



---

Institut National des Sciences Appliquées et de Technologie

UNIVERSITÉ DE CARTHAGE

## Projet de Fin d'Études

Filière : Réseaux informatiques et Télécommunications

---

---

### Conception et mise en place d'un centre d'opération de sécurité (SOC)

---

Présenté par

**Marwa CHAIEB**

Encadrant INSAT : **Mr YOUSFI Souheib**  
Encadrant ENTREPRISE : **Mr JRAD Mehdi**

Présenté le : **17/06/2017**

### JURY

M. President Bassem BEN SALAH (Président)  
M. Rapporteur Zied DRIDI (Rapporteur)

Année Universitaire : 2016/2017



---

# Remerciements

Au terme de ce projet de fin d'études, mes vifs remerciements sont dédiés à tous ceux qui ont contribué, directement ou indirectement à l'élaboration de ce projet.

En premier lieu, j'exprime ma gratitude à Monsieur Souheib YOUSFI, mon encadrant à l'INSAT, pour sa confiance, ses directives, ses conseils et pour m'avoir accordé son temps. Ses critiques constructives et son encouragement permanent, m'ont énormément aidée dans l'accomplissement de ce projet. Je le remercie vivement.

J'adresse mes remerciements à Monsieur Mehdi JRAD, mon responsable de stage au sein de l'Office de l'Aviation Civile et des Aéroports pour son accueil, le partage de son temps et de son expertise au quotidien. Grâce aussi à sa confiance et son aide précieuses que j'ai pu m'accomplir dans mes missions et surpasser les moments les plus délicats.

Je remercie également toute l'équipe de l'OACA pour leur accueil et leur esprit d'équipe.

Mes remerciements les plus distingués sont adressés aussi aux membres du jury qui m'ont fait l'honneur de bien vouloir accepter d'évaluer ce travail.

Par la même occasion, je présente ma reconnaissance à tous les enseignants de l'INSAT, à qui je dois toutes les connaissances que j'ai acquises.

---

# Table de Matières

<b>Liste des Figures</b>	<b>v</b>
<b>Liste des Tableaux</b>	<b>ix</b>
<b>Introduction générale</b>	<b>1</b>
<b>I Cadre du projet et état de l'art</b>	<b>3</b>
1 Cadre du projet . . . . .	3
1.1 Présentation de l'organisation d'accueil . . . . .	3
1.1.1 Missions . . . . .	4
1.1.2 Activités internationales . . . . .	5
1.2 Contexte du projet . . . . .	5
1.2.1 Problématique . . . . .	5
1.2.2 Objectifs . . . . .	7
1.2.3 Planification du déroulement du projet . . . . .	7
2 État de l'art : Security Operations Center (SOC) . . . . .	8
2.1 Le personnel . . . . .	9
2.2 Les processus et les procédures . . . . .	9
2.3 La technologie . . . . .	10
2.3.1 SIEM . . . . .	10
2.3.2 Étude comparative des solutions SIEM . . . . .	12
<b>II Spécification des besoins et étude théorique</b>	<b>20</b>
1 Spécification des besoins . . . . .	20
1.1 Besoins fonctionnels . . . . .	20
1.2 Besoins non fonctionnels . . . . .	22
1.3 Topologie réseau . . . . .	22
2 Étude théorique . . . . .	23
2.1 Choix de la solution SIEM . . . . .	23
2.1.1 Présentation générale de la solution choisie . . . . .	24
2.1.2 Architecture . . . . .	24
2.1.3 Fonctionnalités d'OSSIM . . . . .	25
2.2 Staff SOC . . . . .	26

---

2.3	Procédure de gestion des incidents . . . . .	28
2.3.1	La phase de préparation . . . . .	29
2.3.2	La phase de la détection et d'analyse . . . . .	30
2.3.3	La phase de contournement, éradication et récupération . . . . .	31
2.3.4	La phase de l'activité post-incident . . . . .	32
<b>III</b>	<b>Mise en place d'OSSIM : Paramétrage, configuration et déploiement</b>	<b>34</b>
1	Environnement de travail . . . . .	35
1.1	Environnement matériel . . . . .	35
1.2	Environnement logiciel . . . . .	36
2	Mise en place d'OSSIM . . . . .	37
2.1	Installation et configuration d'OSSIM . . . . .	37
2.2	Personnalisation de la solution . . . . .	37
3	Mise en place des systèmes externes . . . . .	39
3.1	Collecte des logs Windows . . . . .	40
3.2	Collecte des logs Linux . . . . .	41
3.3	Collecte des logs Apache . . . . .	42
3.4	Collecte des logs IIS . . . . .	44
3.5	Collecte des logs du pare-feu . . . . .	46
3.6	Collecte des logs routeur . . . . .	47
4	Mise en place de Nagios . . . . .	47
5	Sécurisation de la plateforme . . . . .	50
5.1	Gestion des ports . . . . .	50
5.2	Configuration d'un certificat SSL . . . . .	50
5.3	Sécurisation de l'accès SSH . . . . .	54
5.4	Sécurisation de l'authentification . . . . .	55
<b>IV</b>	<b>Test des fonctionnalités de la solution OSSIM</b>	<b>58</b>
1	Test de la fonctionnalité de génération des tableaux de bord . . . . .	58
2	Test de la fonctionnalité de découverte du réseau . . . . .	61
3	Test de la fonctionnalité de corrélation des événements . . . . .	63
3.1	Corrélation croisée : (cross correlation) . . . . .	63
3.2	Directives de corrélation . . . . .	64
4	Test des politiques de sécurité . . . . .	67
4.1	Définition d'une nouvelle action . . . . .	67

4.2	Définition d'une nouvelle politique . . . . .	68
5	Traitemen manuel d'un événement de sécurité . . . . .	69
6	Test de la génération des rapports . . . . .	70
7	Backup . . . . .	74
<b>Conclusion générale et perspectives</b>		<b>77</b>
<b>Bibliographie</b>		<b>78</b>
<b>Annexe A : Installation et configuration d'OSSIM</b>		<b>81</b>
<b>Annexe B : Installation d'OSSEC sous Windows et Linux</b>		<b>89</b>
<b>Annexe C : Création d'une directive de corrélation</b>		<b>95</b>

---

# Liste des Figures

I.1	Logo OACA . . . . .	4
I.2	Architecture réseau de l’OACA . . . . .	6
I.3	Planification du projet . . . . .	8
I.4	Composantes du SOC . . . . .	9
I.5	Architecture du SIEM . . . . .	11
I.6	Gartner Magic Quadrant pour le SIEM . . . . .	15
II.1	Topologie réseau à intégrer dans le SOC . . . . .	22
II.2	Fonctionnement d’OSSIM . . . . .	25
II.3	Cycle de vie de la réponse aux incidents . . . . .	29
III.1	Fujitsu Siemens Primergy rx4770m2 . . . . .	35
III.2	Création d’une machine virtuelle pour installer OSSIM . . . . .	36
III.3	Page d’authentification par défaut d’OSSIM . . . . .	38
III.4	Nouveau design de la page d’authentification . . . . .	39
III.5	Exemple de logs OSSEC à partir de la machine Windows . . . . .	40
III.6	Cycle de redirection des logs Linux . . . . .	41
III.7	Exemple de logs OSSEC à partir de la machine Linux . . . . .	41
III.8	Exemple de logs Apache collectés par Snare . . . . .	42
III.9	Zoom sur un exemple de log Apache . . . . .	43
III.10	Exemple de logs Apache . . . . .	44
III.11	Exemple de logs du serveur IIS collectés par Snare . . . . .	44
III.12	Zoom sur un exemple de log IIS . . . . .	45
III.13	Exemple de logs IIS reçus en temps réel . . . . .	46
III.14	Configuration du pare-feu . . . . .	46
III.15	Exemple de logs du pare-feu . . . . .	46
III.16	Configuration du routeur central . . . . .	47
III.17	Exemple de logs du routeur central . . . . .	47
III.18	Activation de Nagios . . . . .	48
III.19	Activation de la supervision avec nagios pour un hôte . . . . .	48
III.20	Détails sur les hôtes supervisés par Nagios . . . . .	49
III.21	Détails sur les services d’un hôte . . . . .	49
III.22	Ports utilisés pour la communication entre les composants d’OSSIM . . . . .	50

III.23 Problème de certificat . . . . .	51
III.24 Génération de la clé RSA . . . . .	51
III.25 Génération d'une demande de certificat SSL . . . . .	51
III.26 Demande d'un certificat . . . . .	52
III.27 Conversion de "cer" en "pem" . . . . .	52
III.28 Configuration du certificat d'OSSIM . . . . .	53
III.29 Vérification de la bonne configuration du certificat . . . . .	54
III.30 Création d'un compte dans LDAP . . . . .	55
III.31 Configuration d'OSSIM pour l'authentification avec LDAP . . . . .	56
IV.1 Exemple de tableau de bord : "Executive" . . . . .	59
IV.2 Exemple de tableau de bord : "Security" . . . . .	60
IV.3 Tableau de bord "Netflow" . . . . .	61
IV.4 Exemple de scan d'un hôte . . . . .	62
IV.5 Résultat du scan . . . . .	62
IV.6 Exemple de corrélation croisée : Déetecter une tentative d'authentification MySQL avec un mot de passe vide . . . . .	64
IV.7 Exemple de directive de corrélation - détection d'attaques de force brutale . . . . .	66
IV.8 Déclenchement de l'alarme . . . . .	66
IV.9 Détails de l'alarme . . . . .	67
IV.10 Exemple de création d'une action . . . . .	68
IV.11 Exemple de création d'une politique . . . . .	69
IV.12 Événement suspect . . . . .	69
IV.13 Ouvrir un ticket . . . . .	70
IV.14 Rapport sur les alarmes . . . . .	70
IV.15 Rapport sur un hôte . . . . .	71
IV.16 Rapport du Business et de conformité ISO PCI . . . . .	71
IV.17 Rapport géographique . . . . .	71
IV.18 Rapport sur les évènements SIEM . . . . .	71
IV.19 Rapport sur les Menaces et les vulnérabilités . . . . .	71
IV.20 Rapport sur le statut des tickets . . . . .	72
IV.21 Rapport sur les tickets . . . . .	72
IV.22 Rapport sur l'activité d'un utilisateur . . . . .	72
IV.23 Extrait du rapport sur l'activité d'un utilisateur . . . . .	73
IV.24 Rapport sur les vulnérabilités . . . . .	73

IV.25 Rapport de vulnérabilité de sécurité . . . . .	74
IV.26 Configuration du backup . . . . .	75
IV.27 Exemple d'historique des opérations effectuées sur les fichiers de backup . . . . .	76
A.1 Choix de l'option "Install AlienVault OSSIM" . . . . .	81
A.2 Choix de la langue d'OSSIM . . . . .	82
A.3 Choix de la localisation . . . . .	82
A.4 Choix du clavier . . . . .	83
A.5 Chargement des composants d'installation . . . . .	83
A.6 Choix de l'interface de gestion . . . . .	84
A.7 Adresse IP et masque de sous réseau . . . . .	84
A.8 Adresse de la passerelle par défaut . . . . .	85
A.9 Adresse du serveur DNS . . . . .	85
A.10 Mot de passe de l'utilisateur "root" . . . . .	86
A.11 Installation d'OSSIM . . . . .	86
A.12 La console d'OSSIM . . . . .	87
A.13 Configuration des interfaces réseaux . . . . .	87
A.14 Tableau de bord d'OSSIM . . . . .	88
B.1 Activation du plugin OSSEC . . . . .	89
B.2 Enregistrement de la modification . . . . .	90
B.3 Ajout d'un nouvel agent OSSEC . . . . .	90
B.4 Extraction de la clé client . . . . .	91
B.5 Configuration de l'agent OSSEC client sous Windows . . . . .	92
B.6 Choix du type de l'installation . . . . .	92
B.7 Choix de l'emplacement de l'installation . . . . .	93
B.8 Saisie de l'adresse IP de l'agent serveur OSSEC . . . . .	93
B.9 Liste des fichiers logs à analyser par OSSEC . . . . .	93
B.10 Fin de l'installation de l'agent OSSEC sous Linux . . . . .	94
B.11 Importation de la clé client . . . . .	94
B.12 Détails des deux agents OSSEC . . . . .	94
C.1 Ajout d'une nouvelle directive . . . . .	95
C.2 Ajout de la règle du premier niveau . . . . .	95
C.3 Choix du plugin_id . . . . .	96
C.4 Liste des plugin_sid . . . . .	97

## Liste des Figures

---

C.5 Suite de la liste des plugin_sid . . . . .	97
C.6 Configuration des adresses IP et des ports . . . . .	98
C.7 Configuration de la valeur du paramètre "reliability" . . . . .	98
C.8 Directive avec un seul niveau de corrélation . . . . .	99
C.9 Directive avec ses trois niveaux de corrélation . . . . .	99

---

# Liste des Tableaux

I.1	Comparaison des solutions SIEM open source	18
II.1	Membres du staff SOC	27

---

# Introduction générale

Toute organisation est dotée d'un "périmètre de sécurité" qui entoure les ressources qu'elle doit protéger contre les accidents naturels ou les attaques humaines. Ce périmètre englobe l'espace physique (les locaux, les équipements, les documents, les personnes...) et le "cyberespace" ou l'espace logique de cette organisation (les données, les systèmes d'exploitation, les programmes informatiques...).

Les menaces naturelles ou d'origine humaine que l'institution peut confronter ne sont pas nouvelles. Mais dans l'espace logique, elles prennent des formes nouvelles. Elles pénètrent l'institution en empruntant des procédés et vecteurs nouveaux. Elles peuvent enfin, s'appuyant sur la puissance de l'informatique, causer des dommages d'une ampleur inédite.

La prévention des attaques connues est déjà assez dure, mais comment font les organisations pour construire des contrôles de sécurité pour limiter les risques qu'ils ne connaissent même pas encore ?

La force des entreprises, pour la défense de leur patrimoine informationnel, repose alors sur la détection rapide de tout incident et la réaction immédiate appropriée. C'est ostensiblement le rôle de centres de supervision de la sécurité, tels que les Security Operations Center (SOC). Un soc peut former une solution de détection très efficace, une telle infrastructure peut maximiser les investissements de sécurité existants en liant des composants de sécurité individuels (les anti-virus, IPS, IDS, etc) d'une manière qui étend les avantages que ces systèmes apportent et permettent une réponse plus rapide, une meilleure collaboration ainsi qu'un partage des connaissances.

Un SOC bien établi représente une base solide pour l'excellence opérationnelle, conduite par des processus bien conçus et exécutés, une forte gouvernance des individus et une recherche constante de l'amélioration continue afin de rester solide face aux cyber-adversaires. Un bon SOC doit respecter les objectifs d'affaires et améliore la posture de risque d'une entreprise pour atteindre ses objectifs.

C'est dans ce cadre que s'inscrit mon projet de fin d'études qui consiste à étudier, concevoir et mettre en place une plateforme SOC basée sur des solutions open source au profit de l'Office de l'Aviation Civile et des Aéroports (OACA).

L'objectif de ce stage est de concevoir l'architecture du SOC qui répond bien aux besoins de l'entreprise, d'identifier ses différentes composantes ainsi que d'étudier les différentes solutions open source existantes et de choisir la plus adéquate par la suite. La dernière étape consiste à

déployer les solutions choisies afin de garantir un niveau de sécurité élevé et une vision globale de l'état du réseau informatique.

Tous ces objectifs font l'objet du présent rapport qui synthétise mon projet de fin d'études clôturant ma formation en Réseaux informatiques et Télécommunications au sein de l'Institut Nationale des Sciences Appliquées et de la Technologie. Il est composé de quatre chapitres et présentant les différentes étapes du déroulement du projet.

Dans le premier chapitre intitulé "cadre du projet et état de l'art", nous allons présenter le cadre du projet, partant de la présentation de l'organisation d'accueil, ses rôles, sa structure et les services qu'elle offre, allant jusqu'à présenter le contexte du projet et décrire la planification du déroulement du projet. Nous allons aussi étudier le concept du SOC et son implémentation. Nous mènerons par la suite une étude comparative des solutions existantes dans le marché. Le deuxième chapitre "Spécification des besoins et étude théorique" va porter sur les besoins de l'entreprise ainsi qu'une étude théorique de la solution choisie pour répondre à ces besoins. Dans le troisième chapitre nous détaillerons les étapes de mise en place et la configuration des éléments de l'architecture que nous avons proposée.

Finalement, le quatrième chapitre, est consacré aux tests réalisés pour valider l'aptitude de la plateforme à garantir les besoins de l'entreprise.

---

---

# Chapitre I

---

## Cadre du projet et état de l'art

### Plan

<b>1</b>	<b>Cadre du projet</b>	<b>3</b>
1.1	Présentation de l'organisation d'accueil	3
1.2	Contexte du projet	5
<b>2</b>	<b>État de l'art : Security Operations Center (SOC)</b>	<b>8</b>
2.1	Le personnel	9
2.2	Les processus et les procédures	9
2.3	La technologie	10

### Introduction

Ce premier chapitre est consacré à la présentation du contexte général du projet et de l'état de l'art. Nous commençons par présenter l'entreprise d'accueil ainsi que ses différentes activités. Puis, nous entamerons une présentation de la problématique qui a poussé l'équipe de sécurité à proposer ce projet. Nous enchaînerons par expliciter le contexte, les objectifs ainsi que les différentes étapes de réalisation du projet. Ensuite, nous présentons le concept SOC et ses différentes composantes pour finir par une comparaison des différents outils existants sur le marché.

## 1 Cadre du projet

Dans cette partie, nous introduisons le cadre de notre projet ainsi que la problématique et la planification de la période du stage.

### 1.1 Présentation de l'organisation d'accueil

L'Office de l'Aviation Civile et des Aéroports (OACA) [1] est un établissement public à caractère industriel et commercial doté de la personnalité civile et de l'autonomie financière. Il

## I.1 Cadre du projet

---

est sous tutelle du Ministère du Transport et est chargé de gérer, de développer et d'exploiter les 7 Aéroports Internationaux :

- Tunis-Carthage,
- Djerba-Zarzis,
- Sfax-Thyna,
- Tozeur-Nefta,
- Tabarka-Ain Draham,
- Gafsa-Ksar,
- Gabès-Matmata.

L'OACA a concédé l'exploitation de l'Aéroport "Monastir Habib Bourguiba" à partir du 01 janvier 2008 et la construction de l'Aéroport "Enfidha Hammamet" au mois de Mai 2007 à une entreprise privée. Ce dernier est entré en exploitation au mois de Décembre 2009.



**Figure I.1 – Logo OACA**

### 1.1.1 Missions

L'OACA est chargé des missions suivantes :

- L'exploitation, l'aménagement et le développement des aéroports ainsi que l'accomplissement de toutes les opérations et services nécessaires aux voyageurs, au public, aux aéronefs, au fret et au courrier aérien dans les aéroports,
- Le contrôle régional et local de la navigation aérienne et la participation à l'exécution des plans de recherches et de sauvegarde,
- Les opérations de délivrance et de renouvellement des titres du personnel civil naviguant et des documents d'aéronefs,
- L'application des exigences réglementaires dans le domaine de la navigabilité des aéronefs [1].

### 1.1.2 Activités internationales

Sur le plan international, l’OACA occupe une place de plus en plus importante au sein des instances arabes, africaines et mondiales telles que le Conseil de l’Aviation Civile des Pays Arabes, la Commission Africaine de l’Aviation Civile, l’Organisation de l’Aviation Civile Internationale, le Conseil International des Aéroports...

L’OACA est membre du Conseil International des Aéroports Région Afrique et préside le Groupe Régional de Planification et de Mise en Œuvre de Plan de Navigation Aérienne pour l’Afrique et l’Océan Indien. Il est également membre du Conseil d’Administration du Fonds. L’Office s’est distingué ces dernières années par la qualité de l’organisation, en Tunisie, de manifestations et de conférences de taille se rapportant aux domaines de l’aviation civile, la gestion et la sûreté aéroportuaire.

IL a également signé des conventions de partenariat avec son homologue au Maroc, la Société des Aéroports en Mauritanie, la Société des Aéroports de Paris et l’Aéroport de Nice Côte d’Azur.

L’OACA emploie des compétences souvent sollicitées pour des travaux d’assistance et d’échange d’expérience avec d’autres pays de notre continent.

Les associations et les structures qui évoluent au sein de l’OACA, telles que l’Association Tunisienne des Contrôleurs de la Circulation Aérienne, l’Association des Electroniciens de la Sécurité Aérienne, l’Association des retraités de l’Office, l’amicale du personnel ainsi que l’Association Sportive, contribuent à renforcer le rayonnement de l’office à l’échelle internationale par la participation de ces associations et structures à ce niveau à des activités diverses sportives, techniques, sociales [1]....

## 1.2 Contexte du projet

Dans cette partie, nous allons présenter le contexte du projet à savoir la problématique, les objectifs ainsi que les différentes étapes de déroulement du projet.

### 1.2.1 Problématique

Le système d’information de l’OACA représente un actif aussi important que les actifs liés au système de production classique (actifs physiques, actifs humains, actifs financiers, actifs sociaux,...). Il contient des informations très critiques pour le déroulement des activités de l’entreprise. Il est donc essentiel de le protéger contre les intrusions et les accès non autorisés. La sécurité du SI est ainsi un enjeu majeur pour l’OACA ainsi que pour l’ensemble des acteurs qui l’entourent.

## I.1 Cadre du projet

Afin d'assurer la sécurité de son système d'information, l'OACA faisait recours à plusieurs équipements de sécurité informatique à savoir les pare-feu, les IPS, les IDS ...

Nous décrivons dans la figure I.2 l'architecture réseau de cet office :

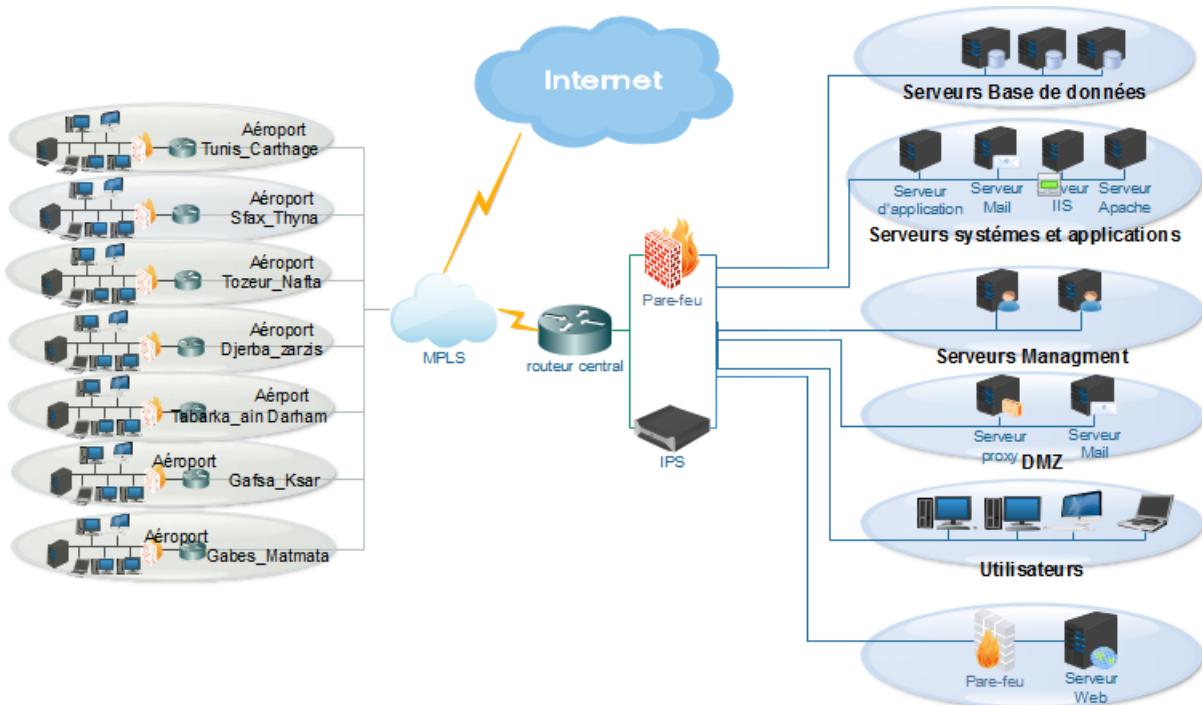


Figure I.2 – Architecture réseau de l'OACA

Le système d'information de l'OACA est réparti entre les sites de l'OACA à Tunis et les différents Aéroports de l'intérieur. L'OACA et ses différentes structures sont interconnectés au moyen de liaisons MultiProtocol Label Switching (MPLS) [2], en plus des liaisons en fibre optique.

L'architecture existante est composée des blocs fonctionnels suivants :

- **Internet** : Module destiné à la connexion Internet pour les utilisateurs de l'OACA,
- **Branches** : Module destiné à la connexion des sites distants et des sites partenaires,
- **CORE** : Module destiné à la sécurité des applications, des bases de données, de la zone de publication web et du management,
- **CAMPUS** : Module destiné à la connexion et le contrôle d'accès des différents profils utilisateur de l'OACA.

Comme représenté dans la figure I.2, le périmètre de protection de l'OACA est composé d'un ensemble de pare-feu et des systèmes de détection / prévention d'intrusion qui ont été considérés comme des solutions de protection efficace contre les menaces réseaux internes et externes.

Cependant, les attaques informatiques deviennent de plus en plus sophistiquées et la sécurité

## I.1 Cadre du projet

---

des Systèmes d'Informations (SI) statique n'est plus suffisante. L'OACA doit donc évoluer vers une sécurité dynamique et intelligente qui se base sur l'analyse de comportement ou sur la corrélation des données. En effet, tous les évènements des systèmes ainsi que les équipements au sein de l'entreprise doivent être sous contrôle et en supervision continue à travers leurs fichiers journaux ou fichier log.

D'où vient le besoin de notre projet qui vise à renforcer la gestion de la sécurité informatique au sein de l'entreprise par la mise à disposition d'un centre de sécurité opérationnelle (SOC) qui permettra de centraliser la gestion et d'avoir une visibilité globale sur la sécurité du SI de l'OACA.

### 1.2.2 Objectifs

Notre projet consiste à concevoir et à déployer un SOC (Security Operations Center) qui s'appuie sur une organisation et un ensemble d'outils performants pour réduire les risques et diminuer au maximum l'indisponibilité des composants critiques du système d'information.

Ce SOC devrait réaliser ce qui suit :

- Centralisation des services de sécurité dans un seul endroit en collectant les événements remontés par les différents équipements de sécurité de l'entreprise,
- Analyse des événements et détection des attaques,
- Prévention du risque,
- Surveillance du comportement des utilisateurs et des équipements en temps réel,
- Gestion des alertes de sécurité,
- Mise en place des procédures à suivre en cas d'émission d'alertes,
- Gestion des rapports et génération de tableau de bord de sécurité,
- Backup régulier des fichiers logs et des données collectées.

### 1.2.3 Planification du déroulement du projet

Dans cette partie, nous allons présenter le planning que nous avons suivi durant la réalisation de notre projet.

Ce projet est établi en sept étapes :

- **Etape 1** : État de l'art et étude de l'existant,
- **Etape 2** : Conception de la plateforme SOC,
- **Etape 3** : Étude théorique de la solution,
- **Etape 4** : Mise en place de la plateforme OSSIM,
- **Etape 5** : Intégration des systèmes externes à la plateforme OSSIM,
- **Etape 6** : Test et Validation de la plateforme,

## I.2 État de l'art : Security Operations Center (SOC)

- **Etape 7** : Rédaction du rapport.

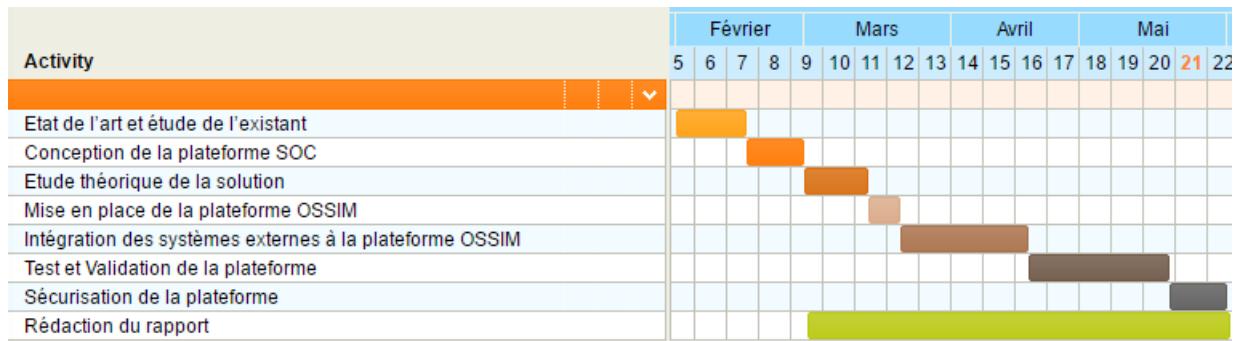
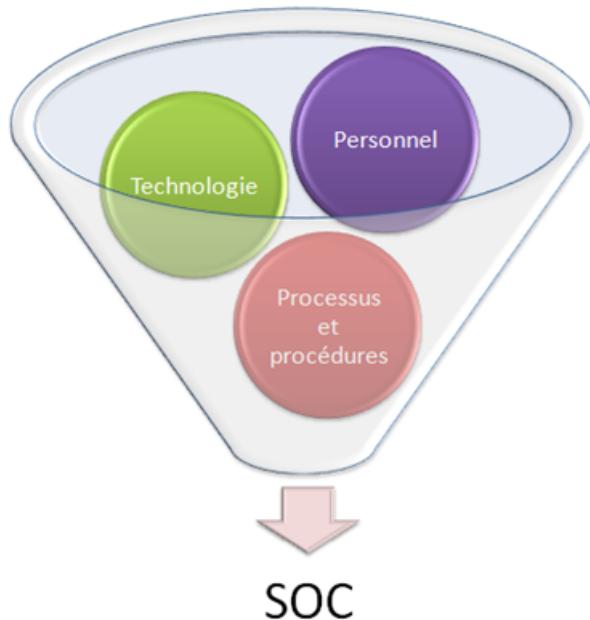


Figure I.3 – Planification du projet

## 2 État de l'art : Security Operations Center (SOC)

Le Security Operations 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) remontés par les composants de sécurité, les analyser, détecter les anomalies et définir des réactions en cas d'émission d'alerte. Comme le montre la figure I.4, la construction d'un SOC nécessite la collaboration et la communication entre trois parties : le personnel, la technologie et les processus et les procédures.

## I.2 État de l'art : Security Operations Center (SOC)



**Figure I.4** – Composantes du SOC

### 2.1 Le personnel

Un SOC exige des professionnels de la sécurité hautement qualifiés pour enquêter sur les incidents de sécurité, effectuer des interventions en cas d'incident, faire de l'investigation et aider à maintenir une organisation à flot en cas de violation des données.

Ces professionnels de la sécurité sont chargés de fournir des informations précises à la direction afin que l'entreprise puisse prendre des décisions judicieuses.

Sans un personnel qualifié aucune technologie ne peut contribuer à construire une structure appropriée et efficace .

Nous devons identifier les compétences actuelles et les compétences requises pour analyser l'exigence et travailler en conséquence pour une meilleure production.

L'étape suivante consiste à déterminer les écarts entre les compétences actuelles et requises du personnel de soutien existant. En outre, l'équipe de soutien devrait recevoir une formation appropriée dans les différents domaines et l'environnement afin qu'ils puissent travailler plus tard dans un environnement vivant.

### 2.2 Les processus et les procédures

Les processus et les procédures au sein d'un SOC définissent clairement les rôles et les responsabilités ainsi que les procédures de suivi. Ces derniers comprennent les processus opéra-

## I.2 État de l'art : Security Operations Center (SOC)

---

tionnels, technologiques, et analytiques. Ils décrivent les mesures à prendre en cas d'alerte ou de violation, y compris les procédures d'escalade, les procédures de notification et les procédures de réponse à la violation.

