Sommaire

Dédicaces i
Remerciements ii
Avant-propos iii
Résumé iv
Abstract v
Sommaire vi
Table des figures viii
Table des tableaux x
Sigles et abréviations xi
Introduction 1
Partie I : Cadre de référence et méthodologique 3
Chapitre 1 : cadre de référence 4
1.1 *Présentation de la structure* 4
Chapitre 2 : cadre Méthodologique 6
2.1 Etude de l'existant 6
2.2 *Problématique* 6
2.3 *Objectif* 7
Partie II : généralités sur le Security Operations Center (SOC) et la sécurité des systèmes d'information 8
Chapitre 3 : La sécurité des systèmes l'information 9
3.1 *Le système d'information et le système informatique* 9
3.2 *La sécurité des systèmes d'information* 9
3.3 *Les attaques informatiques* 11
3.4 *Lois et recommandations régissant la cyber-sécurité au Sénégal* 12
Chapitre 4 : généralités sur le Security Operations Center 16
4.1 *Présentation générale du SOC* 16
4.2 *Le rôle d'un SOC* 17
4.3 *Catalogue de service et fonction d'un SOC* 18
4.4 *Les différents modèles de SOC* 20

4.5 Complémentarité entre le SOC et CERT/CSIRT 21
4.6 Journaux, événement, flux, alertes et incidents 23
Chapitre 5 : les composants du SOC....26
5.1 *Technologies* 26
5.2 *Ressources humaines* 30
5.3 *Gestion des processus* 33
Chapitre 6 : Etude comparative des solutions et choix des outils....35
6.1 *Les SIEMs*....35
6.2 *Scanner de vulnérabilité* 44
Chapitre 7 : Conception du SOC 50
7.1 *Aspect infrastructure et matériel*....50
7.2 *Aspect fonctionnel* 53
Partie III : Simulation et testes....56
Chapitre 8 : Déploiement des outils....57
8.1 *Mise en place de Nessus*....57
8.2 Déploiement du SIEM Alien Vault d'OSSIM 66
Chapitre 9 : Simulation d'une attaque interne....76
9.1 *Démarche* 76
9.2 Réaction d'OSSIM....79
Conclusion....82
Webographie 83
Annexe....86

Table des figures

Figure 1: Architecture générale du réseau 6
Figure 2: Roue de Deming PDCA 10
Figure 3: les principaux service offerts par un SOC 18
Figure 4: Architecture fonctionnelle 21
Figure 5: Limite des responsabilités SOC/CERT 22
Figure 6: Complémentarité entre SOC et CERT 22
Figure 7: chronologie (journal/évènement/alerte/incident) 24
Figure 8: Les composants du SOC 26
Figure 9: rôles de l'équipe SOC 32
Figure 10:Architecture All-in-On du Qradar 36
Figure 11:Architecture distribuée du Qradar 36
Figure 12: Type de données collecté par Splunk 38
Figure 13: Fonctionnalités de Splunk 39
Figure 14: Architecture d'OSSIM 40
Figure 15: Magic cadran de Gatner sur l'étude comparative des SIEM 42
Figure 16:Interconnexion de QualysGuard 46
Figure 17: Architecture applicative du SOC 28
Figure 18: Architecture proposée 51
Figure 19:Balayage des ports actifs 57
Figure 20: résultat du Ip Angry Scanner 58
Figure 21: Authentification sur Nessus Essentiel 59
Figure 22: Tableau de bord Nessus 60
Figure 23:Création de scan avancé 60
Figure 24: création d'une nouvelle stratégie 61
Figure 25: planification d'un scan automatique 61
Figure 26: Règle de conformité 62
Figure 27: Activation des plugins 63
Figure 28: Démarrage du scan 63
Figure 29: Résultat de scan Avancée 64
Figure 30: détection de vulnérabilités 65
Figure 31:détails sur la vulnérabilité 66
Figure 32: Ajout d'un compte l'administrateur 67
Figure 33: Connexion à l'administrateur Web OSSIM 68
Figure 34: Menu principal OSSIM 69
Figure 35: Ajout des hôtes 70
Figure 36: Remplissage de formulaire pour création d'hôte 71
Figure 37: Création de groupe 71

Figure 38: Ajout des hôtes dans le groupe 72
Figure 39: Déploiement de HIDS 72
Figure 40:Ajout d'adresse IP de l'agent HIDS.....73
Figure 41: Ajout de l'agent HIDS avec succès.....73
Figure 42: Téléchargement de l'agent OSSIM.....74
Figure 43: Installation de l'agent OSSIM 74
Figure 44: Redémarrage du HIDS.....75
Figure 45: L'agent HIDS a été bien activé 75
Figure 46: Capture de la machine qui sera attaquée.....76
Figure 47:installation du metasploit 76
Figure 48: lancement de l'exploit par l'attaquant 77
Figure 49: Utilisation de la commande show option pour voir les détails de l'exploit.....77
Figure 50: définition de la machine cible 78
Figure 51: introduction de l'attaquant dans la machine cible 78
Figure 52: Affichage des dossiers de la cible par l'attaquant.....79

Table des tableaux

Tableau 2: Etude comparative sur l'accessibilité entre Qradar, Splunk et OSSIM.....43
Tableau 4: Etude comparative des solutions des vulnérabilités 49

Sigles et abréviations

SOC	Security Operation center
ANSSI	Agence nationale de la sécurité des systèmes d »information
CNIL	Commission Nationale de l'Information et des Libertés
SIEM	Security information and Event management
CERT	Computer Emergency Response Team
AOF	Afrique Occidentale Française
DEA	Diplôme d'Etudes Approfondies
ADIE	Agence de l'informatique de l'Etat
AES	Advenced Encryption Standard
SIEM	Security Event Information Management
SSI	Sécurité des Systèmes Information
SMIS	Système de Management de la sécurité de l'information
MSSP	Management Security Service Provider
HSRP	Hot Standby Router Protocol
OSSIM	Open Source Security Information Management
SLA	Service-level agreement

Introduction

Aujourd'hui la majorité des populations possèdent un accès à internet et il est possible de se connecter avec le bout du monde depuis n'importe où, pour garder le contact avec ses proches ou travailler à distance ou que l'on soit, grâce à un accès continu aux informations. Les réseaux sont devenus une partie intégrante de notre vie quotidienne. Les entreprises en tout genre, tout comme les instituts médicaux, ou les établissements financiers, étatiques et scolaires, utilisent ces réseaux pour leur bon fonctionnement.

Elles utilisent le réseau en recueillant, en traitant, en stockant et en partageant d'énormes quantités d'informations numériques. Cependant, puisse que le volume d'information numérique rassemblé et partagé croit quotidiennement et sans contrôle, il est devenu essentiel de protéger notre identité, nos données, nos périphériques informatique contre les violations de données, et la cybercriminalité en général.

Les cybers menaces entrent de façon pérenne dans la réalité quotidienne des entreprises. Elles ne ciblent plus seulement les systèmes technologiques, mais aussi directement les personnes (salariés, prestataires, fournisseurs, clients), en leur dérobant des informations primordiales qui accroissent ensuite considérablement leur capacité de nuisance. Les cybers attaques sont et seront de plus en plus fréquentes, multiples, discrètes et évolués. L'écosystème complet de l'entreprise s'en trouve directement menacé. L'impact des attaques réussies peut être immense sur le plan social, économique, politique et personnel et les motivations des cybercriminels sont aussi diverses que leur techniques. Alors que certains attaquants ont des motivations purement financière, d'autres poursuivent des objectifs politiques ou étiques.

Face à ces menaces croissantes contre nos systèmes et nos données, le concept de cyber-sécurité est né. La cyber-sécurité consiste en l'effort continu de protection des systèmes mis en réseau et des données contre leur utilisation non autorisée. Parmi les stratégies de défenses contre les cyber-attaques, l'une des plus pertinentes est la mise en place d'un centre opérationnel de cyber-sécurité (CSOC) ou SOC (Security Operations Center).

Un SOC peut être défini comme une équipe organisée, et hautement qualifiée, dont la mission est de surveiller, prévenir, détecter, analyser, et réagir aux incident de cyber-sécurité, et d'améliorer continuellement la posture de sécurité d'une organisation à l'aide des technologies et des procédure bien définis. Le but de ce mémoire est de faire une étude exhaustive des outils existants qui pourront nous aider sur la mise en place du SOC. Le document est structuré en trois parties étalées sur 6 chapitres :

- La première partie intitulée cadre de référence et méthodologique, où il s'agira de faire une présentation de la structure et du sujet d'étude, une élaboration de la problématique et les solutions à apporter.
- La deuxième partie endossera l'étude de la sécurité des SI de façon générale, les concepts et fondamentaux du SOC, l'étude comparative des solutions ainsi que le choix des outils.

- La troisième partie s'accentuera sur la mise en œuvre de la solution, les tests et simulations.

Partie I : Cadre de référence et méthodologique

Chapitre 1 : cadre de référence

1.1 *Présentation de la structure*

a. *Présentation de la Présidence de la république du Sénégal*

La présidence de la république est une institution étatique construite en 1902 sous les ordres de Gaston Doumergue, ministre des Colonies, qui visait à loger dans la capitale le gouverneur général de l'AOF qui résidait alors à Saint-Louis. L'architecte est d'Henri Deglane. Après cinq années de travaux, ce bâtiment de facture néoclassique, surmonté d'une tour inspirée du Trocadéro de Paris, est inauguré le 28 juin 1907 comme palais du Gouvernement général. Le gouverneur général alors en fonction, Ernest Roume, est le premier à y demeurer. Il avait pour tâche de transférer le siège du Gouvernement général de l'AOF de Saint-Louis à Dakar et mettre en place les structures administratives centrales de ce vaste ensemble territorial.

Entre temps, le bâtiment fut modernisé par le haut-commissaire Paul Bechard, locataire des lieux de 1947 à 1951. Et c'est sous sa nouvelle configuration que l'occupa, pour la première fois, le premier Président de la République du Sénégal, Léopold Sédar Senghor. [1]

b. *Secrétariat général de la présidence de la république et les services rattachés*

Le Secrétariat général de la Présidence de la République est dirigé par un Secrétaire général, nommé par décret et placé sous l'autorité du Président de République, dont il peut recevoir délégation de signature. Il assiste aux Conseils des ministres, aux Conseils présidentiels et aux Conseils interministériels. Le Secrétaire général est entouré d'un ou plusieurs Secrétaires généraux adjoints, également nommés par décret. [1]

Les services rattachés au secrétariat général de la présidence de la république sont :

- Contrôle financier
- Bureau Organisation et Méthodes (BOM)
- Bureau de suivi
- Direction des Moyens généraux
- Direction de la Coopération technique
- Commission de Contrôle des Véhicules Administratifs (CCVA)
- Commission de contrôle et de Suivi du Patrimoine immobilier de l'Etat à l'étranger (CSPIE)
- Pôle Economie
- Pôle Finances et Fiscalité
- Pôle Santé et Sport
- Pôle Cohérence territoriale
- Cellule de passation des Marchés publics
- Bureau du Courrier général et de la Documentation
- Service du Parc automobile
- Service informatique

- Service technique central du Chiffre et de la Sécurité des Systèmes d'information (STCC/SSI)
- Laboratoire radioélectrique
- Bureau d'Assistance sociale
- Cellule des Affaires juridiques
- Cellule Formation, Education et Culture
- Conseil des Infrastructures
- Comité national chargé de la Gestion de la Situation des Réfugiés, Rapatriés et Personnes déplacées
- Parc spécial automobile

Chapitre 2 : cadre Méthodologique

2.1 Etude de l'existant

A considérer que tout ce qui est gestion des SI au sein de la Présidence a toujours été géré par l'Agence de l'Informatique de l'Etat (ADIE), donc une étude approfondie de notre réseau s'impose au préalable afin de déterminer les limites de ce dernier.

En outre, nous avons trouvé sur place un Firewall ASA 5515, situé sur l'interface entre la structure et le réseau de l'opérateur. Le réseau est aussi subdivisé en plusieurs Vlans toujours pour renforcer la sécurité. Pour les échanges de données, un serveur autority certificat est mis en place pour chiffrer les documents (les documents ne partent pas en clair) ainsi que le canal de transmission. On a aussi un réseau VPN AES 256 qui permet de sécuriser les échanges de données entre les différentes structures (départements).

Sur ce, les limite du réseau ainsi que les solutions apportées par notre SOC seront présentées aux autorités. C'est après validation que nous passerons à la mise en place proprement dite de la plateforme.

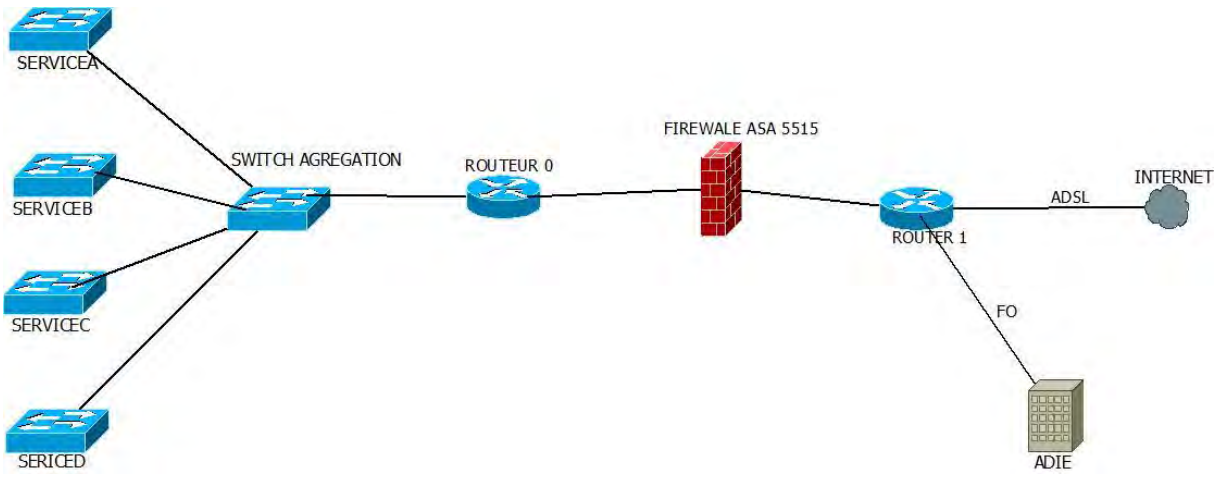


FIGURE 1: ARCHITECTURE GÉNÉRALE DU RÉSEAU

2.2 Problématique

La Présidence de la République étant une institution étatique, est par définition une cible, car toutes les stratégies de sécurité sont gérées à ce niveau. Cependant, nous avons notés beaucoup manquement dans la sécurité de leur système d'information :

- La confidentialité des échanges d'information au sein de la Présidence et entre la Présidence et les autres institutions (ministères, assemblée nationale, primature …) est insuffisant.
- La non supervision du réseau est à déplorer : en effet, les autorités étatiques ne savent pas si leurs données sont en train d'être dérobés ou pas, pire encore, ils n'ont aucune visibilité sur cela à l'heure actuelle, et ce qui est sûr, c'est que des personnes malveillants feront tout (si ce n'est pas déjà fait) pour savoir ce qui se passe au sein de la structure.

- L'absence d'outils performants pour assurer le contrôle d'accès ainsi que l'authentification des utilisateurs du réseau font que les risques d'attaques deviennent récurrents.
- L'absence d'outils pouvant nous permettre, après une attaque d'en connaitre l'origine et l'ampleur (qui a fait l'attaque, d'où vient l'attaque, par où est passé l'attaquant pour faire son action …) ne va pas à notre avantage.

Donc l'axe d'effort sera d'abord d'unifier le réseau, c'est à dire trouver les outils nécessaire qui nous permettrons de centraliser l'administration de la sécurité du réseau. D'où l'idée de la mise en place d'une salle de supervision fonctionnelle avec des équipes qui tourne 24h/7 pour avoir une meilleure visibilité à temps réel du réseau, a l'occurrence le Security Opération Centre (SOC).

En effet, le SOC apparait comme étant un modèle d'organisation qui répond aux problématiques opérationnelles de cyber sécurité. Il est conçu pour être au centre d'un très grand nombre d'évènements qui doivent être surveillés, analysés et corrélés. Ceci nous permettra donc je centraliser la surveillance des différentes activités au sein de la Présidence elle-même, mais entre cette dernière et ses différentes branches. De plus, sachant que les attaques sont motivés par trois raisons essentielles : soit frauder, espionner ou saboter ; alors, que les données soient stockées, en traitement ou en transit, leur sécurité doit être assurée.

2.3 *Objectif*

La présidence de la république a besoin d'une solution de qualité et sur mesure pour la protection et la surveillance de ses données. Mais aussi pour assurer un haut niveau de réactivité par rapport aux incidents.

L'objectif principal de notre travail consistera à :

- Mettre en place un SOC qui nous permettra de recenser les vulnérabilités afin de prévenir certaines attaques.
- D'unifier le réseau, afin d'en avoir une vue d'ensemble ;
- Détecter les intrusions en passant par l'analyse, l'exploitation et la corrélation des logs.
- Faire une étude de la faisabilité de notre projet en termes de temps, d'espace et de moyen.

Cependant, notons que le SOC assure de plus larges fonctionnalités, notamment :

- La réponse aux incidents, c'est à dire les actions à mener en cas d'attaque informatique
- le maintien des activités après une attaque.
- la récupération et l'investigation en cas d'incident ;
- …

Mais nous nous limiterons sur ce document à l'analyse, l'exploitation et la corrélation des logs.

Partie II : généralités sur le Security Operations Center (SOC) et la sécurité des systèmes d'information

Chapitre 3 : La sécurité des systèmes l'information

3.1 *Le système d'information et le système informatique*

Ce sont deux concepts très souvent mélangés, ou utilisé avec une imprécision flagrante. En effet, le système d'information (SI) peut être défini comme un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de traiter, de communiquer des informations de toutes formes dans une organisation.

Le système informatique quant à lui est l'ensemble des actifs matériels et logiciels de l'entreprise ayant pour vocation d'automatiser le traitement de l'information. C'est la partie visible à laquelle tout le monde pense quand on parle de projets et d'infrastructures informatiques.

Donc en d'autres termes, le système d'information est plus vaste que le système informatique. En fait, le système d'information peut être analogique, physique, numérique etc. Et quand il est numérique, il se sert du système informatique pour travailler. Le système informatique est un outil de travail du système d'information. Le système informatique utilisera des ordinateurs, imprimantes, Switch, routeurs, connexion … alors qu'un autre système utilisera le papier.

Il faudra donc protéger le système informatique en protégeant le système d'information en entier.

3.2 *La sécurité des systèmes d'information*

a) La sécurité des SI de manière générale

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire à la mise en place des moyens visant à empêcher l'utilisation non autorisé, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Aujourd'hui, la sécurité est un enjeu pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien. Sa finalité sur le long terme est de maintenir la confiance des clients et des utilisateurs.

La finalité sur le moyen terme est la cohérence de l'ensemble du système d'information. Sur le court terme, l'objectif est que chacun ait accès aux informations dont il a besoin. La norme traitant de SMIS est l'ISO/CEI 27001 qui insiste sur les termes Disponibilité, Intégrité et Confidentialité.

b) Objectifs de la sécurité des SI

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité des systèmes d'information vise les objectifs suivants :

- La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
- L'intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En somme, les éléments considérés doivent être exacts et complets
- La confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leurs sont destinées. Tout accès indésirable doit être empêché.
- La traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables
- L'authentification : l'identification des utilisateurs est fondamentale pour gérer l'accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- Le non répudiation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur. [2]

Par ailleurs, la sécurité des systèmes d'informations peut être renforcée par un ensemble de mesures politiques, légales, et/ou technologiques appelé **cyber-sécurité**.

c. Démarche générale de sécurisation des systèmes d'information

Assurer la sécurité des SIs ne se limite pas tout simplement à la mise en place d'un système bien sécurisé, mais plutôt garantir la sécurité de manière durable, continuelle et évolutive. Pour assurer une telle continuité, nous faisons appel à la roue de Deming avec PDCA.

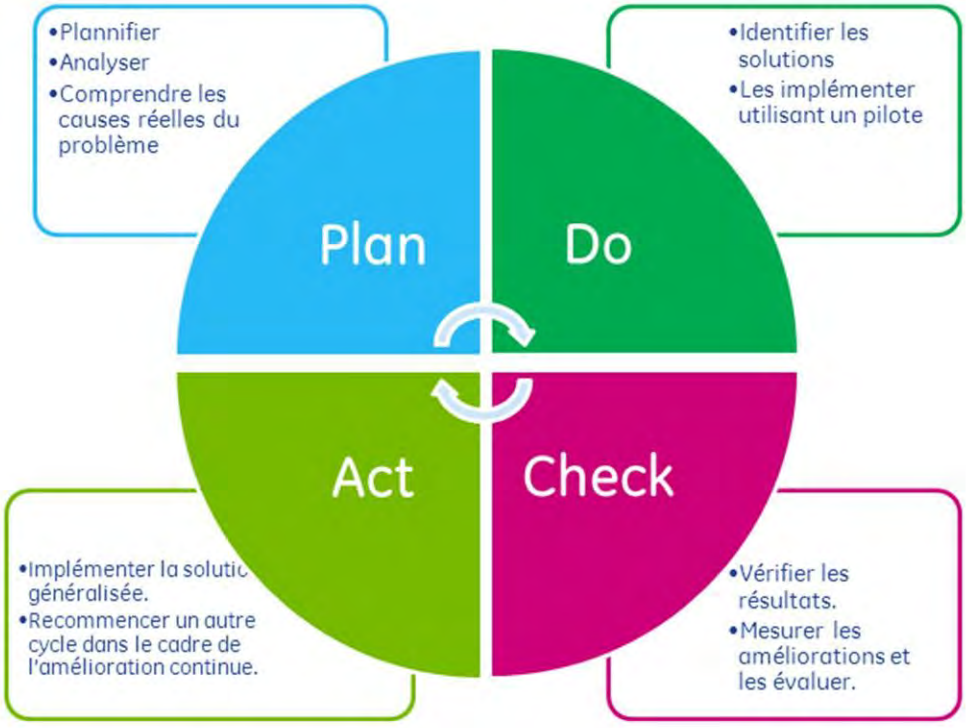


Figure 2: Roue de Deming PDCA

Phase plan : Planification de la démarche de sécurité des systèmes d'informations

- ✓ Périmètre et politique
- ✓ Evaluation des risques
- ✓ Traiter le risque identique
- ✓ Sélectionner les mettre en place

Phase Do : Mise en place des objectifs

- ✓ Plan de traitement des risques
- ✓ Déployer les mesures de sécurité
- ✓ Générer des indicateurs
- ✓ Former et sensibiliser le personnel
- ✓ Gérer le SMSI au quotidien
- ✓ Détection et réaction rapide des incidents

Phase Check : Mise en place de moyens de contrôle

Il doit y avoir des moyens de contrôle pour surveiller l'efficacité du SMSI ainsi que sa conformité grâce à des audits et contrôles internes. Par exemple : COBIT, ITIL, ISO/CEI 27007.

Phase Act : Mise en place des actions

Après la mise en lumière de dysfonctionnement grâce à la phase Check, il est important de les analyser et de mettre en place :

- ✓ Des actions correctives : il faut agir sur le dysfonctionnement et en supprimer son effet ;
- ✓ Des actions préventives : on agit avant que le dysfonctionnement ne se produise ;
- ✓ Des actions d'améliorations : on améliore les performances d'un processus. [3][4]

3.3 *Les attaques informatiques*

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.

a) Les différents types d'attaques

Les menaces informatiques sont variées et redoutables d'efficacité. Toutes les études arrivent à la même conclusion : les entreprises sont de plus en plus victimes de piratage informatique. Au bilan de l'année 2017, une hausse de 170% des cyberattaques avec prise de contrôle par rapport à l'année passée (chiffre du rapport « Cybercrime Report 2017 : A tear in Review », publié par Threat Metrix).

Dans la plupart des cas, les cybercriminels cherchent à récupérer de l'argent ou à monnayer les données qu'ils ont dérobées. Voici un tour d'horizon des différentes menaces auxquelles sont confrontées les entreprises.

Il est ainsi possible de catégoriser les risques de la manière suivante :

- ➔ Accès physique : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

- Coupure de l'électricité,
- Extinction manuelle de l'ordinateur,
- Vandalisme,
- Ouverture du boitier de l'ordinateur et vole du disque dur,
- Écoute du trafic sur le réseau,
- Ajout d'éléments (clé USB, point d'accès wifi …)

➔ Interception de communication :
- Vol de session,
- Usurpation d'identité,
- Détournement ou altération de messages,

➔ Dénis de service : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de service suivant :
- Exploitation de faiblesse des protocoles TCP/IP,
- Exploitation de vulnérabilité des logiciels serveurs,

➔ Intrusions :
- Balayage de ports,
- Élévation de privilèges,
- Malicieux (virus, verts chevaux de Troie)

➔ Ingénierie sociale : c'est une attaque d'accès qui tente de manipuler les individus dans l'exécution d'actions ou la divulgation d'informations confidentielles. Les ingénieurs sociaux comptent souvent sur la volonté des gens d'être utiles. Ils s'attaquent aussi aux faiblesses des gens. Il existe de nombreux exemples d'outils d'ingénierie sociale disponibles :
- Pretexting
- Phishing
- Spear phishing
- Spam
- Tailgating
- Quelque chose pour quelque chose (Quid pro quo)
- Appâtage

3.4 *Lois et recommandations régissant la cyber-sécurité au Sénégal*

Dans sa volonté de réussir le défi de son développement, le Sénégal a adopté une stratégie nationale qui rompt avec les approches des dernières décennies et inscrit le Sénégal dans une nouvelle trajectoire de développement économique et social, car force est d'avouer que la sécurité informatique au Sénégal laisse à désirer. En effet, tous les jours plusieurs failles sont découvertes dans les systèmes d'information des grandes entreprises qui sont souvent très négligentes. Dans ce monde technologique, toutes erreurs se paient cash et les conséquences sont parfois désastreuses. Les niveaux de vulnérabilité et le taux de négligence sont très élevés, hacker un système ou un site internet devient un jeu d'enfants pour ces hommes de l'ombre.

Dès lors, protéger ces systèmes et ces informations devient alors une priorité nationale pour le Sénégal, et dans ce sens plusieurs stratégies nationales sont mises en place pour transformer le Sénégal en une société numérique mais aussi plus sur pied en cyber-sécurité à savoir :

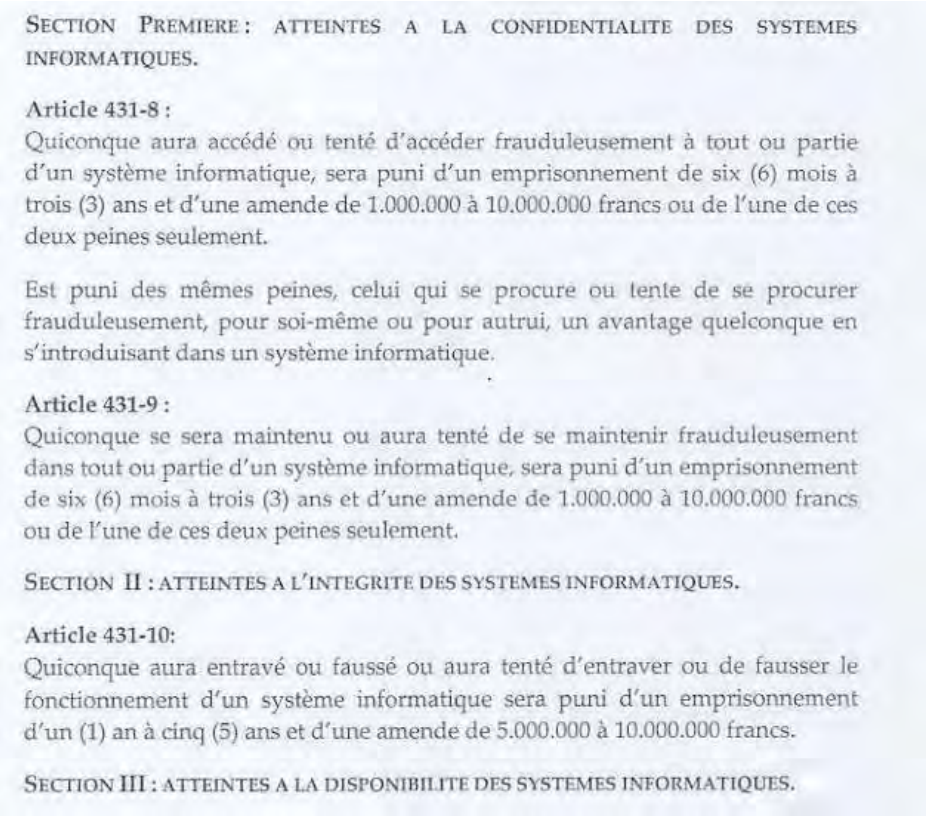
- Le Sénégal Numérique 2025 « SN2025 »
- La stratégie nationale de cyber-sécurité 2022 « SNC 2022
- La politique de sécurité des systèmes d'information de l'Etat du Sénégal (PSSI-ES) [5]

a) Les lois sur la cybercriminalité au Sénégal

Afin de garder l'intégrité des propos concernant les lois et les atteints prisent ici au Sénégal, nous avons jugé nécessaire d'être fidèles au document, raison pour laquelle nous avons fait des prises de captures d'écran de la source au lieu de copier ou rédiger les lois.

La loi sur les documentations est énorme du coup nous avons juste prie une partie nous informant sur tout ce qu'il faut savoir pour tout individus utilisant les technologies de l'information et de la communication. Voir les images ci-dessous :

Référence : https://www.sec.gouv.sn/sites/default/files/PSSI-ES.pdf.



SECTION PREMIERE : ATTEINTES A LA CONFIDENTIALITE DES SYSTEMES INFORMATIQUES.

Article 431-8 :
Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 431-9 :
Quiconque se sera maintenu ou aura tenté de se maintenir frauduleusement dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

SECTION II : ATTEINTES A L'INTEGRITE DES SYSTEMES INFORMATIQUES.

Article 431-10:
Quiconque aura entravé ou faussé ou aura tenté d'entraver ou de fausser le fonctionnement d'un système informatique sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs.

SECTION III : ATTEINTES A LA DISPONIBILITE DES SYSTEMES INFORMATIQUES.

