmes d'information nécessaire au fonctionnement des applications : sécurité physique, sécurité logique, sécurité des réseaux, plan de secours.

2) **Livrable :**

Rapport contenant les faiblesses relevées, leur niveau de risque et les mesures correctives proposées.

✓ **Audit d'un système**

1) **Mission :**

Assister l'équipe de projet à évaluer les risques lors des différentes étapes de réalisation d'un système / application informatique, proposer des mesures de réduction et de contrôle des risques importants et vérifier la qualité des processus de gestion des changements et de test du nouveau système / de la nouvelle application.

On distingue les contrôles applicatifs suivants :

- Création et autorisation ;
- Saisie et enregistrement des données ;
- Traitement des données ;
- Sorties des données (output) ;
- Interfaces

✓ **Audit d'une application informatique**

1) **Mission :**

Apprécier une application informatique en production, par exemple une application de gestion des salaires, une application financière, etc. Très souvent plusieurs domaines font partie d'un audit d'une application en particulier :

- Les données opérationnelles ;
- Les données de base ;
- Les paramètres ;
- Les interfaces entre application et d'autres applications ;
- La gestion des droits d'accès à l'application

Bien entendu, tout audit d'une application doit également apprécier la sécurité de l'infrastructure informatique nécessaire au fonctionnement de l'application.

2.5.2. Description des Normes ISO 2700x

L'organisation international de normalisation (ISO) a réservé la série ISO/IEC 27000 pour une plage de normes dédiée au pilotage de la sécurité de l'information, tout en s'accordant avec les normes de gestion de qualité et gestion des questions relatives à l'environnement que sont les normes ISO 9000 et ISO 14000. Appelée à devenir une référence internationale reconnue, la famille des normes ISO 27000 donne aux responsables de la sécurité des systèmes d'information, l'opportunité de mettre en œuvre un véritable système de management de la sécurité de l'information.

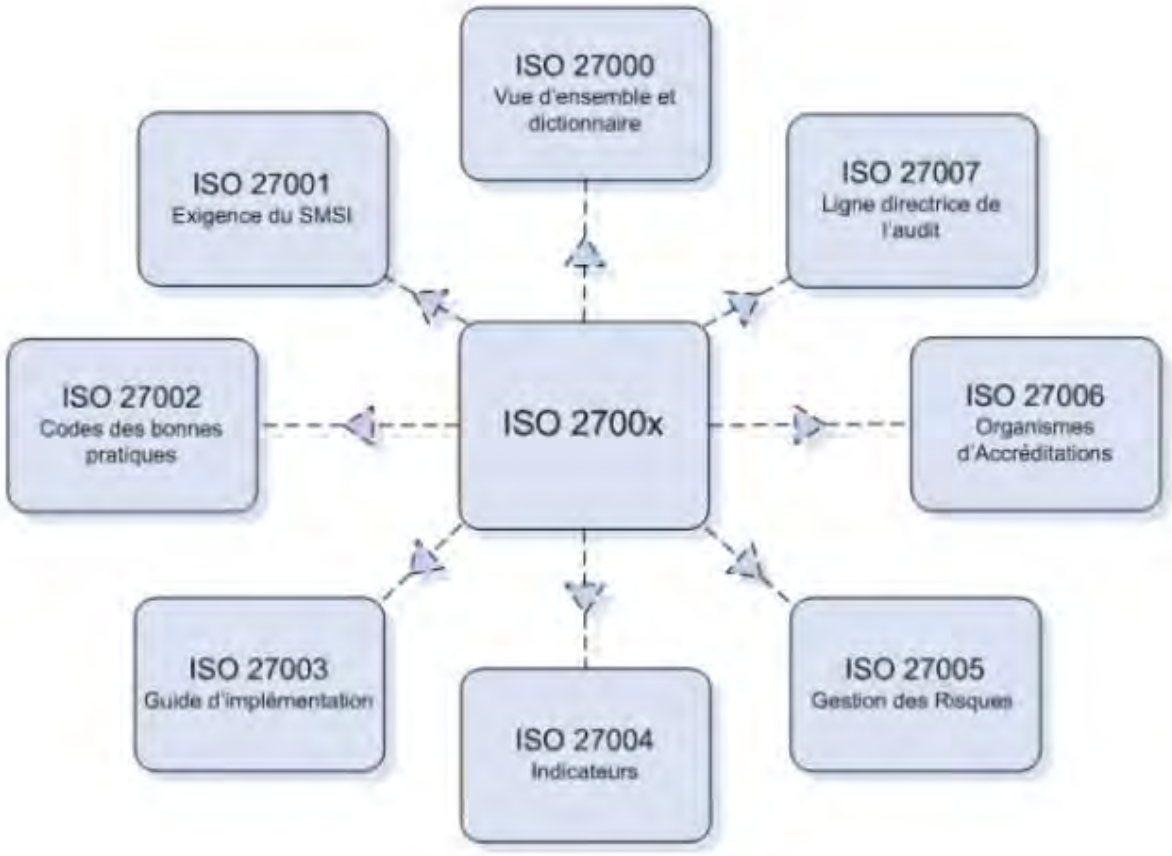


Figure 6: Famille ISO 2700x

Elle porte essentiellement sur les questions de sécurité de l'information, chaque norme porte sur les aspects précis suivants de la sécurité de l'information :

- ISO 27001 : la norme définit les exigences de sécurité d'un système de management de la sécurité (SMSI) ;

- ISO 27002 : la norme propose un code de bonne pratiques pour la gestion de la sécurité de l'information ;
- ISO 27003 : des lignes directrices pour la mise en œuvre et l'implémentation d'un système de management de la sécurité de l'information (SMSI) ;
- ISO 27004 : des métriques du management de la sécurité de l'information est traitée dans cette norme ;
- ISO 27005 : la gestion du risque en matière de sécurité de l'information est traitée dans cette norme ;
- ISO 27006 : les exigences pour les organismes auditant et certifiant un SMSI font l'objet de cette norme ;
- ISO 27007 : les directrices concernant le processus d'audit d'un SMSI se trouve dans cette norme.

2.5.3. Cycle de vie d'un audit de sécurité des systèmes d'information

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie qui est schématisé à l'aide de la figure suivante.

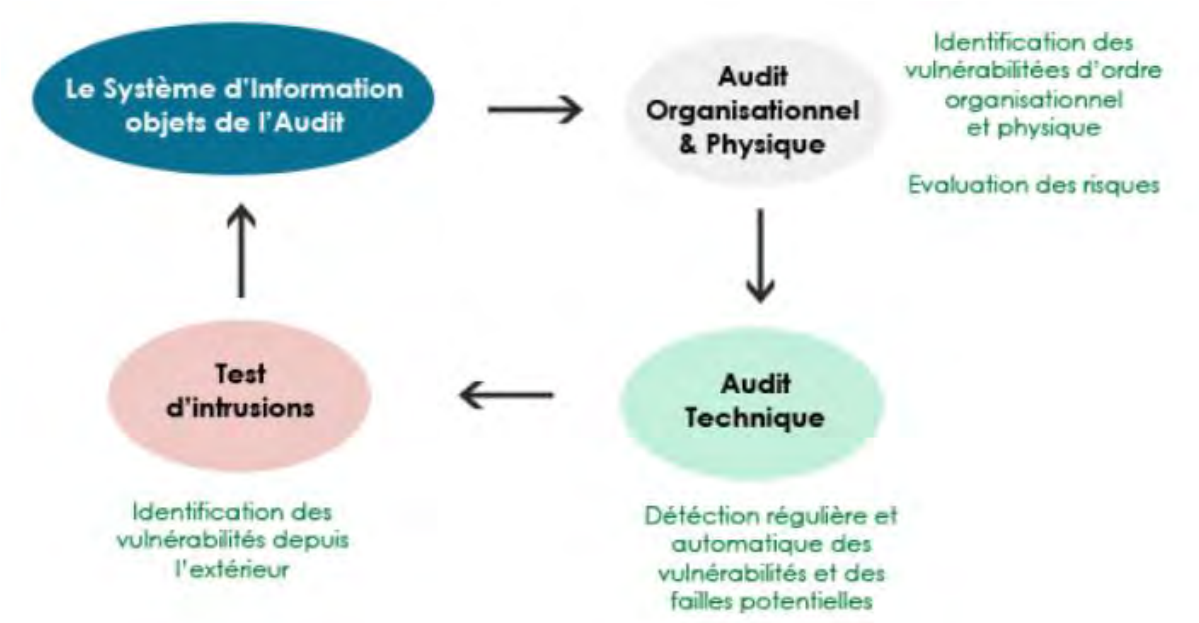


Figure 7: Cycle de vie d'un audit

L'audit de sécurité informatique se présente essentiellement suivant deux parties comme le présente la figure précédente :

- L'audit organisationnel et physique

- L'audit technique

Une troisième partie optionnelle peut être également considérée. Il s'agit de l'audit Intrusif (test d'intrusions). Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit. Il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées.

2.6. Les terminologies et les types d'attaques

2.6.1. Présentation des terminologies

- **Menace :** une menace désigne un élément, généralement externe, capable de montrer une attaque exploitant une vulnérabilité ou une faille de sécurité au niveau des services, application et des systèmes informatiques ;
- **Vulnérabilité :** toute faiblesse des ressources informatiques qui peuvent être exploitée par des menaces dans le but de les compromettre ;
- **Exploit :** un exploit est un programme permettant d'exploiter une faille de sécurité informatique dans un système qui se soit à distance (remote exploit) ou sur la machine sur laquelle cet exploit est exécuté (local exploit) ;
- **Impact :** l'impact ou enjeu est le résultat de l'exploitation d'une vulnérabilité par une menace ;
- **Risque :** le risque de sécurité, des systèmes d'information peut être défini comme étant une combinaison d'une menace avec les pertes qu'elle peut engendrer.

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Sur internet les attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques. Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives. Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système ;

- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Glaner des informations personnelles sur un utilisateur ;
- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise, utilisateur, etc.) ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.6.2. Les types d'attaques

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau. Les attaques peuvent intervenir à chaque maillon de cette chaine, pour peu qu'il existe une vulnérabilité exploitable.

1) **Attaque par force brute :** on appelle ainsi « attaque par force brute » (en anglais « brute force cracking », parfois également attaque exhaustive) le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.
2) **Attaques par dictionnaire :** les outils d'attaque par brute force peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « attaque par dictionnaire ». En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut-être craquer en quelques minutes.
3) **Attaque hybride :** le dernier type d'attaque de ce type, appelées « attaque hybride », vise particulièrement les mots de passe constitué d'un mot traductionnel et suivi d'une lettre ou d'un chiffre. Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire. Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs : les key loggers (littéralement enregistrement de touches), sont

des logiciels qui, lorsqu'ils sont installés sur un poste de l'utilisateur, permettent enregistrer les frappes de claviers saisies par l'utilisateur. Les système d'exploitation récents possèdent des mémoires tampon protégées permettant de retenir temporairement le mot de passe et accessible uniquement par le système. L'ingénieur social consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence, l'espionnage représente la plus veille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

4) **Attaque man in the middle :** l'attaque « man in the middle » (attaque de l'homme du milieu) parfois notée MITM est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. La plupart des attaques de type man in the middle consistent à écouter le réseau à l'aide d'un outil appelé sniffer.
5) **Attaque DoS :** une attaque par déni de service (en anglais Denial of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés. Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information. On distingue habituellement deux types de dénis de service :
   - **Les dénis de service par saturation,** consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles
   - **Les dénis de service par exploitation de vulnérabilités,** consistant à exploiter une faille du système distant afin de le rendre inutilisable.

   Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution, inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services

réseau qu'elles proposent. Lorsqu'un déni de service est provoqué par plusieurs machines, on parle de **déni de service distribué (DDOS),** les attaques par déni de service distribué les plus connues sont : **Tribal Flood Network** et **Trinoo.**

6) **Attaque SYN :** l'attaque SYN appelée également **TCP/SYN Flooding** est une attaque réseau par saturation (déni de service) exploitant le mécanisme de poignée de main en trois temps (en anglais Three-ways handshake) du protocole TCP. Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à internet (utilisant le protocole TCP) s'effectue : lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet SYN/ACK et enfin le client valide la connexion par un paquet ACK (acknowledgement, qui signifie accord ou remerciement). Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchises. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet ACK. Les machines vulnérables aux attaque SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet ACK. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquet SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage de la machine.
7) **L'usurpation d'adresse IP ;** l'usurpation d'adresse IP (en anglais spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis. Ainsi, certains tendent à assimiler l'utilisation d'un proxy (permettant de masquer d'une certaine façon l'adresse IP) avec du spoofing IP. Toutefois, le proxy ne fait que relayer les paquets. Ainsi, même si l'adresse est apparemment masquée, un pirate peut facilement être retrouvé grâce au fichier de logs (journal) du proxy.
8) **Le vol de session TCP :** le vol de session TCP (en anglais TCP session hijacking) est une technique consistant à intercepter une session TCP initiée entre deux machine afin de la détourné. Dans la mesure où le contrôle d'authentification s'effectue uniquement

à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

Partie II : Etude Conceptuelle

Chapitre 3 : cadre management et organisationnelle d'un CERT

3.1 Qu'est-ce qu'un CSIRT

L'acronyme CSIRT qui signifie Computer Security Incident Response Team, est principalement utilisé comme synonyme du terme protégé CERT (Computer Emergency Response Team), déposé aux Etats-Unis par CERT Coordinateur Center (CERT/CC). La première apparition d'un ver dans l'infrastructure informatique mondiale remonte à la fin des années 1980 avec Morris, qui s'est rapidement propagé pour contaminer de très nombreux systèmes IT dans le monde entier.

Cet incident a été un véritable signal d'alarme, dans la mesure où il a fait prendre conscience de la nécessité impérative d'une coopération et d'une coordination au niveau des administrateurs systèmes et des responsables informatiques pour lutter contre ce type de phénomène. Le temps étant un facteur critique, il convenait d'adopter une approche davantage organisée et structurée de la gestion des incidents de sécurité informatique. Aussi, quelques jours à peine après « l'incident de Morris », l'DARPA (Defense Advanced Research Projects Agency) créait-elle le premier CSIRT, en l'occurrence CERT, implanté à la Carnegie Mellon University de Pittsburgh (Pennsylvanie).

Un CSIRT est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La plupart des CSIRT offrent également à leurs parties prenantes, dans le but d'atténuer les risques et de minimiser le nombre d'interventions requises, des services à caractère préventif et éducatif. Ils publient des bulletins et avis de vulnérabilités concernant les logiciels et matériels en usage, et informent les utilisateurs des exploits et virus tirant parti des failles constatées. Les parties prenantes sont dès lors en mesure de procéder rapidement à l'application de correctifs et à la mise à jour de leurs systèmes.

- **Les avantages d'un CSIRT**

Disposer d'une équipe spécialisée en sécurité informatique aide toute entreprise à réduire, voire à prévenir, les incidents majeurs et à protéger un patrimoine précieux.

Le CSIRT peut offrir en autre les avantages suivants

- La centralisation de la coordination en matière de sécurité informatique au sein de l'entreprise ;
- La centralisation et la spécialisation du traitement et de la réponse aux incidents informatiques ;
- La disponibilité d'une expertise permettant de soutenir les utilisateurs et de les aider à la restauration de leurs systèmes après un incident de sécurité ;
- La gestion des aspects juridiques et la protection des preuves en cas d'action en justice ;
- Le suivi des évolutions dans le domaine de la sécurité ;
- La sensibilisation des parties prenantes en matière de sécurité informatique

- **Les services d'un CSIRT**

Un CSIRT peut proposer un très large éventail de services, mais aucun CSIRT n'en propose actuellement la gamme complète. La sélection des services les mieux adaptés apparaît donc comme une décision essentielle.

Services réactifs	Services proactifs	Traitement des artefacts
Alertes et avertissements Traitement des incidents Analyse des incidents Appui à la réponse aux incidents Coordination de la réponse aux incidents Traitement des vulnérabilités Analyse des vulnérabilités Réponse aux vulnérabilités Coordination des réponses aux vulnérabilités	Veille technologique Audits ou évaluations de la sécurité Configuration et maintenance de la sécurité Développement des outils de sécurité Services de détection des intrusions Diffusion d'information relatives à la sécurité	Analyse des artefacts Réponse aux artefacts Coordination des réponses aux artefacts

Tableau 1: Les services d'un CSIRT

3.2 Types et rôle d'un CSIRT

✓ Types

Il existe trois (3) principaux types de CSIRT à savoir :

- Public
  - CSIRT Gouvernemental : en charge des institutions gouvernementales
  - CSIRT d'Infrastructure Critique : en charge des infrastructure critique
  - CSIRT National : en charge de tous les intérêts de la nation (institution, gouvernementales, grand public, entreprises …)
- Public-Privé
  - CSIRT Sectoriel : en charge d'un secteur d'activité (défense, santé…)
  - CSIRT Universitaire : en charge d'un réseau universitaire
- ✓ Privé :
  - CSIRT Sectoriel : en charge d'un secteur d'activité (finance, énergie…)
  - CSIRT Privé : en charge de la réponse à incident pour une entreprise privée

✓ Rôle

Dans le processus d'identification et gestion des incidents, les équipe de réponse aux incidents de sécurité informatique (CSIRT) jouent un rôle d'assistance auprès des victimes. Grâce à leur expérience et à leur savoir-faire, elles sont en mesures aider les personnes ou les organisations en difficulté, de manière efficace, rapide et à bas coût. Un CSIRT aide les organisations à juguler et à réparer les failles de sécurité et les menaces informatique. Cette fonction réactive est appelée gestion des incidents. En général, elle comprend trois aspects principaux :

1. La fonction « signalement des incidents » (incident reporting) qui permet à un CSRIT de servir de point de contact centralisé pour signaler des problèmes locaux. Tous les rapports d'incident sont collectés dans un lieu unique où l'information peut être analysée ;
2. La fonction « analyse de l'incident » (incident analysis) cette fonction est utilisée pour déterminer les tendances et modes intrusion et pour recommander des stratégies de prévention adaptées à l'organisation. Une analyse de l'incident implique également une étude en profondeur du rapport ou de l'activité d'incident afin d'en déterminer la portée, la priorité et la menace, ainsi que la recherche de réponse possibles et de stratégies d'atténuation ;

3. La fonction « réponse aux incident » (incident response) qui peut prendre leurs formes. Un CSIRT peut envoyer des recommandations pour la récupération, le confinement ou la prévention à l'organisation ou effectuer ces étapes lui-même.

Un autre rôle des CSIRT dans le processus de gestion des incidents consiste à collecter des informations sur les incidents afin d'établir des statistiques permettant d'avoir une vue complète sur la cybersécurité et de prendre les décisions politiques adaptées.

3.3 Gestion des incidents en cybersécurité

Comme illustré dans la norme de gestion des incidents de sécurité de l'information ISO 27035, la chaine d'incident de cybersécurité se présente comme suit ;

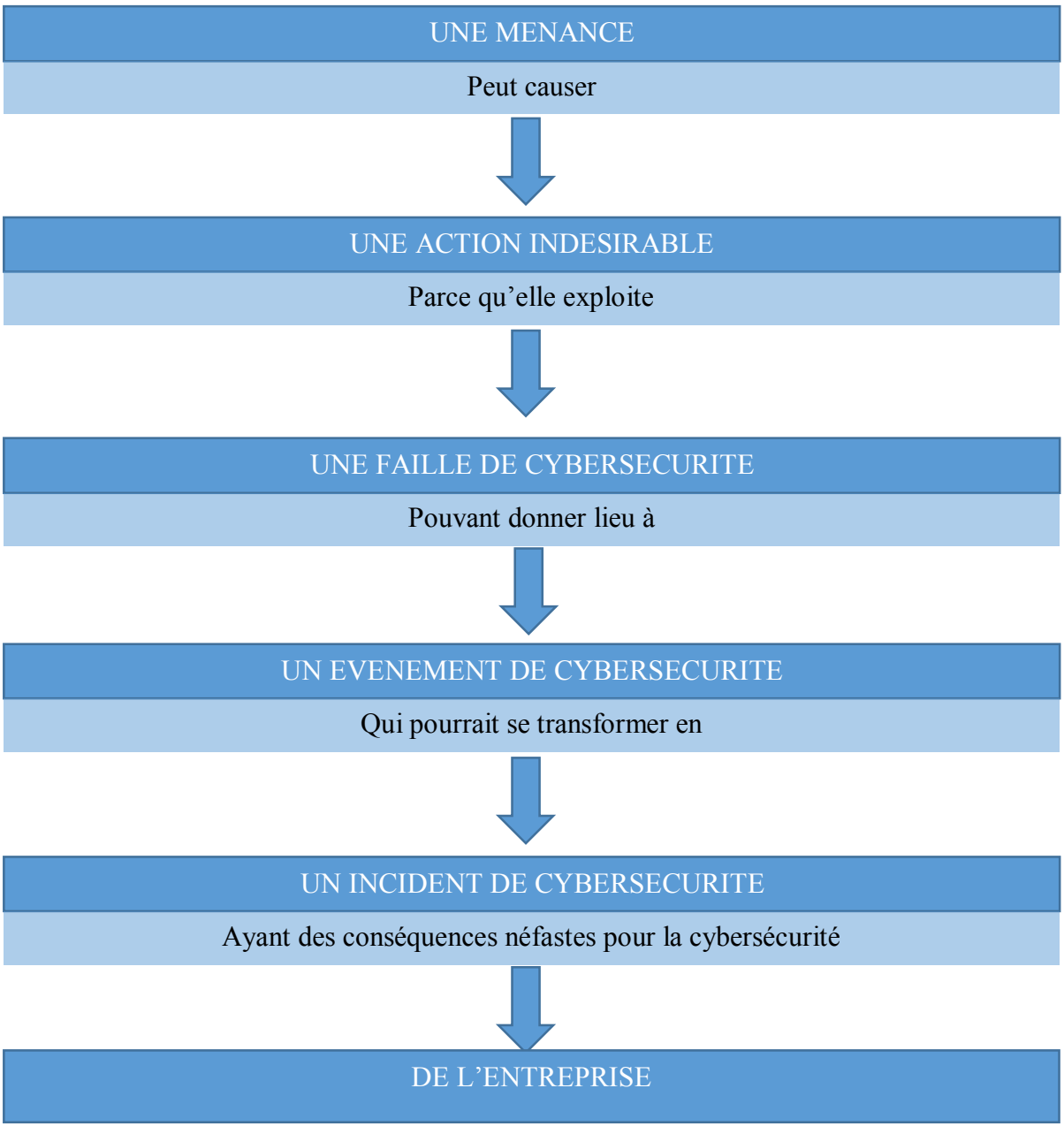


Figure 8:chaine d'incident de cybersécurité

- ✓ **Faille de cybersécurité :**

C'est une vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.

- ✓ **Evénement de cybersécurité :**

C'est l'occurrence identifiée de l'état d'un service, d'un système ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

- ✓ **Incident de cybersécurité :**

Un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'entreprise et de menacer la sécurité de l'information. De ce fait, il a des impacts sur l'un des critères de la sécurité : Confidentialité, Intégrité, Disponibilité, Authentification.

La gestion d'un incident de sécurité ne s'improvise pas. Il est donc important de procéder de façon structurée afin de concilier efficacité et rapidité, tout en conservant une démarche d'amélioration continue.

Comme les atteintes à la sécurité sont de plus en plus sophistiquées, il est estimé qu'un nombre important des incidents demeure non décelé. Ceci est dû, d'une part, à l'absence de déploiement de méthodes de prévention avérées et moyens de détection et de contrôle en matière de cybersécurité, et d'autres part, au manque de compétences techniques.

Ainsi ; planifier et préparer une politique et un plan de gestion d'incident de cybersécurité s'avère indispensable pour une détection et une réponse efficaces aux incidents. La politique de gestion des incidents de cybersécurité doit fournir les principales démarches formellement documentées pour assurer une mise en œuvre cohérente et appropriée des processus et procédures. Elle doit faire partie de la stratégie de sécurité de l'information de chaque entité et doit être conforme à la politique et aux procédures appliquées par l'entreprise.

Pendant la phase de préparation, chaque entreprise vise également à limiter le nombre d'incidents qui pourraient se produire en sélectionnant et en mettant en œuvre un ensemble de contrôles et mesures basés sur les résultats des évaluations des risques. Le but est d'être en

mesure de prévenir les incidents tout en gardant les systèmes, les réseaux et les applications suffisamment sécurisés.

Par ailleurs, garder le nombre d'incidents raisonnablement bas est très important pour protéger les processus métiers de l'entreprise. Si les contrôles de sécurité sont insuffisants, un nombre important et élevé d'incident peuvent se produire, mettant à mal l'équipe de réponse aux incidents. Cela peut conduire à des réponses lentes et incomplètes, qui se traduisent par un impact négatif plus important. Bien que les équipes de réponse aux incidents ne soient généralement pas responsables de la sécurisation des ressources, elles peuvent émettre et faire valoir les bonnes pratiques de sécurité suite à l'identification des défaillances et des problèmes que l'entreprise ignore.

3.4 Détecter et identifier les incidents en cybersécurité

La phase de détection consiste à déceler un événement susceptible de constituer un incident de cybersécurité et d'en informer les responsables des systèmes touchés et de déclencher le processus de réponse à l'incident

De façon générale, lors de la phase de détection l'entreprise doit entreprendre les actions clés suivantes :

- Journaliser l'activité système et réseau de l'entreprise ;
- Collecter des informations permettant d'assurer une connaissance de la situation à partir de source de données internes et externes ;
- Disposer des outils de détection et les configurer selon les risques et menaces qui pèsent sur l'entreprise ;
- Assurer un suivi et monitoring permanent par l'équipe de sécurité ;
- Détecter et signaler l'occurrence d'un événement de sécurité de l'information ou l'existence d'une vulnérabilité, que ce soit manuellement ou automatiquement ;
- Surveiller les alertes transmises par les systèmes de sécurité internes ;
- Surveiller l'information communiquée et les alertes diffusées par les organismes spécialisés dans la détection des incidents de cybersécurité et la réponse aux attaques informatique ;

Pour pouvoir mette en place les recommandations susvisées et réussir la phase de détection, il est primordial pour chaque entreprise de comprendre les signes d'un incident et pouvoir les

collecter à partir des différentes sources disponibles au sein de l'entreprise en fonction de son secteur d'activité.

La phase d'identification repose sur l'évaluation des événements de cybersécurité décelés pendant la phase de détection. Cette évaluation vise à déterminer s'il s'agit réellement d'un incident de cybersécurité, de déterminer son incidence et son envergure, son impact ainsi que la cause probable de l'incident. Les tâches à accomplir lors de cette phase se présentent comme suit :

- Evaluer l'événement et confirmer qu'il s'agit d'un incident ;
- Désigner les personnes responsables de l'incident ;
- Déterminer le type de l'incident ;
- Déterminer le vecteur d'attaque susceptible ;
- Déterminer les données, systèmes ou réseaux touchés ;
- Cerner l'impact sur la confidentialité, l'intégrité et la disponibilité ;
- Aviser les personnes compétentes

3.5 Réponse aux incidents en cybersécurité

Conformément aux actions menées durant la phase de détection et d'identification, cette étape consiste à apporter les réponses adéquates aux incidents de cybersécurité détectés. Une fois qu'un incident de cybersécurité est confirmé, les activités suivantes doivent être exécutées :

- Attribuer les responsabilités et les rôles aux différents membres de l'équipe d'intervention interne ou externe ou mixte ;
- Elaborer des procédures formelles à suivre pour chaque personne impliquée dans l'incident ;

La première phase d'une réponse à incident est l'acquisition des preuves de compromission. Les analystes doivent reconstituer le scénario complet d'attaque (Exploitation d'une vulnérabilité, élévation de privilèges, exfiltration de données …). Les évidences collectées doivent être stockées en toute sécurité. L'acquisition des données peut se faire :

- ✓ **À chaud :** sur un système en marche (on parle de « live forensics ») la réponse à chaud permet de mener des investigations en collectant des « artefacts » sur des systèmes en marche. A ce stade, les détails de la menace sont toujours inconnus, il faut donc commencer par identifier et quantifier la menace à travers la collecte des informations à savoir :

- La mémoire volatile ;
- Les « prefetch files » ;
- Les clés de registre ;
- Les connexions réseau ouvertes ;
- Les comptes système :
- Etc

✓ **À froid :** sur un système éteint cette manière d'acquisition des évidences est très couteuse en termes de temps. Elle repose sur la création d'une image du disque authentique à celle utilisé par le système compromis. Cette action est primordiale dans le cas où on est sûr que la machine cible est compromise.

Après analyse des informations relatives à l'incident, il faut lancer la procédure de restauration et d'éradication qui consiste à

- Supprimer tous les éléments et évidences associés à l'incident :
- Corriger toutes les vulnérabilités exploitées par l'attaquant :
- Restaurer à partir d'une sauvegarde saine ou réinstaller le système en entier :
- Déterminer la source du problème pour sécuriser d'avantage

Après le traitement d'un incident, un rapport de synthèse des résultats de l'investigation doit être rédigé et doit être communiqué à toutes les parties concernées.

3.6 La communication des incidents en cybersécurité

La gestion des incidents de cybersécurité nécessite une coordination minutieuse au sein de l'équipe de réponse, mais également avec diverses parties prenantes internes autant qu'externes. Un plan de communication dédie est alors essentiel : il fournit conseils et orientation à ces efforts de communication. Comme pour les éléments du plan de réponse à incident, il est nécessaire d'élaborer le plan de communication au préalable pour assurer une prise de décision saine et sereine, malgré la forte pression qui s'exerce inéluctablement sur les équipes dans un contexte de crise.

3.7 Suivi et clôture des incidents en cybersécurité

Après le traitement d'un incident, l'entreprise doit passer en revue l'ensemble des décisions prises et les étapes suivies tout au long du cycle de traitement de l'incident afin de déterminer les points à l'égard desquels des améliorations devraient être apportées.

En outre, des réunions périodiques doivent être programmées pour identifier et corriger les faiblesses systémiques et les lacunes identifiées dans les politiques et les procédures adoptées. Enfin, les rapports de suivi pour chaque incident résolu doivent être exploités pour mieux traiter les futurs incidents et utilisés comme cas d'études dans la formation des nouvelles recrues.

Chapitre 4 : Etude de solutions

4.1. Sonde d'analyse détaillée de trafic réseau NetFlow :

Toutes les informations concernant le réseau sont importantes pour gérer et mesurer la bande de passante (le volume de données pouvant être transmis sur une période donnée) et il est essentiel d'assurer la disponibilité de la bande passante pour garantir la prestation de services.

L'analyse du trafic réseau peut présenter de nombreux avantages. Elle permet d'identifier les goulots d'étranglement du réseau résultant d'une capacité insuffisante de traitement des données pour gérer le volume du trafic en transit. Elle peut également vous permettre d'identifier les utilisateurs ou applications les plus bavards sur le réseau. Cette analyse présente des avantages en terme de sécurité, car l'augmentation injustifiée du volume de trafic peut indiquer une cyberattaque.

NetFlow est un protocole réseau utilisé pour comptabiliser le trafic du réseau IP. Il a été développé par Cisco Systems. De nos jours, NetFlow est devenu une norme industrielle pris en charge par de nombreux périphériques. Il existe plusieurs versions du protocole, mais les versions les plus courantes sont les versions 5 et 9. NetFlow utilise le concept d'un flux pour capturer des données sur le comportement du réseau, telles que la source et la destination du trafic réseau, les applications utilisant le réseau et la quantité de bande passante allouée à ces applications.

Un flux est une séquence unidirectionnelle de paquets entre une source et une destination donnée, définie par une clé de 7-tuple comprenant les champs suivants :

- Adresse IP source
- Adresse IP de destination
- Source Port
- Le port de destination
- Protocole IP
- Interface de saisie
- Type de service IP

Les informations NetFlow collectées par Flow Publisher sont gérées en créant des enregistrements pour chaque flux. Chaque enregistrement est géré dans le cache NetFlow. Lorsque les paquets sont capturés, les statistiques relatives aux flux actifs sont mises à jour.

Une fois qu'un flux a été créé et placé dans le cache NetFlow, il reste actif jusqu'à ce qu'il expire. Une fois l'écoulement écoulé, l'enregistrement de flux est ajouté à un datagramme d'exportation NetFlow pour transmission au collecteur NetFlow.

Nous allons faire une étude comparative entre le NetFlow Analyzer de **ManageEngine** et le Nagios Network analyzer pour pouvoir implémenter la meilleure solution et avoir une analyse détaillée de notre réseau. Afin de détecter une attaque via une montée de charge anormale du trafic réseau.

4.1.1. NetFlow Analyzer

NetFlow Analyzer, outil d'analyse de trafic complet, exploite les technologies de flux pour assurer un suivi en temps réel de la performance de la bande de passante réseau. NetFlow Analyzer est à l'origine un outil d'analyse de la bande passante. Il est une solution unifiée qui collecte, analyse et affiche les détails d'utilisation de la bande passante réseau (objet et utilisateur).

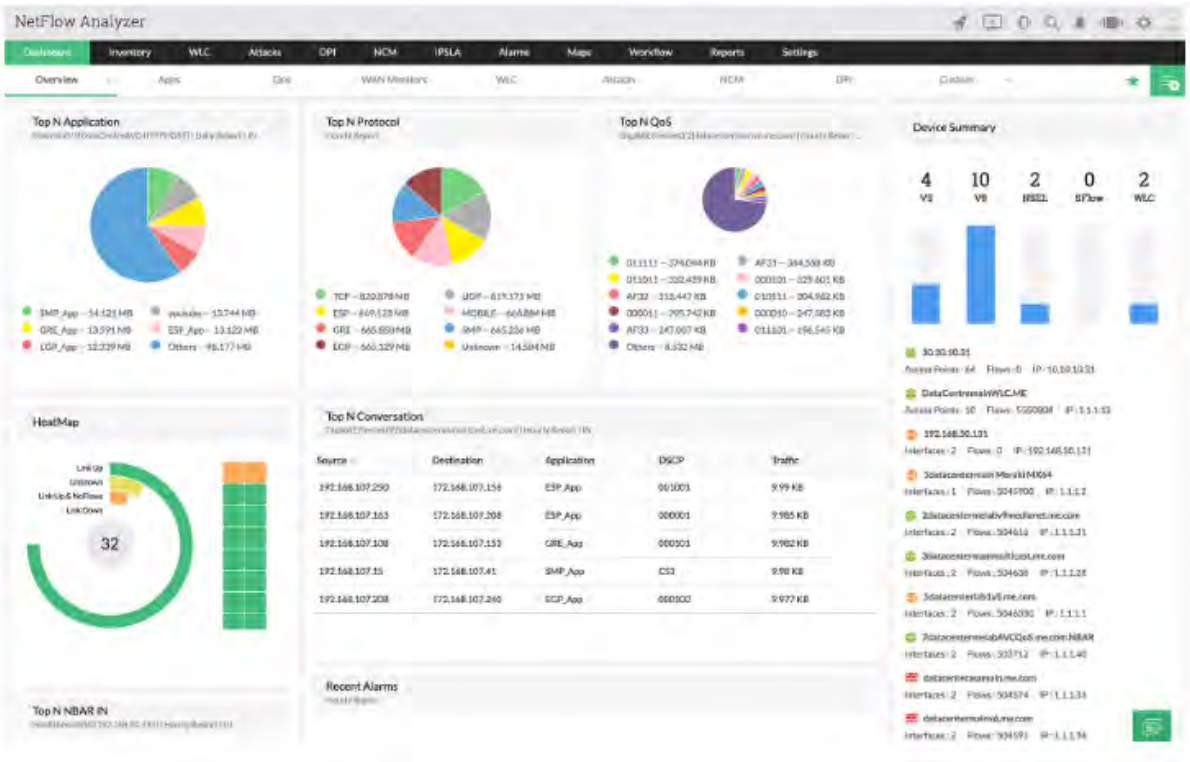


Figure 9: Tableau de bord NetFlow Analyzer

Les fonctionnalités de NetFlow analyzer :

- ✓ **Suivi de la bande passante et analyse du trafic**
- Analyser la bande passante du réseau et les tendances du trafic à un niveau interface ;

- Zoomer sur les détails au niveau interface pour découvrir les tendances du trafic et la performance des périphériques ;
- Obtenir un aperçu en temps réel de la bande passante du réseau avec des rapports de granularité instantanés.

✓ **Audit réseau et analyse de la sécurité**

- Détecter une vaste gamme de menaces de sécurité externes et internes avec une technologie de moteur d'exploration en flux continu ;
- Suivre les anomalies réseau qui échappent au pare-feu :
- Identifier des anomalies contextuelles et des intrusions zero-day

✓ **Analyse orientée application et forme du trafic**

- Identifier et classifier les applications non standards qui monopolisent la bande passante du réseau ;
- Reconfigurer des stratégies avec une technologie de mise en forme du trafic via ACL ou une stratégie basée sur la classe pour maîtriser les applications gourmandes en bande passante ;
- NetFlow analyzer exploite le moteur Cisco NBAR pour assurer un suivi précis du trafic de couche 7 et identifier les applications utilisant des numéros de port dynamiques ou se masquant derrière des ports connus.

✓ **Planification de capacité et facturation**

- Prendre des décisions éclairées quant à la croissance de la bande passante avec les rapports de planification de capacité ;
- Mesurer la croissance de la bande passante sur une période avec des rapports à long terme ;
- Déterminer la tendance exacte sur de longues périodes passées ;
- Générer des factures à la demande pour la comptabilité et la rétro facturation aux services.

✓ **Analyse efficace du trafic voix, vidéo et données**

- Analyser les niveaux de service IP pour les applications et les services réseau grâce à l'analyseur IP SLA ;
- Garantisse des niveaux élevés de qualité de communication données et voix avec la technologies Cisco IP SLA ;
- Surveillez des indicateurs de performance clés du trafic voix et données.

✓ **Technologie de flux hétérogène**

- Collecte et analyse les flux des principaux périphériques de grands fournisseurs comme Cisco, 3COM, Juniper, Foundry Network, Hewlett-Packard, Extreme et autres ;
- Suive tous les formats de flux répandus comme NetFlow, sFlow, cflow, FNF, IPFIX, NetStream, Appflow, etc.

4.1.2. Nagios Network Analyzer :

Nagios, avec Network Analyzer, propose une solution dédiée à l'analyse et la surveillance de l'utilisation de la bande passante.

