CHAPITRE 3 : PRESENTATION DE LA SOLUTION CHOISIE

3.1 Introduction

Dans ce chapitre, nous allons parler de la solution OSSIM, de ses différentes fonctionnalités, de son fonctionnement en interne, expliquer son architecture, de ses limites et avantages.

3.2 Présentation de Alien Vault OSSIM

OSSIM (Open Source Security Information and Management) est une solution open source de sécurité des informations et de gestion des événements(SIEM). Il permet de faire la collecte d'informations provenant de divers fichiers de journalisation au sein d'une entreprise telle que les contrôles de sécurité d'entreprise, les systèmes d'exploitation et les applications. Il convertit les données collectées en format qu'il comprend. Il illustre une mise en œuvre de la cartographie pour améliorer la détection d'intrusions. Son atout principal est que OSSIM n'est qu'un seul outil contenant plusieurs outils open source existants permettant d'avoir une meilleure gestion de la sécurité réseaux. Avec OSSIM il est possible de définir des règles de sécurité relatives à la politique de sécurité adoptée, de connaître la cartographie du réseau et de corréler les différents outils pour optimiser la supervision (réduire les faux positifs par exemple). On cherche à exploiter les caractéristiques des différents outils déjà existants pour collecter le plus d'information nécessaire pour une meilleure vision du réseau. OSSIM garantit l'interopérabilité des différents outils

OSSIM assure toutes les fonctionnalités d'un SIEM que sont :

- La collecte des Logs
- L'agrégation
- La normalisation
- La corrélation
- Le reporting
- L'archivage
- L'interprétation des évènements

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

- Des détecteurs d'intrusions : Snort (NIDS), Ossec, Osiris (HIDS)
- Un détecteur de vulnérabilités : Nessus, OpenVas
- Des détecteurs d'anomalies : Arp Watch, p0f, pads.
- Un gestionnaire de disponibilité : Nagios.
- Un outil de découverte du réseau : Nmap.
- Un inventaire de parc informatique : OCS-Inventory
- Un analyseur de trafic en temps réel : Ntop, TCPTrack, NetFlow.

3.3 Principe de la solution OSSIM

OSSIM est une plateforme centralisée fédérant plusieurs outils open source au sein d'une infrastructure complète de supervision de sécurité. Elle a pour objectif de centraliser, d'organiser et d'améliorer la détection et l'affichage pour la surveillance des évènements liés à la sécurité du système d'information d'une entreprise. OSSIM est constitué de composants de supervision suivants :

- Un panneau de contrôle
- Des moniteurs de supervision de l'activité et des risques.
- Des moniteurs de supervision réseau et des consoles d'investigation

Ces éléments s'appuient sur des mécanismes de corrélation, de gestion des priorités et d'évaluation des risques afin d'améliorer la fiabilité et la sensibilité des détections au sein de la solution.

3.4 Architecture de OSSIM

OSSIM repose principalement sur trois composants :

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

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

- **Le prétraitement de l'information**: géré par des équipements comme des systèmes détections d'intrusion(IDS), des sondes de collecte d'information(SENSOR) consiste à collecter les logs (fichiers de journalisation) de toutes les machines du parc informatique et de normaliser les différents logs reçus.
- **Le post traitement de l'information**: assuré par l'ensemble des processus interne de la solution et qui vont prendre en charge l'information brute telle quelle a été collecté pour ensuite l'analyser, la traiter et en fin la stocker dans une base de données.

Toutes ces informations collectées sont spécifiques et ne représentent qu'une petite quantité d'information circulant sur le réseau de l'entreprise. La possibilité d'utiliser les informations remontées par les détecteurs en utilisant un nouveau niveau de traitement, de compléter et d'améliorer le niveau d'information est appelée : la corrélation. Son objectif est de rendre cette remontée d'information plus efficace par rapport à la quantité d'information disponible sur le réseau de l'entreprise.