Capture 1: Lois sur la cyber-sécurité au Sénégal

b) Recommandation de l'ANSSI et du CNIL

- Recommandation du CNIL

Le responsable d'un système d'information doit mettre en place un dispositif de traçabilité, adaptés aux risques associés à son système. Celui-ci doit enregistrer les événements pertinents, garantir que ces enregistrements ne peuvent être altérés, et dans tous les cas conserver ces éléments pendant une durée non excessive. Les journaux doivent conserver les événements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou demande de la CNIL, de conserver ces informations pour une durée plus longue).

Prévoir au minimum la journalisation des accès des utilisateurs incluant leur identification, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. Le format de l'horodatage doit de préférence prendre comme référence le temps UTC. Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que les données consultées par exemple. Les précautions à prendre sont les suivantes :

-informer les utilisateurs de la mise en place d'un tel système.

-protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés

-établir des procédures détaillant la surveillance de l'utilisation du traitement et procéder périodiquement à l'examen des informations journalisées.

-le responsable de traitement doit être informé dans les meilleurs délais des failles éventuelles de sécurité.

-en cas d'accès frauduleux à des données personnelles, le responsable de traitement devrait le notifier aux personnes concernées. [6]

➢ Recommandation de l'ANSSI pour la mise en place d'un SOC

- Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.
- Le prestataire doit respecter la législation et la réglementation en vigueur sur le territoire national.
- Le prestataire doit décrire l'organisation de son activité de détection des incidents de sécurité auprès du commanditaire.
- Le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire.
- Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de sa prestation et en particulier les éventuels dommages causés au commanditaire. À ce titre, le prestataire doit préciser les types de dommages concernés et les modalités de partage des responsabilités dans la convention de service, en tenant compte de toutes les éventuelles activités sous-traitées.
- Le prestataire doit souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de sa prestation.

- Le prestataire doit s'assurer du consentement du commanditaire avant toute communication d'informations obtenues ou produites dans le cadre de sa prestation.
- Le prestataire doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.
- Le prestataire doit apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts.
- Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de son personnel et de son infrastructure.
- Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.
- Le prestataire doit demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auquel il est soumis et notamment celles liées à son secteur d'activité.
- Le prestataire doit informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

La sécurité des systèmes d'informations en générale et la mise en place d'un SOC en particulier sont régis par des lois et règlements qui permettent à toutes les entreprises d'être en conformité avec les normes internationaux. [7]

Chapitre 4 : généralités sur le Security Operations Center

4.1 *Présentation générale du SOC*

Le Security Operating Center est un centre de supervision et d'administration de la sécurité. Le terme SOC désigne ainsi une plateforme dont la fonction est de fournir des services de détection des incidents de sécurité, mais aussi de fournir des services pour y répondre. Le centre de sécurité va ainsi collecter les événements (sous forme de logs notamment) remontés par les composants de sécurité, les analyser, détecter les anomalies et définir des réactions en cas d'émission d'alerte.

Le développement des SOC s'explique notamment par une amélioration des débits et la maturité des outils d'acquisition et de stockage des logs. Le durcissement réglementaire, le besoin d'assurer la traçabilité et la maitrise de la sécurité du système d'information encouragent également la création de SOC (ou le recours à des prestataires disposant de tels centres).

Un SOC est avant tout une équipe d'experts en sécurité chargée de surveiller, détecter, analyser et qualifier les évènements de sécurité. Cette équipe assure le pilotage des réactions appropriées aux incidents avérés de sécurité. Pour certaines organisations, cette équipe administre et contrôle au quotidien des dispositifs et dispositions de sécurité.

Un SOC est pour une entreprise ou un organisme quelconque la possibilité d'administrer la sécurité de son parc informatique à distance en collectant et corrélant les logs de ses différents équipements et applicatifs de sécurité (pare-feu, IDS/IPS, VPN, antivirus, etc.), ou réseau. La corrélation d'événements provenant de sources différentes et l'analyse en temps réel peuvent ainsi permettre une identification rapide des risques, notamment d'intrusion.

Il doit également contribuer à réduire les risques et l'indisponibilité des composants critiques du système d'information, mais aussi à identifier les menaces, à les prévenir, à raccourcir les délais d'intervention ou encore à simplifier l'administration. Il reste néanmoins complexe de collecter et de corréler de très nombreux logs émis dans des formats divers pour n'identifier que les alertes pertinentes. [9] [10]

Figure 3: Vue globale du SOC

4.2 *Le rôle d'un SOC*

Un SOC a pour objectif de réduire à la fois la durée et l'impact des incidents de sécurité qui tirent profit, perturbent, empêchent, dégradent ou détruisent les systèmes dédiés aux opérations habituelles et standards. Cet objectif est atteint grâce à une surveillance efficace et à un suivi des incidents de bout en bout.

Le SOC a la responsabilité, d'une part, de déclarer qu'il y a effectivement un incident sur le SI, et, d'autre part, il est responsable de la conduite des opérations qui lui permettront de déclarer l'incident clos. Du point de vue opérationnel c'est le couple des entités SOC et CERT/C-SIRT qui assure la résolution d'un incident.

Par ailleurs, selon les choix organisationnels, le SOC peut également assurer les missions suivantes :

- Suivi des vulnérabilités (de la détection à la correction) ;
- Veille en sécurité informatique ;
- Sensibilisation des utilisateurs en fonction des observations faites sur le SI ;
- Expertise et conseil auprès des équipes informatiques ;
- Pilotage de la mise en œuvre des correctifs de sécurité.

Compte tenu de la variété des missions, des impacts technologiques ainsi que des impacts organisationnels majeurs, la mise en œuvre d'un SOC représente un réel investissement en temps et ressources pour l'Entreprise concernée; même avec l'aide d'un prestataire qualifié (type MSSP). C'est aussi pourquoi il est généralement nécessaire que l'Entreprise atteigne une taille critique avant de consacrer des ressources internes à l'opération de son propre SOC. Dans

le cas des entreprises constituées de plusieurs entités, il est fréquent que le SOC soit porté par l'une d'entre elle de façon transverse pour les autres. [11]

4.3 Catalogue de service et fonction d'un SOC

On peut regrouper les services d'un SOC en 4 principales catégories aux objectifs distincts : voir figure ci-dessous.

Figure 3: les principaux services offerts par un SOC

a. Fonction de prévention sécurité

Le SOC doit être vu comme un outil de prévention sur la base des informations traitées et des actions préventives qui peuvent en découler. La prévention passe également par des actions de sensibilisation auprès des interlocuteurs du SOC.

- **Gestion des vulnérabilités** :

Ce service peut être rendu par le SOC ou si ce n'est pas le cas, le SOC doit bénéficier des informations sur les vulnérabilités connues du système d'informations pour affiner ses analyses d'impacts des événements de sécurité. La gestion des vulnérabilités comprend la veille, la qualification, les préconisations puis le suivi du déploiement des patchs indiqués. Elle s'effectue également en lien avec le service de détection de vulnérabilités et de contrôle sur les actifs du périmètre surveillé par le SOC.

- **Implication dans le processus de sensibilisation :**

Les incidents remontés par le SOC peuvent être le déclenchement d'actions de sensibilisation. Ces actions peuvent être ciblées pour recadrer par exemple un utilisateur déviant, ou généralisées pour toucher plus de monde sur des données plus transverses.

b. Fonction de détection

La fonction de détection est toujours à la base du SOC. La détection nécessite le traitement d'informations remontées par le SI surveillé. Ce traitement est plus ou moins automatisé selon les outils mis en place, mais il nécessite encore aujourd'hui un traitement manuel par des analystes sécurité. Les outils doivent être configurés pour analyser des données en relation avec des scénarios de détection prédéterminés. Ces outils classiques peuvent être complétés par des

outils d'analyse de comportements. Deux cas de figure peuvent arriver : trop de données inutiles engorgent les outils avec le risque de rater un événement permettant la mise en exergue d'un incident de sécurité, ou au contraire, il manque des données nécessaires à la détection et à la qualification de certains incidents. Le SOC doit continuellement adapter le paramétrage de ses outils pour limiter l'occurrence de faux positifs ou de vrais négatifs par exemple en adaptant les niveaux de seuil de détection.

- **Collecte des événements de sécurité et qualification des incidents**

L'objectif de ce service est de disposer d'une vision centralisée des événements de sécurité, permettant de réaliser des rapprochements et des corrélations mettant en évidence des incidents potentiels.

Les informations collectées sont analysées pour déterminer d'éventuelles anomalies ou incidents. Cette analyse nécessite des outils de traitements de logs ou des SIEM, complétés par les outils de gestion documentaire et la messagerie pour les informations en dehors des logs.

- **Contrôle**

Des contrôles de sécurité de divers niveaux peuvent être portés par le SOC.

Les contrôles basés sur des scanneurs de vulnérabilités configurés pour analyser les vulnérabilités visibles sur le système d'information, permettent de remonter au SOC l'état de sécurité des actifs du SI, et d'identifier d'éventuelles vulnérabilités ou menaces.

Les contrôles de conformité aux standards techniques permettent quant à eux de vérifier le respect des politiques de sécurité (ex : présence de droits administrateurs sur les postes, logiciels interdits,…), qui peuvent constituer autant de sujets à traiter. Des audits manuels peuvent également être réalisés par des auditeurs indépendants ou appartenant au SOC. Au niveau d'expertise le plus élevé, des tests d'intrusion peuvent être réalisés afin d'éprouver sans prévenir au préalable la perméabilité des systèmes.

- **Veille sur les menaces et « threat intelligence »**

Même si le SOC n'est pas en charge de maintenir la cartographie des risques, le SOC doit connaitre les menaces qui pèsent sur l'infrastructure surveillée et maintenir à jour le niveau des menaces pour renforcer si besoin certains contrôles ou actions de surveillance spécifiques à une menace.

La « threat intelligence » va plus loin en ce sens en réalisant une surveillance dans les milieux pirates des menaces en cours ou à venir vers l'entreprise ou son secteur d'activité. Le SOC permet alors de suivre les menaces externes réelles, concernant d'autres acteurs ou partenaires du même secteur d'activité ou de l'entreprise elle-même.

c. Fonction de réaction

La mise en œuvre d'un SOC oblige une réflexion de l'entreprise sur sa capacité à réagir à un incident de sécurité. Détecter sans réagir n'est clairement pas une solution. L'enjeu du SOC est d'adapter son niveau de support à la réaction à l'organisation de l'entreprise sachant que le SOC ne peut pas être le seul à réagir (le CSIRT entre fréquemment dans la partie).

- **Investigations et contribution à l'analyse**

En cas d'identification d'un incident, le SOC peut avoir un rôle à jouer (souvent en complément du CSIRT) dans la réalisation d'investigations permettant de mieux comprendre l'attaque en cours. Le SOC a en effet à sa disposition le SIEM et d'autres outils de détection, d'investigation et d'analyse post mortem qui permettent de réaliser des opérations d'investigation : analyse des logs passés, filtrage des logs, rapports de scans sur des actifs particuliers, opérations sur les produits de sécurité des postes de travail (antivirus, HIPS,…).

- **Participation à la réaction**

Le SOC peut également contribuer à la réaction dans la limite de son périmètre de responsabilité, via ses activités d'administration d'outils de sécurité. L'activation d'une règle IPS, la fermeture d'un compte administrateur ou VPN, l'ajout d'une règle pare-feu sont des exemples de réactions pouvant faire intervenir le SOC.

d. Fonction d'administration sécurité

Au-delà de son infrastructure et de ses outils propres (Logs manager, SIEM et autres), le SOC peut exploiter les composants sécurité ainsi que l'infrastructure de collecte. Ce service doit être rendu pour l'infrastructure SOC par l'équipe SOC. Pour les autres composants sécurité, le SOC peut être en charge ou non. Dans ce dernier cas, le SOC se doit d'être en relation directe avec l'équipe d'exploitation sécurité. [12]

4.4 *Les différents modèles de SOC*

La mise en place d'un SOC est un projet d'envergure transverse avec des impacts opérationnels importants. Le Support explicite de la direction est indispensable pour justifier les dépenses récurrentes induites par une telle organisation. Encore faut-il opter pour le bon modèle de SOC selon son organisation, ses enjeux et ses moyens.

- **SOC virtuel** : Pas d'installation dédiée, les membres de l'équipe à temps partiel, réactif, activé en cas d'alerte ou d'incident critique.
- **SOC dédiée** : Installation dédiée, équipe dédiée, entièrement à l'interne.
- **SOC externalisé** : il s'agit ici de faire appel à un prestataire externe qui dispose des ressources humaines et technologique pour offrir les services d'un SOC.
- **SOC distribué / co-géré** : les membres de l'équipe sont dédiés et semi-dédiés, avec typiquement 5×8 au niveau opérationnels, lorsqu'il est utilisé avec un MSSP, ce SOC est cogéré.

En plus de ces principaux modèles listés ci-dessus, nous trouvons encore d'autres modèles tels que :

- **SOC de commande** : il coordonne les autres SOC, fournit des renseignements sur les menaces, la connaissance de la situation et une expertise supplémentaire. Il est rarement impliqué directement dans les opérations au jour le jour.
- **Centre d'opérations SOC / Network Operations Center (NOC)** : c'est une installation dédiée, avec une équipe dédiée effectuant non seulement la sécurité mais également d'autres opérations informatiques critiques 24/7 de la même installation pour réduire les coûts.

- **Next gen SOC ou fusion SOC** : ce type de SOC reprend les fonctions du SOC traditionnelles et les nouvelles fonctions telles que l'intelligence des menaces (Threat intelligence), une équipe d'intervention en cas d'incident informatique (CIRT) et les fonctions de technologie opérationnelle (OT). [13]

a) Architecture d'un SOC

L'architecture du SOC est composée d'une première phase qui consiste à la collecte de journaux d'événements sur les applications et équipements grâce aux collectors, ces journaux d'événements sont envoyés directement aux processeurs. La deuxième phase est l'ensemble des mécanismes qui consiste à traiter les journaux afin de dégager les incidents de sécurité par le biais des processors. Après l'identification et la prise en charge de l'alerte, la dernière phase est le reporting qui consiste à faire un rapport d'activité sur l'incident.

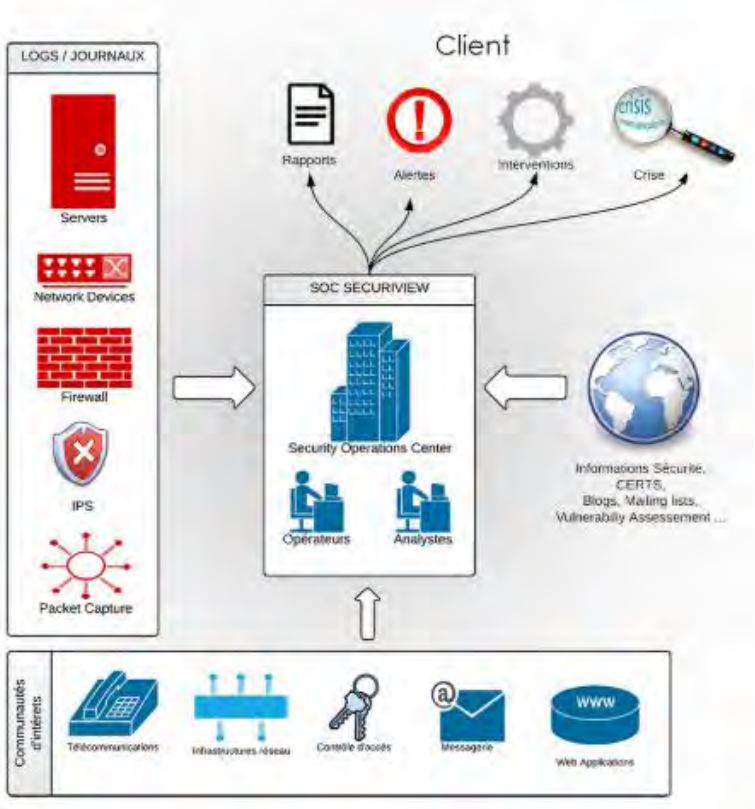


Figure 4: Architecture fonctionnelle

4.5 Complémentarité entre le SOC et CERT/CSIRT

a) Différence entre SOC et CERT/CSIRT

Selon l'ENISA, un CSIRT est défini comme 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 limite entre SOC et CSIRT n'est pas toujours évidente à tracer. Seul un modèle de gouvernance et des responsabilités clairement établies permettent de partager détection, réaction et suivi des incidents. Les adhérences entre le modèle de sécurité de l'Entreprise et l'organisation de l'Entreprise peuvent constituer un frein supplémentaire au partage des tâches et responsabilités (il n'est pas rare que les fonctions/rôles des deux entités soient portés par les mêmes personnes). [13]

Figure 5: Limite des responsabilités SOC/CERT

Il est cependant communément admis que le SOC est responsable de la gestion des vulnérabilités, de la détection et de la qualification des incidents de sécurité alors que le CSIRT est responsable de la gestion de crise cyber (notion plus large que la réaction à un incident de sécurité) et de la veille autour des cyber-menaces (y compris les analyses *forensics*).

a) Synergie entre SOC et CERT

Si la limite entre les deux entités n'est pas clairement définie, les adhérences et interfaces n'en sont que plus nombreuses. Ainsi, en considérant la chaîne plus détaillée présentée ci-dessous, le curseur du partage des missions est laissé à l'appréciation de l'organisation. L'efficacité de la sécurité dépend de la complétude de la chaine et non de la répartition des missions.

Figure 6: Complémentarité entre SOC et CERT

En complément, il est primordial de bien organiser le ou les passages de témoins (*a minima* qualité et quantité de l'information transmise et moyen de transmission) entre les différents acteurs responsables des missions. Toutes les interactions entre les missions et activités doivent être prises en compte et pas seulement les grandes interfaces.

Si le traitement et la veille sont généralement confiés au CSIRT, il faut noter que l'objectif est que le SOC gagne en maturité et en efficacité au fur et à mesure du traitement des incidents. La façon la plus simple d'atteindre cet objectif est de constituer des fiches de retours d'expériences (REX ou REEX) à l'issue de toute intervention du CSIRT. Ainsi, au fur et à mesure, si un incident est enregistré à propos de technologies, produits ou attaques connues, et que celui-ci fait l'objet d'une fiche ou procédure qui permet le traitement de l'incident, le SOC pourra dérouler la chaine sans avoir à solliciter l'entité CSIRT.

Selon ce modèle de maturité, le CSIRT n'est alors sollicité (en escalade) qu'en cas de nouvelle attaque (inédite) nécessitant une expertise spécifique. Le CSIRT pilote alors la résolution le temps de pouvoir industrialiser la remédiation. [13] [14]

4.6 Journaux, événement, flux, alertes et incidents

a) Les journaux

Les « journaux » ou « enregistrements » constituent la matière première (généralement à l'état brut) que le SOC devra manipuler, analyser, corréler tout au long de la journée. Tout élément d'un système d'information produit désormais des enregistrements agrégés en journaux. C'est à partir de ces éléments que sont créés les premières métriques et rapports d'activités d'un SOC. Constituant les logs d'un système actif, ces journaux sont généralement conservés à des fins d'exploitation ou d'investigation.

Ils sont parfois les seuls éléments (à charge) qui peuvent être utilisés en cas de comportement anormal ou suspicieux d'un système. Ils sont donc généralement protégés voire séquestrés pour être utilisés en tant que preuve.

Etant donné que tous les systèmes, et leurs composants (et leurs sous-composants) génèrent des traces, des enregistrements et des journaux, le défi consiste à déterminer le bon compromis entre la granularité (aussi appelée verbosité) des éléments produits par rapport à l'utilisation qu'un SOC peut en faire.

b) Les évènements et flux

Selon la norme ITIL v3, un « événement » correspond à un changement d'état suffisamment important pour être notifié à un gestionnaire du service. Ainsi, il peut s'agir d'un changement d'état normal ou, au contraire, d'un changement pour un état anormal (ex. une défaillance). Un événement peut être transcrit par un ou plusieurs enregistrements dans un journal. Dans le cadre de ce document, nous préférerons la définition de la norme ISO 27000 (2.20) qui précise qu'un événement de sécurité est une 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.

La différence majeure entre les données d'événement et les flux de données est la suivante :

Un événement, en général un journal d'une action spécifique telle une connexion utilisateur ou une connexion VPN, survient à une heure précise, et est consigné à ce moment-là.

Un flux d'enregistrement d'une activité réseau peut durer plusieurs secondes, minutes, heures ou jours, selon l'activité dans la session. Par exemple, une demande Web peut télécharger plusieurs fichiers tels que des images, des annonces, et des vidéos, et durer 5 ou 10 secondes, ou la session d'un utilisateur qui regarde un film en ligne peut durer quelques heures. Le flux est un enregistrement d'activité réseau entre deux hôtes.

c) Les alertes

Une alerte correspond à un événement ou à un groupe d'événements pondéré. Cette pondération est particulièrement importante puisqu'elle permet de classer les événements et de ne retenir que ceux qui atteignent ou dépassent un seuil de vigilance. Tout comme pour les enregistrements et journaux, le défi consiste à fixer correctement le seuil (ou à le retenir auprès d'un organisme tiers) pour ne conserver que les événements qui nécessitent une attention particulière.

Parce que les mécanismes qui associent une pondération à l'événement peuvent être défaillants ou inadaptés, les alertes peuvent être classées en différentes catégories :

- *Faux positif* : la pondération a été positionnée de façon inadaptée, rendant un événement important à tort. Dans ce cas, le comportement du système est considéré défaillant à tort.
- *Vrai positif* : la détection a été correctement positionnée. Il s'agit d'une alerte qui correspond réellement à un événement redouté ou à comportement anormal du système.
- *Faux négatif* : le mécanisme de détection n'a pas correctement fonctionné et un événement qui aurait dû être identifié en tant qu'alerte n'a pas été repéré et classé. Le système est défaillant et aucune alerte n'appuie ce statut.
- *Vrai négatif* : le mécanisme de détection est adapté. Le comportement du système n'est pas défaillant et aucun événement n'est identifié en tant qu'alerte à tort.

d) Incidents

Toujours selon la norme ITIL, un incident est une interruption non planifiée d'un service, une réduction de la qualité d'un service ou la défaillance d'un élément du système. Un incident est associé à un impact négatif (perçu ou non) sur la qualité de service globalement perçue par les utilisateurs du système. Un incident est généralement (mais pas toujours) caractérisé par une série d'alertes. Il est généralement enregistré, analysé et traité sur la base des éléments d'information le constituant. Un incident appelle une réponse.
Dans le contexte de la sécurité des systèmes d'information, la norme ISO 27000 (2.21) définit un incident comme un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information.
La chronologie suivante peut être établie :

Figure 7: chronologie (journal/évènement/alerte/incident)

Les incidents peuvent être catégorisés par le SOC ou le CSIRT, selon des critères propres à l'organisation, pour permettre un reporting à plus haut niveau et, outiller le pilotage de la sécurité des S.I. [13]

Chapitre 5 : les composants du SOC

Généralement, le SOC implique une combinaison d'outils technologiques, de processus et de personnel dédiés à la collecte, au tri et à l'investigation des incidents de sécurité :

- **Des technologies** : il s'agit de l'ensemble des moyens techniques utilisés pour collecter, corréler, stocker et établir un rapport sur les événements de sécurité. La solution de sécurité principale du SOC est le SIEM (Security Information and Event Management). C'est un outil de gestion des évènements du système d'information.
- **Des processus** : Les processus du SOC sont spécifiques à la supervision et à l'administration de la sécurité du SI. Ils ont pour objectif d'assurer la supervision du SI, la détection et la résolution des incidents de sécurité mais également d'apporter des améliorations au SOC sur la base de l'évaluation de ses processus, de l'évolution des menaces et des évolutions réglementaires.
- **Des moyens humains** : ce sont des experts en sécurité informatiques, Opérateurs, Analystes, Pentesteurs. Leur mission est d'interagir avec les équipes responsables de la sécurité des systèmes d'information au sein de l'entreprise, afin d'adapter au mieux le dispositif à l'organisation. Leur objectif principal est d'analyser les événements pour répondre aux incidents dans un délai réduit.

Figure 8: Les composants du SOC

5.1 *Technologies*

a) SIEM

i. Les fonctions d'un SIEM

Le SIEM ou encore Security Information and Event Management (système de gestion des informations et des événements de sécurité) est l'outil principal du SOC puisqu'il permet de gérer les évènements d'un SI. On peut définir le SIEM comme la collecte d'événements en temps réel, la surveillance, la corrélation et l'analyse des événements à travers des sources disparates.

Un SIEM est composé d'une première brique, le SEM ou Security Event Management (système de Gestion des Événements de Sécurité). Il répertorie tous les événements relatifs à la sécurité de notre Système d'Information en récoltant les logs, ou journaux, de nos serveurs informatiques, réseau, appareils, outils de sécurité… bref, tous les éléments qui le composent. Le SEM corrèle alors ces informations en temps réel afin de signaler tout comportement douteux, et d'alerter votre Security Manager afin qu'il puisse réagir immédiatement et protéger votre système d'information. L'avantage du SEM est qu'il permet une analyse plus fine de ces événements, et peut donc repérer davantage de menaces, que les outils de sécurité installés sur votre architecture. Grâce à une console, vous visualisez en temps réel ce qu'il se passe sur votre Système d'Information.

En plus du SEM, qui permet donc la collecte et l'analyse en temps réel des événements de sécurité, un **SIEM** se compose également d'un SIM (Security Information Management, ou Gestion des Informations de Sécurité). Cette deuxième brique permet de bénéficier d'une vision d'ensemble sur votre Système d'Information et sa sécurité, et de réaliser des analyses plus poussées… pour une amélioration continue de votre protection. Toutes les données récupérées puis corrélées par le SEM sont envoyées au SIM, qui les place dans un référentiel central et garde un historique complet. [15]

ii. Les principaux rôles d'un SIEM

Entre autre le SIEM rempli une panoplie de fonctionnalités, parmi lesquelles nous allons citer et définir quelques une :

➔ **La collecte des évènements**

Un SIEM regroupe des enregistrements qui détaillent ce qui se passe dans des applications spécifiques dans un environnement donné, comme un ordinateur de bureau périphériques, serveurs, routeurs et plus encore. Il regarde ce qui se passe, enregistre cela, puis l'organise. Cela prend ces données non seulement pour leur propre surveillance, mais aussi pour que vous puissiez trouver ces informations si vous en avez besoin - par exemple, ces enregistrements peuvent être nécessaires pour satisfaire aux normes de conformité d'une organisation. La collecte peut être passive ou active avec une mise en place directement sur les différents équipements ou à distance. La plupart des SIEM fonctionnent en déployant une multitude d'agents de collecte de manière hiérarchique. Ces agents collectent alors des événements liés à la sécurité sur les appareils des utilisateurs, les serveurs, les équipements réseau, voire les équipements spécialisés de sécurité, tels que les pare-feu, ou encore les systèmes antivirus et anti-intrusions.

➔ **La normalisation des évènements**

La normalisation des traces collectées au travers d'analyseurs spécifiques offre une corrélation multicritères standardisées (métadonnées : date, heure, IP, port et service…). Les traces brutes sont stockées sans modification pour garder une valeur juridique. De nombreux analyseurs natif sont disponible pour les solutions éditeurs et Open-source. Dans le cas échéant, la création d'un analyseur, spécifique pour des éléments à raccorder au SIEM est réalisable (offre une grande flexibilité d'intégration).La normalisation des évènements permet donc la conservation des logs bruts pour valeur juridique puis l'enregistrement de ces logs dans un format interprétable.

➔ **La corrélation**

La corrélation consiste à faire correspondre des événements de plusieurs systèmes (hôtes, dispositifs réseau, contrôles de sécurité, n'importe quelle source de logs). Des événements de plusieurs sources peuvent être combinés et comparés afin d'identifier des patterns de comportement invisibles avec une simple analyse. La corrélation permet d'automatiser la détection d'événements qui ne devraient pas se produire au sein d'un réseau. En somme, elle permet de faire une identification d'une ou de plusieurs menaces à l'origine d'un ou de plusieurs évènement.

➔ **Le reporting**

Il s'agit de la génération de tableaux de bord et de rapports pour avoir une visibilité sur la sécurité **et** la conformité du SI.

➔ **L'archivage**

La plupart des solutions de type SIEM disposent d'un système d'archivage des incidents et de toute trace ayant conduit à la génération de ceux-ci, afin de disposer de sauvegardes complètes des évènements survenus sur le SI. Pour garantir une meilleure sécurité, les données stockées pourront être chiffrées**,** signées, hachée, ou stockées sur des architectures distribuées et/ou dupliquées. La sécurité mise en place sur la sauvegarde de ces traces permettra de s'assurer qu'elles ne seront ni perdues ni modifiées au cours du temps, et permettra donc de les utiliser à des fins inforensiques ou juridiques. [16] [17] [18]

Le SIEM reste donc le cœur technologique du SOC à côté des analystes de processus et de sécurité, comme illustré dans la figure ci-dessous :

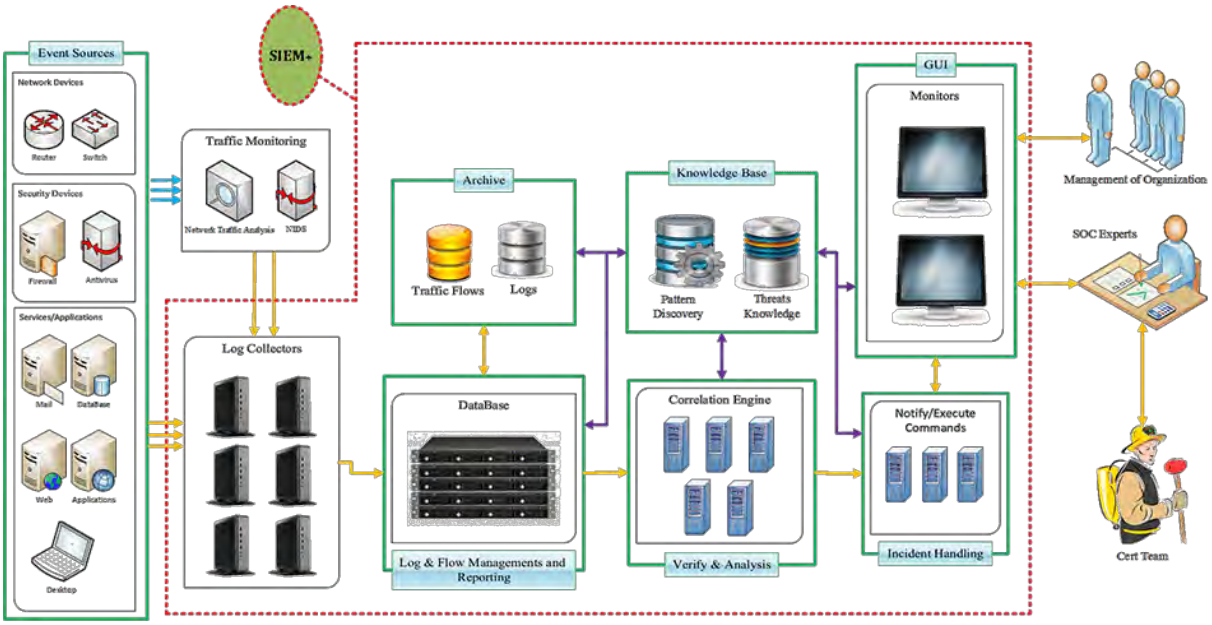


Figure 9: Architecture applicative du SOC

Nous avons dans un premier temps les sources de logs (machines, switchs, routeurs…) et le monitoring de trafic qui génère aussi des logs. Tous ces logs vont par la suite être collectés et

directement stockés dans la base de données du SIEM. Ils feront ensuite office d'analyse et de corrélation. Et dès qu'un incident ou évènement inhabituel est détecté, une alarme est directement lancée au niveau des écrans de monitoring gérés par l'équipe SOC. Cette dernière apportera les mesures correctives nécessaires selon le degré d'importance de l'alerte. Le manager SOC (ou chef de projet) aura aussi en sa disposition un tableau de bord pour pouvoir suivre l'aspect sécurité de son environnement réseau.

iii. Les limites du SIEM

Dans un système informatique, les logs permettent de savoir ce qui vient de se passer ou s'est passé il y a un certain temps. Le rôle d'un SIEM (Security Information Management System) est d'exploiter les logs.