En complément de Nagios XI avec qui elle s'intègre parfaitement, la solution Network Analyzer vient fournir un aperçu approfondi de toutes les sources de trafic réseau et des menaces potentielles pour la sécurité.

Network Analyzer permet une visualisation avancée fournit des informations rapides et approfondies sur le trafic, la bande passante et l'état général du réseau. Il est capable d'alerter les utilisateurs lorsqu'une activité suspecte a lieu sur le réseau. Il met à votre disposition des requêtes, des vues et des rapports personnalisables vous permettent de surveiller l'utilisation du réseau pour des applications spécifiques. Une intégration avec Nagios XI pour voir les rapports de l'analyseur de réseau et qui communique avec n'importe quel serveur de votre réseau depuis le système XI.

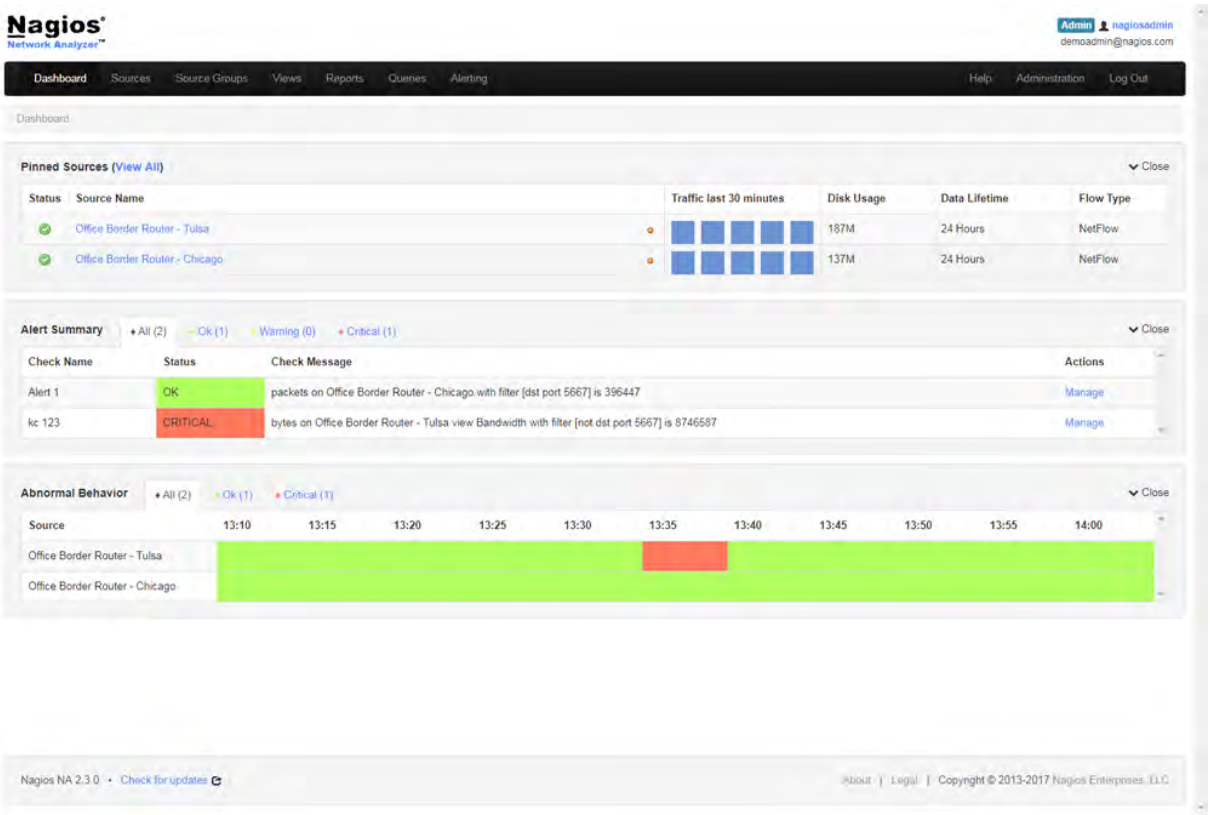


Figure 10: Tableau de bord Network Analyzer

Les fonctionnalités de Nagios Network Analyzer :

- ✓ **Analyse approfondie du réseau :** Network Analyzer fournit un examen approfondi de toutes les sources de trafic réseau et des menaces de sécurité potentielles, permettant aux administrateurs système de collecter rapidement des informations de haut niveau sur la santé du réseau ainsi que des données hautement granulaires pour une analyse complète et approfondie du réseau.
- ✓ **Une vue sur le réseau :** Network Analyzer fournit une vue centrale de votre trafic réseau et de vos données de bande passante ainsi que des éventuels compromis réseau. Le puissant tableau de bord offre une vue d'ensemble des sources de données critiques NetFlow ou sFlow, des mesures du système serveur et du comportement anormal du réseau pour une évaluation rapide de l'état du réseau. Les utilisateurs peuvent facilement explorer pour voir des informations spécifiques sur les adresses IP, le port source et port de destination.
- ✓ **Adaptabilité :** Créez un environnement Network Analyzer qui reflète l'identité de votre réseau. Les groupes de sources permettent aux administrateurs d'organiser des sources similaires et d'appliquer des vues et des requêtes à plusieurs sources simultanément et

selon vos spécifications exactes. Des fonctionnalités complémentaires supplémentaires permettent aux utilisateurs de Network Analyzer de transmettre des notifications SNMP aux systèmes de surveillance et de gestion des interruptions SNMP. Network Analyzer s'adapte à votre environnement existant pour un processus de mise en œuvre sans douleur qui ne prend que quelques minutes pour être opérationnel.

- ✓ **Conception intuitive :** Avec une interface Web puissante et intuitive, Network Analyzer est facile à utiliser, tout en offrant des performances et une vitesse optimale. Network Analyzer s'intègre de manière transparente à la solution de surveillance de réseau, Nagios XI, permettant la consolidation des alertes et des notifications ainsi que le maintien d'un réseau sûr et sécurisé. Configurez facilement des alertes et ajoutez des sources avec les assistants intuitifs de Network Analyzer en quelques clics.
- ✓ **Aperçu détaillé :** Les capacités avancées d'alerte et de reporting de Network Analyzer fournissent au personnel informatique une meilleure connaissance de leur réseau. Des données hautement granulaires et actualisées peuvent être consultées et archivées pour un suivi et une analyse plus poussés. Lorsque les seuils critiques sont dépassés, qu'une activité réseau anormale se produit ou que les restrictions de bande passante sont respectées, Network Analyzer peut déclencher des alertes permettant aux administrateurs de commencer à résoudre les problèmes immédiatement.
- ✓ **Calculateur d'utilisation de la bande passante :** Un calculateur d'utilisation de la bande passante entièrement personnalisable est inclus, permettant de créer des rapports pour résumer l'utilisation de la bande passante par source, IP ou toute combinaison souhaitée par l'utilisateur.

4.1.3. Tableau comparatif :

	NetFlow Analyzer	Nagios Network Analyzer
Tableau de bord		
Alertes et remontée des problèmes		
Alertes/Notification		
Rapport		
Licence	Payante	Payante
Analyse Trafic sans fil		
Plateforme	Windows	Cloud/Windows/linux
Intégration à un AD		
Analyse du Trafic du système autonome		
Support client	Support en horaire de bureau	Service de support permanent

Tableau 2:Comparatif entre NetFlow Analyzer et NetFlow Traffic Analyzer

En se basant sur nos critères de comparaison, on voit que Nagios Network Analyzer répond à tous les critères donc sera choisi pour l'implémentation de notre solution d'analyse détaillée de trafic réseau.

4.2. Découverte et mesure de la disponibilité des services du réseau (NMS)

Un NMS (Network Management System) est un système de gestion de réseau et plus globalement des systèmes d'information. Le NMS permet de superviser l'activité du réseau ainsi que les serveurs et les applicatifs.

Parmi les fonctionnalités qu'offre un NMS on retrouve :

- Supervision en temps réel du réseau : Collecte périodique de différents indicateurs (taux d'occupation disque, utilisation de la CPU, bande passante, etc.) et comparaison de leur valeur avec des seuils. Identification d'un passage de seuil et donc d'un "changement d'état" et création d'une alarme.

- Gestion de la métrologie : Stockage et indexation des valeurs d'indicateurs collectées pour l'investigation des pannes ainsi que les analyses de tendances et le "capacity planning".
- Notification : Présentation des informations de supervision de façon condensée et opérationnelle pour faciliter la prise en charge et la résolution des incidents. Mise à disposition d'outils d'investigation et de gestion des workflows de résolution.
- Cartographie : Représentation synoptique du réseau avec possibilité de navigation de cartes en sous cartes.

La supervision réseau est un ensemble de protocoles, matériels et logiciels informatiques assurant les activités suivantes : surveiller, visualiser, analyser et agir. Cette opération est assuré par l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) capable de fournir des informations sur l'état des réseaux et ses machines distantes. Il faut donc disposer d'une console de supervision qui regroupe et synthétise toutes les informations. On supervise pour avoir une visibilité sur le système d'information. Cela permet de disposer rapidement des informations, de connaître l'état de santé du réseau, des systèmes, ainsi que leurs performances. Ce qui donne rapidement une image du système étudié.

Grace à Ces informations on peut gérer de manière automatique les pannes et les problèmes de surcharge survenant sur le réseau.

✓ **Principe de supervision :**

Le suivi régulier du bon fonctionnement de l'ensemble des équipements présents sur le réseau d'une entreprise et l'optimisation permanente de ses performances sont des fonctions incontournables.

En général, La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble en temps-réel des équipements supervisés. Elle permet de visualiser à tout moment l'état des différents équipements configurés. Ainsi les objectifs sont multiples :

- Eviter les arrêts de service
- Remonter des alertes
- Détecter et prévenir les pannes

✓ **Les méthodes de supervision**

L'opération de supervision se fait selon 2 manières, la supervision active et la supervision passive :

- **La supervision active** : consiste sur le fait que l'outil de supervision décide quand il fait le test sur l'équipement à superviser. Elle se base sur l'envoi des requêtes avec différents protocoles de communications vers une destination d'un équipement pour tester sa connectivité et son bon fonctionnement.
- **La supervision passive** : c'est l'hôte qui décide quand elle renvoie ces informations vers la plate-forme de supervision. Ses informations sont de types des traps SNMP, syslogs etc., puis déclenche une action en fonction de l'analyse des informations reçues.

Dans notre cas nous allons faire une étude de deux outils de supervision que sont **Cacti** et **Nagios XI** afin de choisir la meilleure solution à mettre en œuvre dans notre projet.

4.2.1. Nagios XI :

Nagios est un logiciel permettant de superviser le système et le réseau, qui s'appuie sur 3 composants principaux : l'ordonnanceur, les plugins et l'interface web d'administration

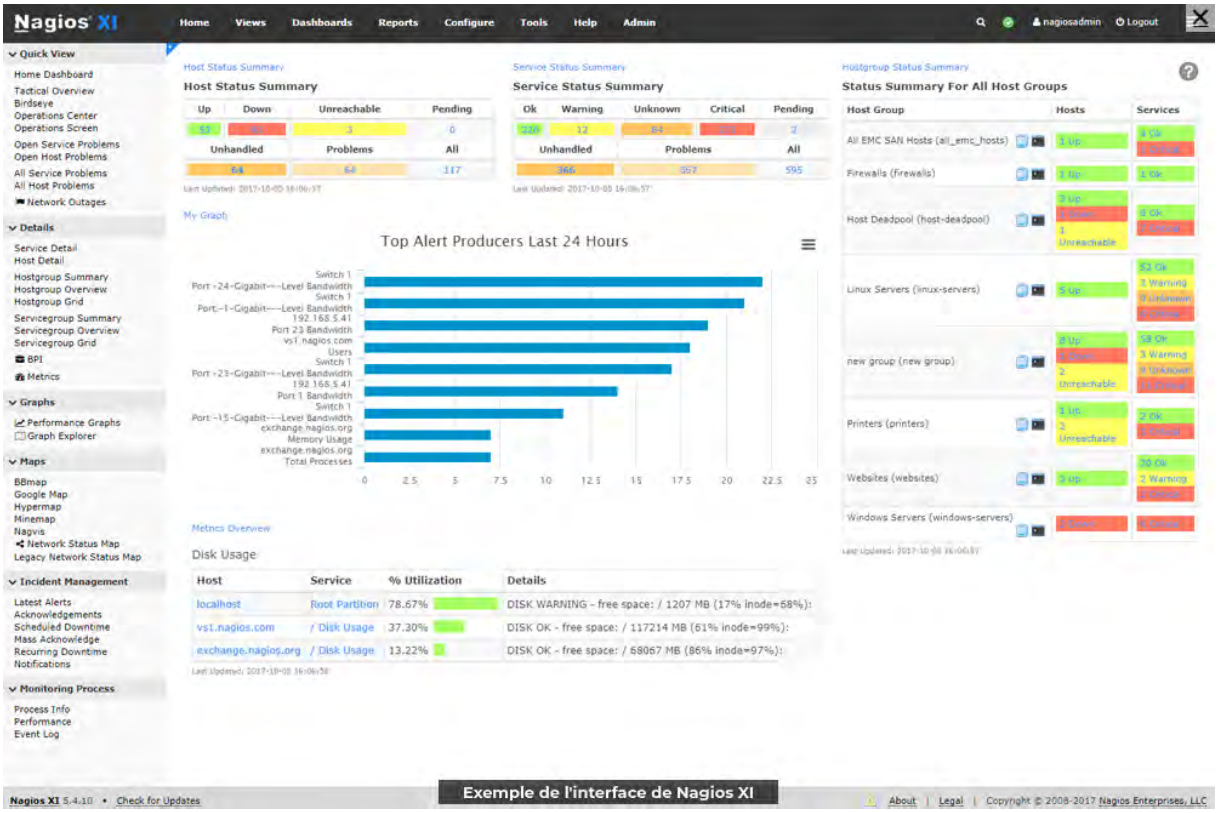


Figure 11: Interface web de Nagios IX

- ✓ **L'ordonnanceur :**

L'ordonnanceur est le cœur du programme. Il s'agit d'un processus qui se lance en tant que service système. Son mode de fonctionnement est simple mais très efficace : il paramètre des objets **host** et **service**, qui seront supervisés par l'intermédiaire d'un objet **command**. Celui-ci lancera, à intervalles réguliers et paramétrables, des sondes sous la forme de programmes exécutables. Les résultats de ces actions de supervision sont stockés dans des fichiers au format texte. Bien entendu, configurer des objets permet, entre autre, de :

- observer le temps entre chaque exécution de la sonde ;
- définir des seuils permettant de juger les résultats (aussi appelés « statuts », **OK**, **WARNING** ou **CRITICAL**, par exemple pour les objets de type service) ;
- gérer efficacement les notifications vers les acteurs responsables de la maintenance de ces objets ;
- indiquer un minimum de topologie concernant le schéma d'architecture réseau ;
- déclencher des actions particulières sur certains statuts ;

✓ **Les plugins :**

Les plugins (aussi appelés « sondes ») sont des programmes qui fonctionnent de manière autonome et servent à superviser les caractéristiques des objets configurés. Parmi ces caractéristiques, on peut notamment citer la charge CPU, l'occupation de la mémoire ou du disque, les services HTTP, SSH, FTP, SNMP, PING, WMI, POP3, et beaucoup d'autres encore. Les plugins Nagios étant normalisés et très bien documentés, il est possible de coder soi-même un plugin spécifique à son besoin.

✓ **L'interface Web d'administration :**

Ce composant très pratique, codé en CGI/PHP, va lire les informations stockées dans les fichiers résultat de Nagios afin d'afficher ces données sur des pages Web. Il est possible de générer des rapports ou de gérer un minimum de droits utilisateur. Un système de pipe, Unix, permet à l'utilisateur de donner des ordres au moteur Nagios (forcer le lancement d'une sonde à l'instant T, redémarrer le service, modifier la configuration d'un objet, etc.).

4.2.2. Cacti :

Cacti est un logiciel de supervision réseau basé sur RRDTool. RRDTool est un outil de gestion de base de données RRD créé par Tobias Oetiker. Il est utilisé par de nombreux outils open source, tels que Cacti, collectd, Lighttpd, et Nagios, pour la sauvegarde de données cycliques et le tracé de graphiques, de données chronologiques.

Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs...) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le Ping d'un élément actif.

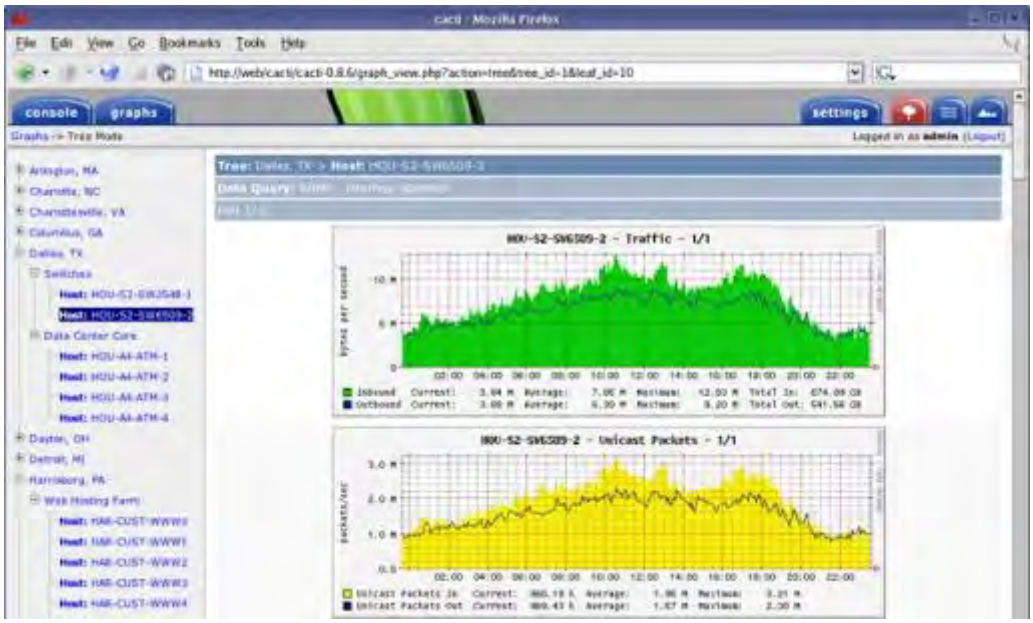


Figure 12: Interface web de Cacti

✓ **Collecter des données :**

A intervalle donné (5 minutes par défaut), Cacti va collecter des valeurs ou mesurer des temps de réponse grâce à son ordonnanceur intégré. Il existe plusieurs types d'ordonnanceurs, du plus simple écrit en PHP au plus performant écrit en C. Cacti interroge les hôtes principalement par l'intermédiaire du protocole SNMP. Une majorité d'équipements réseaux et informatiques proposent cette fonctionnalité mais si ce n'est pas le cas, Cacti peut aussi interroger via des scripts étendant grandement les possibilités.

✓ **Alimenter des bases de données :**

Cacti s'appuie sur RRDTool développé par Tobias Oetiker. Le grand principe de RRDTool est de stocker les valeurs dans des bases de données tournantes à taille fixe, appelées "Round Robin Archive". On ne conserve que les "n" dernières valeurs, les valeurs sont moyennées pour alimenter une autre base portant sur une période de temps plus grande, et ainsi de suite.

✓ **Générer des graphes :**

S'appuyant sur RRDTool, Cacti fournit une représentation graphique de ces valeurs et de leur évolution dans le temps. Les graphes sont générés en temps réel et l'on peut zoomer ou

changer l'échelle de temps. Une arborescence permet de naviguer simplement entre les équipements et les graphes associés.

- ✓ **Interface graphique :**

Cacti permet aux utilisateurs de consulter les graphes à travers une interface web écrite en PHP. Mais elle permet aussi d'effectuer très simplement toute la configuration de l'outil. De plus, afin de permettre une délégation des taches, Cacti propose une gestion des accès très fine.

4.2.3. Tableau comparatif :

	Nagios	Cacti
Scan et découverte réseau, cartographie et visualisation	✓	✗
ICMP, SNMP	✓	✓
Alertes Base de donnée	✓	✓
Surveillance SLA	✓	✗
Surveillance Matériel	✓	✓
Surveillance Serveur Web	✓	✓
Surveillance et Alertes AD	✓	✗
Rapports et graphiques des tendances historiques	✓	✓
Application Mobile iOS et Android	✓	✗

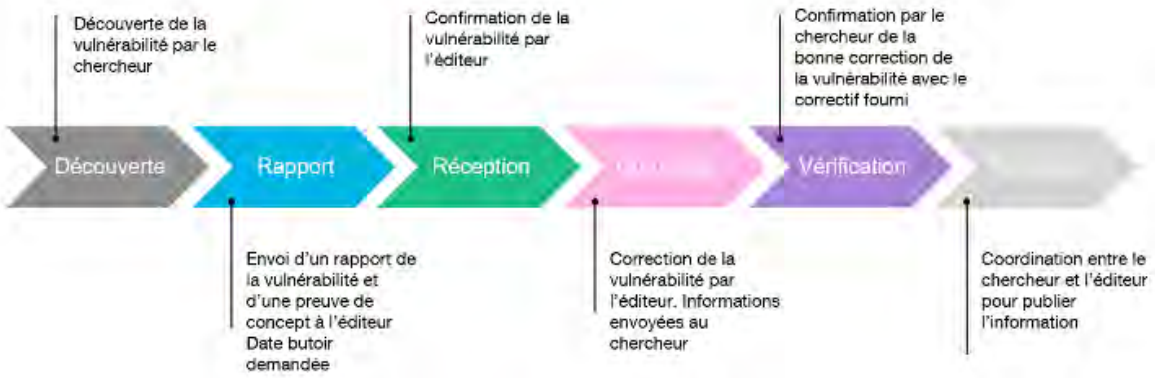
Tableau 3: Comparatif entre les solution Nagios et Cacti

Au vue des caractéristiques des deux solutions on voit que Nagios répond au mieux les critères définis dans le tableau. Notre choix se portera alors sur la solution de Nagios pour la supervision des actifs de notre infrastructure.

4.3. Gestion intégrée des vulnérabilités :

Une vulnérabilité est une faille de sécurité. Elle provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel.

Toutes les vulnérabilités ne mènent pas forcément à une cyberattaque. En effet, elles sont majoritairement rendues publiques et corrigées. On dit qu'elles font l'objet d'un traitement en divulgation complète, full disclosure en anglais.

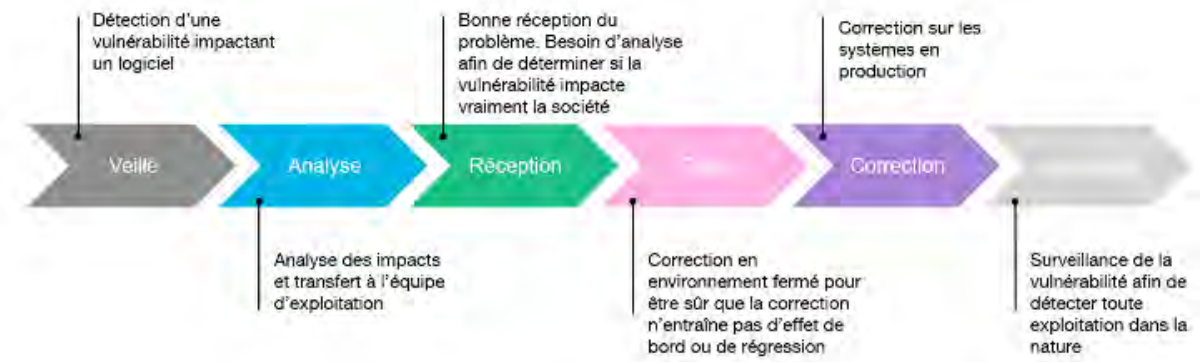


Source : Timeline de divulgation complète, CERT Orange Cyberdefense, département Vulnerability Intelligence Watch, 2019

Figure 13: Chronologie de divulgation d'une vulnérabilité

Actuellement, moins de 5% des vulnérabilités publiées disposent d'un code d'exploitation final. C'est ce code qui permet d'exploiter la vulnérabilité et rend possible une attaque. En effet, la plupart des vulnérabilités ne sont pas exploitées (aucun code d'exploitation ou difficulté de s'en procurer, manque d'intérêt). De plus, bien qu'un code d'exploitation soit mis à disposition par un chercheur ou la communauté, ce dernier est en réalité rarement utilisé à des fins de pandémie. Pour qu'une vulnérabilité soit intéressante à exploiter, elle doit répondre aux critères suivants :

- toucher un grand nombre de cibles ;
- être simple à exploiter ;
- avoir un but lucratif direct (ransomware) ou indirect (vol de données à des fins de revente ou de chantage).



Source : Timeline de correction, CERT Orange Cyberdefense, département Vulnerability Intelligence Watch, 2019

Figure 14: Chronologie de correction d'une vulnérabilité

Une fois découvertes, les vulnérabilités peuvent faire l'objet d'une identification appelée CVE pour Commom Vulnerabilities and Exposures. Celle-ci est donnée, sur demande des chercheurs, par le Massachussetts Institute of Technology Research Establishment (MITRE).

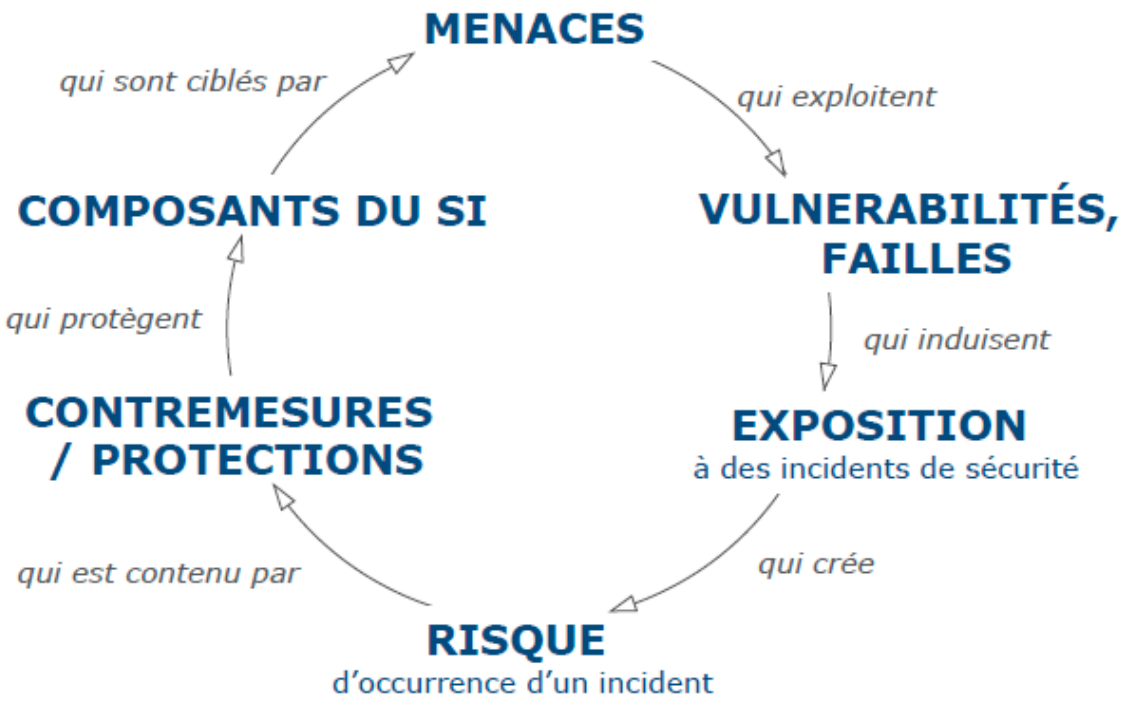


Figure 15: Diagramme d'analyse de vulnérabilités

- ✓ **Qu'est-ce qu'une CVE ?**

L'acronyme CVE, pour Common Vulnerabilities and Exposures en anglais, désigne une liste publique de failles de sécurité informatique. Lorsque l'on parle d'une CVE, on fait généralement référence à l'identifiant d'une faille de sécurité répertoriée dans cette liste. Les CVE aident les professionnels à coordonner leurs efforts visant à hiérarchiser et résoudre les vulnérabilités, et ainsi renforcer la sécurité des systèmes informatiques.

Chaque CVE se voit attribuer un numéro appelé identifiant CVE. Les identifiants CVE sont attribués par l'une des quelque 100 autorités de numérotation CVE (CNA). Les CNA comprennent des fournisseurs informatiques, des organismes de recherche tels que des universités, des sociétés de sécurité et même MITRE eux-mêmes. Un identifiant CVE prend la forme de CVE- [Année] - [Numéro]. L'année représente l'année au cours de laquelle la vulnérabilité a été signalée. Le numéro est un numéro séquentiel. Par exemple, CVE-2019-0708, correspond à une faille dans l'implémentation du protocole RDP (Remote Desktop Protocol) de Microsoft.

CVE est la base de données des vulnérabilités et expositions connues. Chaque entrée de cette base de données à un score CVSS correspondant. Le score CVSS évalue la gravité de la CVE.

- ✓ **Qu'est-ce que le CVSS (Common Vulnerability Scoring System) ?**

Plusieurs systèmes permettent d'évaluer la gravité d'une vulnérabilité. Il existe notamment le système CVSS (Common Vulnerability Scoring System), un ensemble de normes ouvertes utilisées pour attribuer un nombre à une vulnérabilité afin d'en évaluer la gravité. Les scores sont compris entre 0.0 et 10.0, et les nombres les plus élevés correspondent au plus haut degré de gravité pour une vulnérabilité. De nombreux fournisseurs de solutions de sécurité ont également créé leurs propres systèmes d'évaluation.

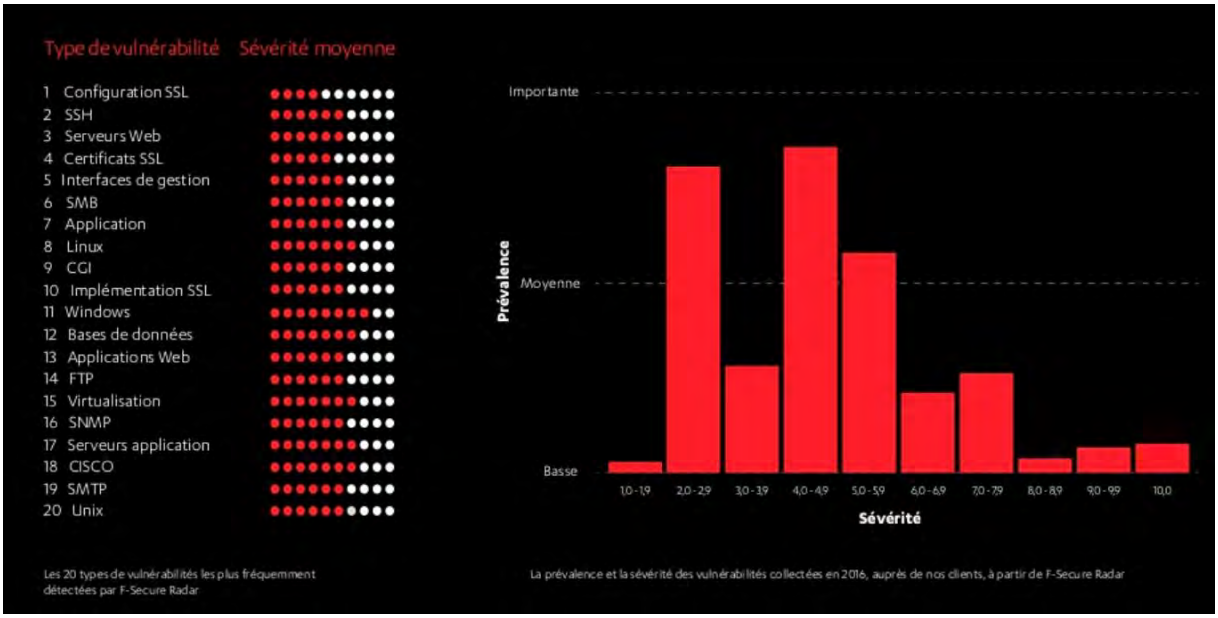


Figure 16: Type de vulnérabilités

4.3.1. OpenVAS (Open Vulnerability Assessment Scanner) :

OpenVAS est un logiciel Open Source de sécurité informatique. C'est un scanner de vulnérabilités. Il se présente sous la forme d'un client/serveur. C'est un fork de Nessus, développé par Tenable Network Security.

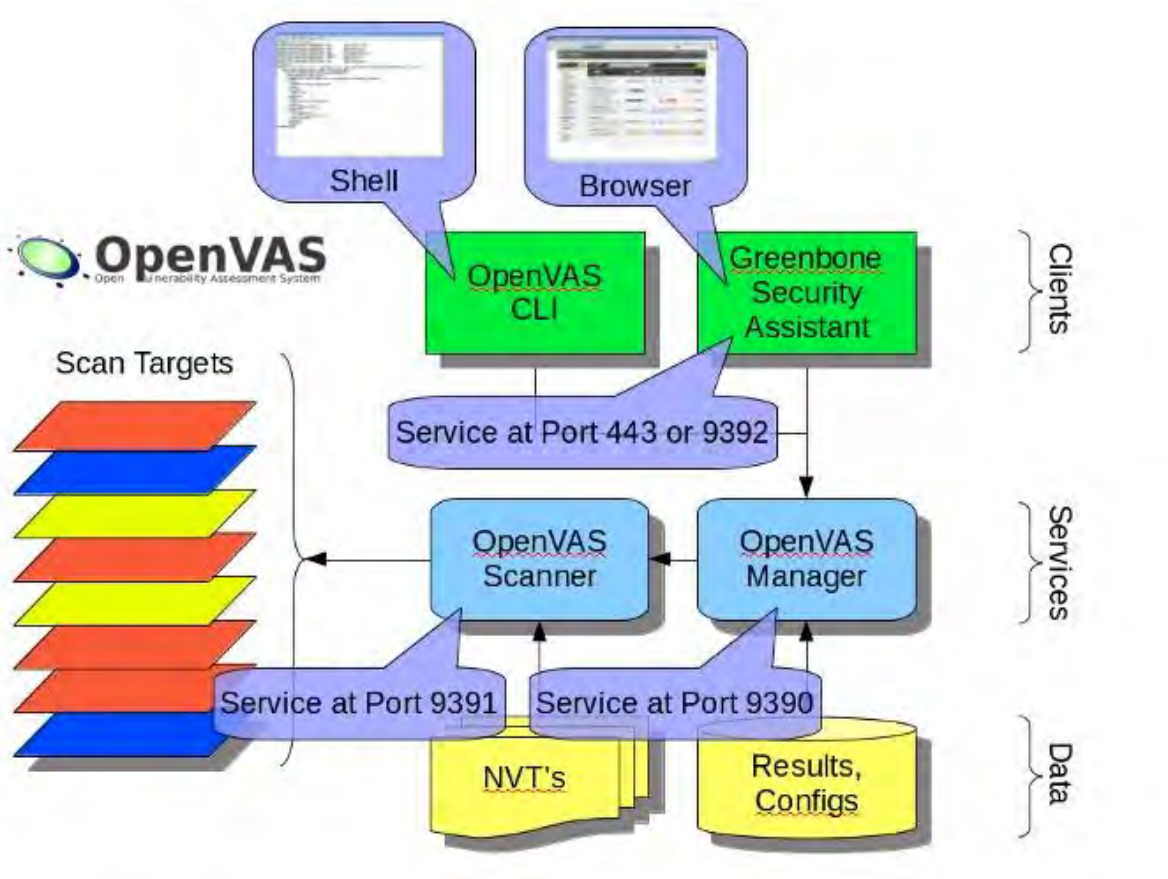


Figure 17: Architecture de OpenVAS

Le client permettant de définir le périmètre (plage d'adresse, type de machine) et les paramètres de l'audit (audit externe ou interne). Il se décline en CLI (ligne de commande), GUI (interface graphique) et API (Python notamment). Il est disponible sous GNU/Linux. Le serveur effectuant le scan des différentes vulnérabilités (appelés NVT pour "Network Vulnerability Test") disponibles dans sa base (plus de 26.000 NVTs). Le serveur existe uniquement sous GNU/Linux.

Les caractéristiques de OpenVAS :

- Greenbone Security Assistant (GSA), l'interface Web qui permet d'administrer l'outil de scan ;
- Greenbone Desktop Security (GDS) qui permet d'avoir une application de bureau pour l'administration ;
- OpenVAS Manager est l'outil principal du logiciel. Il permet de faire la relation entre les informations données par l'administrateur et les autres composants du logiciel. Gestion des utilisateurs, des scans avec une BDD SQL, etc.

- OpenVAS Scanner est l'outil qui nous permettra d'évaluer les vulnérabilités sur les cibles ;
- OpenVAS Administration est un autre outil qui permet d'administrer le logiciel, de créer des utilisateurs, de gérer les mises à jour de la BDD CVE, etc.
- Scan Targets sont tout simplement les cibles de des différents scans.

4.3.2. Nessus :

Nessus est la solution d'analyse des vulnérabilités la plus largement déployée sur le marché. Elle identifie les vulnérabilités, réduit le risque et assure la conformité dans les environnements physiques, virtuels, mobiles et cloud. Elle offre de multiples fonctionnalités : recherche rapide des ressources, audit de configuration, profilage cible, détection de malware, examen des données sensibles, intégration de la gestion des correctifs et analyse des vulnérabilités. Avec la plus vaste bibliothèque de contrôles de vulnérabilité et de configuration, actualisée en permanence. La solution Nessus assure une intégration étroite et une extensibilité par API à d'autres produits de sécurité de type SEIM, dispositifs de défense antimalware, outils de gestion des correctifs, systèmes de protection des appareils mobiles, pare-feu et plateformes de virtualisation.