3.5 Fonctionnement interne de OSSIM

Pour une meilleure compréhension du fonctionnement de notre solution, la figure suivante sera l'illustration parfaite de son fonctionnement :

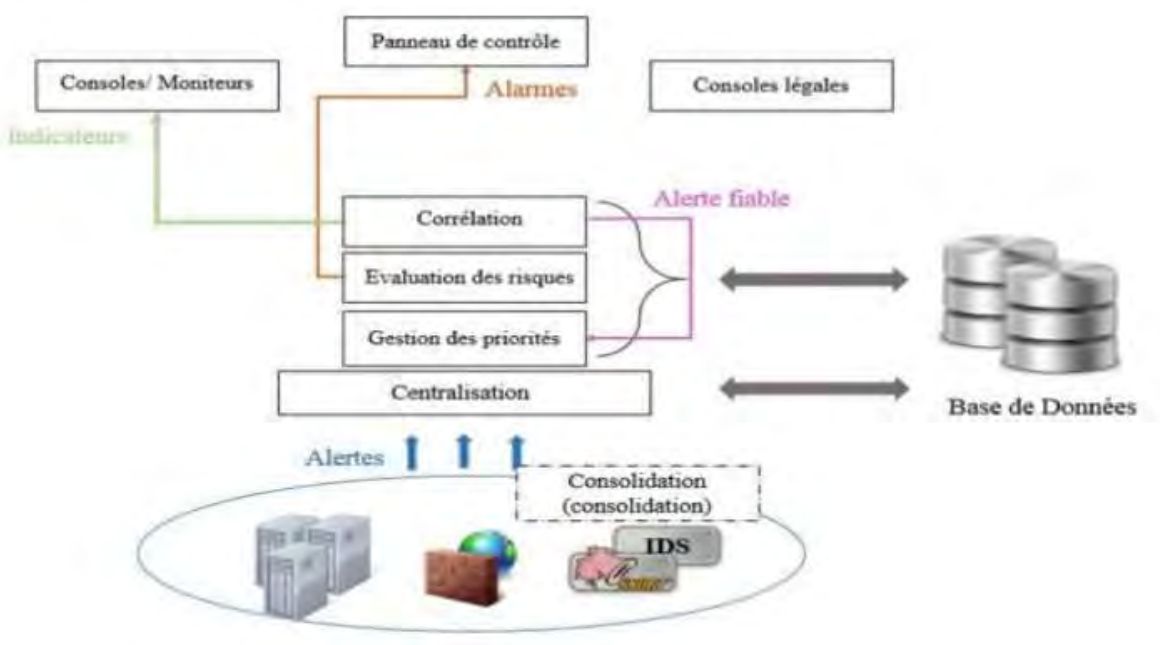

Figure 7 Fonctionnement de OSSIM

Les détecteurs traitent les évènements jusqu'à ce qu'une alerte soit identifiée soit par signature, soit par la détection d'une anomalie.

- Le collecteur récupère les différentes alarmes provenant de divers protocoles (P2P, SNMP…)
- Le parseur se charge de normaliser les alarmes et de les stocker dans une base de données d'événements, ensuite de les situer par priorité en fonction des politiques de sécurité mises en place.
- Le parseur évalue aussi les risques immédiats inhérents à l'alerte et remonte si besoin une alarme au niveau de panneau de contrôle.
- Les alertes une fois priorisées sont envoyées à chaque processus de corrélation, qui met à jour leurs variables d'état et renvoie éventuellement de nouvelles alertes aux informations plus complètes ou plus fiables. Ces nouvelles alertes sont renvoyées au parseur pour être à nouveau stockées, priorisées et évaluées par rapport aux politiques de risques et ainsi de suite.
- Le parseur de risque affiche périodiquement l'état de chaque index de risque selon la méthode de calcul CALM (Compromise and Attack Level Monitor).
- Le panneau contrôle quant à lui remonte les alarmes les plus récentes, met à jour l'état de toutes les métriques qu'il compare à leurs seuils, et envoie alors de nouvelles alarmes ou effectue les actions appropriées selon les besoins.
- L'administrateur peut également voir et/ou établir un lien entre tous les évènements qui se sont produit à l'heure de l'alerte à l'aide de la console d'investigation.
- L'administrateur peut enfin vérifier l'état de la machine impliquée en utilisant les consoles d'utilisation, de profil ou de session.

3.6 Fonctionnalité de OSSIM

Dans cette sous-partie, nous énumérerons les diverses fonctionnalités qu'offrent OSSIM en les classant par niveau.