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

Le SEM est limité en performances qui nécessitent de limiter le périmètre du système d'information à superviser. Il ne prend pas en compte des pans complets du système d'information, ciblent privilégiés des nouvelles attaques

Les principaux outils sont les solutions de contrôles de conformité en continue, de vulnérabilités et d'intégrité. Ces solutions permettent de fournir des informations sur les brèches utilisables par un attaquant, et suivent et tracent en profondeur les variations des systèmes ou les signes d'actions potentiellement illicites. [19]

b) Le scanner de vulnérabilité

Aujourd'hui la question n'est plus "sommes-nous en sécurité ?" mais plutôt "quel est mon niveau de sécurité et quelles actions mettre en place pour l'améliorer ?". Pour répondre à celle-ci et être en règle avec la législation et le RGPD notamment, l'outil le plus adapté est le scanner de vulnérabilités. Automatisé, il surveille en continu les failles exploitables par les hackers et détecte toutes les nouvelles vulnérabilités référencées. Il procure un gain de temps pour les équipes techniques qui n'auront plus à faire des analyses manuelles chronophages. Elles pourront donc corriger plus rapidement les failles, notamment les plus critiques qui sont les plus dangereuses.

Simple, rapide et efficace, le scanner de vulnérabilités a tout pour rassurer les entreprises et accompagner le travail des RSSI. A l'heure du RGPD et du durcissement des contraintes pénales, il serait regrettable que les entreprises pâtissent d'actions juridiques qui affecteraient grandement leur activité.

5.2 *Ressources humaines*

Afin d'assurer la bonne mise en place du SOC, et son efficacité, il est nécessaire de constituer une équipe dédiée à ce dispositif.

a) Les compétences que doit avoir l'équipe SOC

Il est possible de répartir les compétences d'analyste sur plusieurs personnes, mais le SOC nécessite les compétences suivantes :

- **Compétences en communication.** C'est l'une des principales compétences personnelles dont tous les membres de l'équipe ont besoin. Que ce soit pour communiquer avec les autres membres de l'équipe en mode d'urgence, ou pour communiquer calmement et efficacement avec les clients, le public et les cadres, la capacité de transmettre des informations clairement et au niveau approprié est essentielle chez un professionnel CSIRT. La communication écrite est également importante, car les membres doivent être en mesure de rédiger des politiques efficaces, de communiquer clairement avec les parties prenantes via des e-mails et des avis, ainsi que de documenter les incidents en profondeur.
- **La capacité d'écoute.** La capacité de faire une pause et d'écouter les préoccupations et les demandes des clients ainsi que la direction est primordiale lorsque vous travaillez pendant la résolution d'une urgence. Un membre du CSIRT qui ne prend pas le temps d'écouter les autres membres de l'équipe ou les clients, diminue sa capacité à résoudre l'incident de manière plus efficace.
- **Tact et diplomatie.** Chaque fois que des professionnels sont invités à faire face à une urgence, ils peuvent se retrouver dans une situation où ils ont du mal à obtenir des informations ou à traiter avec des clients et / ou des gestionnaires anxieux et en colère. La capacité de gérer calmement toutes les situations avec tact et diplomatie peut grandement aider l'organisation à se concentrer sur ce qui doit être fait pour minimiser l'impact d'un incident, ainsi que pour empêcher la divulgation d'informations qui ne devraient pas être publiques. domaine.
- **Travail en équipe.** C'est évident. Dans un groupe complexe de professionnels ayant des compétences techniques, une expérience et des rôles différents, il est important que tous les membres soient capables de bien travailler en groupe, d'accepter les différences d'approche, de comprendre les rôles des autres et de pouvoir se soutenir mutuellement sans réserve. Ils doivent également être en mesure d'interagir avec d'autres sections des organisations et du personnel non technique, ainsi que de reconnaître et d'accepter les dirigeants de leur groupe de travail.
- **Fiabilité et discrétion.** Les membres d'un CSIRT sont souvent mis au courant d'informations très sensibles et doivent conserver les informations qui leur sont fournies. Les membres doivent être en mesure de trouver le juste équilibre entre ce qu'il est légitime de divulguer aux parties prenantes et les informations qui doivent être bien protégées contre toute divulgation inutile.
- **Résolution de problème.** C'est l'une des compétences les plus importantes. Tous les incidents ne sont pas créés égaux, et les professionnels doivent être capables de s'adapter

à des situations changeantes, à de nouveaux scénarios et à une variété d'attaques afin de répondre le plus rapidement possible. De solides compétences en résolution de problèmes et de la créativité soutiennent les capacités techniques des membres de l'équipe et leur permettent de faire face et de résoudre même les situations les plus inattendues.

- **Capacité à faire face au stress.** Bien que tous les emplois nécessitent la capacité de garder son calme et de se ressaisir dans les moments difficiles, cela est particulièrement important lors de la réponse aux incidents. Un professionnel hautement qualifié qui s'effondre sous pression est une faiblesse qu'aucune équipe du CSIRT ne peut se permettre.
- **Compétences organisationnelles.** En cas d'urgence, la capacité d'organiser le travail, de le hiérarchiser et d'appliquer des compétences en gestion du temps est l'un des traits les plus importants. Jongler entre la réponse technique réelle à l'attaque ou à la vulnérabilité tout en informant les parties prenantes, en documentant les résultats et les actions et en maintenant si possible le reste des systèmes de l'organisation, nécessite les deux types de compétences pour effectuer un certain travail ou une certaine tâche.

b) Les rôles au sein de l'équipe

L'appartenance à un SOC variera d'une organisation à l'autre, mais les rôles suivants seront communs à la plupart des SOC :

- **Chef de la sécurité de l'information (RSSI):** il est responsable de définir le fonctionnement global de la sécurité de l'organisation, il est également chargé de gérer les tâches de conformité et communiquer avec la direction concernant les problèmes de sécurité.
- **Manager:** Supervise toutes les activités SOC, y compris la gestion des autres membres et la création de nouvelles politiques et procédures.
- **Ingénieur sécurité:** entretient et recommande de nouveaux outils de surveillance / analyse; construit une architecture de sécurité et assure la liaison avec les développeurs pour s'assurer que les systèmes sont à jour.
- **Analyste de la sécurité:** détecte, enquête et répond aux menaces; peut également mettre en œuvre des mesures de sécurité supplémentaires si nécessaire.

Par ailleurs, l'équipe des analystes peut être divisées en trois parties :

- Le Tiers 1 (ou niveau 1) : Il s'agit d'une équipe d'analystes dont la mission est de trier et qualifier les événements avant de faire remonter au Tiers 2 ceux nécessitant une plus grande attention. En effet, le Tiers 1 effectue une analyse des événements en temps réel, celle-ci doit être brève et basée sur des scénarios prédéfinis afin de faire une première évaluation. La politique de sécurité mise en place dicte la durée maximum de l'analyse (moins d'un quart d'heure généralement). Tout événement dont l'étude n'est pas finie à ce moment-là est remonté vers le Tiers 2.
- Le Tiers 2 (ou niveau 2) : Cette équipe reçoit les alertes du niveau 1 et lance une analyse plus approfondie afin de déterminer avec plus de précision l'origine et les conséquences liées à l'évènement en cours. Contrairement au Tiers 1, ces équipes

ne sont pas tenues de travailler en temps réel : elles peuvent ainsi allouer plus de temps pour étudier les alertes et déterminer si un incident a eu lieu. Elles rédigent aussi les procédures de traitement des événements pour le niveau 1 et participent à l'amélioration des règles de corrélation permettant au Tiers 1 de lever des alertes pertinentes.

- Le Tiers 3 (ou niveau 3) : Ce Tiers est légèrement différent des autres : premièrement il n'est pas présent dans tous les SOC. Son objectif étant plutôt d'éviter les incidents avant qu'ils ne se produisent, son rôle se rapproche du CSIRT. D'ailleurs dans certaines entreprises, c'est le CSIRT qui s'occupe de cette partie. Il s'agit donc ici d'une expertise plus poussée que pour les niveaux 1 et 2. Au sein du Tiers 3 peuvent être réalisés des activités de forensic ou de reverse-engineering afin d'analyser au maximum un incident et d'anticiper de futurs événements. En cas d'attaque non connue, les niveaux 1 et 2 ne sont pas alertés, c'est au niveau trois de faire une veille sur les menaces. [12]

Cependant, le **SOC Manager** reste le responsable de l'ensemble des trois niveaux du SOC et reporte directement au RSSI ou au DSI (en fonction de l'organisation de l'entreprise).

Figure 10: rôles de l'équipe SOC

5.3 *Gestion des processus*

Les processus sont le second pilier du SOC, ils vont permettre de mettre en place une organisation proactive et coordonnée face aux incidents de cyber sécurité. Plusieurs peuvent être définis au sein d'un SOC en fonction de son catalogue de service. Nous allons en décrire les processus liés à la supervision des évènements de sécurité :

- Processus de détection.
- Processus de qualification
- Processus de veille

a) Processus de détection

Le processus de détection est principalement axé sur les moyens de supervision des risques et la réception d'alertes. Néanmoins, la supervision opérationnelle des propres équipements d'un SOC doit également faire partie de ce processus. La première activité composant ce processus est de filtrer les événements entrants pour ne retenir que les éléments pertinents notamment suppression des faux positifs à partir des bases de connaissances du SOC et d'opérer un tri selon des caractères de pertinence de l'événement.

Cette activité est la charge d'un analyste de niveau 1, cette tache doit être rapide. Si l'analyste niveau 1 ne peut effectuer un tri et communiquer de manière exploitable l'alerte au processus de gestion d'incident (c'est-à-dire si l'alerte n'a pas déjà rencontré et n'a pas de procédure associée), il doit faire appel à un niveau 2.

b) Processus de qualification

Le processus de qualification est un ensemble de taches attribuées au rôle d'analyste niveau 2 du SOC. Ces taches incluent :

- L'étude de slots d'alertes remontées par les analystes niveau 1 après tri et priorisation.
- L'enrichissement et la contextualisation des informations liées aux alertes remontées par les analystes niveau 1.
- La détermination de la véracité et de la sévérité de l'incident de sécurité sous-jacent.
- Dans le cas d'un incident de sécurité avéré, la détermination de la nécessité de passer ces alertes à un processus de gestion d'incidents.
- L'isolation et la description des faux-positifs afin de les passer en entrée du processus d'administration du SOC.

Les investigations de qualification conduites par les analystes de niveau 2 conduisent :

- Soit à l'émission d'une alerte avérée à passer à un processus de gestion d'incident.
- Soit à la nécessité de procéder à d'avantage d'investigations ou de détecter d'autres événements liés, ce qui renvoie en entrée du processus de détection.

c) Processus de veille

Le SOC se trouve confronté en permanence aux vulnérabilités du système d'information, aux cybers menaces et aux attaquants qui en sont à l'origine. La veille dans ces domaines est donc

une fonction centrale du SOC pour garder un tempo de défense convenable. Tous les membres du SOC doivent plus ou moins être impliqués dans ce processus. Cependant cette implication revêt une importance particulière.

Le responsable du SOC doit s'assurer que son équipe se tient à jour des grandes tendances d'évolution des menaces et des moyens de détections ainsi que de l'évolution du cadre réglementaire et des exigences des métiers. Il doit également suivre la mise en œuvre des actions correctives ou préventives à moyen et long terme.

Les analystes doivent collecter et synthétiser l'actualité en matière de scénarios d'attaque, collecté et hiérarchiser les avis de sécurité publiés, rester informés des vulnérabilités des composants du système d'information supervisé. Ils doivent également s'assurer de l'efficacité des règles en fonction des nouvelles vulnérabilités et alertes.

d) Gestion des incidents

Les étapes de la gestion des incidents de sécurité sont :

- La détection et signalement ;
- Prise en compte ;
- Réponse à l'incident SSI ;
- Actions post-incident. [20]

Chapitre 6 : Etude comparative des solutions et choix des outils

L'étude comparative des solutions SOC existantes se fera à deux niveau, d'abord par une comparaison des types de technologies SIEM existantes, ensuite, par une comparaison des outils de scanner de vulnérabilité.

6.1 *Les SIEMs*

Les outils SIEM seront mis en comparaison sur la base de quelques notions essentielles à savoir :

- La taille de l'infrastructure que le SIEM peut contenir
- La capacité d'enregistrement des logs
- Le prix

1.1. Le IBM security Qradar

a) Présentation de la solution IBM Security SIEM Qradar

IBM Security QRadar SIEM est une architecture modulaire qui fournit une visibilité en temps réel de votre infrastructure informatique, que nous pouvons utiliser pour la détection et la hiérarchisation des menaces. Le QRadar peut être adapté à nos besoins en matière de collecte de journaux et de flux, ainsi que d'analyse. Nous pouvons de même ajouter des modules intégrés à notre plateforme QRadar, comme QRadar Risk Manager, QRadar Vulnerability Manager et QRadar Incident Forensics.

Le IBM security Qradar est une solution propriétaire appartenant au constructeur / éditeur IBM (international Business Machines Corporation). Il intègre dans une solution unifiée, la gestion des informations et des évènements de sécurité (SIEM), la gestion des journaux, la détection des anomalies et la gestion des configurations et des vulnérabilités.

Il normalise et met en corrélation des données brutes pour identifier des infractions à la sécurité et il utilise un moteur avancé Sense Analytics pour définir un comportement normal de base, détecter des anomalies et des menaces avancées et supprimer des faux positifs. Qradar trie, agrège, corrèle et affiche tous les évènements de sécurité indépendamment des types d'équipements surveillés.

b) Les fonctionnalités de Qradar

Qradar offre les trois fonctions principales d'un SIEM :

- Alerter : à temps réel sur les intrusions dans les systèmes d'informations
- Archiver : à temps différé toutes les informations de sécurité
- Analyser : l'ensemble de ces données

Outre ces fonctionnalités, IBM SIEM Qradar

- Affiche et gère l'activité du réseau.
- Affiche et gère les infractions ; lesquelles sont des alertes signalant une activité réseau ou de journal suspecte.

- Utilise des tests de règle et des réponses pour tester le réseau et l'activité du journal.
- Affiche et gère les actifs et les vulnérabilités du réseau.
- Utilise plusieurs types de rapport, notamment les vulnérabilités des actifs, les flux, les principales adresses IP source ou de destination et les principales infractions.
- Gère plusieurs vues de tableau de bord et ajoute de nouveaux éléments de tableau de bord liés aux infractions, sources et destinations.

c) Architecture du Qradar et ses composants

Lorsqu'on planifie ou crée un déploiement IBM Security QRadar, il est utile de bien connaître l'architecture QRadar pour pouvoir évaluer le fonctionnement des composants QRadar dans le réseau, puis planifier et créer un déploiement QRadar.

Le Qradar engendre deux types d'architectures qui sont les suivants :

- Architecture distribuée
- Architecture ALL-IN-ONE (tout en un)

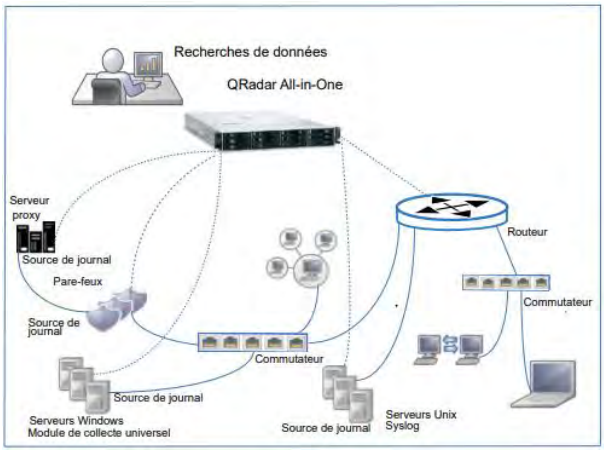


Figure 12:Architecture distribuée du Qradar

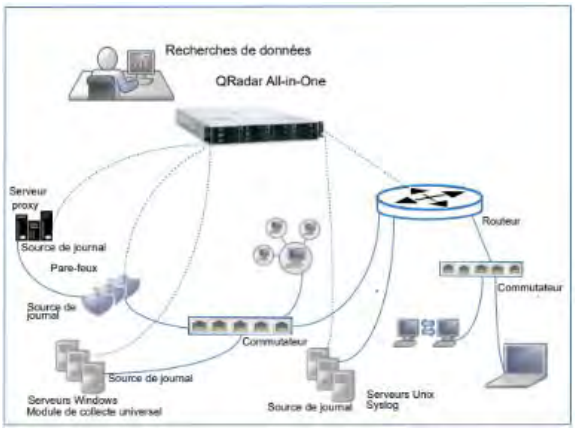


Figure 11: Architecture All-in-On du Qradar

- L'architecture distribuée

La plateforme QRadar Security Intelligence fonctionne avec trois couches qui s'appliquent à toute structure de déploiement QRadar, quelle que soit sa taille et sa complexité. La figure ci-dessus illustre les couches constituant l'architecture de QRadar.

Le dispositif Qradar, pour remplis sa mission se compose de différents modules jouant chacun un rôle primordial depuis la phase de collecte jusqu'à l'analyse des données.

Ces composants sont :

- Console
- Event collector, Event processor
- Flow corrector, Flow processor
- Data node

- L'architecture ALL-IN-ONE

Lors d'un déploiement QRadar d'hôte unique, vous pouvez utiliser un dispositif QRadar tout-en-un. Il s'agit d'un serveur unique collectant des données, comme des journaux de données d'événement syslog, des événements Windows ou encore des données de flux, depuis votre réseau.

Un dispositif tout-en-un est adapté aux entreprises de taille moyenne dont la visibilité est faible sur Internet, ou à des fins de test et d'évaluation. Les déploiements de serveur unique sont idéaux pour les entreprises qui surveillent l'activité réseau et les événements tels que les services d'authentification et l'activité de pare-feu.

Remarque : IBM security Qradar SIEM est une architecture modulaire qui fournit une visiblilité en temps réel de notre infrastructure informatique, que nous pouvons utiliser pour la détection et la hiérarchisation des menaces. Nous pouvons adapter Qradar à nos besoins en matière de collecte de journaux et de flux, ainsi que d'analyse. Nous pouvons ajouter des modules intégrés à notre plateforme Qradar comme :

- Qradar Risk Manager.
- Qradar Vulnerability Manager.
- Qradar Incident Forensics. [21] [22]

1.2 Splunk

a) Description de la solution Splunk

Splunk Enterprise Security est le centre névralgique de l'écosystème de sécurité, donnant aux équipes la perspicacité de détecter et de répondre rapidement aux attaques internes et externes, de simplifier la gestion des menaces en minimisant les risques. Splunk ES aide les équipes à acquérir une visibilité et des informations de sécurité à l'échelle de l'organisation pour une surveillance continue, la réponse aux incidents, les opérations SOC et offre aux cadres une fenêtre sur les risques commerciaux.

Splunk ES est un SIEM basé sur l'analyse qui permet aux équipes de sécurité de détecter, enquêter et répondre aux attaques internes et externes, et de simplifier la gestion des menaces. Il centralise et agrège tous les événements liés à la sécurité lorsqu'ils sont générés à partir de leur source. En outre, il prend en charge divers mécanismes de réception / collecte et fournit des recherches et des rapports ad hoc pour l'analyse des violations.

Concernant le Licencing, Splunk est gratuit jusqu'à 500Mo de données indexées par jour. Au-delà de ce, Splunk devient payant avec une licence basée sur le droit d'indexation pour un certain volume de données ajoutées quotidiennement. Il est donc recommandé d'utiliser la version Splunk Enterprise qui inclut un nombre illimité d'utilisateurs, de volume de données indexées. Avec Splunk, vous collectez et indexez en temps réel toutes les données machine, provenant des applications, serveurs Web, bases de données, réseaux, machines virtuelles, appareils mobiles, capteurs IoT, mainframes et autres. Il possède plusieurs méthodes de captures standard et personnalisées. Splunk dispose également de **forwarders** à installer sur les équipements à superviser afin qu'ils puissent lui envoyer leurs logs.

Figure 13: Type de données collecté par Splunk

b) Points forts de Splunk

Splunk Entreprise Security accompagne les organisations dans les processus suivants :

- Surveiller en permanence: visualiser clairement la posture de sécurité avec des tableaux de bord, indicateurs clés de sécurité, les seuils statiques et dynamiques et tendances
- Prioriser et agir: optimiser, centraliser et automatiser les flux de travail de réponse aux incidents avec des alertes, des journaux centralisés, et des rapports et des corrélations prédéfinies
- Mener des enquêtes rapides: utiliser des recherches ad hoc et des corrélations pour détecter les activités malveillantes
- Gérer les enquêtes en plusieurs étapes: retracer les activités associées aux systèmes compromis et appliquer la méthodologie de la chaîne de destruction pour voir le cycle de vie des attaques.

Splunk ES peut être déployé sous forme de logiciel, de service Cloud, dans le Cloud public ou privé, ou dans le cadre d'un déploiement hybride (à la fois en tant que logiciel et dans le cloud). [23]

Figure 14: Fonctionnalités de Splunk

1.3 OSSIM

a) Description de la solution OSSIM

OSSIM (Open Source Security Information and Management) est un gestionnaire d'informations de sécurité basé sur des technologies open source. Son objectif est de centraliser et d'analyser ces contenus issus de divers outils, et de prendre les décisions adéquates tout en gardant un suivi. Il possède un ensemble d'outils intégrés permettant une multitude de possibilités de traitement de l'information. L'analyse et la corrélation des événements fiabilisent les alertes, évitent quantités de faux positifs. Elles permettent une levée d'alarme très fine.

Son atout principal est qu'OSSIM ne constitue 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 connaitre la cartographie du réseau et de corréler les différents outils pour optimiser la supervision (réduire des faux positifs par exemple). On cherche à exploiter les caractéristiques des différents outils déjà existants pour collecter le plus d'information nécessaire pour une meilleur vision du réseau. OSSIM garantit l'interopérabilité des différents outils.

De plus, il intègre des outils open source tels que :

- ✓ Des détecteurs d'intrusions : Snort (NIDS), Ossec, Osiris (HIDS).
- ✓ Un détecteur de vulnérabilité : Nessus, Open Vas.
- ✓ Des détecteurs d'anomalies : Arp Watch, p0f, pads.

- ✓ Un gestionnaire de disponibilité : Nagios.
- ✓ Un outil de découverte du réseau : Nmap.
- ✓ Un inventaire de parc informatique : OCS-Inventory
- ✓ Un analyseur de trafic en temps réel : Ntop, TCPTrack, NetFlow.

b) Architecture de la solution OSSIM

L'architecture de la solution OSSIM repose principalement sur trois composants :

- ✓ Le serveur : contenant les différents moteurs d'analyse, de corrélation et les bases de données.
- ✓ L'agent : prenant en charge la collecte et l'envoie des événements au serveur OSSIM.
- ✓ Le Framework : regroupant les consoles d'administrations et les outils de configuration et de pilotage et permettant également d'assurer la gestion des droits d'accès.

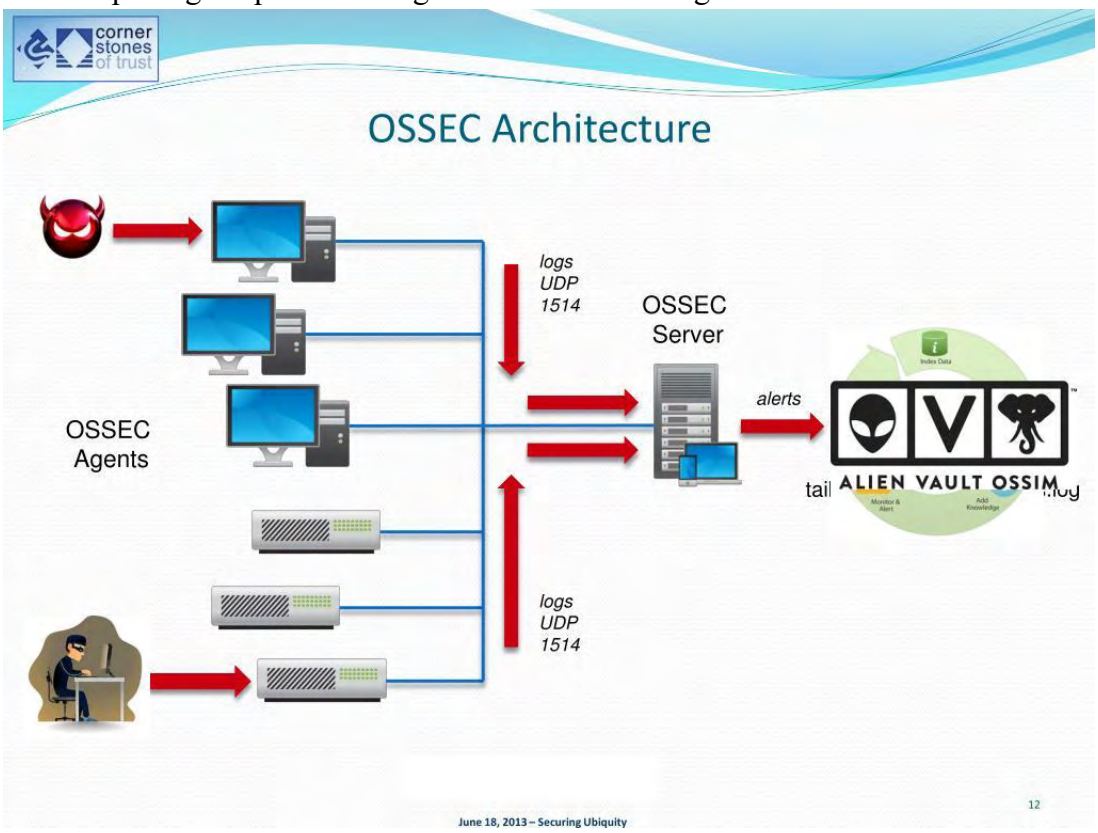


Figure 15: Architecture d'OSSIM

Le fonctionnement de la solution OSSIM se base sur ces deux principales étapes suivantes :

Le prétraitement de l'information : géré par des équipements comme des systèmes de détection d'intrusions (IDS), des sondes de collecte d'information (SENSOR) consiste à collecter les logs (fichiers de journalisation) de toutes les machines du parc informatique et de normaliser les différents logs reçus.

Le post traitement de l'information : assuré par l'ensemble des processus interne de la solution et qui vont prendre en charge l'information brute telle quelle a été collecté pour ensuite

l'analyser, la traiter et en fin la stocker dans une base de données. Toutes ces informations collectées sont spécifiques et ne représentent qu'une petite quantité d'information circulant sur le réseau de l'entreprise. La possibilité d'utiliser les informations remontées par le détecteur en utilisant un nouveau niveau de traitement, de compléter et d'améliorer le niveau d'information est appelé : la corrélation.

Son objectif est de rendre cette remontée d'information plus efficace par rapport à la quantité d'information disponible sur le réseau de l'entreprise.

Sa suite de solutions de sécurité fournit aux entreprises une protection contre les menaces de niveau entreprise à différents niveaux. De plus, il combine une appliance virtuelle avec une détection d'intrusion basée sur le réseau et l'hôte, un SIEM et une intelligence continue des menaces.

Une autre caractéristique notable d'AlienVault USM est l'Open Threat Exchange: une base de données de sécurité composée de plus de 26 000 participants dans 140 pays partageant plus d'un million de menaces potentielles sur une base quotidienne. [24]

c) Ce que Alien Vault peut faire

Alien Vault OSSIM assure les rôles suivants :

- SIEM et log management : Corréler et analyser rapidement les données d'événements de sécurité de l'ensemble de votre réseau avec SIEM et gestion des journaux intégrés ;
- Suivi comportemental : détecter instantanément les comportements réseau suspects avec l'analyse NetFlow, surveiller des services et la capture complète des paquets ;
- Détection d'intrusion : détecter et répondre plus rapidement aux menaces avec notre IDS réseau intégré, notre IDS basé sur l'hôte et la surveillance de l'intégrité des fichiers ;
- Évaluation de la vulnérabilité : Identifier les systèmes vulnérables aux exploits grâce à l'analyse active du réseau et à la surveillance continue des vulnérabilités ;
- Découverte et inventaire des actifs : trouver tous les actifs sur votre réseau avant qu'un mauvais acteur ne le fasse avec la découverte de réseau active et passive.

