Université Cheikh Anta DIOP de Dakar

Faculté des Sciences et Techniques

Département Mathématiques et Informatique

Laboratoire d'Algèbre de Cryptologie de Géométrie Algébrique et Applications

LACGAA

Mémoire pour l'obtention du diplôme de Master 2

Transmission de Données et Sécurité de l'Information

Thème :

Mise en place d'un Security Operation Center(SOC) basé sur un serveur SIEM Open Source (Alien Vault).

Présenté et soutenu par :
Abdoulaye MBAYE

Encadreur: Mr. Ahmedou khalifa
Superviseur : Mr Demba Sow

Dakar le 11 septembre 2019

Jury :

Président : M. Oumar Diankha	UCAD
Membres : M Ismaïla Diouf	UCAD
M. Demba Sow	UCAD

Avant propos

Pour l'obtention du Master professionnel, TDSI demande à ces étudiants d'élaborer un mémoire de fin de cycle.

C'est dans ce cadre que nous avons rédigé ce document qui a comme sujet : Mise en place d'un Security Operation Center (SOC) basé sur un serveur SIEM Open-Source (AlienVault OSSIM).

Dans ce mémoire, je présenterai ce qu'est le Centre d'Opération de Sécurité (SOC), la technologie SIEM indispensable à tout SOC et ensuite faire une étude sur le SIEM open-source OSSIM avant de terminer par une mise en œuvre de la solution OSSIM

DEDICACES

Au nom d'Allah (swt) le clément, le miséricordieux, à son prophète Mouhamed

Je dédie ce mémoire :

- *A mon père BABACAR LAYE MBAYE pour son amour, sa patience et ses multiples sacrifices et conseils*
- *A ma mère DIAMA LAYE NIANG source de ma vaillance*
- *A mes frères SEYDINA ISSA LAYE MBAYE, MAMADOU LAYE, OUSSEYNOU LAYE, IBRAHIMA LAYE, ALASSANE LAYE, BAYE ABOU, PAPA ISSA et BAYE DJINE*
- *A mes sœurs DIAMA, MAIMOUNA, MANTOULAYE et SOKHNALAYE*
- *A mon ami CHEIKHLAYE DJITÈ*
- *A tous mes amis et camarades*

REMERCIEMENTS

Après avoir rendu grâce DIEU et prier sur le prophète PSL, je tiens à remercier tous ceux qui de loin ou de près ont participé à l'élaboration de ce mémoire :

- *Je tiens à remercier l'équipe pédagogique de la Faculté des Sciences et technique plus particulièrement ceux du Laboratoire d'Algèbre de Cryptologie de Géométrie Algébrique et Applications (LACGAA) pour le haut niveau de leurs enseignements.*

- *C'est l'occasion pour moi de remercier le professeur Mr DIANKA responsable du master TDSI, pour l'excellent niveau de ses enseignants ainsi que la qualité des enseignements dont mes camarades de promotion et moi avions bénéficié.*

- *Je tiens à remercier Mr Ahmedou Khalifa, professeur de réseaux et systèmse à TDSI d'avoir bien voulu consacrer une partie de son temps sur ce mémoire.*

- *Aux membres du jury, pour avoir voulu évaluer ce travail.*

En fin, je tiens à remercier mes parents qui m'ont soutenu et aidé tout au long de ma vie et de mes études.

SOMMAIRE

.