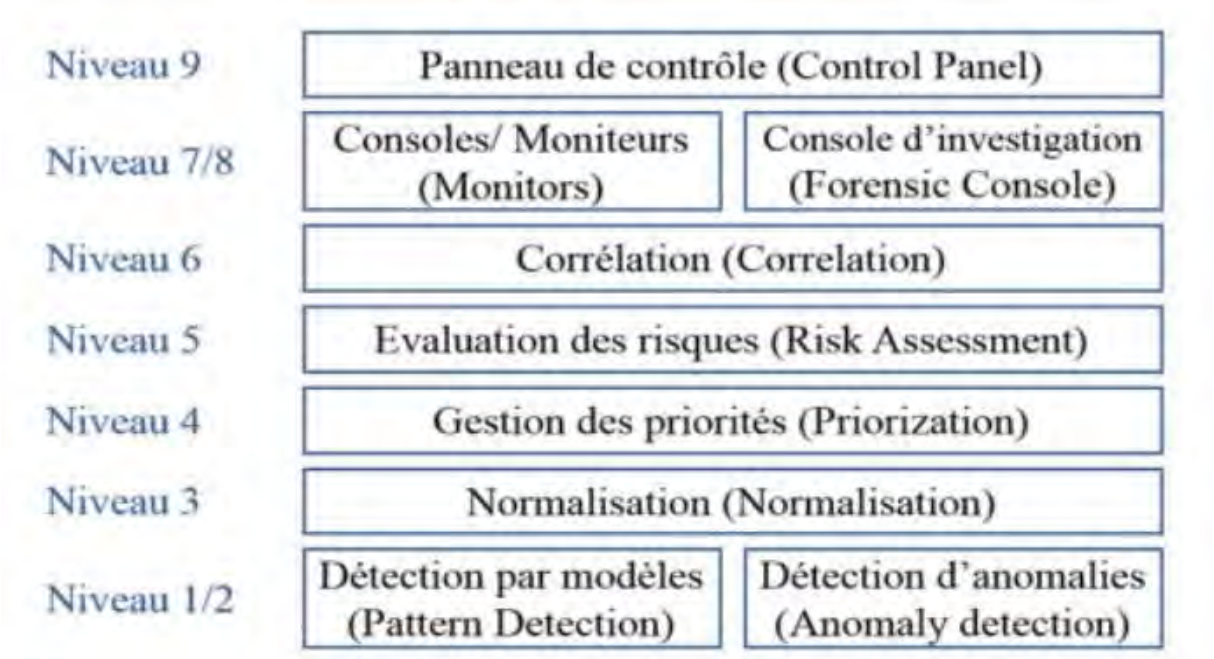

Figure 8 Fonctionnalité de OSSIM

✓ Niveau 1 : La détection par modèles (Pattern Detector)

Cette méthode est depuis longtemps utilisée par les IDS (Intrusion Detection System) pour détecter les modèles d'attaque en utilisant les signatures ou des règles bien définis. La recherche de motif est ce qui permet à un NIDS de trouver le plus rapidement possible les informations dans un paquet réseau.

✓ Niveau 2 : La détection par anomalies (Anomaly Detector)

Le principe n'est pas d'indiquer au système de détection ce qui est bon et ce qui ne l'est pas. En fait, le système doit apprendre un modèle de référence qu'il considère comme une situation normale et remonter une alerte quand le comportement dévie de ce modèle de référence. C'est cette fonction qui le différencie de la détection par modèles. Par exemple, dans le cas d'une nouvelle attaque pour laquelle il n'y a toujours aucune signature qui produirait une anomalie évidente pourtant ignorée par les systèmes de détection de modèle.

✓ Niveau 3 : La centralisation et la Normalisation

La centralisation et la normalisation ont pour objectif de réunir tous les événements de sécurité au sein d'une plateforme afin de faciliter leurs manipulations. Cette plateforme permettra d'avoir une vue plus détaillée sur l'entreprise. Ainsi, grâce à l'ensemble des fonctionnalités d'OSSIM disponibles par le panneau de contrôle, il est possible d'établir des procédures pour détecter des scénarii d'attaques plus complexes et fragmentées. De cette façon, il est donc possible d'observer tous les évènements de sécurité pendant une période donnée (qu'ils viennent d'un routeur, d'un firewall, d'un IDS, ou d'un serveur) sur le même écran et dans le même format. La normalisation est donc une composante essentielle et pour cela OSSIM s'appuie sur le standard IDMEF.

L'utilisation de ce standard est vivement encouragée par la communauté de développeur d'OSSIM et bon nombre d'acteurs de la sécurité en général.

L'IDMEF est un standard établi par l'IETF. Le modèle de données de l'IDMEF est une représentation orientée objet au format XML des alertes envoyées par les équipements de détection vers OSSIM. Les équipements qui vont émettre les alertes sont divers et variés.