1.4 Etude comparative de ces trois SIEMs

Nous avons choisi les leaders en solution propriétaire et la meilleure en solution libre, nous procéderons ensuite à une étude comparative de ces 3 solutions en soulevant les forces, les fonctionnalités et les limites de chacune d'elle pour en choisir celle qui répond à nos besoins.

Selon Gatner 2018, et des années précédentes, nous remarquons que les deux solutions propriétaire (IBM security Qradzr et Splunk) demeurent les leaders les mieux réputés par rapport à OSSIM avec sa version commerciale Alien Vault, qui est encore NichePlayer jusqu'à présent (voir l'image suivante). [25]

Figure 16: Magic cadran de Gatner sur l'étude comparative des SIEM

Selon Gatner, nous notons que Qradar et Splunk ont un niveau de maturité largement supérieur à la solution open source OSSIM communément appelé Alien Vault en nom commercial. [29]

Tableau 1: Etude comparative sur l'accessibilité entre Qradar, Splunk et OSSIM

Produits	Lieu d'utilisation	Capacité d'enregistrement	Intelligence	Livraison	Prix
Splunk	Entreprises et industries	Ingestion des données journalièrement	S'intègre à Splunk UBA et à la boîte à outils d'apprentissage automatique	Logiciel et cloud	Basé sur le volume de données quotidien maximum; commence à 1800 $ / Go / jour
IBM	Industries et entreprises	Plus de 4oo sources de données et des millions EPS	UBA, Forensics, inspection des paquets, intégration Watson	Machine, Logiciel, et VM	Le cloud commence à 800 $ / mois; sur place à 10 400 $
OSSIM	PME	Offre une capacité très puissante	Intégration d'outils open source existants	logiciel et VM	Open Source

Les trois plates-formes possèdent des capacités puissantes que nous attendions de nos plates-formes de sécurité en couches de qualité entreprise. AlienVault USM a été conçu pour être une plate-forme tout-en-un combinant SIEM, IDS basé sur le réseau / l'hôte, la surveillance de l'intégrité des fichiers, l'évaluation de la vulnérabilité, la découverte d'actifs et l'analyse de netflow. Bien que QRadar offre des fonctionnalités telles que l'analyse des vulnérabilités et l'analyse du trafic, sa principale force réside dans ses capacités SIEM et d'agrégation / analyse des données de sécurité. De même pour Splunk, il offrir des tableaux de bord statiques c'est-à-dire que les données peuvent être monitorées en temps réel.

Notre choix se portera toute fois sur la solution open source OSSIM car, IBM QRadar est principalement une offre d'entreprise avec des ressources d'assistances minimales en dehors d'IBM et de son réseau de partenaires, bien que des supports d'aide en ligne substantiels soient accessibles, les sites web non affiliés à IBM, tels que QRadar Insights, proposent des didacticiels et des supports d'assistance limités. Autrement dit, la version d'essai du Qradar ne nous permet pas de tester l'ensemble des fonctionnalités d'un SIEM (idem pour Splunk). Par

contre, OSSIM offre de nombreuses sources de supports communautaires pour démarrer notre interface et est relativement intuitive et facile à utiliser, chaque page du console de gestion se compose d'éléments interactifs et personnalisables, et nous permettra donc de tester l'ensemble des fonctionnalités d'un SIEM.

6.2 *Scanner de vulnérabilité*

Nombreux facteurs sont primordiaux pour choisir un scanner de vulnérabilités, entre périmètre de couverture, détection de faux positives, l'apprentissage automatique des équipements… .

1.1. 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, et le support de nos équipes d'experts spécialisés, Nessus constitue la référence en termes de rapidité et d'exactitude.

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. Elle couvre plus de technologies que toute autre solution concurrente, analysant les systèmes d'exploitation, les périphériques réseau, les hyperviseurs, les bases de données, les tablettes, les téléphones, les serveurs Web et les infrastructures critiques à la recherche de vulnérabilités, menaces et atteintes à la conformité. Par rapport aux autres scanners de vulnérabilité, Nessus a la particularité d'être basé sur une architecture client/serveur et d'être compatible avec Windows et Linux. En plus, Nessus stocke et gère toutes ses failles de sécurité grâce à un système de plugins.

Les principales caractéristiques de Nessus sont :

- Déploiement flexible : logiciel, matériel, appliance virtuelle déployée dans un cloud de fournisseur de services ou service de cloud hébergé par Tenable (Nessus Enterprise Cloud)
- Options d'analyse : analyse sans agent pour faciliter le déploiement et la gestion. Intègre les analyses à distance sans authentification et celles locales avec authentification pour une détection plus approfondie et précise
- Reporting flexible : personnalisation des rapports avec un tri par vulnérabilité ou hôte, création d'une synthèse ou comparaison de résultats d'analyse pour mettre en évidence les changements
- Notification par e-mail ciblée des résultats d'analyse, des conseils de correction et des améliorations de la configuration d'analyse
- Détection : recherche précise et ultra-rapide des ressources

- Analyse : détection des vulnérabilités (y compris réseaux IPv4/IPv6/ hybrides)
- Couverture : vaste couverture et profilage des ressources
- Audit de correctifs : intégration aux solutions de gestion des correctifs (IBM, Microsoft, Red Hat et Dell)

Nessus nous permet de faire des scans de vulnérabilité pour plusieurs machines, notamment 16 adresses IP pour la version gratuite et illimitée pour la version Pro. [26]

1.2.Qualys

QualysGuard Vulnerability Management automatise l'audit du réseau et la gestion des vulnérabilités à travers l'entreprise, notamment grâce à la découverte et à la cartographie du réseau, à la classification des actifs par priorité, au reporting de l'évaluation des vulnérabilités et au suivi des actions correctives en fonction des risques métier. Grâce à QualyGuard Vulnerability Management, les responsables de la sécurité peuvent auditer, appliquer et documenter les efforts réalisés en matière de sécurité du réseau, conformément aux politiques internes et à la réglementation en vigueur.

Cette solution de sécurité logicielle disponible sous la forme de service à la demande (SaaS : Software as a Service) ne nécessite aucun déploiement. Grâce à QualyGuard VM, les entreprises peuvent gérer efficacement leurs vulnérabilités et garantir le contrôle de leur sécurité réseau avec des rapports centralisés, des solutions approuvées ainsi que des fonctionnalités complètes de gestion des actions correctives avec génération de tickets d'incidents. QualyGuard fournit des rapports complets sur les vulnérabilités, notamment avec les niveaux de gravité, des estimations sur les délais de résolution et l'impact sur l'activité, ainsi que des analyses de tendances concernant les problèmes de sécurité.

- Les fonctionnalités de la solution

Les fonctionnalités des applications incluent la découverte et l'inventaire des actifs, la gestion des vulnérabilités, la priorisation des mesures correctives, la surveillance de la conformité, la sécurité des conteneurs, l'analyse des applications Web et le pare-feu, la surveillance de l'intégrité des fichiers, l'indication de compromission, etc.

Cette solution engendre entre autre une panoplie de fonctionnalité, parmi lesquels nous choisissons et citons quelques-unes :

- Découvrir et hiérarchiser tous les actifs réseaux sans logiciel à installer ou à maintenir.
- Identifier et résoudre de manière proactive les failles de sécurité.
- Gérer et réduire les risques pour notre entreprise.
- Garantir la conformité aux lois, réglementations et politique de sécurité de l'entreprise.
- Intégrer des applications tierces et clientes via une API XML extensible.
- Distribuer les mesures correctives via un moteur de workflow complet.

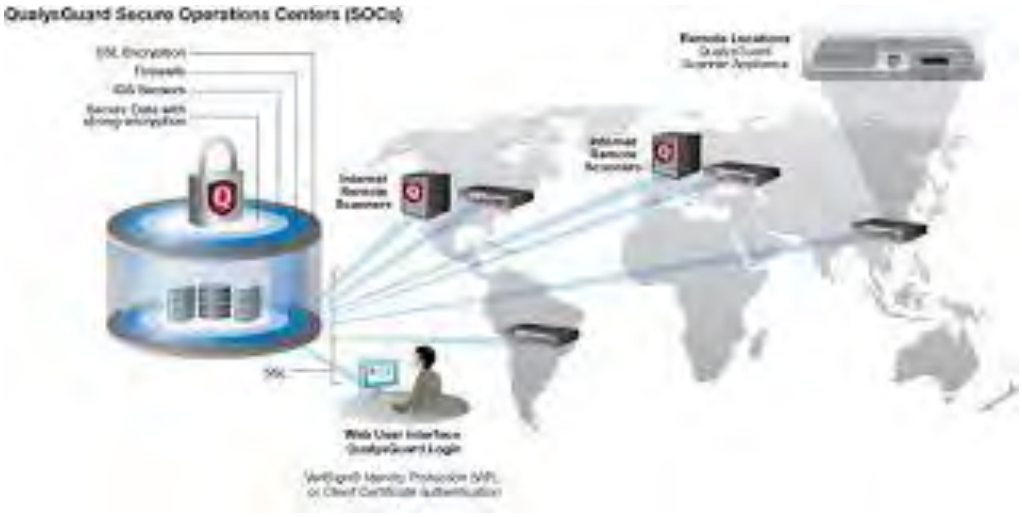


Figure 17:Interconnexion de QualysGuard

- Avantages de la solution

- Atténuation des risques grâce à l'identification automatisée des vulnérabilités et en appliquant les solutions correctives par niveau de priorité, en fonction de l'importance du risque pour l'entreprise
- Audit sans agent, journaux d'audit infalsifiables et garantie apportée par une évaluation tierce
- Avantages économiques sensibles grâce à la technologie SaaS. Aucune dépense d'investissement, pas de ressources humaines supplémentaires ni infrastructure à déployer et à gérer
- Solution d'une évolutivité sans précédent et idéale pour les grands comptes multi-sites
- Identification, visualisation et organisation rapides des actifs réseaux en entités et groupes d'actifs– Identification, visual. [27]

1.3.IKARE

La solution de gestion des vulnérabilités IKare analyse les réseaux informatiques et détecte les équipements mal configurés, les défaillances ou mots de passe faibles et les applications non mises à jour. IKare aide aussi bien les petites que les grandes organisations à maintenir un environnement informatique sécurisé. Elle effectue les évaluations en continue afin de détecter les nouvelles vulnérabilités à temps, et permet d'accélérer l'atténuation ou la correction des risques.

IKare automatise la mise en place des meilleures pratiques de sécurité en vulnerability management. L'outil vous fournit à la fois une solution simple de monitoring de l'ensemble du système d'information ainsi qu'une gestion et un contrôle faciles des principaux facteurs de sécurité. IKare s'articule autour de 4 grandes fonctionnalités : audit de vulnérabilité, réduction des risques, console d'administration unique (web) et une gestion des utilisateurs / groupes. IKare est un outil non intrusif. Le scanneur de vulnérabilité n'a aucune incidence sur vos postes de travail et les applications surveillées. Dès qu'une faille, une vulnérabilité ou un changement

suspect sur le réseau ou un poste de travail est détecté, des notifications sont immédiatement envoyées.

Ikare automatise les processus de gestion et contrôle des vulnérabilités dans toute l'organisation. Ainsi quelle que soit la taille de notre organisation, Ikare nous permet de garder le contrôle et de gérer efficacement la sécurité de notre réseau. Ikare inclut les caractéristiques suivantes :

- Découvertes des actifs réseaux
- Monitoring sécurité
- Gestion des vulnérabilités
- Analyse des menaces

- Les avantages d'Ikare

La solution présente une multitude d'avantage parmi lesquels :

- Identification des vulnérabilités
- Supervision de l'application des mises à jour systèmes
- Vérification des contrôles de sécurité et d'intégrité
- Reporting détaillé avec la solution IKare
- Réalisation de scans « à la demande » pour s'assurer de la correction
- Traçabilité des corrections effectuées.
- Accompagnement organisationnel par des Ingénieurs spécialisés en Sécurité.
- Rassurement de vos clients sur vos efforts pour maintenir un niveau de sécurité maximal.

- Les apports de la solution Ikare

Les principaux apports de la solution sont les suivants :

- Audit des vulnérabilités à temps réel.
- Identification proactive des problèmes de sécurité, alertes de sécurité.
- Découverte automatisée de l'infrastructure et des applications.
- Gestion de Business Unit.
- Groupes virtuels permettant une vue décisionnelle de la sécurité.
- Conformité CNIL et E-Privacy et règles métier. [28]

1.4. Étude comparative des solutions de scanner de vulnérabilité

Les scanners de vulnérabilités sont principalement comparés sur la base de plusieurs critères mais nous en choisirons que quelques un qui nous aiderons à mieux faire notre choix.

Scanner de vulnérabilité	Nessus	QualysGuard	Ikare

Topologie principale de client	Grands compte, PME	Grand compte	PME
Détection de faux positives	Oui	Oui	Pas totalement
Apprentissage automatique	Oui	Oui	Oui
Possibilité de générer des attaques intrusives	Oui	Oui	Oui
Format de fichiers de rapport	CSV et PDF	HTML, XML, PDF	XML, PDF, CSV et HTML
Couverture du Top 20 selon NIST et ANSSi	Oui	Oui	Oui
Possibilité d'importer une liste d'adresse IP issue d'un autre outil	Non	Non	Non
Possibilité de scanner plusieurs machines IP simultanément	Oui	Oui	Oui
Possibilité de scanner de façon exhaustive et automatique des machines modifiées	Non	Oui	Non

Nombre IP version gratuite	IP illimité	Licence externe	Licence 32 IPS bridée internet et 1 URL

Tableau 2: Etude comparative des solutions des vulnérabilités

Suite à la comparaison des outils de scanner de vulnérabilité, le choix s'est porté sur le Nessus. Il est installable sous forme de logiciel sur un PC en local et à partir de ce dernier nous avons l'habileté de scanner tous les équipements connectés sur le réseau.

Chapitre 7 : Conception du SOC

7.1 *Aspect infrastructure et matériel*

La première étape du projet est de désigner le pilote du SOC. Celui-ci va s'entourer des premiers collaborateurs qui vont permettre de déterminer l'ensemble des besoins et de les obtenir.

Au nombre de ces besoins, citons :

- L'architecture du SOC ;
- Les outils ;
- Les ressources humaines ;
- Les moyens de pilotage : comitologie, … ;
- Les SLA, indicateurs et reporting attendus ;
- Le fonctionnement (24x7 ou pas) ;
- Le budget ;
- Les moyens internes ou partiellement ou totalement externalisés.

a. Architecture Proposée

Il est très important de définir l'architecture applicative du SOC en premier lieu. Pour cela, nous devrons recenser le catalogue de service, en déduire les SI spécifiques à mettre en place et le socle sur lequel ces outils devront être installés (contraintes ou obligations internes à l'entreprise, adhérences avec les politique de sécurité, contraintes réglementaire…).

C'est ainsi que nous avons mis en place cette architecture type de la figure suivante. Elle est composée de :

- La partie interne : où on trouve les équipements locaux de l'entreprise,
- Le DMZ dans lequel sera placé le SIEM,
- Le Datacenter de l'ADIE dans lequel les outils seront déployés,
- Et la partie externe qui mène vers internet à travers un par-feu et un routeur.

Par ailleurs, nous avons proposé une deuxième sortie vers internet par HSRP pour assurer la haute disponibilité.

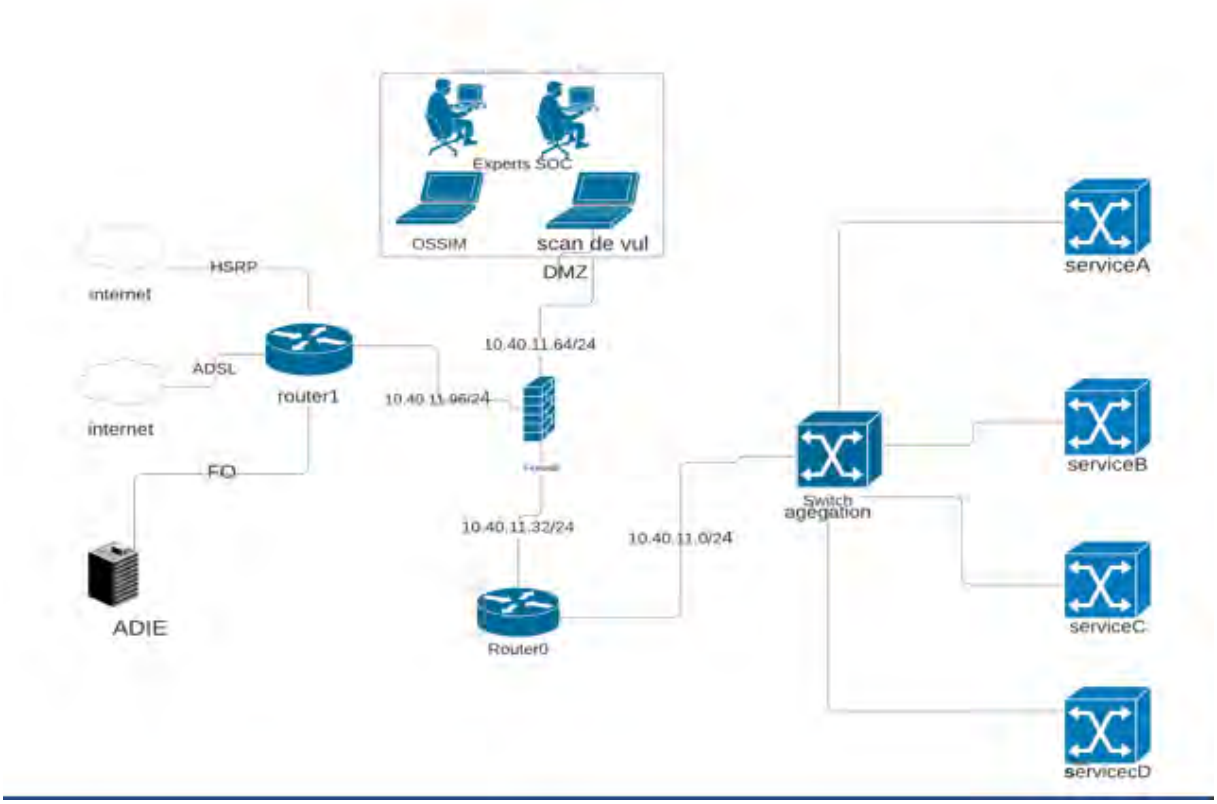


Figure 18: Architecture proposée

Nous aurons ainsi quatre sous réseau dont :

- **L'adresse réseau 10.40.11.0/24 :** appartient à l'interface qui lie Router0 au Switch d'agrégation ;
- **L'adresse réseau 10.40.11.32/24 :** pour l'interface qui mène vers le Firewale ;
- **L'adresse réseau 10.40.11.64/24 :** pour l'interface qui mène vers le DMZ ;
- **L'adresse réseau 10.40.11.96/24 :** pour l'interface qui mène vers le Router1.

b. Choix et emplacement des outils

Dans la phase initiale du projet, le choix des outils demandera la rédaction d'un cahier des charges dédié et l'analyse des solutions du marché. La durée de cette phase de sélection est à prendre en compte lors de la définition du planning global du projet. Par la suite, il sera nécessaire de s'assurer de la bonne formation et compétence des équipes sur ces technologies. Et cette réflexion peut amener à externaliser certains outils. C'est le point de vue de l'ANSSI concernant les SOC qui s'assure par la qualification PDIS de la maîtrise des entreprises qualifiées sur les outils de détection d'incident.

Par ailleurs, l'idéal serait de placer les outils de notre SOC au niveau du Datacenter de l'ADIE, pour une meilleure gestion de nos données.

Le périmètre d'action du SOC est défini généralement par le l'administrateur du SOC. Cependant, pour notre SOC nous nous concentrerons uniquement sur la supervision de certains équipements notamment les machines utilisateurs. S'agissant des autres équipements à savoir

routeurs, switch, serveurs… la détection de leurs vulnérabilités sera mise en perspective pour les projets à venir

c. Les ressources humaines

Le pilote du SOC devra donc définir cette organisation et définir les ressources disponibles dans l'entreprise pour remplir certains rôles et celles qui devront être recrutées. Il devra aussi préciser les rôles SOC qui occupent un plein temps et ceux qui ne sont requis qu'en partie du temps.

d. La gouvernance

Les comités doivent être mis en place et démarrer dès le lancement du projet.

e. Les SLA, indicateurs et reporting

A ce stade, il est important de mettre en place l'outillage qui va permettre de surveiller les SLA, de produire les indicateurs et les différents rapports sur l'activité du SOC.

f. Le fonctionnement

Il est nécessaire de déterminer si le fonctionnement du SOC en 24x7 est requis. Il faut distinguer la surveillance des SI du système d'alertes. Il est à peu près évident que la collecte des logs et la détection d'incidents doivent fonctionner en 24x7. En revanche, la question de l'utilité d'un service d'alerte en 24x7 peut se poser si les utilisateurs ne sont présents que pendant les heures ouvrées.

Reste à chaque entreprise le soin de déterminer suivant la nature de ses activités si elle a besoin d'un système d'alerte en 24x7.

g. Le budget

Le budget d'un SOC est relativement complexe et se répartit selon les axes suivants :

- Frais de personnel : que ce soit des ressources internes ou des recrutements, il convient de prévoir l'ensemble des personnes nécessaires au bon fonctionnement du SOC. Certains profils rares sur le marché peuvent avoir des prétentions salariales importantes ;
- Achats de matériels informatiques et licences des outils : ils font partie des investissements et certaines entreprises préfèrent répartir le budget plus en OPEX qu'en CAPEX ce qui amènerait à choisir une solution où l'infrastructure informatique est en mode cloud ;
- Les frais de maintenance récurrents et inhérents tant à l'achat de matériels que de logiciels sont à projeter sur plusieurs années ;
- Les frais d'abonnement éventuels à des services comme les CSIRT par exemple, sont à inclure dans le projet. Externaliser tout ou une partie du SOC provoque une restructuration de ces postes budgétaires avec des modèles CAPEX/OPEX différents suivant la répartition des services.

Nous retiendrons en résumé que le SOC coute excessivement cher en ce jour, pouvant aller même à hauteur de milliards.

h. Externalisation totale ou partielle du SOC

L'externalisation du SOC est une question fréquente qui apparaît lors du cadrage des projets SOC. Il n'y a bien entendu pas de réponse unique, les contraintes et attentes étant fort différentes d'un contexte à l'autre. Certaines organisations sont soumises à des exigences limitant les possibilités d'externalisation.

L'externalisation de tout ou une partie du SOC est à envisager, aux différentes phases du déploiement du SOC, pour des raisons très variées :

- Besoin d'accompagnement pour monter en maturité ;
- Manque de ressources ou d'expertise ;
- Besoin de service en 24x7 ;
- Réduction des coûts liés à la mutualisation ;
- Bénéficier d'un label PDIS pour une prestation qualifiée.

7.2 *Aspect fonctionnel*

La conception du soc passera dans un premier temps par la collecte et le traitement des événements existant. Il s'agit du socle primaire. Sa construction est séquentielle :

- Collecte des journaux d'événements (déjà concentré une première fois par le SIEM)
- Construction des scénarios de corrélation et implémentation dans le SIEM
- Alimentation du SOC en événements et résultats des corrélations.

En complément de ce socle, la construction considère :

- L'identification des profils des opérateurs/acteurs du SOC.
- Les moyens de réaction.
- Elaboration de scénarios de menaces et des priorités de traitement.
- Pilotage du niveau de sensibilité (pour améliorer la qualité de l'alerte).

Dans le cadre de la mise en œuvre dans un contexte multi-entités, des activités complémentaires propres aux échanges d'informations et processus de collaboration peuvent être nécessaires. Encore une fois, ces activités s'inscrivent après la construction du socle primaire. Dans ces cas-là, il convient également de déterminer :

- La localisation du stockage des événements,
- L'entité qui porte les consoles de gestion des alarmes,
- Et, plus globalement, de distribuer les rôles et les responsabilités.

e) La phase de collecte

La construction du système de collecte est une activité très dépendante de la technologie (des éléments collectés et des solutions de collecte elles-mêmes). Des prérequis techniques parfois complexes à mettre en œuvre doivent avoir été vus et discutés en phase de conception technique.

Dans un premier temps, la collecte concerne :

- Les équipements de sécurité,
- Les applications,
- les équipements réseaux.

En complément de la collecte, nous devons veiller à :

- La normalisation des événements collectés pour permettre leur exploitation ;
- Le stockage des événements collectés (dans le respect des contraintes réglementaires) en tenant compte de la localisation du stockage ;
- L'archivage des événements collectés ; en tenant compte des obligations de non-répudiation et d'intégrité des données.

a. La phase de traitement

Le traitement a pour objectif de s'attacher à la détection des risques les plus redoutés par la structure. Ceux-ci sont généralement connus via les analyses de risques cyber dont va découler la priorité d'analyse. Le traitement des événements de sécurité est conditionné par les scénarios d'infrastructures et métiers.

Les scénarios d'infrastructures visent à définir les règles de bases liées aux événements produits par les systèmes d'infrastructure et plus particulièrement par les équipements de sécurité. Ces règles sont dites « **events driven security** » ce qui implique que les équipements d'infrastructure produisent des événements de sécurité. Ces règles sont indispensables pour le traitement mais produisent un nombre de faux positif important et nécessitent un travail de qualification important.

Pour compléter l'efficacité du SOC et réduire le nombre de faux positifs, il est nécessaire de créer des scénarios métiers qui s'appuient sur des règles de corrélation issues des applications métiers et des règles d'infrastructure. Les scénarios métiers sont conçus spécifiquement pour le secteur d'activité dont le SOC est en charge. La détection d'événements métier est appelée « **data driven security** », l'objectif est d'analyser les informations issues des applications et pas simplement de l'infrastructure. L'objectif des personnes malveillantes n'est pas de passer les systèmes de sécurité liés à l'infrastructure mais les données qui elles sont hébergées sur les applications. Les scénarios métiers ne produisent qu'un nombre très faible de faux positif, qui augmente l'efficacité globale du SOC tout en augmentant l'implication des métiers dans le système de défense global.

La conception des règles de corrélations d'infrastructures et métiers est un poste central du dispositif du SOC. Suivant la taille de la structure, une « usine à corrélation » est mise en place. Celle-ci est composée d'un poste pour la conception des règles d'infrastructure en masse et un poste pour la conception des règles métiers qui va être alimenté par les règles d'infrastructure, les informations sur les métiers, les analyses inforensics et le « *threat intelligence* ». Cependant il est primordial que nous mettions en place un processus de gestion des règles qui permet de s'assurer du suivi de l'efficacité de la détection.

b. La phase communication

Objectif des communications du SOC (reporting global/local) :

- Garder l'intérêt et le sponsorship de la direction ;
- Préserver le budget voire augmenter le budget de la SSI ;
- Suivre l'évolution de l'état de la menace ;

- Proposer des évolutions des dispositifs et processus de sécurité

Elle s'appuie sur des success stories : c'est-à-dire les communications à la direction sur les attaques détectées et qui auraient pu porter préjudice majeur à la structure ; et consolide ces détections dans un rapport d'activité du SOC.

Partie III : Simulation et testes

Chapitre 8 : Déploiement des outils

Dans ce chapitre, nous allons aborder la mise en place de Nessus et celle d'OSSIM.

8.1 *Mise en place de Nessus*

Tout d'abord, pour aider Nessus à bien faire son travail et éviter de rechercher et de scanner des hots inactifs qui pourraient agir sur l'utilisation des ressources, nous allons utiliser ***Angry IPScanner*** qui est un logiciel libre de balayage de port, utilisé pour rechercher la présence de périphériques informatique connecté à un réseau TCP/IP appelé.

Il suffit de lui renseigner une adresse réseau ou une plage d'adresse puis il se charge directement du travail. En effet, nous voyons sur la figure ci-dessous qu'en moins de 21s il a pu scanner plus de *254 hôtes dont il trouve 37 hôtes* actifs avec leurs adresses IPs et leurs noms respectifs.