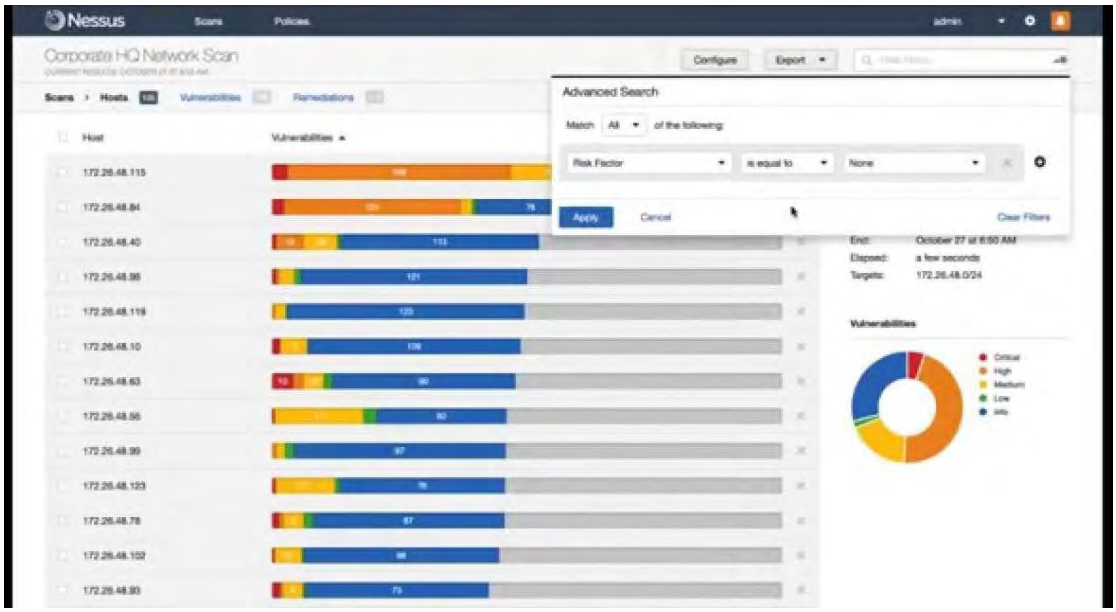


Figure 18: Résulta d'un scan avec Nessus

Les caractéristiques de Nessus :

- Indices de risque : notation des vulnérabilités selon le CVE, cinq degrés de gravité (critique, élevé, moyen, faible, info), degrés de gravité personnalisables pour reclassement du risque ;
- Reporting flexible : personnalisation des rapports au format (PDF, HTML et CSV) avec un tri par vulnérabilité ou hôte, création d'une synthèse ou comparaison de résultats d'analyse pour mettre en évidence les changements ;
- Analyse : détection des vulnérabilités (y compris réseaux IPv4/IPv6/ hybrides)
- Systèmes d'exploitation : Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries ;
- Applications Web : serveurs Web, services Web, vulnérabilités OWASP ;
- Détection des virus, programmes malveillants, portes dérobées, hôtes communiquant avec des systèmes infectés par un réseau de bots, processus connus/inconnus, services Web reliés à un contenu malveillant.

4.3.3. Tableau comparatif :

	Nessus	OpenVAS
CVE prise en charge	60000 CVE	< 26000 CVE
Précision des scans	Taux de faux positif faible	Non communiqué
Modèles de scan prédéfinis	Modèles pour les vulnérabilités majeures (WannaCry, Spectre et Meltdown, etc.)	Pas de modèles pour WannaCry, Spectre et Meltdown, etc.
Délai de publication des contrôles de vulnérabilité	Nouveaux contrôles de vulnérabilité (plug-ins) publiés dans un délai moyen de 24 heures après la divulgation d'une vulnérabilité	Non communiqué
Création de rapports flexible	Les modèles de rapport prédéfinis simplifient la création de rapports. Les rapports peuvent être personnalisés	Modèles de rapport et capacités de filtrage limités

Formats d'exportation des rapports	HTML, CSV, PDF, Nessus XML et Nessus DB	HTML, PDF, XML et texte
Distribution automatique du rapport par e-mail une fois le scan terminé	Inclus	Non disponible
Systèmes d'exploitation pris en charge	Debian/Kali Linux, Red Hat, CentOS, Oracle Linux, FreeBSD, Fedora, SUSE Linux Enterprise, Ubuntu, Windows Server (2008, 2008 R2, 2012, 2012 R2, 2016), Windows (7, 8, 10)	Les utilisateurs doivent créer leurs propres fichiers binaires OpenVAS à partir de code source ou utiliser des packages de la communauté non prise en charge. Ne fonctionne pas sous Windows.
Options de déploiement	Clé USB live, cloud ou installation traditionnelle	Installation traditionnelle
Coût d'acquisition, d'exploitation et de support du produit	Abonnement Nessus Professional : < 3 000 $/an pour un nombre illimité d'adresses IP. Les nombreuses fonctions prédéfinies, l'automatisation et le support fournisseur réduisent les efforts manuels.	Téléchargement gratuit. Un travail manuel important est nécessaire pour déployer la solution, l'exploiter et assurer soi-même le support.
Investissement dans le produit	Tenable investit énormément dans Nessus : rien qu'en 2018, une version majeure, deux mineures et neuf versions de correction ont été publiées	OpenVAS a publié seulement 2 versions au cours des 4 dernières années

Tableau 4: Comparatif des solution Nessus et OpenVAS

D'après les éléments comparatifs qu'on a utilisé Nessus dépasse de loin OpenVAS, ce qui nous amène à choisir Nessus comme outil de gestion de vulnérabilités pour notre projet. Tout de même OpenVAS reste parmi les meilleurs outils de gestion de Vulnérabilités et est en plus open

source et gratuit. Pour des infrastructure vaste les deux solutions peuvent être jumelées afin profiter de leurs avantages. Dans le cadre de notre projet nous utiliserons Nessus.

4.4. Centralisation et analyse des événements (SIEM)

Une solution de SIEM (Security Information and Event Management) a pour objectif de répondre au besoin des entreprises d'analyser les événements de sécurité en temps réel, au regard de la gestion interne et externe des menaces. Cette solution permet de surveiller des applications, des comportements utilisateurs et des accès aux données. A travers les fonctionnalités fournis par la solution, il est donc possible de collecter, normaliser, agréger, corréler et analyser les données des événements issus des machines, systèmes et applications (pare-feu, IDS/ISP, Machines réseau, Machines de sécurité, Applications, bases de données, serveurs, annuaires, IAM).

Une solution SIEM assure la gestion, l'intégration, la corrélation et l'analyse en un seul endroit, ce qui facilite la surveillance et la résolution des problèmes dans une infrastructure informatique en temps réel. Sans SIEM, un analyste de sécurité doit passer en revue des millions de données non comparables, stockées dans des « silos » pour chaque matériel, chaque logiciel et chaque source de sécurité. En bref, SIEM est synonyme de simplicité.

Deux briques constituent une solution de SIEM (Security Information and Event Management) :

La première brique appelée SEM, pour Security Event Management, permet l'analyse des logs en temps réel (ou quasi réel) en provenance des systèmes de sécurité, réseaux, d'exploitation et applicatifs :

- gestion des événements de sécurités ;
- corrélation des événements ;
- réponse aux incidents sur des menaces internes comme externes ;
- analyse en temps réels.

La seconde brique appelée SIM, pour Security Information Management, permet de fournir des rapports en conformité avec la réglementation, et de surveiller les menaces internes :

- gestion des logs ;
- rapports ;
- analyses différées.

Le SIEM, qui regroupe ces 2 systèmes, accélère donc l'identification et l'analyse des événements de sécurité, atténue les conséquences d'attaques et facilite la restauration qui s'ensuit. Pour y parvenir, il collecte les événements, les stocke (avec normalisation) et agrège des données pertinentes mais non structurées issue de plusieurs sources. L'identification des écarts possibles par rapport à la moyenne / norme nourrit la prise de décision. En outre, les tableaux de bord générés contribuent à répondre aux exigences légales de conformité de l'entreprise.

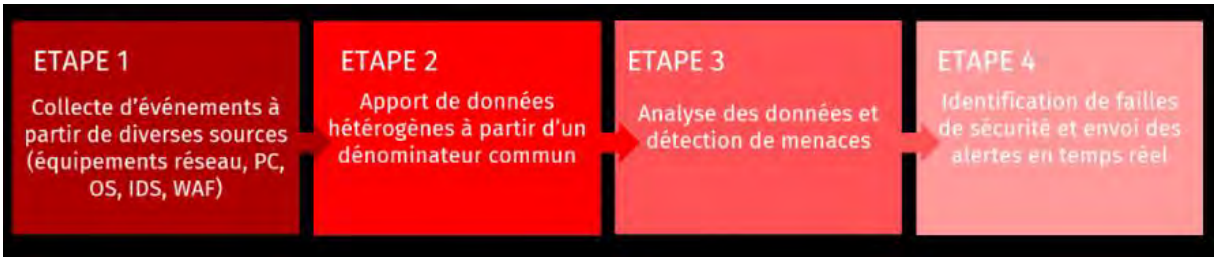


Figure 19: Les différentes étapes de traitement des données dans un SIEM

- ✓ **Détection proactive d'incidents**

Un SIEM s'avère capable de détecter des incidents de sécurité qui seraient passés inaperçus. Pour une raison simple : les nombreux hôtes qui enregistrent des événements de sécurité ne disposent pas de fonctions de détection d'incidents.

Le SIEM dispose de cette faculté de détection grâce à sa capacité de corrélation des événements. Contrairement à un système de prévention d'intrusion qui identifie une attaque isolée, le SIEM regarde au-delà. Les règles de corrélations lui permettent d'identifier un événement ayant causé la génération de plusieurs autres (hack via le réseau, puis manipulation sur un équipement précis…).

Dans de tels cas de figure, la plupart des solutions ont la capacité d'agir indirectement sur la menace. Le SIEM communique avec d'autres outils de sécurité mis en place dans l'entreprise (ex : pare-feu) et pousse une modification afin de bloquer l'activité malveillante. Résultat, des attaques qui n'auraient même pas été remarquées dans l'entreprise sont contrecarrées.

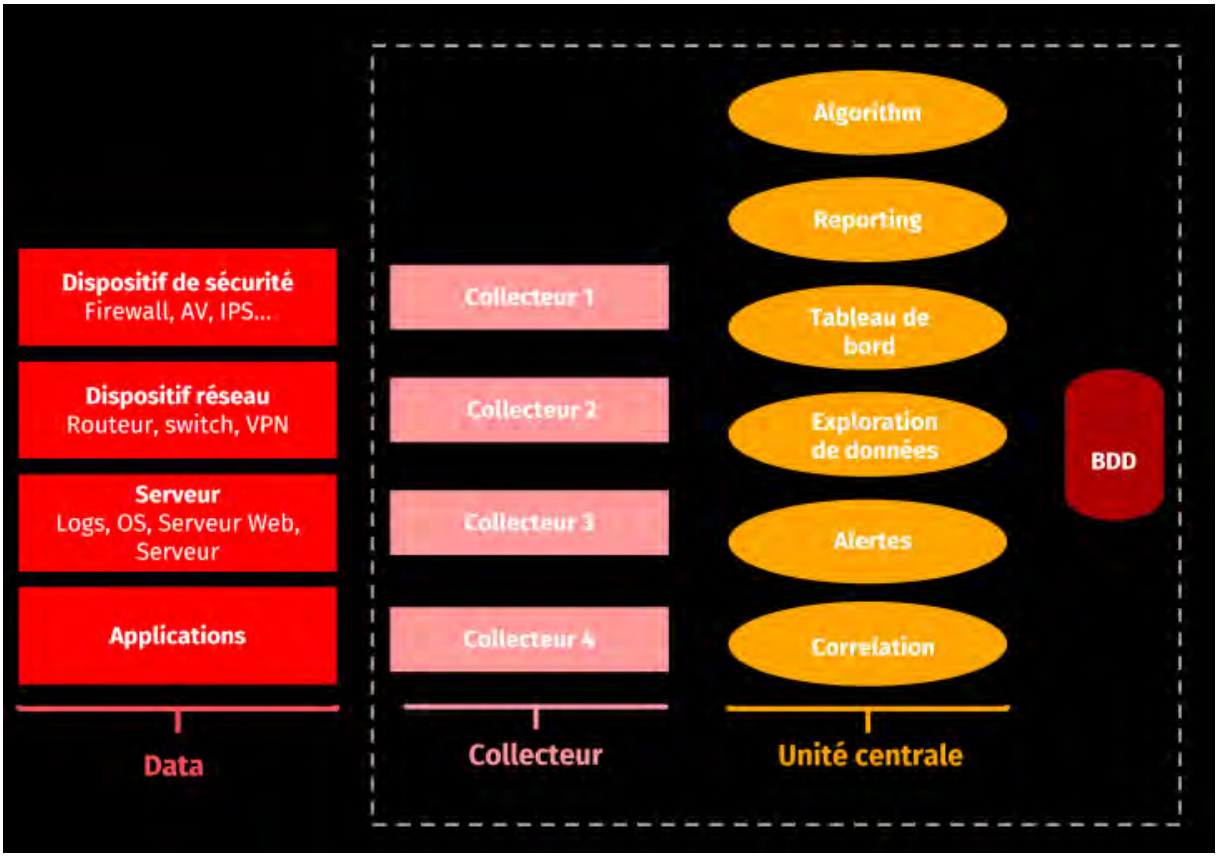


Figure 20: Architecture d'un SIEM

✓ **Principaux fonctionnalités :**

Un SIEM fonctionne comme une mémoire des évènements de sécurité. Premièrement, il faut savoir que celui-ci s'articule autour de plusieurs fonctions dites « principales » :

- **Collecte des données de contexte et des logs** : Cette fonction consiste à recueillir des logs et des données de contexte, notamment des informations d'identité ou les résultats des analyses de vulnérabilité, à l'aide d'une combinaison de méthodes basées ou non sur un agent.
- **Normalisation** : Cette fonction convertit les logs originaux collectés dans un format universel à des fins d'utilisation au sein du SIEM. Pour permettre une interprétation efficace des données sur les différentes sources et la corrélation des événements, les systèmes SIEM sont en mesure de normaliser les journaux. Ce processus de normalisation consiste à traiter les journaux dans un format lisible et structuré, à en extraire les données importantes et à mapper les différents champs qu'ils contiennent.

- **Corrélation :** La corrélation constitue le backbone analytique du SIEM. Cette fonction est basée sur des règles, comme la mise en relation de différents événements entre eux ou la mise en relation d'événements avec des données de contexte. La corrélation peut s'effectuer en temps réel, mais tous les outils ne prennent pas en charge cette fonction. En effet, certains outils se concentrent sur la corrélation des données historiques provenant de leurs bases de données. En outre, d'autres méthodes d'analyse des logs sont parfois incluses dans cette catégorie. Les moteurs de corrélation utilisent l'intelligence artificielle pour réduire les faux positifs augmentant ainsi l'efficacité de la détection d'événement.
- **Notification et alertes :** Cette fonction comprend le déclenchement de notifications ou d'alertes auprès d'opérateurs ou de gestionnaires. Les mécanismes d'alerte courants comprennent les e-mails, les SMS ou même les messages envoyés via le protocole SNMP.
- **Hiérarchisation :** Cette fonction comprend différentes options qui mettent en évidence les événements importants par rapport aux événements de sécurité moins graves. Pour ce faire, il est possible de corréler les événements de sécurité avec des données de vulnérabilité ou d'autres informations sur les ressources. Les algorithmes de hiérarchisation utilisent souvent des informations sur la gravité fournie par le log original.
- **Présentation :** La possibilité de visualiser des données et des événements est un autre composant clé des systèmes SIEM, car elle permet aux analystes de visualiser facilement les données. Les tableaux de bord contenant plusieurs vues permettent d'identifier les tendances et les anomalies et de surveiller l'état général ou de sécurité d'un environnement. Certains outils SIEM seront livrés avec des tableaux de bord prédéfinis, tandis que d'autres permettront aux utilisateurs de créer et d'ajuster leurs propres tableaux de bord.
- **Création de rapports :** La création de rapports standard et planifiés prend en compte toutes les vues historiques des données recueillies par le produit SIEM. Certains produits sont également dotés d'un mécanisme de distribution des rapports aux directeurs informatiques ou au personnel en charge de la sécurité, soit par e-mail soit à l'aide d'un portail Web sécurisé dédié.

4.4.1. AlienVault OSSIM : 

OSSIM (Open Source Security Information and Event Management) est un SIEM open source d'Alien Vault fait spécialement pour la collecte d'événements, la normalisation et la corrélation. Ce SIEM a été conçu pour répondre aux difficultés que font face les professionnels de la sécurité, qu'il soit libre ou propriétaire un SIEM est inutile s'il ne sait pas gérer les contrôles de base nécessaire à la sécurité de l'entreprise. Il convertit les données collectées en format qu'il comprend. Il illustre une mise en œuvre de la cartographie pour améliorer la détection d'intrusions. Son atout principal est que OSSIM n'est qu'un seul outil contenant plusieurs outils open source existants permettant d'avoir une meilleure gestion de la sécurité réseaux. Avec OSSIM il est possible de définir des règles de sécurité relatives à la politique de sécurité adoptée, de connaître la cartographie du réseau et de corréler les différents outils pour optimiser la supervision (réduire les faux positifs par exemple). On cherche à exploiter les caractéristiques des différents outils déjà existants pour collecter le plus d'information nécessaire pour une meilleure vision du réseau. OSSIM garantit l'interopérabilité des différents outils. En tant que système SIEM, OSSIM est destiné à fournir aux analystes et aux administrateurs de la sécurité une vue de tous les aspects liés à la sécurité de leur système, en combinant la gestion des journaux et la gestion et la découverte des actifs avec des informations provenant de systèmes de contrôle et de détection dédiés. Ces informations sont ensuite mises en corrélation pour créer des contextes non visibles d'un seul tenant. OSSIM exécute ces fonctions en utilisant d'autres composants de sécurité de logiciel open source bien connus, en les unifiant sous une interface utilisateur unique basée sur un navigateur. L'interface fournit des outils d'analyse graphique pour les informations collectées à partir du composant logiciel open source sous-jacent (la plupart ne sont que des outils en ligne de commande qui ne se connectent que dans un fichier texte brut) et permettent une gestion centralisée des options de configuration.

- ✓ **Les composants de AlienVault OSSIM**

OSSIM comprend les composants logiciels suivants :

PRADS : utilisé pour identifier les hôtes et les services en surveillant passivement le trafic réseau.

OpenVAS : utilisé pour l'évaluation de la vulnérabilité et pour la corrélation croisée des informations (alertes du système de détection d'intrusion (IDS) par rapport au scanner de vulnérabilité).

Snort : utilisé comme système de détection d'intrusion (IDS) et également utilisé pour la corrélation croisée avec Nessus.

Suricata : utilisé en tant que système de détection d'intrusion (IDS), il s'agit de l'IDS utilisé dans la configuration par défaut Tcptrack, utilisé pour les informations de données de session pouvant accorder des informations utiles pour la corrélation d'attaque.

Nagios : utilisé pour surveiller les informations de disponibilité des hôtes et des services en fonction d'une base de données d'actifs hôtes.

OSSEC : un système de détection d'intrusion basé sur l'hôte (HIDS).

Munin : pour l'analyse du trafic et la surveillance des services.

NFSen / NFDump : utilisé pour collecter et analyser les informations NetFlow.

FProbe : utilisé pour générer des données NetFlow à partir du trafic capturé.

OSSIM inclut également des outils développés par l'utilisateur, le plus important étant un moteur de corrélation générique avec prise en charge de directives logiques et une intégration des journaux avec des plugins.

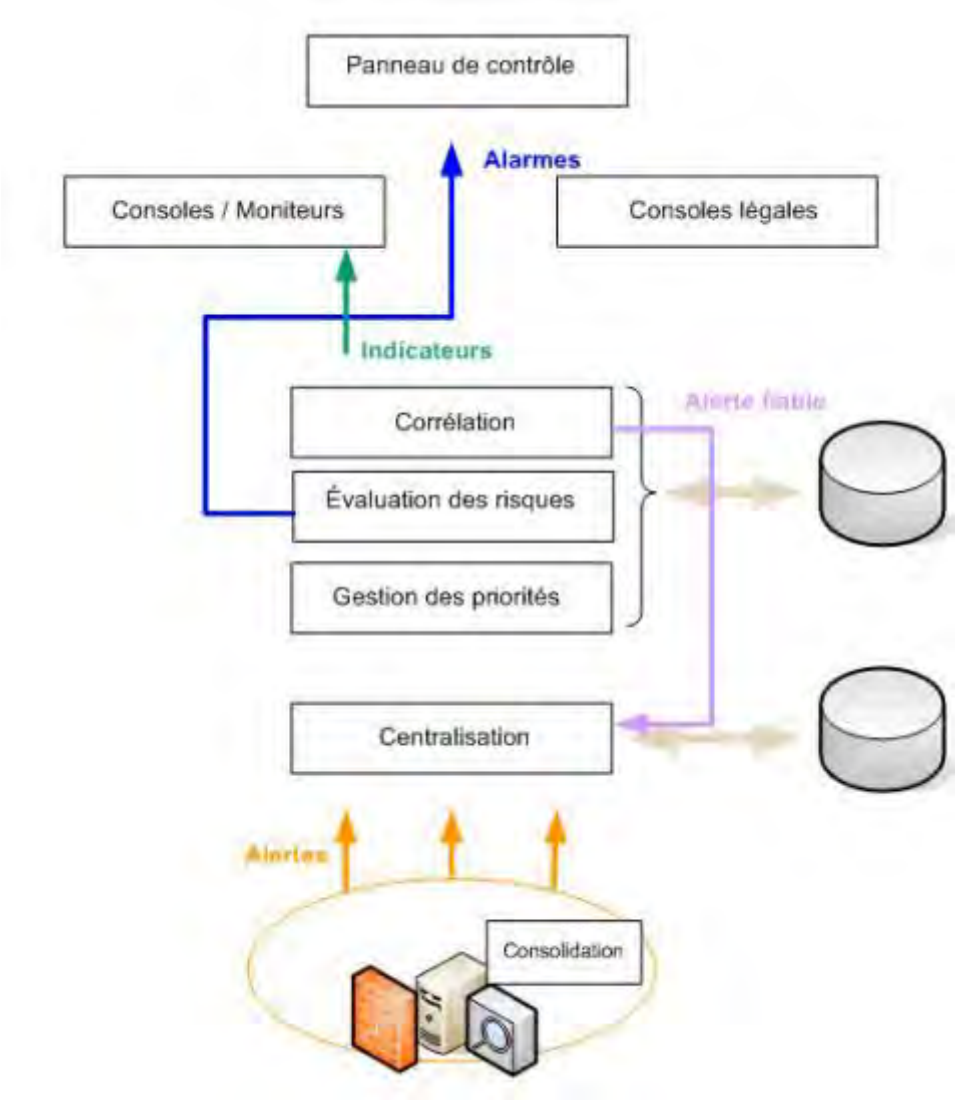


Figure 21: Architecture de fonctionnement OSSIM

✓ **Points Forts :**

- Fournit des rapports flexibles et des tableaux de bord pour rendre les audits sans facile.
- Découvre tous les actifs critiques de votre organisation et les évalue en permanence pour déterminer les vulnérabilités.
- Détecte les menaces avec les IDS basés sur l'hôte et sur le réseau.
- Surveille les perturbations et les intrusions à l'aide de la surveillance du trafic réseau et de l'intégrité des fichiers.
- Fournit des renseignements de sécurité pour la corrélation SIEM, la gestion des incidents, les rapports et les alertes.
- Démontre la conformité en évaluant les contrôles de sécurité en temps réel.

- Conserve de manière sécurisée les données de journal brutes pour répondre aux exigences de conservation des données et de gestion des logs.

✓ **Points Faibles :**

OSSIM présente quelques limites telles que :

- Complexité relative d'amélioration vue son potentiel élevé de manipulation et son utilisation assez lourde d'outils puissants en documentation.
- Des difficultés dans la configuration.

4.4.2. Splunk :

Splunk est une plateforme logicielle permettant de chercher, d'analyser et de visualiser les données générées par des machines, collectées à partir de sites web, d'applications, de capteurs, et d'appareils en tout genre. Il suffit de transférer les données sur la plateforme pour laisser Splunk se charger de les traiter et de les transformer en informations exploitables. Splunk Entreprise Security (ES) fournit une surveillance en temps réel pour donner aux administrateurs une vue claire de la 'posture de sécurité' de leur entreprise, avec des interfaces facilement personnalisables et la possibilité d'accéder aux détails des événements bruts si nécessaire. Splunk ES offre la flexibilité nécessaire pour personnaliser des recherches de corrélations, des alertes, des rapports et des tableaux de bord, afin de répondre à des besoins spécifiques.

✓ **Composants de l'architecture Splunk :**

Il y a 3 composants principaux dans Splunk :

Splunk Forwarder, utilisé pour le transfert de données

Splunk Indexer, utilisé pour l'analyse et l'indexation des données

Search Head, est une interface graphique utilisée pour rechercher, analyser et créer des rapports.

- **Splunk Forwarder :** Splunk Forwarder est le composant utilisé pour collecter les journaux. Dans le cas d'une collecte de journaux sur un ordinateur distant, on peut utiliser les redirecteurs distants de Splunk, qui sont indépendants de l'instance principale de Splunk. En fait, vous pouvez installer plusieurs redirecteurs de ce type sur plusieurs ordinateurs, ce qui permettra de transférer les données du journal vers un indexeur Splunk pour le traitement et le stockage.

- **Splunk Indexer :** L'indexeur est le composant Splunk que vous devrez utiliser pour indexer et stocker les données provenant du redirecteur. Splunk instance transforme les données entrantes en événements et les stocke dans des index pour effectuer efficacement les opérations de recherche. Si vous recevez les données d'un redirecteur universel, alors l'indexeur les analysera d'abord, puis les indexera. L'analyse des données est effectuée pour éliminer les données indésirables. Toutefois, si vous recevez les données d'un transitaire lourd, l'indexeur n'indexera que les données.
- **Splunk Search Heads :** Ce composant utilisé pour interagir avec Splunk. Il fournit aux utilisateurs une interface graphique permettant d'effectuer diverses opérations. Vous pouvez rechercher et interroger les données stockées dans l'indexeur en saisissant les mots à rechercher et vous obtiendrez le résultat attendu. Vous pouvez l'installer sur des serveurs distincts ou avec d'autres composants Splunk sur le même serveur. Il n'existe pas de fichier d'installation distinct, il vous suffit d'activer le service Splunkweb sur le serveur Splunk pour l'activer.

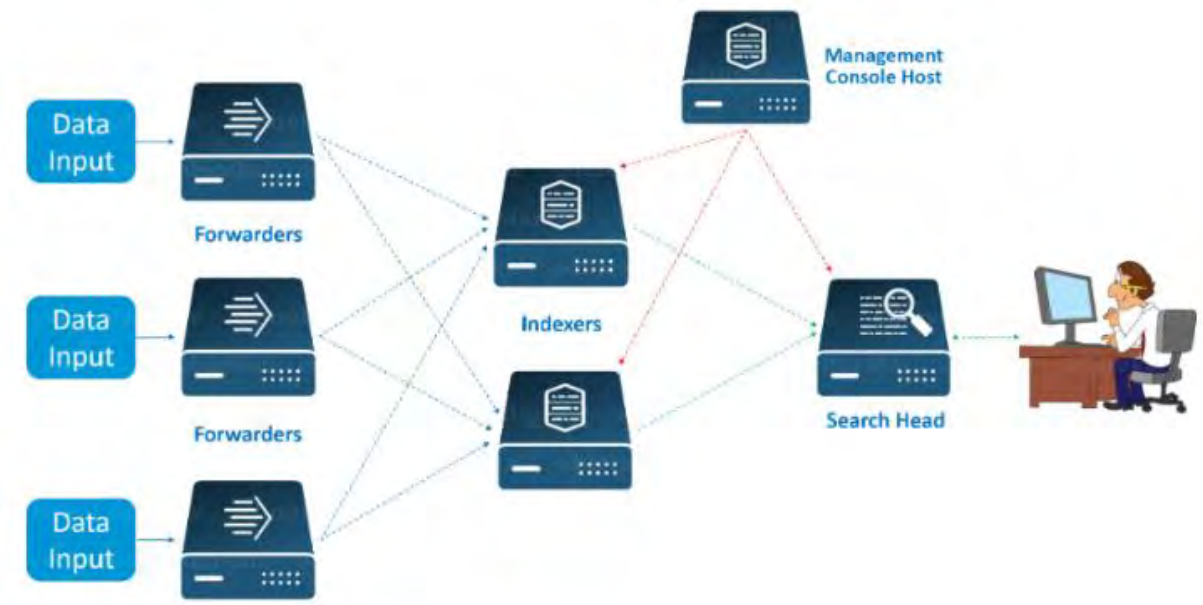


Figure 22: Architecture de fonctionnement Splunk

✓ **Points Forts :**

- Détection automatique de modèles intéressants dans vos données.
- Surveillance en temps réel des modèles et des seuils, déclenchement d'alertes lorsque des conditions spécifiques se présentent.

- Rapports et analyses puissants
- Tableaux de bord et vues personnalisés pour différents utilisateurs et rôles.
- Sécurité et contrôles d'accès granulaires basés sur les rôles.
- Prise en charge de la multi-location et de déploiements flexibles et distribués.
- La connectivité avec d'autres magasins de données comprend une intégration évolutive en temps réel avec des bases de données relationnelles et une connectivité bidirectionnelle avec les magasins de données Hadoop et NoSQL.
- Plateforme robuste et flexible pour le développement d'applications d'entreprise.

✓ **Points faibles :**

- Le principal frein à son expansion demeure son modèle de Licence, Splunk limite le nombre de nouvelles données pouvant être indexées par jour. Il existe bien une version gratuite mais celle-ci plafonne à 500 Mo/jours valable deux mois. Lorsque l'on acquiert une licence Splunk Enterprise, on achète un droit d'indexation pour un certain volume de données ajoutées quotidiennement à Splunk, peu importe la durée de rétention des données, le nombre d'utilisateurs ou de serveurs.

4.4.3. Tableau Comparatif :

	Splunk	**AlienVault**
Lieu d'utilisation	Entreprises et industries	Entreprise et PME
Capacité d'enregistrement	Ingestion des données journalièrement	A partir de 15000 EPS
Intelligence	Apprentissage automatique	Réseau de partages de plus de 1M menace par jour
Déploiement	Logiciel, cloud, VM	Logiciel et cloud
Licence	Payante	Gratuit

Tableau 5: Comparatif des solutions Splunk et AlienVault

En étudiant les différentes solutions ci-dessus, nous avons donc constater que :

La solution OSSIM qui est un SIEM open source peut être déployer dans les petites comme dans les grandes entreprises. C'est une solution complète lorsqu'on parle de SIEM et il intègre d'autres outils pour renforcer et améliorer le niveau de sécurité. Son principal défaut est sa complexité pour le déploiement et l'absence de support pour nous assister en cas de

problème. Splunk est un SIEM à part entière car il fait en son sein toutes les fonctionnalités que ce dernier est capable de réaliser et la gestion de son interface est d'autant plus facile que son implémentation. Donc Splunk est la solution que nous retenons pour cette étude pour le déploiement de notre SIEM.

4.5. Outil de gestion des incidents de sécurité :

Alors que les cyberattaques continuent de croître en volume, en diversité et en sophistication, en plus d'être de plus en plus perturbatrices et dommageables, les entreprises doivent être prêtes à les gérer efficacement. En plus de déployer des solutions et des pratiques de sécurité efficaces, ils doivent pouvoir identifier et traiter rapidement les attaques, garantissant ainsi un minimum de dommages, de perturbations et de coûts.

Chaque système informatique est une cible potentielle d'une cyber-attaque, et la plupart des gens conviennent qu'il ne s'agit pas de savoir si, mais quand cela se produira. Cependant, l'impact varie en fonction de la rapidité et de l'efficacité avec lesquelles vous abordez le problème, d'où la nécessité d'une préparation à la réponse aux incidents. Une réponse aux incidents de cybersécurité fait référence à une série de processus qu'une organisation prend pour faire face à une attaque contre ses systèmes informatiques. Cela nécessite une combinaison des bons outils matériels et logiciels ainsi que des pratiques telles qu'une planification, des procédures, une formation et un soutien appropriés de la part de tous les membres de l'organisation.

Les outils de réponse aux incidents sont essentiels pour permettre aux organisations d'identifier et de traiter rapidement les cyberattaques, les exploits, les logiciels malveillants et autres menaces de sécurité internes et externes. Les outils aident à surveiller, identifier et résoudre automatiquement et rapidement un large éventail de problèmes de sécurité, rationalisant ainsi les processus et éliminant le besoin d'effectuer la plupart des tâches répétitives manuellement. La plupart des outils modernes peuvent fournir de multiples fonctionnalités, notamment la détection et le blocage automatiques des menaces et, en même temps, alerte les équipes de sécurité concernées pour des enquêtes plus avancés sur le problème.

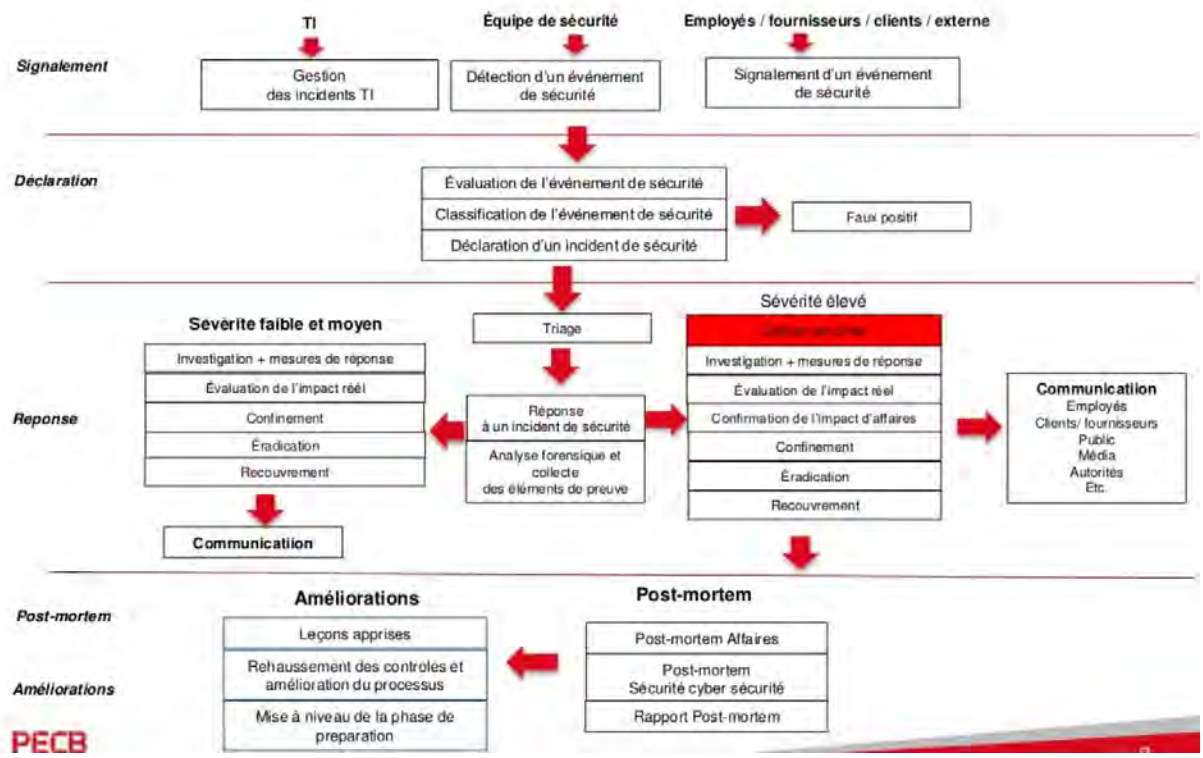


Figure 23: Processus de gestion des incidents de sécurité

✓ **Pourquoi gérer les incidents :**

L'expérience a montré qu'aucun système informatique n'est sécurisé à 100%, ce qui signifie que des incidents de sécurité vont se produire tôt ou tard. L'utilisation croissante des technologies de l'information et de la communication (TIC) offre un champ d'attaque toujours plus grand aux criminels.

Le premier but de la gestion des incidents est de minimiser l'impact (l'envergure) de l'incident et de rétablir un fonctionnement normal dans les meilleurs délais. Dans le domaine professionnel, cela se traduit par la volonté de ne pas violer le contrat de niveau de service (Service Level Agreement (SLA)).

Le deuxième but de la gestion des incidents est d'analyser la situation afin de comprendre l'incident en détail et d'en tirer des conclusions qui permettront éventuellement de prévenir des incidents similaires dans le futur. La conservation des traces est un élément clé pour une gestion d'incidents réussie.

Enfin, il convient de collecter des informations sur les incidents afin de pouvoir établir des statistiques.

Dans cette partie nous allons faire l'étude de deux outils de gestion des incidents en sécurité que sont : Cyphon et TheHive / Cortex. / MISP

4.5.1. Cyphon :

Cyphon est une plateforme de réponse aux incidents qui reçoit, traite et trie les événements pour créer un flux de travail analytique plus efficace, regroupant et hiérarchisant les données et les alertes, et permettant aux analystes d'enquêter et de documenter les incidents.

De nombreuses organisations gèrent les événements de sécurité post-traités sous forme de notifications par e-mail, ce qui est incroyablement inefficace. Une boîte de réception inondée de notifications d'alerte crée un environnement dans lequel les problèmes critiques sont négligés et rarement étudiés.

Le Cyphon élimine ce problème en limitant les événements et en les hiérarchisant en fonction des règles définies par l'utilisateur. Les analystes peuvent rapidement enquêter sur les incidents en corrélant d'autres ensembles de données avec des indicateurs importants. Ils peuvent ensuite annoncer les alertes avec les résultats de leur analyse.