INTRODUCTION

Face à l'augmentation de la surface d'exposition aux cyber-risques et à la professionnalisation des menaces, les investissements réalisés dans les outils de sécurité sont de plus en plus importants, aussi bien en prévention, qu'en détection et réponse à incident. Cependant, pendant plusieurs années, après avoir tenté d'enrayer les menaces et incidents de sécurité dans les systèmes d'informations, les entreprises sont aujourd'hui en voie d'admettre qu'aucun système n'est aujourd'hui invulnérable et inviolable, Pensez pouvoir éviter ces cyber-attaques nombreux et complexes devient malheureusement utopique. Devant les risques d'intrusions, de vol de données sensibles et la difficulté croissante d'obtenir une sécurité des Systèmes d'Information efficace en interne, La force des entreprises, pour la défense de leur patrimoine informationnel, repose alors sur la détection rapide du moindre incident et la réaction immédiate appropriée.
Pour cela, La gestion des événements/incidents de sécurité des systèmes d'information constitue un élément essentiel du cycle de vie de la sécurité de l'information. Cette démarche consiste à définir un ensemble de mesures techniques et organisationnelles permettant de centraliser l'exploitation, le filtrage, et la corrélation de l'ensemble des logs issus de ces différents équipements/applicatifs (de sécurités ou non) de surveillance pour faire face aux différentes menaces qui pèsent sur le patrimoine informationnel d'une organisation.

Ainsi, la cyber-surveillance est plus que jamais d'actualité et une solution attractive se trouve dans la mise en œuvre d'un centre d'opération de sécurité (SOC) qui a ostensiblement le rôle de centres de supervision, de surveillance et de la défense de la sécurité des systèmes d'information de l'entreprise. Ce qui place le Security Operation Center (SOC) au centre des enjeux de la cyber-sécurité.

Afin de répondre aux questions que tout RSSI pourrait se poser à l'égard des SOC (Ai-je besoin d'un SOC ? En quoi un SOC m'aiderait-il à lutter contre les menaces ? Comment devrais-je le mettre en place ?), ce document à travers une étude tentera de couvrir les principaux aspects que représentent l'implémentation d'un SOC, le monitoring et la réponse aux incident.

Dans ce cadre, le présent rapport se base sur trois axes principaux :
- Présenter les notions d'un Center d'Opération de Sécurité (SOC)
- Etudier la solution choisie en énumérant ses fonctionnalités et apports.
- la réalisation, et la mise en place de cette solution

Première partie : cadre méthodologique et théorique

CHAPITRE I : PRÈSENTATION DU SUJET

I.1 PRÈSENTATION D'UN SOC

Le SOC peut être considéré comme le tour de control d'une organisation de cybersécurité. Il est le centre de tous les rôles et responsabilités cherchant à protéger le système d'information de l'entreprise.
Un SOC est avant tout une équipe d'experts en sécurité chargée de surveiller, détecter, analyser et qualifier les évènements de sécurité. Cette équipe assure le pilotage des réactions appropriées aux incidents avérés de sécurité. Pour certaines organisations, cette équipe administre et contrôle au quotidien des dispositifs et dispositions de sécurité ; par exemple le « durcissement » de systèmes d'exploitation standards en vue de renforcer leur sécurité, ou bien la gestion d'accréditations (droits d'accès à des ressources) voire également la gestion du « patch management ».
Compte tenu de la variété des missions, des impacts technologiques ainsi que des impacts organisationnels majeurs, la mise en œuvre d'un SOC représente un réel investissement en temps et ressources pour l'Entreprise concernée ; même avec l'aide d'un prestataire qualifié (type MSSP). C'est aussi pourquoi il est généralement nécessaire que l'Entreprise atteigne une taille critique avant de consacrer des ressources internes à l'opération de son propre SOC. Dans le cas des entreprises constituées de plusieurs entités, il est fréquent que le SOC soit porté par l'une d'entre elle de façon transverse pour les autres.

Un SOC est un dispositif de supervision et d'administration de la sécurité du système d'information permettant, grâce à la collecte d'événements, de détecter des incidents de sécurité informatique, de les analyser et de définir les réponses en cas d'émission d'alerte.
Il existe une multitude de définitions de ce qu'est, ou devrait être un SOC. Cependant, l'ensemble de la profession s'accorde à dire qu'un SOC doit être avant tout une entité dédiée à la surveillance et à la défense des systèmes d'information de l'entreprise.

Un SOC, ou Security Operations Center est une équipe de la DSI qui est en charge de la gestion et du maintien de la sécurité du système d'information.