En général, les SOC devraient s'efforcer de mettre en place les processus de sécurité suivants avant leur démarrage :

- Procédure de surveillance,
- Procédure d'alertes,
- Procédure d'escalade,
- Procédure de mise à jour de la journalisation,
- Procédure d'enregistrement des incidents,
- Surveillance de la conformité,
- Procédure de reporting.

Le plus important est le processus qui lie chaque étape, assurant que la transition de chaque tâche est clairement définie le jour au jour et de personne à personne. C'est pourquoi, en cas d'attaque réelle, tout le monde au sein du SOC connaît sa responsabilité et la façon dont elle s'inscrit dans le processus de bout en bout.

## 2.3 La technologie

Un SOC doit être équipé d'une suite d'outils technologiques qui fournissent la bonne visibilité sur l'environnement de sécurité de l'organisation.

Le SOC est généralement basé sur un système de gestion des informations de sécurité et d'événements (SIEM) qui regroupe et corrèle les données et les événements en relation avec la sécurité.

### 2.3.1 SIEM

Le SIEM est un système de supervision centralisé de la sécurité composé de deux solutions :

- Security Information Management (SIM) : Fourni un moyen de rétention des informations, de support à l'analyse Forensic et de reporting des données de logs,
- Security Event Management (SEM) : Garantit la supervision en temps réels ou quasi, la corrélation et le traitement des événements [3].

Comme le montre la figure I.5, le SIEM prend en entrée les événements et les journaux collectés des équipements du réseau qui peuvent être de différents formats (Syslog, Simple Network Management Protocol (SNMP), fichiers RAW, formats propriétaires, etc.) et crée à la fin des tableaux de bord et des rapports contenant une analyse complète sur tout le système d'information (nombre d'attaque, nombre d'alertes par jour . . . ).

## I.2 État de l'art : Security Operations Center (SOC)

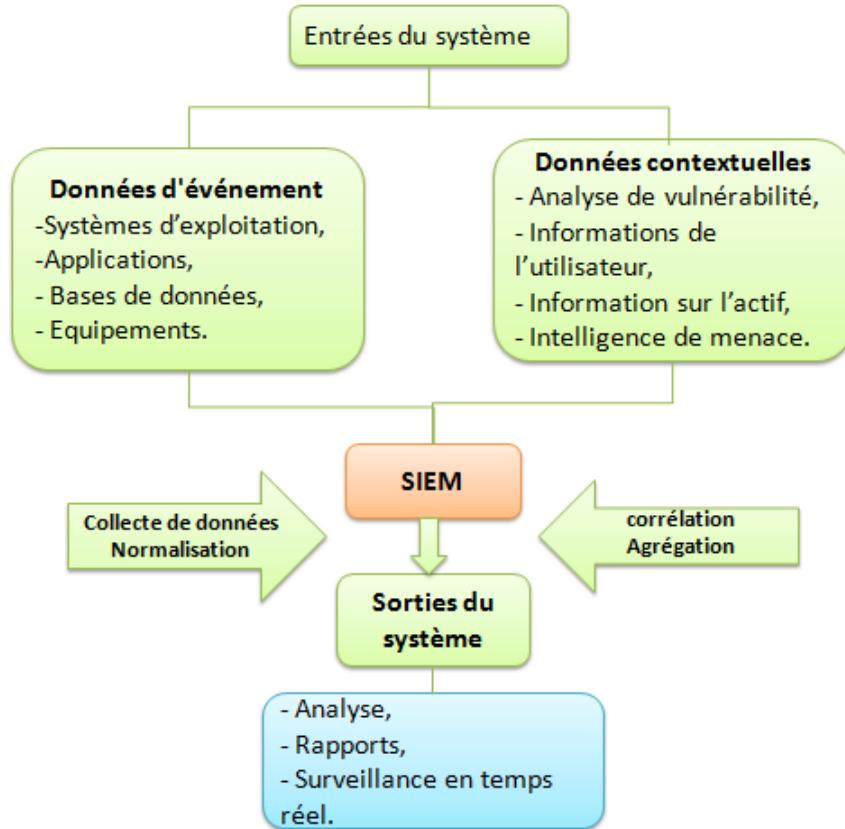


Figure I.5 – Architecture du SIEM

Les principales fonctionnalités proposées par un outil SIEM sont :

- **Collecte des données de contexte et des logs** : Cette fonction consiste à recueillir des logs et des données de contexte, notamment des informations d'identité ou les résultats des analyses de vulnérabilité, à l'aide d'une combinaison de méthodes basées ou non sur agent,
- **Normalisation et catégorisation** : Cette fonction convertit les logs originaux collectés dans un format universel à des fins d'utilisation au sein du produit SIEM. Par ailleurs, les événements sont classés dans des catégories utiles : modifications de la configuration, accès aux fichiers ou encore attaque par surcharge de tampon,
- **Corrélation** : Cette fonction inclut la corrélation algorithmique, statistique ou basée sur des règles ainsi que d'autres méthodes, comme la mise en relation de différents événements entre eux ou la mise en relation d'événements avec des données de contexte. La corrélation peut s'effectuer en temps réel, mais tous les outils ne prennent pas en charge cette fonction. En effet, certains outils se concentrent sur la corrélation des données historiques provenant de leurs bases de données. En outre, d'autres méthodes d'analyse des logs sont parfois incluses dans cette catégorie,

## I.2 État de l'art : Security Operations Center (SOC)

---

- **Notification et alertes** : Cette fonction comprend le déclenchement de notifications ou d'alertes auprès d'opérateurs ou de gestionnaires. Les mécanismes d'alerte courants comprennent les e-mails, les SMS ou même les messages envoyés via le protocole SNMP,
- **Hiérarchisation** : Cette fonction comprend différentes options qui mettent en évidence les événements importants par rapport aux événements de sécurité moins graves. Pour ce faire, il est possible de corrélérer les événements de sécurité avec des données de vulnérabilité ou d'autres informations sur les ressources. Les algorithmes de hiérarchisation utilisent souvent des informations fournies par le log original sur la gravité de l'événement,
- **Vues en temps réel** : Cette fonction comprend des tableaux de bord de monitoring de la sécurité et affiche des opérations à l'usage du personnel. Ainsi, les analystes peuvent voir les informations collectées mais aussi les résultats des corrélations pratiquement en temps réel. Les données historiques et archivées peuvent également être présentées de cette manière,
- **Création de rapports** : La création des rapports standards et planifiés prend en compte toutes les vues historiques des données recueillies par le produit SIEM. Certains produits sont également dotés d'un mécanisme de distribution des rapports aux directeurs informatiques ou au personnel en charge de la sécurité, soit par e-mail soit à l'aide d'un portail Web sécurisé dédié,
- **Workflow des rôles de sécurité** : Cette fonction comprend la gestion des incidents, notamment la création des dossiers et l'organisation de tâches d'enquête, mais aussi la mise en place automatique ou semi-automatique de tâches types dans le cadre d'opérations de sécurité. Certains produits intègrent également des fonctions de collaboration qui permettent à plusieurs analystes de travailler sur la même initiative de réponse en matière de sécurité [4].

### 2.3.2 Étude comparative des solutions SIEM

#### Présentation des solutions SIEM les plus connues du marché

- **IBM QRadar SIEM** : IBM QRadar SIEM consolide les données d'événements de journaux et de flux réseau à partir des milliers de terminaux et d'applications distribués sur l'ensemble d'un réseau. Il normalise et met en corrélation des données brutes pour identifier des infractions à la sécurité. IBM QRadar SIEM peut aussi mettre en corrélation les vulnérabilités systèmes avec des données réseau et d'événements, afin d'aider à prioriser les incidents de sécurité [5].
- **SPLUNK** : Splunk est développé par l'entreprise du même nom, fondée en 2003. Il

## I.2 État de l'art : Security Operations Center (SOC)

---

fournit la gestion des journaux, la recherche, l'alerte, la corrélation en temps réel et un langage de requête qui prend en charge la visualisation. Cette solution offre une version gratuite et une version professionnelle (payante). Son utilisation est gratuite pour des petites quantités de données (jusqu'à 500 Mo par jour). Le prix de la version payante dépend des giga-octets de données traitées par jour [6].

- **LogRhythm** : LogRhythm vend ses solutions SIEM aux moyennes et grandes entreprises. Le SIEM de LogRhythm peut être déployé comme un appareil, un logiciel ou des instances virtuelles et prend en charge une architecture décentralisée évolutive N-tier, composée du gestionnaire de plate-forme, du moteur d'alimentation, des processeurs de données, des indexateurs de données et des collecteurs de données. LogRhythm combine les fonctionnalités d'événements, de points d'extrémité et de surveillance de réseau, un workflow intégré de réponse aux incidents et des capacités de réponse automatisée [7].
- **Intel Security** : McAfee Enterprise Security Manager (ESM) d'Intel Security est disponible en tant qu'appareil physique, virtuel ou logiciel. Les capacités Core SIEM sont livrées avec ESM, l'Event Receiver et Enterprise Log Manager. Les composants facultatifs incluent le moteur de corrélation avancé , le moniteur d'événement de base de données et le moniteur de données d'application. McAfee ESM fournit en outre des intégrations à l'Advanced Threat Defense (ATD) de McAfee, à une solution de surveillance de réseau et de stockage en réseau, et à la Threat Intelligence Exchange, un cadre pour la défense de sécurité intra-opératoire en permettant aux technologies de sécurité de détecter et de bloquer collectivement les menaces [7].
- **Hewlett Packard Enterprise (HPE)** : C'est l'un des plus anciens systèmes SIEM du marché. L'entreprise offre deux versions de la solution : Enterprise Security Manager pour les déploiements à grande échelle, et ArcSight Express, un appareil pour le marché intermédiaire. La licence est basée sur l'utilisation de giga-octets par jour [8].
- **Alienvault** : La solution de la gestion de la sécurité d'AlienVault fournit un lieu centralisé pour la configuration et la gestion de ses composants : SIEM, évaluation de la vulnérabilité, découverte d'actifs, détection d'intrusion réseau et hôte et surveillance de l'intégrité des fichiers. AlienVault peut également fournir des informations sur les menaces grâce à sa communauté Open Threat Exchange et Threat Intelligence.

AlienVault offre deux produits de SIEM :

**Open Source Security Information Management (OSSIM)** : C'est une plate-forme open source de gestion de la sécurité qui a été disponible depuis 2003. Ce projet, en amélioration continue, se distingue par la compatibilité totale avec les outils open source qui peuvent être déjà déployés dans le réseau à contrôler. Etant une solution logicielle, OSSIM peut être déployée dans une architecture tout-en-un ou dans une ar-

## I.2 État de l'art : Security Operations Center (SOC)

---

chitecture distribuée selon les besoins de l'entreprise [9].

**Unified Security Management (USM)** : En 2010, AlienVault décide de lancer son produit SIEM commercial basé sur le projet OSSIM. USM est constitué de composants propriétaires et open source. AlienVault intègre OSSIM dans sa solution SIEM, en l'étendant à des améliorations de performance d'administration des réseaux. Cette solution est recommandée surtout pour les entreprises qui cherchent une solution commerciale basée sur des produits open source [10].

### Classement Gartner :

Gartner Inc. est une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées. Elle mène des recherches, fournit des services de consultation, tient à jour différentes statistiques et maintient un service de nouvelles spécialisées [11].

**Le Quadrant Magique du Gartner** : Gartner classe les fournisseurs selon deux critères :

- **L'intégralité de la vision (completeness of vision)** : Représente l'innovation du vendeur, si le vendeur conduit ou suit le marché, et si la vue du fournisseur de la manière dont le marché va se développer correspond aux perspectives de Gartner,
- **La capacité d'exécution (ability to execute)** : Résume des facteurs tels que la viabilité financière du fournisseur, la réactivité du marché, le développement de produits, les canaux de vente et de la clientèle.

En utilisant une méthodologie que Gartner ne divulgue pas, les scores de composants donnent lieu à une position de vendeur dans l'un des quatre quadrants :

- **Les dirigeants (leaders)** : Les vendeurs dans ce quadrant ont les scores composites les plus élevés pour leur exhaustivité de la vision et leur capacité à exécuter. Ils ont la capacité de marché, la crédibilité et les capacités de marketing et de vente nécessaires pour accepter les nouvelles technologies. En outre, ils sont présents dans les cinq principales régions géographiques, une performance financière cohérente et un large soutien de la plate-forme,
- **Challengers** : Un fournisseur du quadrant de Challengers participe au marché et s'exécute assez bien pour constituer une grave menace pour les vendeurs dans le quadrant Leaders. Ils ont des produits solides, ainsi qu'une position et des ressources de marché suffisamment crédibles pour soutenir une croissance continue,
- **Visionnaires (visionaries)** : Un fournisseur du quadrant Visionnaires propose des produits innovants qui abordent des problèmes d'utilisateurs finaux opérationnellement ou financièrement importants à grande échelle, mais n'ont pas encore démontré la capacité de capturer des parts de marché ou une rentabilité durable,

## I.2 État de l'art : Security Operations Center (SOC)

- **Acteurs de niche (niche players) :** Ce quadrant inclut des fournisseurs qui adaptent leurs produits existants pour entrer sur le marché considéré, ou des fournisseurs qui ont du mal à développer et à exécuter leur vision.

Dans le domaine des SIEM, Gartner publie un rapport annuel sur les parts du marché de chaque produit ainsi que les caractéristiques techniques et les informations relatives qui peuvent influencer le choix de la solution.

Nous nous intéressons dans ce qui suit au dernier rapport publié par Gartner, celui de août 2016 [12] :



**Figure I.6 – Gartner Magic Quadrant pour le SIEM**

Le marché SIEM est relativement mature. Il a été dominé par quelques grands fournisseurs : HPE, IBM, Intel et Splunk qui commandent plus de 60% des revenus du marché, qui ont augmenté de 4% pour environ 1,73 milliard de dollars en 2015, selon Gartner [9]. Dans cet esprit, il n'est pas surprenant que, comme l'année dernière, Gartner a nommé IBM, HPE, Splunk, Intel

## I.2 État de l'art : Security Operations Center (SOC)

---

Security et LogRhythm en tant que cinq leaders dans SIEM, avec quelques légères variations de positionnement parmi eux.

IBM et Splunk demeurent relativement inchangés dans leur positionnement, tandis que LogRhythm a réalisé des gains considérables dans la "capacité d'exécution" et "l'exhaustivité de la vision", poussant le fournisseur dans la troisième place sur le graphique. Pendant ce temps, HPE et Intel se glissent tous deux sur les autres leaders, avec des pertes notables tant dans la "capacité à exécuter" que dans "l'exhaustivité de la vision".

Nous remarquons qu'il existe plusieurs solutions qui sont assez matures et performantes, cependant ces dernières sont trop coûteuses. Donc, nous allons faire une étude comparative des différentes solutions SIEM open source les plus connus. Cette comparaison est présentée dans le tableau I.1.

Les solutions que nous allons comparer sont les suivantes :

- **Elasticsearch, Logstash et Kibana (ELK)** : Il s'agit de coupler les 3 logiciels pour obtenir une solution d'analyse de log performante et complète [13] :
  - ElasticSearch : moteur de stockage et d'indexation de documents et moteur de requête/d'analyse de ces documents,
  - Logstash : analyse, filtrage et découpage des logs pour les transformer en documents, parfaitement formatés notamment pour ElasticSearch,
  - Kibana : dashboard interactif et paramétrable permettant de visualiser les données stockées dans ElasticSearch.
- **Enterprise Log Search and Archive (ELSA)** : Il s'agit d'un récepteur de log, un archiveur, un indexeur et un serveur Web de trois niveaux pour le syslog entrant. Il exploite l'analyseur pattern-db de syslog-ng pour une normalisation de journal efficace et l'indexation de texte intégral Sphinx pour la recherche de journaux. L'authentification et l'autorisation peuvent être basées sur LDAP (Lightweight Directory Access Protocol est un protocole permettant l'interrogation et la modification des services d'annuaire), mais l'utilisateur doit spécifier la configuration des groupes et des filtres de recherche [14].
- **Graylog** : Graylog est une solution open-source de gestion de logs. Chaque message est enregistré dans une base de données Elasticsearch et une interface web permet de gérer et analyser les logs.

Graylog est découpé en 2 parties : graylog-server et graylog-web-interface. La première est une application Java qui accepte les messages sur différents protocoles : User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Graylog Extended Log Format (GELF), Advanced Message Queuing Protocol (AMQP), ... Chaque message

## I.2 État de l'art : Security Operations Center (SOC)

---

est analysé puis enregistré dans la base Elasticsearch. Une API Rest est également intégrée à l'outil et est notamment utilisée par la partie web-interface. Celle-ci permet de gérer des utilisateurs, des streams et des dashboard [15]

- **OSSIM** : OSSIM est un gestionnaire d'information de sécurité basé sur des technologies open source. Son objectif est de centraliser et d'analyser l'information de sécurité, venant de différentes sources d'outils open source, 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. Il permet de fiabiliser les alertes et donc d'éviter un maximum de faux positifs (ou encore une fausse alarme, c'est un résultat d'une prise de décision à deux choix, déclaré positif, là où il est en réalité négatif) grâce à la corrélation des événements [9].

## I.2 État de l'art : Security Operations Center (SOC)

Tableau I.1 – Comparaison des solutions SIEM open source

	Support Windows	Support Linux	Intégration de "Active Directory"	Contrôle d'accès à base de rôles	Corrélation des logs	HIDS	NIDS	Recherche en temps réel	Threat intelligence	Rapports de conformité	Soutien communautaire
ELK	Oui	Oui	Non	Non	Oui	Non	Non	Oui	Non	Non	Oui
ELSA	Oui	Oui	Ldap	Oui	Oui	Non	Non	Oui	Non	Non	Non
Graylog	Oui	Oui	Ldap	Oui	Oui	Non	Non	Oui	Non	Non	Oui
OSSIM	Oui	Oui	Ldap	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

## **I.2 État de l'art : Security Operations Center (SOC)**

---

### **Conclusion**

Durant ce chapitre, nous avons présenté le cadre général du projet, le concept de SOC et ses différentes composantes.

Après avoir présenté les solutions SIEM et leur importance dans la gestion de sécurité du réseau, nous avons réalisé une étude comparative des différentes solutions SIEM présentes sur le marché en se référant au classement de Gartner de l'année de 2016.

Nous avons conclu ce chapitre par un tableau comparatif des solutions SIEM open source les plus connues sur le marché.

Dans le chapitre suivant, nous allons spécifier les besoins de l'entreprise afin de choisir la meilleure solution parmi celles étudiées.

---

---

# Chapitre II

---

## Spécification des besoins et étude théorique

### Plan

<b>1</b>	<b>Spécification des besoins</b>	<b>20</b>
1.1	Besoins fonctionnels	20
1.2	Besoins non fonctionnels	22
1.3	Topologie réseau	22
<b>2</b>	<b>Étude théorique</b>	<b>23</b>
2.1	Choix de la solution SIEM	23
2.2	Staff SOC	26
2.3	Procédure de gestion des incidents	28

## Introduction

Après avoir présenté l'importance de la mise en place d'un SOC au sein de l'entreprise moderne, et après avoir étudié les différentes solutions existantes sur le marché, nous étudions maintenant les besoins de l'entreprise pour pouvoir choisir la solution convenable qui pourra lui assurer les fonctionnalités voulues et élever le niveau de sécurité de son infrastructure réseau.

## 1 Spécification des besoins

Dans cette partie, nous allons spécifier les besoins fonctionnels et non fonctionnels de l'OACA ainsi que la topologie réseau à superviser.

### 1.1 Besoins fonctionnels

L'OACA a besoin de concevoir et de mettre en place un SOC qui doit répondre à ses besoins de sécurité. Ces besoins sont de nature technologique et organisationnelle.

Sur le plan technologique, l'entreprise a besoin de centraliser les logs de ses différents équipements réseaux et de sécurité, les normaliser, les analyser et les corrélérer entre eux en s'appuyant

## II.1 Spécification des besoins

---

sur une solution SIEM open source.

Les fonctionnalités principales que doit assurer notre solution SIEM pour répondre aux besoins de l'entreprise sont les suivantes :

- **Collecte de logs des équipements hétérogènes** : Une liste de quelques équipements sera fournie ultérieurement. La solution proposée doit supporter tout ajout supplémentaire d'une nouvelle source de logs. Les sources de logs peuvent être des équipements de sécurité, des bases de données, des équipements réseaux ou des applications développées en interne... ,
- **Stockage de données** : il est primordial pour l'OACA d'enregistrer les informations journalisées par les postes de travail, les serveurs, les équipements réseaux et les applications spécifiques. Il est exigé que la solution embarque un mécanisme de rotation de logs pour garantir la compression des fichiers logs et pour éviter l'augmentation de taille de ces fichiers,
- **Génération des alertes** : la solution doit inclure un moteur de corrélation basé sur la définition de règles et de différents scénarios. Le système doit permettre à l'administrateur la définition de nouvelles règles/scénarios de corrélation. En résultat d'une règle de corrélation, la solution doit permettre : la génération d'une alerte, l'envoi d'un e-mail automatisé vers un ou plusieurs destinataires ou l'exécution d'une tâche ou d'un script,
- **Génération des tableaux de bord** : le système doit disposer d'un tableau de bord en temps réel permettant de superviser le statut de réception des logs pour toutes les sources et de suivre de l'utilisation des ressources systèmes de la solution,
- **Génération des rapports** : le système mis en place doit permettre de générer des rapports. Ces rapports devront pouvoir être envoyés par email. Le système doit permettre aussi une exportation manuelle ou automatique de ces rapports.

Sur le plan organisationnel, l'OACA a besoin de mettre en place une équipe dédiée et fixer ses objectifs. Le but est de lister les compétences de chacun des membres de l'équipe et de les comparer par rapport aux objectifs fixés. Cette étape permet de mettre en place un plan de formation pour l'équipe. Avoir des équipes informées des dernières nouveautés et dotées d'une compétence technique adéquate est en effet primordial. Une veille interne et des sessions de formation régulières sont donc à prévoir.

L'OACA a besoin aussi de définir un process de gestion des incidents. Ce dernier doit comprendre 3 phases principales : identification de l'incident, réponse en fonction du niveau de criticité et rétablissement du réseau à un niveau normal.

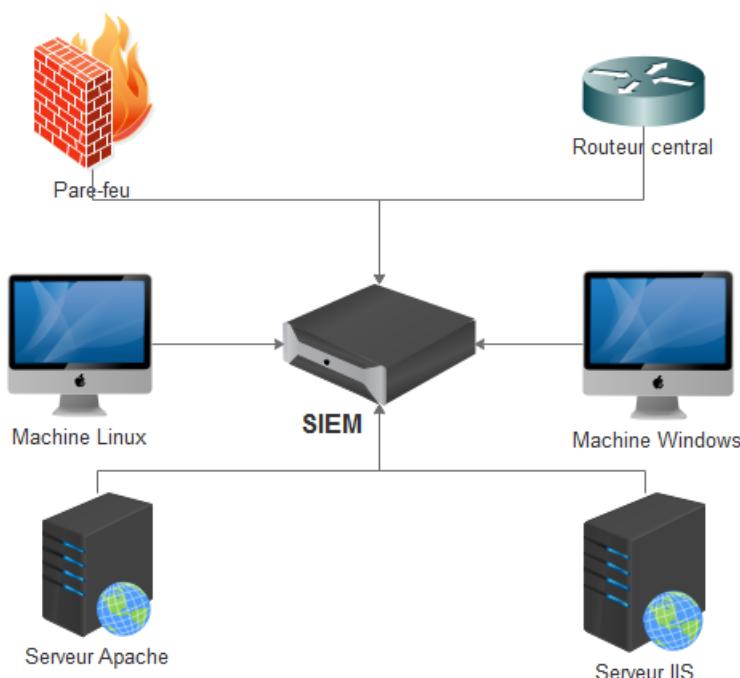
### 1.2 Besoins non fonctionnels

Afin d'offrir une solution complète et performante à différents niveaux, notre plateforme doit couvrir les besoins non fonctionnels suivants :

- **Ergonomie des tableaux de bord** : les tableaux de bord doivent permettre à l'utilisateur de trouver rapidement l'information dont il a besoin et lui donner la possibilité de faire des recherches personnalisées.
- **Sécurité** : la plateforme à mettre en place va contenir des informations sensibles sur l'activité de l'entreprise. De ce fait, il faut assurer la sécurité de ces informations à différents niveaux : l'accès à la plateforme doit se faire via le protocole "https", tout utilisateur doit s'authentifier avant d'accéder à la solution, il faut définir les informations que chaque utilisateur a le droit de consulter.
- **Flexibilité** : La possibilité d'intégrer tout type d'équipement réseau.

### 1.3 Topologie réseau

Dans cette partie nous allons spécifier les différents équipements à inclure dans notre SOC comme spécifié par la figure II.1



**Figure II.1** – Topologie réseau à intégrer dans le SOC

Notre SOC inclut ainsi :

- **Un serveur Web Apache et un serveur web Internet Information Services (IIS)** : les serveurs web sont des logiciels permettant aux employés au sein de l’OACA d'accéder à des pages web stockées dans des serveurs.  
Tout accès à un serveur web ainsi que toute modification dans les fichiers de config du serveur sera enregistré. Toute tentative d'attaque ou détection d'anomalie dans le service web doit être enregistrée. Pour chaque connexion, les serveurs Web enregistrent les informations suivantes : l'adresse Internet Protocol (IP) demandant l'accès au site, les différentes données d'authentification dans le cas d'un accès authentifié, la page demandée, les liens consultés, les informations fournies par le client, le type de la requête (GET, POST), la date et l'heure de l'accès,
- **Deux postes de travail utilisateurs** : nous optons pour l'enregistrement de toute tentative d'ouverture de session ou d'augmentation de privilèges. Toute modification des paramètres de l'hôte doit être aussi enregistrée ainsi que la modification des fichiers système,
- **Des équipements réseaux** : ces équipements sont un pare-feu CISCO-Asa et un routeur CISCO. Il est impératif de collecter les données internes à l'équipement et les paquets qui le traversent. Les informations suivantes doivent être collectées : les adresses IP source et destination, les numéros de port source et destination ainsi que les protocoles utilisés, la date et l'heure de la tentative, le service offert par l'équipement, le nombre de paquets traités et les messages d'alerte s'ils existent.

## 2 Étude théorique

Dans cette section, nous allons choisir et argumenter notre choix de la solution SIEM à mettre en place, nous allons définir un staff SOC selon les besoins de l'entreprise et finalement nous mettons en place une procédure à suivre en cas d'incident.

### 2.1 Choix de la solution SIEM

Comme nous avons vu dans le chapitre précédent, les produits commerciaux SIEM offrent des fonctionnalités robustes, y compris le support pour le traitement de diverses sources de journaux et d'événements, des données de signatures d'alerte et de menace mises à jour régulièrement et des rapports pour la conformité à de multiples normes. Cependant, ces solutions ont des coûts très élevés.

La principale contrainte pour la sélection de la solution SIEM pour l’OACA est le coût du

produit, ce qui a immédiatement éliminé toutes les solutions commerciales dignes.

Après l'élimination des options commerciales, nous avons réduit notre champ de sélection aux solutions axées sur la corrélation des données, avec des capacités de reporting et d'alerte avancées. De plus, nous avons considéré les solutions open source qui avaient des communautés actives de développement et de soutien et la capacité à ingérer des données provenant de sources multiples.

Après avoir examiné plusieurs options pouvant prendre en charge la journalisation, la génération de rapports et l'évolutivité souhaitée, la solution OSSIM d'AlienVault a dépassé le reste. OSSIM est la meilleure solution pour un SIEM Open Source capable de répondre aux besoins immédiats et à long terme de notre entreprise.

En effet, OSSIM existe depuis plusieurs années et a une communauté de soutien très active. En outre, OSSIM dispose d'une prise en charge de l'extension externe ainsi que de l'option de mise à niveau vers le SIEM commercial d'AlienVault (USM).

De plus, contrairement aux solutions log-only telles que Graylog et ELSA, OSSIM a une corrélation intégrée avec des flux de menaces ainsi que des données IDS basées sur le réseau et l'hôte qui nous permettront d'intégrer et de corrélérer davantage d'événements à l'avenir. Ces capacités étendues d'OSSIM permettront à l'OACA d'acquérir une meilleure compréhension des risques et des événements liés à la sécurité dans son environnement.

### 2.1.1 Présentation générale de la solution choisie

OSSIM est un projet open source de gestion de la sécurité de l'information. Cette solution s'appuie sur une gestion des logs basée sur la corrélation de ceux-ci ainsi qu'une notion d'évaluation des risques.

OSSIM est un projet axé essentiellement sur l'intégration d'outils puissants en matière de sécurité. Afin de les faire fonctionner ensemble, un collecteur, un moteur de corrélation, et plusieurs outils de gestion de rapports sont développés permettant la collecte, la normalisation et le traitement des informations à partir d'une console unique.

### 2.1.2 Architecture

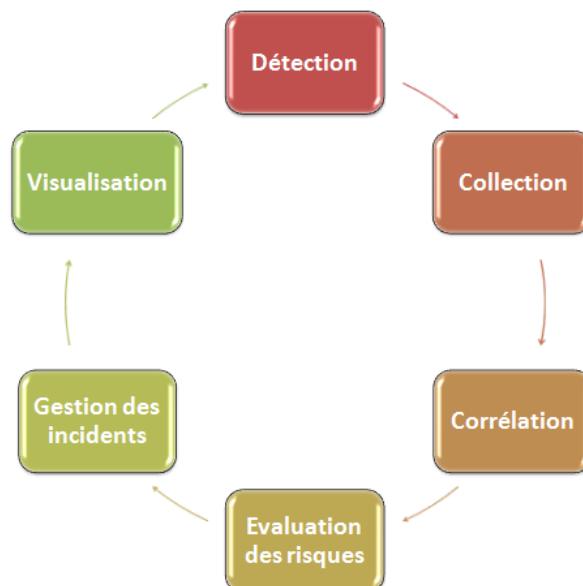
L'architecture d'OSSIM est axée autour de quatre éléments principaux qui peuvent être installés séparément ou dans une seule machine [16] :

- **La sonde d'OSSIM** : elle recueille et normalise les événements générés par les différents équipements de sécurité. Nous pouvons déployer autant de sondes dans une même architecture s'il est nécessaire,

- **Le serveur d’OSSIM :** Il reçoit les évènements à partir des différentes sondes pour évaluer les risques et corréler les évènements de différentes sources,
- **La base de données d’OSSIM :** C'est une base de données MySQL qui contient les événements, les configurations et des informations utiles,
- **Framework d’OSSIM :** elle est codé en Hypertext Preprocessor (PHP) / Python et permet d'afficher les informations sur le web front-end.

### 2.1.3 Fonctionnalités d’OSSIM

La figure II.2 permet de décrire le processus de fonctionnement d’OSSIM de la récupération des événements par ses capteurs jusqu'à la sortie finale sur son interface graphique web.



**Figure II.2** – Fonctionnement d’OSSIM

- **Détection :** Un détecteur est défini comme étant un programme qui écoute sur le réseau, surveille les sockets ou les journaux à la recherche de signes d'attaques, et émet des alertes en conséquence. Il existe essentiellement deux types de détecteurs : les détecteurs à base de modèles et les détecteurs à base d'anomalies :
  - Les détecteurs à base de modèles disposant des signatures et des règles pour identifier les comportements interdits,
  - Les détecteurs à base d'anomalies qui disposent d'une base de signatures des activités permises génèrent des alertes dans le cas d'activités non correspondantes à cette base,
- **Collecte :** La collecte a pour but de centraliser tous les événements normalisés en un format unique pour permettre un traitement ultérieur par le serveur d’OSSIM,

- **Corrélation :** Le rôle du moteur de corrélation est de réduire le taux de faux positifs et d'éviter les faux négatifs. Pour ce faire, OSSIM effectue deux types de corrélations :
  - La corrélation logique (Logical-Correlation) qui se base sur la vérification des caractéristiques de l'événement avec les règles déjà prédéfinies ou les règles personnalisées et ajoutées par l'utilisateur,
  - La corrélation croisée (Cross-Correlation) est la comparaison des informations recueillies par les détecteurs et les scanner de vulnérabilités pour décider de l'importance de l'évènement.
- **Évaluation des Risques :** C'est le processus de mesure des risques qui vise à déterminer l'ordre d'importance d'un évènement donné. Cette évaluation représente une étape nécessaire pour le processus de prise de décision. OSSIM calcule un paramètre de risque pour chaque événement sur la base des trois paramètres suivants :
  - La priorité de l'événement (Priority) qui varie entre 0 et 5. Par défaut, elle vaut 1,
  - La fiabilité de l'événement (Reliability) qui varie entre 0 et 10. Par défaut, elle vaut 1,
  - La valeur associée à l'hôte (Asset Value) qui a généré l'événement. Cette valeur est entre 0 et 5. Par défaut, elle est mise à 1.