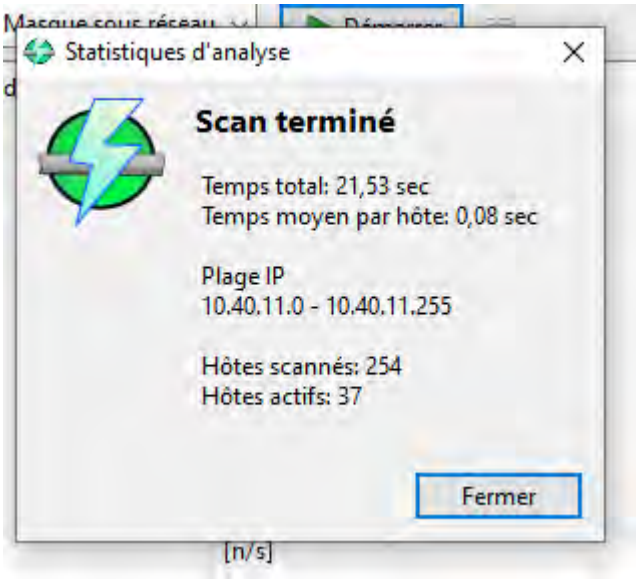


Figure 19:Balayage des ports actifs

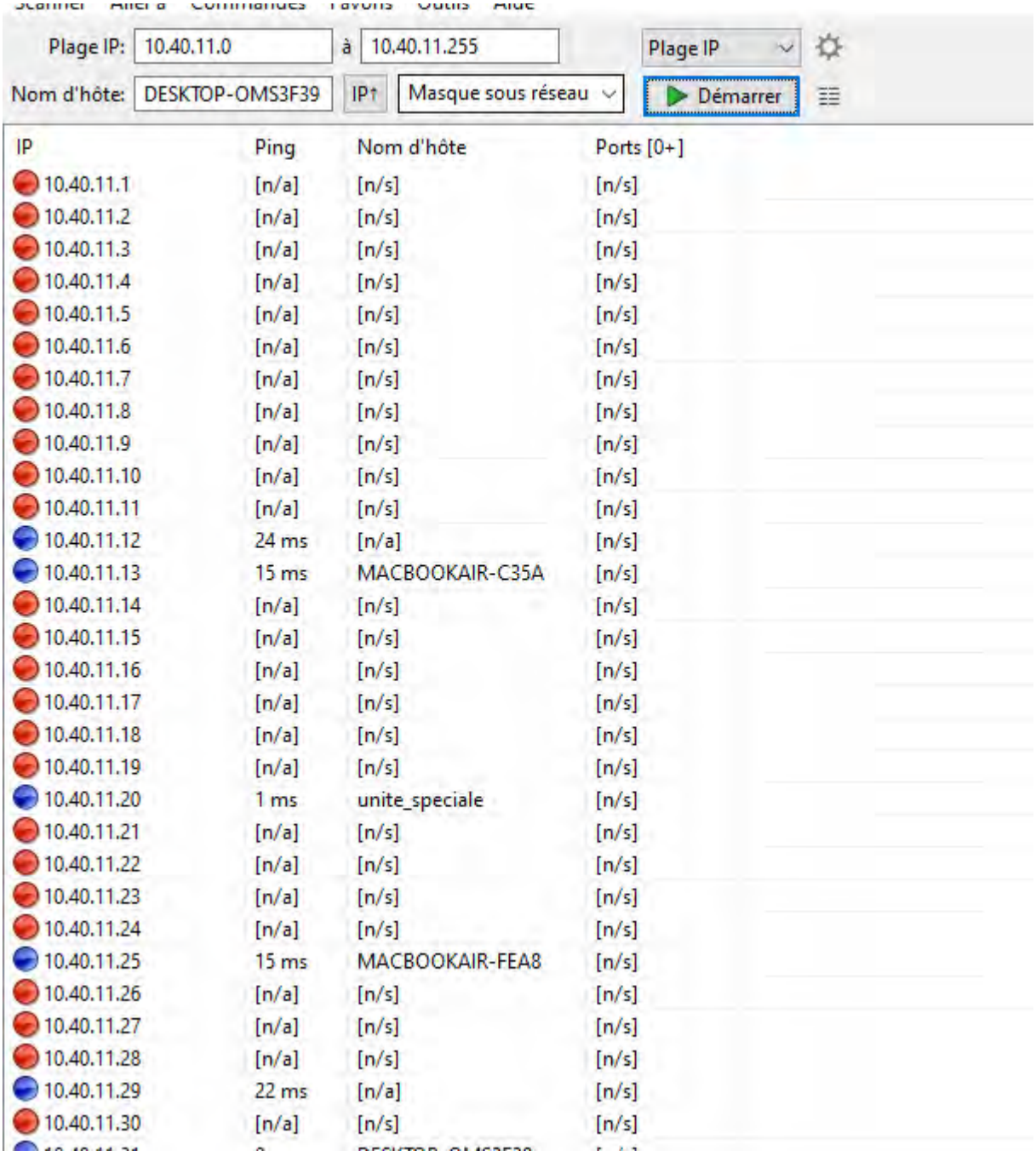


Figure 20: résultat du Ip Angry Scanner

Suite à cela nous sommes passés à l'installation de Nessus Essentials.
Prérequis :

- CPU 4 cœurs 2 GHz
- Mémoire 4 Go de RAM (8Giga recommandé)
- Et un espace disque de 30 Go sans compter l'espace utilisé par le système d'exploitation hôte.

Dans la figure ci-dessous nous renseignons sur un login et un mot de passe pour pouvoir accéder au tableau de bord proprement dit de Nessus.

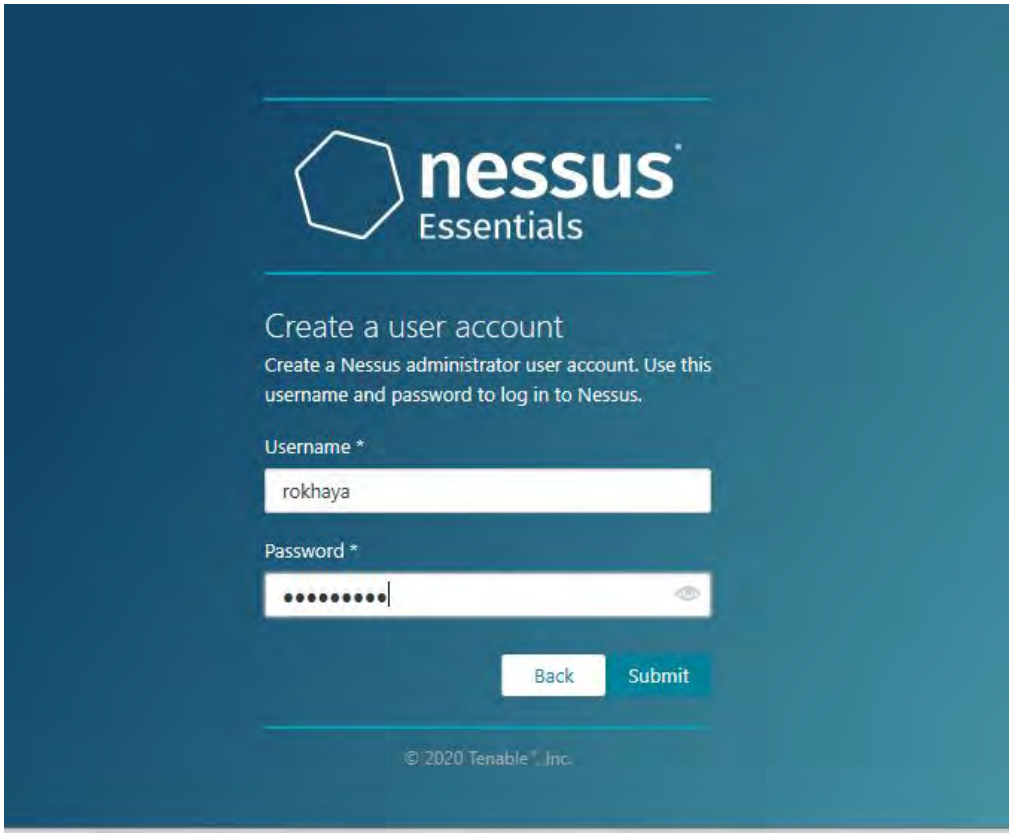


Figure 21: Authentification sur Nessus Essentiel

Lors de la connexion, nous accédons directement à l'interface graphique qui demeure complète, simple et intuitive avec ses différents services (Policies, Scan, Plugins Rules) et les assistances natives permettant de mettre en place des stratégies qui peuvent être utilisés à des fins de scanner de vulnérabilité ou d'audit. Voir figure ci-dessous.

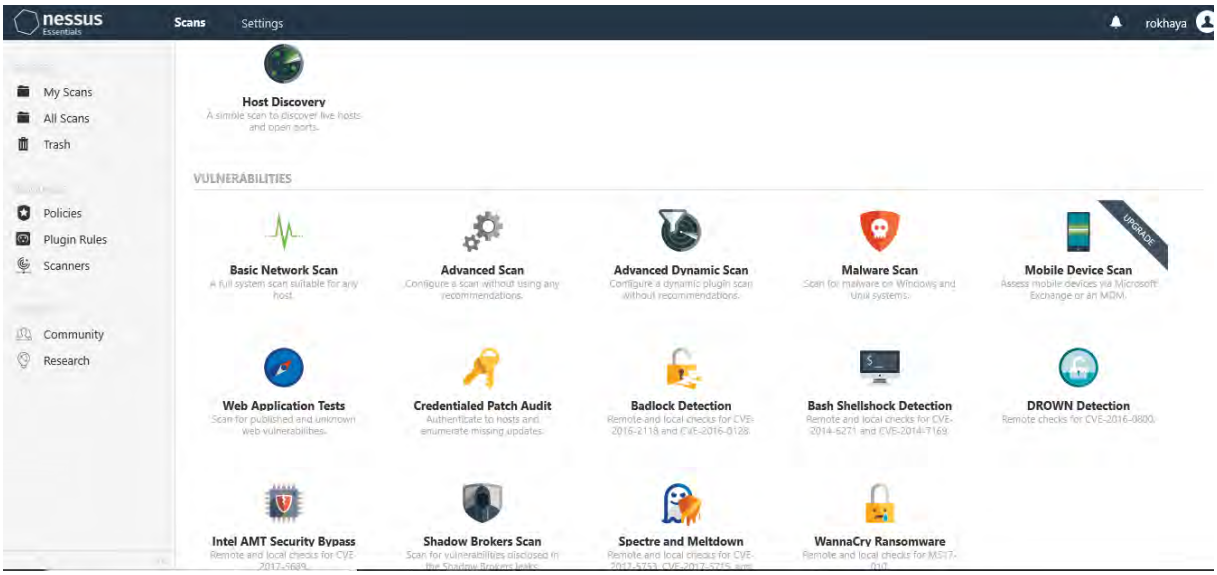


Figure 22: Tableau de bord Nessus

La figure ci-dessus engendre plus de 20 assistants de stratégies natives déjà préconfiguré selon nos besoins d'audit ou scan qui pourrait nous aider à bien faire notre travail. Il nous suffit de cliquer sur une assistante pour s'imprégner de la documentation, en effet nous pouvons sélectionner selon notre choix de travail étant donné que chaque assistant est différent de l'autre.

Dans notre cas, nous souhaitons faire un scan avancé du travail local, afin de recenser tous les vulnérabilités existant au sein de notre parc informatique et apporter une couche corrective.

Création de scanner avancer

Pour ce faire, nous choisissons l'assistance « **Advanced Scan** » pour effectuer un scan avancé de notre parc informatique.

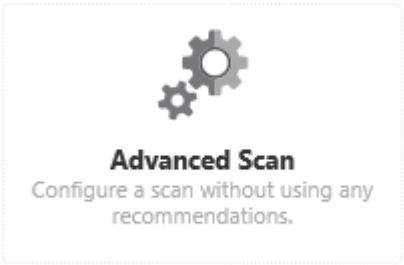


Figure 23:Création de scan avancé

Il engendre quatre onglets de configuration : les paramètres généraux, la gestion de la conformité et les Plugins. Voir figure ci-dessous.

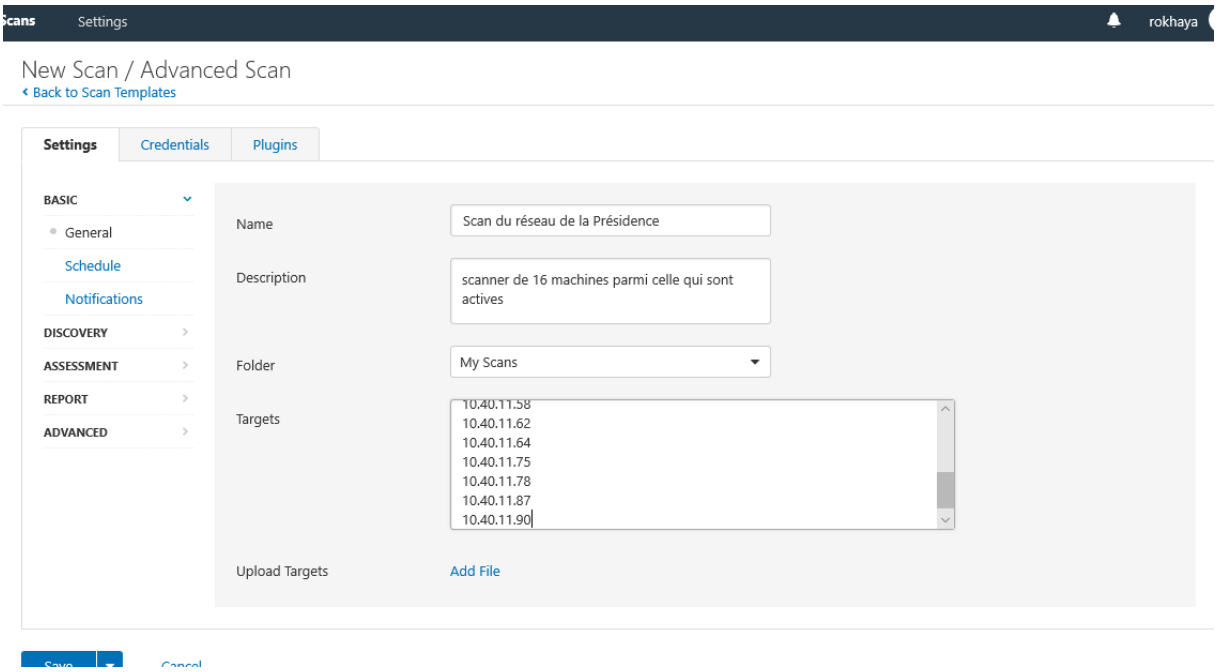


Figure 24: création d'une nouvelle stratégie

Lorsqu'on accède à l'interface advanced Scan, nous pouvons renseigner les paramètres de bases tels que :

- Le nom
- La description
- Les cibles (14 parmi les 37 adresses IP actifs trouvées en amont par le logiciel Angry ipscan). Voir la figure ci-dessus.

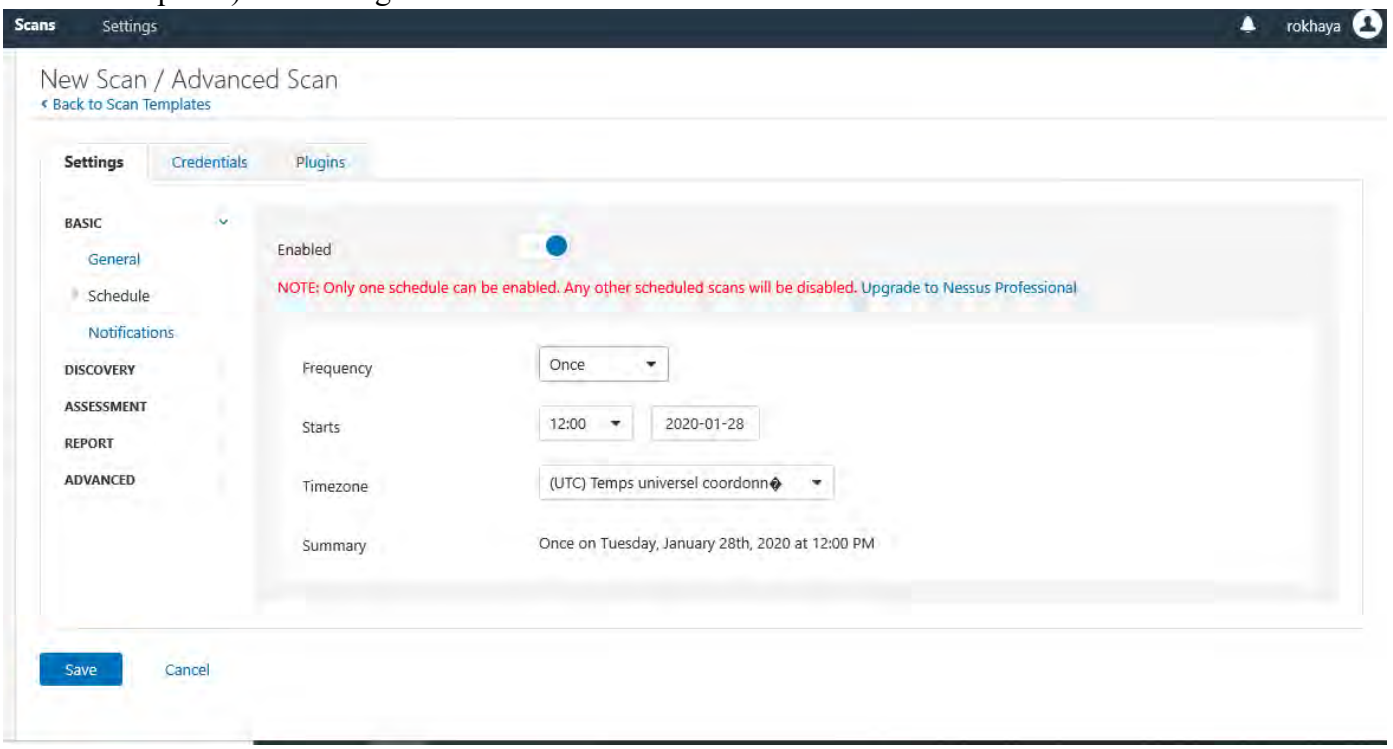


Figure 25: planification d'un scan automatique

La rubrique suivante désignée *Schedule*, nous permet de planifier le moment des scans (soit journalière ou hebdomadaire, mensuelle, trimestrielle, annuelle) en plus de la date de l'heure et du nombre de répétitions (par exemple : on peut configurer de telle sorte que chaque mardi à 17h30 se déclenche un scan automatique du réseau) voir figure ci-dessus.

Sur les rubriques suivantes, nous pouvons renseigner notre email pour recevoir les notifications sous forme de rapport en type CSV, PDF, HTML.

La rubrique *discovery* ou découverte gère les pings avec les différents protocoles utilisés (ARP, TCP, ICMP etc…) suivi d'un balayage de port et la découverte de serveur.

L'onglet conformité

La notion de conformité est un point crucial qui permet de vérifier si notre entreprise s'aligne bien à la règlementation internationale par exemple les règlements liés aux audits applicatifs OW ASP aux bases de données, aux données personnelles RGDP… pur ce faire, il nous suffit de dérouler la liste des catégories et en choisir avec un simple glisser déposer de la gauche vers la droite. Voir figure ci-dessous.

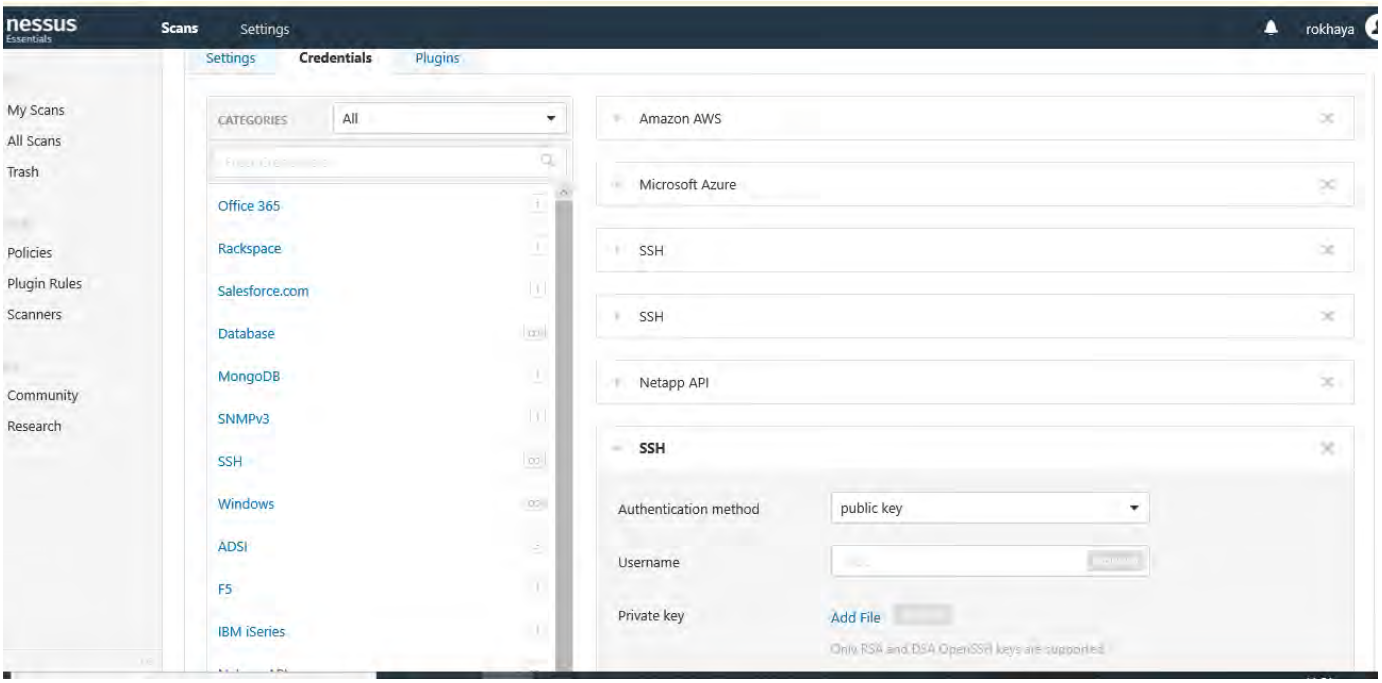


Figure 26: Règle de conformité

L'onglet plugin

L'onglet plugin permet à l'utilisateur de choisir des contrôles de sécurité spécifique en fonction du groupe de plugins ou des contrôles individuels.

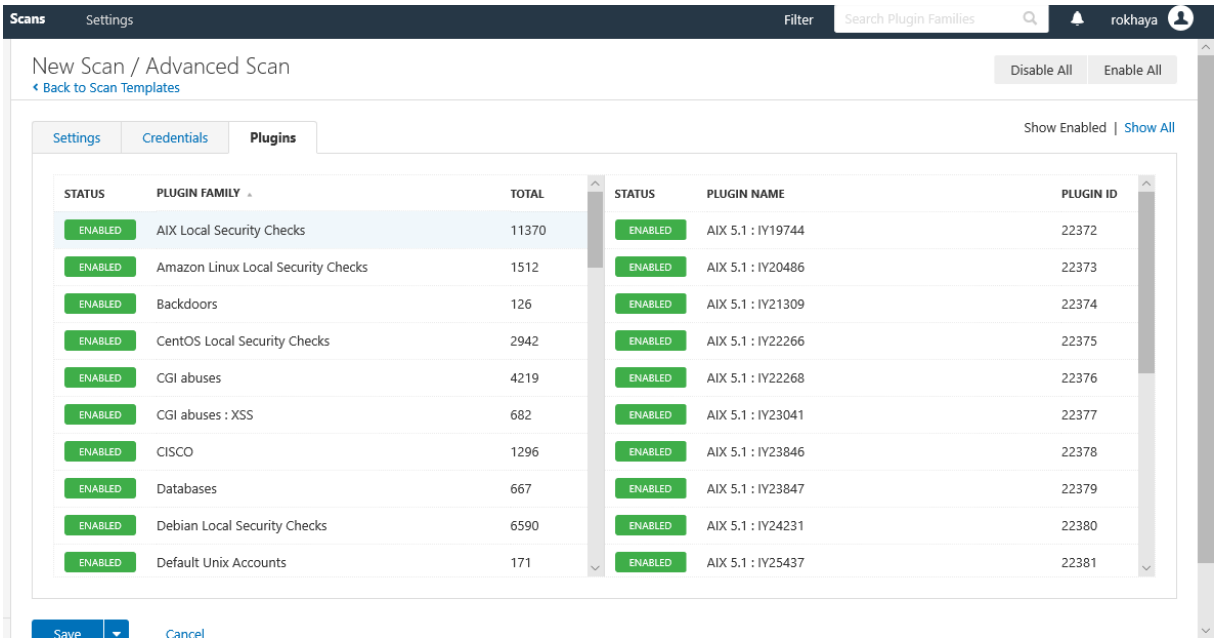


Figure 27: Activation des plugins

Après avoir paramétré les informations sur le scan, nous cliquons sur « Save » (Enregistrer). Une fois la soumission effectuée, le scan commence immédiatement si « Now » a été sélectionné, avant que l'affichage ne revienne à la page générale « Scans ».

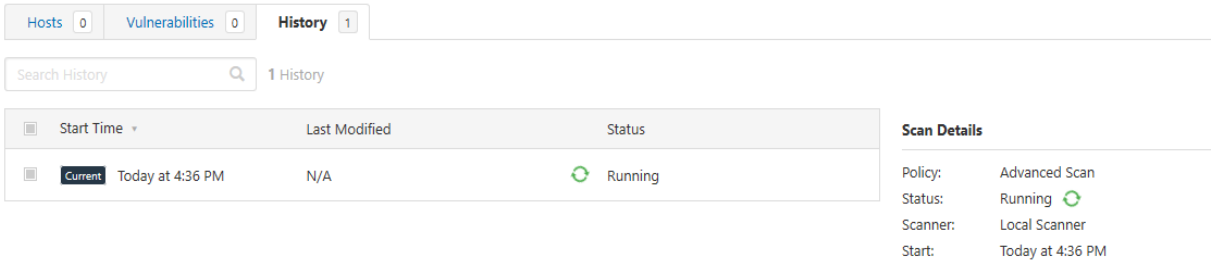


Figure 28: Démarrage du scan

a. Résultats de scan avancé

A la fin du scan, nous pouvons parcourir les résultats du scan de « *Scan du réseau de la Présidence* » en cliquant sur un rapport dans la liste.

La figure ci-dessous montre relativement le résultat du scan des 14 hôtes avec un code couleur indiquant le degré de criticité, cela nous permet d'avoir une vision récapitulative sur les équipements vulnérables au sein de notre parc informatique.

Nous pouvons également exporter le résultat en extension (Nessus, HTML, CSV etc…).

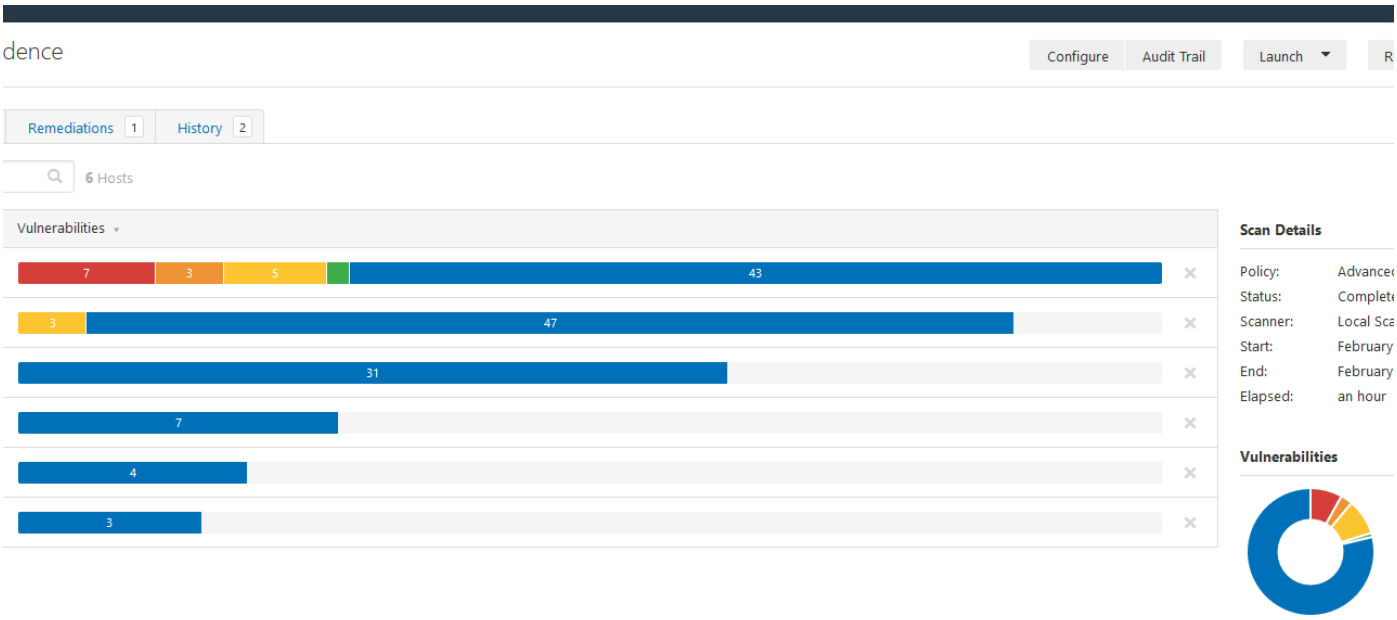


Figure 29: Résultat de scan Avancée

Juste avec 14 hôtes nous recensons plus de 46 vulnérabilités, agencés selon le degré de criticité des vulnérabilités, les plus critiques sont en tête de fil pour que nous puissions les traiter le plus rapidement possible et ainsi de suite jusqu'en bas du fil désignant les messages d'information en bleu.

Le degré de criticité est illustré ci-dessous par des couleurs, *rouge* pour critique, *orange* élevé, *jaune* moyen, vers faible et *bleu* informations.

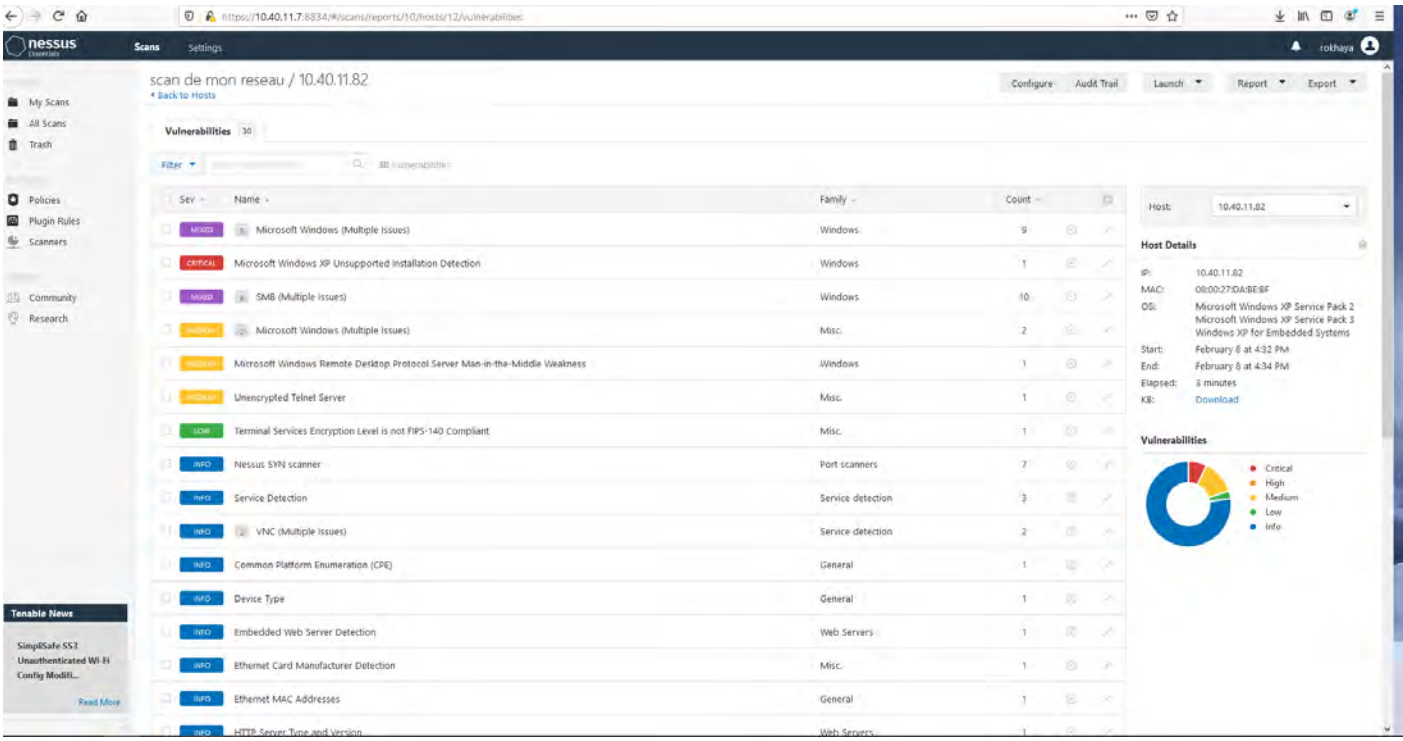


Figure 30: détection de vulnérabilités

Ces résultats nous donnent l'avantage d'une aperçue sur les faiblesses dans notre parc informatique, qui doivent être remédié avec des méthodes correctives (mise à jour, patch, etc…) le plus rapidement possible avant que les malicieux exploitent les faillent.