De façon plus générale, un SOC désigne :
Les personnes, processus et technologies qui permettent d'obtenir un état du niveau de sécurité à travers la détection, le confinement et la résolution des menaces informatiques. Un SOC gère les incidents de sécurité pour une entreprise, assurant qu'ils sont convenablement identifiés, analysés, documentés, résolus et investigués. Le SOC monitore également les applications pour identifier les possibles « cyber-attaques » ou intrusions (événements), et détermine si ce sont des attaques réelles et malicieuses (incidents), et si elles peuvent avoir des impacts sur l'activité de l'entreprise. »
Il est donc de la responsabilité du SOC de gérer les événements et incidents de sécurité qui surviennent sur le SI surveillé. Il doit être capable de les détecter, de procéder à des investigations afin d'obtenir le plus d'informations possible à leur sujet, puis de les résoudre. Le SOC peut également donner des préconisations et règles de bonnes pratiques afin d'éviter que ces incidents se reproduisent. Le SOC permet également de maintenir un haut niveau de sécurité sur le système d'information qu'il monitore.

I.2 **contexte du sujet :**

Ce travail se positionne dans un contexte de mémoire de fin d'étude pour la validation de notre formation en Master **transmission de données et sécurité de l'information** (TDSI) à l'UCAD.
Le sujet de la supervision des Systèmes d'Information (S.I.) revient sur le devant de la scène notamment en raison de nouvelles réglementations auxquelles sont soumis certains domaines d'activité, mais également en raison des menaces accrues qui pèsent sur les S.I. et qui ont des impacts de plus en plus graves. Engagés dans une transition et transformation numériques, les S.I. se retrouvent pour la plupart au contact d'Internet, siège de la cybercriminalité et des « cyber-convoitises », l'exposition aux risques est certaine.
Dans le domaine de la supervision de la SSI, 3 difficultés majeures sont rencontrées :
1. la masse et la diversité des informations à traiter ;
2. l'identification des d'évènements précurseurs d'alertes de sécurité ;
3. l'appropriation du sujet et la réunion des compétences requises pour un projet d'envergure.

Il est recommandé, et c'est généralement le cas, que la supervision SSI soit assurée par une entité spécialisée :
Le Centre Opérationnel de Sécurité COS (COS en anglais devient le SOC pour Security Operation Center).

I.3 **PROBLÈMATIQUE**

La récente étude **M-Trends** 2018 qui est une publication annuelle sur la cybersécurité estime à 175 jours le délai moyen de détection d'une attaque informatique sur une entreprise européenne. La moyenne mondiale est de 101 jours.
Afin de palier au plus vite ce manque de protection flagrant, les entreprises doivent aujourd'hui revoir leur approche de la cybersécurité.
L'approche qui consiste à empiler les solutions de sécurité n'est plus suffisante.
Les entreprises doivent aujourd'hui analyser leurs systèmes d'information en continue dans l'intérêt de détecter, de traiter, de neutraliser et d'investiguer rapidement les attaques informatiques.
Les connaissances et compétences mises en œuvre dans le cadre de ces attaques démontrent que les acteurs malveillants n'hésitent plus à investir dans des moyens techniques et humains importants pour atteindre leurs objectifs.

L'actualité démontre que l'activité des entreprises attaquées est fortement perturbée, voire interrompue de façon durable. Les impacts financiers, organisationnels, juridiques et d'image peuvent être très importants, voire fatidiques lorsqu'ils font vaciller la confiance entre l'entreprise et ses clients, ses partenaires ou ses salariés dans le cas de vol ou divulgation de donnée personnelles, stratégiques ou critiques. Les dispositifs existants de gestion de crise et de continuité d'activité doivent être renforcés pour répondre aux risques associés.