Le risque est calculé alors selon la formule suivante :

$$Risque = \frac{(Priorité \times Fiabilité \times Valeur Hôte)}{25}$$

Pour une valeur supérieure ou égale à 1, ce résultat entraîne la génération d'une alerte. Il est à noter que ces valeurs peuvent être associées par l'utilisateur en fonction de ses besoins,

- **Gestion des Incidents :** Une fois qu'une attaque est détectée, recueillie, évaluée et validée, un ticket peut être généré pour suivre l'incident. Les tickets sont générés à partir du tableau de bord. Chaque ticket contient des informations sur le propriétaire de l'incident, les événements contenus dans l'incident, l'état actuel de l'incident, et l'historique de l'incident,
- **Visualisation :** Les tableaux de bord sont prévus pour présenter visuellement les données d'une manière facile à utiliser. Chaque analyste peut sélectionner et travailler avec les tableaux de bord qui lui permettront de remplir les tâches requises d'une manière plus efficace.

## 2.2 Staff SOC

Le tableau II.1 énumère les différents membres de Staff SOC en précisant leurs fonctions ainsi que les différentes formations requises pour chaque membre.

## II.2 Étude théorique

Tableau II.1 – Membres du staff SOC

Poste	Fonctions	Formations requises
Analyste d'alerte	Surveillance de la file d'attente d'alerte, triage des alertes de sécurité, surveillance des capteurs de sécurité et des points de terminaison et collecte des données nécessaires pour lancer le travail du répondeur d'incident.	Procédures de triage d'alerte, détection d'intrusion, SIEM, formation d'investigation et d'autres formations spécifiques aux outils. Les certifications pourraient inclure :SANS SEC401 : Security Essentials Bootcamp Style [17]
Répondeur d'incident	Effectue une analyse profonde des incidents en corrélant les données de diverses sources, détermine si un système critique ou un ensemble de données a été affecté, conseille sur l'assainissement, fournit un support pour de nouvelles méthodes pour détecter les menaces.	Procédures d'intervention en cas d'incident, examens des journaux, évaluation des logiciels malveillants, analyse de la criminalistique et intelligence des menaces. Les certifications pourraient inclure SANS SEC501 : Advanced Security Essentials - Enterprise Defender[18], SANS SEC503 : Intrusion detection in-depth[19], SANS SEC504 : Hacker Tools, Techniques, Exploits, and Incident Handling[20]
Expert en la matière	Possède une connaissance approfondie des réseaux, des terminaux, de l'intelligence des menaces, de la médecine légale (forensics) et de l'ingénierie inverse des logiciels malveillants. Il agit comme un "chasseur" d'incidents, étroitement impliqué dans le développement, le réglage et la mise en œuvre des analyses de détection des menaces.	Formation avancée sur la détection d'anomalie, formation spécifique aux outils pour l'agrégation et l'analyse des données et l'intelligence des menaces. Les certifications pourraient inclure : SANS SEC503 : Intrusion Detection In-Depth, SANS SEC504 : Hacker Tools, Techniques, Exploits and Incident Handling, SANS SEC561 : Intense Hands-on Pen Testing Skill Development[21], SANS FOR610 : Reverse-Engineering Malware : Malware Analysis Tools and Techniques[22]
Gestionnaire de SOC	Gère le personnel, le budget, la planification des horaires de travail et la stratégie technologique afin de respecter les accords de niveau de service, communique avec la direction, fournit une orientation générale pour le SOC et la contribution à la stratégie globale de sécurité.	Gestion de projet, gestion de la réponse aux incidents, compétences générales en gestion des personnes. Les certifications comprennent : Certified Information Systems Security Professional (CISSP) [23], Certified Information Systems Auditor (CISA) [24], Certified Information Security Manager (CISM) [25], Certified in the Governance of Enterprise IT (CGEIT) [26]

Le gestionnaire de SOC devrait élaborer un modèle de workflow et mettre en œuvre des procédures opérationnelles normalisées pour le processus de traitement des incidents qui guide les analystes à travers le triage et les procédures de réponse.

### 2.3 Procédure de gestion des incidents

Afin de bien gérer un incident au sein de l'entreprise, il faut définir un processus bien précis en suivant les bonnes pratiques. Notre processus de réponse aux incidents contient plusieurs phases.

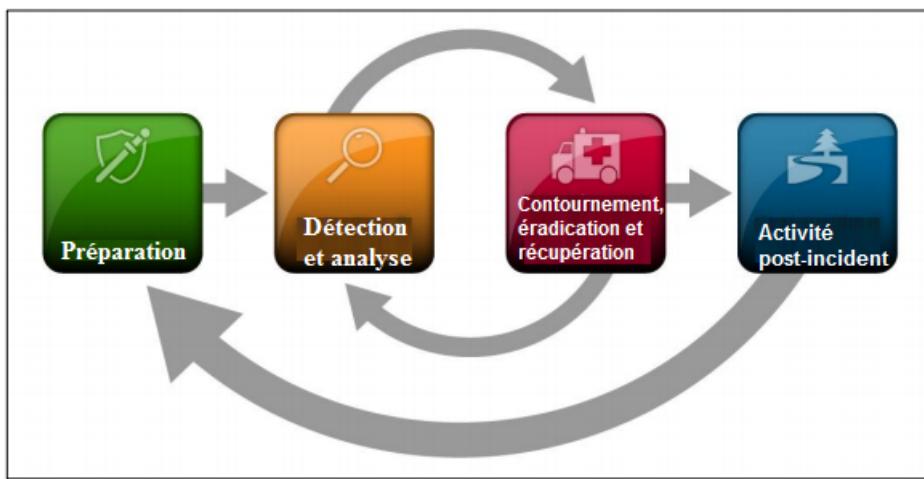
La phase initiale implique l'établissement et la formation d'une équipe de réponse aux incidents et à l'acquisition des outils et des ressources nécessaires. Au cours de la préparation, l'organisation tente également de limiter le nombre d'incidents qui se produiront en sélectionnant et en mettant en œuvre un ensemble de contrôles en fonction des résultats des évaluations des risques. Cependant, le risque résiduel persistera inévitablement après la mise en œuvre des contrôles. La détection de violations de sécurité est donc nécessaire pour alerter l'organisation chaque fois que des incidents se produisent. Conformément à la gravité de l'incident, l'organisation peut atténuer l'impact de l'incident en la contenant et en récupérant finalement.

Au cours de cette phase, l'activité revient souvent à la détection et à l'analyse, par exemple, pour voir si d'autres hôtes sont infectés par des logiciels malveillants tout en éradiquant un incident de malware.

Une fois que l'incident a été traité correctement, l'organisation émet un rapport qui détaille la cause et le coût de l'incident et les étapes que l'organisation doit prendre pour prévenir les incidents futurs.

Maintenant nous allons détailler les phases principales du processus de réponse aux incidents qui sont : "la préparation", "la détection et l'analyse", "le contournement, l'éradication et la récupération" et "l'activité post-incident".

La figure II.3 illustre le cycle de vie de la réponse aux incidents [27].



**Figure II.3** – Cycle de vie de la réponse aux incidents

### 2.3.1 La phase de préparation

Cette phase, comme son nom l'indique, implique la préparation d'une équipe pour être prête à traiter un incident à tout moment. C'est la phase la plus cruciale par rapport à toutes les autres, car elle déterminera à quel point notre équipe sera en mesure de répondre en cas de crise. Il existe plusieurs éléments clés à mettre en œuvre dans cette phase afin d'atténuer les problèmes potentiels qui peuvent entraver la capacité de gérer un incident. Ces éléments sont :

- **Une politique :**

C'est l'un des éléments clés qui fournissent des indications pour savoir si un incident s'est produit dans l'entreprise. Une bannière de connexion peut être une façon de s'assurer que les personnes qui tentent de se connecter au réseau de l'organisation seront conscientes de ce qui est prévu lors de l'utilisation des ressources d'information de l'organisation. Par exemple, la bannière de connexion peut indiquer que toutes les activités seront surveillées et que les utilisateurs non autorisés peuvent avoir des sanctions civiles ou pénales, etc. Sans politiques claires, nous pouvons laisser notre organisation légalement vulnérable aux lois,

- **Un plan ou une stratégie d'intervention :**

Après avoir établi des politiques organisationnelles, il faut créer un plan ou une stratégie pour gérer les incidents. La priorisation des incidents devrait être basée sur l'impact organisationnel, par exemple, une station de travail unique non fonctionnelle peut être considérée comme mineure, alors qu'un serveur en panne pourrait être considéré comme un impact modéré et les données sont volées directement à partir de ressources humaines qui contiennent des informations privilégiées aussi élevées. La priorisation des types

## II.2 Étude théorique

---

d'incidents en fonction de l'impact organisationnel peut aider à construire le cas pour recevoir un buy-in de gestion, car sans soutien de la direction, il est probable que l'équipe d'intervention ne reçoive pas les ressources nécessaires pour gérer correctement une crise,

— **Un plan de communication :**

Il est nécessaire de disposer d'un plan de communication, en raison du fait qu'il peut être nécessaire de contacter des personnes spécifiques lors d'un incident.

En n'ayant pas de plan de communication, il est probable que le temps de réponse sera retardé ou que des personnes non concernées seraient contactées et que l'on n'aurait pas les ressources nécessaires pour atténuer le problème.

On cite quelques exemples de mécanismes qui doivent être mis en place :

- Mécanismes de déclaration des incidents : tels que les numéros de téléphone, les adresses électroniques, les formulaires en ligne et les systèmes de messagerie instantanée sécurisés que les employés peuvent utiliser pour signaler les incidents suspects,
- Système de suivi des problèmes pour le suivi de l'information sur les incidents, le statut etc,
- Les Smartphones doivent être pris en charge par les membres de l'équipe de gestion des incidents pour le soutien hors-heures et les communications sur site,
- Logiciel de cryptage utilisé pour les communications entre les membres de l'équipe, au sein de l'entreprise et avec les parties externes,

— **Des outils :**

Il est fortement recommandé d'avoir tout logiciel et matériel disponibles qui peuvent être facilement utilisés lors d'un incident. Cela peut aller de logiciels anti-malveillants aux ordinateurs portables avec des sniffers de paquets, des servomoteurs et d'autres outils, ainsi que des listes de contrôle de réponse aux incidents et d'autres éléments qui seraient utiles,

— **Des formations :**

Cet élément est primordial, car sans cela, l'équipe pourrait être mal préparée et entraîne un échec complet de la gestion d'un incident malgré une bonne planification. Il est recommandé de faire des exercices à intervalles réguliers pour s'assurer que chaque personne de l'équipe est en mesure et sait comment s'acquitter de ses tâches pendant un incident.

### 2.3.2 La phase de la détection et d'analyse

C'est l'étape où nous déterminons si un incident s'est produit. Sur la base de l'observation des événements, des indicateurs, nous recherchons des écarts par rapport aux opérations nor-

males. Nous recherchons des actes malveillants ou des tentatives de faire du mal. Le mécanisme de sécurité en place nous aidera à faire l'identification. L'équipe de traitement des incidents utilisera leur expérience pour examiner les signes et les indicateurs. L'observation pourrait se produire au niveau du réseau, au niveau de l'hôte ou au niveau du système. C'est là que nous exploitons les alertes et les journaux de nos routeurs, pare-feux, IDS, SIEM, passerelles AV, système d'exploitation, flux de réseau, etc.

Après avoir identifié un incident, nous devons évaluer l'impact et notifier les personnes appropriées ou les parties externes. S'il y a des raisons de croire que nous engagerons l'application de la loi, c'est là que nous assurons la chaîne de garde. C'est aussi à ce stade que nous définissons les prochaines étapes, telles que le confinement.

### 2.3.3 La phase de contournement, éradication et récupération

#### — Contournement :

Le but principal de cette phase est de limiter les dégâts et de prévenir tout nouveau dommage. Il y a plusieurs étapes dans cette phase. Chacune de ces étapes nécessaire pour atténuer complètement l'incident et empêcher la destruction de toute preuve qui pourrait être nécessaire plus tard pour des poursuites. La première étape est le confinement à court terme. Il s'agit de limiter les dommages dès que possible. Le confinement à court terme peut être aussi simple que d'isoler un segment de réseau de postes de travail infectés pour retirer les serveurs de production qui ont été piratés et ayant tous les trafics acheminés vers les serveurs basculants. Le confinement à court terme est uniquement destiné à limiter l'incident avant qu'il ne s'aggrave. La deuxième étape consiste à sauvegarder le système. Il est nécessaire avant d'effacer et de réimplanter tout système pour prendre une image forensale du (des) système (s) affecté (s) avec des outils bien connus dans la communauté forensique de l'ordinateur, tels que Forensic Tool Kit. La raison est que le logiciel judiciaire capte le (s) système (s) affecté (s) tel qu'il était pendant l'incident et conserve ainsi les preuves dans le cas où l'incident résultait d'un acte criminel ou d'être utilisé pour observer comment le (s) système (s) ont été compromis au cours de la phase des leçons apprises. La dernière étape de cette phase est le confinement à long terme, qui est essentiellement l'étape où les systèmes affectés peuvent être temporairement réparés afin de leur permettre de continuer à être utilisés en production, si nécessaire, tout en reconstruisant les systèmes de nettoyage dans la prochaine phase. Un bon exemple de confinement est de déconnecter les systèmes concernés en déconnectant le câble réseau du système affecté ou en coupant les interrupteurs ou les routeurs sur des parties entières du réseau pour isoler les systèmes infectés de ceux qui sont restés indemnes. Cela isolera

## **II.2 Étude théorique**

---

le problème du reste du réseau de production et limitera la propagation de tout logiciel malveillant ou réduira le risque d'infection d'autres systèmes,

— **Éradication :**

Après avoir contenu avec succès l'incident. La prochaine étape consiste à supprimer la cause de l'incident. Dans le cas d'un incident de virus, il peut être nécessaire d'enlever le virus. Sur d'autres cas d'incidents complexes, nous devrons identifier et atténuer les vulnérabilités exploitées. C'est sur cette étape que nous devrions déterminer comment il a été initialement exécuté et appliquer les mesures nécessaires pour éviter de se reproduire. Un bon exemple d'actions réalisées pendant la phase d'éradication serait d'utiliser les images de disque d'origine qui ont été créées avant qu'un système déployé en production pour restaurer le système, puis l'installation de correctifs et la désactivation des services non utilisés pour durcir le système contre d'autres attaques. Nous analyserons également les systèmes ou les fichiers affectés avec un logiciel anti-malware pour s'assurer que tout malware qui est latent est supprimé,

— **Récupération :**

Le but de cette étape est de ramener les systèmes affectés dans l'environnement de production. Afin de s'assurer qu'il ne conduira pas à un autre incident, il est essentiel de tester, surveiller et valider les systèmes qui sont remis en production pour vérifier qu'ils ne sont pas réinfectés par des logiciels malveillants ou compromis par d'autres moyens. Certaines des décisions importantes à prendre au cours de cette phase sont les suivantes :

- Heure et date pour restaurer les opérations,
- Comment tester et vérifier que les systèmes compromis sont propres et entièrement fonctionnels,
- La durée de la surveillance pour observer les comportements anormaux,
- Les outils pour tester, surveiller et valider le comportement du système,

### **2.3.4 La phase de l'activité post-incident**

L'activité de suivi est cruciale. C'est là que nous pouvons réfléchir et documenter ce qui se passe. C'est là où nous identifions des améliorations pour nos processus et procédures de traitement des incidents et nous écrivons notre rapport final.

Un bon exemple d'interprétation des leçons apprises est d'avoir un point d'alimentation qui résume les informations suivantes :

- Quand le problème a été détecté pour la première fois et par qui,
- La portée de l'incident,
- Comment il a été contenu et éradiqué,

## **II.2 Étude théorique**

---

- Domaines dans lesquels les équipes de gestion des incidents ont été efficaces,
- Domaines qui nécessitent une amélioration.

Cette phase est extrêmement bénéfique pour que les membres partagent des idées et des informations afin d'améliorer l'efficacité de l'équipe dans les incidents futurs.

### **Conclusion :**

Dans ce chapitre, nous avons spécifié les besoins fonctionnels et non fonctionnels de l'OACA. Nous avons aussi décrit les équipements que nous allons superviser ainsi que la topologie du réseau. Nous avons effectué notre choix de la solution SIEM ainsi qu'une étude théorique de cette dernière. Finalement, nous avons définie un staff SOC et une procédure à suivre en cas d'incident au sein de l'entreprise.

Dans le chapitre suivant, nous présenterons les différentes étapes de mise en place de la solution SIEM, nous serons aussi amenés à faire d'autres choix concernant les logiciels de sécurité à installer et les versions correspondantes mais nous tiendrons toujours l'open source comme un critère de choix principal.

---

---

# Chapitre III

---

## Mise en place d’OSSIM : Paramétrage, configuration et déploiement

### Plan

<b>1</b>	<b>Environnement de travail . . . . .</b>	<b>35</b>
1.1	Environnement matériel . . . . .	35
1.2	Environnement logiciel . . . . .	36
<b>2</b>	<b>Mise en place d’OSSIM . . . . .</b>	<b>37</b>
2.1	Installation et configuration d’OSSIM . . . . .	37
2.2	Personnalisation de la solution . . . . .	37
<b>3</b>	<b>Mise en place des systèmes externes . . . . .</b>	<b>39</b>
3.1	Collecte des logs Windows . . . . .	40
3.2	Collecte des logs Linux . . . . .	41
3.3	Collecte des logs Apache . . . . .	42
3.4	Collecte des logs IIS . . . . .	44
3.5	Collecte des logs du pare-feu . . . . .	46
3.6	Collecte des logs routeur . . . . .	47
<b>4</b>	<b>Mise en place de Nagios . . . . .</b>	<b>47</b>
<b>5</b>	<b>Sécurisation de la plateforme . . . . .</b>	<b>50</b>
5.1	Gestion des ports . . . . .	50
5.2	Configuration d’un certificat SSL . . . . .	50
5.3	Sécurisation de l’accès SSH . . . . .	54
5.4	Sécurisation de l’authentification . . . . .	55

### Introduction

Dans ce chapitre, nous allons présenter les étapes de mise en place et de configuration de la plateforme OSSIM. Nous allons détailler aussi les différentes étapes de collecte, de normalisation et de corrélation des logs.

Mais avant tout, nous allons étudier l'environnement matériel et logiciel dont nous disposons pour faciliter les tâches d'installation et éviter tout problème d'incompatibilité du matériel avec les besoins des programmes installés ainsi qu'éviter tout conflit de versions des programmes. Une fois tout est en place nous devons vérifier la bonne connexion entre les différents compartiments ainsi que gérer les problèmes rencontrés.

## 1 Environnement de travail

Dans cette section nous allons présenter l'environnement matériel et logiciel dédié à l'implémentation d'OSSIM au sein de l'OACA.

### 1.1 Environnement matériel

Nous allons héberger notre plateforme sur un serveur **Fujitsu Siemens Primergy rx4770m2**



**Figure III.1** – Fujitsu Siemens Primergy rx4770m2

#### Caractéristiques :

Vitesse d'horloge du processeur : 2700 MHz

Nombre de processeurs : 4

Type de multi-coeur : 8

Mémoire vive : 64 Go

Disque dur : (6\*300) Go

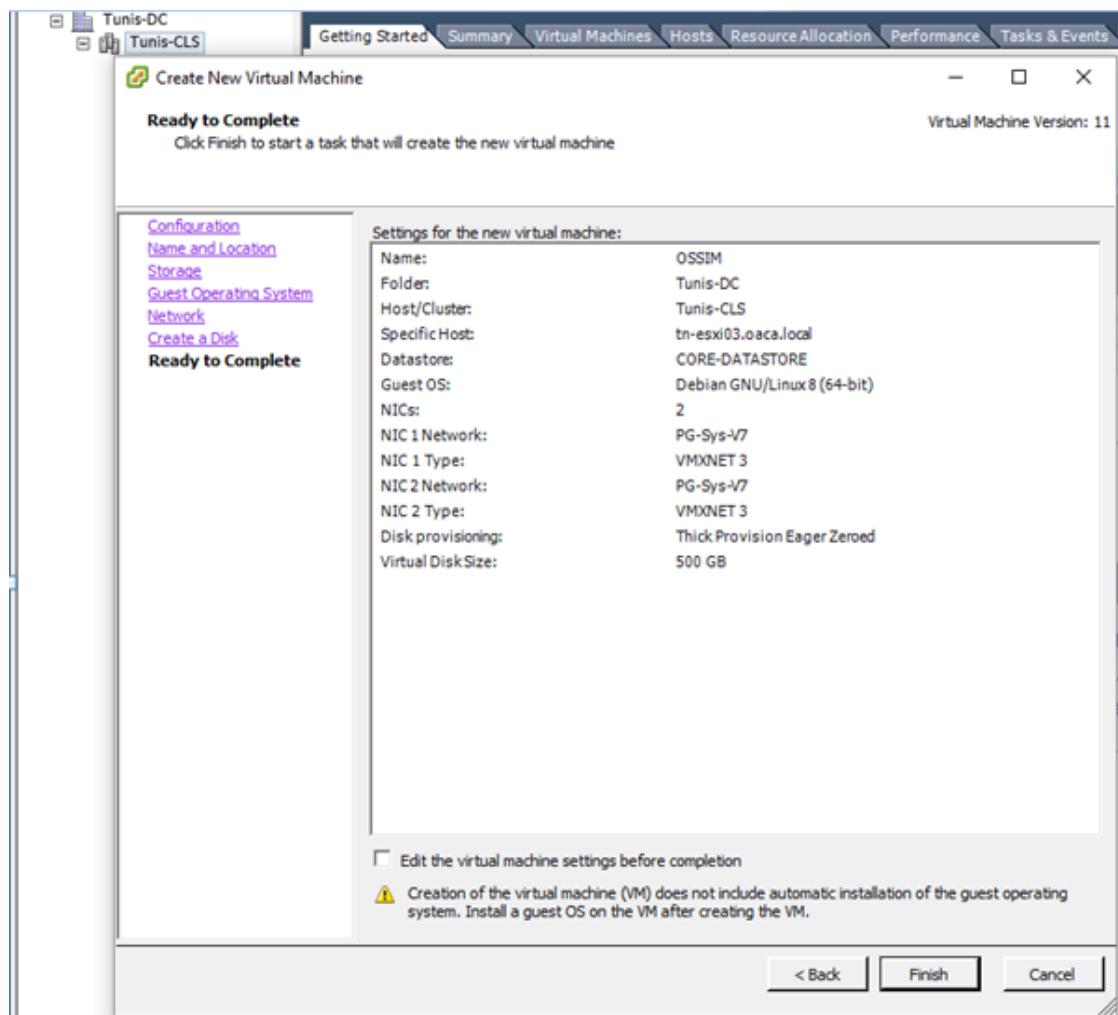
Pour installer OSSIM nous avons réservé les ressources suivantes :

Mémoire vive : 16 Go

### III.1 Environnement de travail

Disque dur : 500 Go

La figure suivante résume les caractéristiques et les ressources réservées pour la machine virtuelle sur laquelle nous allons installer OSSIM :



**Figure III.2** – Crédit d'une machine virtuelle pour installer OSSIM

## 1.2 Environnement logiciel

Le serveur web Apache est équipé de Windows 2003, le serveur IIS tourne sous windows 2012 et la machine linux d'où nous allons collecter les logs possède la distribution Ubuntu server 16.04 LTS.

Le pare-feu est de type cisco-asa ayant comme Operating System (OS) "PIX OS 8.X", le routeur est de type cisco et les autres hôtes sont équipés de différents systèmes d'exploitation à savoir Windows 2003, Windows 2010, Linux,etc.

L'installation d'OSSIM concernera la version 5.3.6 (64 bits) disponible sous format iso basé sur Debian [9].

Nous allons utiliser Win Secure Copy Protocol (WinSCP) [28] comme client File Transfer Protocol (FTP) pour accéder aux machines à distance et réaliser tout transfert de fichiers nécessaires ainsi que Putty [29] comme client Secure Shell (SSH) pour l'accès SSH aux machines distantes. Nous utilisons aussi l'hyperviseur Elastic Sky X (ESXi) [30] du coté serveur, VMware vSphere Client [31] et l'application bureau à distance [32] pour accéder aux interfaces graphiques des ordinateurs distants.

## 2 Mise en place d'OSSIM

La deuxième partie de ce chapitre est consacrée à l'installation et la configuration d'OSSIM ainsi que sa personnalisation. Nous créons aussi notre environnement de travail en ajoutant les hôtes à traiter par notre plateforme.

### 2.1 Installation et configuration d'OSSIM

Nous avons téléchargé le fichier d'installation iso depuis le site officiel d'AlienVault OSSIM [9] puis nous l'avons installé sur le serveur. Une fois l'installation terminée nous pouvons accéder à l'interface web d'OSSIM en saisissant l'Uniform Resource Locator (URL) ‘**http ://@IP**’ dans un navigateur web sachant qu'on a configuré cet URL pendant l'installation.

L'annexe A détaille les différentes étapes d'installation et de configuration d'OSSIM.

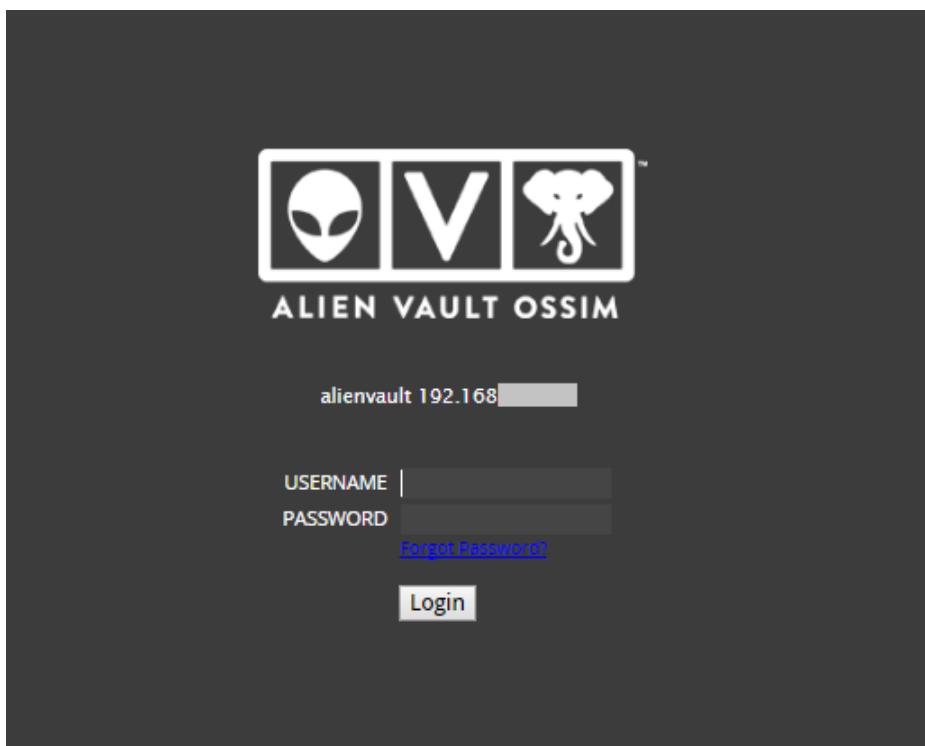
### 2.2 Personnalisation de la solution

Le design par défaut de l'interface d'authentification d'OSSIM n'est pas si professionnel et n'est pas cohérent avec le design du site web de l'OACA (comme le montre la figure III.3).

De ce fait nous avons choisi de le modifier en ajoutant le logo de l'OACA et en modifiant les couleurs.

## III.2 Mise en place d'OSSIM

---



**Figure III.3** – Page d'authentification par défaut d'OSSIM

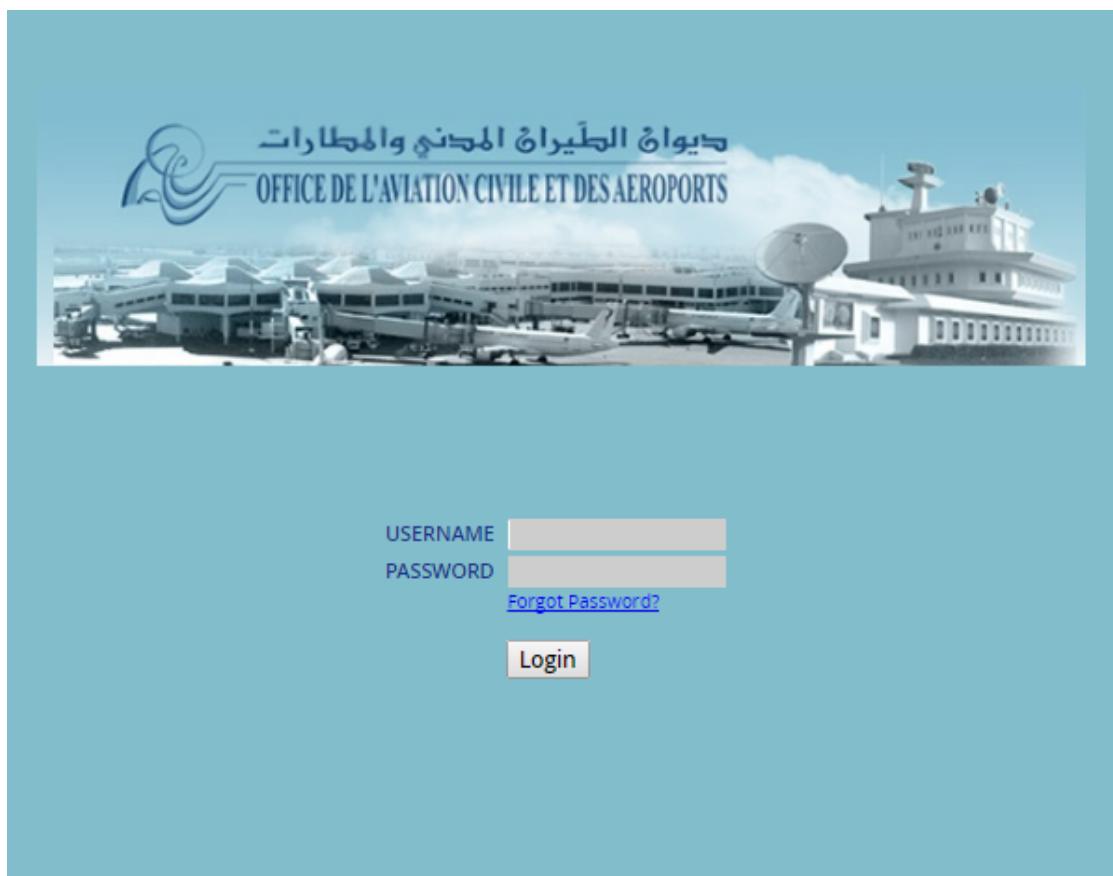
Pour appliquer les changements nous allons modifier les deux fichiers :

/usr/share/ossim/www/session/login.php

/usr/share/ossim/www/style/session/login.css

Une fois les changements appliqués nous obtenons le nouveau design de l'interface d'authentification dans la figure III.4

### III.3 Mise en place des systèmes externes



**Figure III.4** – Nouveau design de la page d’authentification

## 3 Mise en place des systèmes externes

Dans cette partie, nous allons détailler le processus de collecte des événements de sécurité, de tous les équipements définis dans la maquette de test. Les méthodes de collecte de logs peuvent être avec ou sans l'utilisation d'un agent.