✓ Niveau 4 : La gestion des priorités

La gestion de priorités est pour ainsi dire un processus de contextualisation, en d'autres termes, l'évaluation de l'importance d'une alerte par rapport à l'environnement de l'entreprise, qui est décrit dans une base de connaissance (KDB) pour le réseau comportant :

- Un inventaire des machines et réseaux (marques, systèmes d'exploitation, services, etc.)
- Une politique d'accès (si l'accès est autorisé ou interdit…) :

Les processus de gestion des priorités dans OSSIM sont définis au niveau du framework où sont configurés les éléments suivants :

- Les politiques de sécurité et des flux de données
- Inventaire du parc informatique
- Définition des alarmes

- Evaluation de la fiabilité des alertes

✓ Niveau 5 : L'évaluation des risques

Au niveau de la solution OSSIM, l'importance d'une alerte dépend de trois principaux facteurs:

- La valeur des équipements associée à l'événement
- Le degré d'occurrence
- L'impact de l'événement

On distingue d'une part des risques intrinsèques ou internes qui sont des risques qu'une entreprise assume en vertu à la fois des équipements qu'elle possède afin de développer ses affaires mais également des menaces circonstancielles liées à ces équipements. Le poids d'un risque peut être corrigé par un dispositif de maitrise des risques (DMR). OSSIM prend en compte le DMR dans son fonctionnement. La figure suivante présente la mesure de risque :

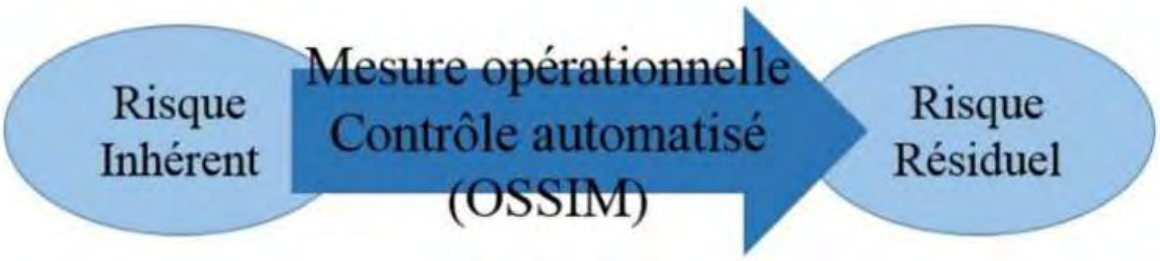

Figure 9 Mesure opérationnelle de contrôle automatisé (OSSIM)

D'autre part on a les risques immédiats qui peut donc être définit par l'état de risque produit quand une alerte est reçue et évaluée instantanément comme une mesure des dommages qu'une

Attaque pourrait produire, pondérée par la fiabilité du détecteur qui a remonté l'information.

OSSIM calcule le risque immédiat de chaque évènement reçu, et utilise cette mesure objective pour évaluer l'importance de l'évènement en termes de sécurité. OSSIM utilise cette mesure seulement pour évaluer la nécessité d'agir.

✓ Niveau 6 : La corrélation

La corrélation est le noyau de la solution OSSIM. Le mécanisme de corrélation peut donc être vu comme la possibilité d'utiliser les informations remontées par les détecteurs et, en utilisant un nouveau niveau de traitement, pour compléter et améliorer le niveau d'information.

Le but étant de rendre cette remontée d'information le plus efficace possible par rapport à l'étendue de la quantité d'information disponible sur le réseau d'entreprise.

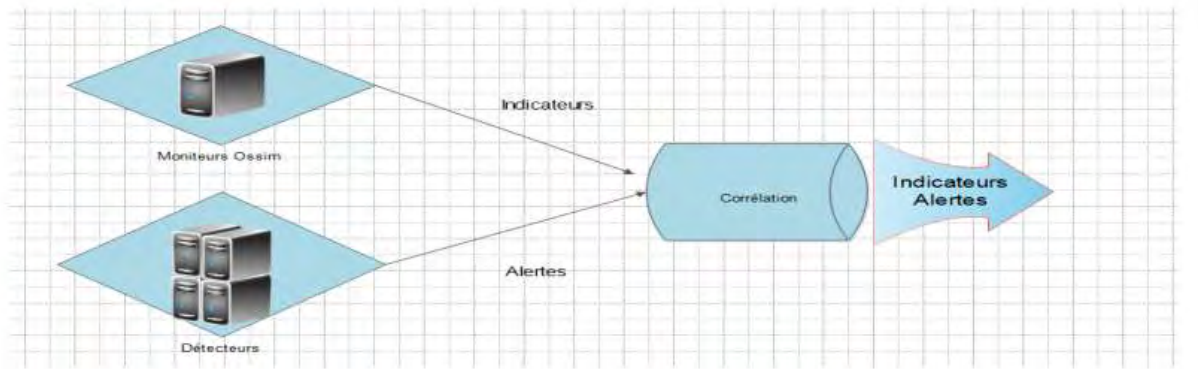

Figure 10 Système de corrélation de OSSIM

En entrée, les moniteurs fournissent normalement des indicateurs et des détecteurs des alertes.