Ces observations s'inscrivent dans une ère de transformation numérique de l'Entreprise sous-tendue par l'apparition de nouvelles technologies comme la mobilité, le cloud et l'ouverture des données de l'Entreprise à ses clients et partenaires via ses propres systèmes et/ou les réseaux sociaux. La multiplication et la diversification des systèmes technologiques mis en œuvre induit une augmentation sans précédent du nombre de vulnérabilités. La surface d'attaque de l'Entreprise tend ainsi à croitre de façon très importante.

La cybercriminalité est désormais agile, industrialisée, structurée et professionnelle. Elle exploite toutes les vulnérabilités et failles techniques, organisationnelles et humaines. Quel que soit le secteur d'activité, plus aucune entreprise n'est épargnée.

Parallèlement à cette omniprésence de la cybercriminalité, les entreprises peuvent se retrouver face à un besoin de conformité, de législation et de réglementation qui définissent et précisent les objectifs de sécurité à atteindre Parmi elles, on distingue :

- Contraintes réglementaires de l'ANSSI telle que le projet de Loi de Programmation Militaire (LPM) liées au domaine d'activité des entreprises opérateurs d'intérêt vitaux (OIV) ;
    - Un OIV ou (Opérateur d'Intérêt Vital) est une organisation définie par l'état comme ayant des activités indispensables ou dangereuses pour la population.
    - La LPM (Loi de Programmation Militaire) précise qu'il est de la responsabilité de l'état d'assurer une sécurité suffisante des systèmes d'informations critiques de ces OIV par la mise en place d'un système de détection d'attaque informatique et de notification d'incident aux autorités compétentes ; d'où la nécessité pour ces OIV de disposer d'un SOC selon l'ANSSI
- Contraintes des réglementations internationales telles que PCI-DSS, (norme de sécurité de l'industrie des cartes de paiement
    - La norme PCI-DSS exige que les commerçants ou les fournisseurs de services interviennent sur le stockage, le traitement ou la transmission des données des titulaires pour :
        - Construire et maintenir un réseau informatique sécurisé ;
        - Protéger les données des titulaires ;
        - Maintenir un programme de gestion des vulnérabilités ;
        - Mettre en place des mécanismes de contrôle d'accès Robustes ;
        - Surveiller et tester régulièrement les réseaux ;
        - Maintenir une politique de sécurité de l'information.

- Le règlement général sur la protection des données RGPD de l'UE
    - Le RGPD des 28 états membre de l'UE estime que les organisations doivent obligatoirement pouvoir garantir leur conformité en matière de protection des données personnelles
        - Obligation de localisation des données ;
        - Obligation de notification d'incidents.

- La norme ISO 27035 relative à la gestion des incidents de sécurité

Egalement entre en jeu dans cette problématique, la responsabilité de la Direction de l'entreprise qui est de plus en plus engagée car devant assurer le respect de ces exigences (légales, réglementaires, contractuelles) ci-dessus.

I.4 **OBJECTIFS**

A. Le soc dans la stratégie SSI

Selon les standards des Systèmes de Management de la Sécurité des S.I. (SMSI), la Politique de Sécurité des SI (PSSI) définit les objectifs SSI de l'Entreprise. Ces objectifs sont généralement justifiés ou adossés à des risques portés par l'Entreprise et à son activité. Le SOC, qui est une mesure de sécurité pour réduire un ou plusieurs de ces risques, contribue à l'atteinte de ces objectifs mais n'est généralement pas décrit dans ce document fondateur. Autrement dit, la mise en œuvre d'un SOC ne nécessite pas la réécriture ou la modification de la PSSI Entreprise.