Lorsqu'on clique sur la rubrique ***Critical***, on obtient plus de détails sur la machine vulnérable, à savoir le système d'exploitation contenu sur la machine, son nom, son adresse IP, les causes de la vulnérabilité. Une éventuelle solution nous est aussi proposition pour remédier aux causes de vulnérabilité de la machine. Voir figure ci-dessous.

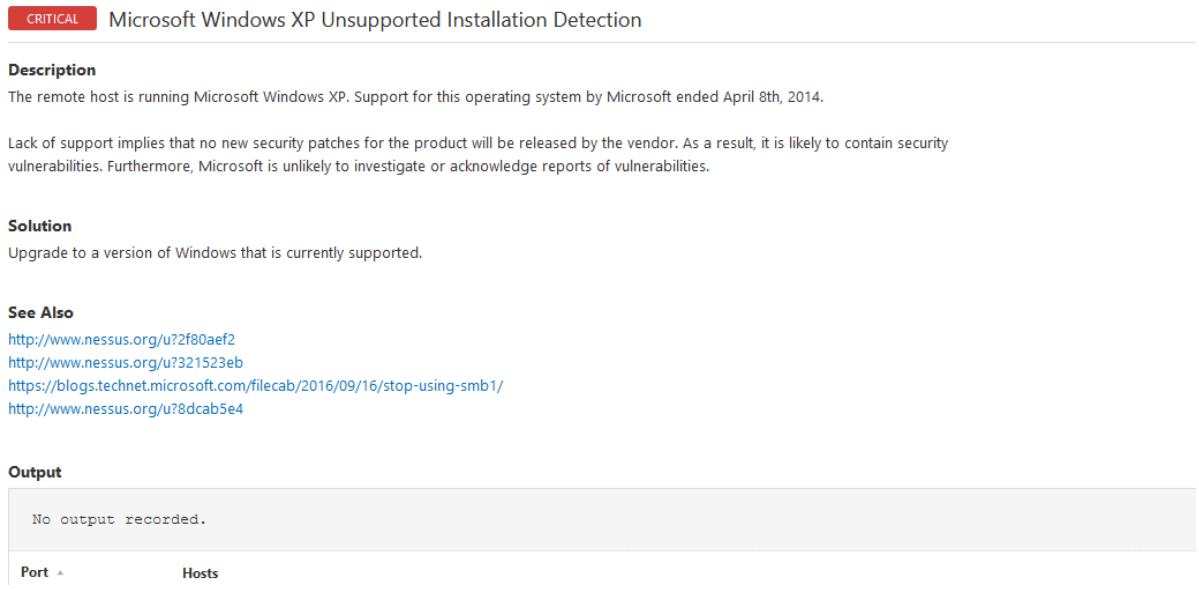


Figure 31:détails sur la vulnérabilité

8.2 Déploiement du SIEM Alien Vault d'OSSIM

a. Prérequis

Nous téléchargerons d'abord l'installation du fichier ISO pour exécuter ce logiciel sur une machine virtuelle nous utiliserons Vmware Workstation Pro. Téléchargez le logiciel du produit alienvault OSSIM sur leur site Web : https://www.alienvault.com/products/ossim .

Après avoir réussi à télécharger le fichier du logiciel ISO OSSIM, nous installerons ensuite ce logiciel sur la station de travail VM. Nous aurons besoin au minimum d'un RAM de 8Go, Processeur 4core, Harddisk 40GB.

Nous pouvons maintenant mettre l'invité de la machine virtuelle sous tension et démarrer l'installation.

b. Mise en place

Après avoir installé avec succès (Voir annexe), nous pouvons nous connecter à l'administrateur Web OSSIM à partir du navigateur, accéder à l'administrateur Web avec l'adresse https: // < 10.40.11.6>, et nous allons tout d'abord afficher le formulaire pour ajouter un compte administrateur comme sur l'image ci-dessous ;

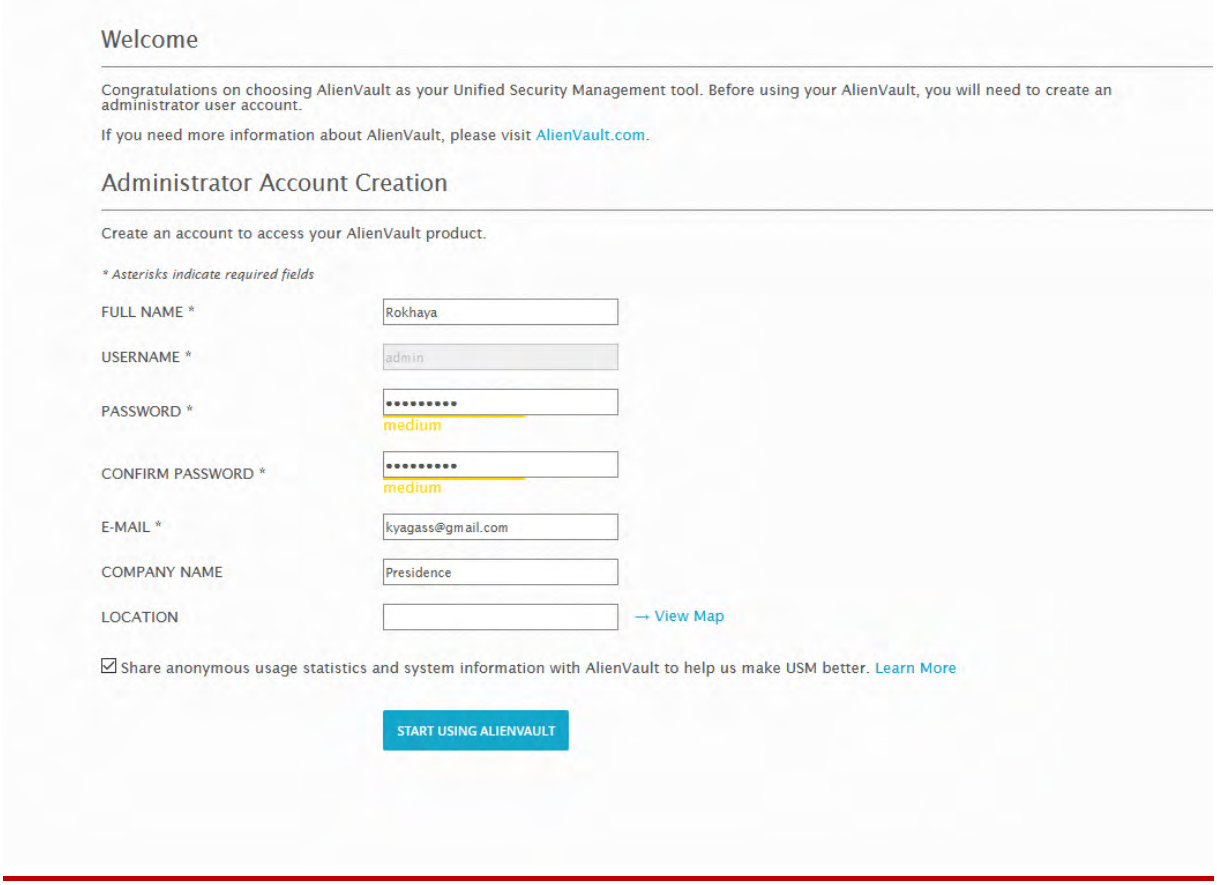


Figure 32: Ajout d'un compte l'administrateur

Saisissez le nom d'utilisateur, le mot de passe et toute information confidentielle, puis cliquez sur commencer à utiliser AlianVault.

Ci-dessous, nous nous connectons à la page pour accéder à l'administrateur Web OSSIM, avec *admin* comme nom d'utilisateur et du mot de passe.

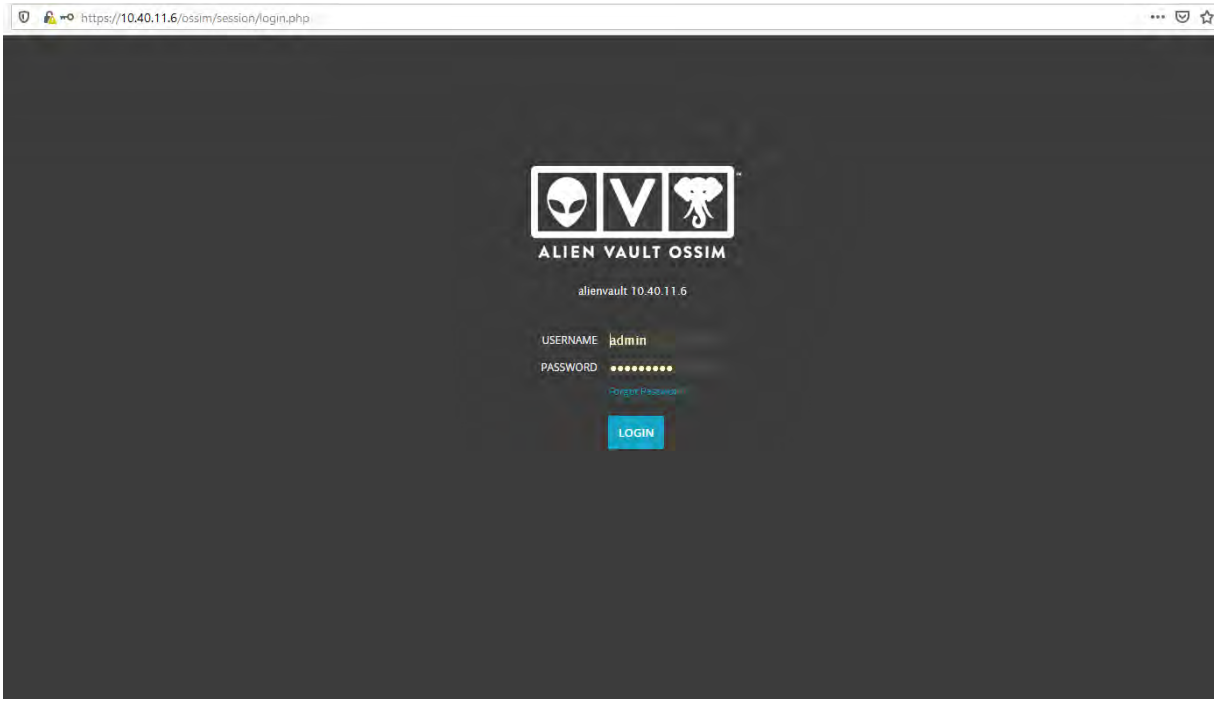


Figure 33: Connexion à l'administrateur Web OSSIM

Nous ferons ensuite les configurations de base que vous pourrez voir en annexe.

Toutes les étapes étant effectuées avec succès, nous pouvons voir le menu principal du tableau de bord de gestion de l'administrateur d'OSSIM, voir image ci-dessous.

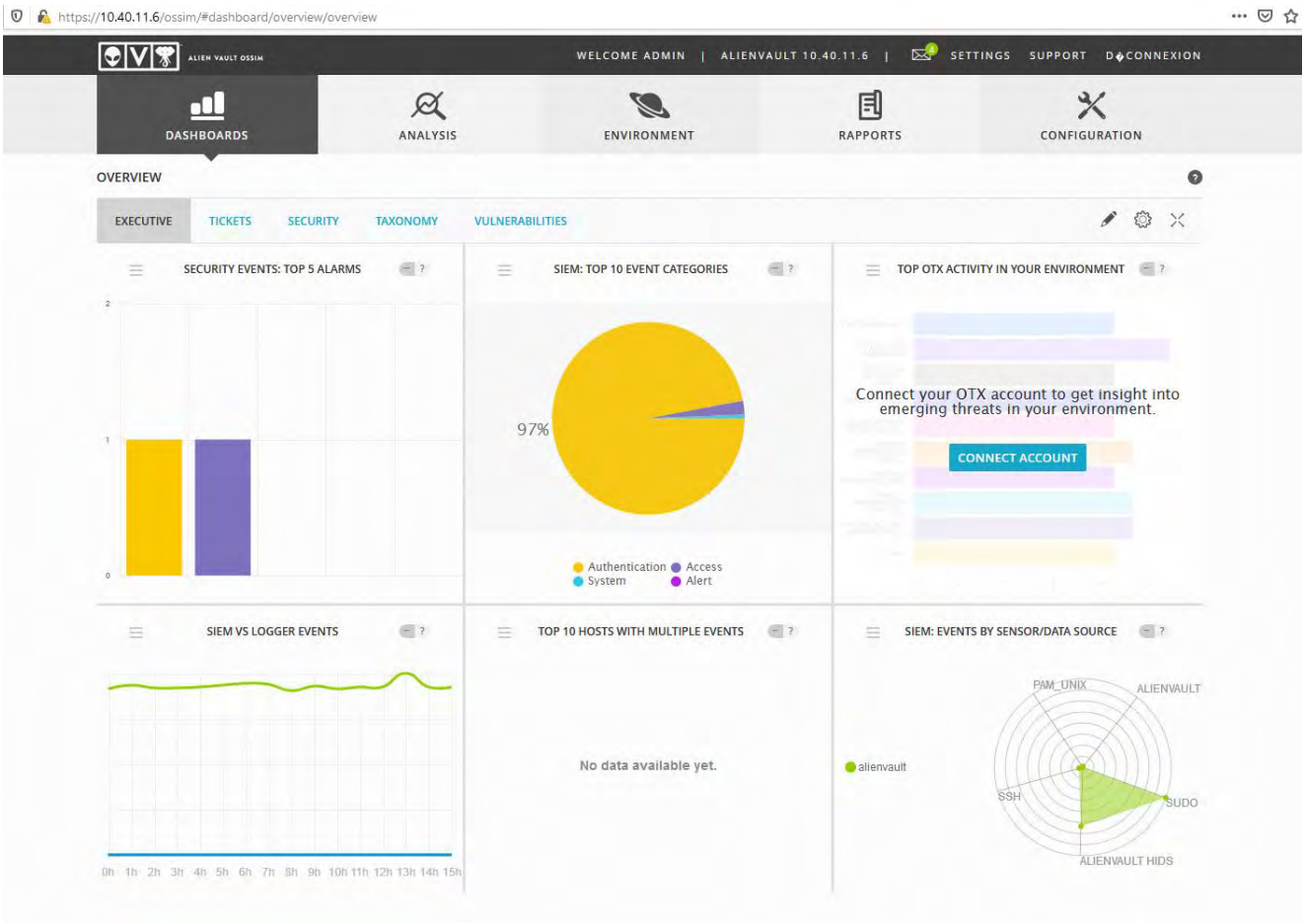


Figure 34: Menu principal OSSIM

Ajout des actifs

A cette étape, nous devons ajouter plus d'hôte à la surveillance en tant **qu'actif** dans le système OSSIM pour connaître leur partie de sécurité et les informations sur les événements Dans le menu **Environnement** aller à **Actif et groupe** comme sur l'image ci-dessous :

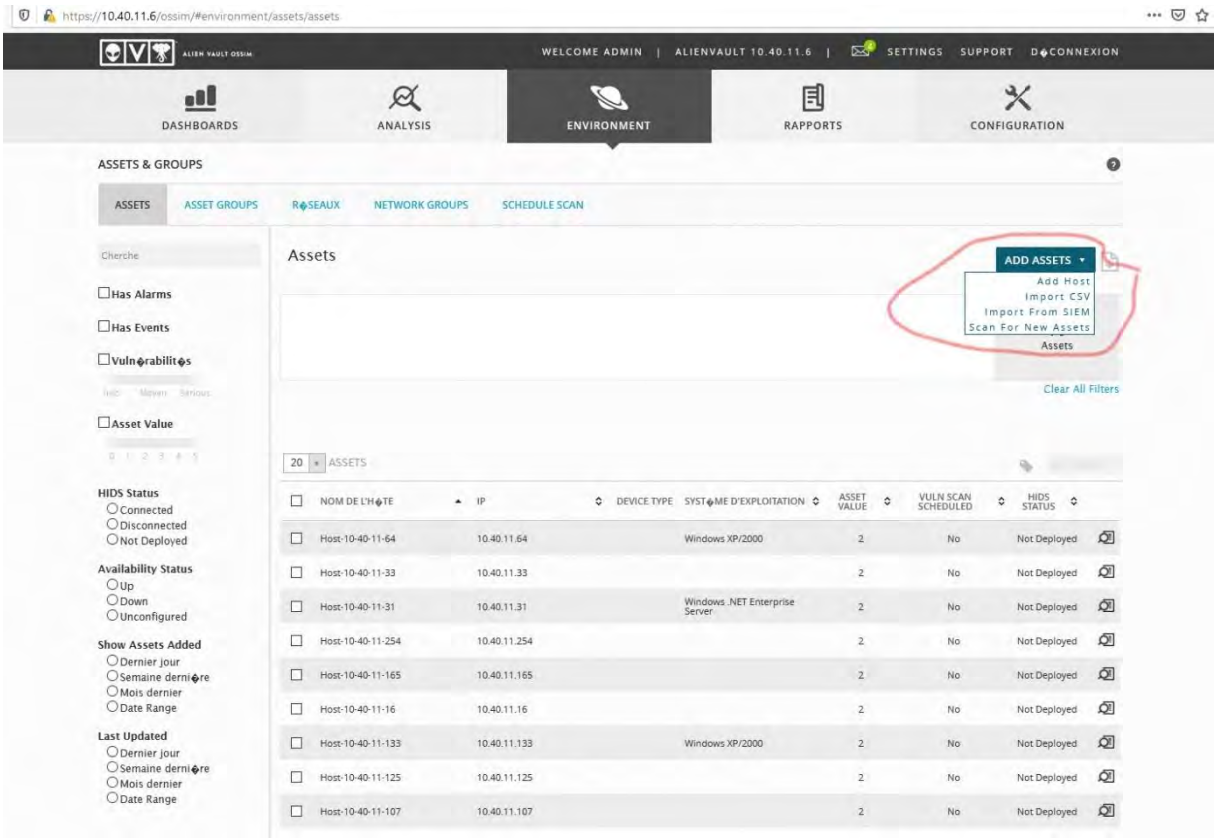


Figure 35: Ajout des hôtes

Cliquez sur " **Ajouter** un élément **-> Ajouter un hôte** " pour ajouter plus d'éléments.

Remplissez l'actif du formulaire, comme le système d'exploitation et tapez le périphérique comme sur l'image ci-dessous, dans ce cas, j'essaie d'ajouter une station de travail PC MACBOOKPRO.

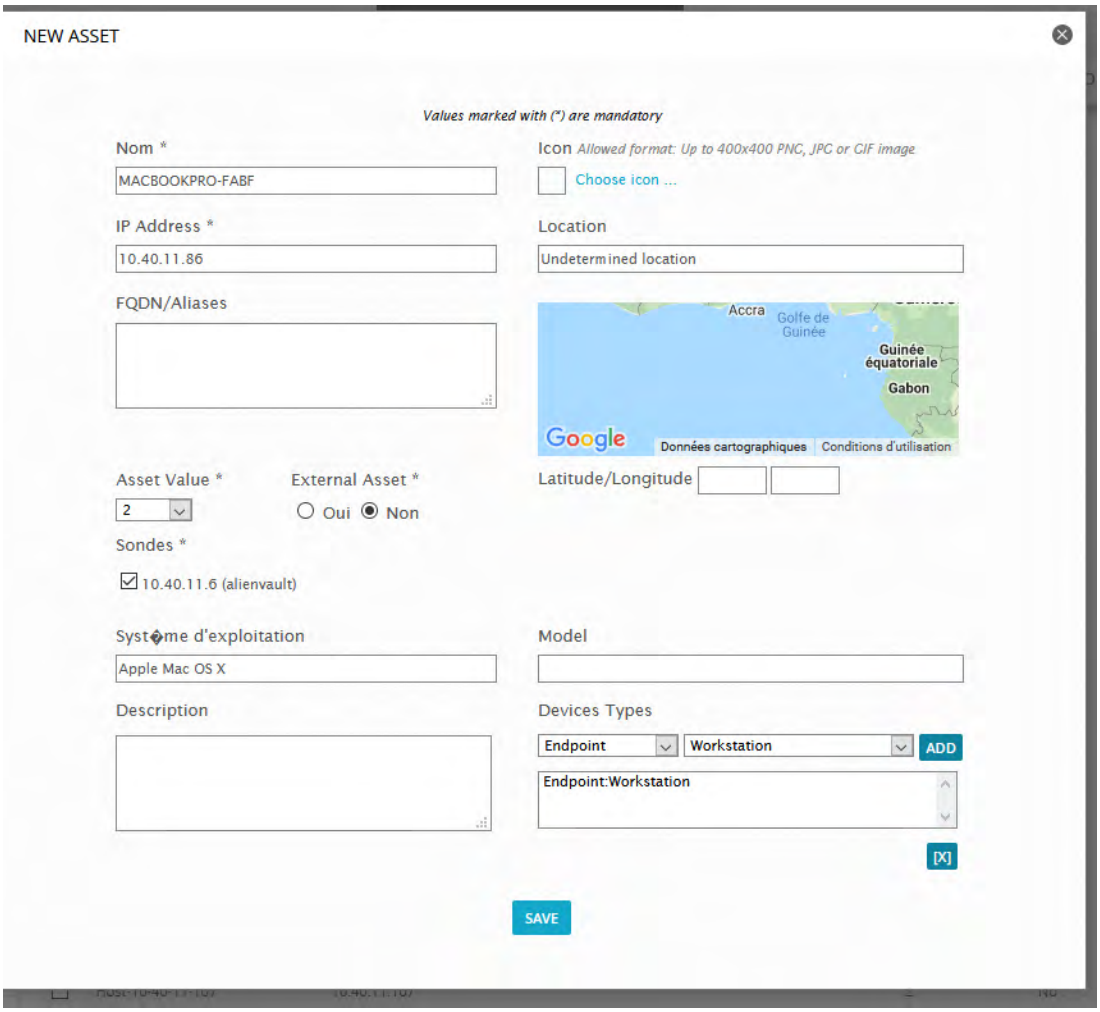


Figure 36: Remplissage de formulaire pour création d'hôte

Après avoir ajouté les hôtes en tant qu'actif, ils apparaîtront sous la forme d'une liste sur la colonne d'actif, pour une gestion facile, nous avons ajouté les actifs dans un groupe dénommé **groupe 1.**

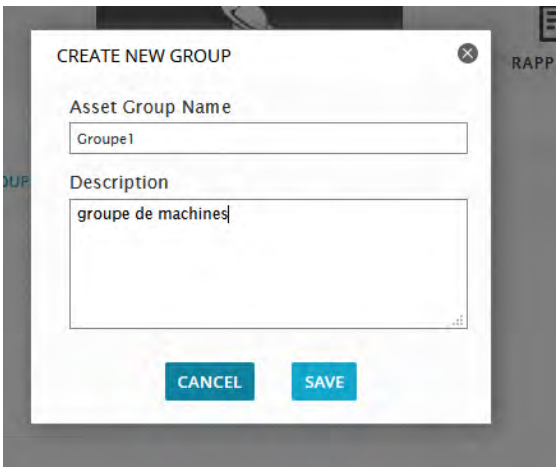


Figure 37: Création de groupe

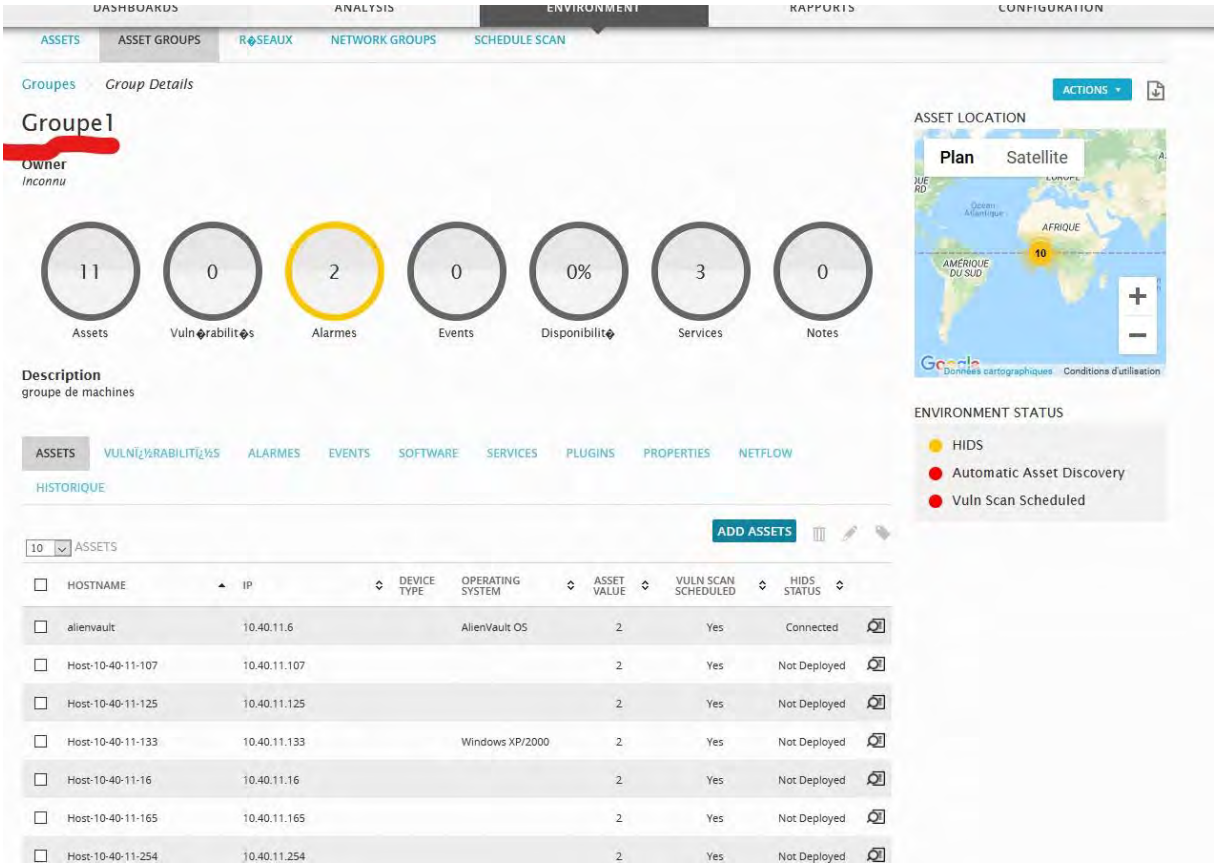


Figure 38: Ajout des hôtes dans le groupe

Nous constatons que les hôtes sont affichés en tant qu'actif du groupe **Groupe1**.

Déploiement de HIDS

Maintenant, nous allons déployer HIDS (Host intrusion Detected System) par configuration manuelle, à partir du menu **Environnement -> Détection -> HIDS -> Agent :**

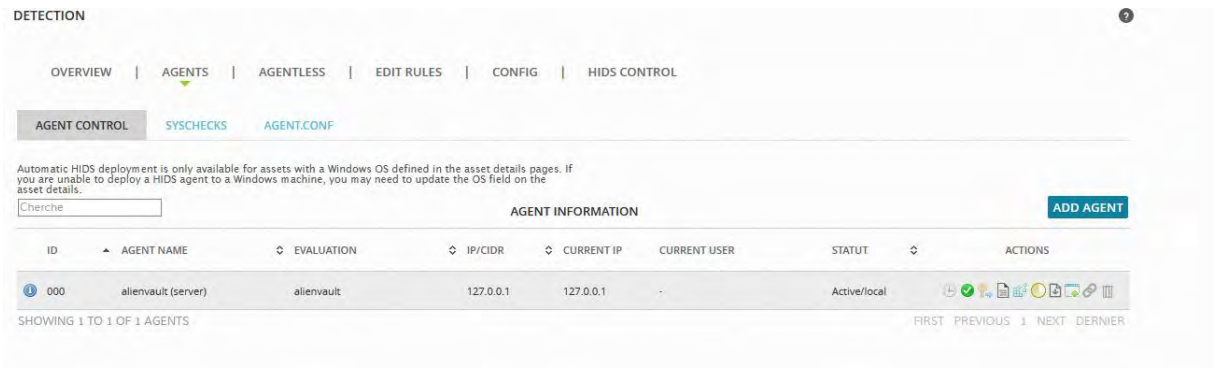


Figure 39: Déploiement de HIDS

Cliquez sur "ADD AGENT" et la ressource d'adresse IP de recherche déploiera l'agent HIDS sur le système comme sur cette image.