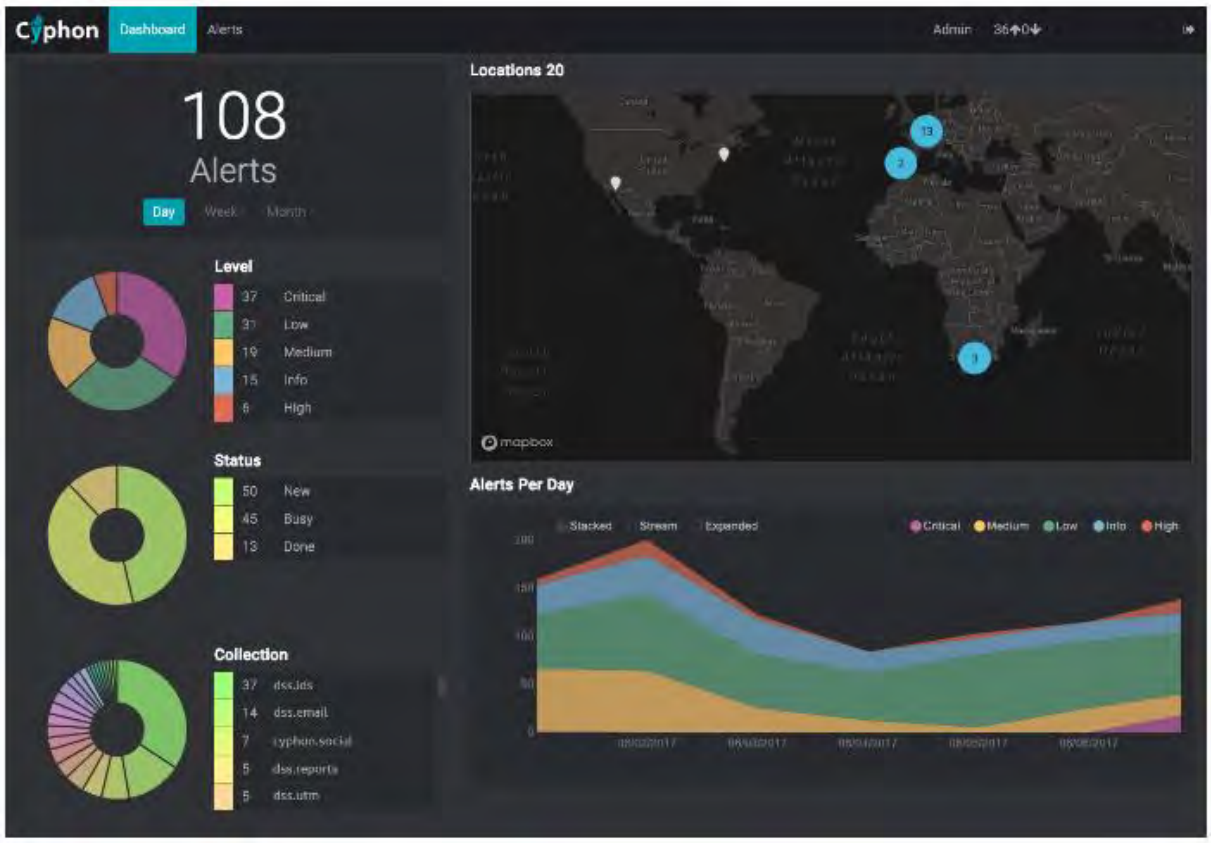


Figure 24: Vue tableau de bord Cyphon

Aujourd'hui, Cyphon prend en charge les intégrations avec Bro, Snort, Nessus et d'autres produits de sécurité populaires.

✓ **Architecture de Cyphon :**

La plateforme Cyphon est composée d'un moteur de traitement de données backend (« Cyphon Engine ») et d'une interface utilisateur frontale d'opérations de sécurité pour la visualisation (« Cyclops »). Ils sont maintenus dans des projets séparés.

Cyphon ingère, filtre, remodèle, améliore et stocke les données. Il peut également générer des alertes, récupérer des données liées au contexte d'une alerte et permettre aux utilisateurs de prendre des mesures sur les alertes.

✓ **Déploiement de Cyphon :**

Cyphon travaille avec l'aide de plusieurs projets open source. Pour que Cyphon soit opérationnel, nous devons installer toutes ses dépendances. Ce processus à était simplifié en utilisant Docker, qui nous permet de déployer facilement une application sous la forme d'un ensemble de microservices. De plus, nous avons créé un ensemble de fichiers pour exécuter Cyphon dans les environnements de développement et de production. L'utilisation d'un fichier Docker Compose nous permet d'installer et d'exécuter rapidement Cyphon et les autres services qu'il utilise, notamment :

- Base de données relationnelle PostgreSQL
- Courtier de messages RabbitMQ
- Outil d'ingestion de données Logstash

4.5.2. TheHive / Cortex / MISP :

TheHive est une plate-forme de réponse aux incidents de sécurité évolutive, open source et gratuite, étroitement intégrée à MISP (Malware Information Sharing Platform), conçue pour faciliter la vie des SOC, CSIRT, CERT et de tout professionnel de la sécurité de l'information confronté à des incidents de sécurité qui doivent être étudiés et traités rapidement.

✓ **Les fonctions de TheHive :**

- **Collaboration :** Plusieurs analystes SOC et CERT peuvent collaborer sur des enquêtes simultanément. Grâce au flux en direct intégré, les informations en temps réel relatives aux cas, tâches, observables et CIO nouveaux ou existants sont disponibles pour tous les membres de l'équipe. Des notifications spéciales leur

permettent de gérer ou d'attribuer de nouvelles tâches et de prévisualiser les nouveaux événements et alertes MISP à partir de plusieurs sources telles que les rapports par e-mail, les fournisseurs CTI et les SIEM. Ils peuvent ensuite les importer et les étudier immédiatement.

- **Élaboration** : Les cas et les tâches associées peuvent être créés à l'aide d'un moteur de modèles simple mais puissant. Vous pouvez ajouter des métriques et des champs personnalisés à vos modèles pour piloter l'activité de votre équipe, identifier le type d'enquêtes qui prennent beaucoup de temps et chercher à automatiser les tâches fastidieuses grâce à des tableaux de bord dynamiques. Les analystes peuvent enregistrer leur progression, joindre des éléments de preuve ou des fichiers importants, ajouter des balises et importer des archives ZIP protégées par mot de passe contenant des logiciels malveillants ou des données suspectes sans les ouvrir.
- **Acte** : Ajoutez une, des centaines ou des milliers d'observables à chaque cas que vous créez ou importez-les directement à partir d'un événement MISP ou de toute alerte envoyée à la plateforme. Triez et filtrez rapidement. Exploitez la puissance de Cortex et de ses analyseurs et répondeurs pour obtenir des informations précieuses, accélérer votre enquête et contenir les menaces. Tirez parti des balises, signalez les IOC, les observations et identifiez les observables précédemment vus pour alimenter vos informations sur les menaces. Une fois les enquêtes terminées, exportez les IOC vers une ou plusieurs instances du MISP.

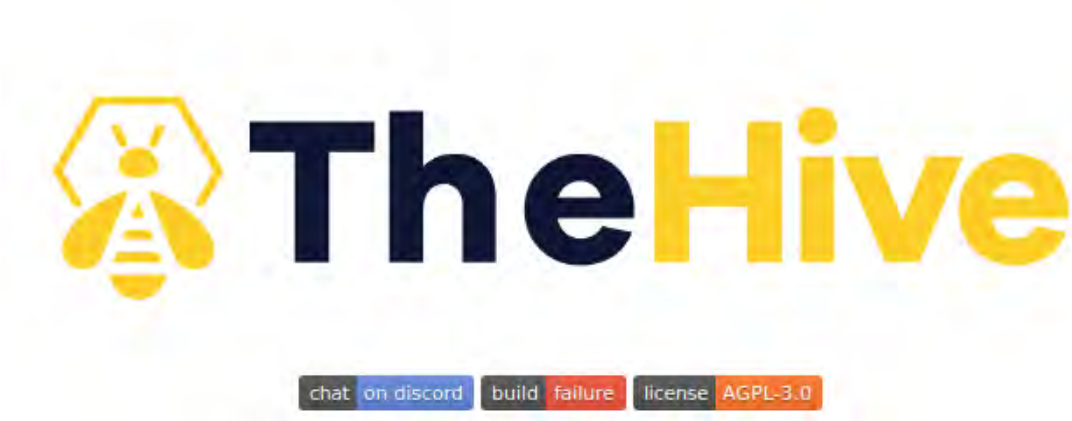


Figure 25: TheHive

Grâce à Cortex, les observables tels que les adresses IP et e-mail, les URL, les noms de domaine, les fichiers ou les hachages peuvent être analysés à l'aide d'une interface Web. Les analystes peuvent également automatiser ces opérations et soumettre de grands ensembles

d'observables à partir de TheHive ou via l'API Cortex REST à partir de plates-formes SIRP alternatives, de scripts personnalisés ou de MISP. Lorsqu'il est utilisé en conjonction avec TheHive, Cortex facilite largement la phase de confinement grâce à ses fonctionnalités Active Response.

- ✓ **Les fonctions de Cortex :**
  - **Taches répétitif :** En utilisant Cortex, vous n'aurez pas besoin de réinventer la roue à chaque fois que vous voudrez utiliser un service ou un outil pour analyser un observable et vous aider à enquêter sur l'affaire en cours ou à contenir des menaces avant qu'il ne soit trop tard. Tirez parti de son très grand ensemble d'analyseurs ou créez votre propre analyseur ou répondeur en utilisant n'importe quel langage de programmation pris en charge par Linux et partagez-les avec votre équipe ou, mieux, avec toute la communauté. Vous pouvez également interroger simultanément plusieurs instances MISP.
  - **Intégration avec TheHive :** Cortex est le compagnon idéal de TheHive. TheHive peut se connecter à une ou plusieurs instances Cortex et en quelques clics, vous pouvez analyser des dizaines voire des centaines d'observables à la fois ou déclencher des réponses actives. En utilisant le moteur de rapport de TheHive, il est facile d'analyser la sortie Cortex et de l'afficher comme vous le souhaitez. Vous pouvez également utiliser Cortex en tant que produit autonome grâce à sa puissante interface utilisateur Web pour gérer plusieurs organisations, analyseurs et configurer les limites de requêtes. Cortex peut être interfacé avec d'autres produits via son API REST ou en utilisant Cortex4py.
  - **Analyse :** Cortex est livré avec plus d'une centaine d'analyseurs pour des services populaires tels que VirusTotal, Joe Sandbox, DomainTools, PassiveTotal, Google Safe Browsing, Shodan et Onyphe. Identifiez les contacts abusifs, analysez les fichiers dans plusieurs formats tels que OLE et OpenXML pour détecter les macros VBA, générez des informations utiles sur PE, fichiers PDF et bien plus encore. Les analyseurs de cortex peuvent également être interrogés à partir du MISP pour enrichir les événements et étendre la couverture de vos investigations.

Figure 26: Cortex

MISP (Malware Information Sharing Platform) est une plate-forme open source pour la collecte, le stockage, la distribution et le partage d'indicateurs et de menaces de cybersécurité concernant l'analyse des incidents de cybersécurité et l'analyse des malwares. Le MISP est conçu par et pour les analystes d'incidents, les professionnels de la sécurité et des TIC ou les inverseurs de logiciels malveillants afin de prendre en charge leurs opérations quotidiennes et de partager efficacement des informations structurées. MISP fournit des fonctionnalités pour supporter l'échange d'informations mais aussi la consommation de ces informations par les Systèmes de Détection d'Intrusion Réseau (NIDS), NIDS et avec les outils d'analyse de logs et les SIEM.

✓ **Quelques fonctionnalités de base :**

- Une base de données IOC et d'indicateurs efficace permettant de stocker des informations techniques et non techniques sur les échantillons de malwares, les incidents, les attaquants et les renseignements.
- Corrélation automatique pour trouver des relations entre les attributs et les indicateurs des programmes malveillants, des campagnes d'attaque ou des analyses. Le moteur de corrélation inclut la corrélation entre les attributs et des corrélations plus avancées comme la corrélation de hachage flou (par exemple ssdeep) ou la correspondance de blocs CIDR.
- Un modèle de données flexible dans lequel des objets complexes peuvent être exprimés et liés entre eux pour exprimer des informations sur les menaces, des incidents ou des éléments collectés.
- Une interface utilisateur intuitive pour créer, mettre à jour et collaborer sur des événements et des attributs / indicateurs. Une interface graphique pour naviguer de

manière transparente entre les événements et leurs corrélations. Une fonctionnalité de graphique d'événements pour créer et afficher des relations entre les objets et les attributs. Fonctionnalités de filtrage avancées et listes d'avertissement pour aider les analystes à contribuer sur des événements et sur des attributs et limiter le risque de faux positifs.

- Stockage des données dans un format structuré (permettant une utilisation automatisée de la base de données à des fins diverses) avec un support étendu d'indicateurs de cybersécurité ainsi que d'indicateurs de fraude comme dans le secteur financier.
- Partage de données : échangez et synchronisez automatiquement avec d'autres parties et groupes de confiance à l'aide du MISP.
- Délégation de partage : permet à un mécanisme pseudo-anonyme simple de déléguer la publication d'événement / d'indicateurs à une autre organisation.

Figure 27: MISP

En étudiant les différentes solutions ci-dessus nous constatons que :

Cyphon est une solution open-source et gratuit mais son installation nécessite l'utilisation des Docker ce qui constitue une autre charge de travail. Nous avons constaté que Cyphon ne peut pas être intégré à notre solution de SIEM ce qui est un frein pour notre projet puis qu'on ne pourra pas centraliser la gestion des incidents.

TheHive-project est un excellent outil de gestion des incidents, il est open-source et gratuit. Il est facilement intégrable à notre solution de SIEM et son déploiement est facile. Si l'on ajout la plate-forme MISP nous obtenons une solution complète de gestion des incidents.

Donc nous retenons les outils TheHive / Cortes et MISP pour la gestion des incidents.

4.6. Protection des applications web contre les cyberattaques WAF :

Un Web Application Firewall (WAF) protège le serveur d'applications Web dans le backend des multiples attaques (phishing, ransomware, attaque DDOS, malware). La fonction du WAF est de garantir la sécurité du serveur Web en analysant les paquets de requête HTTP / HTTPS et les modèles de trafic. WAF examine chaque demande envoyée au serveur, avant qu'elle n'atteigne l'application, de manière à vérifier que cette demande soit en conformité avec les règles du pare-feu. Un WAF est une protection du protocole de la couche 7 (dans le modèle OSI) et n'est pas conçu pour défendre contre tous les types d'attaques. Cette méthode d'atténuation des attaques fait généralement partie d'une suite d'outils qui forment une défense holistique contre une variété de vecteurs d'attaque. En déployant un WAF devant une application web, un bouclier est placé entre l'application web et Internet. Un serveur proxy protège l'identité d'une machine client en utilisant un intermédiaire ; un WAF est un type de proxy inversé qui protège le serveur en faisant passer les clients par le WAF avant d'atteindre le serveur.

Un WAF suit un ensemble de règles souvent appelé politiques. Ces politiques visent à se protéger des vulnérabilités dans l'application en filtrant le trafic malveillant. La valeur d'un WAF provient en partie de la rapidité et de la facilité avec laquelle la modification de politique peut être appliquée, permettant une réponse plus rapide aux différents vecteurs d'attaque. Lors d'une attaque DDoS, le mécanisme de rate limiting peut être rapidement activé en modifiant les politiques du WAF.

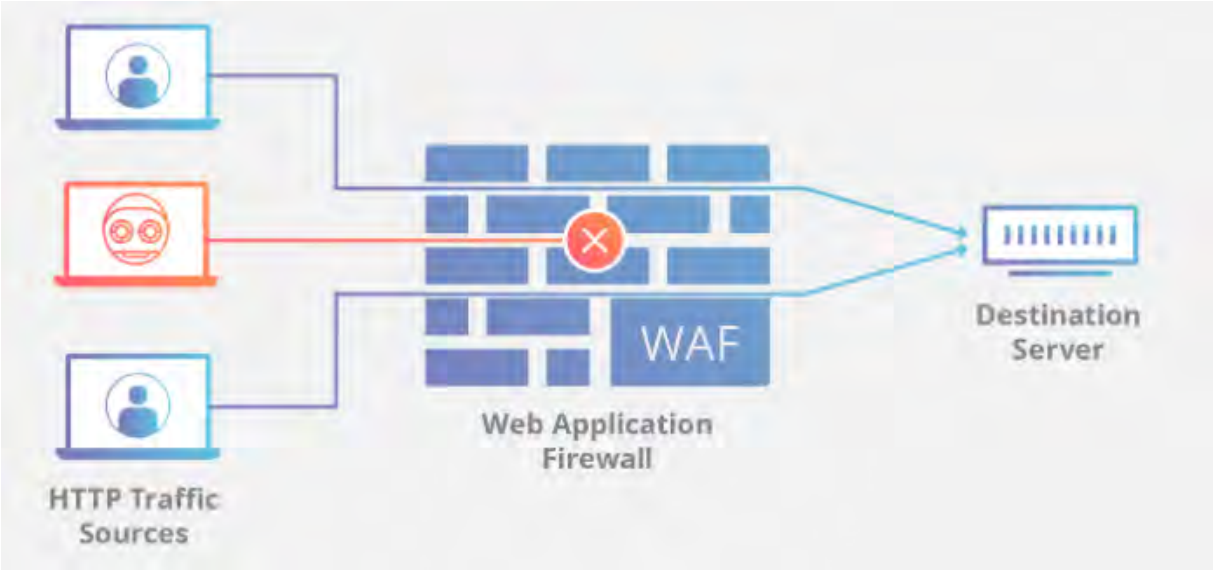


Figure 28: Architecture WAF

- ✓ **La différence entre les WAF basés sur une « liste bloquée » et sur une « liste autorisée »**

Un WAF qui fonctionne en se basant sur une liste bloquée (modèle de sécurité négative) protège contre les attaques connues. On peut comparer un WAF basé sur une liste bloquée à un videur de discothèque chargé de refuser l'accès aux clients qui ne respectent pas le code vestimentaire. À l'inverse, un WAF basé sur une liste autorisée (modèle de sécurité positive) ne laisse entrer que le trafic préalablement approuvé. On peut le comparer à un agent de sécurité à l'entrée d'une soirée privée qui ne laisse entrer que les personnes qui sont sur la liste. Les listes bloquées et approuvées ont des avantages et des inconvénients, c'est pourquoi de nombreux WAF offrent un modèle de sécurité hybride qui utilise les deux listes.

- ✓ **Les WAF basés sur le réseau, sur l'hôte et sur le cloud**

Un WAF peut être mis en place de trois façons différentes, chacune ayant ses propres avantages et inconvénients :

- **Un WAF basé sur le réseau** est généralement matériel. Installés au niveau local, les WAF basés sur le réseau réduisent la latence mais représentent l'option la plus coûteuse. Ils nécessitent de l'espace et la maintenance des équipements physiques.
- **Un WAF basé sur l'hôte** peut être entièrement intégré dans le logiciel d'une application. Cette solution est moins coûteuse qu'un WAF basé sur le réseau et offre plus de possibilités de personnalisation. L'inconvénient d'un WAF basé sur l'hôte est la consommation des ressources du serveur local, la complexité de la mise en œuvre et les coûts de maintenance. Ces composants nécessitent généralement du temps d'ingénierie et peuvent s'avérer coûteux.
- **Les WAF basés sur le cloud** offrent une alternative abordable et très facile à mettre en œuvre ; généralement, ils proposent une installation clé en main aussi simple qu'un changement de DNS pour rediriger le trafic. Les WAF basés sur le cloud ont également un coût initial minimal, car les utilisateurs paient tous les mois ou tous les ans pour la sécurité en tant que service. Les WAF basés sur le cloud peuvent également offrir une solution continuellement mise à jour pour se protéger contre les menaces les plus récentes sans aucun travail ni coût supplémentaire pour l'utilisateur. L'inconvénient d'un WAF basé sur le cloud tient au fait que les utilisateurs transfèrent la responsabilité à un tiers, par conséquent, certaines de ses fonctionnalités peuvent constituer une zone d'ombre pour eux.

4.6.1. FortiWeb :

Les WAF FortiWeb fournissent des fonctionnalités avancées qui protègent vos applications Web et vos API contre les menaces connues et zero-day. En utilisant une approche multicouche avancée, FortiWeb protège contre le Top 10 OWASP et plus. FortiWeb ML personnalise la protection de chaque application, offrant une protection robuste sans nécessiter le réglage manuel fastidieux requis par d'autres solutions. Avec le ML, FortiWeb identifie les comportements anormaux et plus encore, fait la distinction entre les anomalies malveillantes et bénignes. La solution offre également de solides capacités d'atténuation des bots, permettant aux bots bénins de se connecter (par exemple les moteurs de recherche) tout en bloquant l'activité des bots malveillants.

FortiWeb propose des options de déploiement qui peuvent protéger les applications d'entreprise, quel que soit l'endroit où l'application est hébergée. Les options incluent des appliances matérielles, des machines virtuelles et des conteneurs qui peuvent être déployés dans le centre de données, dans des environnements cloud ou dans la solution SaaS cloud native, FortiWeb Cloud WAF as a Service.

- ✓ **Les services de FortiWeb :**

FortiWeb utilise plusieurs services de sécurité FortiGuard pour protéger les applications Web contre les attaques. Ces abonnements annuels peuvent être achetés à la carte ou dans le cadre d'un forfait avec votre solution FortiWeb.

- **Sécurité des applications Web** : FortiGuard Web Application Security utilise des informations basées sur les dernières vulnérabilités des applications, les bots, les modèles d'URL et de types de données suspects, ainsi que les moteurs de détection heuristique spécialisés, pour garantir que vos applications Web restent à l'abri des menaces de la couche application.
- **Réputation IP et sécurité anti-botnet :** Le service FortiGuard IP Reputation regroupe les données IP sources malveillantes du réseau distribué Fortinet de capteurs de menaces, de CERT, de MITRE, de concurrents coopératifs et d'autres sources mondiales qui collaborent pour fournir des informations à jour sur les menaces sur les sources hostiles. L'intelligence quasiment en temps réel des passerelles réseau distribuées, combinée à la recherche de classe mondiale de

FortiGuard Labs, aide les entreprises à rester plus sûres et à bloquer les attaques de manière proactive.

- **Antivirus :** FortiGuard Antivirus protège contre les derniers virus, logiciels espions et autres menaces au niveau du contenu. Il utilise des moteurs de détection avancés de pointe pour empêcher les nouvelles menaces de s'implanter dans votre réseau et d'accéder à votre contenu inestimable.
- **FortiSandbox Cloud** : FortiSandbox Cloud Service est une solution avancée de détection des menaces qui effectue une analyse dynamique pour identifier des logiciels malveillants jusque-là inconnus. Les informations exploitables générées par FortiSandbox Cloud sont réinjectées dans les contrôles préventifs au sein de votre réseau, ce qui désarme la menace.
- **Défense de bourrage d'informations d'identification :** Credential Stuffing Defense de Fortinet identifie les tentatives de connexion à l'aide des informations d'identification qui ont été compromises en utilisant un flux toujours à jour d'informations d'identification volées. Les administrateurs peuvent configurer leurs appareils pris en charge.

4.6.2. Imperva :

Les attaques d'applications Web empêchent les transactions importantes et volent des données sensibles. Imperva Web Application Firewall (WAF) analyse le trafic vers vos applications pour arrêter ces attaques et garantir des opérations commerciales ininterrompues. Imperva WAF est un composant clé d'une pile complète d'applications Web et de protection API (WAAP) qui sécurise de la périphérie à la base de données, de sorte que le trafic que vous recevez est uniquement le trafic que vous souhaitez. Imperva WAF offre une sécurité automatisée conforme à la norme PCI qui intègre des analyses pour aller au-delà de la couverture du Top 10 OWASP et réduit les risques créés par le code tiers.

Vous pouvez utiliser Imperva WAF pour sécuriser :

- Applications actives et héritées ;
- Applications tierces ;
- API et microservices ;
- Applications cloud, conteneurs, VM et plus.

Déployez Imperva WAF sur site, dans AWS et Azure, ou en tant que service cloud. Sécurisez facilement chaque application tout en répondant à son exigence de niveau de service spécifique.

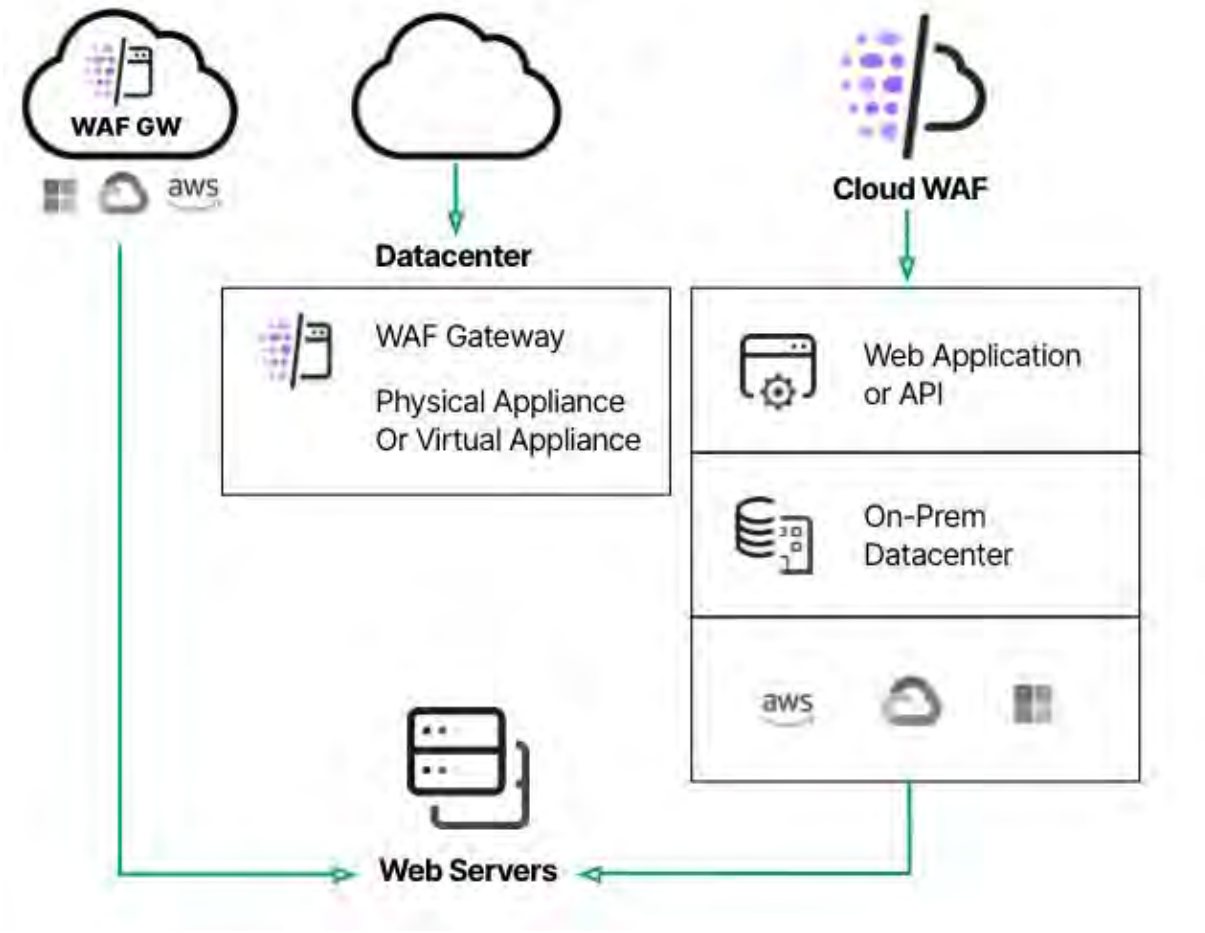


Figure 29: Déploiement Imperva

Par comparaison, nous constatons que tous les deux solutions répondent efficacement au besoin de sécurité d'une application web. Elles proposent des services adapter à nos besoins. Toutefois, pour des contraintes de ressources nous ne disposons que de la solution FortiWeb donc c'est cette solution qui sera mise en place dans le cadre de notre projet.

Partie III : Implémentation

Chapitre 5 : Implémentation des solutions retenues

Au terme de notre étude, nous avons eu à choisir les solutions à implémentées dans le cadre de notre projet. Pour mener à bien cette implémentation nous allons nous baser sur l'architecture suivante.

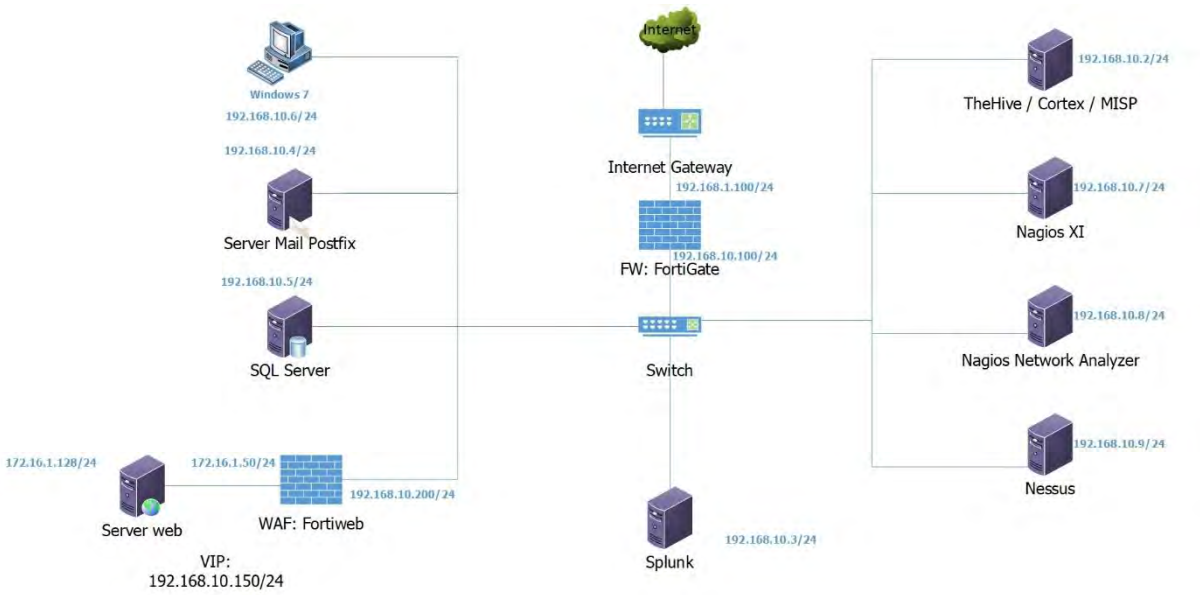


Figure 30: Architecture proposée

Les outils nécessaires à la mise en place de notre CERT :

- **Nagios Network Analyzer :** cet outil nous permettra d'analyser et de surveiller l'utilisation de la bande passante. Afin d'avoir un aperçu sur les sources du trafic réseau.
- **Nagios XI :** nous permettra de surveille la disponibilité des services réseaux.
- **Nessus :** nous permettra d'avoir une gestion centraliser de l'ensemble des vulnérabilités sur le réseau.
- **Splunk :** une centralisation de l'ensemble des évènements des composantes du réseau à des fins de corrélation, d'analyse des évènements de sécurité et de prise de décision.
- **TheHive / Cortex / MISP :** ces outils permettent de gérer les incidents de sécurité de la création de ticket pour un incident jusqu'à sa clôture.
- **FortiWeb :** firewall applicatif permettant de sécuriser notre application web.

5.1. Installation et configuration d'une plateforme de NetFlow :

✓ Pré-requis :

Système : Ubuntu server 20.04 LTS

Processeur : 2 core

Mémoire RAM : 1GB

Mémoire Disque : 20GB

Nous avons téléchargé le package de Nagios Network Analyzer (NA) sur le site officiel de Nagios.

Après téléchargement du package, nous allons le dézippé et lancer le fichier fullinstall

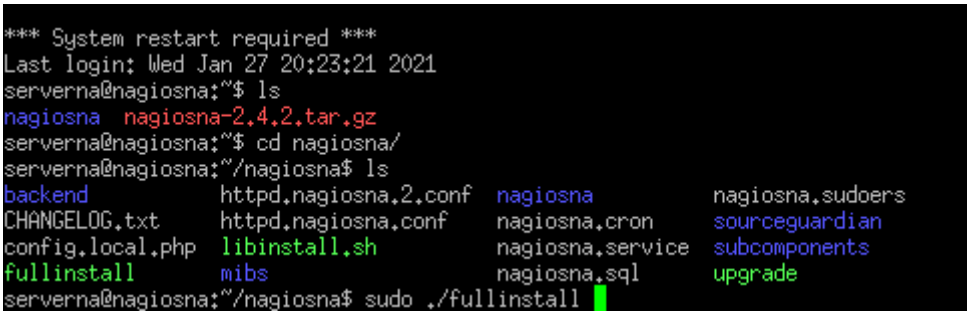


Figure 31: Installation de Nagios Network Analyzer

Installation est terminée avec succès

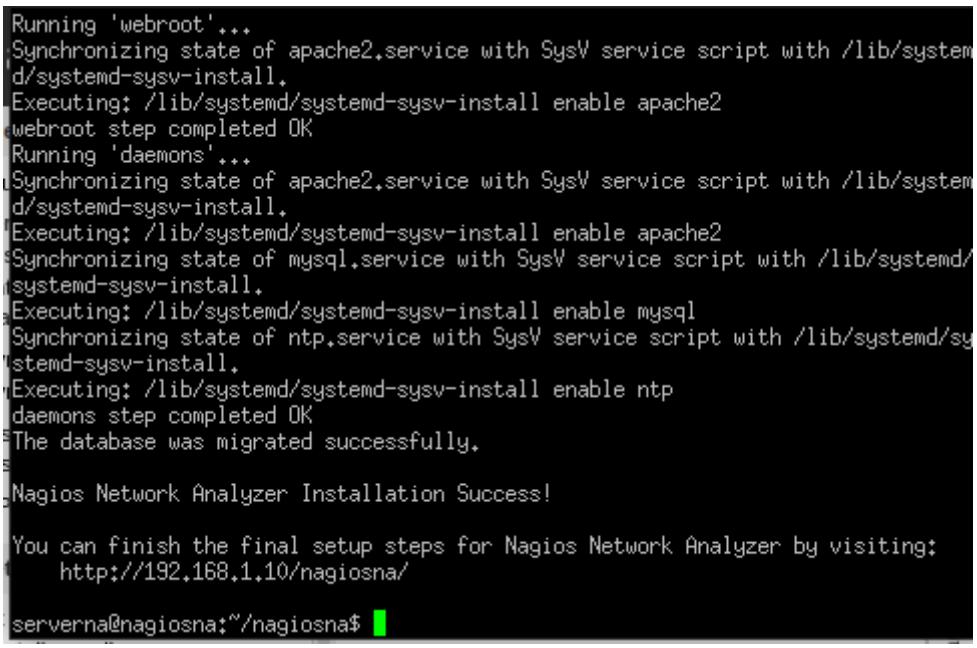


Figure 32: Nagios NA installer avec succès

Nous allons passer à la configuration de Nagios Network Analyzer

Nous finalisons l'installation en configurant les paramètres de connexion.

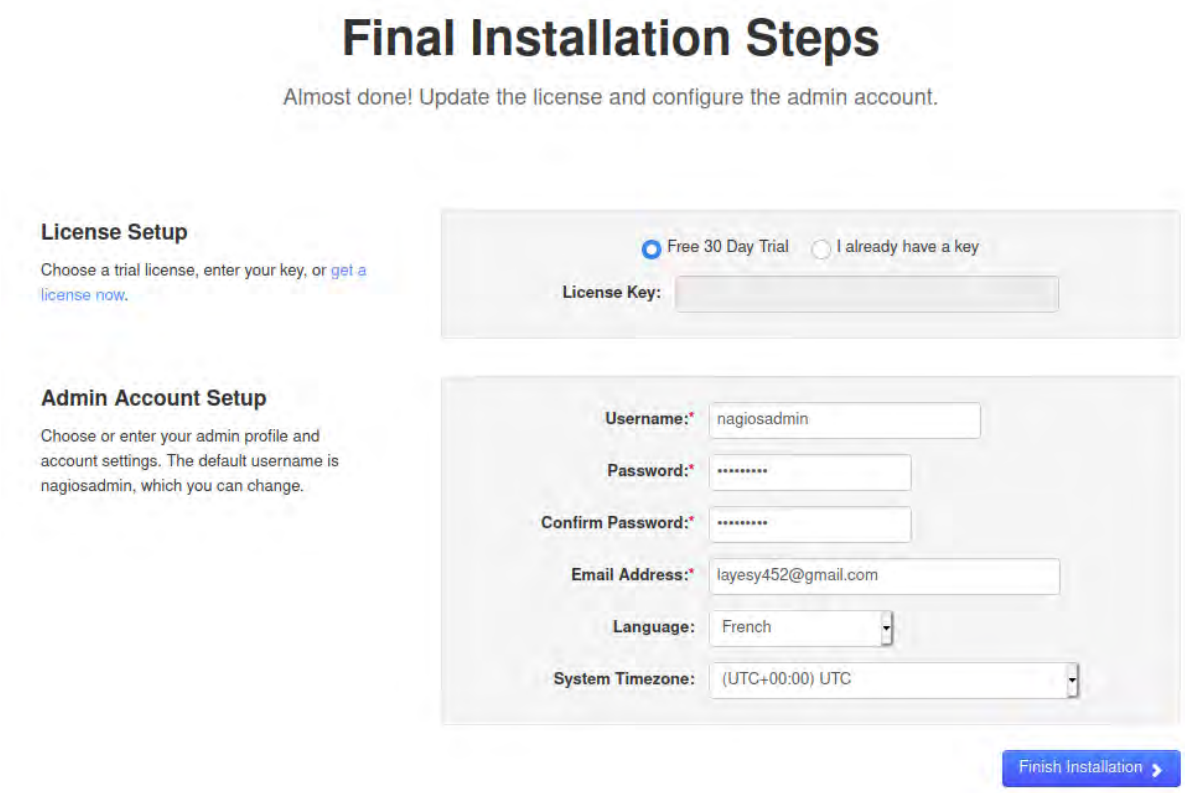


Figure 33: Configuration d'utilisateur de Nagios NA

Nous allons maintenant configurer notre Nagios NA en créant une source de données ce qui va nous permettre d'avoir un aperçu sur l'utilisation de la bande passante. Dans notre cas le collecteur va recueillir les données au niveau du firewall FortiGate.