Cependant, quelle que soit l'organisation retenue, pour être légitime et efficace, le SOC doit avoir une liste de responsabilités correctement définie, attribuée et documentée. Ces responsabilités sont inscrites et documentées dans les procédures de sécurité (directement dérivées de la PSSI). La légitimité des activités du SOC vis-à-vis des autres entités de l'Entreprise est portée par la lettre de mission du SOC signée par le comité exécutif de l'Entreprise (COMEX). Cette lettre précise notamment que le SOC a pour mission de surveiller les événements de sécurité et réagir aux incidents de sécurité du système d'information.
Ces documents (procédure et lettre de mission) peuvent également définir les « partenariats » entre le SOC et d'autres entités capables de soutenir les efforts du SOC (si celui-ci n'est pas omnipotent). Par exemple, il peut être opportun d'indiquer que l'entité en charge de l'exploitation des réseaux peut être sollicitée pour permettre l'intervention sur des équipements filtrants. Les documents de politique indiquent alors les niveaux de priorité des interventions et le cadre des conventions de services entre entités ou équipes.
Le SOC travaille généralement en étroite relation avec les équipes de production pour ses capacités de réaction. Dans d'autres situations, le SOC dispose des moyens d'intervenir sur les équipements de production. Le SOC peut avoir des missions étendues (gestion des identités, habilitations, …).
Si les objectifs de sécurité sont définis au niveau de l'organisation, le consensus en termes de priorités et d'implication est plus facile à atteindre. Documenter clairement les responsabilités de chacun permet également de définir les besoins et les services rendus par un SOC et de communiquer au sein de l'organisation.

B. **Activités d'un SOC**

La mission principale d'un SOC consiste à surveiller, détecter, analyser et qualifier les évènements de sécurité. Elle se décline en 3 activités majeures pouvant être gérées indépendamment :
1. Activité #1 Supervision/Qualification/Alerting ;
2. Activité #2 Pilotage des incidents de bout en bout ;
3. Activité #3 (optionnelle) Traitement standardisé d'un incident.

En complément de cette mission principale, le SOC a la charge de conserver les journaux d'activité (ou logs) qui lui sont remontés pour la durée qui a été définie. Cette mission est essentielle pour permettre des analyses inforensiques à postériori ainsi que la production de rapports et statistiques à valeur ajoutée.
Le SOC peut également se voir confier des missions additionnelles en fonction des organisations, telles que :

- L'investigation sur incident également appelée inforensique ou forensic
- La fourniture d'expertise ponctuelle sur la gestion de crise ;
- La gestion des vulnérabilités ;

- Un rôle de sécurité opérationnelle, au travers du Paramétrage des équipements de sécurité ;

- Gestion des identités et habilitations ;
- Le traitement en profondeur des causes racines de l'incident ;
- La sensibilisation des utilisateurs et la communication de la sécurité.

Un SOC est en charge de piloter la gestion des incidents de sécurité, des vulnérabilités et des risques couvrant un périmètre très large de domaines : infrastructures réseaux, applications, services, postes de travail. Même si le périmètre d'intervention d'un SOC diffère selon le contexte, les activités suivantes sont classiquement incluses dans un SOC : surveillance de logs, gestion des incidents, suivis de l'application des correctifs…

En particulier, un SOC a la responsabilité de :

• Définir les stratégies de défense et les adapter en permanence ;
• Détecter les signaux faibles et anticiper les menaces ;
• Identifier les agresseurs potentiels et leurs méthodes d'attaques ;
• Structurer un mécanisme de défense systématique
• Organiser une réactivité immédiate lors d'attaques.

Les caractéristiques d'un SOC qu'on retrouve chez tous les clients sont :

• Le monitoring en temps réel des événements ;
• L'évaluation des menaces ;
• La prise de décision graduée et basée sur des informations concrètes.
Au sein d'une équipe sécurité, le SOC fait office de système de détection, d'analyse, de prévention de risques, de levées d'alertes (par le biais de produits SIEM), et aussi, d'aide à la décision, de protection et d'exploitation d'éventualités.

Via un SOC bien configuré, l'entreprise peut garantir une continuité d'activités et anticiper d'éventuels problèmes et incidents, car un pare-feu et un système de détection d'intrusion (IDS) ne sont pas toujours suffisants

Son objectif final est d'assurer une surveillance 24h/24 et 7j/7 afin de rétablir dans un délai le plus court possible la sécurité du système d'information lorsqu'elle est menacée.