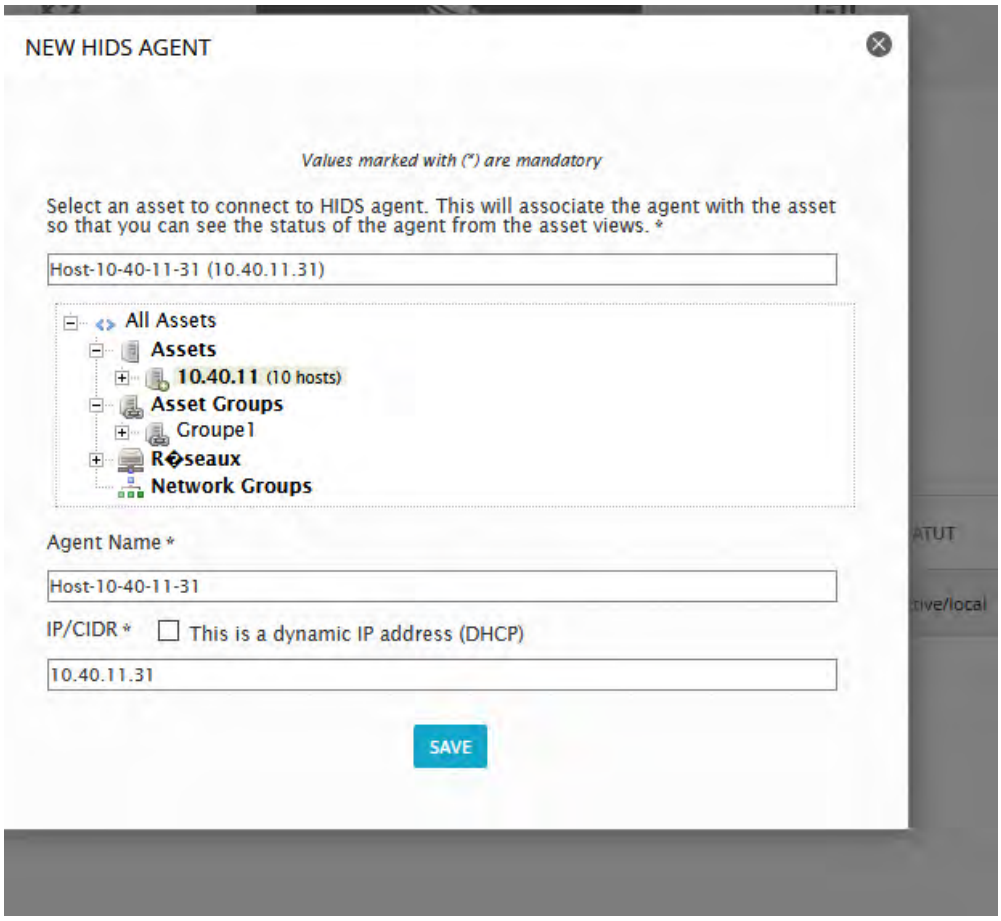


Figure 40:Ajout d'adresse IP de l'agent HIDS

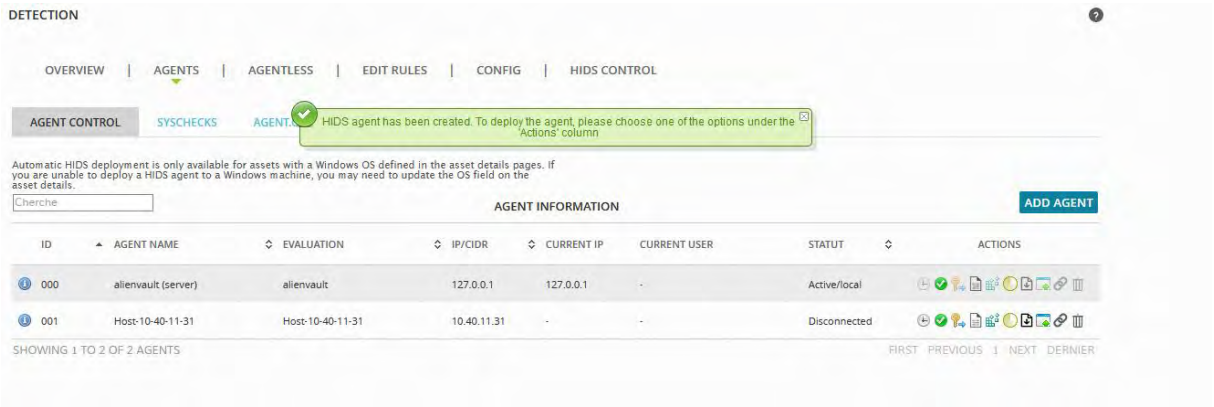


Figure 41: Ajout de l'agent HIDS avec succès

Cliquez sur l'adresse IP de l'actif et cliquez sur enregistrer, puis l'actif apparaîtra dans la colonne HIDS de l'agent, une fois l'actif sur la liste, cliquez sur l'icône « télécharger l'agent préconfiguré pour Windows » pour télécharger l'agent OSSIM sur le disque local et installer ce logiciel sur le système hôte manuellement.

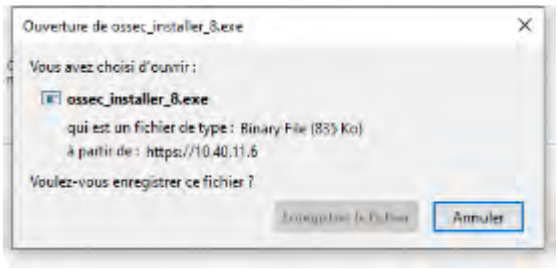


Figure 42: Téléchargement de l'agent OSSIM

Après la réussite du téléchargement de l'agent **AlientVault_OSSIM.exe**, installez l'agent sur le système, ouvrez cette application d'agent et vérifiez l'application de journal que l'agent démarre avec PID, à partir du menu de l'agent d'application **Afficher -> Afficher les journaux.**

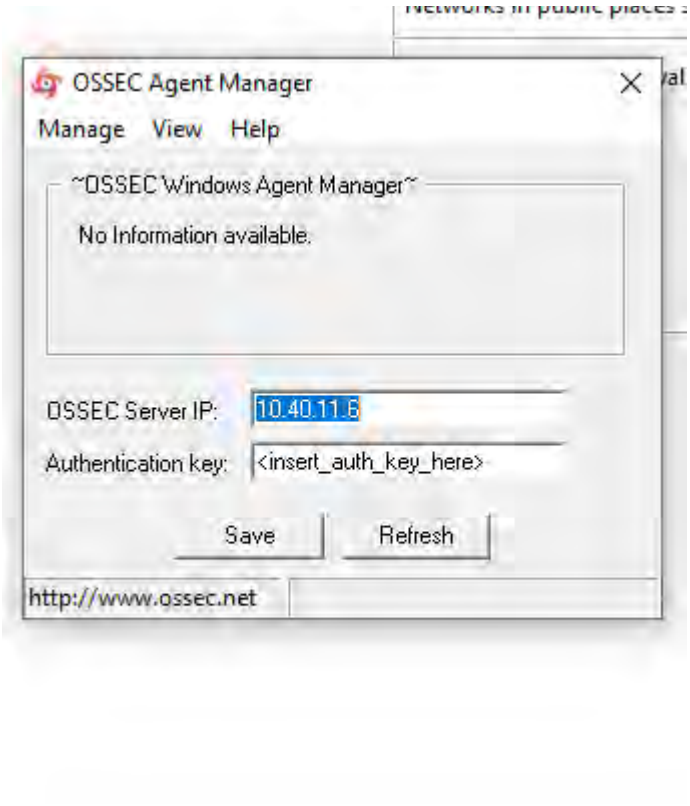


Figure 43: Installation de l'agent OSSIM

Après le démarrage de l'agent de service sur le système d'actif / hôte, redémarrez HIDS, à partir du menu **Environnement -> Détection -> HIDS -> Contrôle HIDS.**

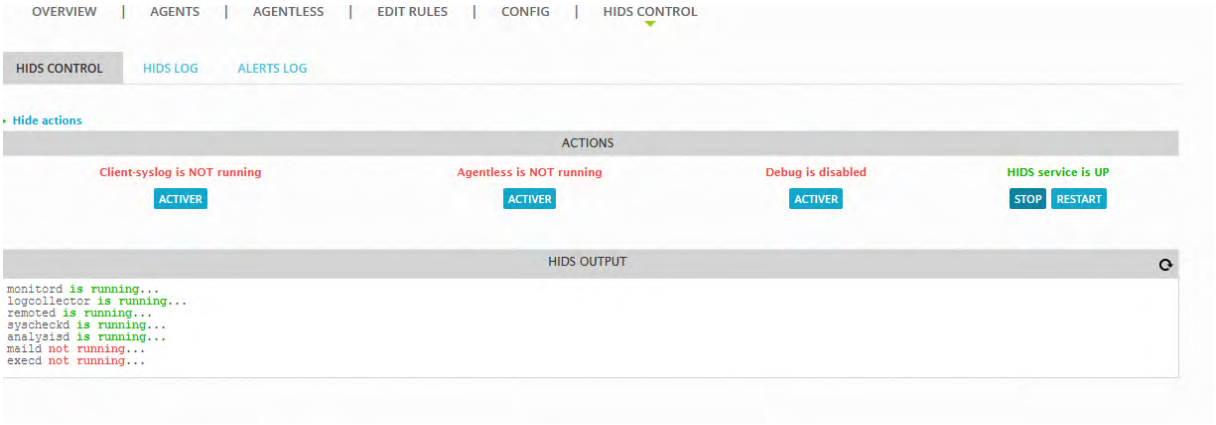


Figure 44: Redémarrage du HIDS

Et si l'agent HIDS fonctionne correctement sur l'actif, le statut HIDS deviendra « **actif** » comme sur l'image ci-dessous :

Figure 45: L'agent HIDS a été bien activé

À partir de cet agent HIDS, nous pouvons surveiller les alarmes, les événements et la vulnérabilité de numérisation de tous les actifs.

Chapitre 9 : Simulation d'une attaque interne

Le travail consiste à contrôler une machine d'un employé de la structure de manière illégale par le biais d'un attaquant possédant un PC (Kali Linux) et enfin d'observer la réaction de AlienVault OSSIM par rapport à l'attaque.

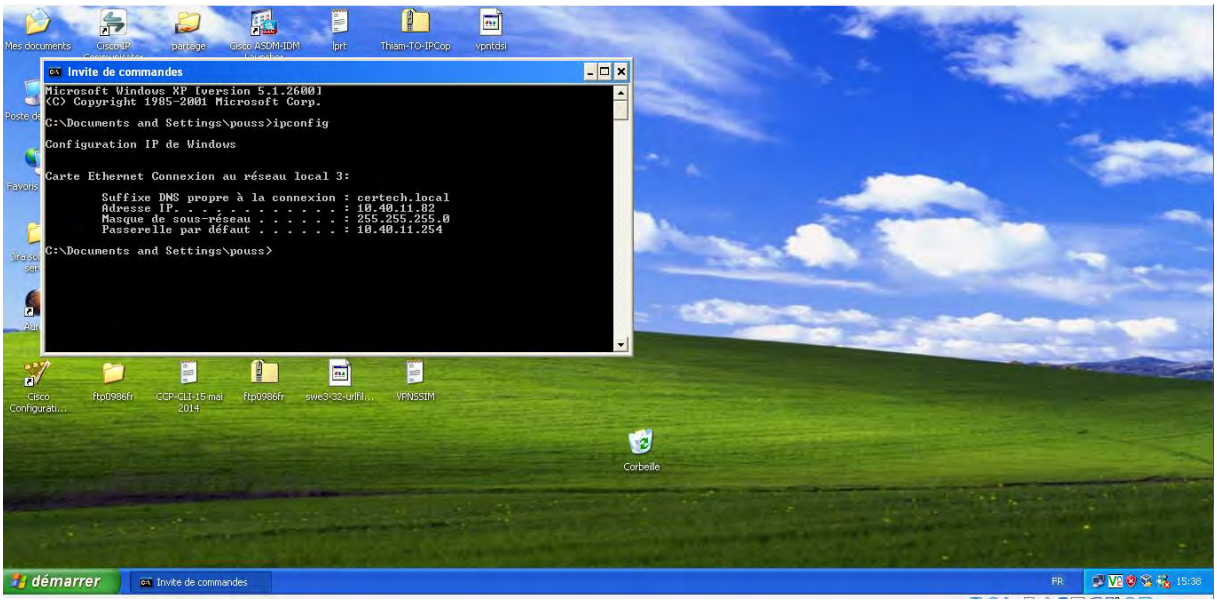


Figure 46: Capture de la machine qui sera attaquée

9.1 Démarche

En résumé, nous avons utilisé Metasploit d'adresse 10.40.11.211 pour s'introduire dans la machine cible ayant un système d'exploitation Windows avec l'adresse 10.40.11.82, détecté comme étant vulnérable. En effet, le Metasploit est un outil pour le développement et l'exécution d'exploits (logiciels permettant d'exploiter à son profit une vulnérabilité) contre une machine distante.

Figure 47:installation du metasploit

Dans la capture ci-dessus, l'attaquant à lancer Metasploit version5.0.41. Ce dernier a pu identifier la vulnérabilité de la machine cible, et va maintenant exploiter cette faille de sécurité. (Voir figure ci-dessous).

Figure 48: lancement de l'exploit par l'attaquant

Après avoir choisi le modèle d'exploit (windows/smb/ms08_067_netapi), l'attaquant tape la commande *show option* pour voir les détails d'exploitation de la vulnérabilité. Rhosts correspond à la machine de la cible, et Rport au port que nous devons utiliser pour s'introduire dans la machine. Voir figure ci- dessous.

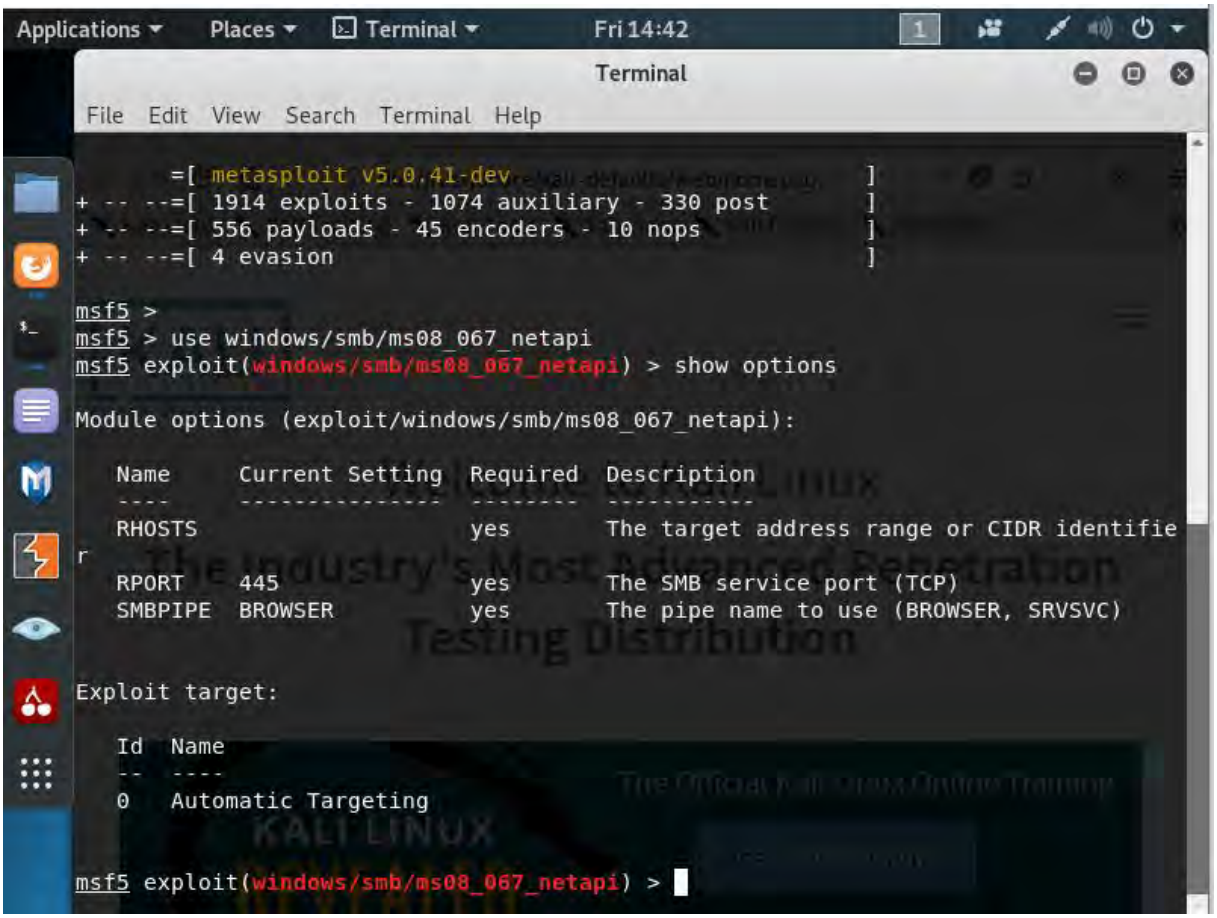


Figure 49: Utilisation de la commande show option pour voir les détails de l'exploit

Nous allons maintenant informer l'exploit de l'adresse IP de la machine qui va être attaquées, avec la commande *set,* et la commande *check* pour confirmer la vulnérabilité.

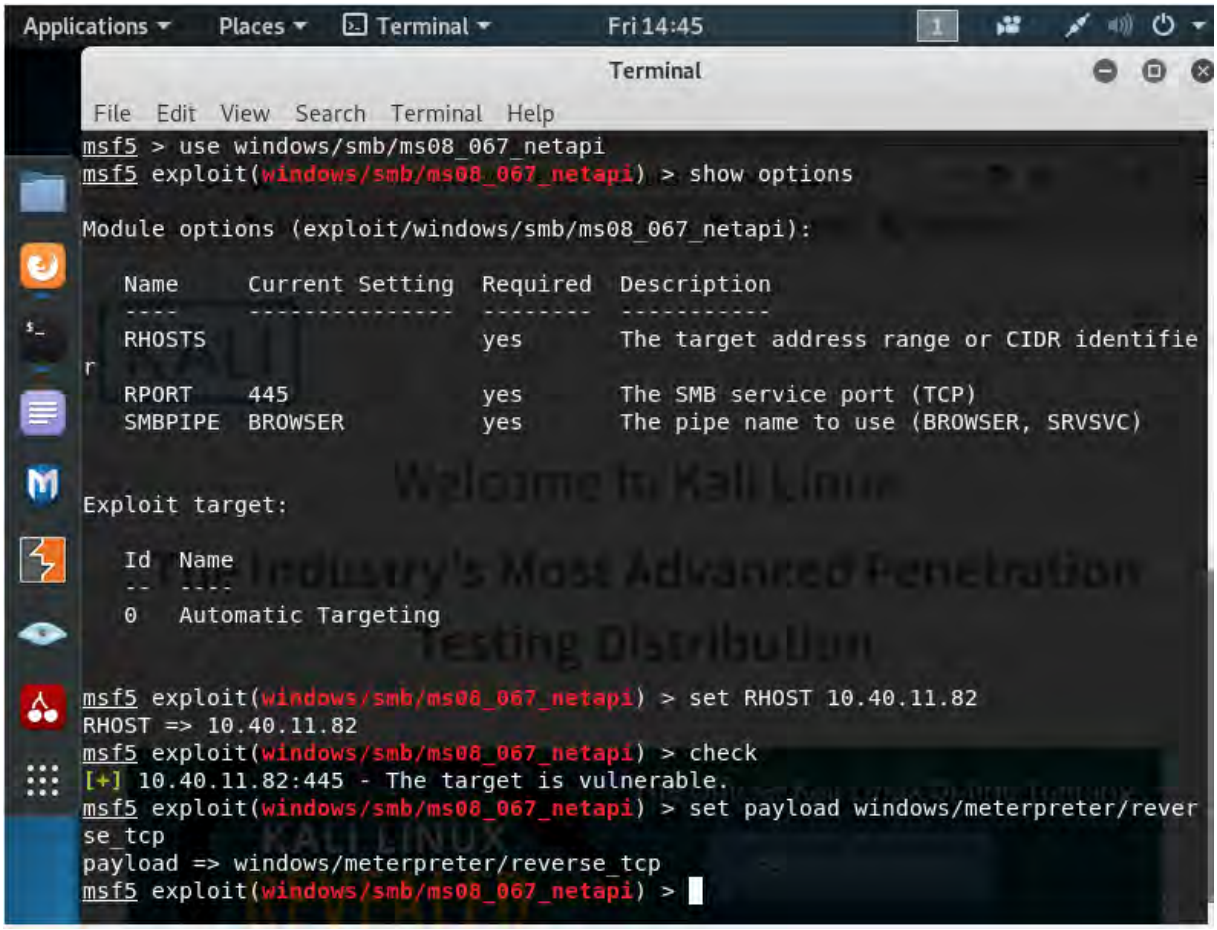


Figure 50: définition de la machine cible

La commande set *payload => windows/meterpreter/reverse_tcp* permet à l'attaquant de s'introduire carrément dans la machine cible.

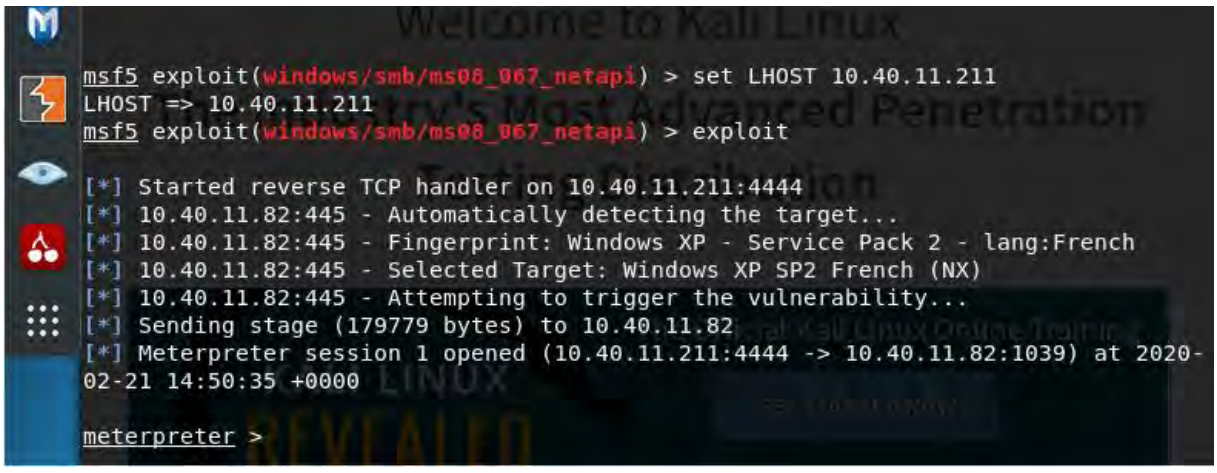


Figure 51: introduction de l'attaquant dans la machine cible

Dans la figure ci-dessus, nous voyons qu'une session a été effectivement ouverte dans la machine cible, le 21 février 2020, à 14h50. L'attaquant est maintenant dans la machine de la cible et à accès à tous ces fichiers.

L’attaquant a listé tous les dossiers de la cible avec la commande cd.

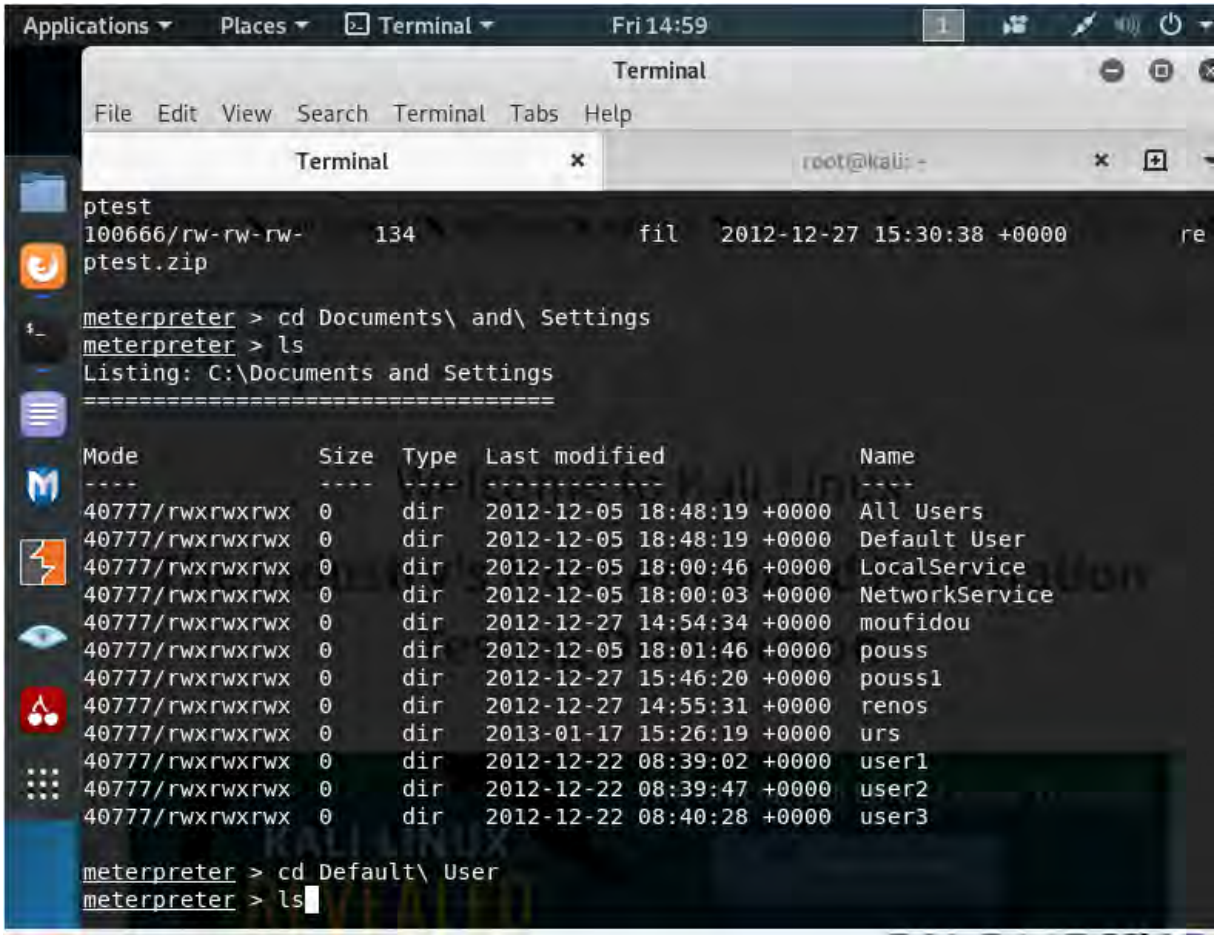
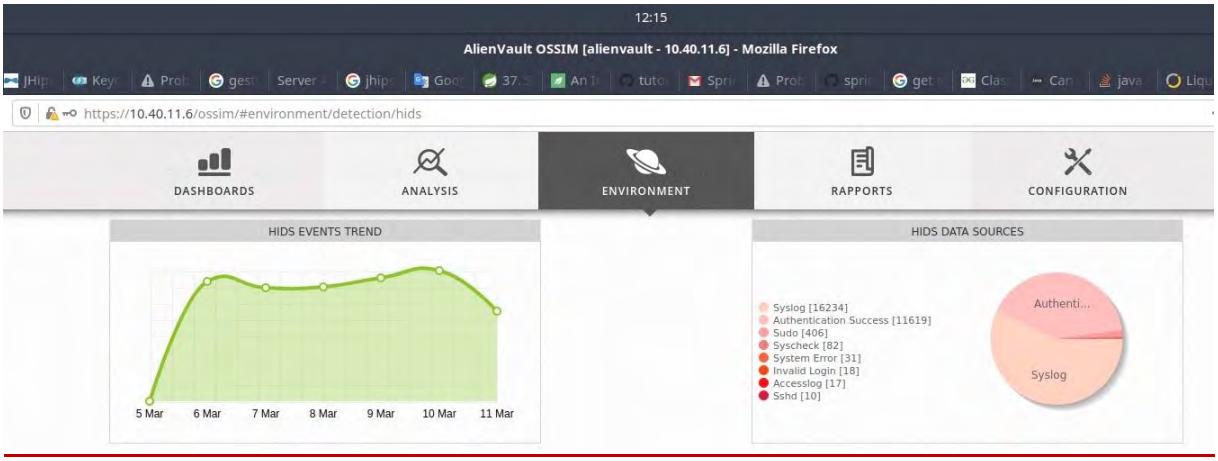


Figure 52: Affichage des dossiers de la cible par l'attaquant

9.2 Réaction d’OSSIM



Host-10-40-11-107	Host-10-40-11-107	10.40.11.107	-	-	Disconnected	Trend chart not available
Host-10-40-11-125	Host-10-40-11-125	10.40.11.125	-	-	Disconnected	Trend chart not available
Host-10-40-11-133	Host-10-40-11-133	10.40.11.133	10.40.11.133	-	Active	
Host-10-40-11-165	Host-10-40-11-165	10.40.11.165	-	-	Disconnected	Trend chart not available

Figure 53: détection des alertes et des événements d'OSSIM

la figure ci-dessus montre les statistiques faite par OSSIM des événements envoyé par les agents HIDS et la liste des agents connecté