Configuration coté firewall :

System config NetFlow

Set collector-ip 192.168.10.8

Set collector-port 2055

End

Activation de NetFlow au niveau de l'interface

Config system interface

Edit port 1

Set NetFlow-sampler both

End

Configuration coté Nagios NA

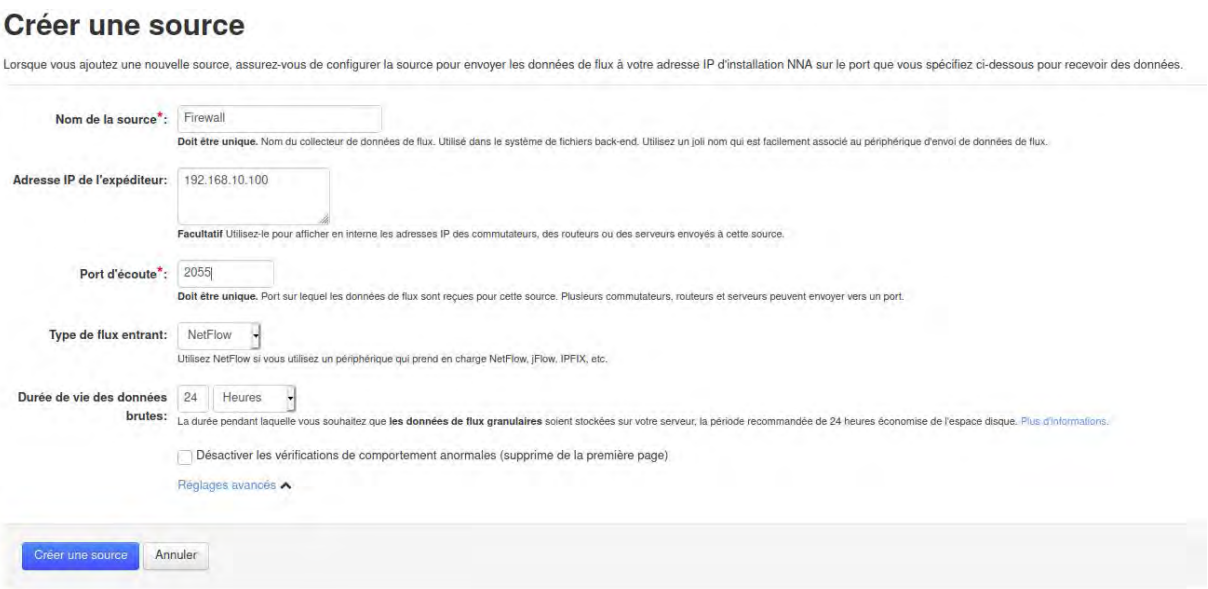


Figure 34: Création de la source de données

Visualisation des données au niveau de Nagios NA

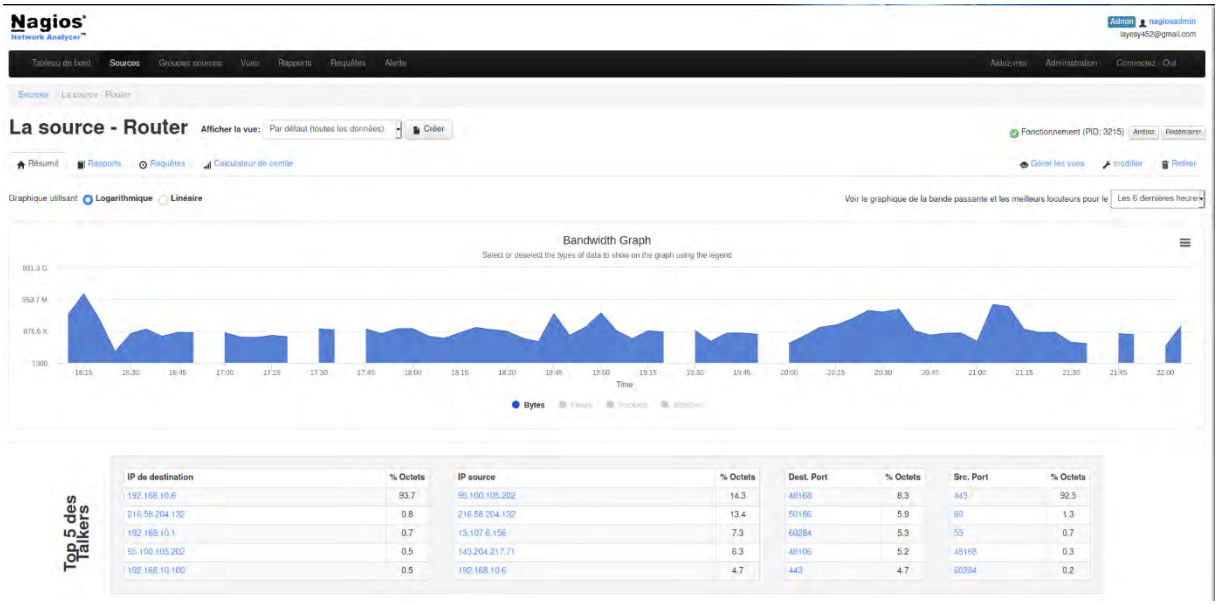


Figure 35: Visualisation des données

Rapport détaillé du trafic réseau

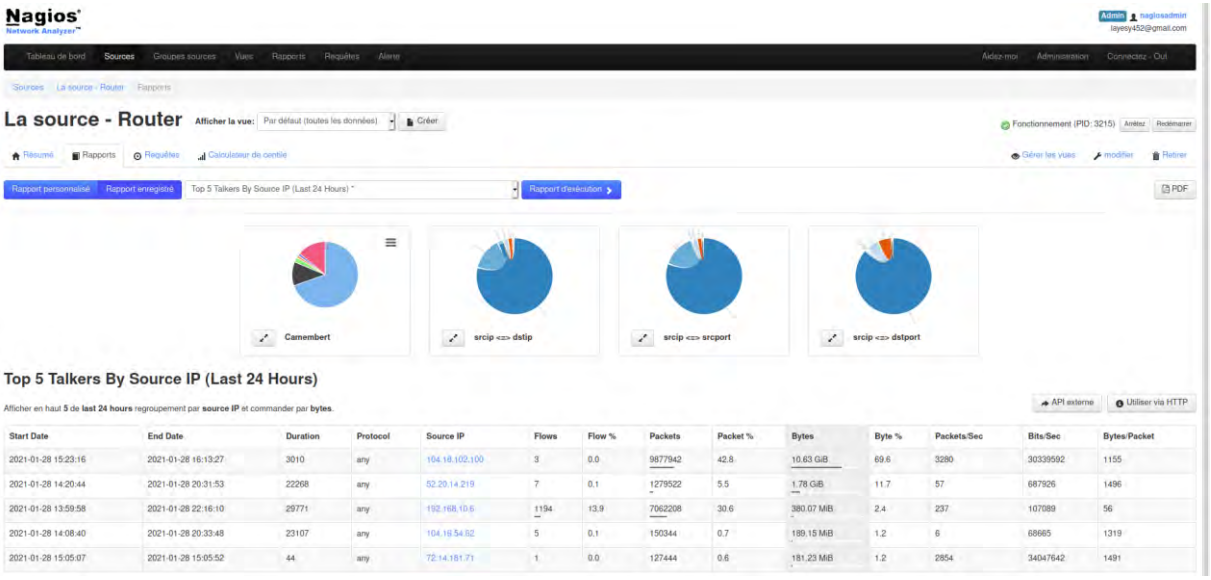


Figure 36: Rapport détail

5.2. Installation et configuration d'une plateforme NMS :

✓ Pré-requis :

Système : Ubuntu server 20.04 LTS

Processeur : 1 GHz

Mémoire RAM : 1GB

Mémoire Disque : 20GB

Nous avons téléchargé le package de Nagios XI sur le site officiel de Nagios.

Nous allons installer Nagios XI au niveau de notre serveur Ubuntu.

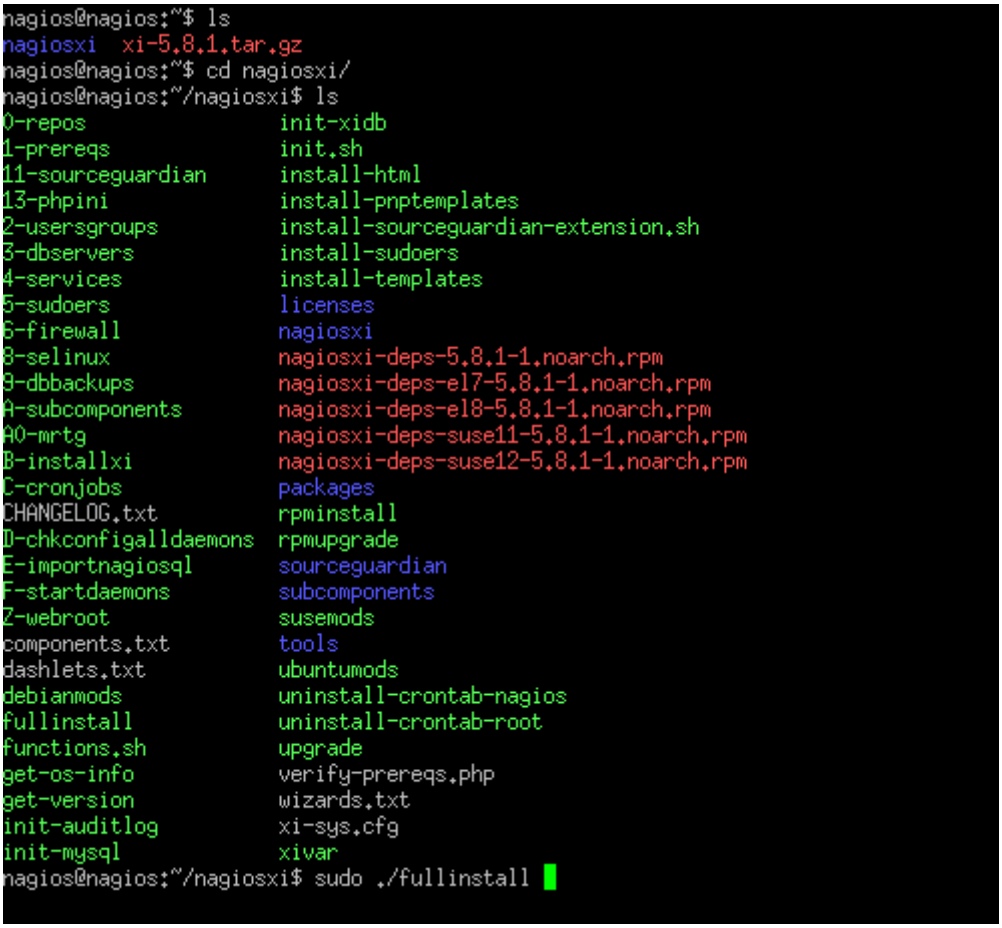


Figure 37: Installation de Nagios XI

Nous lançons l'installation avec le fichier fullinstall.

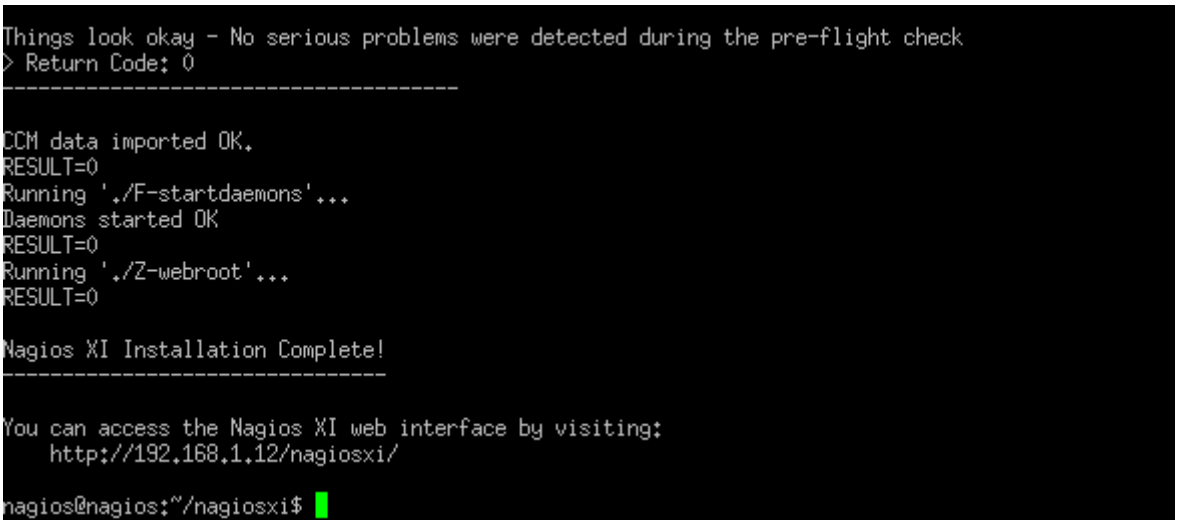


Figure 38: Installation complète

L'installation s'est terminé avec succès.

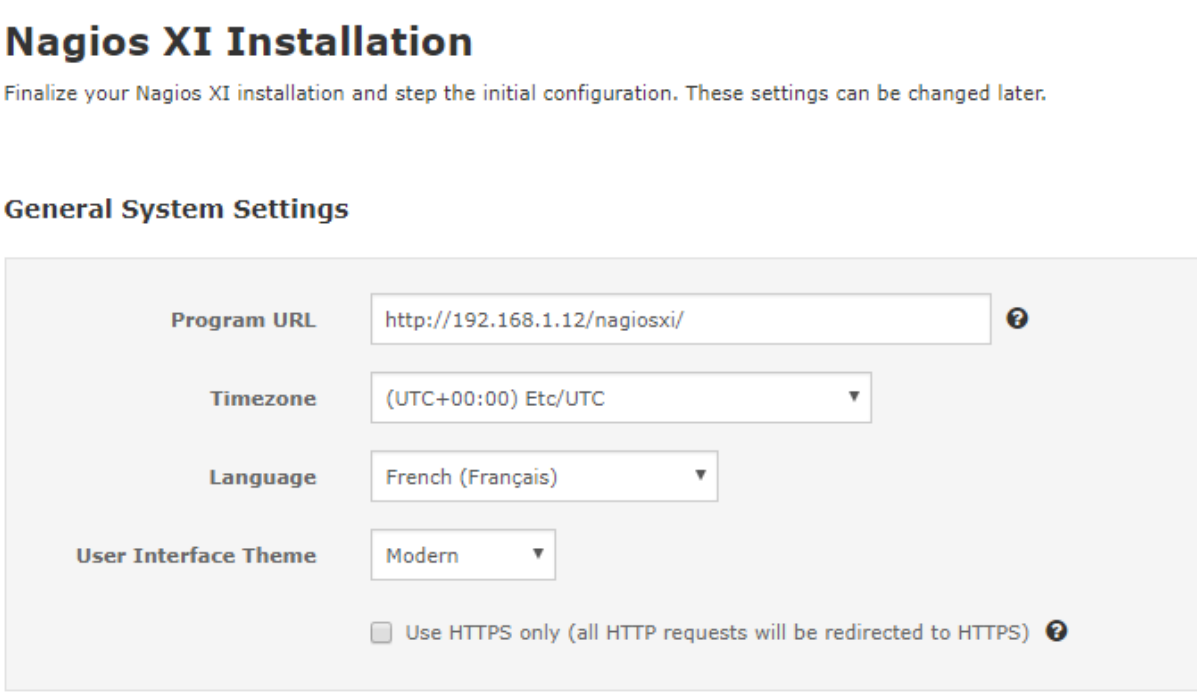


Figure 39: Paramétrage de Nagios XI

Nous finalisons l'installation via l'interface web.

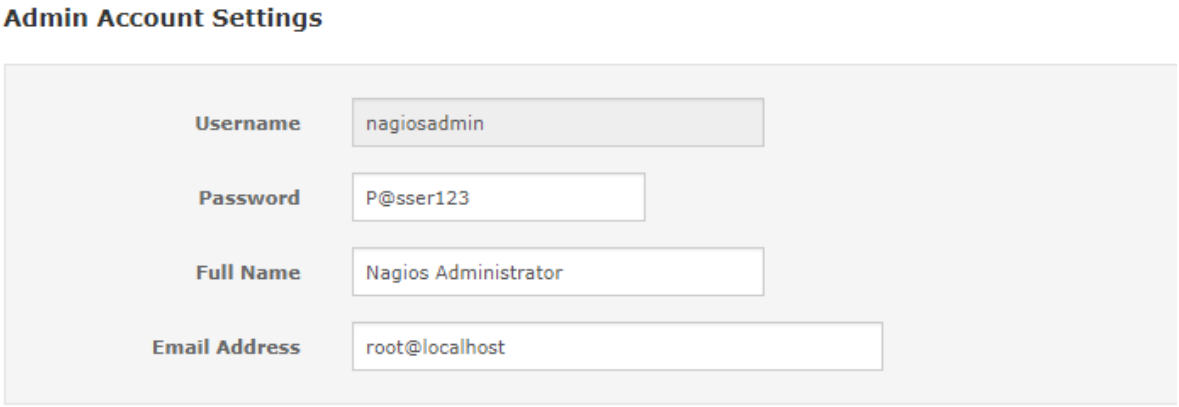


Figure 40: Ajout de l'utilisateur

Nous allons superviser les services web, SQL server et messagerie. Par la même occasion intégré notre Nagios Network Analyzer à Nagios XI et superviser une machine Windows et une machine linux.

- Intégration de Nagios Network Analyzer à Nagios XI

Pour pouvoir intégrer Nagios NA à Nagios XI on renseigne un nom, l'adresse IP de Nagios NA ainsi que la clef API de Nagios NA.

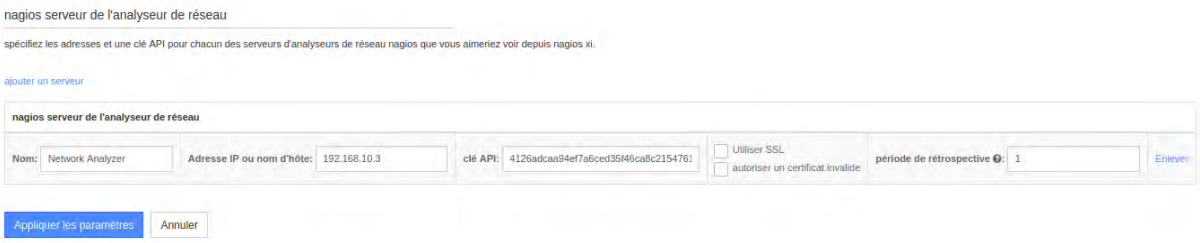


Figure 41: Intégration de Nagios NA à Nagios XI

En intégrant Nagios NA à Nagios XI les données de chaque hôte remontent au niveau de Nagios XI.

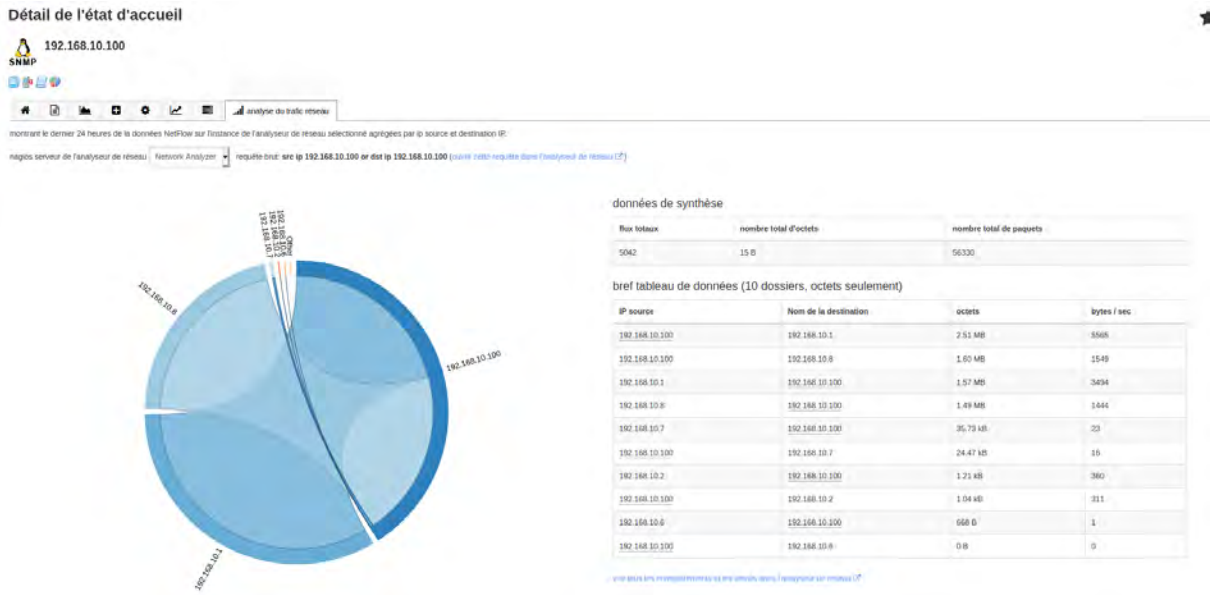


Figure 42: Analyse du trafic réseau

- Supervision du service du SQL server

Figure 43: Configuration de SQL server

Nous allons visualiser la carte de l'ensemble des services supervisés.

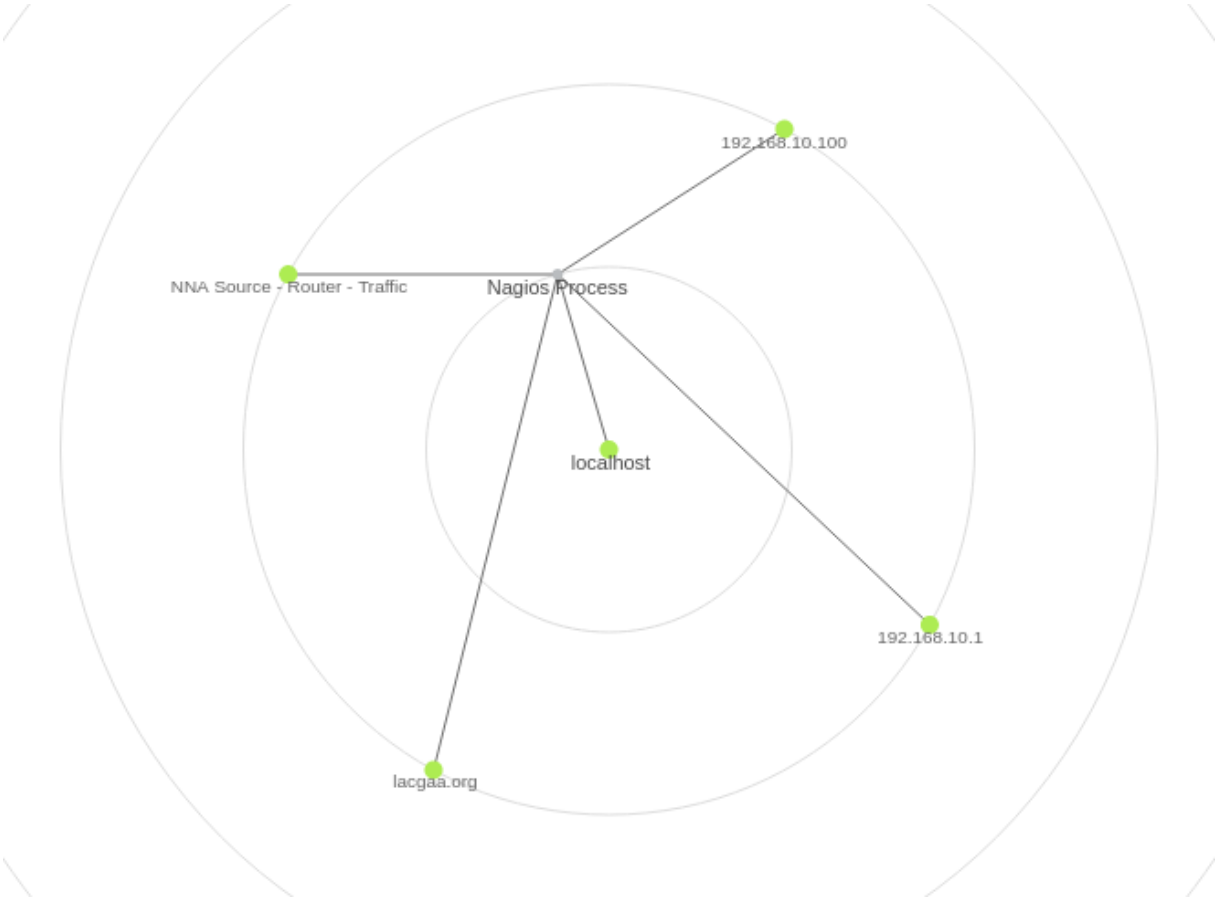


Figure 44: Carte des services supervisés

5.3. Installation et configuration d'une plateforme de management de vulnérabilité :

La plateforme de management de vulnérabilité nous permettra de scanner notre réseau afin de détecter d'éventuelle vulnérabilité s'il y a lieu. Nous allons utiliser Nessus comme plateforme de scan de vulnérabilité.

Après téléchargement du package de Nessus sur le site officiel de tenable. Nous allons l'installer au niveau de notre machine kali linux.

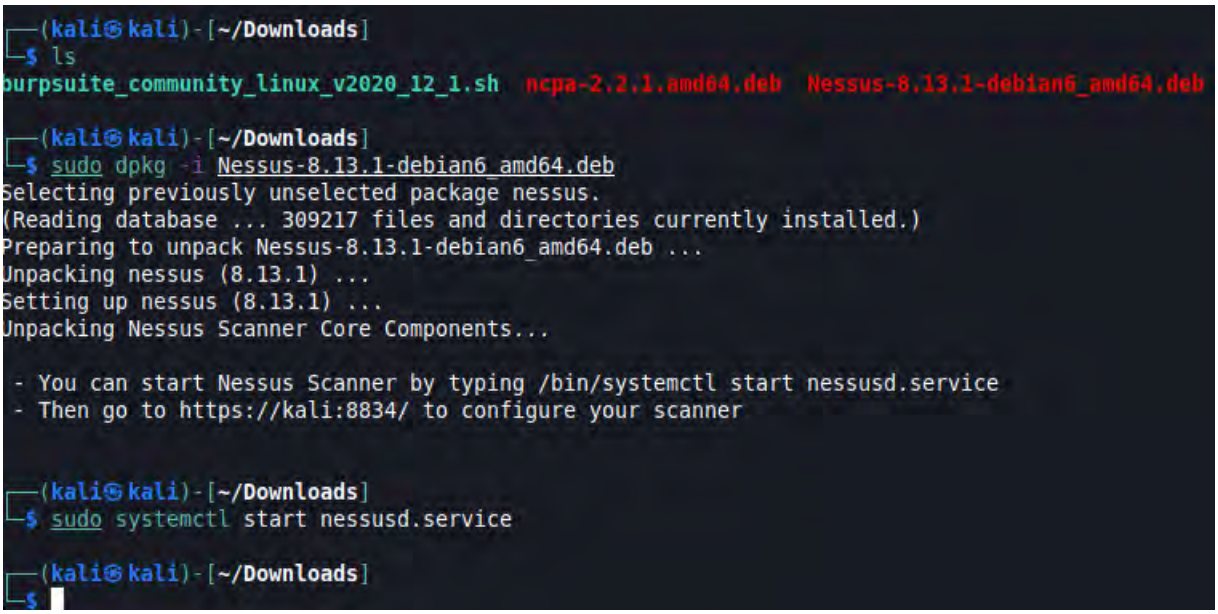


Figure 45: Installation et démarrage de Nessus

Nous allons créer un nouveau scan pour scanner notre réseau 192.168.10.0/24.

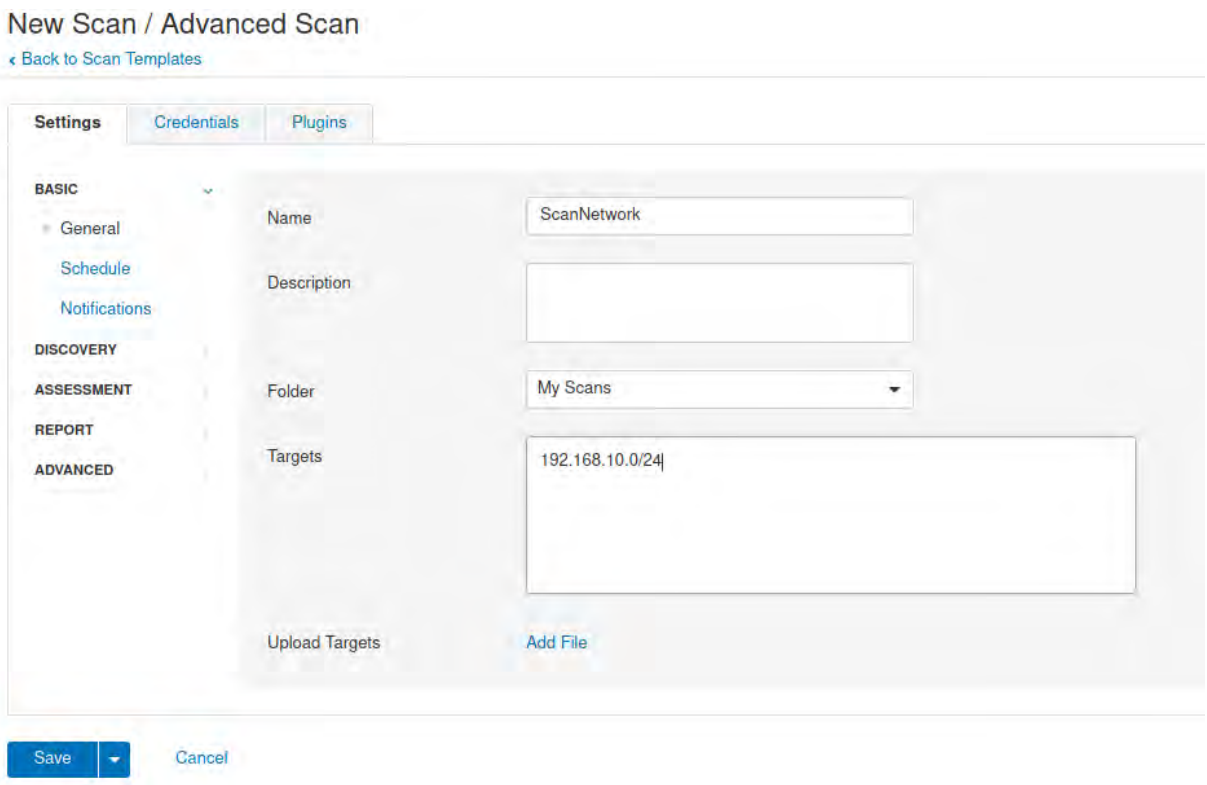


Figure 46:: Création d'un scan sur Nessus

Après avoir scanner notre réseau voici le résultat du scan.

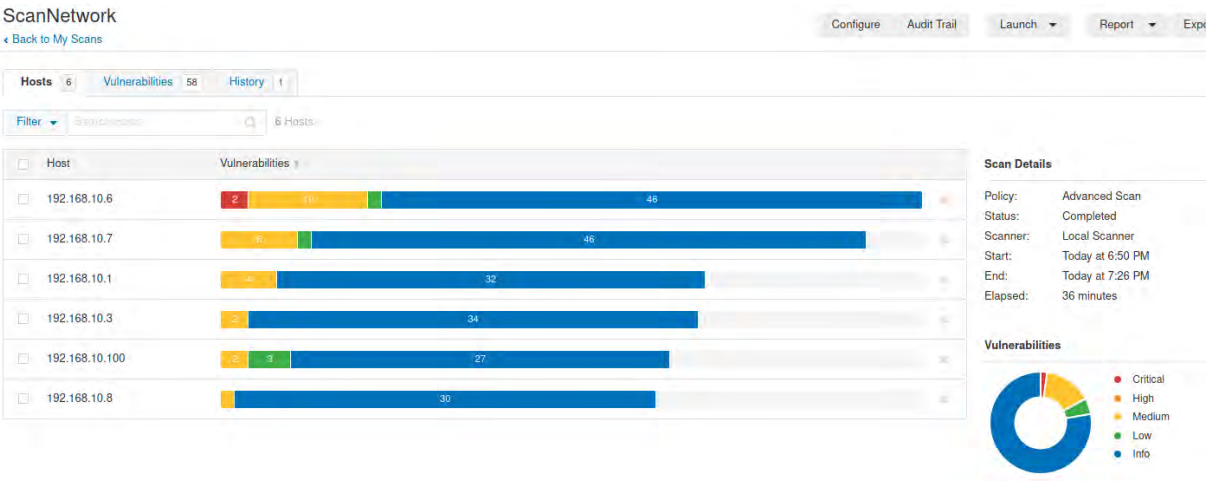


Figure 37 : Résultat du scan

5.4. Installation et configuration d'une plateforme de centralisation et d'analyse d'événement :

Une plateforme de gestion des événements centralise la collecte, le stockage et l'analyse des journaux. Il surveille les menaces de sécurité en temps réel pour détecter rapidement les

attaques, les contenir et y répondre, tout en offrant un processus global de génération de rapport sur la sécurité et de gestion de la conformité.

Pré-requis :

Système : Ubuntu server 20.04 LTS

Processeur : 1 GHz

Mémoire RAM : 1GB

Mémoire Disque : 30GB

Nous allons télécharger le paquet d'installation de Splunk sur leur site officiel.

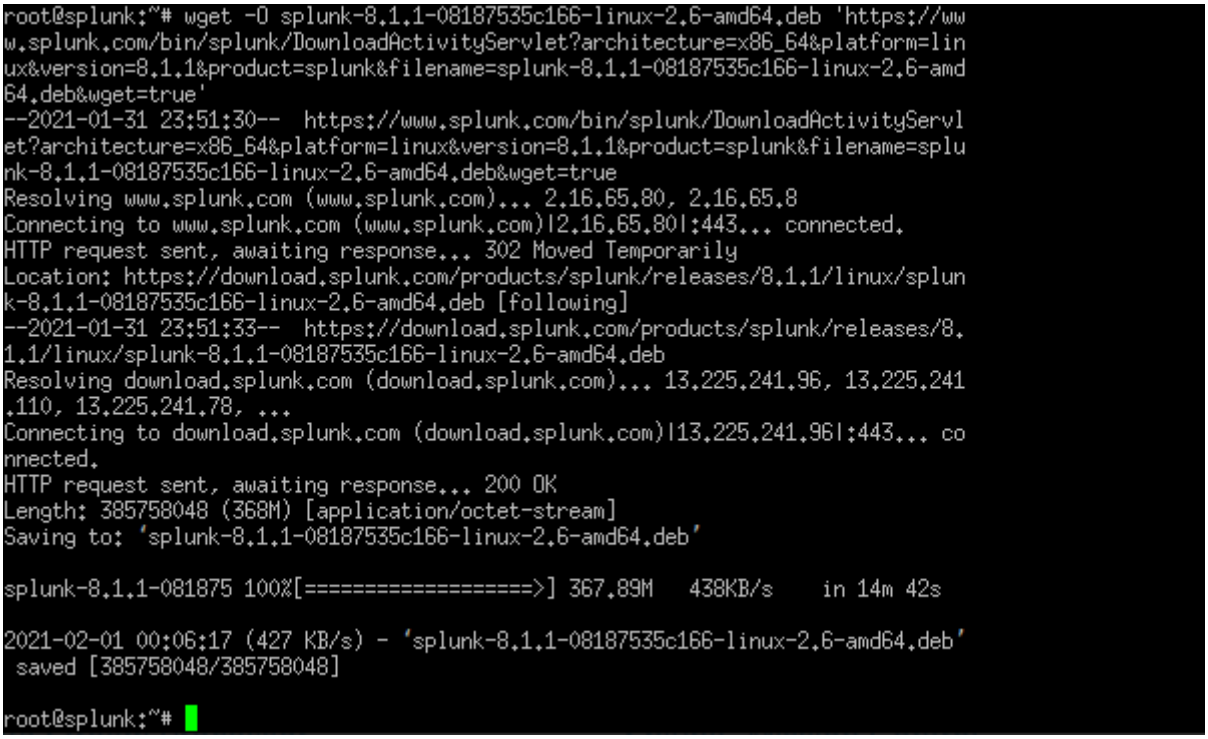


Figure 47: Téléchargement du paquet de Splunk

Nous installons Splunk en lançant la commande :

dpkg –i splunk-8.1.1-08187535c166-linux-2.6-amd64.deb

A la fin de l'installation l'application Splunk nous demande de renseigner un nom d'utilisateur et un mot de passe et pour pouvoir se connecté à l'interface web on utilise l'adresse IP de la machine avec le port 8000 dans notre cas ç a sera : https://192.168.10.3:8000

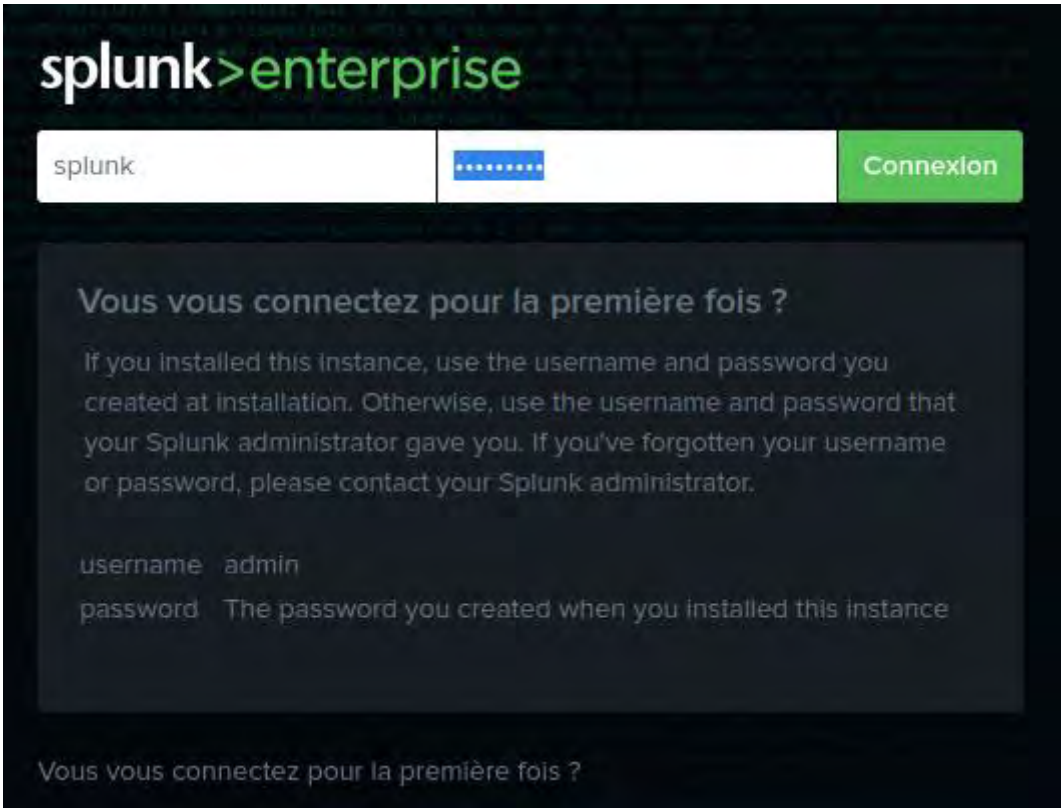


Figure 48: Page d'authentification de Splunk

Nous allons installer les applications qui nous permettrons de faire la gestion et l'analyse des événements de nos serveurs.