Avec ces événements collectés, nous serons en mesure d'observer tous les états de la sécurité liés à un moment donné de différents équipements.

La collecte de données peut se faire de deux façons :

- L'envoi des données de l'hôte à analyser, en utilisant un protocole natif, au capteur (la sonde) qui agit comme un concentrateur,
- L'installation des agents sur l'hôte à analyser, qui vont envoyer les données au capteur.

Le choix de la première ou la deuxième façon dépend généralement de la capacité des machines ou équipements à envoyer ses données à l'extérieur.

### III.3 Mise en place des systèmes externes

#### 3.1 Collecte des logs Windows

La collecte des logs Windows est une étape principale dans le processus de contrôle des machines du réseau et se fait de deux méthodes différentes.

- **Sans agent** : en utilisant Windows Management Instrumentation (WMI). Il s'agit d'un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressource système .Il sert à donner constamment l'état de Windows. Ayant un accès aux logs Windows, WMI peut être configuré pour envoyer les logs systèmes vers une destination prédefinie [33],
- **Avec agent** : pour le choix de l'agent de collecte nous pourrons choisir entre des logiciels spécifiques de collecte de logs, ou encore compter sur une application Host based Intrusion Détection System (HIDS) comme Open Source HIDS SECurity (OSSEC) [34]. Dans notre cas, nous avons remarqué la présence d'une application HIDS qui fait partie des applications préinstallées au niveau de la sonde OSSIM, en effet OSSEC est préinstallé en tant que serveur coté sonde, nous pourrons alors installer OSSEC dans la machine Windows en tant qu'agent de collecte.

Ayant dès le début opté pour les solutions open source, nous avons décidé d'utiliser OSSEC. L'installation des agents se fait d'une façon automatique pour les machines Windows car OSSIM nous fournit un fichier exécutable préconfiguré après avoir fourni les informations nécessaires sur la machine hôte. Les détails de l'installation sont fournis dans l'annexe B.

Après avoir installé OSSEC dans la machine Windows, nous accédons à "**Analysis→Security Events (SIEM)→Real Time**" et nous filtrons par l'adresse IP de la machine Windows.

Un exemple de logs reçus au niveau de serveur est donné par la figure III.5

SECURITY EVENTS (SIEM)								
SIEM		REAL-TIME						
Pause		Done. [0 new rows]						
Date	Event Name	Risk	Data Source	Sensor	OTX	Source IP	Dest IP	
2017-05-25 08:55:53	<a href="#">AlienVault HIDS: Windows Logon Success.</a>	0	AlienVault HIDS-authentication_success	alienvault	N/A	Host-192-168-[REDACTED]	Host-192-168-[REDACTED]	

**Figure III.5** – Exemple de logs OSSEC à partir de la machine Windows

Ce log signifie qu'il y a eu une connexion réussie à cette machine. Il nous donne des informations sur la date de génération de cet événement, son nom, son niveau de risque, sa source de données, la sonde qui l'a collecté et les adresses IP source et destination.Nous pouvons cliquer sur l'événement pour avoir plus de détails comme des informations sur les ports sources et destination, l'identifiant du plugin qui a détecté cet événement ainsi que plusieurs autres informations.

### III.3 Mise en place des systèmes externes

## 3.2 Collecte des logs Linux

Pour la collecte des logs Linux, nous utilisons OSSEC comme agent de collecte.

Une fois les logs sont captés par l'agent de collecte, il les envoie à son tour à l'adresse de la sonde qui est la partie serveuse de l'application. Au niveau de la sonde les logs seront reçus et redirigés vers le plugin correspondant.

La prochaine étape consiste à envoyer les logs vers le serveur qui les affiche sur le tableau de bord du Framework serveur. Ce cycle de redirection des logs est représenté par la figure III.6 :

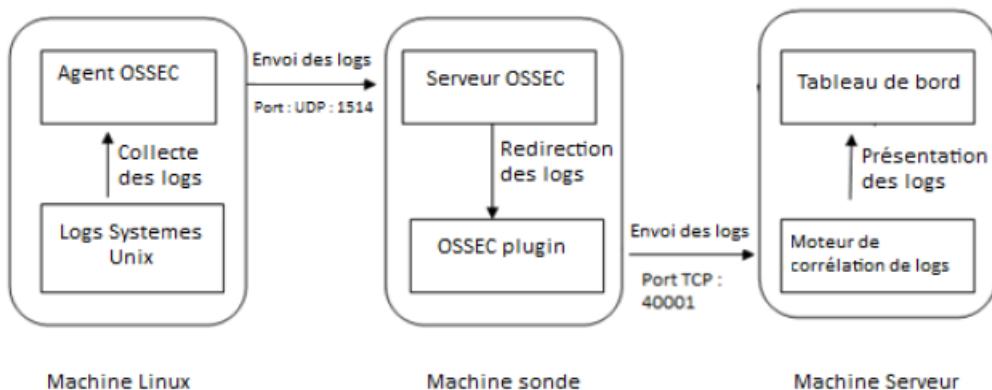


Figure III.6 – Cycle de redirection des logs Linux

Contrairement aux machines Windows, l'installation de l'agent OSSEC pour les machines linux se fait manuellement. Un document détaillant l'installation d'OSSEC est fourni dans l'annexe B.

Une fois OSSEC installé sur la machine linux, nous accédons à "**Analysis→Security Events (SIEM)→Real Time**" et nous filtrons par l'adresse IP de la machine.

Un exemple de logs reçus au niveau de serveur est donné par la figure III.8 :

SECURITY EVENTS (SIEM)								
SIEM		REAL-TIME						
Pause	Date	Event Name	Risk	Data Source	Sensor	OTX	Source IP	Dest IP
	2017-05-19 10:12:11	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	alienvault	N/A		

Figure III.7 – Exemple de logs OSSEC à partir de la machine Linux

Comme dans le cas de la machine Windows, ce log indique aussi une ouverture de session sur la machine Linux en fournissant des informations sur cette session (date, adresses IP, source

### III.3 Mise en place des systèmes externes

de données, sonde ...).

#### 3.3 Collecte des logs Apache

Afin de gérer le serveur web Apache, il est nécessaire de disposer d'un retour d'informations à propos de l'activité et des performances du serveur, ainsi que de tout problème qui pourrait survenir. Le serveur HyperText Transfer Protocol (HTTP) Apache propose des fonctionnalités de journalisation de tout ce qui peut se passer au sein du serveur, depuis la requête initiale, en passant par le processus de mise en correspondance des URLs, et jusqu'à la fermeture de la connexion, y compris toute erreur pouvant survenir au cours du traitement.

Notre serveur apache tourne sous Windows, pour collecter les logs nous avons décidé d'installer Snare [35] comme un agent de collecte.

Après avoir installé Snare sur le serveur Apache, nous configurons cet agent pour qu'il collecte les logs apache et les envoyer vers notre sonde.

Nous accédons à l'interface de configuration de Snare en saisissant l'url suivante : "**localhost :6162**". Nous commençons par choisir le type de logs que nous souhaitons collecter, leur format et leur emplacement. Nous accédons ensuite à Network Configuration et configurer la destination des logs collectés. Nous saisissons l'adresse IP d'OSSIM et le port syslog (514). Finalement nous appliquons la configuration et redémarrer le service Snare.

Nous obtenons ainsi la liste suivante des logs :

Epilog for Windows			
Current Events			
Date	System	Type	Strings
Thu Apr 06 11:48:47 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:48:43 +0100] "GET /officescan/console/html/cgi/cgiChiMasterPwd.exe?id=0011&timeout=1 HTTP/1.1" 200 18384
Thu Apr 06 11:18:44 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:43 +0100] "GET /officescan/console/html/images/icons_alert_off.gif HTTP/1.1" 200 363
Thu Apr 06 11:18:44 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:43 +0100] "POST /officescan/console/html/cgi/cgiShowSummary.exe HTTP/1.1" 200 4545
Thu Apr 06 11:18:44 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:43 +0100] "POST /officescan/console/html/cgi/cgiShowSummary.exe HTTP/1.1" 200 39
Thu Apr 06 11:18:42 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:40 +0100] "POST /officescan/console/html/cgi/cgiShowSummary.exe HTTP/1.1" 200 40
Thu Apr 06 11:18:42 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:40 +0100] "GET /officescan/console/html/images/more_down2_out.gif HTTP/1.1" 200 90
Thu Apr 06 11:18:42 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:40 +0100] "GET /officescan/console/html/images/dot.gif HTTP/1.1" 200 808
Thu Apr 06 11:18:42 2017	DCAITC.OACA.local	ApacheLog	192.168.1.11 - [06/Apr/2017:11:18:40 +0100] "GET /officescan/console/html/images/tab_right_corner_cui.gif HTTP/1.1" 200 122

Figure III.8 – Exemple de logs Apache collectés par Snare

Nous faisons un zoom sur le premier log comme le montre la figure III.9. Il s'agit d'une requête effectuée sur le serveur web apache. Si nous analysons ce log, nous pouvons extraire des informations concernant la requête à savoir la date, le protocole, le time\_out, la méthode (Get ou Post) ...

### III.3 Mise en place des systèmes externes

Date	System	Type	Strings
Thu Apr 06 11:48:47 2017	DCAITC.OACA.local	ApacheLog	192.168. - - [06/Apr/2017:11:48:43 +0100] "GET /officescan/console/html/cgi/cgiChkMasterPwd.exe?id=0011&timeout=1 HTTP/1.1" 200 18384

**Figure III.9** – Zoom sur un exemple de log Apache

Au niveau OSSIM, nous devons activer le plugin Apache et le configurer pour cibler les journaux reçus à partir du serveur web.

En fait, Snare envoie les logs collectés à la sonde via le protocole syslog, donc nous trouvons les logs envoyés dans le fichier "/var/log/syslog".

Dans ce cas nous pouvons directement cibler le fichier principal de Rsyslog mais nous risquons de traiter d'autres logs inutiles, pour cette raison nous avons opté pour l'isolation des logs Apache en les dupliquant vers un autre fichier dédié.

La duplication des logs se fait en ajoutant la règle suivante au fichier "/etc/rsyslog.conf" :

#### **Listing III.1** – Duplication des logs Apache

```
if $programname contains 'apache2' then -/var/log/apache.log
& ~
```

En appliquant cette règle, tout message reçu contenant la valeur "apache2" sera copié dans "/var/log/apache.log".

Le fichier "apache.log" que nous avons créé pour contenir les logs doit être soumis à un processus continu de rotation de log. La rotation de log consiste à compresser les fichiers logs et les diviser en plusieurs fichiers pour permettre de minimiser leurs tailles. Pour la configuration de la rotation de log nous devons créer un nouveau fichier "/etc/logrotate.d/apache.conf", ce fichier doit contenir :

#### **Listing III.2** – Rotation des logs Apache

```
/var/log/apache.log {
    daily # rotate daily
    missingok # if file doesn't exist continue
    rotate 7 # Save the last 7 logs
    compress # Compress the log
    notifempty # if log is empty, the log don't rotate
}
```

Après la fin de la préparation des logs, nous changeons la variable "location" dans le fichier : "/etc/ossim/agent/plugins/apache.cfg" en ajoutant :

#### **Listing III.3** – Configuration du plugin Apache

### III.3 Mise en place des systèmes externes

Location=/var/log/apache.log

Le plugin Apache est maintenant bien configuré et prêt pour traiter les logs d'accès et d'erreurs et assurera leur transfert vers le serveur.

Au niveau du serveur tous les logs Apache reçus seront introduits au moteur de corrélation, pour voir par la suite les événements et les logs dans le tableau de bord d'OSSIM. En cas de détection de tentative d'attaque sur le serveur le système réagira selon la politique de sécurité prédéfinie.

La figure III.10 fourni un exemple de logs Apache

The screenshot shows the OSSIM event viewer interface. At the top, there are filters for 'Event Name' (set to 'Apache: Not Modified'), 'Date (GMT+1:00)', 'Source' (set to '0.0.0.0'), and 'Sensor' (set to 'alienVault'). Below the filters, a single event is listed: 'Apache: Not Modified' on '2017-05-18 11:07:29' from source '0.0.0.0'. The event details show it was collected by 'alienVault' Application Web Misc sensor, with an empty password and a GET request to '/officescan/console/html/images/icons...'. The event has a status of 'Empty'.

Figure III.10 – Exemple de logs Apache

OSSIM nous fournit des détails sur l'événement collecté à savoir son nom, sa date de génération, l'adresse IP source, la sonde qui a collecté cet événement, sa catégorie, sa sous-catégorie et la requête exécutée.

### 3.4 Collecte des logs IIS

Les logs du serveur web IIS constituent aussi une entrée très importante pour notre plate-forme. Pour collecter ces logs, nous procèdons de la même manière que dans le cas du serveur web apache. En effet, nous installons et configurons l'agent Snare pour collecter et envoyer les logs IIS à notre sonde.

La figure III.12 montre un exemple de logs IIS collectés par l'agent Snare après l'avoir installé et configuré convenablement :

The screenshot shows the Snare interface with a red sidebar containing audit configuration options like 'Latest Events', 'Log Configuration', 'Network Configuration', 'Remote Control Configuration', 'Objectives Configuration', 'View Audit Service Status', and 'Apply the Latest Audit Configuration'. The main area is titled 'Epilog for Windows' and shows a table of 'Current Events'. The table has columns for Date, System, Type, and Strings. It lists several log entries for 'IISWebLog' from 'SRVAV.OACA.local' on May 17, 2017, at 15:12:50. Each entry shows a HEAD request to '/officescan/download/server.ini' with various parameters and a status of '200 0 0 0'.

Date	System	Type	Strings
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0

Figure III.11 – Exemple de logs du serveur IIS collectés par Snare

### III.3 Mise en place des systèmes externes

---

Les informations que nous pouvons tirées de ce log sont : la date, l'adresse IP source et les paramètres de la requête exécutée.

Date	System	Type	Strings
Wed May 17 15:12:50 2017	SRVAV.OACA.local	IISWebLog	2017-05-17 14:12:48 192.168. HEAD /officescan/download/server.ini - 8090 - 10.0.12.35 62691CB3BF62DAF233FB2C02782E7BD2 - 200 0 0 0

**Figure III.12** – Zoom sur un exemple de log IIS

Au niveau OSSIM, la configuration du plugin de traitement (IIS) est similaire à celle d'Apache.

Les logs IIS arrivent aussi au niveau de la sonde avec le plugin syslog. Pour les traiter avec le plugin IIS, nous dupliquons ces logs comme nous avons fait pour les logs Apache.

Nous ajoutons donc la règle suivante au fichier "/etc/rsyslog.conf" :

#### **Listing III.4 – Duplication des logs IIS**

```
if $programname contains 'IISWeb' then -/var/log/IISWeb.log
& ~
```

En appliquant cette règle, tout message reçu contenant la valeur "IISWeb" sera copié dans "/var/log/IISWeb.log". Pour la configuration de la rotation de log nous devons créer un nouveau fichier "/etc/logrotate.d/IISWeb.conf", ce fichier doit contenir :

#### **Listing III.5 – Rotation des logs IIS**

```
/var/log/IISWeb.log {
    daily
    missingok
    rotate 7
    compress
    notifempty
}
```

Nous changeons la variable "location" dans le fichier : "/etc/ossim/agent/plugins/IIS.cfg" en ajoutant :

#### **Listing III.6 – Configuration du plugin IIS**

```
Location=/var/log/IISWeb.log
```

Le plugin IIS est maintenant bien configuré et prêt pour traiter les logs provenant du serveur IIS. La figure III.13 fourni un exemple de logs IIS

### III.3 Mise en place des systèmes externes

Date	Event Name	Risk	Data Source	Sensor	OTX	Source IP	Dest IP
2017-05-18 09:36:23	IIS: HTTP Request Method: GET	0	iis	alienVault	N/A	Host-192-168-[REDACTED]	172.22.[REDACTED]:8090
2017-05-18 09:36:23	IIS: HTTP Request Method: GET	0	iis	alienVault	N/A	Host-192-168-[REDACTED]	172.22.[REDACTED]:8090
2017-05-18 09:36:23	IIS: HTTP Request Method: POST	0	iis	alienVault	N/A	Host-192-168-[REDACTED]	● 180.1[REDACTED]:8090
2017-05-18 09:36:23	IIS: HTTP Request Method: POST	0	iis	alienVault	N/A	Host-192-168-[REDACTED]	10.0.[REDACTED]:8090

Figure III.13 – Exemple de logs IIS reçus en temps réel

### 3.5 Collecte des logs du pare-feu

Les journaux de pare-feu révèlent beaucoup d'informations sur les tentatives de menace de sécurité sur notre réseau et sur la nature du trafic entrant et sortant du pare-feu. Ils fournissent des informations en temps réel sur les tentatives de menace de sécurité afin que nous puissions lancer une action corrective rapidement.

De ce fait, nous avons configuré notre pare-feu afin qu'il envoie les logs à la sonde d'OSSIM. Il s'agit d'une simple configuration au niveau du pare-feu représenté par la figure III.14

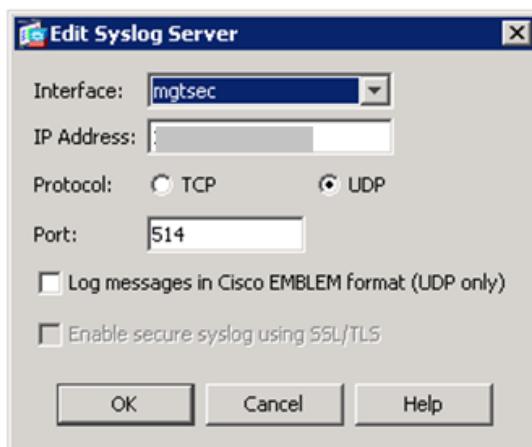


Figure III.14 – Configuration du pare-feu

Au niveau d'OSSIM, il suffit d'activer le plugin "cisco-Asa".

La figure III.15 est un exemple de quelques logs générés par notre pare-feu et collectés par OSSIM. Il s'agit d'un blocage de certains paquets dont les adresses IP sources et destinations et les ports sources et destinations sont donnés par la même figure.

Date	Event Name	Risk	Data Source	Sensor	OTX	Source IP	Dest IP
2017-05-18 11:12:58	ASA: A real IP packet was denied by the ACL	0	cisco-asa	alienVault	N/A	10.0.[REDACTED]:58827	■ 13.107.[REDACTED]:80
2017-05-18 11:12:58	ASA: A real IP packet was denied by the ACL	0	cisco-asa	alienVault	N/A	10.0.[REDACTED]:58828	■ 13.107.[REDACTED]:80
2017-05-18 11:12:58	ASA: A real IP packet was denied by the ACL	0	cisco-asa	alienVault	N/A	10.0.[REDACTED]:60397	■ 131.253.[REDACTED]:443

Figure III.15 – Exemple de logs du pare-feu

## 3.6 Collecte des logs routeur

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Il est indispensable pour transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. C'est donc très important de collecter ses logs et les exploiter afin d'extraire des informations pertinentes quant à l'état de notre réseau.

Dans notre cas nous allons collecter les logs du routeur central (schématisé dans la figure I.2). Nous configurons le routeur (comme indiqué dans la figure III.16) pour envoyer les logs à la sonde d'OSSIM et nous activons le plugin "cisco-router" du coté OSSIM.



```
Rt_Central(config)#logging host 192.168.0.1
```

**Figure III.16** – Configuration du routeur central

Un exemple des logs de ce routeur est illustré par la figure III.17

Date	Event Name	Risk	Data Source	Sensor	OTX	Source IP	Dest IP
2017-05-18 11:18:28	Cisco-OSPF: Open Shortest Path First (OSPF) Warning Event	0	cisco-router	alienvault	N/A	router	0.0.0.0

**Figure III.17** – Exemple de logs du routeur central

Pour plus de détails, nous cliquons sur cet événement. Nous trouvons ce message "No valid authentication send key is available on interface GigabitEthernet0/0". Cet avertissement est dû à un problème d'authentification. En effet, l'authentification au niveau du routeur central a été définie sur MD5 mais la clé d'authentification est définie uniquement pour l'authentification en texte clair. La correction est simple : nous supprimons la commande "ip ospf authentication-key" et, à la place, nous configurons la commande "ip ospf message-digest-key key-id md5 key-string", en remplaçant key-id par un numéro de clé approprié et key-string par un bon mot de passe.

## 4 Mise en place de Nagios

Nagios est un outil open source qui permet d'assurer la supervision des services et des machines d'un réseau. Il permet d'avoir une notification en cas de dysfonctionnement de l'une des machines contrôlées. Il permet aussi de superviser les ressources d'une machine (consommation de mémoire, taux d'utilisation du processeur...) et offre la possibilité d'envoi d'E-mail d'alerte en cas de panne d'une machine du réseau [36].

Nagios est préinstallé au niveau de la sonde, pour mettre en place la surveillance de notre réseau avec nagios, il suffit d'activer le contrôle de disponibilité réseau pour la sonde à partir de la machine serveur en accédant au menu "**Configuration**→**Deployment**→**Components**→**Sensors**"

### III.4 Mise en place de Nagios

et en cliquant sur la sonde à configurer. Nous ajoutons la fonctionnalité Nagios comme indiqué dans la figure III.18.

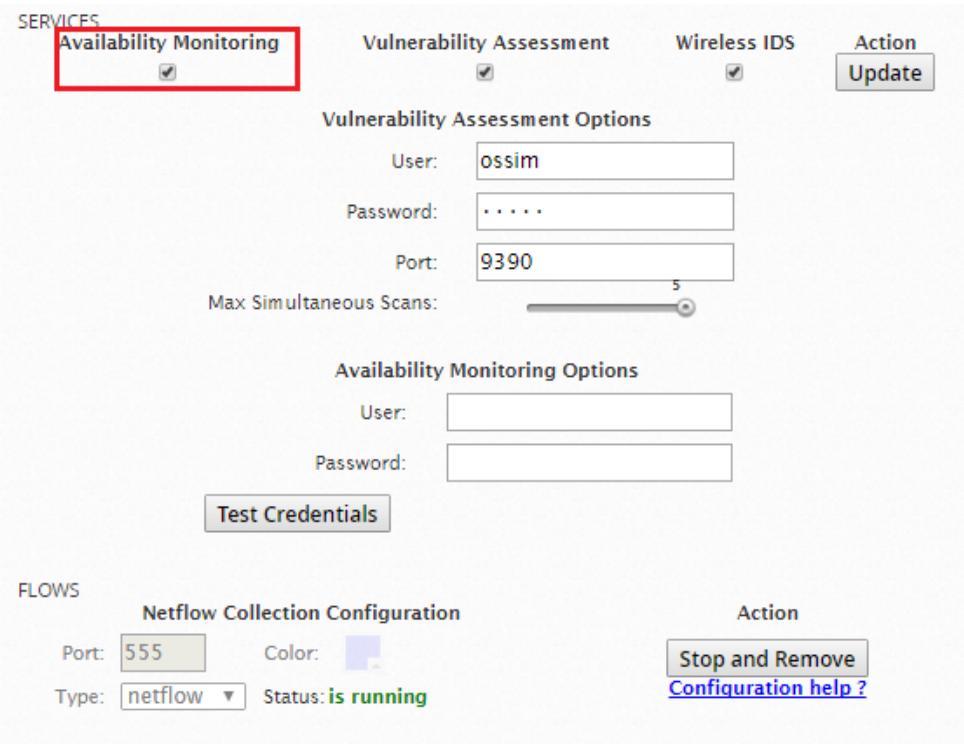


Figure III.18 – Activation de Nagios

Une fois Nagios activé, la gestion de la disponibilité des machines réseau se fait à partir du serveur.

Pour qu'un hôte soit supervisé par nagios il suffit de permettre le suivi de disponibilité pour cet hôte comme indiqué dans la figure III.19

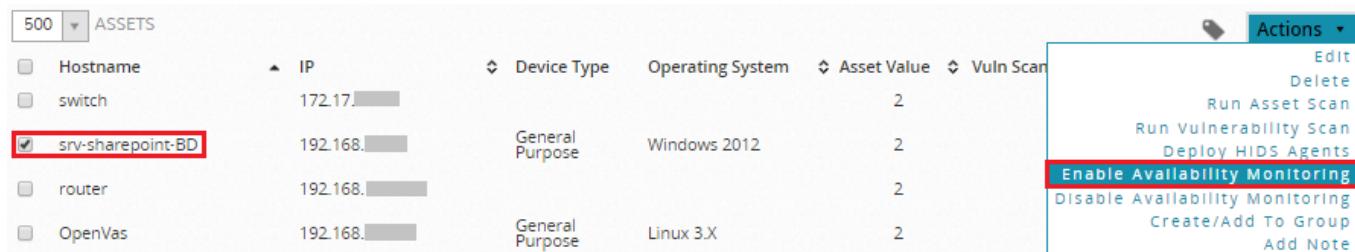


Figure III.19 – Activation de la supervision avec nagios pour un hôte

Nagios offre un menu de statistique de disponibilités des machines à superviser représenté par la figure III.20 :

### III.4 Mise en place de Nagios

The screenshot shows the Nagios reporting interface. At the top, there are tabs for 'MONITORING' and 'REPORTING'. A red oval highlights the text 'Les différents types de statistiques offerts par Nagios' (The different types of statistics offered by Nagios) above a menu bar. The menu bar includes links like 'SERVICE DETAIL', 'HOST DETAIL', 'STATUS OVERVIEW', etc. Below the menu, there are two tables: 'Host Status Totals' and 'Service Status Totals'. The 'Host Status Totals' table shows counts for Up (9), Down (0), Unreachable (0), and Pending (0). The 'Service Status Totals' table shows counts for Ok (29), Warning (0), Unknown (0), Critical (2), and Pending (0). The main content area displays 'Host Status Details For All Host Groups' with a table listing 9 hosts. The table columns include Host, Status, Last Check, Duration, and Status Information. The hosts listed are 222, Host-192-168, OpenVas, alienVault, localhost, and srv-sharepoint-8D, all marked as UP.

Host	Status	Last Check	Duration	Status Information
222	UP	2017-05-18 11:36:29	76d 20h 43m 15s	PING OK - Packet loss = 0%, RTA = 0.22 ms
Host-192-168	UP	2017-05-18 11:33:15	34d 20h 21m 38s	PING OK - Packet loss = 0%, RTA = 0.48 ms
Host-192-168	UP	2017-05-18 11:32:25	34d 20h 22m 38s	PING OK - Packet loss = 0%, RTA = 0.26 ms
Host-192-168	UP	2017-05-18 11:35:39	72d 23h 57m 44s	PING OK - Packet loss = 0%, RTA = 0.03 ms
Host-192-168	UP	2017-05-18 11:32:45	34d 20h 22m 8s	PING OK - Packet loss = 0%, RTA = 0.37 ms
OpenVas	UP	2017-05-18 11:32:25	73d 0h 20m 30s	PING OK - Packet loss = 0%, RTA = 0.20 ms
alienVault	UP	2017-05-18 11:33:49	73d 0h 10m 19s	PING OK - Packet loss = 0%, RTA = 0.03 ms
localhost	UP	2017-05-18 11:35:09	90d 1h 31m 54s	PING OK - Packet loss = 0%, RTA = 0.03 ms
srv-sharepoint-8D	UP	2017-05-18 11:34:19	0d 0h 4m 35s+	PING OK - Packet loss = 0%, RTA = 0.56 ms

Figure III.20 – Détails sur les hôtes supervisés par Nagios

Cet écran fournit des informations sur les statuts des hôtes (up ou down), la date et l'heure de la dernière vérification des statuts, les durées pendant lesquelles les hôtes ont été supervisés et des informations sur leurs statuts (résultats de la commande ping).

Nagios offre d'autres menus de statistiques à savoir "Service Detail", "Status Overview", "Status Grid", "Status Map" ...

Ci-dessous un exemple de statistiques sur les services activés sur un hôte parmi ceux supervisés par nagios (la figure III.21)

The screenshot shows the Nagios reporting interface focusing on service details for the host 'Host-192-168'. A red box highlights the table for 'Host-192-168'. The table lists various TCP services and their status. All services are marked as 'OK'. The columns include Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The services listed are GENERIC\_TCP\_1039, GENERIC\_TCP\_1047, GENERIC\_TCP\_1048, GENERIC\_TCP\_111, GENERIC\_TCP\_135, GENERIC\_TCP\_139, GENERIC\_TCP\_2049, and GENERIC\_TCP\_445. The status information for each service indicates a successful response time on port 192.168.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Host-192-168-	GENERIC_TCP_1039	OK	2017-05-24 09:59:01	40d 18h 40m 56s	1/4	TCP OK - 0.001 second response time on 192.168. port 1039
	GENERIC_TCP_1047	OK	2017-05-24 09:57:03	40d 18h 44m 11s	1/4	TCP OK - 0.001 second response time on 192.168. port 1047
	GENERIC_TCP_1048	OK	2017-05-24 09:54:56	40d 18h 41m 18s	1/4	TCP OK - 0.001 second response time on 192.168. port 1048
	GENERIC_TCP_111	OK	2017-05-24 09:59:20	40d 18h 40m 40s	1/4	TCP OK - 0.001 second response time on 192.168. port 111
	GENERIC_TCP_135	OK	2017-05-24 09:54:55	40d 18h 41m 20s	1/4	TCP OK - 0.001 second response time on 192.168. port 135
	GENERIC_TCP_139	OK	2017-05-24 09:57:37	40d 18h 42m 20s	1/4	TCP OK - 0.001 second response time on 192.168. port 139
	GENERIC_TCP_2049	OK	2017-05-24 09:55:54	40d 18h 40m 23s	1/4	TCP OK - 0.001 second response time on 192.168. port 2049
	GENERIC_TCP_445	OK	2017-05-24 09:56:14	40d 18h 43m 43s	1/4	TCP OK - 0.001 second response time on 192.168. port 445

Figure III.21 – Détails sur les services d'un hôte

Cet écran fournit des informations sur les services actifs sur l'hôte, leurs statuts (OK, Warning, Unknown, Critical ou Pending), les durées de supervision par Nagios, les dates de la dernière vérification de leurs états ...

## 5 Sécurisation de la plateforme

La plateforme OSSIM contient des données très critiques et nécessaires pour le bon fonctionnement de notre entreprise. C'est pour cette raison que nous devons la protéger. Pour ce faire nous avons recours à quatre différents mécanismes de sécurité.

### 5.1 Gestion des ports

Selon les bonnes pratiques de la sécurité, Il est recommandé de n'ouvrir que les ports utiles, et de fermer tous les autres par défaut pour éviter toute faille de sécurité.

C'est ce que nous allons appliquer dans notre cas. En effet, nous allons fermer tous les ports au niveau de notre plateforme OSSIM et ouvrir que les ports utilisés au cours de la collecte des données des équipements et de leurs traitements. La figure III.22 [37] montre les numéros de port utilisés par les composants d'OSSIM pour communiquer entre eux et avec les actifs surveillés.