En sortie Nous retrouvons également l'un de ces deux éléments : alertes ou indicateurs. Les fonctions de corrélation deviennent en fait de nouveaux détecteurs et moniteurs.

Elle a pour objectif sous OSSIM de : développer des algorithmes pour avoir une vue générale de la sécurité au sein de l'entreprise, fournir la capacité de lier des détecteurs et des moniteurs pour objets plus détaillés et plus utiles.

Pour pouvoir voir les objectifs qui ont été fixés, OSSIM a mis en place plusieurs méthodes de corrélation tel que :

- **La Corrélation en utilisant des séquences d'évènements**

À la base, la détection d'une séquence par modèle est simple, il suffit de rédiger des règles. OSSIM

utilise évidemment des séquences plus complexes dans lesquelles sont corrélées les alertes produites par des signatures avec le comportement caractéristique d'une attaque spécifique.

- **La Corrélation par les algorithmes heuristiques**

Cette méthode permet de compenser les imperfections de la corrélation par séquences d'évènements en détectant des situations sans connaitre ou montrer les détails. Ceci est utile pour détecter des attaques inconnues et montrer une vue générale de l'état de la sécurité pour un grand nombre de systèmes. Ossim utilise un algorithme heuristique appelé CALM.

CALM (Compromise and Attack Level Monitor) est un algorithme d'évaluation qui emploie l'accumulation d'évènements et leur rétablissement dans le temps. En entrée, il récupère un volume élevé d'évènements, et en sortie il fournit un indicateur unique de l'état général de la sécurité. Cette accumulation est valable pour n'importe quel objet sur le réseau (n'importe quelle machine, groupe de machines, segments de réseau, etc.) que l'on souhaite surveiller. CALM est donc prévu pour la surveillance en temps réel, de ce fait l'algorithme doit accorder de l'importance aux évènements les plus récents et jeter les plus vieux.

- **La Corrélation croisée**

Ce procédé permet d'augmenter la priorité d'une alerte Snort lorsque l'attaque définie par celle-ci aura été découverte comme possible par Nessus. Les associations entre les alertes de Snort et les règles de Nessus sont affichées dans la console d'administration d'OSSIM

✓ Niveau 7 : Les Consoles ou Moniteurs

Ils ne sont considérés comme des fonctionnalités, parce qu'ils font une représentation des différents processus. Au sein de OSSIM, on distingue différents types moniteurs tels que :

- Moniteur de risque : il montre les résultats de l'algorithme CALM.
- Moniteurs d'utilisation, de session et de profil

- Moniteur de chemin : permet de montrer la traçabilité des machines au niveau du réseau.

✓ Niveau 8 : La Console d'investigation (forensic)

C'est une console qui permet de faire la recherche d'événements sur la base de données de OSSIM. Cette console est un moteur de recherche qui opère sur la base de données d'événement (EDB).

Elle permet à l'administrateur d'analyser des évènements de sécurité par rapport à tous les éléments critiques du réseau a posteriori et d'une façon centralisée.

✓ Niveau 9 : Le Panneau de contrôle (Control Panel)

Le panneau de contrôle permet de regarder l'état de la sécurité du réseau au niveau le plus haut. Il surveille une série d'indicateurs qui mesurent l'état de l'entreprise par rapport à la politique de sécurité mise en place.

Le panneau de contrôle est le « thermomètre » général pour tout qui se produit sur le réseau. Il permet également d'accéder à tous les outils de surveillance pour inspecter n'importe quel problème qui a été identifié. La manière dont l'information est affichée dans le panneau de contrôle est importante, ainsi elle doit être aussi concise et simple que possible. Seule l'information qui est appropriée au moment qui nous intéresse doit être affichée.

3.7 Mise en place de la solution

Dans cette partie, nous allons mettre en place les différents outils utilisés lors de ce projet en les illustrant par les différentes captures d'écran qui ont été faites.