I.5 **LES COMPOSANTES DU SOC**

Le SOC a quatre composantes : gouvernance, processus, technologie et équipe.

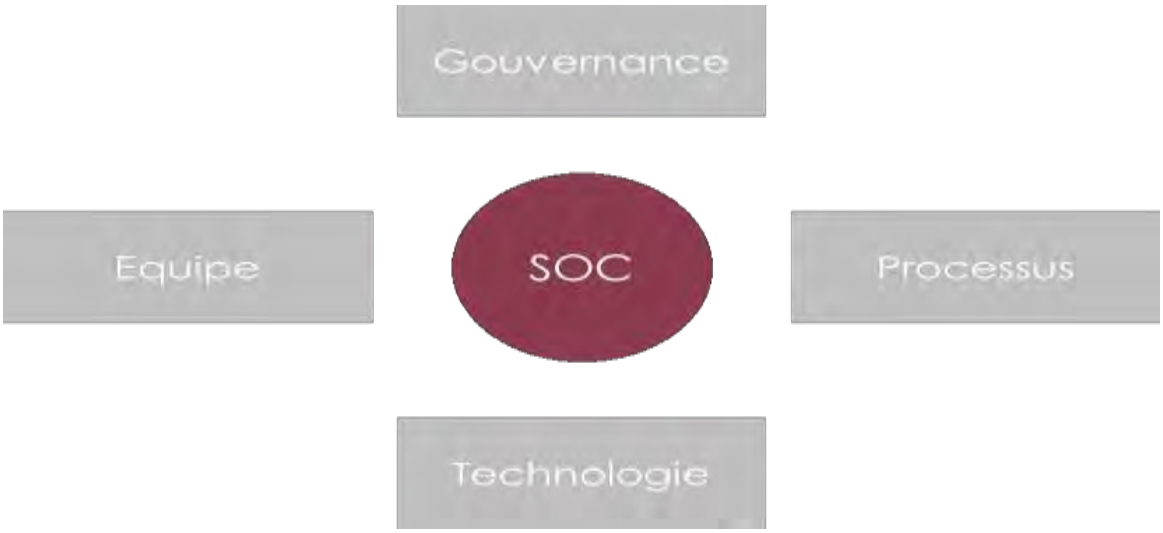


Fig 1 : les composantes du soc

I.5.1 LA GOUVERNANCE / cartographie des risques liés à la cybersécurité

Pour réaliser la cartographie des risques, l'organisation doit tout d'abord identifier quels sont ses process critiques. Elle identifiera ensuite les vulnérabilités et les menaces, basées sur la probabilité et l'impact financier, dont peuvent faire l'objet ces process critiques. Elle s'assurera également de la pertinence et de la mise à jour de toutes les informations liées aux problèmes de cybersécurité. Il est en outre recommandé de classer l'ensemble des risques.

Dans un second temps, l'organisation devra mettre en œuvre des tests d'intrusion afin de fournir des informations précises sur les risques liés à la cybersécurité. Ces tests consistent à simuler une attaque informatique d'un utilisateur mal intentionné ou d'un logiciel malveillant. Ils permettent d'analyser les risques potentiels dus à une mauvaise configuration d'un système, à un défaut de programmation ou encore à une vulnérabilité liée à la solution testée. Son principal objectif est de détecter des vulnérabilités qui permettront de proposer un plan d'actions visant à améliorer la sécurité du système d'information.

La gouvernance consiste à :

- Définir la mission et le périmètre des actifs à mettre sous contrôle ;
- Structurer le SOC ;
- Définir le niveau d'autorité du SOC et ses modalités d'accès aux ressources.

I.5.2 Définition d'un PROCESSUS de management des incidents

Ce process de gestion des incidents doit comprendre 3 phases principales :

- identification de l'incident ;
- réponse en fonction du niveau de criticité ;
- rétablissement du réseau à un niveau normal.