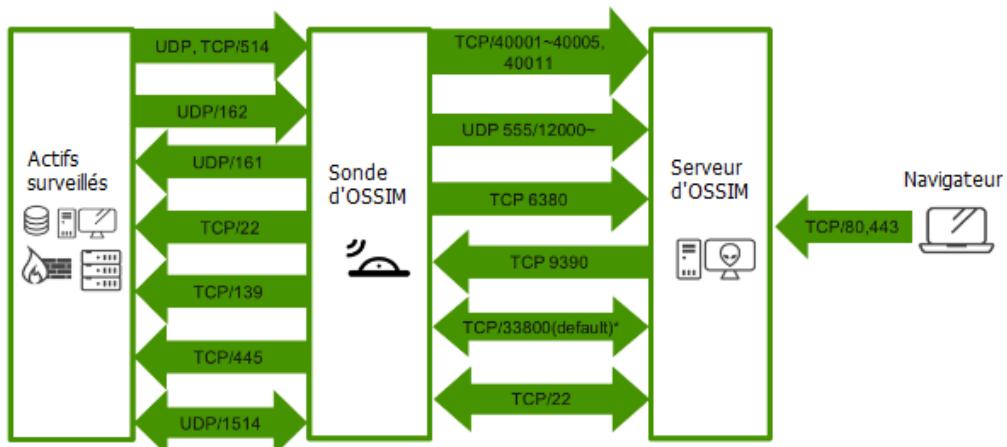
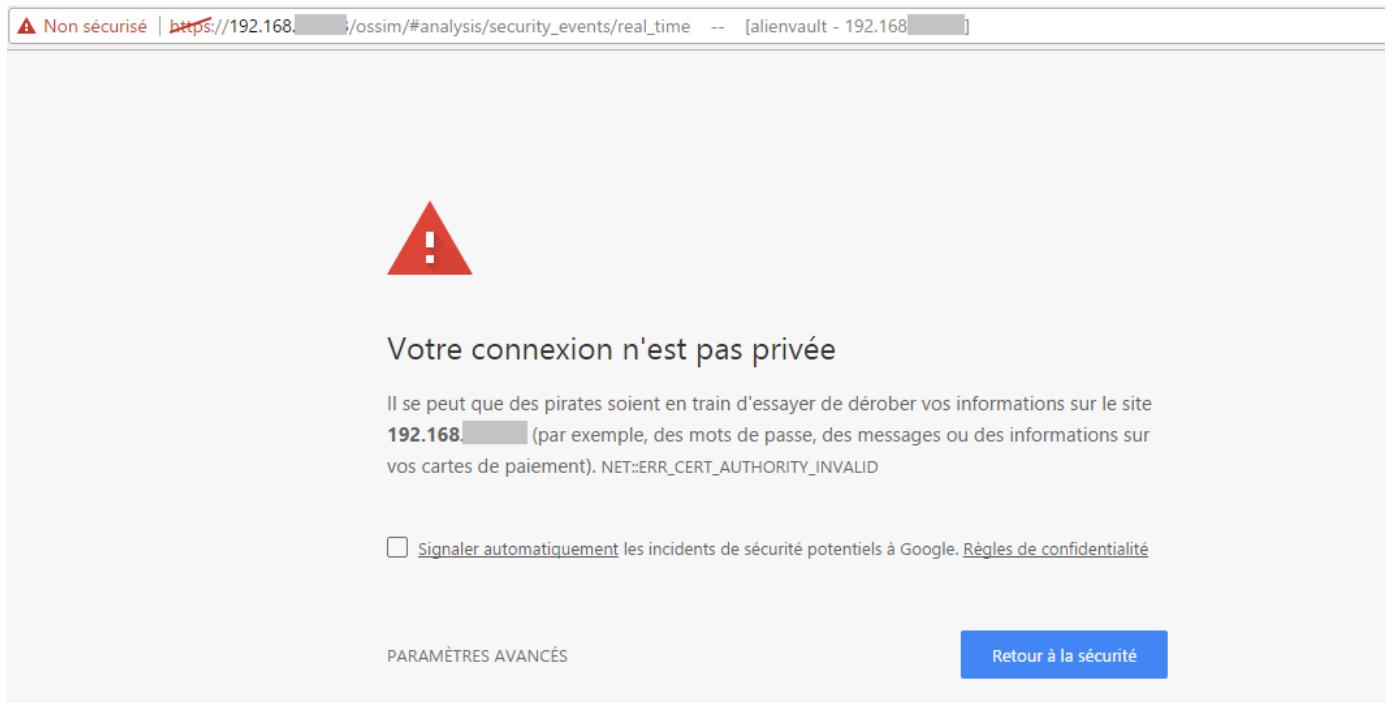


Figure III.22 – Ports utilisés pour la communication entre les composants d'OSSIM

### 5.2 Configuration d'un certificat SSL

Afin de sécuriser l'accès à sa plateforme, OSSIM utilise le protocole HyperText Transfer Protocol Secure (HTTPS). Cependant il reste un problème au niveau de certificat comme le montre la figure III.23

### III.5 Sécurisation de la plateforme



**Figure III.23** – Problème de certificat

Pour résoudre ce problème, OSSIM nous offre la possibilité de sécuriser notre plateforme en fournissant notre propre certificat Secure Socket Layer (SSL) (en format Privacy Enhanced Mail (PEM)).

Nous devons tout d'abord générer un certificat SSL. Pour ce faire, nous procéderons comme suit :

- Nous générerons une clé RSA avec laquelle nous allons générer une demande de certificat SSL. les deux lignes de commande sont données par les figures III.24 et III.29,

```
C:\openssl\bin>openssl genrsa -out ossimnew.key 2048
```

**Figure III.24** – Génération de la clé RSA

```
C:\openssl\bin>openssl req -new -sha256 -key ossimnew.key -out ossimnew.csr
```

**Figure III.25** – Génération d'une demande de certificat SSL

- Pour générer nos certificats, nous utilisons l'outil "Certificate Authority" [38]. Nous copions la demande dans l'emplacement réservé aux demandes de certificat, nous choisissons le modèle "Serveur web" et nous soumettrons notre demande,

### III.5 Sécurisation de la plateforme

**Soumettre une demande de certificat ou de renouvellement**

Afin de soumettre une demande enregistrée à l'Autorité de certification, cochez la case "Demande enregistrée".

**Demande enregistrée :**

Base-64-encoded  
Requête de certificat (CMC ou PKCS #10 ou PKCS #7):

```
C6ghENP8DhOsRvNOKLf64GbJxQzBMM8AJCayfOKW▲
b2Z9oUnNHdGcbyC13AwYWn/HHMfl7onbHMxavJBO
Ue53w+EEiOobhO9gXkKD40MMqYx3syGK108BCgn9
ZHQSv+OFFEaLWtDhwD1XOkc9agRritniZaaJwGWq
NEf0MzNw51Kiwhv10JTJjpMnPBB6bNs30qxeW/LR
-----END CERTIFICATE REQUEST-----
```

[Rechercher un fichier à insérer.](#)

**Modèle de certificat :**

Serveur Web

**Attributs supplémentaires :**

Attributs :

**Envoyer >**

**Figure III.26 – Demande d'un certificat**

- Le certificat généré est en format DER donc nous devons le convertir en PEM grâce à cette ligne de commande,

```
C:\openssl\bin>openssl x509 -inform der -in ossimcernew.cer -out ossimcertnew.pem
```

**Figure III.27 – Conversion de "cer" en "pem"**

- Le certificat est bien généré.

Nous accédons à "**Configuration**→**Administration**→**Main**→**OSSIM Framework**" et copions le certificat SSL ainsi que la clé RSA.

### III.5 Sécurisation de la plateforme

OSSIM FRAMEWORK

PHP Configuration (graphs, acls, database api) and links to other applications

Resolve IPs

Open Remote Netflow in the same frame

MD5 salt for passwords

Internet Connection Availability

Web Server SSL Certificate (PEM format)

-----BEGIN CERTIFICATE-----  
MIIF/jCCBOagAwIBAgIKLwroiQAAAAAYI  
CZImiZPyLGQBGRYFbG9jYWwxFDASBgoJl

Web Server SSL Private Key (PEM format)

-----BEGIN RSA PRIVATE KEY-----  
MIIEowlBAAKCAQEAyW/ep89jkLffhWedD  
dB7Q3S5DCMYBViIL/CJ8FqbjTNadOMsI2

Web Server SSL CA Certificates (PEM format) [optional]

-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----

Resolve IPs###  
Open Remote Netflow in the same frame###  
MD5 salt for passwords###  
Internet Connection Availability### You can configure if you have an internet connection available so that you can load external libraries.

- No: It will not load external libraries.
- Yes: It will check if we have internet connection and if so, it will load external libraries.
- Force Yes: It will always try to load external libraries.  
This option requires to login again.

Web Server SSL Certificate (PEM format)### PEM encoded X.509 certificate. Cut and paste the certificate including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines  
Web Server SSL Private Key (PEM format)### PEM encoded private key. Cut and paste the private key including the "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" lines  
Web Server SSL CA Certificates (PEM format) [optional]### PEM encoded X.509 certificates. Cut and paste the certificates including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines

Figure III.28 – Configuration du certificat d’OSSIM

Le certificat est bien configuré et le problème est résolu

### III.5 Sécurisation de la plateforme

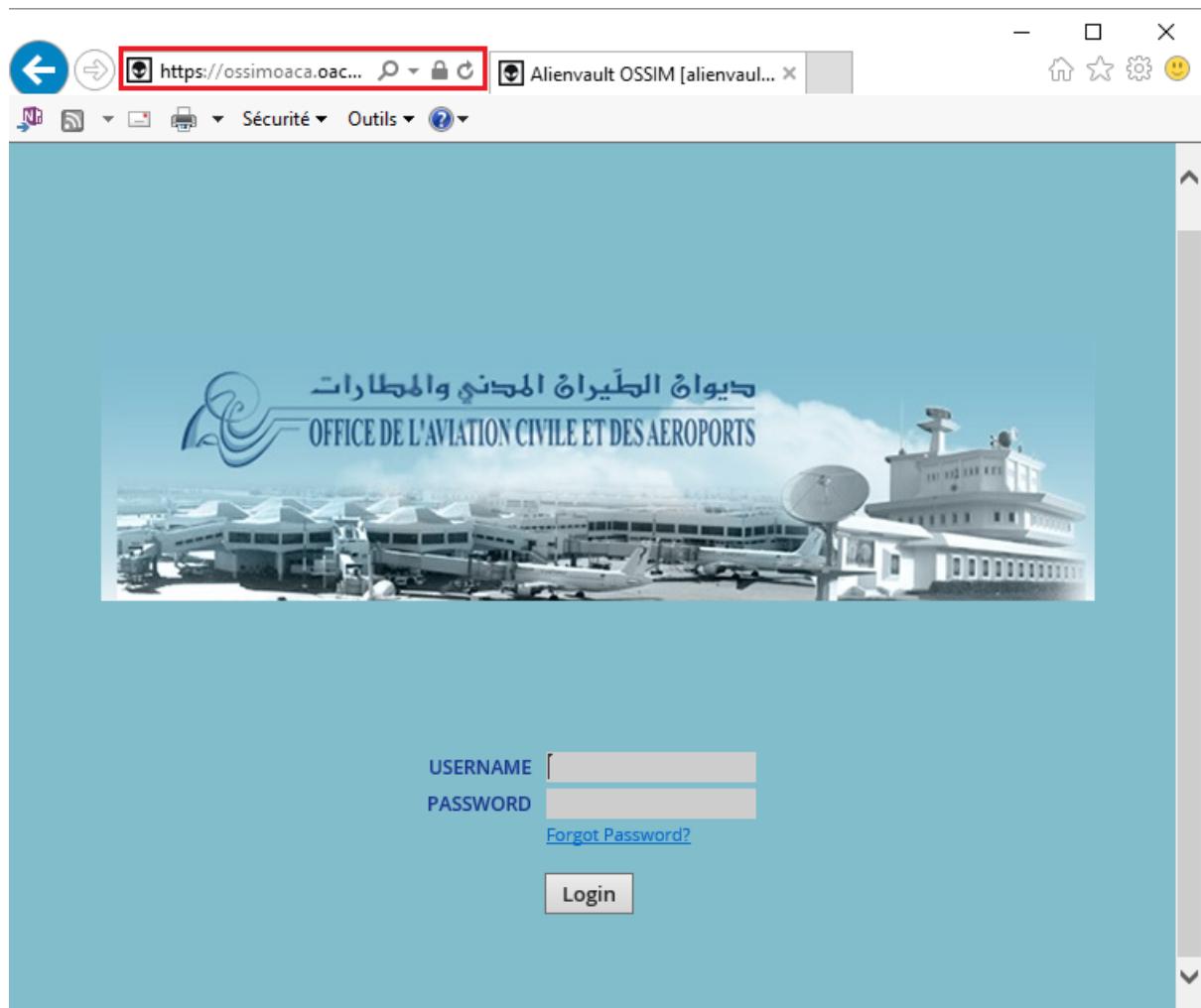


Figure III.29 – Vérification de la bonne configuration du certificat

### 5.3 Sécurisation de l'accès SSH

Pour sécuriser l'accès SSH à la plateforme nous allons activer le plugin "fail2ban" qui détecte les attaques par "Brute Force" en scannant les fichiers de logs du système. Si une attaque est détectée, il bannit l'adresse IP incriminée. Puis nous allons sécuriser l'accès ssh en modifiant le fichier "/etc/ssh/sshd\_config" en :

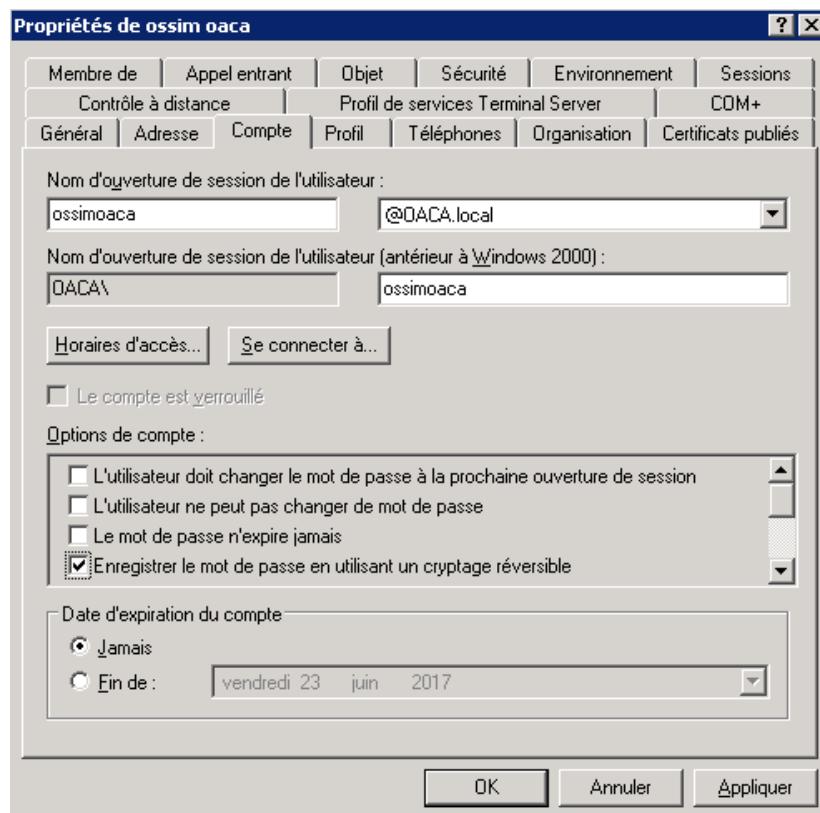
- Changeant le port par défaut de ssh,
- Désactivant le login root,
- Ajoutant un nouvel utilisateur avec lequel nous allons nous authentifier puis monter vers le root,
- Limitant le nombre de sessions ssh ouvertes.

## 5.4 Sécurisation de l'authentification

La sécurité de notre plateforme passe nécessairement par l'authentification des utilisateurs afin de pouvoir restreindre l'accès à nos ressources. Dans ce contexte, OSSIM offre un mécanisme d'authentification qui se réfère à une base de données locale dans laquelle sont stockées les informations sur les différents comptes créés au niveau d'OSSIM (login et mot de passe).

Pour renforcer ce mécanisme d'authentification, nous avons recours à son externalisation en utilisant l'annuaire LDAP (Lightweight Directory Access Protocol) [39] ce qui nous offre une sécurité accrue grâce aux mécanismes de chiffrement et de protection que nous allons embarquer. Pour permettre à OSSIM d'interroger Lightweight Directory Access Protocol (LDAP) pour l'autorisation, nous devons d'abord créer un compte de service dans LDAP.

Nous configurons le nom de compte et le mot de passe. Dans la section "option de compte" nous choisissons d'enregistrer le mot de passe en utilisant un cryptage réversible. Selon la politique de sécurité de l'entreprise, le mot de passe définie expirera dans 3 mois et force l'utilisateur de ce compte de le changer. Cette configuration est illustrée par la figure III.30



**Figure III.30 – Crédit d'un compte dans LDAP**

L'étape suivante est de créer un compte de liaison dans LDAP qui va permettre la connexion

### III.5 Sécurisation de la plateforme

entre OSSIM et notre annuaire. Ce compte posséde nom "ossimldap" et un mot de passe de ce compte qui n'expirera jamais.

Pour configurer OSSIM pour demander l'authentification des utilisateurs LDAP, nous accèdons à "**Configuration→Administration→Main→Login Methods/Options section**" et nous tapons les valeurs représentées par la figure III.31

Setup main login methods/options

Remote login key

Enable LDAP for login Yes ▾

LDAP server address 192.168.1.1

LDAP server port 636

LDAP server SSL Yes ▾

LDAP server TLS No ▾

LDAP server baseDN dc=oaca,dc=local

LDAP server filter for LDAP users (&(sAMAccountName=%u)(objectCategory=Person)

LDAP Username ossimldap@oaca.local

LDAP password for Username .....

Require a valid ossim user for login? No ▾

**Figure III.31** – Configuration d'OSSIM pour l'authentification avec LDAP

- **Remote Login Key** : Pour usage interne uniquement. Nous laissons cette case vide,
- **Enable LDAP for Login** : Nous activons LDAP pour l'authentification,
- **LDAP server address** : Adresse IP du serveur LDAP,
- **LDAP server port** : C'est un port TCP utilisé pour se connecter au serveur LDAP.  
Sa valeur par défaut est 389 ou 636 si on utilise SSL,
- **LDAP server SSL, LDAP server TLS** : Notre serveur LDAP supporte le protocole SSL. Donc, nous activons "LDAP server SSL". La communication entre OSSIM et LDAP est ainsi encrypté,
- **LDAP server baseDN** : Nom distinctif du serveur LDAP (DN) au format dc = <domaine>, dc = <suffixe de domaine>,

- **LDAP server filter for LDAP users** : Filtre sur les utilisateurs de LDAP,
- **LDAP Username** : Le nom du compte de liaison,
- **LDAP password for Username** : Le mot de passe du compte de liaison,
- **Require a valid OSSIM user for login** : Nous choisissons de ne pas créer un compte utilisateur local dans OSSIM puisque nous allons externaliser l'authentification.

## Conclusion

Tout au long de ce chapitre, nous avons mis en place la solution OSSIM. Nous avons explicité ses étapes d'installation ainsi que les principales étapes de configuration. Nous avons aussi, détaillé les étapes de collecte de logs. Nous avons clôturé le chapitre en mettant en place des mécanismes de sécurisation de la plateforme.

Une fois la plateforme est prête, nous allons maintenant vérifier les fonctionnalités que nous avons fixées dès le chapitre II par une série de tests pour valider les performances attendues.

---

---

# Chapitre IV

---

## Test des fonctionnalités de la solution OSSIM

### Plan

<b>1</b>	<b>Test de la fonctionnalité de génération des tableaux de bord . . . . .</b>	<b>58</b>
<b>2</b>	<b>Test de la fonctionnalité de découverte du réseau . . . . .</b>	<b>61</b>
<b>3</b>	<b>Test de la fonctionnalité de corrélation des événements . . . . .</b>	<b>63</b>
3.1	Corrélation croisée : (cross correlation) . . . . .	63
3.2	Directives de corrélation . . . . .	64
<b>4</b>	<b>Test des politiques de sécurité . . . . .</b>	<b>67</b>
4.1	Définition d'une nouvelle action . . . . .	67
4.2	Définition d'une nouvelle politique . . . . .	68
<b>5</b>	<b>Traitemen manuel d'un événement de sécurité . . . . .</b>	<b>69</b>
<b>6</b>	<b>Test de la génération des rapports . . . . .</b>	<b>70</b>
<b>7</b>	<b>Backup . . . . .</b>	<b>74</b>

## Introduction

Une fois la solution est mise en place, nous allons maintenant valider les fonctionnalités déjà détaillées dans le chapitre II. Nous commençons par tester les fonctionnalités de génération des tableaux de bords et de découverte du réseau. Nous entamons ensuite la partie du threat intelligence en exploitant les fonctionnalités de corrélations d'événements et des politiques de sécurité. Nous détaillons aussi la partie de traitement manuelle des événements de sécurité. Finalement nous testons les fonctionnalités de reporting et de backup.

## 1 Test de la fonctionnalité de génération des tableaux de bord

OSSIM offre plusieurs catégories prédéfinies de tableaux de bords.  
Il nous offre aussi la possibilité de personnaliser des tableaux de bords selon nos besoins.

## IV.1 Test de la fonctionnalité de génération des tableaux de bord

Parmi ces catégories de tableaux de bords nous citons :

- **Executive** : Donne des statistiques sur les évènements dans le SIEM. Ces statistiques concernent le nombre d'événements de sécurité en fonction du temps et une classification des événements reçus par source de données. Nous aurons aussi un classement des dix premiers événements enregistrés classés par catégories d'événements. Nous pourrons aussi avoir des statistiques plus pertinentes en matière de sécurité. En effet OSSIM nous fournit des diagrammes de classement des dix hôtes les plus actifs en matière d'événements de sécurité et des 5 événements et alarmes les plus enregistrés,

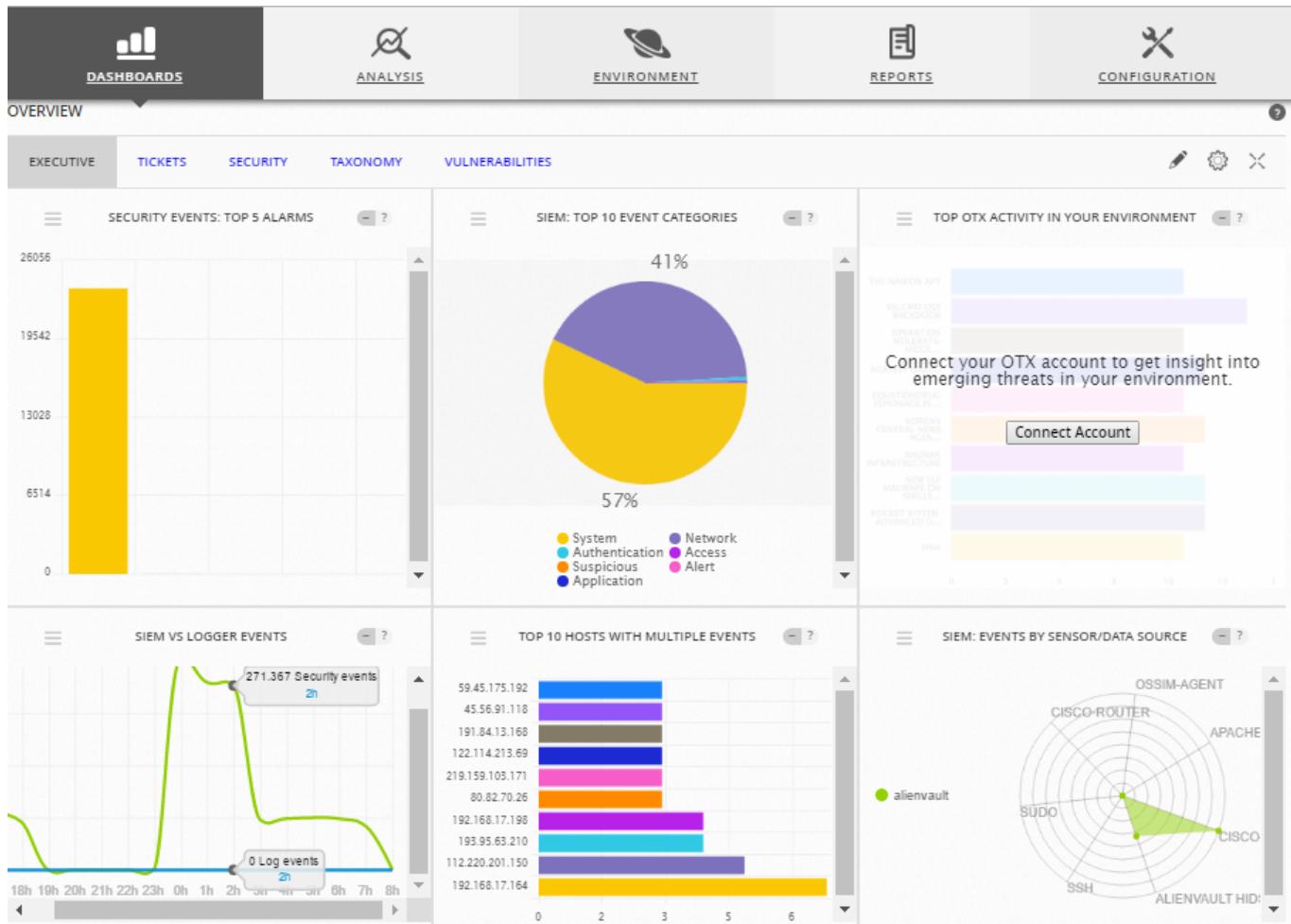


Figure IV.1 – Exemple de tableau de bord : "Executive"

- **Tickets** : Offre des statistiques sur les tickets dans le SIEM à savoir leurs statuts (ouverts ou fermés), leur temps de résolution, des classifications des tickets ouverts par utilisateurs, par classes et par types. Cette catégorie de tableau de bord offre aussi des

## IV.1 Test de la fonctionnalité de génération des tableaux de bord

- statistiques sur le nombre de tickets fermés par mois,
- **Security** : Contient des statistiques sur les événements de sécurité dans le SIEM et des classifications des hôtes selon ces événements,

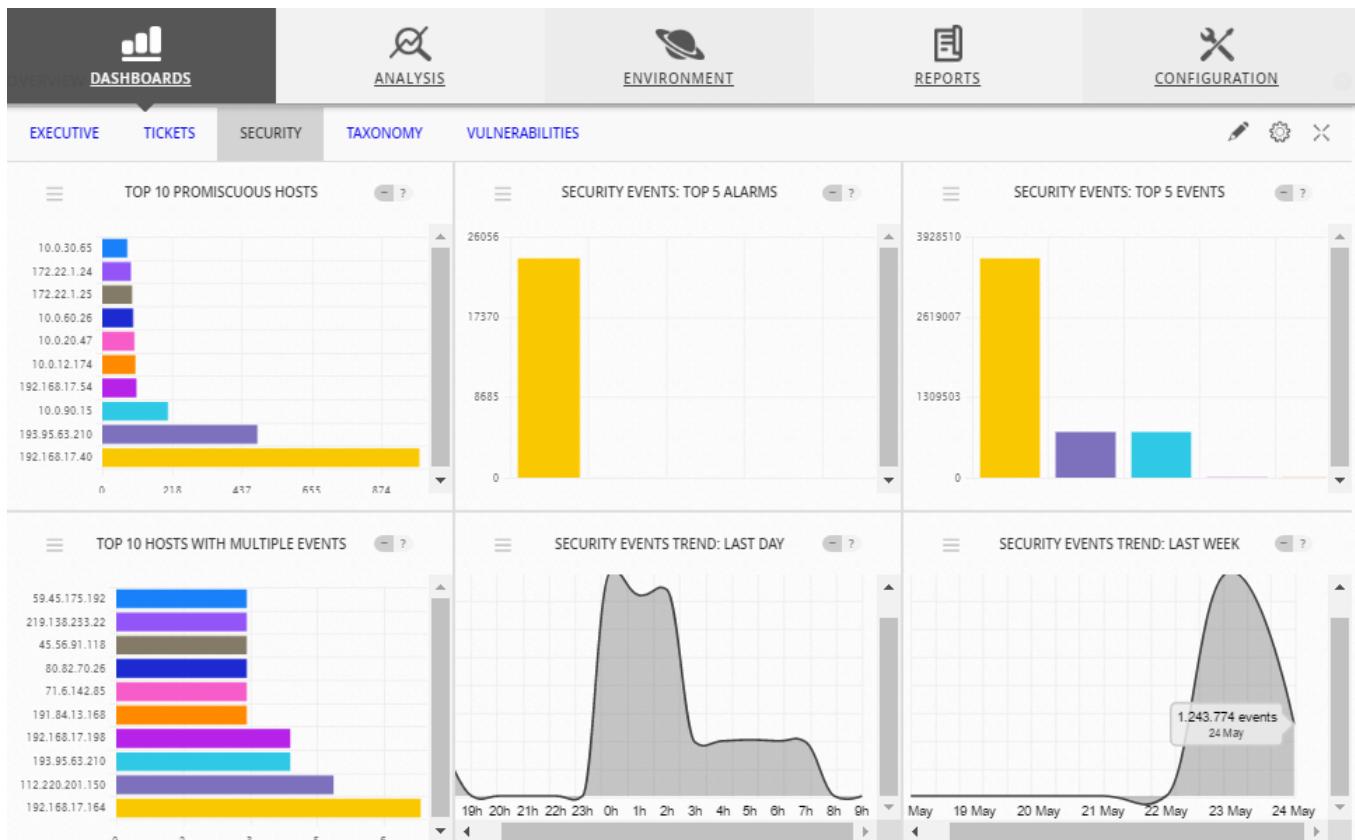
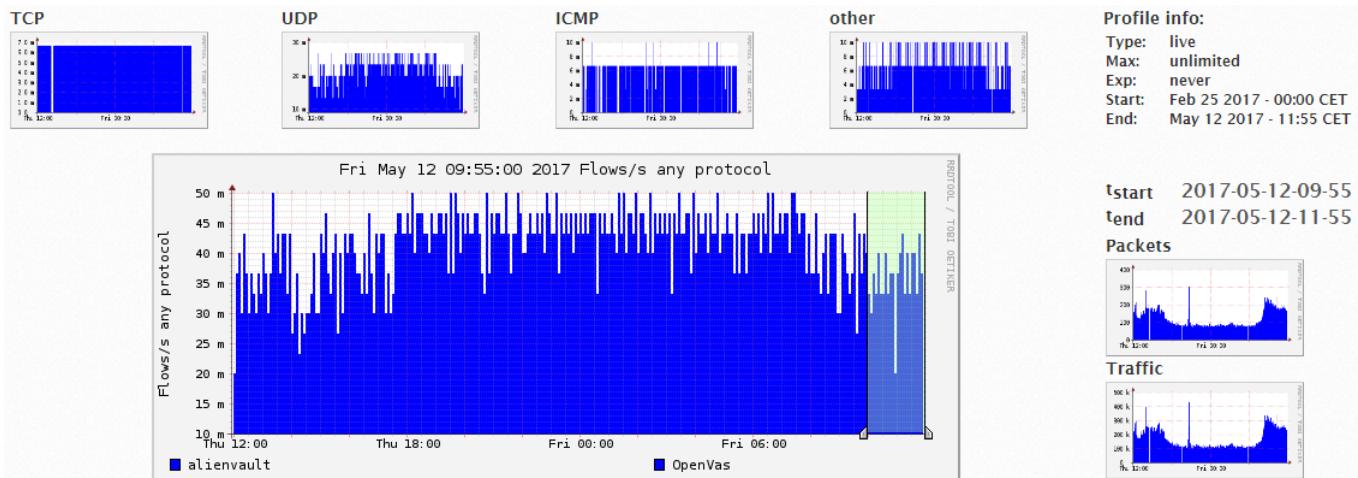


Figure IV.2 – Exemple de tableau de bord : "Security"

- **Taxonomy** : Donne une classification des évènements de sécurité,
- **Vulnerability** : Donne des statistiques sur les vulnérabilités trouvées des équipements connectés à la sonde du SIEM,
- **Netflow** : fournit des statistiques réseaux pertinentes qui concernent toutes les informations du trafic, protocoles utilisés, ports sources et destinations. Les capacités d'analyse d'OSSIM sont dûs à l'utilisation du sniffer NTOP implanté dans la sonde. Network TOP (NTOP) reçoit l'ordre d'analyse du trafic, écoute le réseau et retourne un fichier du type "pcap" au serveur. En analysant ce fichier le serveur génère les statistiques réseaux nécessaires :

## IV.2 Test de la fonctionnalité de découverte du réseau

---



**Figure IV.3** – Tableau de bord "Netflow"

## 2 Test de la fonctionnalité de découverte du réseau

L'outil qui assure la fonctionnalité de découverte du réseau est Nmap. Il est préinstallé dans le serveur et la sonde d'OSSIM ce qui nous permet de choisir entre le lancement d'un scan local ou distant à partir de l'une des sondes disponibles.