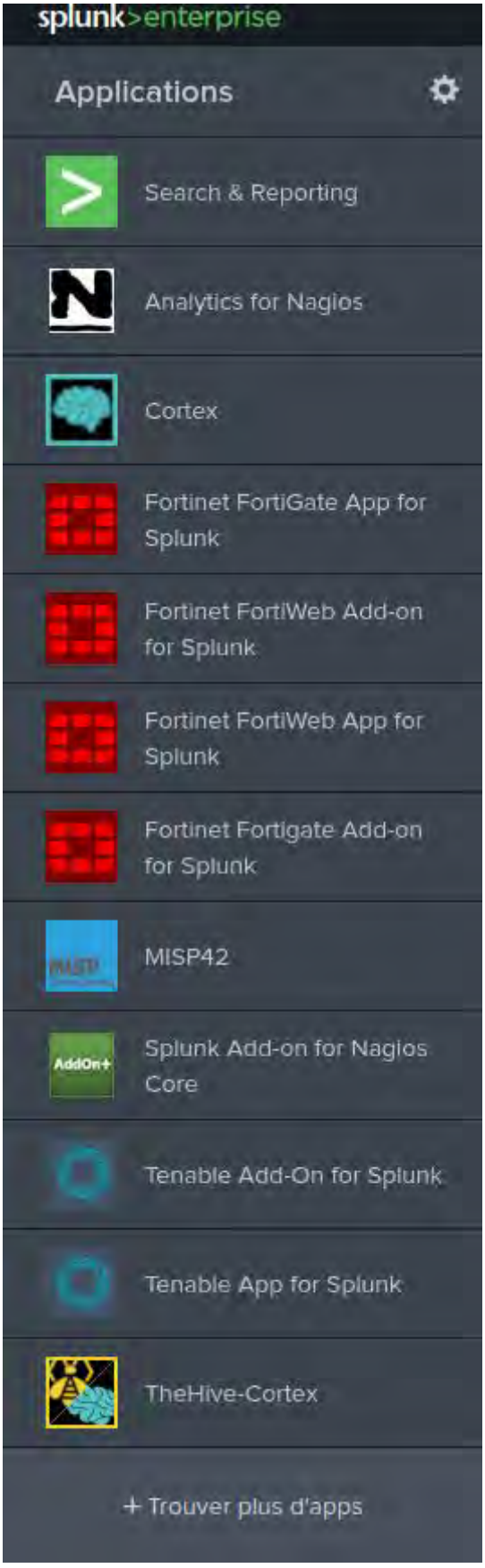


Figure 49: Les applications de Splunk

Configuration de Splunk pour recevoir les logs de Fortigate en utilisant le port 514.

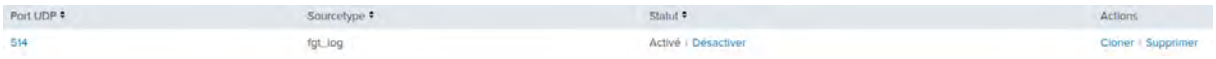


Figure 50: Configuration du port 514

Configuration de fortigate pour envoyer ces logs à Splunk. On active le protocole Syslogs au niveau du fortigate.

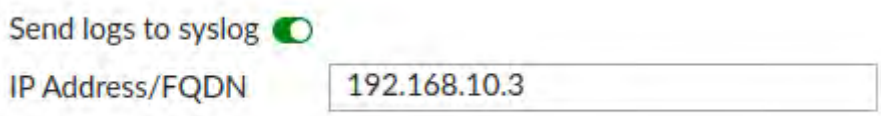


Figure 51: Activation Syslogs de Fortigate

Activation du statut de Syslogs pour qu'il envoie les données au serveur Splunk.

```
FortiGate-VM64 # config log syslogd2 setting

FortiGate-VM64 (setting) # set status enable

FortiGate-VM64 (setting) # set server 192.168.10.3

FortiGate-VM64 (setting) # end

FortiGate-VM64 #
```

Figure 52: Activation du statut Syslogs

Visualisation des événements de notre firewall fortigate :

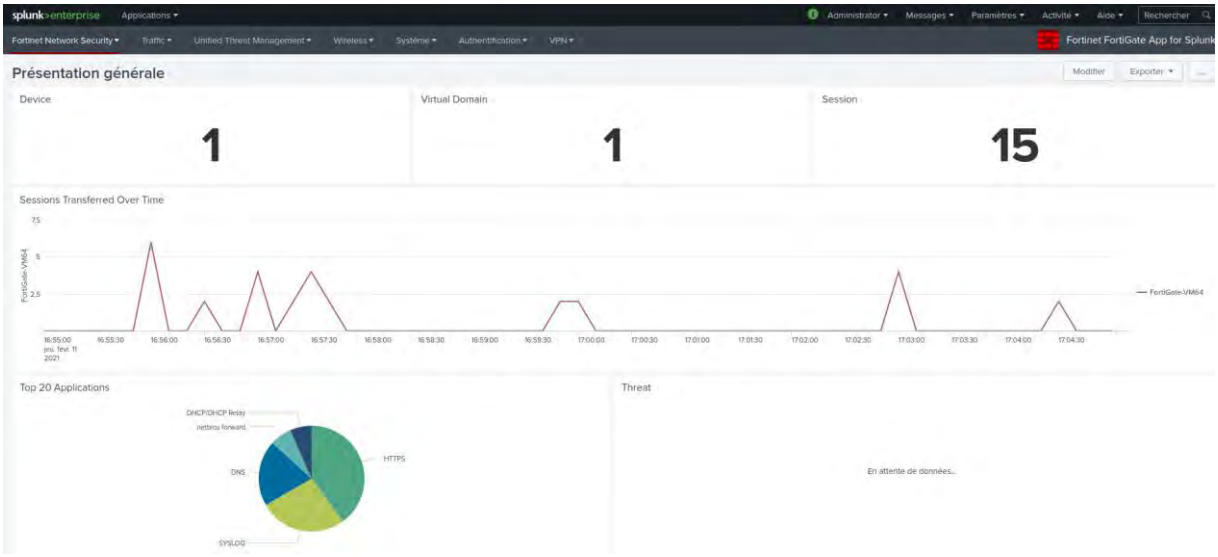


Figure 53: Evénements fortigate

5.5. Installation et configuration d'un outil de gestion des incidents de sécurité :

La plateforme de gestion des incidents de sécurité nous permettra de faire un suivi de l'ensemble des incidents qui interviendront dans notre système d'information.

Pré-requis :

Système : Ubuntu desktop 20.04 LTS

Processeur : 1 GHz

Mémoire RAM : 3GB

Mémoire Disque : 60GB

Sur cette machine nous allons installer TheHive pour la création des tickets, gestion des alertes et le suivi des incidents, Cortex pour l'analyse et la réponse aux incidents et MISP pour le partage d'information sur les incidents et la création d'événements.

Pour faire fonctionner la plateforme TheHive et Cortex nous avons besoin d'installer elasticsearch qui fera office de base de donnée.

- **Installation de Elasticsearch et TheHive :**

Ajout à notre source liste les paquets de Elasticsearch et TheHive.

Figure 54: Ajout repository

Après téléchargement des paquets nous allons lancer la commande suivante pour installer Elasticsearch :

 # apt install elasticsearch

Nous allons configurer elasticsearch en modifiant le fichier elasticsearch.yml.

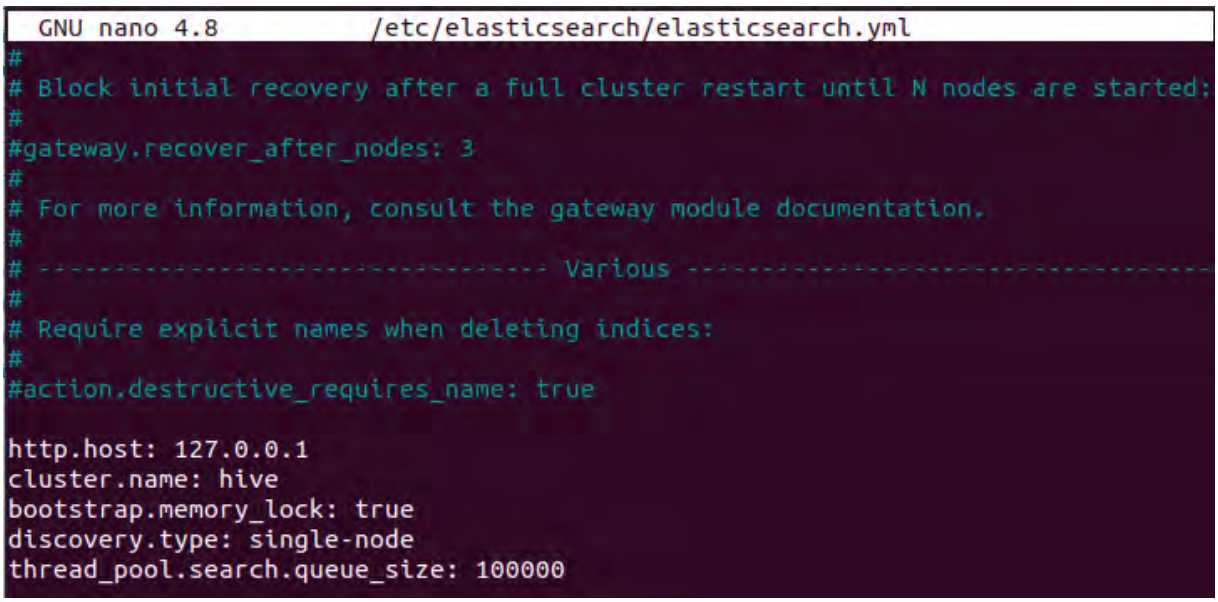


Figure 55: Configuration elasticsearch

On se connecte avec localhost sur le port 9200 pour tester le fonctionnement de elasticsearch.

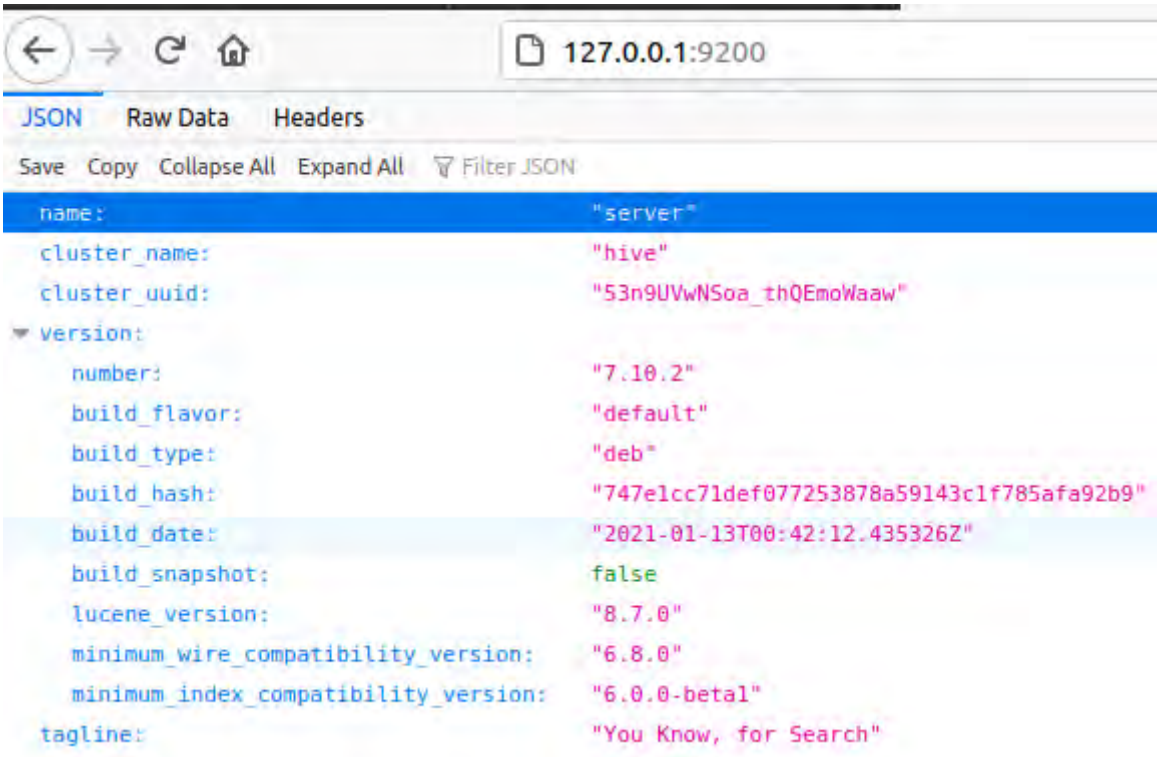


Figure 56: Connexion à elasticsearch

Après l'installation de Elasticsearch, on installe TheHive avec la commande suivante :

 # apt install thehive

Nous allons configurer TheHive en éditant le fichier application.conf. Nous générons une clef secrète aléatoire qui nous permettra de se connecter à l'interface web de TheHive avec l'adresse IP http://192.168.10.2:9000.

```
  GNU nano 4.8                /etc/thehive/application.conf
# Secret Key
# The secret key is used to secure cryptographic functions.
# WARNING: If you deploy your application on several servers, make sure to use >
play.http.secret.key="hll0XyA5886UJrroZ7htClBMTdo1BzBXvQ02ImXFPeC2AulKt6CHRlaHa>

# Elasticsearch
search {
  ## Basic configuration
  # Index name.
  index = the_hive
  # ElasticSearch instance address.
  uri = "http://127.0.0.1:9200/"

  search.ssl.enabled = false
## Advanced configuration
  # Scroll keepalive.
  #keepalive = 1m
  # Scroll page size.
  #pagesize = 50
  # Number of shards
```

Figure 57: Configuration TheHive

Création d'un compte administrateur à la première connexion.

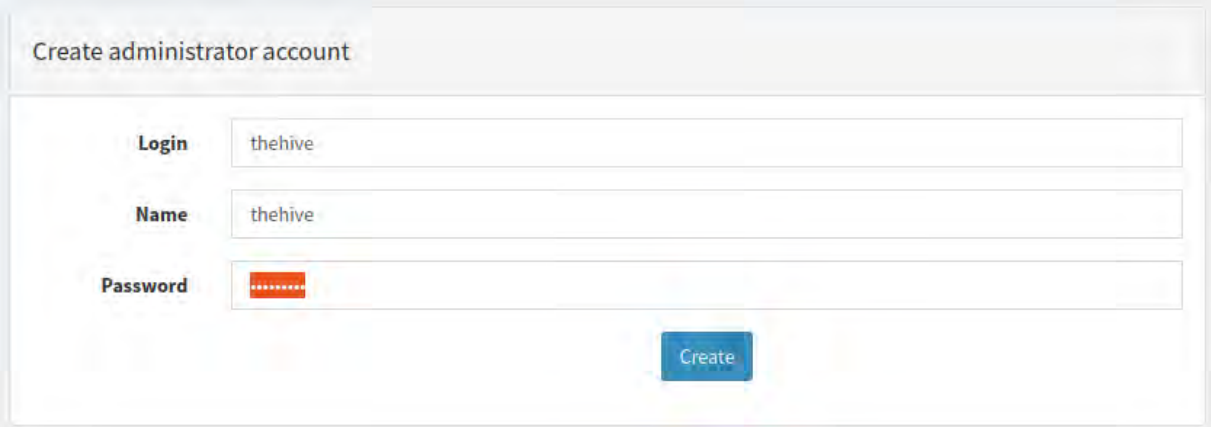


Figure 58: Création utilisateur

Connexion à l'interface web de TheHive.

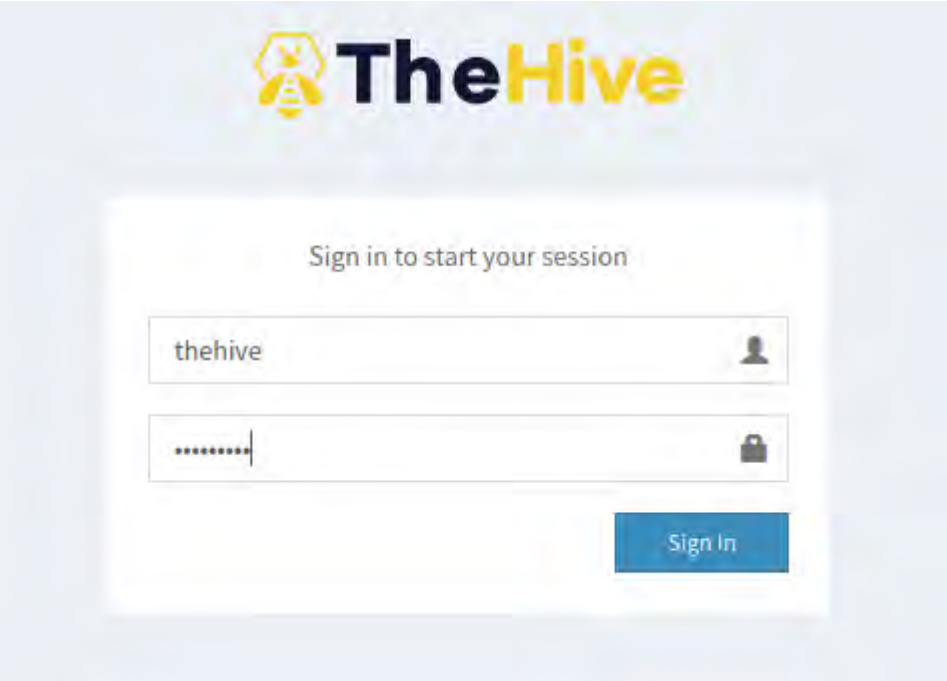


Figure 59: Connexion à TheHive

- **Installation de Cortex :**

```
server@server:~$ sudo apt install cortex
[sudo] password for server:
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  cortex
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 90,9 Mo dans les archives.
Après cette opération, 90,7 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://dl.bintray.com/thehive-project/debian-beta any/main amd6
4 cortex all 3.0.1-1 [90,9 MB]
90,9 Mo réceptionnés en 3min 17s (460 ko/s)
Sélection du paquet cortex précédemment désélectionné.
(Lecture de la base de données... 130756 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../cortex_3.0.1-1_all.deb ...
Dépaquetage de cortex (3.0.1-1) ...
Paramétrage de cortex (3.0.1-1) ...
Creating system group: cortex
Creating system user: cortex in cortex with cortex daemon-user and shell /bin/fa
lse
Traitement des actions différées (« triggers ») pour systemd (245.4-4ubuntu3.4)
...
```

Figure 60: Installation de Cortex

Après installation nous allons configurer Cortex en modifiant le fichier application.conf. Nous générons une clef secrète aléatoire qui nous permettra de se connecter à l'interface web de Cortex avec l'adresse IP http://192.168.10.2:90001.

```
  GNU nano 4.8                  /etc/cortex/application.conf
# Sample Cortex application.conf file

## SECRET KEY
#
# The secret key is used to secure cryptographic functions.
#
# IMPORTANT: If you deploy your application to several  instances,  make
# sure to use the same key.
play.http.secret.key="GCQzPwkhS5npW25FmKFxoW4QK95MWlUAUfdICtcwXjOjMGzs4jSXGBKgi>

## ElasticSearch
search {
  # Name of the index
  index = cortex
  # ElasticSearch instance address.
  # For cluster, join address:port with ',': "http://ip1:9200,ip2:9200,ip3:9200"
  uri = "http://127.0.0.1:9200"
```

Figure 61: Configuration de Cortex

Nous allons créer un utilisateur qui sera l'administrateur de Cortex.

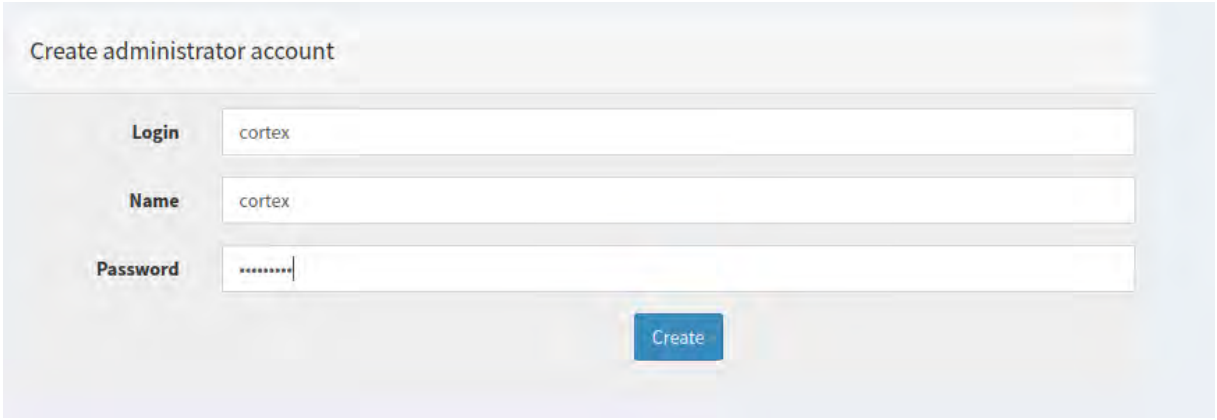


Figure 62: Création utilisateur

Cortex nous propose de créer une organisation à la première connexion.

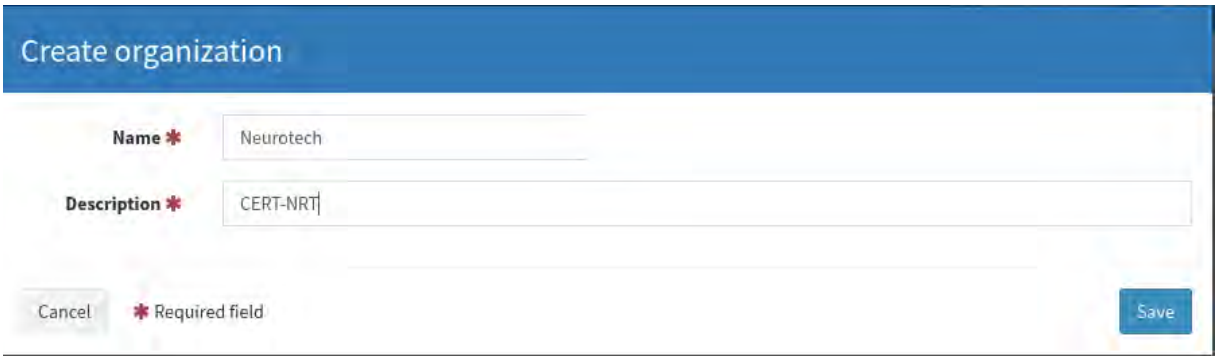


Figure 63: Création d'une organisation

Pour que Cortex fonctionne correctement nous devons l'intégrer à TheHive et à Cortex-Analyzers et au Répondeur.

Intégration de Cortex à TheHive, au niveau du fichier de configuration de TheHive application.conf. Nous allons décommenter ces lignes en ajoutant l'adresse IP de Cortex et son port et utiliser une clef API d'un utilisateur de Cortex qui a les droits d'écriture, de lecture et d'exécution.

```
play.modules.enabled += connectors.cortex.CortexConnector

cortex {
   "CORTEX-SERVER-ID" {
     url = "http://192.168.10.2:9001"
     key = "mCvoNlUg1Qr4qpjuvSkTfZ/6UWGEsJ0e"
  #  # HTTP client configuration (SSL and proxy)
  #  ws {}
   }
}
```

Figure 64: Intégration de Cortex à TheHive

On intègre Cortex à Cortex Analyzer et au Répondeur, on édite le fichier de configuration de Cortex application.conf et on indique à Cortex le dossier de Cortex Analyers.

```
analyzer {
  # analyzer location
  # url can be point to:
  # - directory where analyzers are installed
  # - json file containing the list of analyzer descriptions
  urls = [
    "https://download.thehive-project.org/analyzers.json"
    "/etc/cortex/Cortex-Analyzers/analyzers"
  ]
```

```
# RESPONDERS
#
responder {
  # responder location (same format as analyzer.urls)
  urls = [
    "https://download.thehive-project.org/responders.json"
    "/etc/cortex/Cortex-Analyzers/responders"
  ]
```

Figure 65: Intégration de Cortex-Analyers / Responder à Cortex

- **Installation de MISP :**

MISP est un outil qui permet le partage d'information sur les Malware. L'installation de MISP est simple, nous allons compiler deux fichiers : premier fichier est le INSTALL.tpl.sh et le deuxième fichier est le INSTALL.sh.

```
server@server:~$ sudo git clone https://github.com/MISP/MISP.git
[sudo] password for server:
Cloning into 'MISP'...
remote: Enumerating objects: 208, done.
remote: Counting objects: 100% (208/208), done.
remote: Compressing objects: 100% (129/129), done.
remote: Total 125360 (delta 106), reused 131 (delta 54), pack-reused 125152
Receiving objects: 100% (125360/125360), 103.06 MiB | 577.00 KiB/s, done.
Resolving deltas: 100% (94911/94911), done.
server@server:~$
```

Figure 66: Téléchargement MISP

Après compilation de ces deux fichiers l'installation prendra quelques minutes, une fois l'installation terminées on se connecte via l'interface Web : https://192.168.10.2

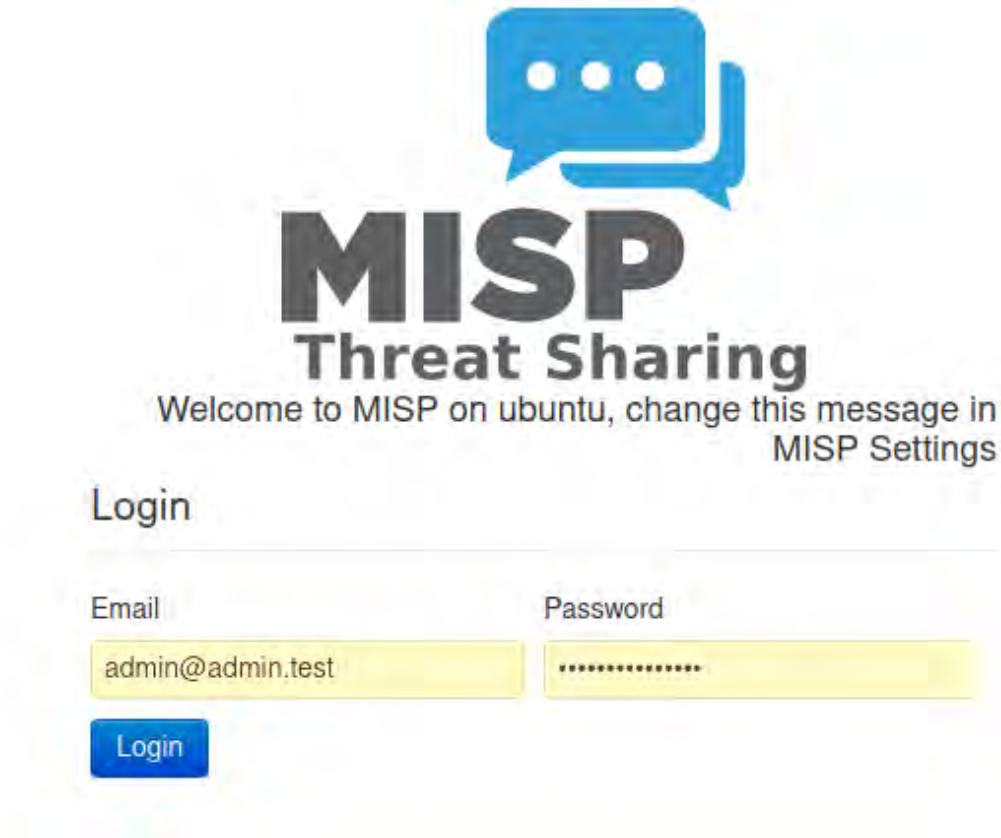


Figure 67: Connexion MISP

Page d'accueil de MISP

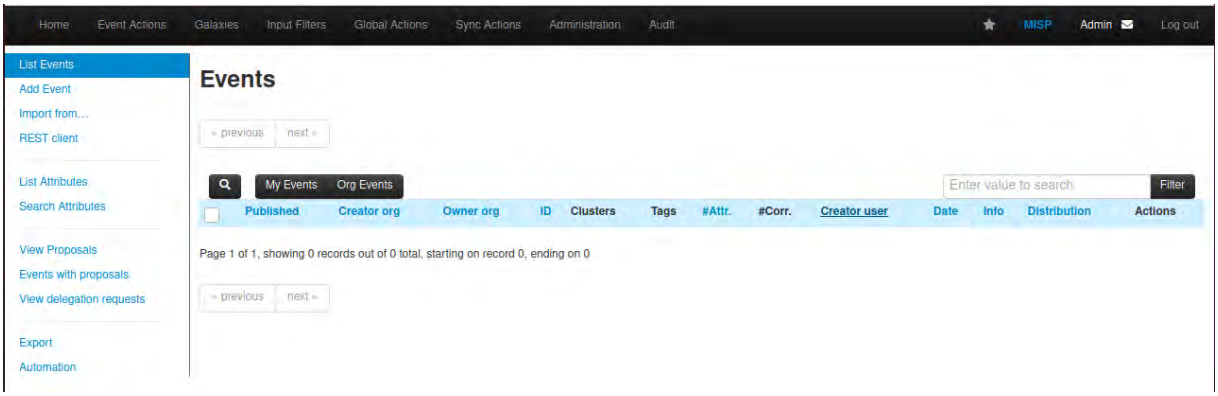


Figure 68: Page d'accueil MISP

Intégration de MISP à TheHive, dans le fichier de configuration de TheHive application.conf on décommette les lignes suivant et en ajoutant la clef API de MISP et son adresse IP.

```
 GNU nano 4.8                /etc/thehive/application.conf
misp {
  # Interval between consecutive MISP event imports in hours (h) or
  # minutes (m).
  interval = 5m

  "MISP-SERVER-ID" {
  #  # MISP connection configuration requires at least an url and a key. The ke>
  #  # be linked with a sync account on MISP.
    url = "https://192.168.10.2"
    key = "8jYy9eIoxR76DgaxPFPnaXVY8Z4aXWoQcFPVZVUm"
  #
  #  # Name of the case template in TheHive that shall be used to import
  #  # MISP events as cases by default.
    caseTemplate = "MISP-Event"
  #
  #  # Optional tags to add to each observable  imported  from  an  event
  #  # available on this instance.
    tags = ["misp"]
  #
```

Figure 69: Intégration de MISP à TheHive

5.6. Installation et configuration d'un WAF :

WAF (Web Application Firewall) aide à protéger les applications web en filtrant et en surveillant le trafic HTTP entre une application web et Internet. Il protège généralement les applications web des attaques notamment de type cross-site forgery, cross-site scripting (XSS), d'inclusion de fichier et d'injection SQL.

Dans notre cas nous avons télécharger une VM FortiWeb qu'on a importé dans notre environnement virtuel. Nous allons mettre notre serveur Web derrière ce WAF, afin de le protège des attaques de type DDoS, XSS, injection SQL etc.

Une fois la machine virtuelle démarrée nous allons configurer notre WAF via l'interface Web en l'attaquant par son adresse IP par défaut qui est le https://192.168.1.99.

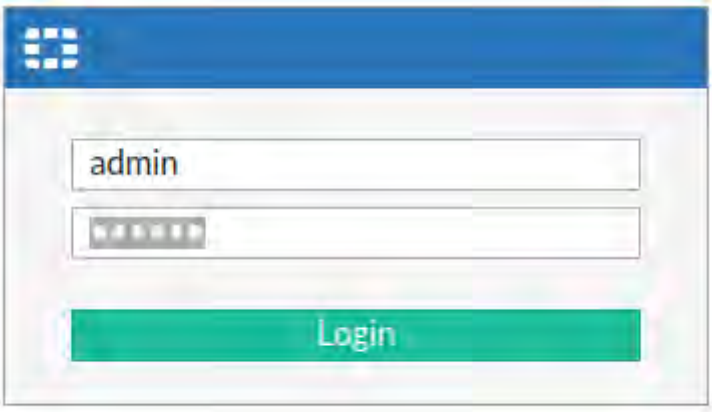


Figure 70: Connexion à FortiWeb

Nous allons configurer les différentes interfaces que nous utiliserons pour notre WAF.

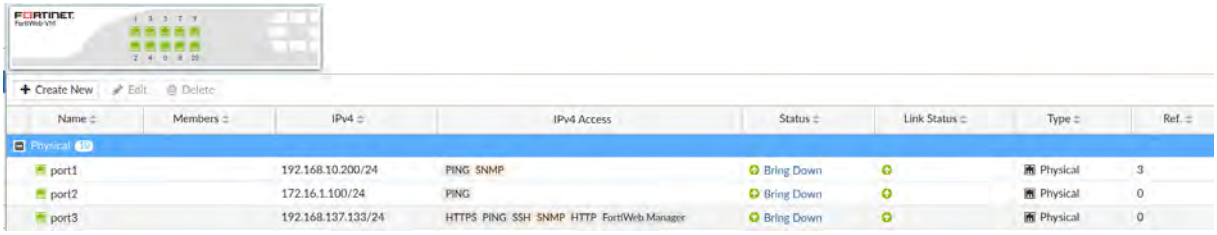


Figure 71: Interface WAF

Le port 1 est celui qui nous relie à notre LAN, le port 2 est le réseau partagé entre notre WAF et le serveur WEB et le port 3 est notre port de management.

Après avoir identifié les différentes parties de notre réseau, nous allons configurer notre WAF pour qu'il protège notre serveur Web.

Nous allons en premier lieu crée un pool de serveur en donnant adresse IP de notre serveur Web.

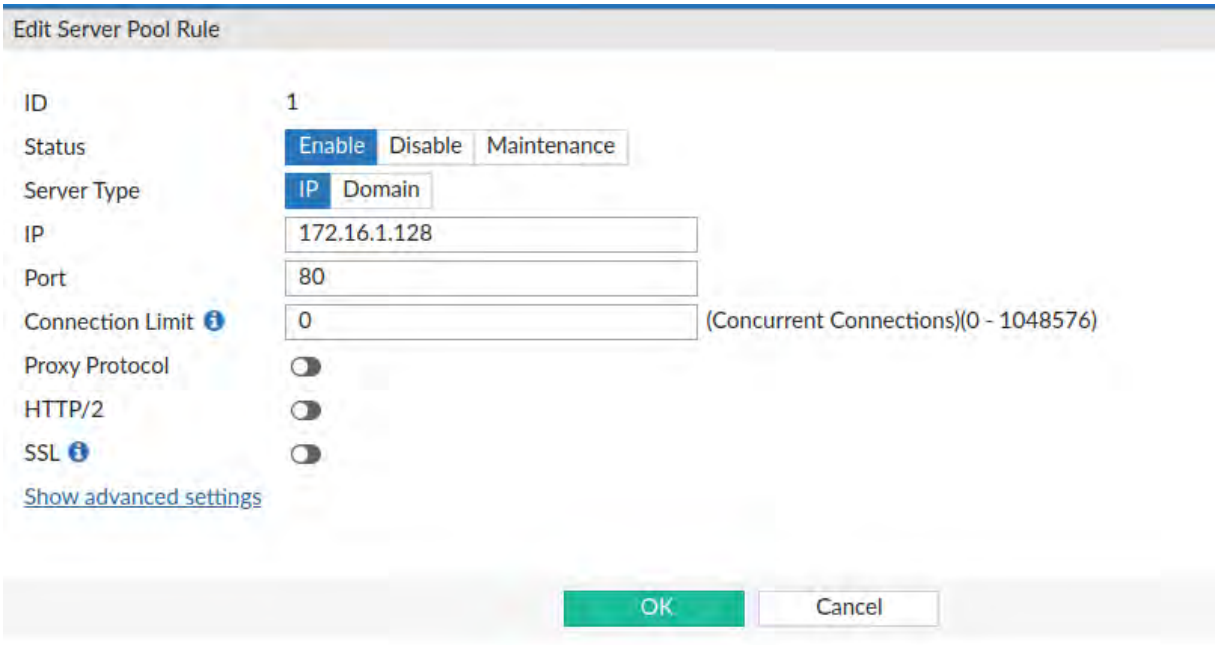


Figure 72: Création de pool de serveur

En deuxième lieu nous allons créer un adresse IP virtuelle, c'est cette adresse IP qui sera utilisée pour contacter notre serveur Web.

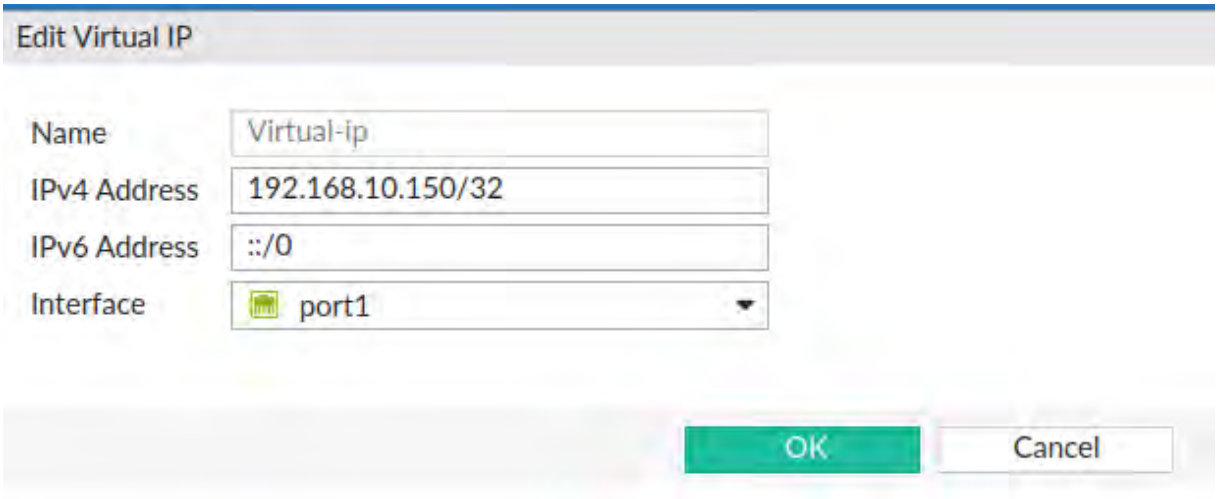


Figure 73: Création d'adresse IP virtuelle

En dernier lieu nous créons une règle qui dit que s'il y a une requête qui vient sur le WAF avec l'adresse IP 192.168.10.150 de le translater vers le 172.16.1.128 qui est l'adresse IP du serveur.