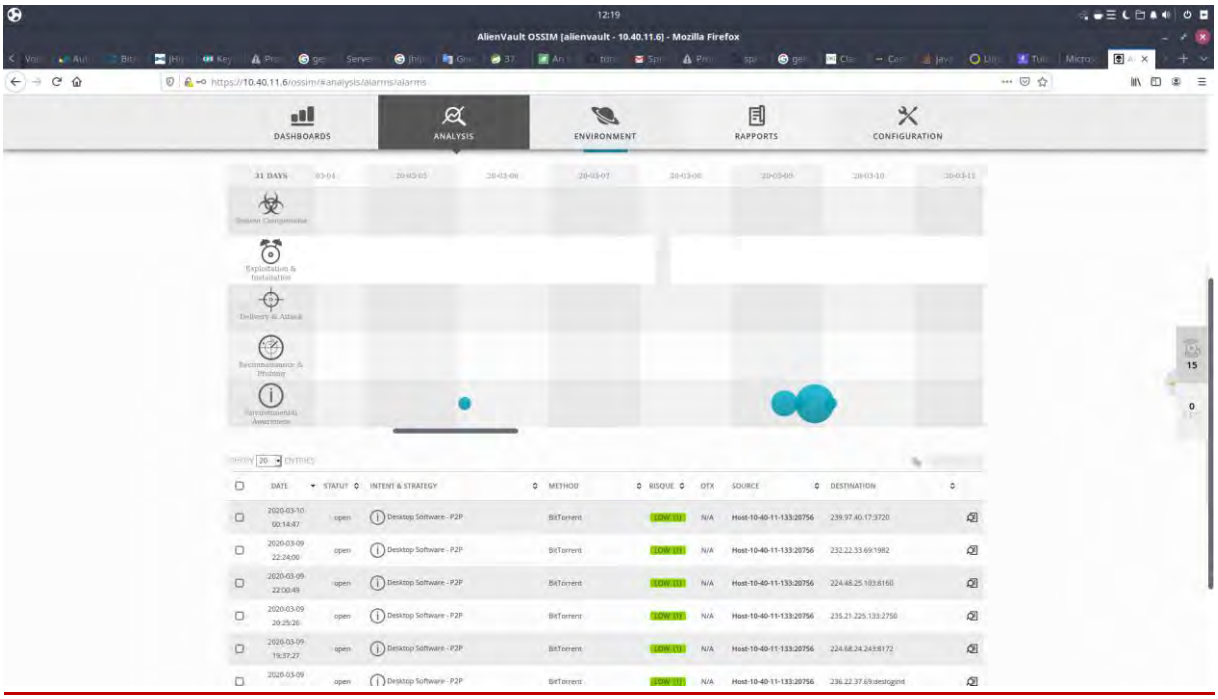


Figure 54: Vue des alertes

Cette figure représente les alertes détectées

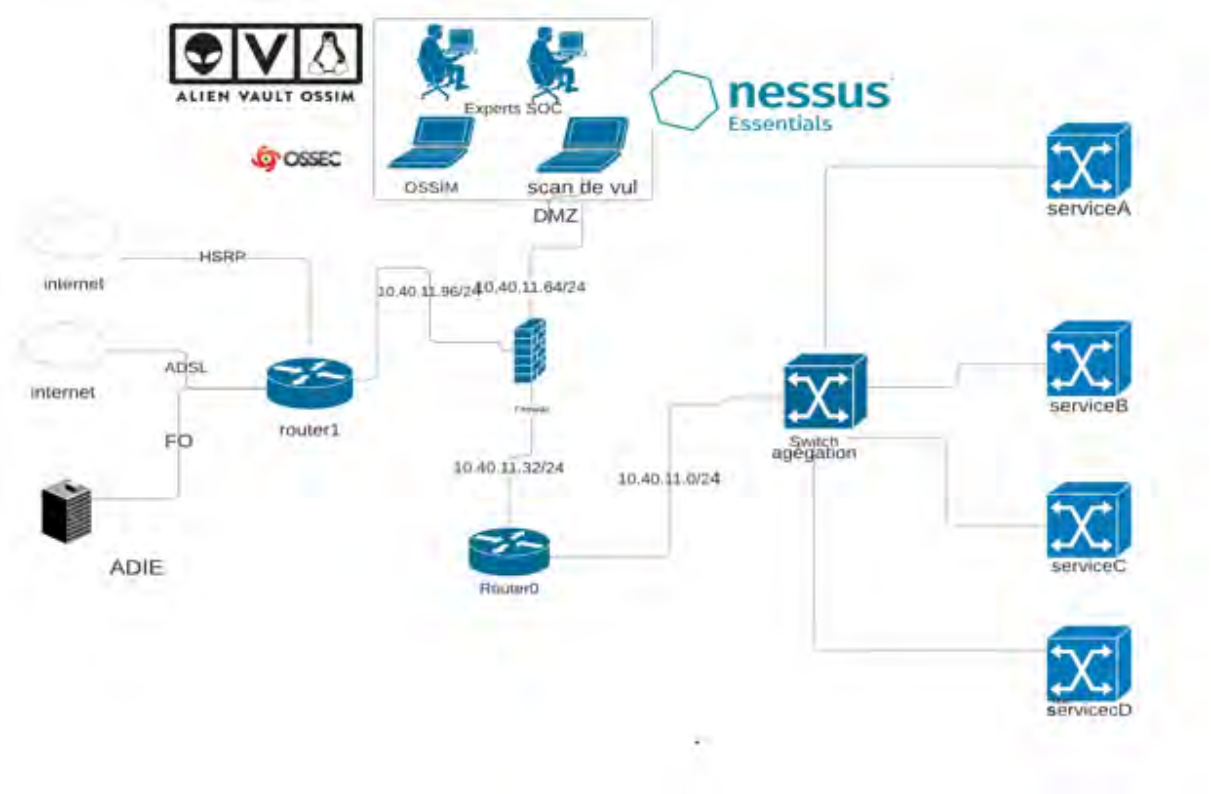


Figure 55: Récapitulatif de l'architecture réseau après le déploiement des solutions de sécurité

Conclusion

Le travail technique consistait d'abord à évaluer certains des risques auxquels la structure est exposée, définir ses équipements critiques grâce à l'outil Nessus Essentiel. Nous sommes ensuite passés directement à l'implémentation de notre SIEM AlientVault OSSIM, suivi de la configuration de ces différents modules, permettant à notre SOC d'être plus proactif et plus performant. Et enfin la dernière étape qui consistait à faire une simulation d'attaque interne afin de mesurer la capacité de détection de notre SOC.

Par ailleurs, les fonctions assurées par un SOC vont au-delà de tout cela, notamment la réaction face à un incident avec l'intervention de l'équipe CERT. L'élaboration des documents comme le Plan de reprise d'activité (PRA) et le Plan de continuité d'activité (PCA) qui sont des études préparatoires permettant d'assurer le fonctionnement vital de la structure en cas de crise aussi divers qu'ils soient (risques naturels, sanitaire, énergétiques…). La mise sur pied du Network Operation Center (NOC) qui est une entité très importante du SOC et qui a pour rôle essentiel d'assurer le bon fonctionnement de ce dernier.

En guise de perspectives, ces fonctionnalités pourront faire l'objet d'étude dans le but d'améliorer notre SOC et le rendre plus conforme aux normes internationales.

Webographie

1 http://www.presidence.sn/presidence/president [Date de dernière consultation le 10/12/2019]

2 https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.htm [Date de dernière consultation le 17/12/2019]

3https://www.manager-go.com/management-de-la-qualite/dossiers-methodes/pdca-deming-en-pratique [Date de dernière consultation le 10/11/2019]

4 https://www.supplychaininfo.eu/la-roue-de-deming/ [Date de dernière consultation le 09/10/2019]

5 https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf [Date de dernière consultation le 09/10/2019]

6https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/ [Date de dernière consultation le 24/12/2019]

7 https://www.ssi.gouv.fr/uploads/2015/02/guide_admin_securisee_si_anssi_pa_022_v2.pdf [Date de dernière consultation le 24/12/2019]

8 https://actualiteinformatique.fr/cybersecurite/quest-ce-quun-soc-security-operation-center [Date de dernière consultation le 10/02/2020]

9 https://www.itrust.fr/ressources/Datasheet/REF_SOC_datasheet_v1.2.pdf [Date de dernière consultation le 10/12/2019]

10https://www.orange-business.com/fr/blogs/securite/actualites/un-cybersoc-comment-ca-marche [Date de dernière consultation le 15/10/2019]

11 https://www.pandasecurity.com/france/mediacenter/securite/soc-role-cybersecurite/ [Date de dernière consultation le 22/12/2019]

12 https://fr.scribd.com/document/410610622/Bachelor-Report-pdf [Date de dernière consultation le 01/10/2019]

13https://www.forum-des-competences.org/assets/files/v1/Livrables/supervision-de-la-securite-des-si-dans-les-secteurs-banque-et-assurance-soc.pdf [Date de dernière consultation le 10/12/2019]

14https://www.orange-business.com/fr/blogs/securite/securite-organisationnelle-et-humaine/computer-emergency-response-team-qu-est-ce-qui-fait-l-efficacite-d-un-cert- [Date de dernière consultation le 10/12/2019]

15 https://blog.bssi.fr/siem-ssi/ [Date de dernière consultation le 10/12/2019]

16https://www.total-device.fr/produits/gestion-et-corr%C3%A9lation-d-%C3%A9v%C3%A9nements-siem/ [Date de dernière consultation le 10/12/2019]

17 https://www.synetis.com/siem-vue-unique-systeme-dinformation/ [Date de dernière consultation le 10/10/2019]

18 https://www.lemagit.fr/conseil/SIEM-une-cle-pour-reponse-a-incident-plus-efficace [Date de dernière consultation le 25/12/2019]

19 https://cybersecurite-hq.fr/2018/02/supervision-de-securite-des-systemes-dinformation-les-limites-du-modele-actuel/ [Date de dernière consultation le 02/12/2019]

20https://docplayer.fr/3644313-Conception-d-un-projet-siem-la-securite-des-systemes-d-information.html [Date de dernière consultation le 05/01/2020]

21https://www.ibm.com/support/knowledgecenter/fr/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_deployment_guide_arch.html [Date de dernière consultation le 10/12/2019]

22https://www.ibm.com/support/knowledgecenter/fr/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_pdfs.html [Date de dernière consultation le 28/12/2019]

23 https://stph.scenari-community.org/contribs/dwh/Splunk/co/Splunk_9.html [Date de dernière consultation le 03/10/2019]

24 http://download.velannes.com/Ossim_doc.pdf [Date de dernière consultation le 12/10/2019]

25 https://www.gartner.com/en/documents/3894573 [Date de dernière consultation le 11/11/2019]

26http://igm.univ-mlv.fr/~dr/XPOSE2009/Nessus/nessus_scan.html [Date de dernière consultation le 04/11/2019]

27https://www.ibm.com/support/knowledgecenter/fr/SS42VS_DSM/com.ibm.dsm.doc/c_vuln_Qualysoverview.html [Date de dernière consultation le 06/11/2019]

28 https://fr.slideshare.net/ITrustFrance/ikare-vulnerability-scanner-datasheet-fr [Date de dernière consultation le 08/09/2019]

29 https://logrhythm.com/gartner-magic-quadrant-siem-report-2018/ [Date de dernière consultation le 10/12/2019]

https://www.informatiquenews.fr/soc-role-cybersecurite-selon-gartner-54048 [Date de dernière consultation le 07/10/2019]

https://www.ssi.gouv.fr/actualite/prevention-detection-et-reponse-aux-incidents-au-centre-des-preoccupations-des-gs-days-2016/ [Date de dernière consultation le 09/10/2019]

https://www.artpsenegal.net/sites/default/files/docs_actualites/pssi-es163250.pdf [Date de dernière consultation le 11/12/2019]

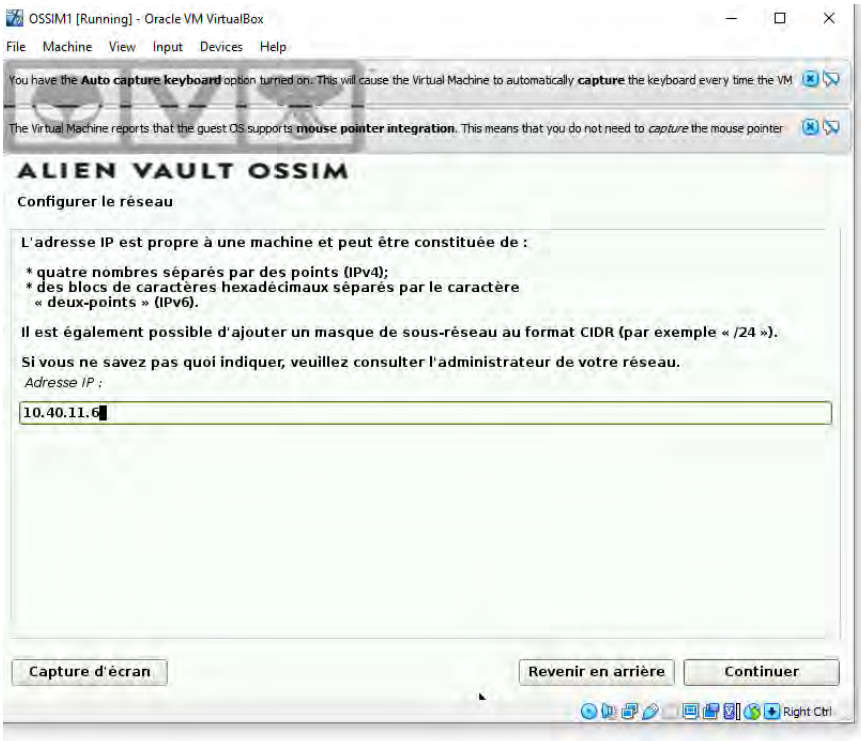
https://www.sekurigi.com/2014/11/comment-reussir-son-security-operation-center-le-guide/ [Date de dernière consultation le 10/11/2019]

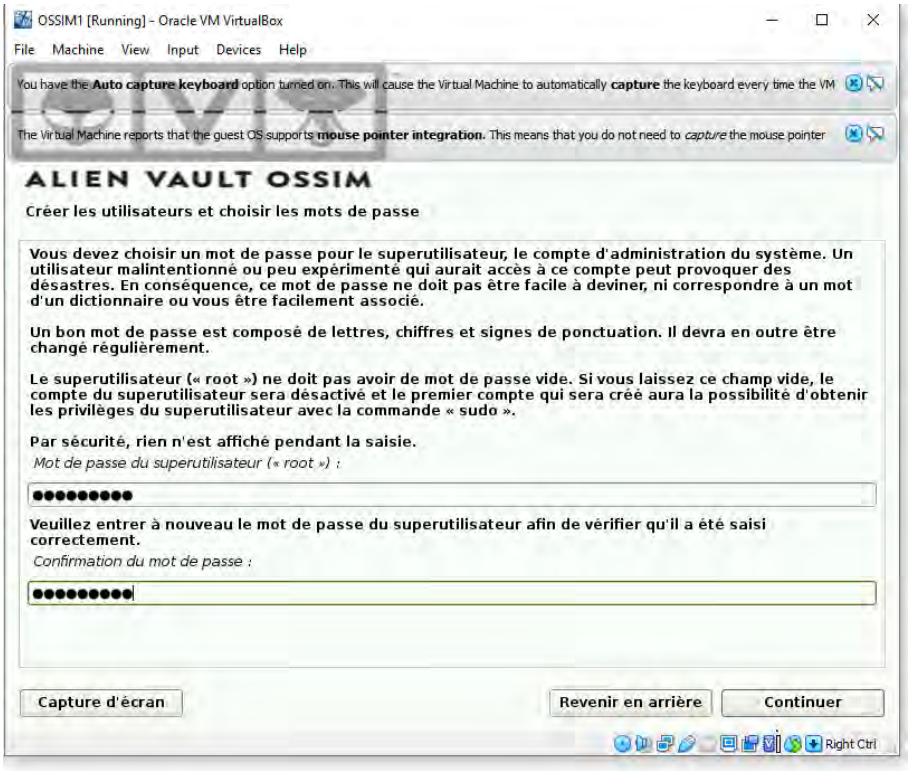
https://www.pandasecurity.com/france/mediacenter/securite/soc-role-cybersecurite/ [Date de dernière consultation le 10/11/2019]

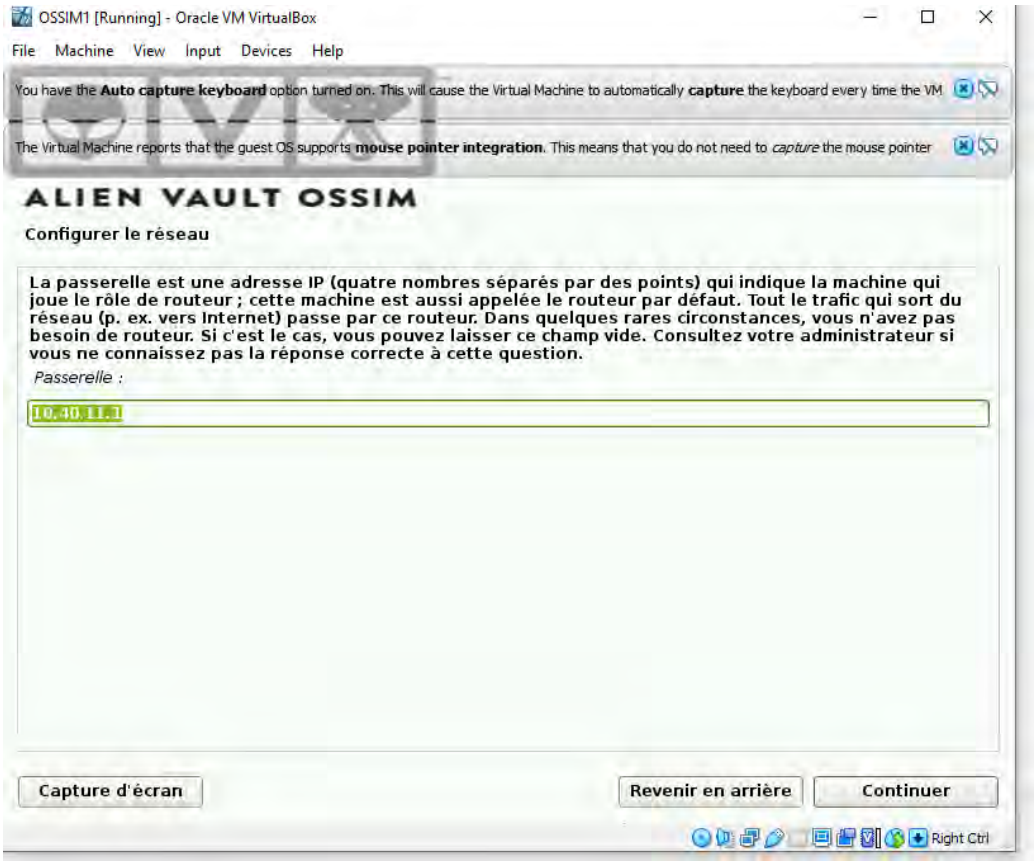
https://www.linkbynet.com/fr/pourquoi-un-soc-est-indispensable-aujourdhui

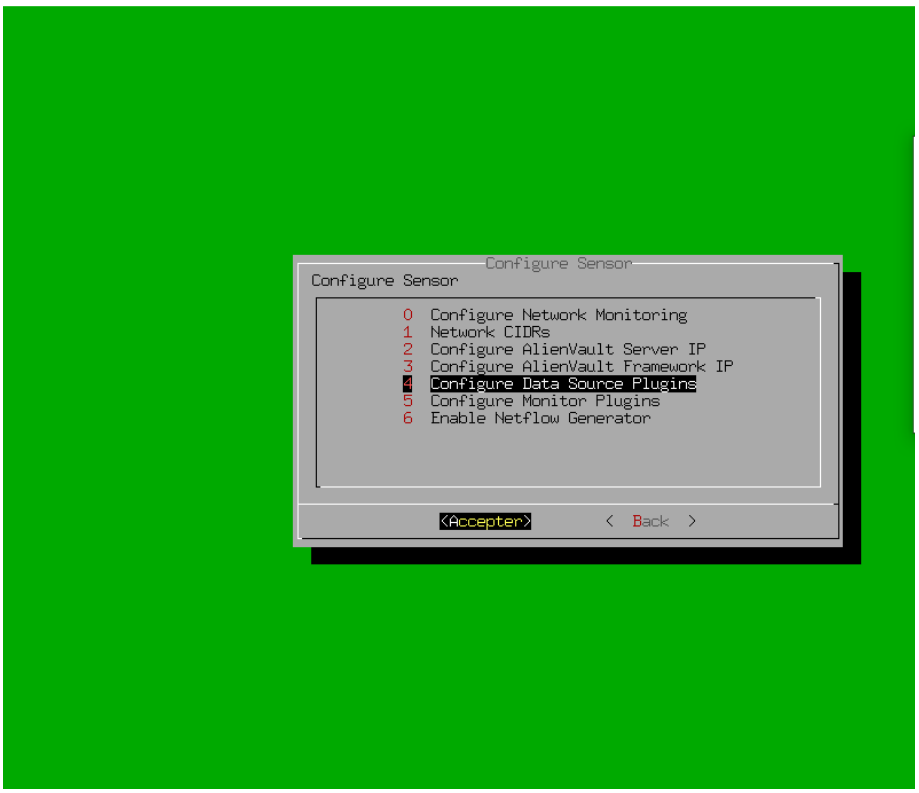
Annexe

Ci-dessous, un petit résumé de la procédure d'installation d'AlienVault OSSIM



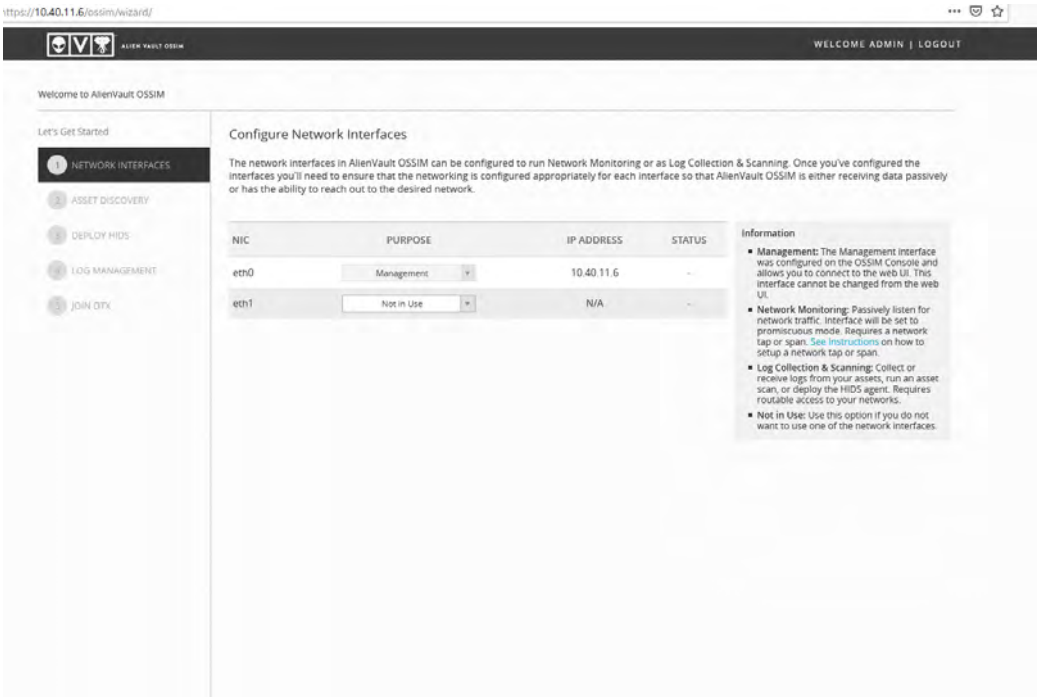


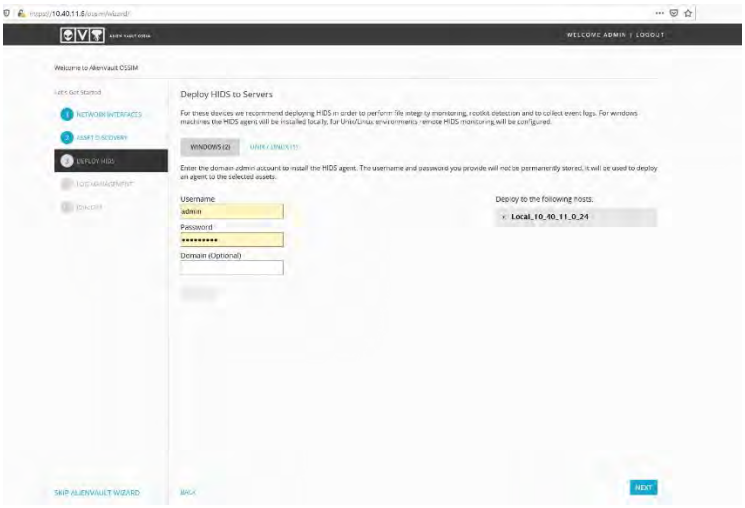

OSSIM1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer
ALIEN VAULT OSSIM
Configurer le réseau
La passerelle est une adresse IP (quatre nombres séparés par des points) qui indique la machine qui joue le rôle de routeur ; cette machine est aussi appelée le routeur par défaut. Tout le trafic qui sort du réseau (p. ex. vers Internet) passe par ce routeur. Dans quelques rares circonstances, vous n'avez pas besoin de routeur. Si c'est le cas, vous pouvez laisser ce champ vide. Consultez votre administrateur si vous ne connaissez pas la réponse correcte à cette question.
Passerelle :
10.40.11.1
Capture d'écran
Revenir en arrière
Continuer
Right Ctrl


Configure Sensor
Configure Sensor
0 Configure Network Monitoring
1 Network CIDRs
2 Configure AlienVault Server IP
3 Configure AlienVault Framework IP
4 Configure Data Source Plugins
5 Configure Monitor Plugins
6 Enable Netflow Generator
<Accepter>
< Back >

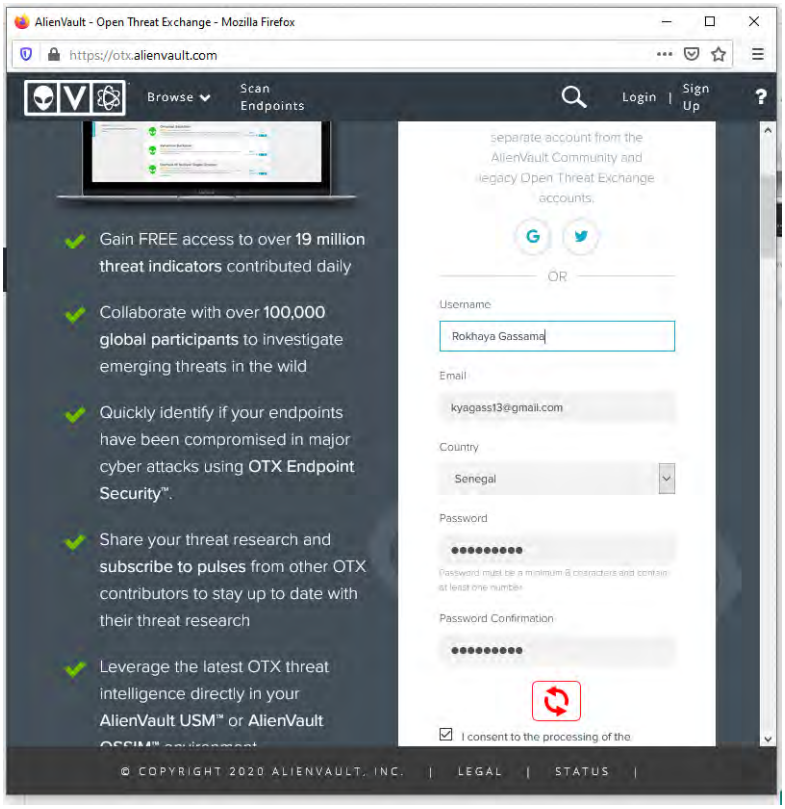
La reconfiguration des paramètres systèmes a été faite avec succès.

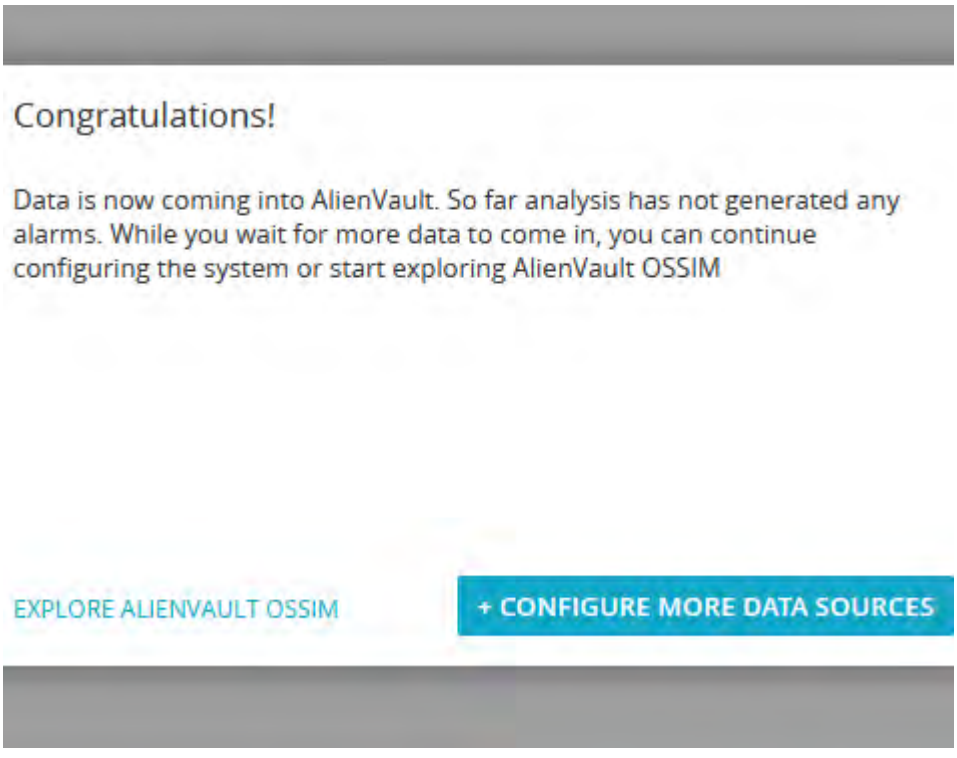
Après avoir connecté l'administrateur WEB à partir du navigateur, nous pouvons faire les configurations de base comme l'image ci-dessous.





À l'étape de rejoindre OTX, nous nous sommes inscrits, remplis nos informations d'identification et après avoir réussi, nous avons obtenu notre clé OTX. Ensuite entrer dans la colonne OTX et cliquez sur Suivant, si OTX ne vous est pas envoyé, vous pourrez vérifier la clé OTX plus tard sur le site Web https://otx.alienvault.com/api/ après votre connexion.


AlienVault - Open Threat Exchange - Mozilla Firefox
https://otx.alienvault.com
Browse
Scan Endpoints
Login | Sign Up
Gain FREE access to over 19 million threat indicators contributed daily
Collaborate with over 100,000 global participants to investigate emerging threats in the wild
Quickly identify if your endpoints have been compromised in major cyber attacks using OTX Endpoint Security™.
Share your threat research and subscribe to pulses from other OTX contributors to stay up to date with their threat research
Leverage the latest OTX threat intelligence directly in your AlienVault USM™ or AlienVault
separate account from the AlienVault Community and legacy Open Threat Exchange accounts.
OR
Username
Rokhaya Gassama
Email
kyagass13@gmail.com
Country
Senegal
Password
Password Confirmation
I consent to the processing of the
© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS |


Congratulations!
Data is now coming into AlienVault. So far analysis has not generated any alarms. While you wait for more data to come in, you can continue configuring the system or start exploring AlienVault OSSIM
EXPLORE ALIENVAULT OSSIM
+ CONFIGURE MORE DATA SOURCES