La cible de scan peut être une seule machine, un groupe d'hôtes ou tout un réseau.

Afin de lancer un scan, nous commençons par saisir la cible, puis nous passons au paramétrage du scan en choisissant un type parmi les cinq choix proposés.

Les différents types de scan possibles sont :

- **Ping scan** : Lance des "Ping" vers toutes les adresses du réseau pour découvrir les hôtes en marche,
- **Normal scan** : Teste tous les ports des machines,
- **Fast scan** : Ne vérifie que les ports les plus connus,
- **Full scan** : Plus lent mais il inclut le scan de l'OS, service, la version du service, et l'adresse Media Access Control (MAC),
- **Custom scan** : Nous spécifions les ports à scanner.

Nous devons aussi spécifier le Template de scan, nous pourrons choisir le mode "Paranoid" ou "Sneaky" pour réaliser une évasion IDS, le mode "Polite" ne sature pas la bande passante et utilise moins de ressources réseau mais ralentit le scan, les modes "Aggressive" et "Insane" accélère le scan mais ils ne sont conseillés que sur des réseaux fiables.

Nous prenons l'exemple du scan représenté par la figure IV.4 :

## IV.2 Test de la fonctionnalité de découverte du réseau

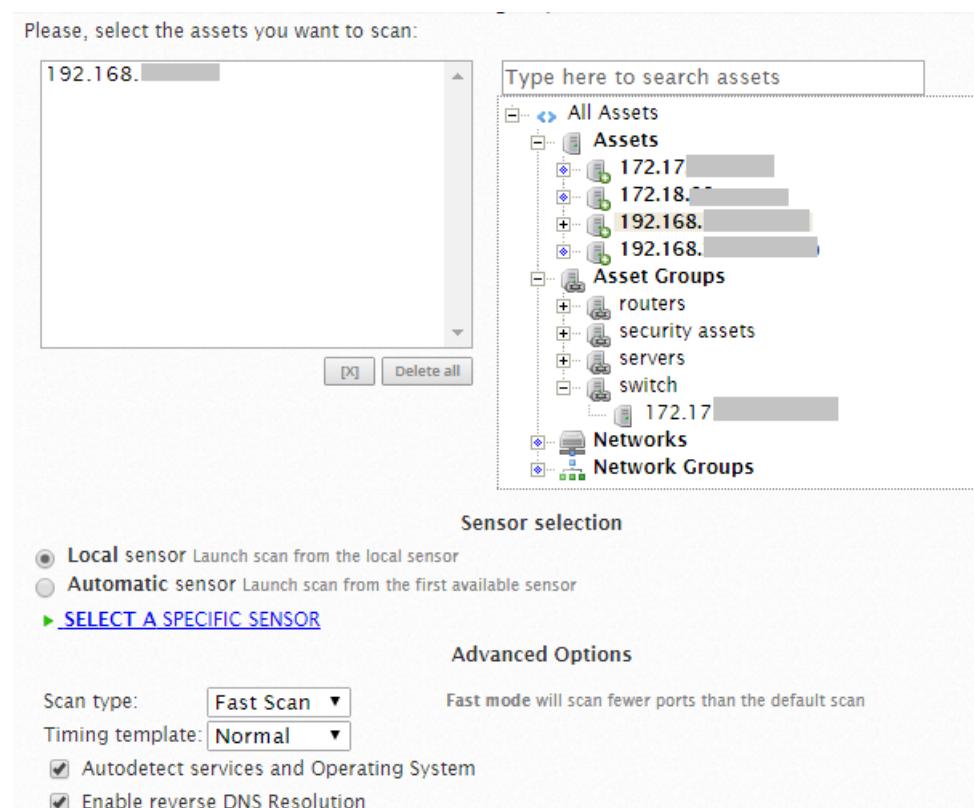


Figure IV.4 – Exemple de scan d'un hôte

Nous avons choisi d'effectuer un scan local de type "fast scan" et de template "normal" sur un seul hôte.

Après la fin de scan nous aurons des informations sur l'hôte à savoir son adresse IP, son nom, son Qualified Domain Name (FQDN) (c'est un nom du domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine.), son type, son adresse MAC, son système d'exploitation et les ports ouverts sur cette machine. Ces informations sont représentées par la figure IV.5 :

SCAN RESULTS							
<input checked="" type="checkbox"/>	Host	Hostname	FQDN	Device types	Mac	OS	Services
<input checked="" type="checkbox"/>	192.168.1.1	alienVault	alienVault.alienVault	General Purpose	-	Linux 3.X	ssh, mysql, https, http, otp
<a href="#">Clear scan result</a> <a href="#">Update managed assets</a>						<input type="checkbox"/> FQDN as Hostname	

Figure IV.5 – Résultat du scan

### 3 Test de la fonctionnalité de corrélation des évènements

Après que le serveur reçoit des événements normalisés à partir d'une sonde, il évalue les événements par rapport aux politiques, effectue l'évaluation des risques, puis effectue une corrélation.

Le moteur de corrélation applique des règles de corrélation aux événements, générant de nouveaux événements, le cas échéant, avec des valeurs de priorité et / ou de fiabilité plus élevées. OSSIM fournit deux types de corrélation :

#### 3.1 Corrélation croisée : (cross correlation)

Le serveur utilise la corrélation croisée pour modifier la fiabilité d'un événement Network Intrusion Detection System (NIDS), affectant par la suite l'évaluation des risques de l'événement.

Cette corrélation est effectuée seulement sur les événements avec l'adresse IP de destination définie, et le système vérifie si une vulnérabilité a été identifiée sur cette destination. Si l'IDS a découvert une attaque sur une adresse IP et une vulnérabilité associée a été trouvée sur la même adresse IP, la fiabilité de l'événement IDS augmente jusqu'à 10.

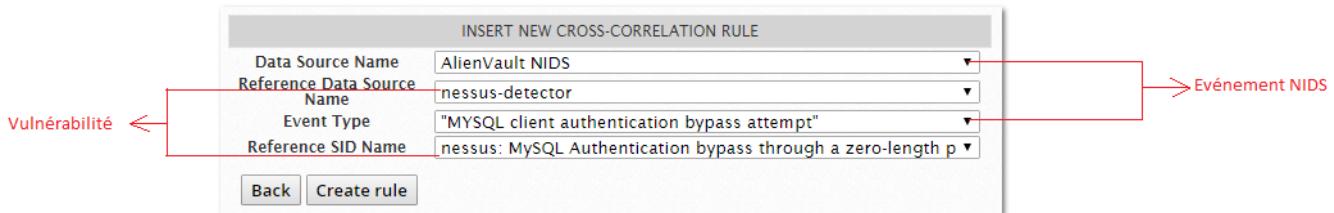
Dans ce qui suit, nous allons fournir un exemple de corrélation croisée qui sert à détecter une tentative de dérivation d'authentification MySQL avec un mot de passe vide (MySQL authentication bypass attempt with an empty password).

Pour créer cette nouvelle règle de corrélation croisée nous accédons à "**Configuration→Threat Intelligence→Cross Correlation**", puis nous cliquons sur New. Nous choisissons "AlienVault NIDS" comme Data Source Name. A ce niveau, OSSIM charge la liste Event Type, nous choisissons "My Structured Query Language (MySQL) client authentication bypass attempt".

Dans Reference Data Source Name nous choisissons "nessus-detector", OSSIM charge la liste Reference SID Name pour le scanner de vulnérabilité, nous choisissons "nessus : MySQL Authentication bypass through a zero length password" et nous cliquons finalement sur "create rule".

La figure IV.6 illustre les différentes étapes de création de la corrélation déjà citées :

### IV.3 Test de la fonctionnalité de corrélation des évènements



**Figure IV.6** – Exemple de corrélation croisée : Détecter une tentative d’authentification MySQL avec un mot de passe vide

## 3.2 Directives de corrélation

Une directive de corrélation se base sur des conditions prédéfinies, quand ces conditions sont remplies, un événement de sécurité sera généré. Cet événement sera traité par le serveur comme s'il était un événement reçu d'une sonde. Sur cet événement nous appliquons la politique de sécurité définie dans le serveur, selon la politique une alerte peut être lancée.

Une directive de corrélation est composée des éléments suivants :

- **Id** : Numéro unique définissant la directive, compris entre 500000 et 999999.
- **Name** : Nom de la directive, peut contenir des variables qui seront remplacées par la suite selon l'environnement de la directive (SRC\_IP, DST\_IP, SRC\_PORT ...)
- **Priority** : une valeur numérique variant entre 0 et 5 définissant la gravité de l'événement (0 est la plus faible priorité).
- **Rule** : une directive peut avoir une ou plusieurs règles.

Une règle est le cœur de la directive, elle permet d'agir sur les événements. Elle est constituée des éléments suivants :

- **Type** : nous distinguons entre "Detector Rules" (qui sont reçues automatiquement d'un agent tel que Snort) et "Monitor Rules" (qui sont contrôlées par l'outil de sniffing du serveur qui est généralement NTOP)
- **Name** : Nom de la règle.
- **Reliability** : Peut être une valeur absolue (0-10) ou une valeur incrémentale (+2, +4...) qui sera ajoutée à la dernière valeur de l'événement généré par la directive.
- **Occurrence** : Le nombre d'événements collectés vérifiant les conditions nécessaires pour que la directive génère un événement. (Pour la règle de niveau 1 l'occurrence est toujours égale à 1)
- **Time\_out** : Limite de la période de temps nécessaire pour satisfaire la règle.
- **From** : Adresse IP source (ANY, HOME\_NET...)
- **To** : Adresse IP destination (ANY, HOME\_NET...)
- **Sensor** : La sonde qui a détecté cette condition (ANY, Sensor Name...)

### IV.3 Test de la fonctionnalité de corrélation des évènements

---

- **Port\_from** : Port source
- **Port\_to** : Port destination
- **Plugin\_id** : l'ID du plugin qui a fourni l'événement.
- **Plugin\_sid** : l'ID de l'événement généré.

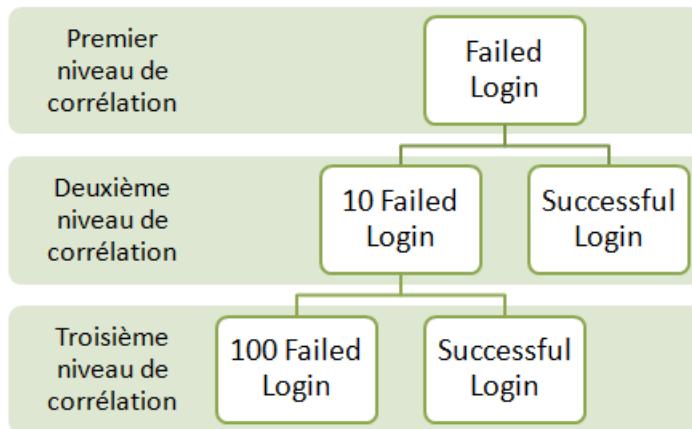
Une directive peut avoir plusieurs niveaux comme elle peut en avoir un seul. À partir du deuxième niveau nous commencerons par tester la sortie du niveau précédent et appliquer les nouvelles règles sur son output.

Dans ces niveaux nous pourrons parler du nombre d'occurrences ainsi que le time out.

Dès leur arrivée au serveur, tous les événements seront testés au niveau 1 de chaque directive. Le premier niveau de chaque directive présente toujours une règle de détection, il se déclenchera dès la première occurrence d'un événement et ne supporte pas de time-out. Il faut souligner qu'une directive ne lancera un événement à partir du niveau 1 que si c'est le seul niveau de la directive. À partir du deuxième niveau, nous pouvons avoir plusieurs règles dans le même niveau, dans ce cas le moteur de corrélation exécutera les règles en parallèle.

La figure IV.7 montre un exemple d'une directive de corrélation. Cette directive détecte les événements d'authentification en force brute (brute force authentication) en connectant deux types d'événements, connexion échouée (failed login) et connexion réussie (successful login). En fonction du nombre d'occurrences d'événements individuels, le moteur de corrélation peut conclure que l'événement représente un cas où un administrateur ne saisit pas de mot de passe (une tentative de connexion échouée suivie d'une connexion réussie), une attaque de force brute réussie avec une faible fiabilité (10 échoués Les tentatives de connexion suivies d'une connexion réussie) ou une attaque de force brute réussie avec une grande fiabilité (100 tentatives de connexion échouées suivies d'une connexion réussie). Tous ces événements doivent provenir de la même adresse IP et accéder à la même adresse IP, afin que l'événement de la directive soit créé.

### IV.3 Test de la fonctionnalité de corrélation des évènements



**Figure IV.7** – Exemple de directive de corrélation - détection d'attaques de force brutale

Les étapes de création de cette directive sont fournies dans l'Annexe C.

Pour tester cette directive, nous allons effectuer des tentatives d'accès SSH non réussis à partir d'une même adresse IP et sur l'adresse IP du serveur OSSIM. Nous pouvons vérifier le déclenchement des alarmes en accédant à "**Analysis→Alarms**". Nous obtenons la date de génération de l'alarme et son type comme représentés dans la figure IV.8 :

31 DAYS	17-05-05	17-05-06	17-05-07	17-05-08	17-05-09
System Compromise					
Exploitation & Installation					
Delivery & Attack					
Reconnaissance & Probing					
Environmental Awareness					

**Figure IV.8** – Déclenchement de l'alarme

Pour avoir plus de détails sur l'événement, nous cliquons sur l'alarme. Nous obtenons des informations sur la date et l'heure de l'événement, son statut, les valeurs des champs "intent and strategy" et "Method" définies lors de la création de la directive, le risque de l'événement

## IV.4 Test des politiques de sécurité

ainsi que ses adresses IP source et destination.

Ces informations sont données par la figure IV.9

Date	Status	Intent & Strategy	Method	Risk	OTX	Source	Destination
2 mins	●	Bruteforce Authentication	SSH	low (1)	N/A	Host-172-18-1-58839	0.0.0.0
3 mins	●	Bruteforce Authentication	SSH	low (1)	N/A	Host-172-18-1-58820	0.0.0.0:ssh

Figure IV.9 – Détails de l'alarme

## 4 Test des politiques de sécurité

La mise en œuvre d'une nouvelle politique de sécurité consiste à identifier les risques, à savoir les mesurer et à mettre en œuvre les outils nécessaires pour diminuer ces risques. Les politiques de sécurité sont les règles définissant comment le système doit réagir face aux événements de sécurité reçus. Pour cela nous devons tout d'abord définir les types d'actions possibles et ensuite associer l'action à l'événement correspondant.

### 4.1 Définition d'une nouvelle action

Lors de la définition d'une nouvelle action, nous définissons :

- **Un nom** : nous pouvons utiliser des variables compréhensibles par le système comme (DATE, PLUGIN\_ID, PLUGIN\_SID, RISK, PRIORITY...),
- **Une description** : une brève description de l'action,
- **Un type** : nous distinguons entre trois types d'action : envoyer un e-mail de notification, ouvrir un ticket (un ticket est un élément dans OSSIM qui contient des informations sur les alertes détectées ou tout autre problème que nous souhaitons suivre dans un flux de travail) [40] ou exécuter un programme externe,
- **Une condition d'exécution** : nous pouvons choisir "ANY" pour ne rien définir ou exiger une alarme ou mettre sa propre condition logique qui doit être écrite sous forme d'une expression Python booléenne.

Nous allons enchainer avec l'exemple de l'attaque d'authentification par force brutale.

Nous créons alors l'action suivante :

## IV.4 Test des politiques de sécurité

The screenshot shows a configuration form for creating a new action. The fields are as follows:

- Name \***: Test SSH Brute Force Attack Rule
- Description \***: Tester la nouvelle directive SSH Brute Force Attack
- Type \***: Open a ticket
- Condition**: Any (radio button selected)
- To: \***: ossimoaca@oaca.nat.tn
- In Charge:**: User: admin
- Save** button

Figure IV.10 – Exemple de création d'une action

Nous avons choisi d'ouvrir un ticket dont la personne qui s'en charge est l'administrateur. Une fois que nous avons créé la directive et l'action à effectuer, nous allons créer la politique de sécurité qu'elle va associer les conditions et les conséquences des événements de sécurité.

## 4.2 Définition d'une nouvelle politique

Pour ajouter une nouvelle politique nous devons définir principalement deux parties :

- **La partie condition** : consiste à définir l'adresse source et destination du paquet qui a vérifié cette condition, nous précisons par la suite le port source et destination ainsi que le type d'événement. Pour le choix du type d'événement nous avons le choix entre une liste de types d'événements connus (Get IP request, Network anomalies, Suspicious DNS, Snort HTTP INSPECT, Snort IDS...). Pour le choix des ports nous pouvons définir au préalable un groupe de ports (Exp : Ports-Web). Si nous n'avons pas de conditions pour un champ, nous pourrons utiliser la variable "ANY" pour vérifier la condition indépendamment la valeur de ce champ,
- **La partie Conséquences** : elle définit comment réagir face à l'événement qui a vérifié tous les champs de la partie condition. Le champ action définit la réaction du système, pour le remplir nous choisissons l'une des actions déjà définies dans la section précédente. Le champ SIEM définit les actions du serveur vis-à-vis de cet événement ce qui nous permet d'appliquer une corrélation logique à cet événement, stocker l'événement dans la base de données ou lui définir une priorité. Les champs "Logger" et "Forwarding" sont réservés à la version commerciale d'Alienvault.

Nous créons alors la politique suivante :

## IV.5 Traitement manuel d'un événement de sécurité

The screenshot shows the OSSIM Policy Rule creation interface. The policy rule name is "SSH Brute Force Attack Policy". The "Enable" option is set to "Yes". The "Policy Group" is "Default policy group". The "Conditions" section includes "Source ANY", "Dest ANY", "Src Ports ANY", "Dest Ports ssh", "Event Types ANY", and "DS Groups: ANY". The "Actions" section lists "Test SSH Brute Force Attack Rule" and "SIEM (Yes)". The "Consequences" section includes "SIEM", "Logger (No)", and "Forwarding". Below these, there are additional settings: "Set Event Priority: Do not change", "Risk Assessment: Yes", "Logical Correlation: Yes", "Cross-correlation: Yes", and "SQL Storage: Yes".

Figure IV.11 – Exemple de création d'une politique

## 5 Traitement manuel d'un événement de sécurité

OSSIM nous offre la possibilité de réagir manuellement à un événement suspect qui n'a pas violé une règle de la politique de sécurité.

Par exemple si le serveur reçoit un événement signifiant l'ouverture de session sur une machine alors que nous savons que l'employé chargé de travailler sur cette machine est absent, dans ce cas nous pouvons réagir en ouvrant un nouveau ticket, par exemple, pour demander des renseignements sur l'événement. Les actions de ce genre sont difficiles à automatiser vu que les données de présence et d'absence des employés ne constituent pas un "Input" pour le serveur. Pour consulter les différents événements reçus par le serveur nous accédons à "**Analysis → Security Events (SIEM)**". Nous pouvons appliquer un filtre personnalisé sur l'affichage des événements en choisissant par exemple une source de données bien précise ou une sonde etc.

Si nous décidons que l'événement de la figure IV.12 (encadré en rouge) est suspect et que nous devrons réagir en ouvrant un ticket par exemple nous procéderons comme suit :

The screenshot shows the OSSIM Analysis interface. At the top, there are navigation tabs: DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below the tabs, a message "Événement suspect" is displayed. A red circle highlights a specific event entry. The event details are: "AlienVault HIDS: Windows Logon Success.", timestamp "2017-05-15 10:15:27", source "alienVault", status "N/A", host "Host-192-168-", priority "low (0)", and a correlation ID "2->2".

Figure IV.12 – Événement suspect

Nous choisissons l'utilisateur qui va se charger de ce ticket, sa priorité et son type. Ces différents paramètres sont illustrés par la figure IV.18

## IV.6 Test de la génération des rapports

Values marked with (\*) are mandatory

NEW TICKET

Title *	AlienVault HIDS: Windows Logon Success.
Assign To *	User: ossimoaca
Priority *	1
Type *	Anomalies
Source Ips	192.168.
Dest Ips	192.168.
Source Ports	0
Dest Ports	0
Start of related events	2017-05-15 09:15:27
End of related events	2017-05-15 09:15:27

**Save**

Figure IV.13 – Ouvrir un ticket

## 6 Test de la génération des rapports

OSSIM nous offre la possibilité de consulter plusieurs types de rapport, les générer sous format PDF téléchargeable ou les envoyer par e-mail. Ces différents types de rapports offerts par OSSIM sont :

- **Rapport sur les alarmes** : nous avons la possibilité de cocher les informations que nous souhaitons avoir dans le rapport. Les actions possibles pour ce type de rapport sont le téléchargement ou l'envoie par e-mail.

Report Name	Report Options	Actions
Alarms Report <input checked="" type="checkbox"/> Title Page <input checked="" type="checkbox"/> Top 10 Attacker Host <input checked="" type="checkbox"/> Top 10 Attacked Host <input checked="" type="checkbox"/> Top 10 Used Ports <input checked="" type="checkbox"/> Top 15 Alarms <input checked="" type="checkbox"/> Top 15 Alarms by Risk	Date Range 2017-04-12 - 2017-05-12	 Download PDF  Send by e-mail

Figure IV.14 – Rapport sur les alarmes

- **Rapport sur un hôte** : nous devons saisir le nom de l'hôte pour lequel nous souhaitons générer un rapport, son adresse IP ou l'adresse d'un réseau. Nous pouvons seulement consulter ce rapport.

## IV.6 Test de la génération des rapports



Figure IV.15 – Rapport sur un hôte

- **Rapport sur la disponibilité** : si nous disposons de plusieurs sondes dans notre architecture, nous devons choisir une. Nous avons seulement la possibilité de consulter ce rapport.
- **Rapport du Business et de conformité ISO PCI** :

Business & Compliance ISO PCI Report

Title Page

Threat overview

Business real impact risks

C.I.A Potential impact

PCI-DSS 2.0

PCI-DSS 3.0

Trends

ISO27002 Potential impact

ISO27001

Date Range

2017-04-12 - 2017-05-12

[Download PDF](#)

[Send by e-mail](#)

Figure IV.16 – Rapport du Business et de conformité ISO PCI

- **Rapport géographique** :

Geographic Report

Title Page

Date Range

2017-04-12 - 2017-05-12

[Download PDF](#)

[Send by e-mail](#)

Figure IV.17 – Rapport géographique

- **Rapport sur les évènements SIEM** :

SIEM Events +

Title Page

Top 10 Attacker Host

Top 10 Attacked Host

Top 10 Used Ports

Top 15 Events

Top 15 Events by Risk

Date Range

2017-04-12 - 2017-05-12

[Download PDF](#)

[Send by e-mail](#)

Figure IV.18 – Rapport sur les évènements SIEM

- **Rapport sur les Menaces et la Base de données des vulnérabilités** :

Figure IV.19 – Rapport sur les Menaces et les vulnérabilités

## IV.6 Test de la génération des rapports

- Rapport sur le statut des tickets :

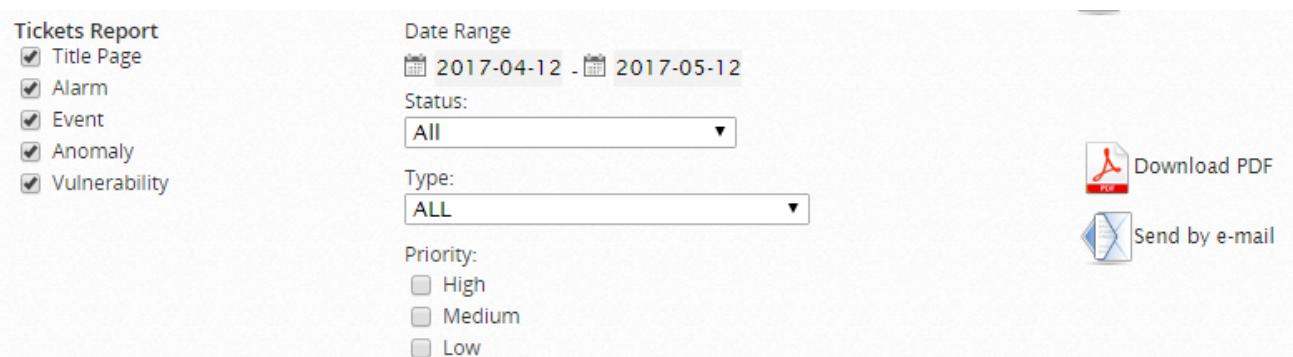


Tickets Status

[View Report](#)

Figure IV.20 – Rapport sur le statut des tickets

- Rapport sur les tickets : nous pouvons choisir le statut, le type et la priorité des tickets à générer leur rapport.



Tickets Report

Date Range: 2017-04-12 - 2017-05-12

Status: All

Type: ALL

Priority: High, Medium, Low

[Download PDF](#)

[Send by e-mail](#)

Figure IV.21 – Rapport sur les tickets

- Rapport sur l'activité d'un utilisateur : nous choisissons tout d'abord l'utilisateur que nous avons besoin de consulter son rapport d'activités et une action parmi la liste proposée. Nous pouvons choisir toutes les actions.



User Activity Report

User: admin

Action: All

[View Report](#)

Figure IV.22 – Rapport sur l'activité d'un utilisateur

Ci-dessous est un extrait de ce rapport :

## IV.6 Test de la génération des rapports

MY PROFILE		CURRENT SESSIONS		USER ACTIVITY	
USER ACTIVITY FILTER					
Date range		User		Action	
<input type="button" value="2017-04-12"/>	-	<input type="button" value="2017-05-12"/>	User	admin ▾	All <input type="button" value="View"/>
Date	User	Source IP	Code	Action	
2017-05-12 11:19:25	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:19:24	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:19:23	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:19:19	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:19:18	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:19:16	admin	172.18.	19	Reports - PDF report generated	
2017-05-12 11:00:01	admin	172.18.	46	Policy - Policy: new policy added BEA992AEE536BDED6302ABD431E85CCD (SSH Brute Force Attack Policy)	
2017-05-12 10:47:37	admin	172.18.	82	Policy & Actions - Actions: New action added 3 (Tester la nouvelle directive SSH Brute Force Attack##@##admin)	
2017-05-12 10:20:46	admin	172.18.	2	User admin logged out	
2017-05-12 10:19:52	admin	172.18.	1	User admin logged in	
2017-05-12 10:08:48	admin	172.18.	50	Reports - Ticket added to 11	
2017-05-12 10:01:07	admin	172.18.	50	Reports - Ticket added to 11	
2017-05-12 09:46:33	admin	172.18.	1	User admin logged in	
2017-05-10 13:50:30	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-10 13:12:16	admin	172.18.	1	User admin logged in	
2017-05-10 13:11:52	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-10 12:39:22	admin	172.18.	1	User admin logged in	
2017-05-10 12:39:10	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-10 11:23:30	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-10 10:26:35	admin	172.18.	90	Cross Correlation - Rules: new rule added plugin id: 1001, plugin sid: 3668, reference id: 3001, reference sid: 12639	
2017-05-10 09:50:53	admin	172.18.	1	User admin logged in	
2017-05-10 09:48:51	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-10 09:22:38	admin	172.18.	1	User admin logged in	
2017-05-10 08:37:46	admin	172.18.	2	User admin logged out - Timeout expired	
2017-05-09 14:24:00	admin	172.18.	48	Policy - Policy: policy 4798465BD6924ECB8AB83593B5085C63 (Test Marwa) modified	
2017-05-09 14:23:21	admin	172.18.	82	Policy & Actions - Actions: New action added 3 (simpple test##@##admin)	
2017-05-09 14:21:39	admin	172.18.	48	Policy - Policy: policy 4798465BD6924ECB8AB83593B5085C63 (Test Marwa) modified	

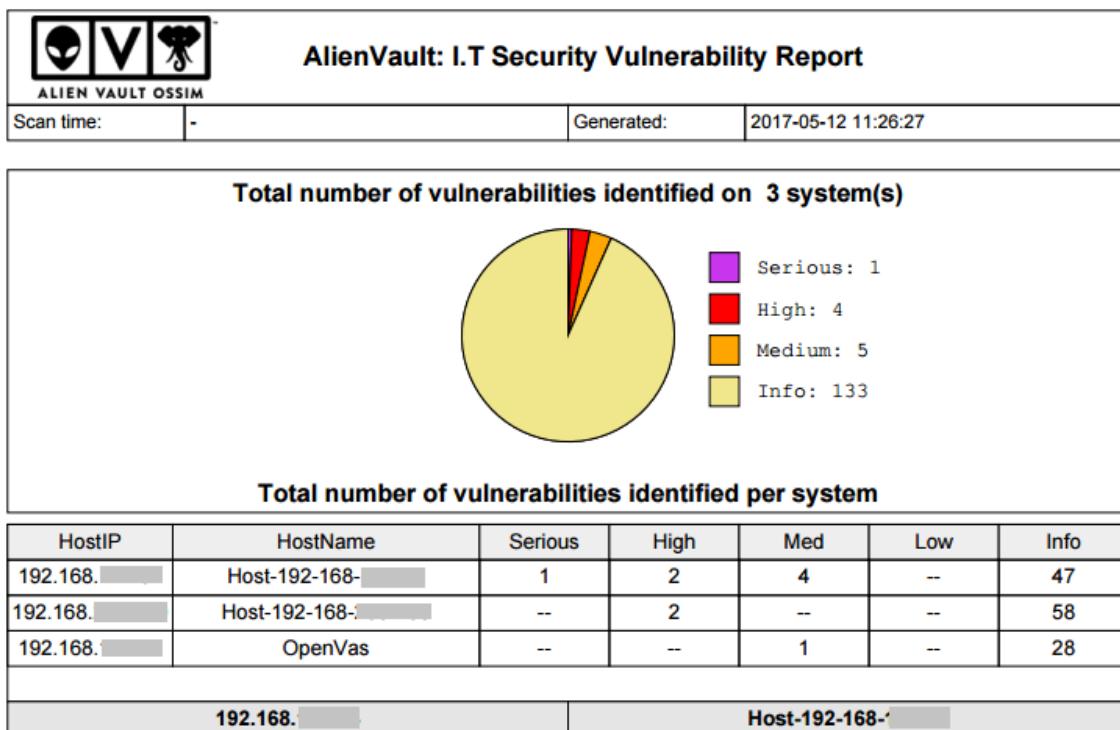
**Figure IV.23 – Extrait du rapport sur l'activité d'un utilisateur**

### — Rapport sur les vulnérabilités :



**Figure IV.24 – Rapport sur les vulnérabilités**

Si nous cliquons sur View Report nous obtenons les informations suivantes :



**Figure IV.25** – Rapport de vulnérabilité de sécurité

Ce rapport fournit des statistiques sur les vulnérabilités identifiées sur le système. Il offre des informations détaillées sur les adresses IP et les noms des hôtes sur lesquels des vulnérabilités ont été détectées. Nous aurons aussi des informations sur le nombre de vulnérabilités classées par degré de严重性 (serious, high, medium ou info).

## 7 Backup

Les données enregistrées au niveau de notre plateforme représentent un actif très important pour notre entreprise. Or, ces événements sont enregistrés pour une période de temps spécifié par l'utilisateur, cette valeur est appelée "Active Netflow Window", au-delà de cette période les événements seront supprimés du Framework et ne sont plus accessibles que sur le disque dur du serveur.

### Configuration des paramètres de Backup

Le serveur SIEM stocke les événements reçus dans une base de données dédiée Backup-DB. Pour configurer les paramètres de Backup, nous accédons à "**Configuration→Administration→Main**". Nous devons tout d'abord activer la sauvegarde de la base de données SIEM, puis définir le nombre de fichiers de backup à garder dans le système, ainsi que le nombre d'événements à

## IV.7 Backup

stocker et le nombre de jours à garder ces données. Nous configurons aussi l'heure de début de sauvegarde au format "HH :MM" ainsi que plusieurs autres paramètres qui sont illustrés par la figure IV.26 :

The screenshot shows a configuration interface for 'Backup'. The top bar has a 'BACKUP' tab. Below it, the title is 'Backup configuration: backup database, directory, interval'. The configuration includes the following fields:

- Enable SIEM database backup:** Yes (dropdown)
- Number of Backup files to keep in the filesystem:** 5
- Events to keep in the Database (Number of days):** 5
- Events to keep in the Database (Number of events):** 4000000
- Backup start time:** 01:00
- Active Netflow Window:** 45
- Alarms Expire:** No (dropdown)
- Alarms Lifetime:** 0
- Logger Expiration:** No (dropdown)
- Active Logger Window:** 0
- Password to encrypt backup files:** ..... (redacted)

Each field has a detailed tooltip explaining its function.