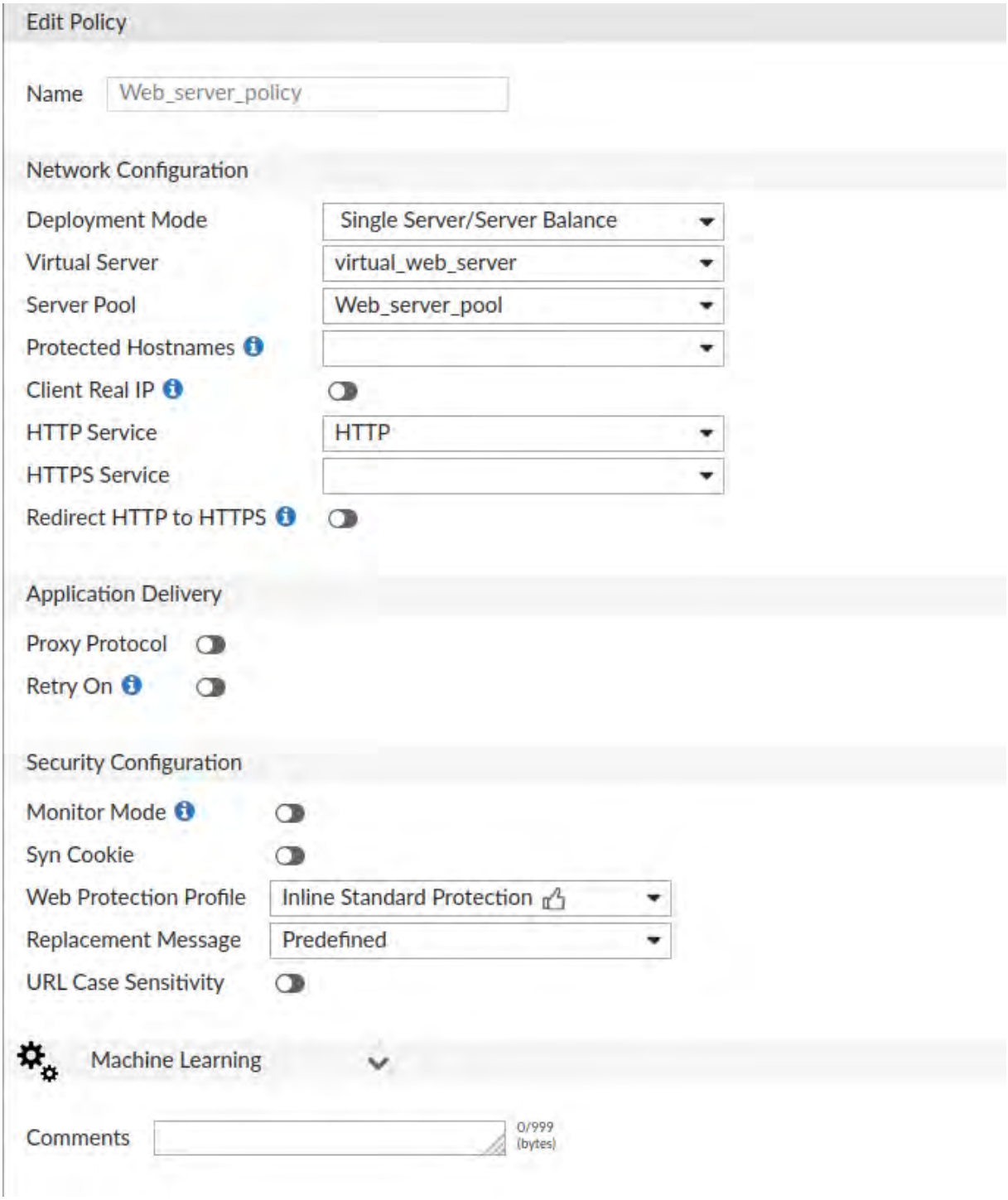


Figure 74: Création d'une règle

Au final on a cette topologie :

Figure 75: Topologie WAF

Chapitre 6 : Test de fonctionnement

6.1. Observation du comportement du réseau avec Nagios Network Analyzer et Nagios XI :

En temps normal quand tous se passe bien Nagios Network Analyzer (NA) émet pas d'alerte et son statut est au vert.

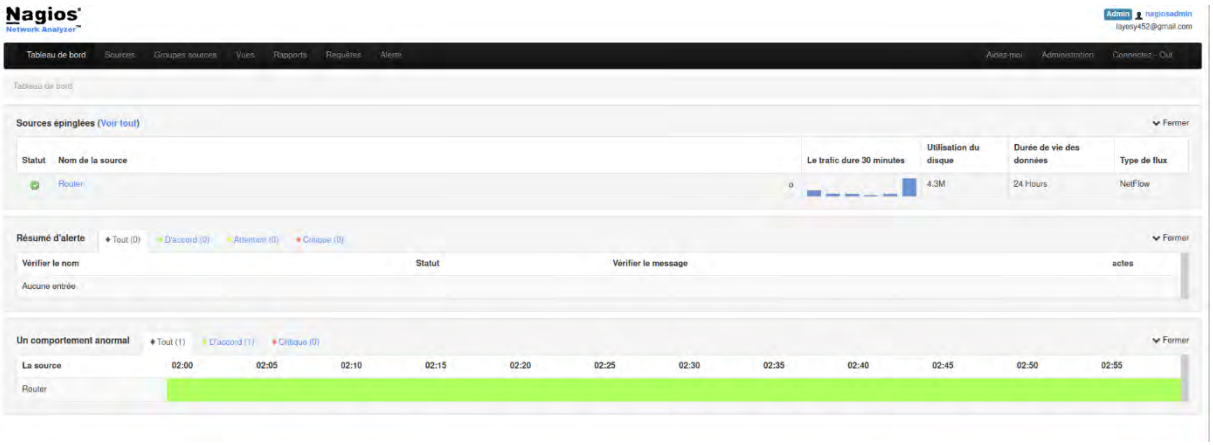


Figure 76: Trafic normal

Dès qu'il y a un changement d'état du trafic réseau Nagios NA émet une alerte en mettant son statut en rouge et nous donne la source de ce problème en identifiant l'adresse IP source et de destination qui ont causées ce problème.

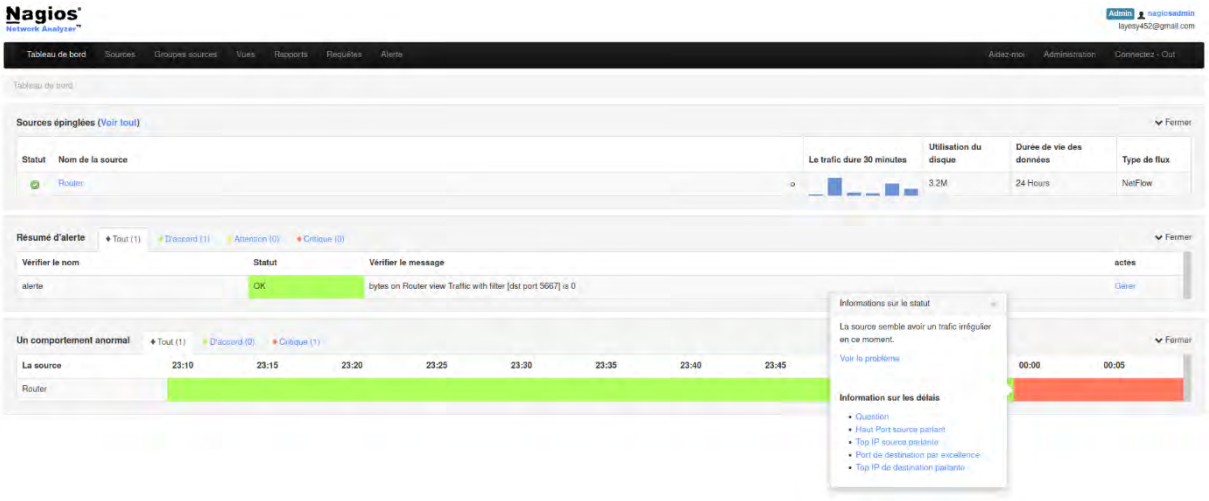


Figure 77: Trafic critique

Nous allons analyser l'adresse IP source qui a causé ce problème.

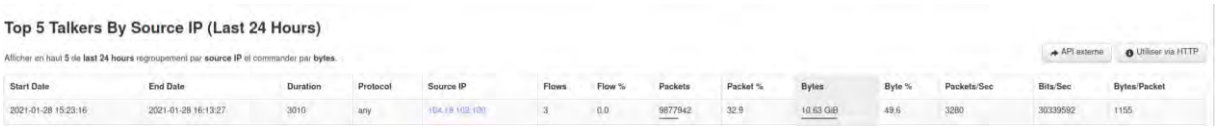


Figure 78: Analyse adresse IP source

Nous constatons que l'adresse IP source à consommer plus de 10GB en moins de 24H ce qui peut être une source de ralentissement du réseau.

En analysant de prêt les évènements de Nagios XI on remarque que sur son tableau de bord le statut des serveurs surveillent remontes en temps réel.

Figure 79: Statut des serveurs

Sur les cinq serveurs supervisés, on a un serveur qui est hors service. On constate qu'il y a des services critique, on peut avoir une vue sur ces services afin de décelai le problème.

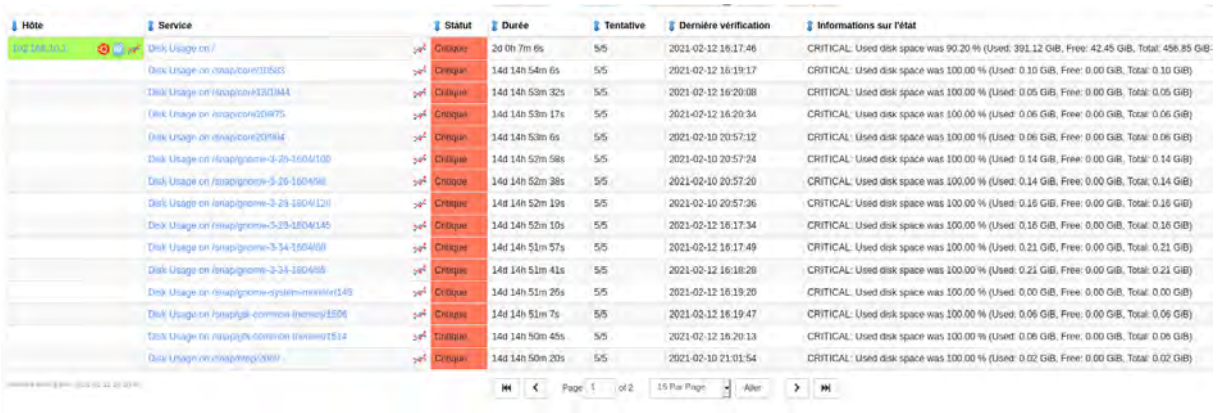


Figure 80: Services critiques

On remarque que le problème vient des disques qui ont atteint le seuil maximal d'utilisation soit 80%. Pour remédier à ce problème on peut soit supprimer des éléments sur les disques ou faire une sauvegarde afin de libérer de l'espace.

6.2. Gestion de vulnérabilité avec Nessus :

Après avoir effectué un scan sur notre réseau, nous devons analyser les résultats du scan pour identifier les vulnérabilités qui se trouvent dans notre système d'information. Pour pouvoir les corrigées en effectuant des mises à jours de sécurité.

Nessus a détecté des vulnérabilités critiques, nous allons analyser ces vulnérabilités.

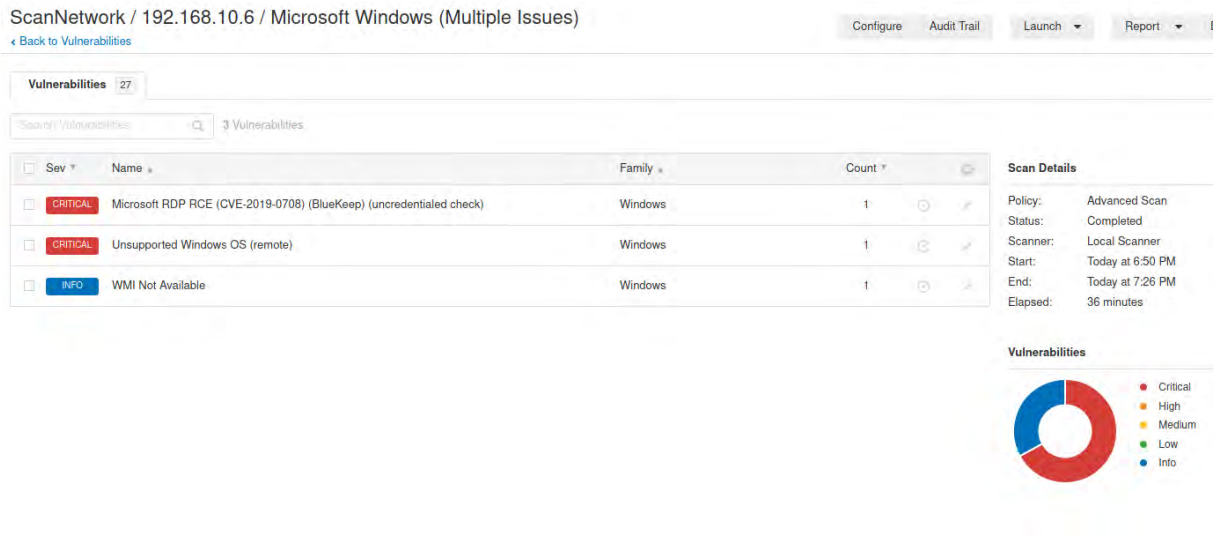


Figure 81: Vulnérabilités détecter

Nous avons deux vulnérabilités critique liée au système d'exploitation de Windows. L'une est liée au protocole de Microsoft qui est le RDP (Remote Desktop Protocol) et l'autre vulnérabilité indique que l'OS n'est plus supporté par Microsoft donc qui est end-off life et end-off support.

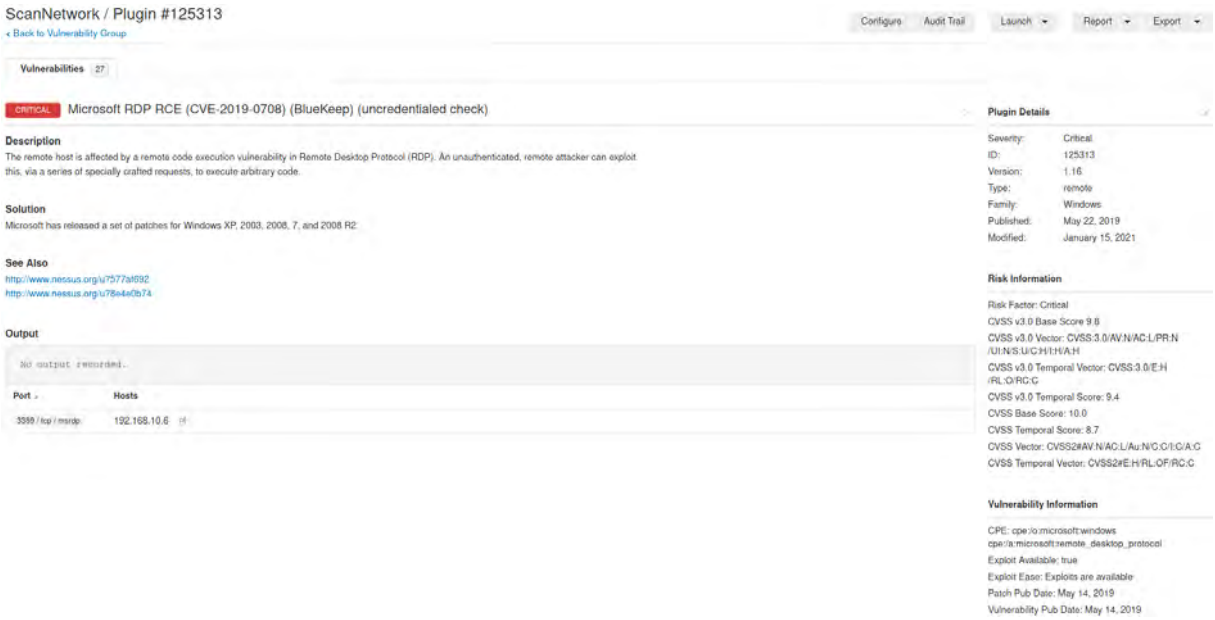


Figure 82: Les détails de la vulnérabilité RDP

Le 14 mai 2019, lors de sa mise à jour mensuelle, Microsoft a publié un correctif pour une vulnérabilité identifiée comme CVE-2019-0708.

Cette vulnérabilité impacte les services de bureau à distance (Remote Desktop Services, RDS), basé sur le protocole de bureau à distance (Remote Desktop Protocol, RDP) et régulièrement utilisé dans le cadre de l'administration à distance. Cette vulnérabilité permet l'exécution de code arbitraire sur un système vulnérable, et ce sans authentification ni interaction d'un utilisateur.

Les systèmes affectés : Windows 7, Windows server 2008 R2, Windows server 2008, Windows vista, Windows 2003 et Windows XP.

6.3. Gestion des événements avec TheHive / Cortex / MISP :

Pour une bonne gestion des incidents sécurité, nous allons créer un ticket pour chaque incident qui interviens dans notre système d'information et le suivre jusqu'à sa clôture.

Dans notre cas nous allons créer un ticket, l'affecter à un membre de l'équipe et le suivre jusqu'à sa clôture.

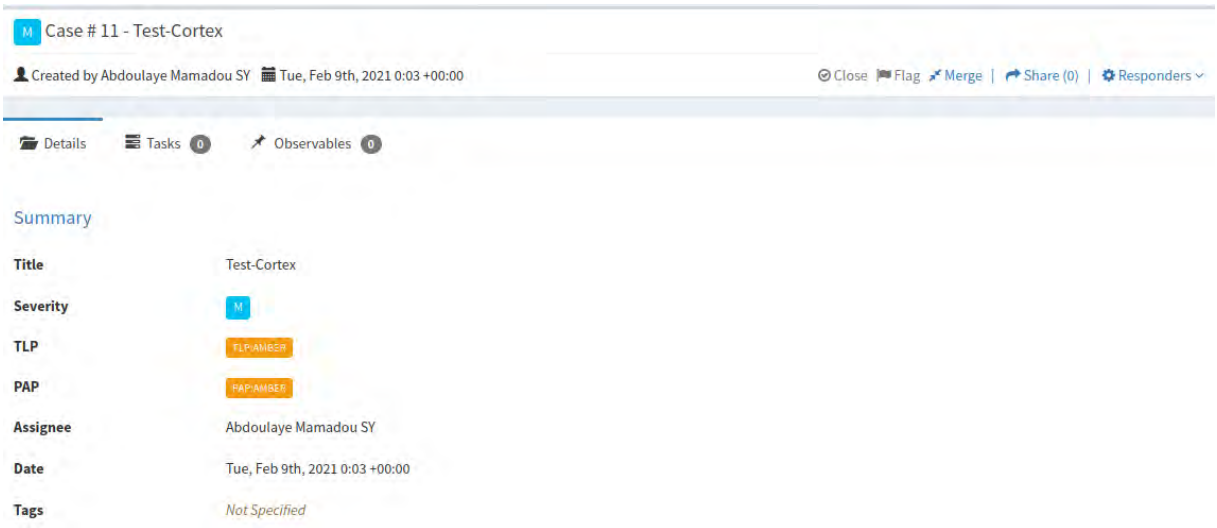


Figure 83: Création d'un ticket

On définit le niveau sévérité de l'attaque, la valeur du TLP (Traffic Light Protocol), la valeur du PAP (Permissible Actions Protocol), la personne à qui on affecte le ticket, la date de création et le Tags s'il y a lieu.

Dans notre cas la sévérité de l'attaque est moyenne, le TLP et PAP ont une valeur de 2 donc de couleur jaune, le ticket est affecté à Abdoulaye Mamadou SY, la date de création mardi 9 février 21 et on n'a pas Tags.

La prochaine étape consiste à créer un observable ce qui nous permettra d'analyser la requête.

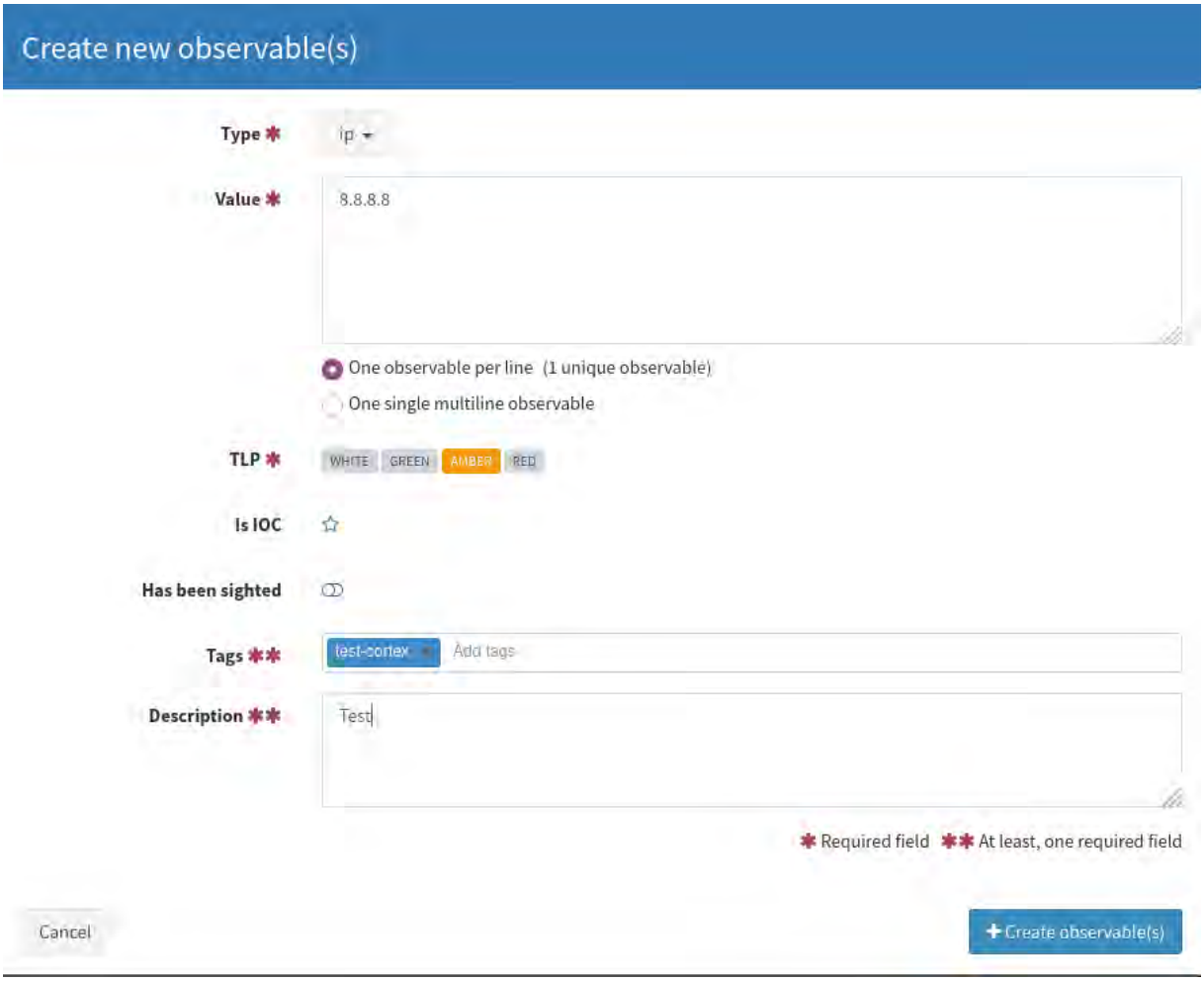


Figure 84: Création d'un observable

On a le type IP, la valeur de l'adresse IP de Google, la valeur du TLP, le Tags le nom du ticket et une description.

Après avoir créé un observable, on doit exécuter une analyse.

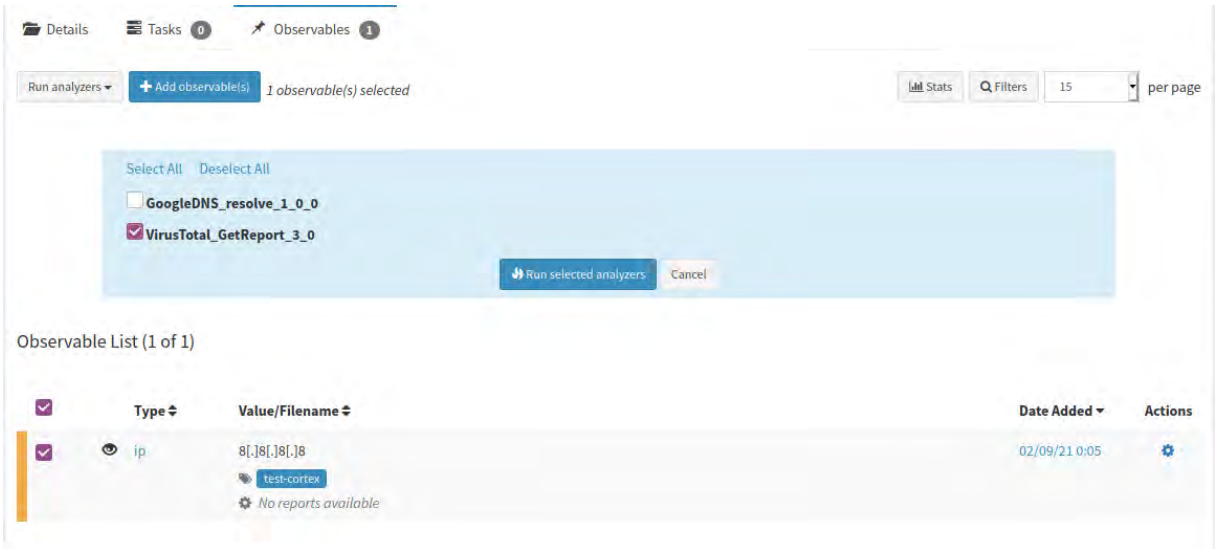


Figure 85: Exécution d'une analyse

Quand on exécute une analyse l'analyseur nous renvoie une réponse de cette analyse. Ici notre Analyzer est le VirusTotal.

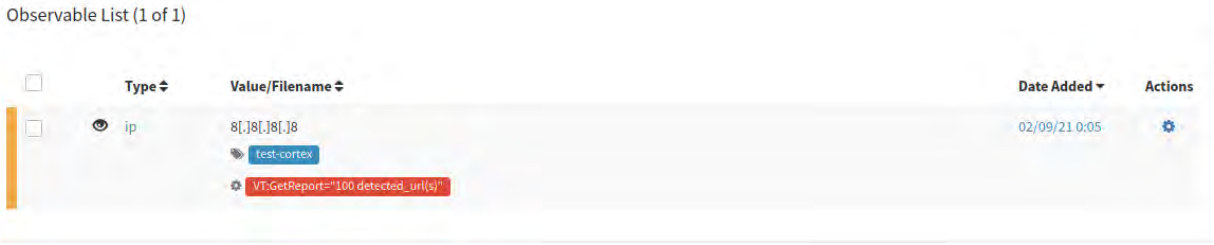


Figure 86: Réponse de l'analyseur

On remarque que sur Cortex l'analysé s'est effectué avec succès.

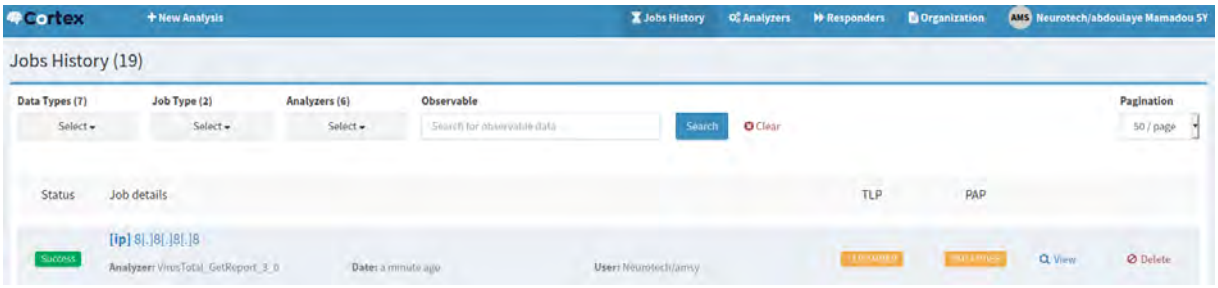


Figure 87: Analyse réussi

Après avoir effectué tous les étapes nécessaires pour le suivi de l'incident nous pouvons clôture le ticket.

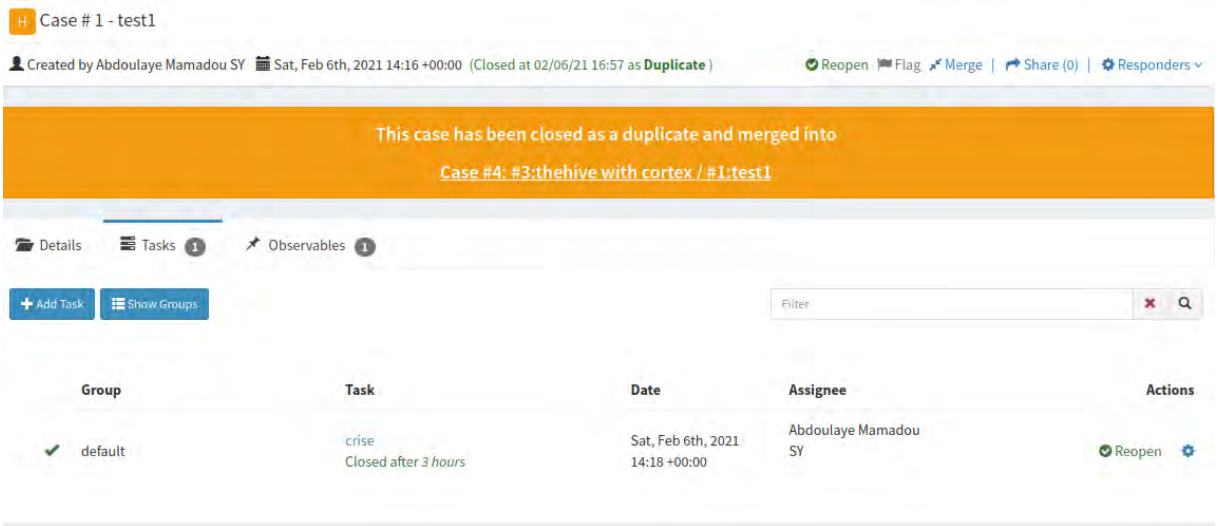


Figure 88: Clôture du ticket

Avec le Dashboard de TheHive nous pouvons avoir une vue sur l'ensemble des jobs crée, le nombre ticket crée et une vue sur le traitement des tickets en cours de traitement.

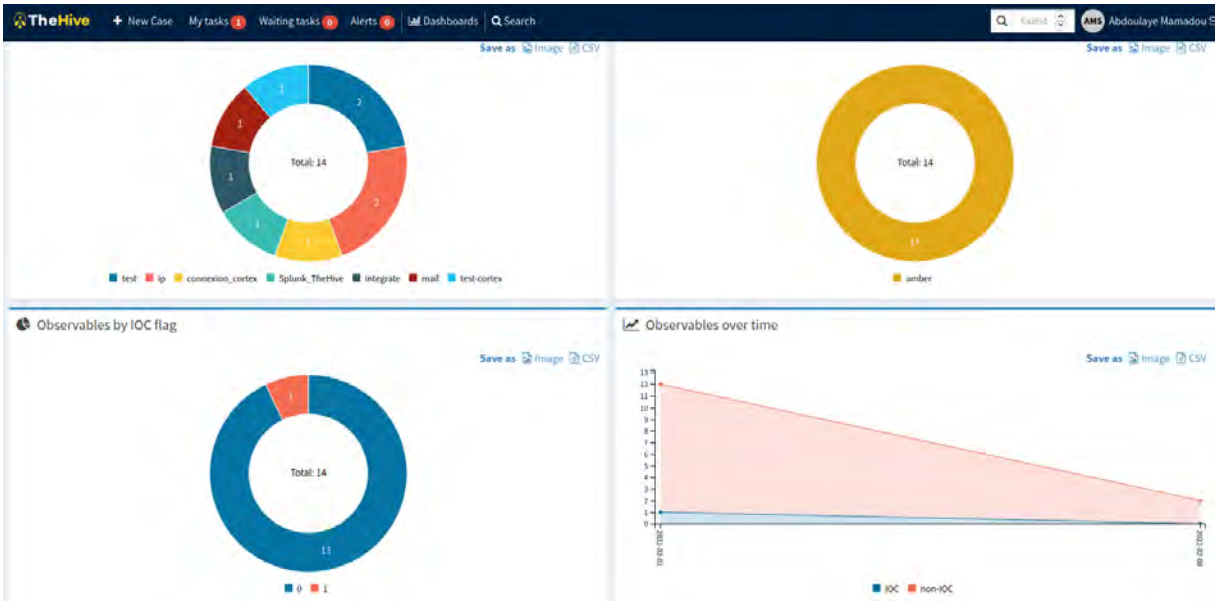


Figure 89: Dashboard TheHive

Les statistiques des jobs.

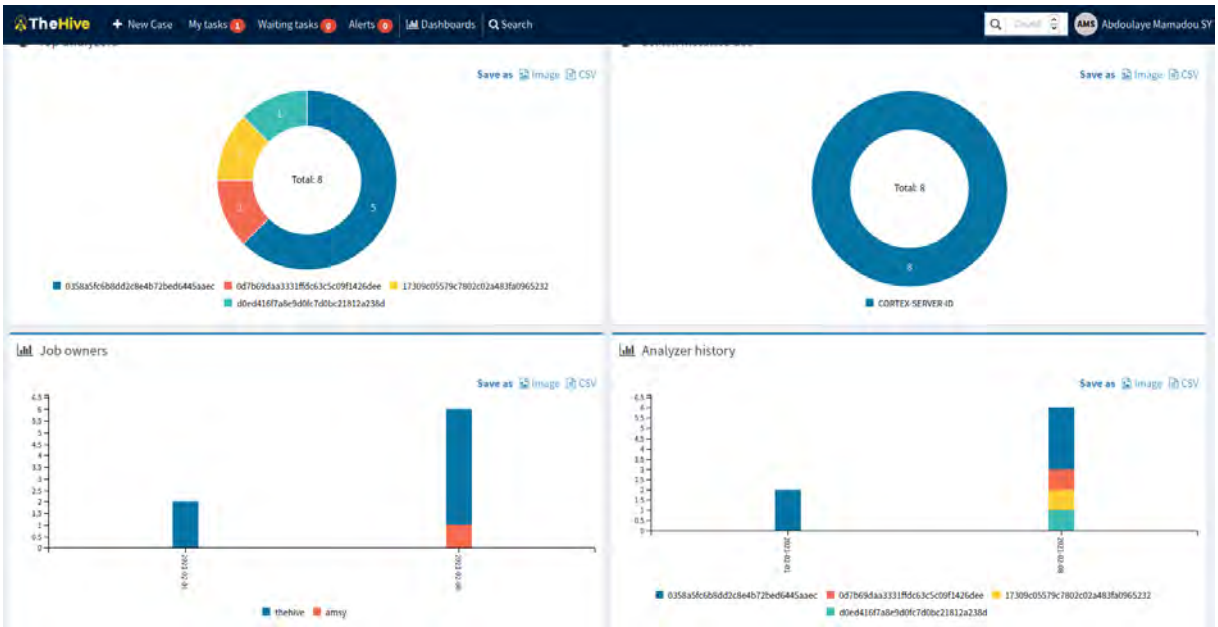


Figure 90: Statistiques des jobs

Une vue sur l'ensemble des tickets crée.

Figure 91: Statistiques des tickets

Pour pouvoir exécuter les Analyseurs on doit les configurés au niveau de notre Cortex. Dans notre cas nous avons configuré l'Analyseur VirusTotal en créant un compte sur leur site pour obtenir une clef API afin de pouvoir activé l'analyseur.

Figure 92: Activation VirusTotal

Nous allons maintenant pouvoir exécuter une analyse directement à partir du Cortex.