Figure IV.26 – Configuration du backup

Après la configuration des paramètres nécessaires nous accèdons à l'interface de gestion de backup "**Configuration→Administration→Backups**", dans cette zone nous aurons un accès au "Backup manager" qui nous permet de consulter les sauvegardes déjà effectuées, de restaurer ou de supprimer une ancienne sauvegarde et d'afficher l'historique des opérations effectuées sur les fichiers de backup. La figure IV.27 illustre un exemple de l'historique des fichiers de backup :

## **IV.7 Backup**

VIEW BACKUP LOGS				
Showing the latest <input type="button" value="100 ▾"/> logs				
Date	Backup Type	Status	All	Message
2017-05-24 10:12:27	Events	INFO	Restoring	
2017-05-24 10:11:45	Events	INFO	status	
2017-05-24 07:00:33	Configuration	INFO	Backups rotated successfully	
2017-05-24 07:00:33	Configuration	INFO	Backup successfully made [127.0.0.1 - configuration]	
2017-05-24 07:00:00	Configuration	INFO	Running Backup [127.0.0.1 - configuration]	
2017-05-24 01:32:41	Events	INFO	Running delete: CALL alienVault_siem.fill_tables('1900-01-01 00:00:00', '2017-05-24 00:00:00')	
2017-05-24 01:32:41	Events	INFO	Running delete: DELETE FROM alienVault_siem.po_acid_event WHERE timestamp <= '2017-05-23 01:28:57';	
2017-05-24 01:32:41	Events	INFO	Running delete: DELETE FROM alienVault_siem.ac_acid_event WHERE timestamp <= '2017-05-23 01:28:57';	
2017-05-24 01:32:41	Events	INFO	Running delete: DROP TABLE alienVault_siem.backup_delete_temporal;	
2017-05-24 01:32:41	Events	INFO	Running delete: DROP TABLE alienVault_siem.backup_delete_memory;	

**Figure IV.27** – Exemple d'historique des opérations effectuées sur les fichiers de backup

## **Conclusion :**

Dans ce chapitre, nous avons testé les différentes fonctionnalités de notre plateforme. Après la réussite de ces tests, nous pouvons valider les objectifs atteints avec l'entreprise. Nous mentionnons aussi que la plateforme OSSIM a encore les capacités d'implémenter de nouvelles fonctionnalités, en effet l'extension de l'architecture, l'ajout d'autres sondes ou encore l'intégration d'autres équipements étrangers est toujours possible selon les besoins futurs de l'entreprise.

---

# Conclusion générale et perspectives

L’élévation de niveau de sécurité de l’infrastructure informatique est devenue un enjeu encore plus important pour les entreprises. C’est pour cette raison que l’OACA a décidé de mettre en place son propre centre d’opérations de sécurité (SOC).

Pour ce faire, nous avons respecté trois étapes qui sont :

- Identification et mise en place d’une équipe dédiée (Staff SOC),
- Définition d’un process de gestion des incidents,
- Implémentation d’une technologie de supervision des événements du système d’information.

Au cours de la première et la deuxième étape, nous avons effectué une étude théorique en étudiant l’existant et en se basant sur des référentiels de sécurité comme le NIST (National Institute of Standards and Technology) afin de définir un staff SOC et une procédure de gestion des incidents bien spécifiques aux besoins de notre entreprise.

Quant au volet technologie, nous avons eu recours à une solution SIEM open source qui s’adapte à l’infrastructure existante. Cette infrastructure, et malgré qu’elle offrait un certain niveau de sécurité, manquait d’harmonie entre ses composantes. Au cours de ce projet, nous avons essayé de créer cette harmonie en mettant en place la pièce maîtresse qui va gérer toutes les composants en introduisant un aspect d’intelligence dans le traitement et permettant d’améliorer le rendement de toute l’architecture.

Nous avons entamé notre projet par une étude comparative des solutions SIEM présentes sur le marché, par la suite et en se basant sur les attentes et besoins de l’entreprise, nous avons opté pour la solution open source OSSIM. Après une étude globale de la solution et de son architecture logique, on a présenté une conception de sa mise en place. Ensuite nous avons installé les différentes composantes de l’architecture. Puis, nous avons intégré les systèmes externes nécessaires. Enfin, nous avons tout validé par une série de tests et de scénarios d’exploitation des fonctionnalités de la plateforme.

Ce projet nous a permis de consolider nos connaissances en matière de sécurité informatique et d’approfondir nos connaissances pratiques pour savoir résoudre les difficultés rencontrées surtout au niveau de l’intégration de la solution.

En guise de perspective, nous proposons de :

- Intégrer d’autres équipements à l’architecture de l’OACA et faire une extension du champ de contrôle réseau, tout en adaptant la politique de sécurité aux besoins futurs de l’entreprise.
- Étendre les fonctionnalités d’envoi d’alerte en intégrant un système de notification par SMS surtout pour les alertes graves de type intrusion et prise de contrôle d’une machine ou encore accès interdit aux équipements critiques.
- Renforcer la sécurité de la plateforme.

---

# Bibliographie

- [1] Site officiel de l'oaca. <http://www.oaca.nat.tn/index.php?id=673>. [Consulté le 1-Avril-2017]. 3, 4, 5
- [2] Introduction à mpls. <http://www.nolot.eu/Download/Cours/reseaux/m2pro/WAN0809/MPLS.pdf>. [Consulté le 23-Mai-2017]. 6
- [3] Siem, une vision centralisée de la sécurité. <https://blog.e-expertsolutions.com/siem/>. [Consulté le 27-Avril-2017]. 10
- [4] DR ANTON CHUVAKIN. *Le livre blanc : Le guide complet de la gestion des logs et événements*. Net IQ (2016). 12
- [5] Ibm security qradar siem. <http://www-03.ibm.com/software/products/fr/qradar-siem>. [Consulté le 04-Avril-2017]. 12
- [6] Site officiel de splunk. [https://www.splunk.com/fr\\_fr](https://www.splunk.com/fr_fr). [Consulté le 26-Mai-2017]. 13
- [7] Critical capabilities for security information and event management. <https://www.gartner.com/doc/reprints?id=1-2Q17LAL&ct=151019&st=sb>. [Consulté le 04-Avril-2017]. 13
- [8] Hpe security arcsight esm. <https://saas.hpe.com/fr-fr/software/siem-security-information-event-management>. [Consulté le 26-Mai-2017]. 13
- [9] AlienVault ossim :the world's most widely used open source siem. <https://www.alienvault.com/products/ossim>. [Consulté le 17-Mai-2017]. 14, 17, 37
- [10] Site officiel d'usm. <https://www.alienvault.com/>. [Consulté le 26-Mai-2017]. 14
- [11] Gartner. <http://www.encyclopedie.fr/definition/Gartner>. [Consulté le 04-Avril-2017]. 14
- [12] Rapport gartner 2016. <https://www.gartner.com/doc/reprints?id=1-2JM104C&ct=150720&st=sb>. [Consulté le 03-Avril-2017]. 15
- [13] An introduction to the elk stack. <https://www.elastic.co/webinars/introduction-elk-stack>. [Consulté le 24-Mai-2017]. 16
- [14] Enterprise log search and archive. <https://github.com/mcholste/elsa>. [Consulté le 24-Mai-2017]. 16

## Bibliographie

---

- [15] Graylog : centraliser vos logs. <https://www.graylog.fr/>. [Consulté le 24-Mai-2017]. 17
- [16] Alienvault installation guide. [https://scadahacker.com/library/Documents/Manuals/AlienVault\\_Installation\\_Guide.pdf](https://scadahacker.com/library/Documents/Manuals/AlienVault_Installation_Guide.pdf). [Consulté le 08-Mai-2017]. 24
- [17] Sec401 :sans security essentials bootcamp style. <http://www.coseinc.com/sans-secure-singapore-2010/docs/61.pdf>. [Consulté le 08-Mai-2017]. 27
- [18] Sec501 : Advanced security essentials - enterprise defender. <https://www.sans.org/course/advanced-security-essentials-enterprise-defender>. [Consulté le 08-Mai-2017]. 27
- [19] Sec503 : Intrusion detection in-depth. <https://www.sans.org/event-downloads/40917/Sec503.pdf>. [Consulté le 08-Mai-2017]. 27
- [20] Sec504 :hacker techniques, exploits, and incident handling. <https://www.sans.org/brochure/course/hacker-techniques-exploits-incident-handling/41>. [Consulté le 08-Mai-2017]. 27
- [21] Sec561 : Intense hands-on pen testing skill development. <https://www.sans.org/brochure/course/immersive-hands-on-hacking-techniques/1497>. [Consulté le 08-Mai-2017]. 27
- [22] For610 : Reverse-engineering malware : Malware analysis tools and techniques. <https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques>. [Consulté le 08-Mai-2017]. 27
- [23] Certified information systems security professional. [https://www.isc2.org/uploadedfiles/credentials\\_and\\_certification/cissp\\_cissp-information.pdf](https://www.isc2.org/uploadedfiles/credentials_and_certification/cissp_cissp-information.pdf). [Consulté le 08-Mai-2017]. 27
- [24] Certified information systems auditor. <http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx>. [Consulté le 08-Mai-2017]. 27
- [25] Certified information security manager. <http://harmony.co.ke/syllabus/CISM.pdf>. [Consulté le 08-Mai-2017]. 27
- [26] Certified in the governance of enterprise it. [http://raw.rutgers.edu/docs/wcars/20wcars/ISACA/CONTECSI/CGEIT\\_BOI\\_June\\_11\\_23.pdf](http://raw.rutgers.edu/docs/wcars/20wcars/ISACA/CONTECSI/CGEIT_BOI_June_11_23.pdf). [Consulté le 08-Mai-2017]. 27
- [27] TIMGRANCE KAREN SCARFONE PAUL CICHONSKI, TOM MILLAR. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology.* (2012). 28

## Bibliographie

---

- [28] Winscp. [http://filehippo.com/fr/download\\_winscp/](http://filehippo.com/fr/download_winscp/). [Consulté le 17-Mai-2017]. 37
- [29] Putty. <http://www.putty.org/>. [Consulté le 17-Mai-2017]. 37
- [30] Vmware esxi. <http://www.vmware.com/fr/products/esxi-and-esx.html>. [Consulté le 17-Mai-2017]. 37
- [31] Documentation vmware vsphere 6.0. <https://pubs.vmware.com/vsphere-60/index.jsp>. [Consulté le 17-Mai-2017]. 37
- [32] Se connecter à un autre ordinateur à l'aide de connexion bureau à distance. <https://support.microsoft.com/fr-fr/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection>. [Consulté le 17-Mai-2017]. 37
- [33] Wmi. [https://msdn.microsoft.com/en-us/library/aa384642\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa384642(v=vs.85).aspx). [Consulté le 17-Mai-2017]. 40
- [34] Ossec open source hids security. <https://ossec.github.io/>. [Consulté le 17-Mai-2017]. 40
- [35] Snare. <https://www.intersectalliance.com/our-product/>. [Consulté le 17-Mai-2017]. 42
- [36] Nagios. <https://www.monitoring-fr.org/solutions/nagios/>. [Consulté le 17-Mai-2017]. 47
- [37] AlienVault documentation : Firewall permissions. <https://www.alienvault.com/documentation/usm-appliance/sys-reqs/firewall-permissions.htm>. [Consulté le 26-Mai-2017]. 50
- [38] Certificate authority (ca). <http://searchsecurity.techtarget.com/definition/certificate-authority>. [Consulté le 26-Mai-2017]. 51
- [39] Ldap : Définition. <http://searchmobilecomputing.techtarget.com/definition/LDAP>. [Consulté le 26-Mai-2017]. 55
- [40] Documentation officielle - notion des tickets. <https://www.alienvault.com/documentation/usm-appliance/kb/2016/01/alienVault-ticketing-system.htm>. [Consulté le 26-Mai-2017]. 67
- [41] Download ossec. <https://ossec.github.io/downloads.html>. [Consulté le 06-Mars-2017]. 91

---

# Annexe A : Installation et configuration d'OSSIM

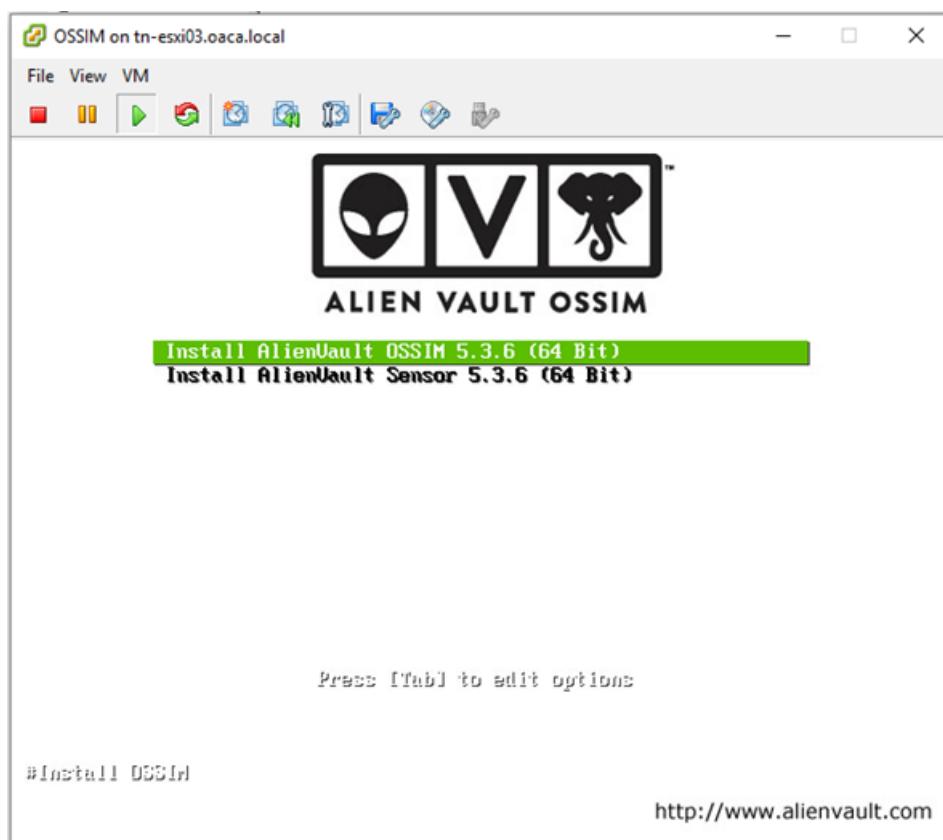
## Installation d'OSSIM

Comme nous avons mentionné dans le chapitre II OSSIM est composé de quatre profils : serveur, Framework, base de données et sonde. En fonction du rôle du nouvel hôte dans le déploiement AlienVault, il est possible de configurer le profil utilisé. Cela peut être configuré pendant le processus d'installation ou après l'installation. Par défaut, l'installation automatique active tous les profils dans la même machine.

Dans notre cas, nous choisissons le mode d'installation automatique.

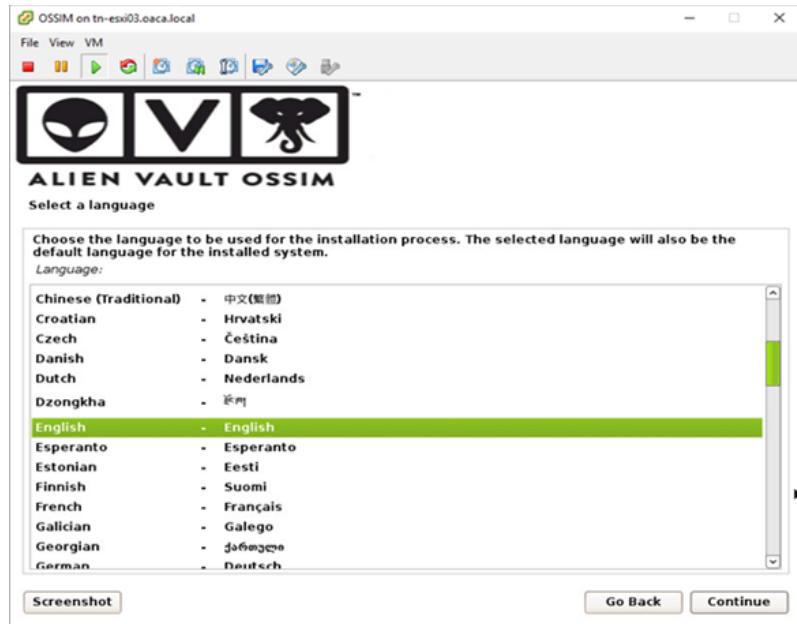
Dans ce qui suit, nous détaillons les différentes étapes d'installation d'OSSIM :

- Nous commençons par choisir l'option "Install AlienVault OSSIM"



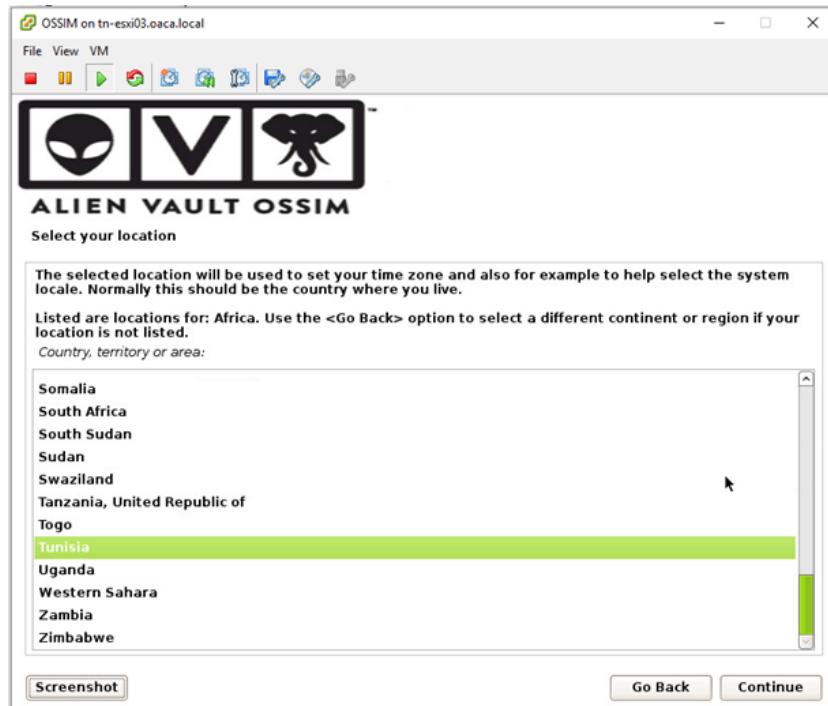
**Figure A.1** – Choix de l'option "Install AlienVault OSSIM"

- Nous choisissons la langue à utiliser pendant le processus d'installation et elle sera également la langue par défaut du système installé



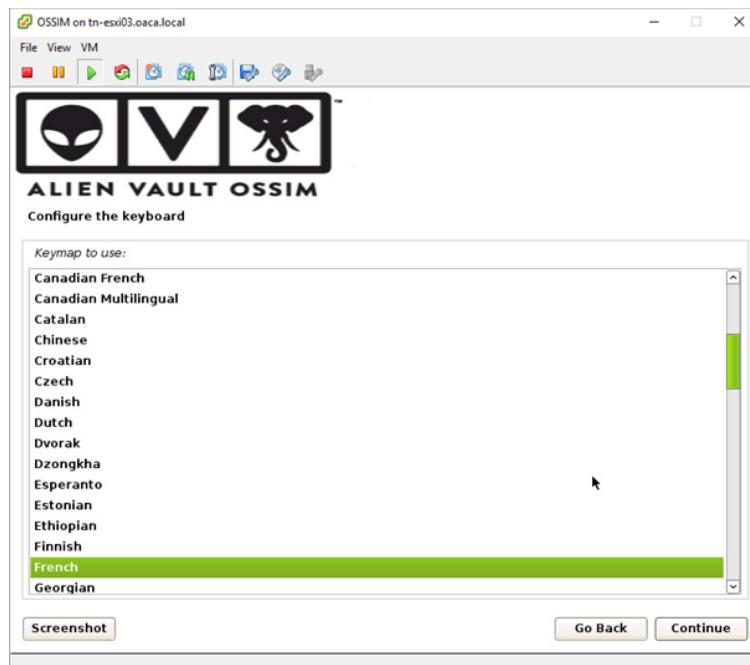
**Figure A.2** – Choix de la langue d’OSSIM

— Nous choisissons notre pays



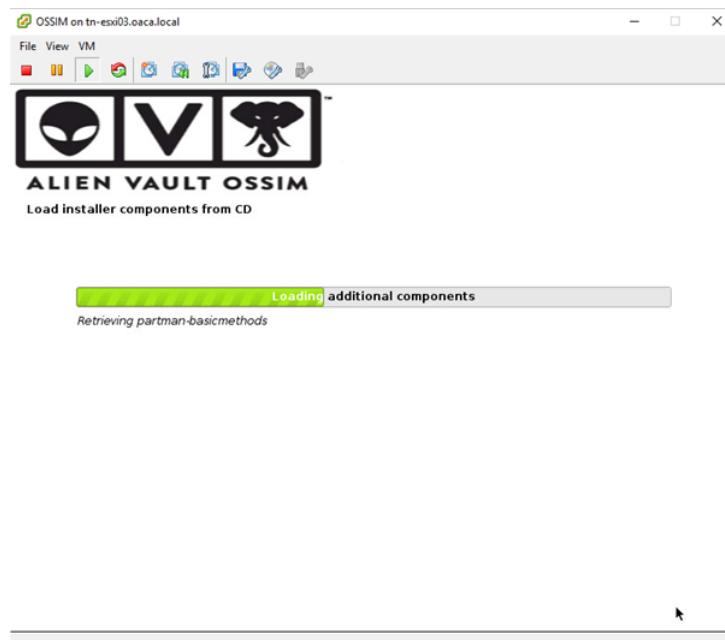
**Figure A.3** – Choix de la localisation

— Nous sélectionnons le clavier que nous utilisons avec notre PC



**Figure A.4** – Choix du clavier

- Maintenant, la configuration va charger les composants nécessaires requis pour l'installation depuis l'image ISO

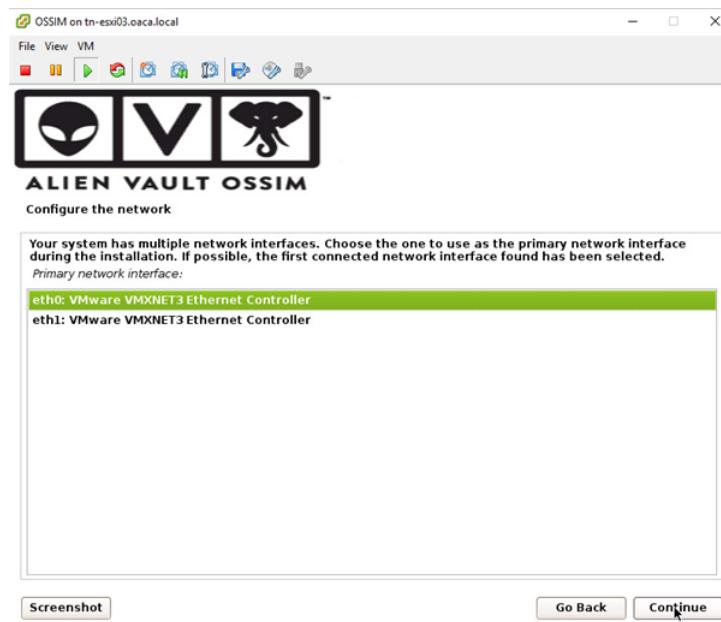


**Figure A.5** – Chargement des composants d'installation

- Nous disposons de plus d'une carte d'interface réseau, comme il est recommandé, donc

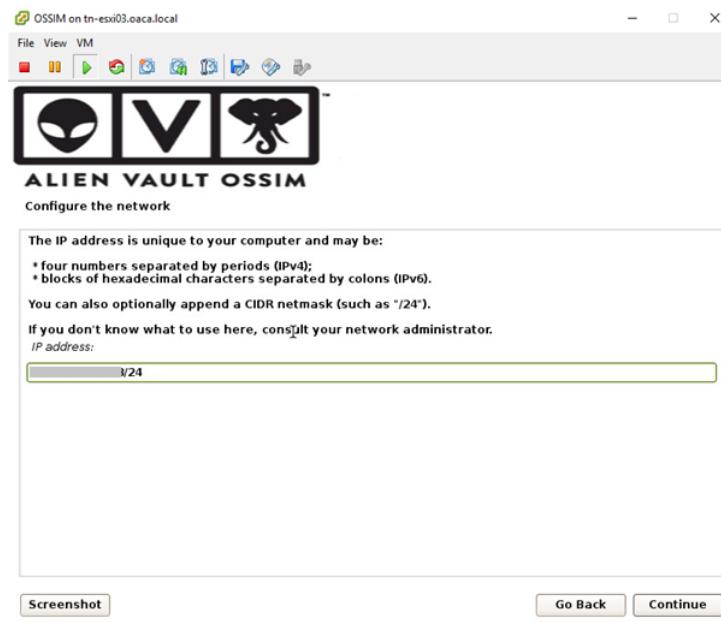
---

nous devons sélectionner l'interface principale à utiliser pour la gestion. L'autre sera configurée ultérieurement.

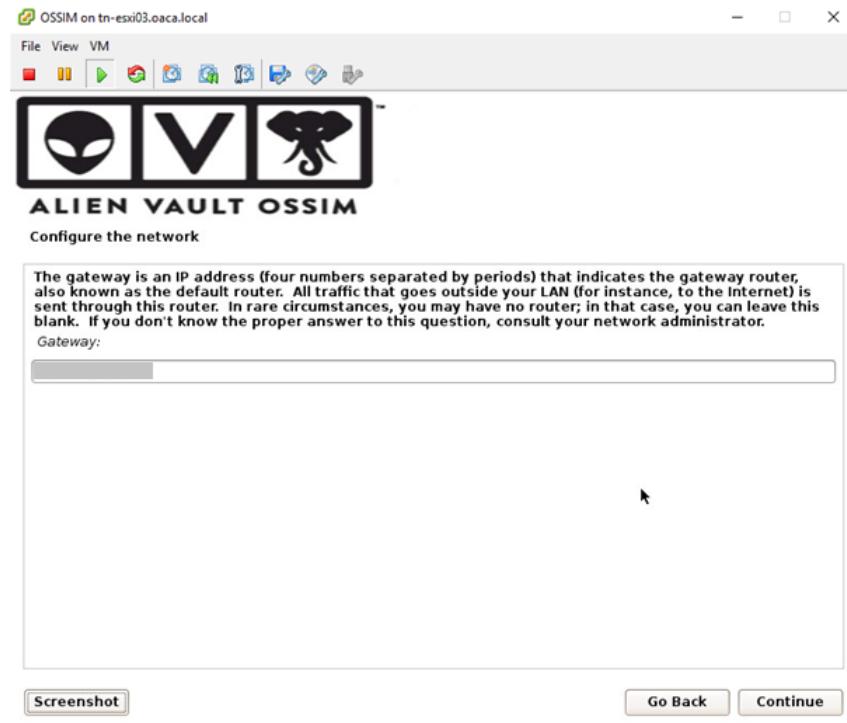


**Figure A.6** – Choix de l'interface de gestion

- L'étape suivante est de fournir une adresse IP pour OSSIM, un masque de sous-réseau, une passerelle par défaut et les adresses IP du serveur DNS, comme indiqué ci-dessous.



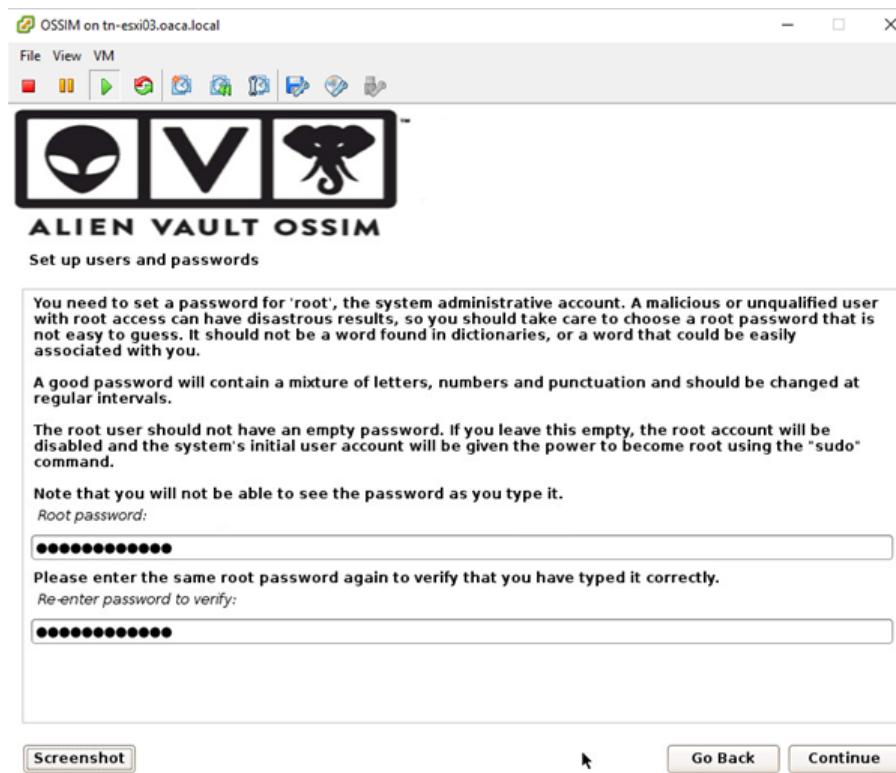
**Figure A.7** – Adresse IP et masque de sous réseau



**Figure A.8** – Adresse de la passerelle par défaut

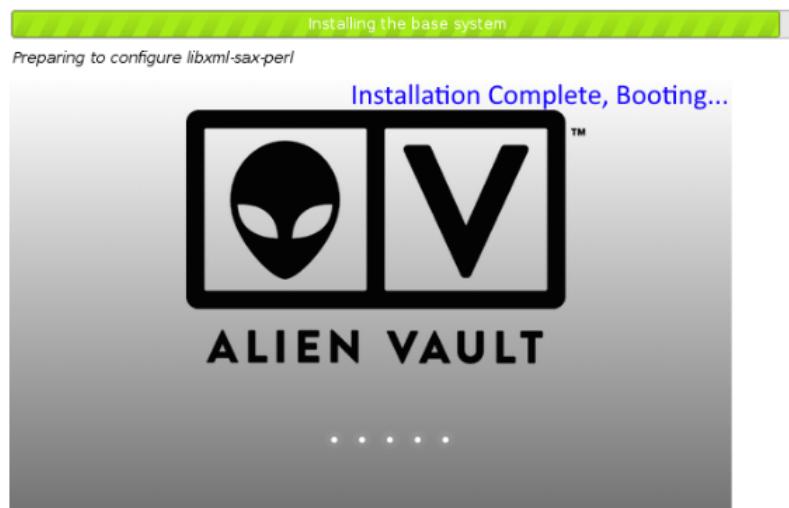
**Figure A.9** – Adresse du serveur DNS

- Nous saisissons ensuite un mot de passe pour l'utilisateur root (l'administrateur de la plateforme)



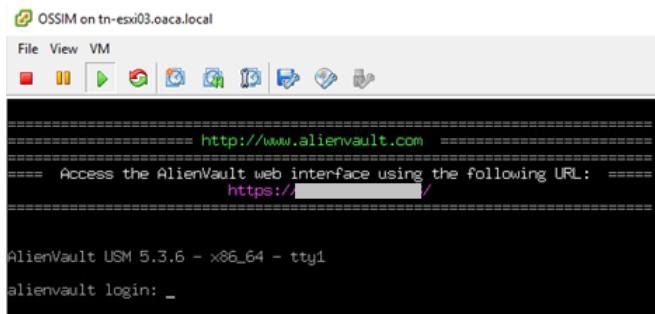
**Figure A.10** – Mot de passe de l'utilisateur "root"

- Maintenant, l'installation d'OSSIM débutera et durera longtemps



**Figure A.11** – Installation d'OSSIM

- Lorsque l'installation est terminée, OSSIM redémarrera automatiquement et affichera l'écran suivant qui indique l'adresse IP pour accéder à l'interface Web



**Figure A.12 – La console d’OSSIM**

**Configuration d’OSSIM** Nous accédons à OSSIM dans le navigateur Web avec l’adresse IP affichée dans la console et nous démarrons l’assistant de configuration en cliquant sur le bouton "Start".