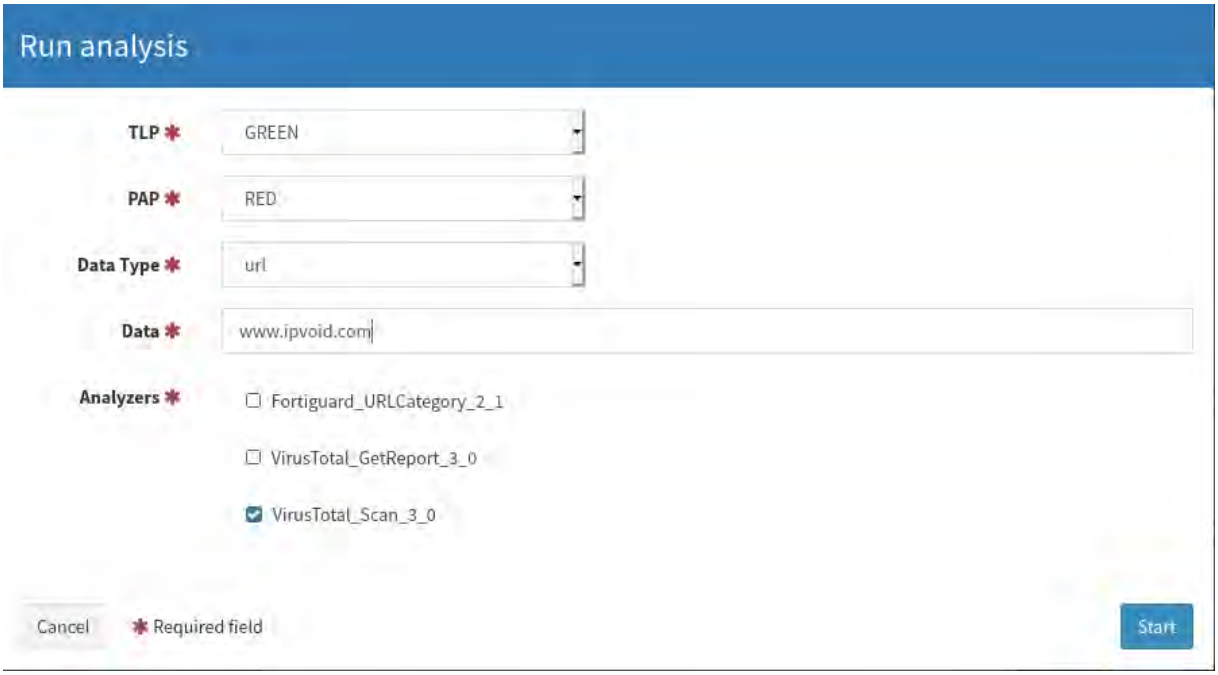


Figure 93: Run analysis Cortex

On choisit la valeur du TLP et du PAP, le type url **ipvoid** qui est une url malveillante puisqu'elle est blacklistée et l'analyser VirusTotal Scan.

Figure 94: ipvoid analysé avec succès

Pour pourvoir partager des informations sur les incidents qu'on a rencontrées on a utilisé MISP (Malware Information Sharing Platform) en activant les différentes taxonomies qui nous intéresse.

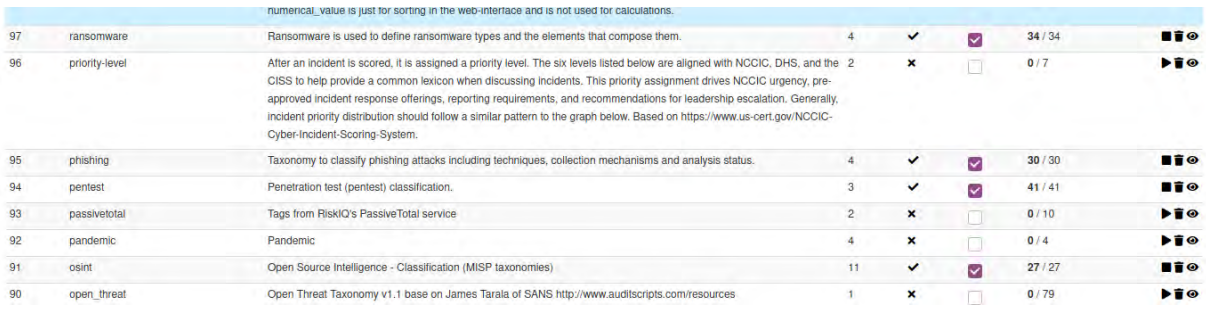


Figure 95: Activation taxonomies MISP

Nous allons créer un évènement en ajoutant les taxonomies concernées.

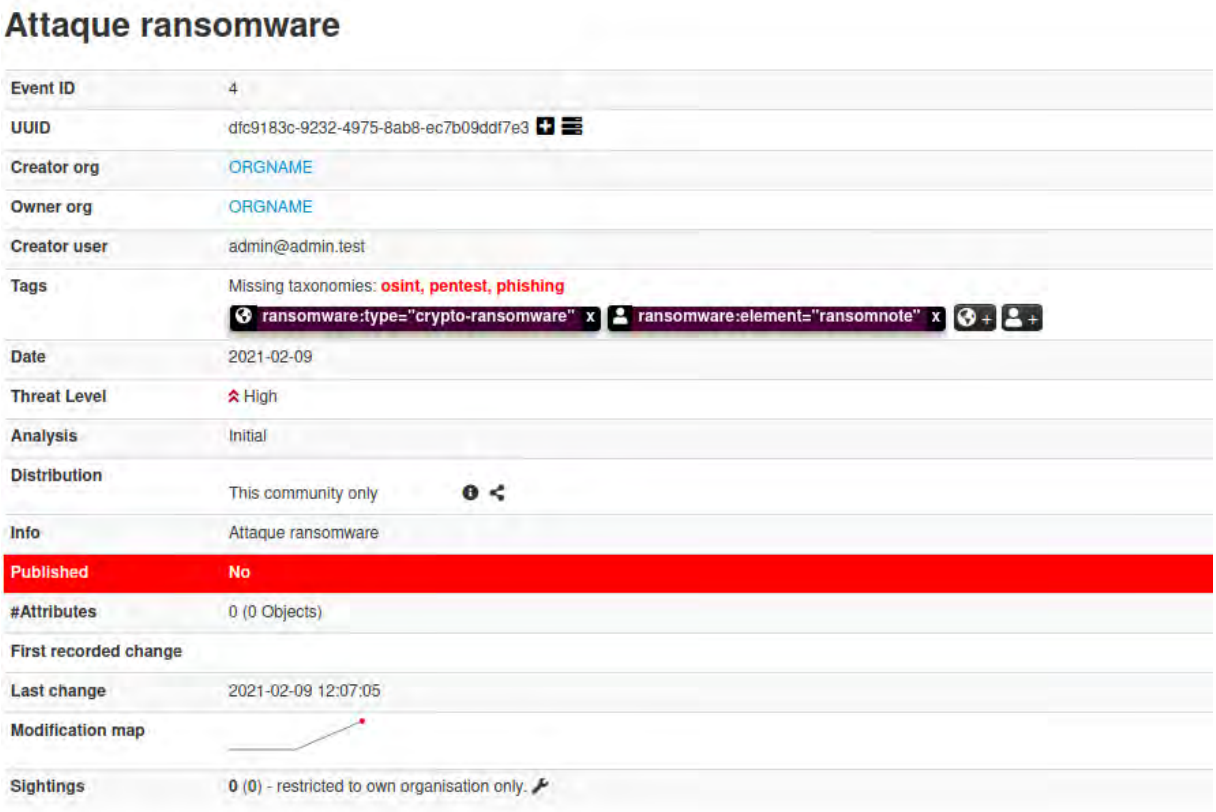


Figure 96: Création évènement MISP

On a une vue sur l'ensemble des évènements créent sur MISP

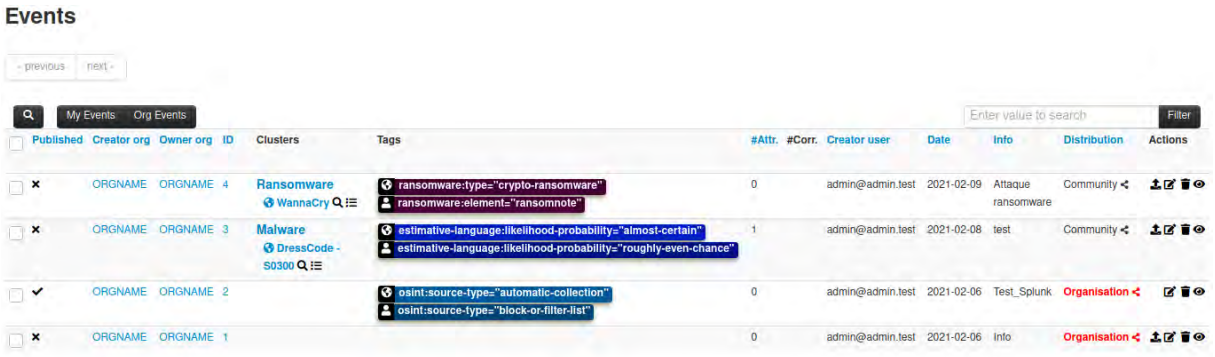


Figure 97: Vue sur les évènements

6.4. Observation du comportement d'un WAF (FortiWeb) :

Nous allons tester si notre WAF protégé notre serveur Web en faussant un scan **Nmap** sur l'adresse IP virtuelle pour joindre le serveur et une attaque DOS avec l'outil **hping3.**

En lançant un scan avec Nmap sur l'adresse IP 192.168.10.150, on constate que le FortiWeb ne laisse passer que le trafic http et donc l'attaquant n'aura pas des informations sur les ports ouvrent sur le serveur.

```
┌──(root💀kali)-[~]
└─# nmap -sV 192.168.10.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-09 17:27 EST
Nmap scan report for 192.168.10.150 (192.168.10.150)
Host is up (0.00057s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:55:DC:48 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds
```

Figure 98: Scan avec Nmap

FortiWeb considère ce scan comme une attaque. En identifiant l'adresse IP source de l'attaque et le destinataire de l'attaque, le type scan et la sévérité de l'attaque critique.

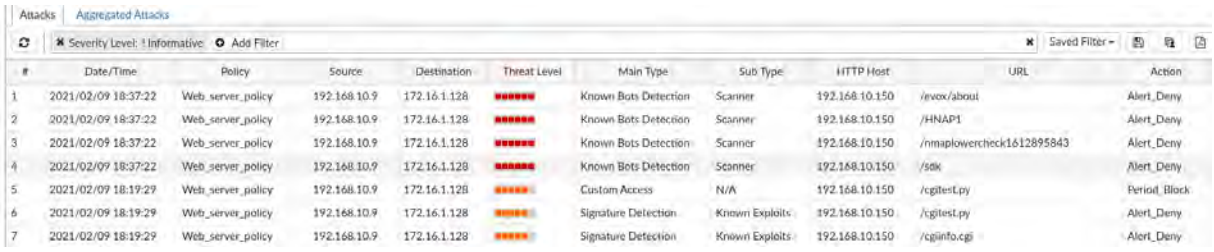


Figure 99: Log de FortiWeb

FortiWeb bloque l'ensemble des paquets envoyés par l'attaquant sauf ceux ayant pour destination le port 80.

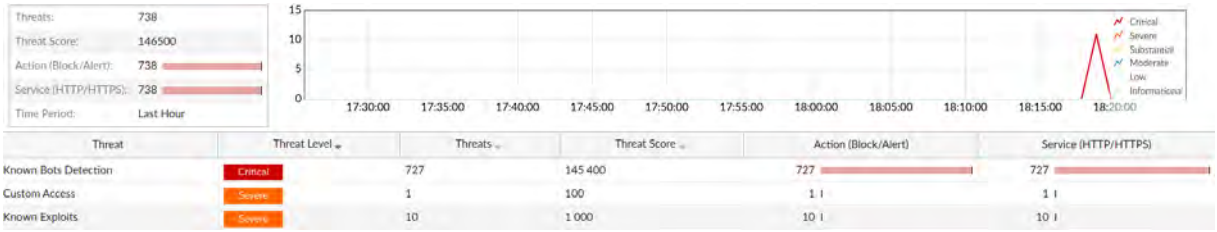


Figure 100: Détection de l'attaque

Pour l'attaque DOS, on constate que sur les 8230120 paquets aucun a atteint notre serveur puisque ces paquets sont bloqués par le WAF.

```
┌──(root💀kali)-[~]
└─# hping3 --flood -p 80 -S 192.168.10.150
HPING 192.168.10.150 (eth0 192.168.10.150): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.10.150 hping statistic ---
8230120 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root💀kali)-[~]
└─#
```

Figure 101: Attaque hping3

On observe l'état du WAF avant et pendant l'attaque. Avant l'attaque le WAF fonctionne normalement sans consommé beaucoup de ressource.

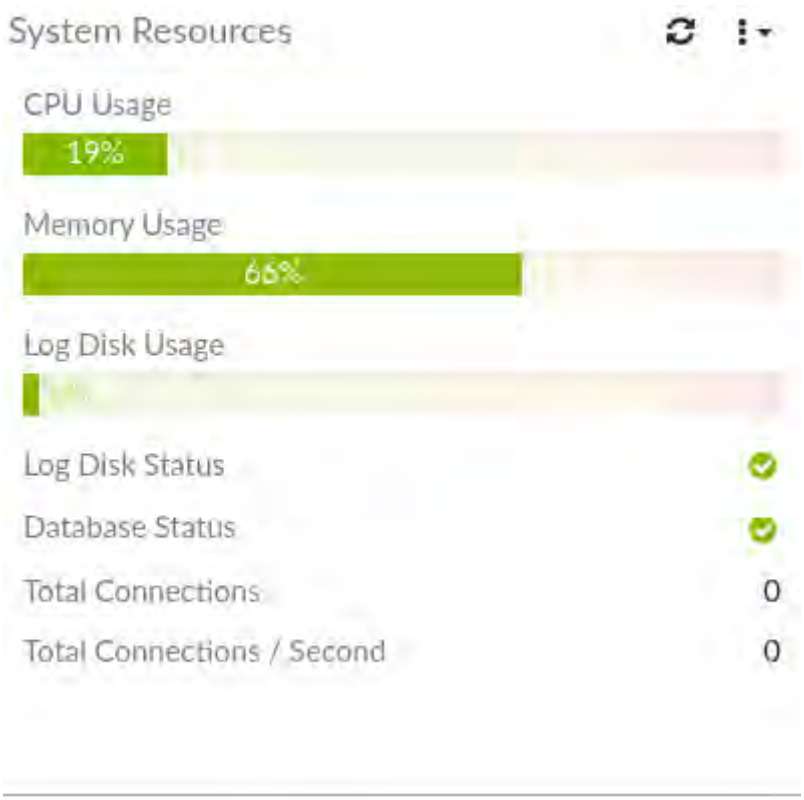


Figure 102: Etat normal du WAF

Pendant le processus d'attaque le WAF consomme beaucoup de ressource CPU pour pouvoir bloquer les paquets envoyés par l'attaquant. Ce qui justifie la monté de charge du CPU.

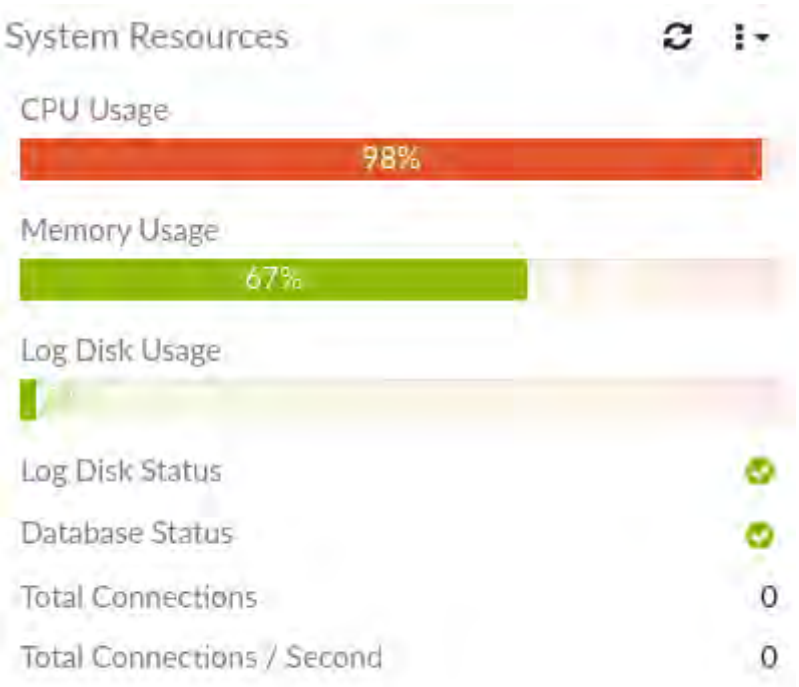


Figure 103: Saturation des ressources en CPU

6.5. Analyse des événements avec Splunk :

Nous allons paramétrer nos applications pour que Splunk puisse recevoir les données de nos différentes plateformes. Ce qui permettra une centralisation de l'ensemble des évènements et ainsi facilité l'analyse de ces derniers.

- Paramétrage de l'application TheHive/Cortex

Nous allons configurer les comptes de TheHive et Cortex pour que Splunk aille collectés leurs données.

On renseigne les paramètres suivants : le nom de l'indexeur, intervalle de temps en seconde, les données à indexées, le protocole utilisé, l'adresse IP de l'hôte, son port de communication ainsi que la clef API d'un utilisateur.

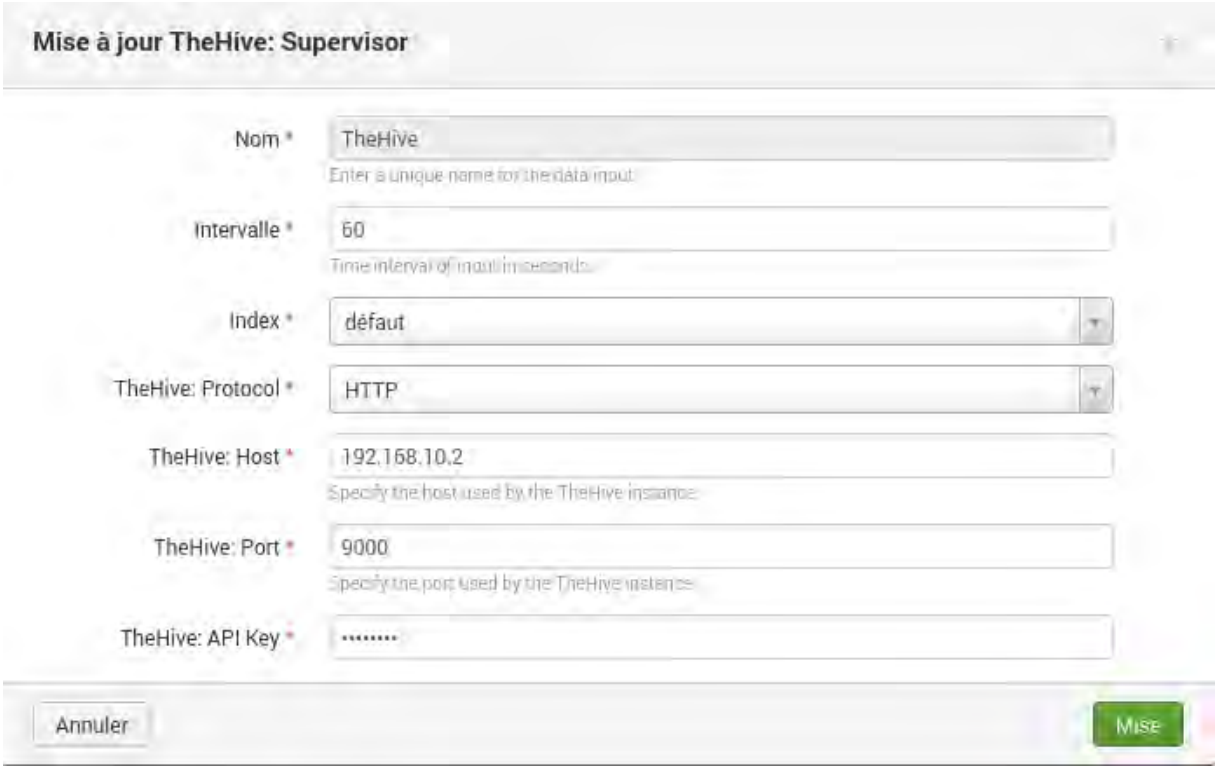


Figure 104: Intégration TheHive à Splunk

On configure Splunk pour s'il détecte une attaque qu'il envoie une alerte à TheHive.

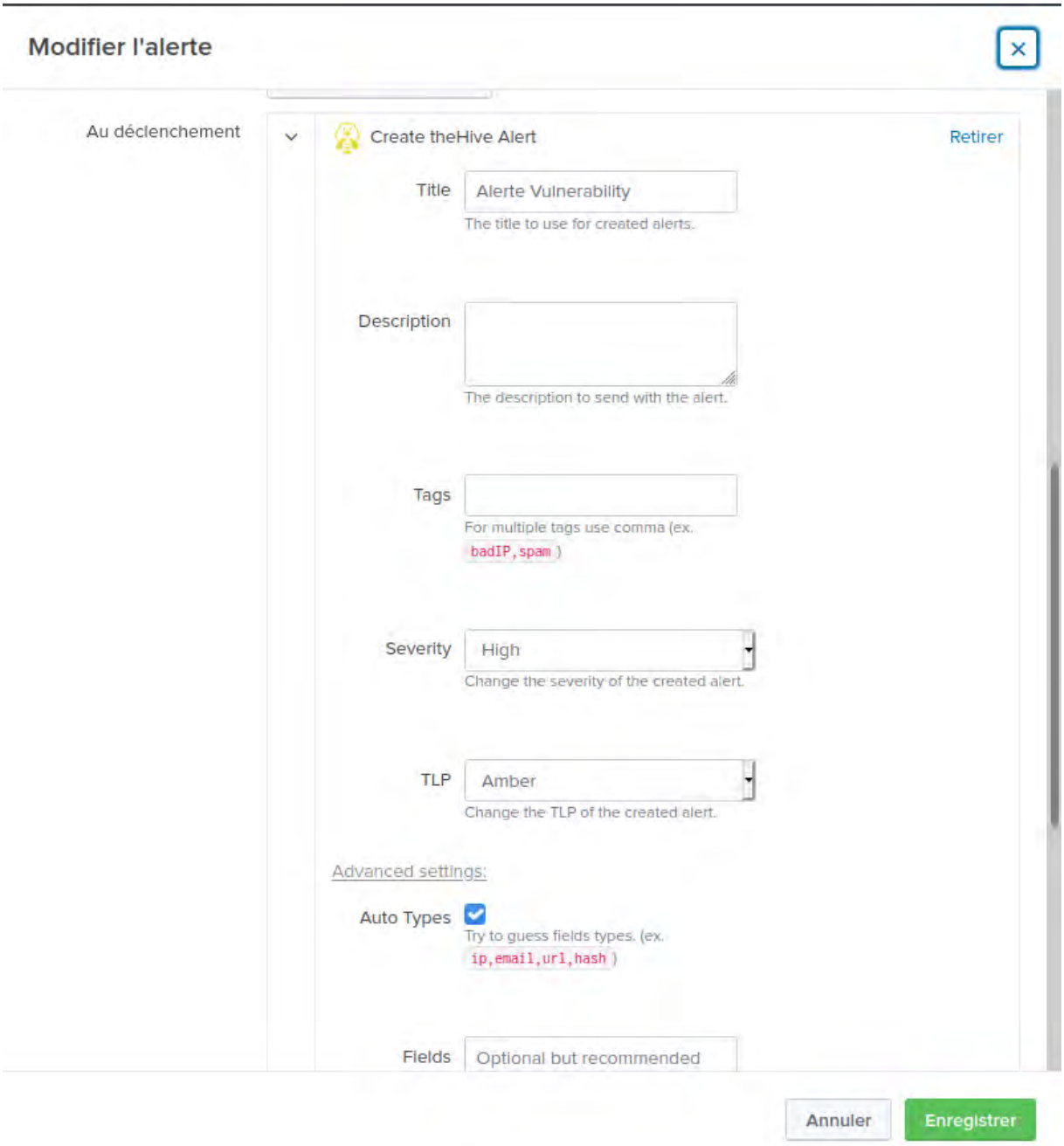


Figure 105: Configuration alerte Splunk

Configuration du compte de Cortex

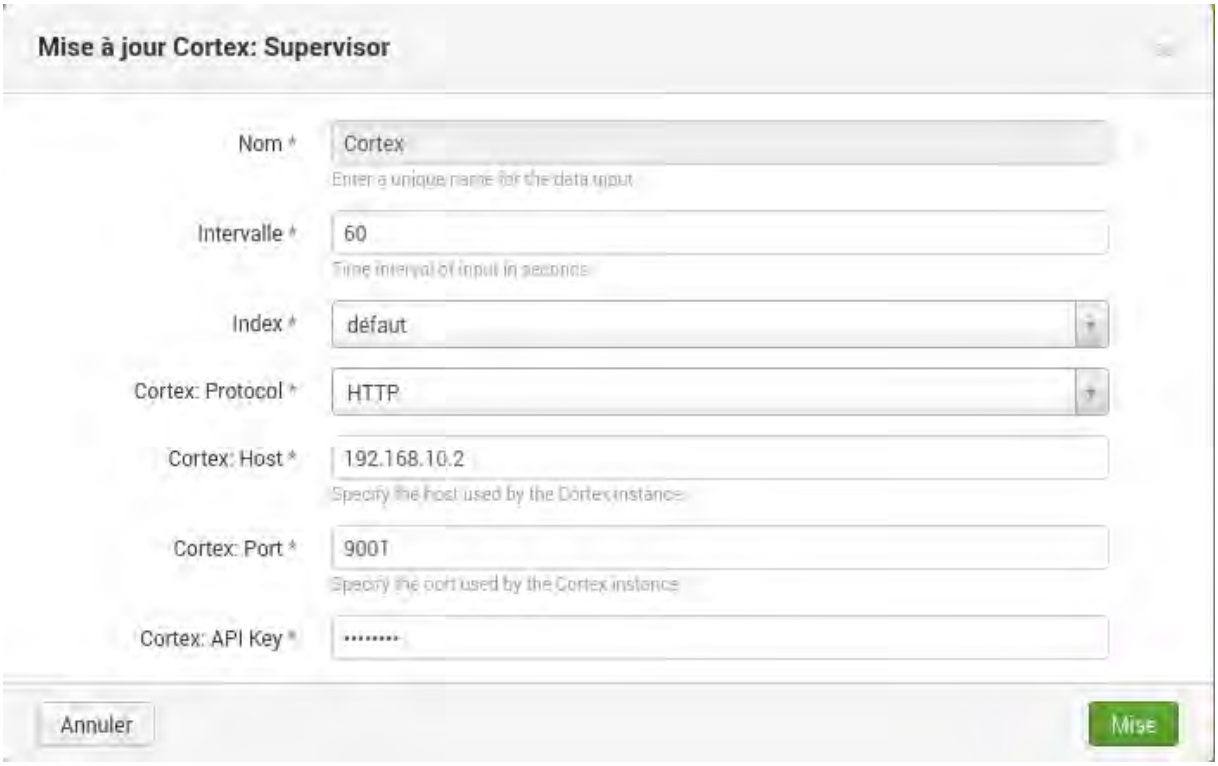


Figure 106: Intégration de Cortex à Splunk

Affichage des évènements au niveau de Splunk.

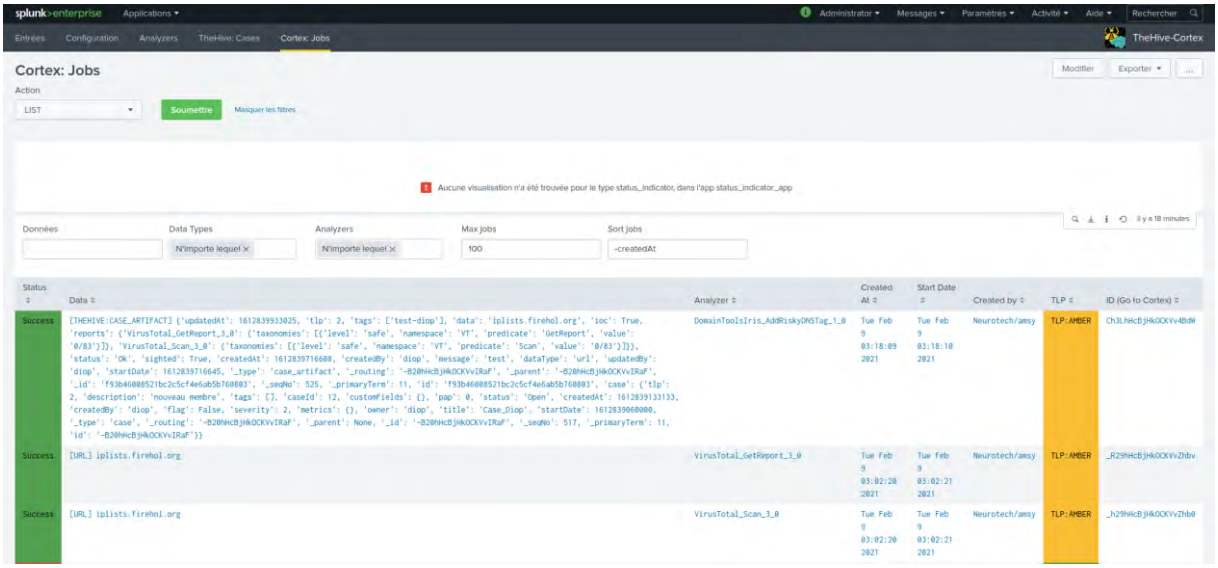


Figure 107: Données d'analyse Cortex

Paramétrage de l'application FortiWeb :

Nous allons ajouter une entrée de donnée sur le port 515 pour que Splunk revoit les données qui seront envoyées par le FortiWeb. Configurer le WAF pour qu'il envoie ces logs à notre serveur Splunk.

Figure 108: Entrée des données FortiWeb

```
Connected

FortiWeb #
FortiWeb # config log syslog-policy

FortiWeb (syslog-policy) # edit syslog_policy_1

FortiWeb (syslog_policy_1) # config syslog-server-list

FortiWeb (syslog-server-~i) # edit 1

FortiWeb (1) # set server 192.168.10.3

FortiWeb (1) # set port 515

FortiWeb (1) # end

FortiWeb (syslog_policy_1) # end

FortiWeb # config sysl
<Enter>


FortiWeb # config log syslogd

FortiWeb (syslogd) # edi
<Enter>


FortiWeb (syslogd) # ed
<Enter>


FortiWeb (syslogd) # set policy syslog_policy_1

FortiWeb (syslogd) # set status enable

FortiWeb (syslogd) # end

FortiWeb #
```

Figure 109: Intégration de FortiWeb à Splunk

Lorsque le WAF fait face à une attaque, les données sont envoyées automatique au niveau de notre SIEM Splunk.

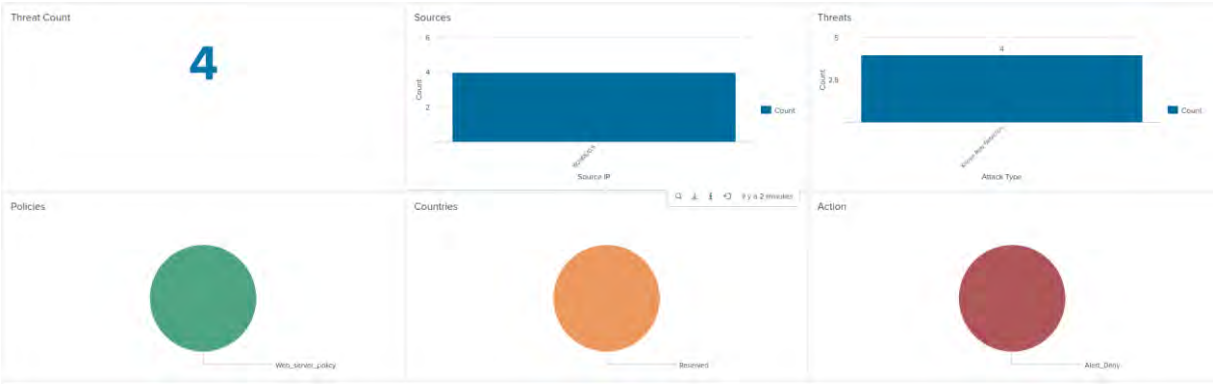


Figure 110: Visualisation des données de FortiWeb sur Splunk

Nous constatons que Splunk détecte automatique le nombre d'attaque qu'a subi le WAF, l'adresse IP source qui a effectué l'attaque le 192.168.10.9, l'action effectué sur les paquets envoyés par l'attaquant **Deny** est la Policy (règle) qui est utilisé. Ainsi à partir de ces données Splunk peut générer une alerte et l'envoyer à TheHive, une fois sur TheHive un ticket sera créé, on effectuera une analyse de l'adresse IP qui est à l'origine de l'attaque et des informations récoltées et partage ces informations avec la communauté de la cybersécurité en passant par le MISP on pourra ainsi suivre l'incident jusqu'à sa clôture.

Conclusion générale :

Au terme de notre travail, nous avons pu mettre en place une plateforme de gestion des incidents de sécurité, cette dernière nous a permis :

- De quantifier nos ressources réseau et la disponibilité de ces services ;
- De faire de la veille des vulnérabilités de notre Système d'information ;
- De créer un ticket pour chaque incident et de le suivre jusqu'à sa clôture ;
- De sécuriser notre serveur web contre les cyber-attaques à l'aide d'un WAF ;
- De centraliser l'ensemble des évènements du système d'information.

Ces résultats qui servent de réponse à la problématique posée et aux objectifs fixés sont résumés dans ce qui suit :

La gestion des incidents de sécurité est un processus qui permet d'anticiper et d'atténuer les cyber-attaques. En détectant le plus rapidement possible une attaque, nous pouvons ainsi réagir à temps pour retrouver l'état initiale de notre système d'information. Ceci est possible si l'entreprise dispose des ressources compétentes capable d'analyser l'état de la menace et d'évaluer les propres vulnérabilités de l'organisation. La cybersécurité ne se limite pas à l'aspect technique, la sensibilisation et la formation des utilisateurs sont essentielles au bon fonctionnement du système d'information.

Les entreprises peuvent adapter différents processus de gestion des incidents en sécurité en fonction de leurs besoins en matière de cybersécurité. On a ainsi :

- Un CERT / CSIRT gouvernemental ;
- Un CERT / CSIRT commercial ;
- Un CERT / CSIRT privé.

Ce dernier a été l'objet de notre étude, dont le fonctionnement est mis en pratique un peu plus haut.

La cybersécurité est également un travail d'équipe et on ne lutte pas efficacement contre ces menaces en restant chacun dans son coin. La coopération et l'échange d'informations restent indispensables pour parvenir à améliorer la sécurité de nos organisations.

BIBLIOGRAPHIE

Livre :

- ✓ **Solange Ghernaouti**, Cybersécurité Analyser les risques et mettre en œuvre les solutions 6éme Edition DUNOD Septembre 2019

Mémoire :

- ✓ **Ndeye Fatou NDOUR**, Etude et Mise en œuvre d'une solution de gestion de la sécurité SI et des évènements : SIEM 2017/2018 72 pages

Articles :

- ✓ Création d'un CSIRT ANSII, 15 pages
- ✓ Charte de l'interCERT-FR-v2-8a 21/06/2018 11pages
- ✓ Global Cyber Security Capacity Centre 23 pages
- ✓ Guide de création d'un CSIRT Pas à Pas ENISA 90 pages
- ✓ Gestion des cyber incidents Guide de planification Juno Risk Solution 33 pages
- ✓ Cybersécurité Guide de gestion des incidents Center for Cyber Security BELGIUM 38 pages
- ✓ La gestion des évènements et des incidents de sécurité ne peut pas être confondue avec le plan de continuité d'activité BCP-Expert 17 pages
- ✓ Référentiel de gestion des incidents de cybersécurité CERT-MAROC 27 pages
- ✓ Resources of CSIRT (Tools and Services of CIRT/CSIRT) AfricaCERT 53 pages

WEBOGRAPHIE

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

https://secureglobal.de/the-csirt-methodology

https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

https://tools.ietf.org/html/rfc2350

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P28

https://www.cert-ist.com/public/fr/presentation

https://pssis.sec.gouv.sn/?q=content/l%E2%80%99adie-vient-de-lancer-le-premier-csirt-du-s%C3%A9n%C3%A9gal-%E2%80%A6

https://www.adie.sn/expertise/s%C3%A9curit%C3%A9

https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/

https://www.cyber-securite.fr/2013/12/13/un-csirt-a-quoi-ca-cert/

https://esdacademy.blogspot.com/2017/04/les-structures-operationnelles-de-la.html

https://cybersecurite.public.lu/fr/administrations/reagir/identification.html

https://www.dnsstuff.com/netflow-traffic-analyzer-review

https://www.manageengine.com/fr/netflow/

https://www.solarwinds.com/fr/netflow-traffic-analyzer/use-cases/what-is-netflow

https://www.solarwinds.com/fr/netflow-traffic-analyzer/use-cases/network-bandwidth-monitoring

https://www.vigilo-nms.com/quest-quun-nms/

https://www.fr.paessler.com/what-is-network-monitoring

https://projet-plume.org/fiche/cacti

https://www.ittsystems.com/nagios-vs-cacti-comparison/

https://open-source-guide.com/Solutions/Infrastructure/Supervision-et-la-metrologie/Cacti

https://nsrc.org/workshops/2012/marwan-nsrc-nmm-sec/raw-attachment/wiki/Agenda/cacti-from-packages-vFR.pdf

https://orangecyberdefense.com/fr/insights/blog/gestion_des_vulnerabilites/gestion-des-vulnerabilites-informatiques-la-detection/

https://fr.slideshare.net/nrc/dmystifier-la-gestion-des-vulnrabilits

https://www.redhat.com/fr/topics/security/what-is-cve#:~:text=L'acronyme%20CVE%2C%20pour%20Common,de%20failles%20de%20s%C3%A9curit%C3%A9%20informatique.&text=Les%20CVE%20aident%20les%20professionnels,la%20s%C3%A9curit%C3%A9%20des%20syst%C3%A8mes%20informatiques.

https://www.balbix.com/insights/what-is-a-cve/

https://fr.tenable.com/products/nessus/nessus-professional/competitive-comparison

https://www.harmonie-technologie.com/siem-security-information-and-event-management

https://www.logpoint.com/fr/comprendre/c-est-quoi-le-siem/

https://www.linkbynet.com/fr/recourir-a-un-siem

https://cyphon.readthedocs.io/en/latest/overview.html#use-cases

https://www.misp-project.org/features.html

https://github.com/TheHive-Project/TheHiveDocs

https://github.com/TheHive-Project/CortexDocs

https://thehive-project.org/

https://www.imperva.com/products/web-application-firewall-waf/

https://www.fortinet.com/products/web-application-firewall/fortiweb#alliance-partners

https://servicenav.coservit.com/documentations/netflow-prerequis-et-configuration/

https://assets.nagios.com/downloads/nagios-network-analyzer/guides/nna-ag/installation.php

https://assets.nagios.com/downloads/nagios-network analyzer/docs/Configuring_Switches_And_Routers_To_Send_Netflow_Data_To_Network_Analyzer.pdf

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-006

https://theexpert.squad.fr/theexpert/security/soc-cert-csirt-decouverte-des-acteurs-de-la-securite-operationnelle/

Table des matières :

Table des matières