Nous commençons par configurer les interfaces réseaux. Dans le cas de plusieurs interfaces réseau, OSSIM demandera à affecter une fonctionnalité à chaque interface, sauf la première (qui est par défaut assignée à sa gestion).

Si nous sélectionnons n’importe quelle interface comme "Log Collection and Scanning", OSSIM demandera l’adresse IP et le sous-réseau pour affecter à cette interface pour la saisie des journaux et du périmètre de numérisation.

The screenshot shows the 'Configure Network Interfaces' page of the AlienVault OSSIM web interface. On the left, there is a sidebar with a 'Let's Get Started' section containing five numbered steps: 1. NETWORK INTERFACES (selected), 2. ASSET DISCOVERY, 3. DEPLOY HIDS, 4. LOG MANAGEMENT, and 5. JOIN OTX. The main content area is titled 'Configure Network Interfaces' and contains the following information:

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	[REDACTED]	-
eth1	Log Collection & Scanning	[REDACTED]	-

**Information**

- Management: The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- Network Monitoring: Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See [Instructions](#) on how to setup a network tap or span.
- Log Collection & Scanning: Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- Not in Use: Use this option if you do not want to use one of the network interfaces.

**Figure A.13 – Configuration des interfaces réseaux**

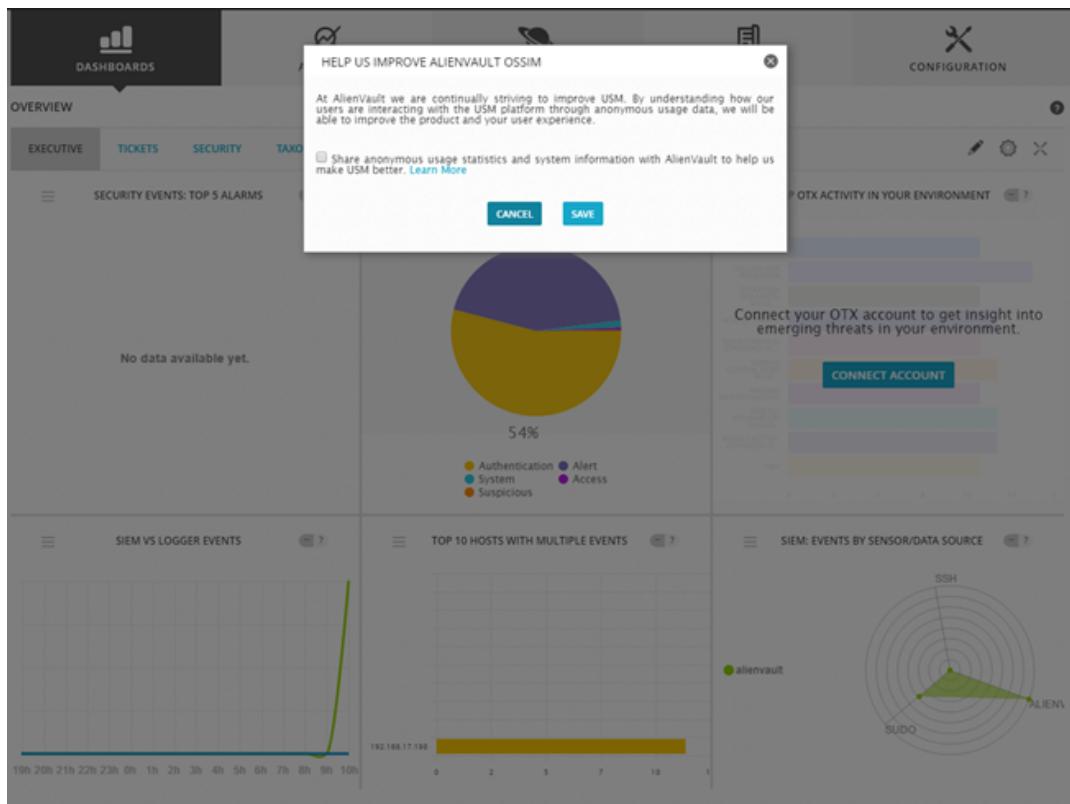
Sur l’écran suivant de "Asset Discovery", OSSIM recherchera automatiquement les hôtes disponibles sur le réseau. Nous pouvons ré-analyser ou ajouter manuellement un hôte individuellement ou utiliser un fichier CSV.

Sur l'écran suivant, OSSIM nous demandera si nous voulons installer des HIDS sur l'hôte scanné, (cela ne montrera que les hôtes Windows et Linux que nous avons sélectionnés dans l'écran "Asset Discovery"). Il demandera un utilisateur privilégié et un mot de passe pour le déploiement de HIDS.

OSSIM demandera ensuite les modèles de logs et les versions des périphériques déjà sélectionnés comme "Network Device" dans l'écran de "Asset Discovery".

Sur l'écran suivant de "Join OTX" OSSIM demandera le jeton d'enregistrement OTX (Open Threat Exchange). L'inscription est gratuite, et il est nécessaire de mettre à jour automatiquement les dernières signatures de menaces. Cependant, pour des raisons de sécurité, nous choisissons d'ignorer cette étape. Nous cliquons sur "Skip" pour terminer cet assistant de configuration.

OSSIM est donc installé et bien configuré. Maintenant, nous pouvons parcourir le tableau de bord OSSIM comme indiqué ci-dessous et nous pouvons poursuivre sa configuration ultérieurement.



**Figure A.14** – Tableau de bord d'OSSIM

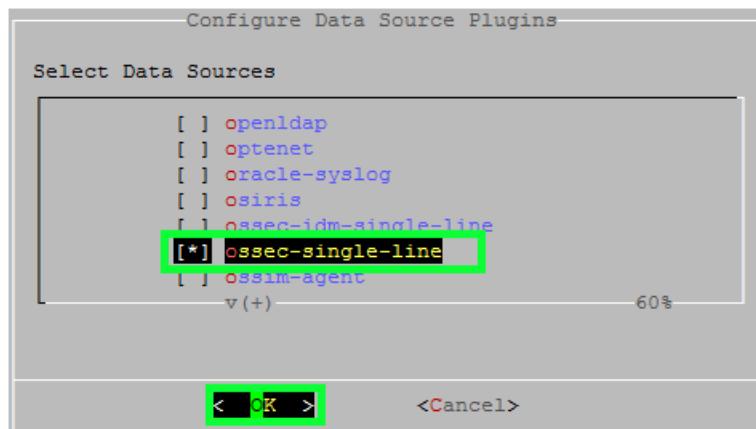
---

# Annexe B : Installation d'OSSEC sous Windows et Linux

Dans cette annexe, nous allons installer les agents OSSEC sur les machines client Windows et Linux pour être surveillées par OSSIM. Pour configurer les clients OSSEC avec OSSIM, nous avons besoin que l'agent OSSEC soit téléchargé et installé sur les hôtes, mais d'abord, nous allons activer le plugin OSSEC au niveau du serveur. **Activation du plugin OSSEC**

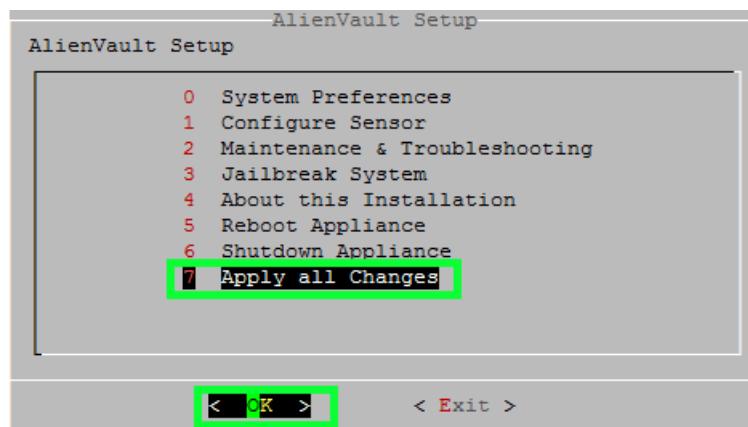
Nous pouvons activer un plugin au niveau du serveur d'OSSIM par deux méthodes différentes :

- **En utilisant l'interface web** : nous accédons à Configuration>Deployment>Sensor>Configuration et on active le plugin "ossec-single-line"
- **En utilisant la console** : nous suivons ces étapes :
  - Accéder à : Configure Sensor>Configure Data Source Plugins>Sélectionner "ossec-single-line">cliquer sur OK,



**Figure B.1** – Activation du plugin OSSEC

- Pour enregistrer ces modifications, nous revenons à l'écran principal, sélectionnons "Apply all changes" et cliquons sur OK,



**Figure B.2 – Enregistrement de la modification**

### Génération des clés client OSSEC

En utilisant la console d'OSSIM, nous accédons à «/var/ossec/bin/manage\_agents» :

- Nous tapons "A" pour ajouter un nouvel agent OSSEC,
- Nous fournissons les informations requises à savoir le nom de l'agent, son adresse IP et son identifiant,
- Nous Appuyons sur "y" pour sauvegarder les informations du client,

```
*****
* OSSEC HIDS v2.8 Agent manager.      *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: A

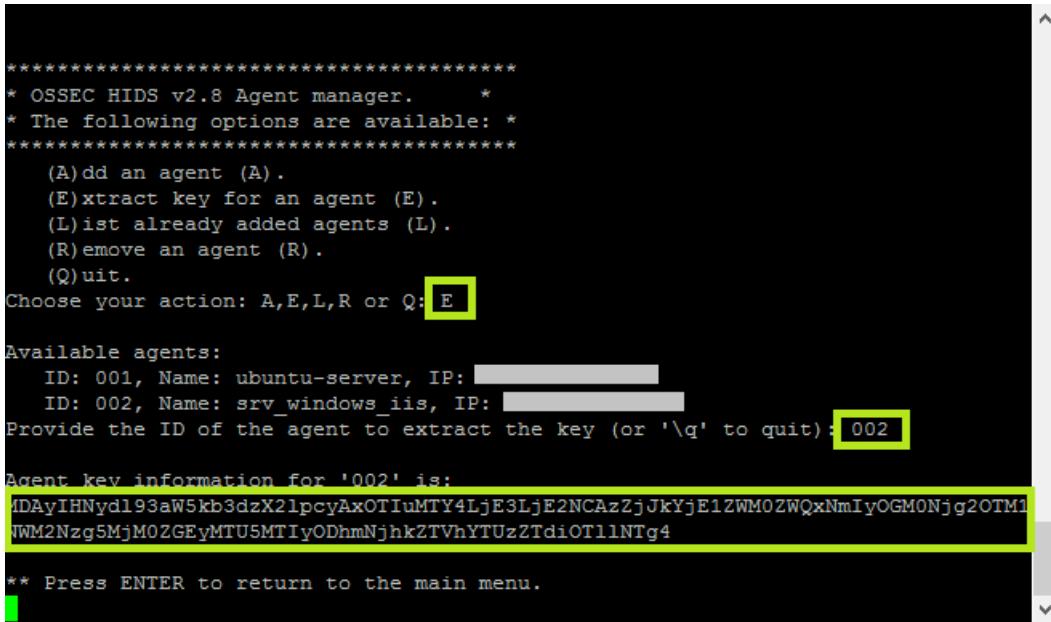
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: srv_windows_iis
* The IP Address of the new agent: [REDACTED]
* An ID for the new agent[002]:
Agent information:
ID:002
Name:srv_windows_iis
IP Address:[REDACTED]

Confirm adding it?(y/n): y
Agent added.
```

**Figure B.3 – Ajout d'un nouvel agent OSSEC**

Maintenant, nous extrayons la clé du client en entrant à nouveau la commande suivante :  
/var/ossec/bin/manage\_agents

- 
- Nous tapons “E” pour extraire la clé du client,
  - Nous saisissons l’ID du client,
  - Nous copions la clé extraite comme indiqué ci-dessous et quittez.



```
*****
* OSSEC HIDS v2.8 Agent manager.      *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: ubuntu-server, IP: [REDACTED]
  ID: 002, Name: srv_windows_iis, IP: [REDACTED]
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIHNydl93aW5kb3dzX21pcyAxOTIuMTY4LjE3LjE2NCAzZjJkYjE1ZWM0ZWQxNmIyOGM0Njg2OTM1
JWM2Nzg5MjM0ZGEyMTU5MTIyODhmNjhkZTVhYTUzZTdiOTl1NTg4

** Press ENTER to return to the main menu.
```

**Figure B.4** – Extraction de la clé client

Nous redémarrons le service «OSSEC Control» en exécutant la commande «/var/ossec/bin/ossec-control restart».

#### Installation de l’agent OSSEC sur la machine Windows

Nous téléchargeons tout d’abord la dernière version stable d’OSSEC Agent pour Windows [41].

Nous exécutons le fichier .exe téléchargé pour commencer l’installation. Nous saisissons l’adresse IP du serveur OSSIM et la clé générée et extraite précédemment et cliquons sur «Save».



**Figure B.5** – Configuration de l’agent OSSEC client sous Windows

Nous démarrons maintenant le client OSSEC pour commencer à envoyer des alertes d’intégrité de fichiers au serveur d’OSSIM.

#### Installation de l’agent OSSEC sur la machine Linux

L’acquisition d’un environnement de construction de logiciel de base dépendra de la plate-forme Linux installé pour le déploiement, mais à un minimum, il faudra un compilateur C et des fichiers de base Kernel et LibC. Ceux-ci peuvent être installés via la commande suivante (pour une distribution ubuntu) :

```
sudo apt-get install build-essential
```

L’étape suivante est de télécharger la dernière version disponible d’OSSEC et l’extraire à l’aide de ces deux commandes :

```
wget http://www.ossec.net/files/ossec-hids-2.8.3.tar.gz
tar -xzvf ossec-hids-2.7.tar.gz
```

Nous exécutons le script d’installation sous le répertoire de l’agent OSSEC :

```
cd ossec-hids-2.7
```

```
/bin/bash ./install.sh
```

Nous appuyons sur la touche «Entrée» pour commencer l’installation. Nous sélectionnons «Installation Type» comme «Agent».

```
I- What kind of installation do you want (server, agent, local, hybrid or help)? agent
- Agent(client) installation chosen.
```

**Figure B.6** – Choix du type de l’installation

Nous saisissons le chemin de l’installation du client OSSEC, l’emplacement par défaut est

---

" /var/ossec " :

```
2- Setting up the installation environment.  
- Choose where to install the OSSEC HIDS [/var/ossec]:  
- Installation will be made at /var/ossec .
```

**Figure B.7** – Choix de l'emplacement de l'installation

Nous tapons l'adresse IP du serveur OSSEC :

```
3- Configuring the OSSEC HIDS.  
3.1- What's the IP Address or hostname of the OSSEC HIDS server?: [REDACTED]  
- Adding Server IP [REDACTED]
```

**Figure B.8** – Saisie de l'adresse IP de l'agent serveur OSSEC

Dans les prochaines étapes nous choisissons d'activer la vérification de l'intégrité et la détection de Rootkit.

Ensuite, OSSEC affichera les options configurées :

```
3.5- Setting the configuration to analyze the following logs:  
-- /var/log/messages  
-- /var/log/auth.log  
-- /var/log/syslog  
-- /var/log/mail.info  
-- /var/log/dpkg.log  
- If you want to monitor any other file, just change  
the ossec.conf and add a new localfile entry.  
Any questions about the configuration can be answered  
by visiting us online at http://www.ossec.net .  
--- Press ENTER to continue ---
```

**Figure B.9** – Liste des fichiers logs à analyser par OSSEC

Maintenant, le script de l'installation va commencer l'installation de l'agent OSSEC. L'installation peut prendre quelques minutes, nous appuyons sur «Entrée» pour terminer, lorsque demandé comme indiqué ci-dessous :

```

- Configuration finished properly.

- To start OSSEC HIDS:
  /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
  /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf

Thanks for using the OSSEC HIDS.
If you have any question, suggestion or if you find any bug,
contact us at contact@ossec.net or using our public maillist at
ossec-list@ossec.net
( http://www.ossec.net/main/support/ ).

More information can be found at http://www.ossec.net

-- Press ENTER to finish (maybe more information below). ---

```

**Figure B.10** – Fin de l'installation de l'agent OSSEC sous Linux

### Configuration du client

Tout d'abord, nous générerons la clé client à l'aide des étapes mentionnées précédemment.

Au niveau du client, en tant qu'utilisateur root, nous exécutons la commande suivante pour ajouter la clé de client OSSEC générée pour la communication avec le serveur d'OSSIM et nous tapons "I" : /var/ossec/bin/manage\_agents

```

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MiBiYXN0aw9uIDE5Mj4xNjguMS4wLzI0IDE0ZWZ1YjAyYmRmYmRhODIx
Pmlu5Yza5Y2E4MD1kNTa0MG01Mm1mZndiMzhIZTcvY2VmMjEzNiEmNjVhM2JmODQ=

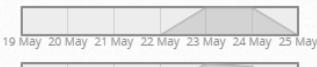
```

**Figure B.11** – Importation de la clé client

Nous confirmons la clé et quittons la console de gestion de l'agent OSSEC en tapant "Q". Ensuite nous redémarrons l'agent OSSEC sur la machine cliente en exécutant la commande suivante : /var/ossec/bin/ossec-control restart

Après avoir configuré les agents OSSEC, il est recommandé de redémarrer l'agent OSSEC sur le serveur d'OSSIM.

OSSEC est bien installé et configuré sur les deux machines Windows et ubuntu. Pour vérifier l'état des ces agents nous accédons à **Environment>Detection**

ID	Agent name	Asset	IP/CIDR	Current IP	Current User	Status	Trend [Time UTC]
001	ubuntu-server	[REDACTED]	192.168	192.168	-	Active	
002	srv_windows_iis	Host	192.168	192.168	-	Active	

**Figure B.12** – Détails des deux agents OSSEC

---

## Annexe C : Création d'une directive de corrélation

Pour créer la directive nous procérons comme suit :

Nous accédons à **Configuration > Threat Intelligence > Directives**, puis nous cliquons sur New. Nous saisissons le nom de la directive «**SSH Brute Force Attack**» ainsi que sa priorité (nous choisissons la valeur 4). Pour la partie Taxonomy, on choisit «Delivery and attack» pour le champ Intent, «Brute force authentication» pour Strategy et «Attack BF» pour Method. La figure C.1 résume ces différents paramètres :

The screenshot shows a configuration dialog for adding a new directive. At the top, it says "Name for the directive" with the value "SSH Brute Force Attack". Below that is a "Taxonomy" section with dropdown menus for "Intent" (set to "Delivery & Attack"), "Strategy" (set to "Bruteforce Authentication"), and "Method" (set to "Attack BF"). Under "Priority", there is a list of numbers from 0 to 5, with the number 4 highlighted by a red rectangle. At the bottom are "Cancel" and "Next" buttons.

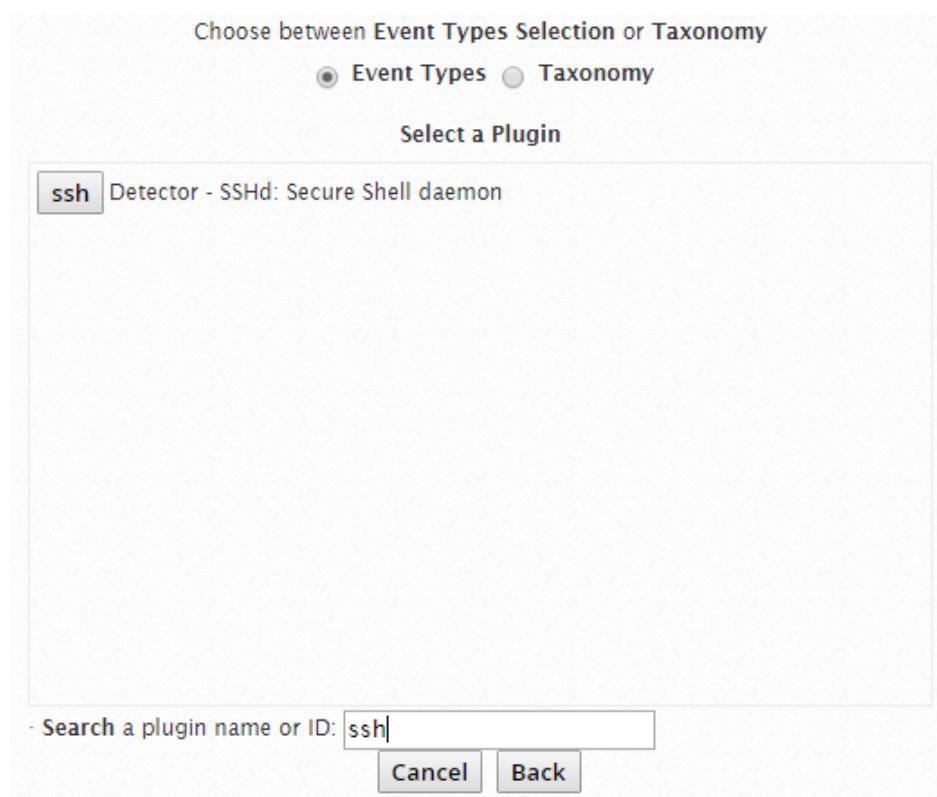
**Figure C.1** – Ajout d'une nouvelle directive

On clique sur «Next». L'étape suivante est de choisir le nom de la règle du premier niveau :

The screenshot shows a configuration dialog for adding a rule level 1. It has a "Name for the rule" field containing "SSH Authentication failure" and "Cancel" and "Next" buttons at the bottom.

**Figure C.2** – Ajout de la règle du premier niveau

Pour le niveau 1 de la directive, chaque règle reste en attente d'un événement du plugin défini, dans notre cas on a choisi le plugin numéro 4003 (SSH detector)



**Figure C.3** – Choix du plugin\_id

Pour le choix des plugins SID on a choisi une liste des événements qui peuvent signifier une tentative d'accès SSH échoué.

La règle de ce niveau se déclenchera dès qu'un événement appartenant à la liste {1,2,3,4,5,6,9,10,12, 13,14,15,16,20} est envoyé par le plugin numéro 4003.

Choose between Event Sub-Types Selection or Taxonomy

Event Sub-Types  Taxonomy

**Plugin Signatures**

14 items selected	Remove all
1 - SSHd: Failed password	-
2 - SSHd: Failed publickey	-
3 - SSHd: Invalid user	-
4 - SSHd: Illegal user	-
5 - SSHd: Root login refused	-
6 - SSHd: User not allowed because listed in DenyUsers	-
9 - SSHd: Bad protocol version identification	-
10 - SSHd: Did not receive identification string	-
12 - SSHd: Authentication refused: bad ownership or modes	-
13 - SSHd: User not allowed because account is locked	-
14 - SSHd: PAM X more authentication failures	-

Add all	
7 - SSHd: Login sucessful, Accepted password	+
8 - SSHd: Login sucessful, Accepted publickey	+
11 - SSHd: Received disconnect	+
17 - SSHd: Server listening	+
18 - SSHd: Server terminated	+
19 - SSHd: Refused connect	+
21 - SSHd: Could not get shadow information	+
22 - SSHd: HPUX Recieved connection - Version	+
23 - SSHd: HPUX Recieved connection - Throughput	+
24 - SSHd: PAM: authentication failure	+
25 - SSHd: PAM: Session Opened	+

· Empty selection means ANY signature

**Cancel** **Back** **Next**

**Figure C.4** – Liste des plugin\_sid

Choose between Event Sub-Types Selection or Taxonomy

Event Sub-Types  Taxonomy

**Plugin Signatures**

14 items selected	Remove all
4 - SSHd: Illegal user	-
5 - SSHd: Root login refused	-
6 - SSHd: User not allowed because listed in DenyUsers	-
9 - SSHd: Bad protocol version identification	-
10 - SSHd: Did not receive identification string	-
12 - SSHd: Authentication refused: bad ownership or modes	-
13 - SSHd: User not allowed because account is locked	-
14 - SSHd: PAM X more authentication failures	-
15 - SSHd: Reverse mapped failed	-
16 - SSHd: Address not mapped	-
20 - SSHd: Denied connection	-

Add all	
7 - SSHd: Login sucessful, Accepted password	+
8 - SSHd: Login sucessful, Accepted publickey	+
11 - SSHd: Received disconnect	+
17 - SSHd: Server listening	+
18 - SSHd: Server terminated	+
19 - SSHd: Refused connect	+
21 - SSHd: Could not get shadow information	+
22 - SSHd: HPUX Recieved connection - Version	+
23 - SSHd: HPUX Recieved connection - Throughput	+
24 - SSHd: PAM: authentication failure	+
25 - SSHd: PAM: Session Opened	+

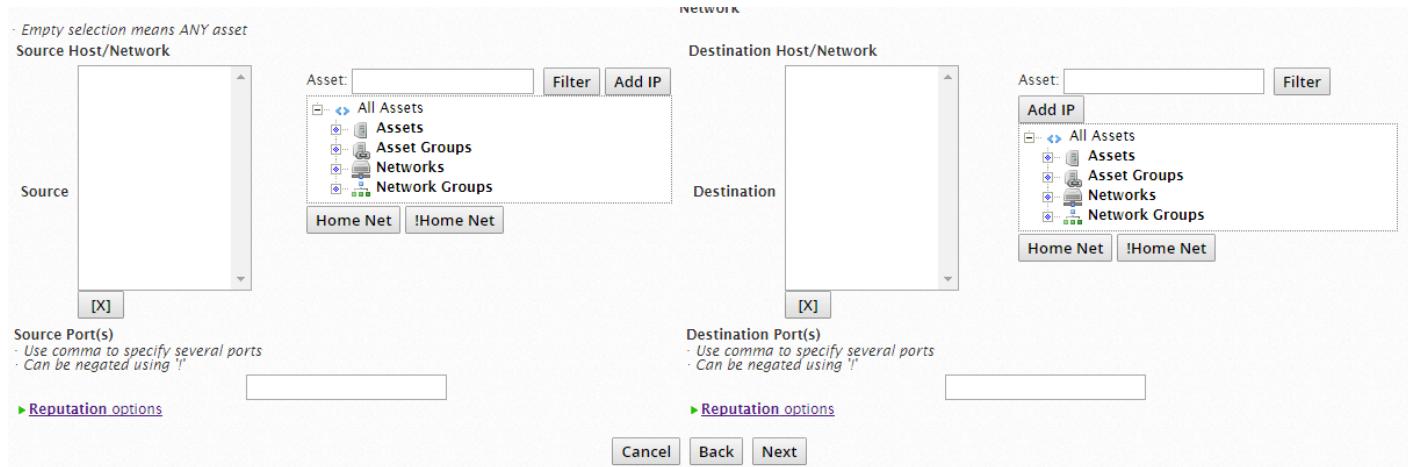
· Empty selection means ANY signature

**Cancel** **Back** **Next**

**Figure C.5** – Suite de la liste des plugin\_sid

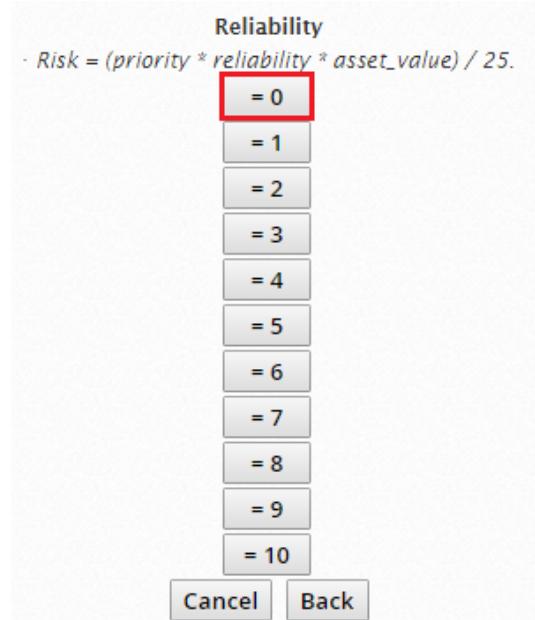
Les adresses IP source et destination ainsi que les ports source et destination auront la

valeur «Any» pour cette directive. Donc on laisse les champs vides et on clique sur «Next»



**Figure C.6** – Configuration des adresses IP et des ports

Le paramètre «reliability» doit avoir la valeur «0» pour garder le risque dans la valeur «0» et éviter de lancer une alerte dès le premier niveau de la directive.



**Figure C.7** – Configuration de la valeur du paramètre "reliability"

Nous cliquons sur «Finish». La directive est ainsi créée avec un seul niveau :

SSH Brute Force Attack											
Delivery & Attack, Bruteforce Authentication, Attack BF - Priority 4											
RULES											
Name	Reliability	Timeout	Occurrence	From	To	Data Source	Event Type	...	[...]	Action	
SSH Authentication failure	0	None	1	◆ ANY	◆ ANY	◆ ssh (4003)	◆ SIDs: 1 2 3 4 5 6 9 10 12 13 14 15 16 20			▶ More	+
▶ DIRECTIVE INFO											

Figure C.8 – Directive avec un seul niveau de corrélation

Pour le reste des niveaux on aura chaque fois à spécifier deux règles :

- **SSH Successful Authentication** : cette règle signifie qu'il ya une connexion réussie après une ou plusieurs connexion échouée. On la crée de la même manière que la première règle mais avec des valeurs différentes pour les paramètres reliability, time\_out et plugin\_sid.
- **SSH authentication failure X times** : cette règle signifie qu'il ya X connexions échouées. On la crée de la même façon que la première règle mais avec des valeurs différentes pour les paramètres : reliability, time\_out et occurrence.

Finalement on obtient :

SSH Brute Force Attack											
Delivery & Attack, Bruteforce Authentication, Attack BF - Priority 4											
RULES											
Name	Reliability	Timeout	Occurrence	From	To	Data Source	Event Type	...	[...]	Action	
Niveau 1	SSH Authentication failure	0	None	1	◆ ANY	◆ ANY	◆ ssh (4003)	◆ SIDs: 1 2 3 4 5 6 9 10 12 13 14 15 16 20		▶ More	+
Niveau 2	SSH Successful Authentication	1	15	1	◆ 1:SRC_IP:1:SRC_PORT	◆ 1:DST_IP:1:DST_PORT	◆ ssh (4003)	◆ SIDs: 7 8		▶ More	...
Niveau 3	SSH Authentication failure 10 times	4	40	10	◆ 1:SRC_IP:1:SRC_PORT	◆ 1:DST_IP:1:DST_PORT	◆ ssh (4003)	◆ SIDs: 1:PLUGIN_SID		▶ More	...
	SSH Successful Authentication	6	100	1	◆ 1:SRC_IP:1:SRC_PORT	◆ 1:DST_IP:1:DST_PORT	◆ ssh (4003)	◆ SIDs: 7 8		▶ More	...
	SSH Authentication failure 100 times	10	400	100	◆ 1:SRC_IP:1:SRC_PORT	◆ 1:DST_IP:1:DST_PORT	◆ ssh (4003)	◆ SIDs: 1:PLUGIN_SID		▶ More	...
	▶ DIRECTIVE INFO										

Figure C.9 – Directive avec ses trois niveaux de corrélation