A noter également que le SOC doit répondre à des exigences légales et réglementaires. Elles visent notamment à mettre en œuvre un dispositif de détection d'attaques informatiques et à notifier les incidents de sécurité aux autorités compétentes.

I.5.3 LA TECHOLOGIE de supervision des événements du système d'information

La technologie regroupe l'ensemble des moyens techniques utilisés pour rassembler, harmoniser, corréler, stocker et faire un reporting sur les événements de sécurité.

En effet la mise en place d'un **Soc** est faite sur la base de solutions logicielles **SIEM**.

I.5.4 Identification et mise en place d'une ÈQUIPE dédiée

L'équipe SOC est constituée d'experts hautement qualifiés qui définissent et mettent en place des processus et procédures permettant de faire face et de réduire le risque sécurité SI. Ils sont également responsables de la gestion des incidents de sécurité SI.

Les entreprises peinent à trouver et conserver des ressources qualifiées :

Le sujet du SOC est encore nouveau et n'est pas encore largement adopté par les entreprises. En conséquence, les compétences sont rares.

En outre, selon HP, les équipes les plus performantes sont celles qui disposent de ressources polyvalentes. En effet, les analystes outre les problématiques du SOC sont au contact des autres équipes sécurité SI de l'entreprise et des équipes risques et conformité notamment. Ils doivent donc disposer des connaissances nécessaires afin d'interagir efficacement avec elles.

Les entreprises sont amenées à développer leurs compétences internes par la mise en place d'un dispositif de formation. Celui-ci ne doit pas se limiter aux aspects techniques et aux équipes du SOC. Il doit aussi permettre de sensibiliser les autres équipes aux problématiques SI.

###L'organisation devra 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. ###

I.6 LES MODELES DE SOC

Il existe principalement deux grandes familles de SOC :

1. Les SOC opérés en interne

2. Les SOC externalisés

Le choix d'un type de SOC est capital lors des études de conception car cela conditionne la nature des travaux et du pilotage pendant la phase de construction. Les paragraphes suivants décrivent les avantages et les inconvénients de chacun des types de service.

L'évolution d'un modèle de SOC à un autre est naturellement envisageable mais nécessite une préparation et une anticipation importante pour éviter de devoir reconduire tous les travaux de conception et de construction lors de la bascule de l'un à l'autre des modèles. Ce changement de nature peut être justifié par l'atteinte d'un certain niveau de maturité par l'Entreprise et/ou l'évolution des objectifs de sécurité ou bien encore un changement de stratégie au niveau de la DSI ou de l'Entreprise.

- **Avantages du SOC dédié/interne :**
  Les SOC dédiés disposent de ressources humaines dédiées, organisées et en capacité de traiter toutes les alarmes reçues par les outils de collecte
    - Les équipes du service connaissent mieux les infrastructures et les applications supervisées et sont donc à même de qualifier plus efficacement les alarmes remontées.

- Les solutions/outils dédiées sont plus flexibles et plus facilement paramétrables. Les scénarios de menaces et les objectifs de sécurité sont considérés de façon précise.
- La communication (investigation) et l'escalade sont plus rapides (puisque utilisant les outils de communication de l'Entreprise)
- Les journaux d'événements et tous les éléments de suivi des alarmes et incidents sont tous stockés en interne.

➢ **Inconvénients du SOC dédié :**

- L'investissement financier initial est très important (pour mettre en œuvre l'outillage, recruter et former les ressources, conduire les études et exécuter la réalisation).
- Le recrutement d'analyste SOC et d'expert en sécurité est un véritable défi et peut prendre un certain temps.
- Le risque d'entente entre des acteurs malveillants et des opérateurs du service SOC est plus important que dans le cas d'un service externalisé.

➢ **Avantages du Soc externalisé/ fournisseur de services de sécurité(MSSP)**

- L'investissement initial est plus raisonnable tant sur le plan technique qu'humain.
- Le service est généralement proposé à plusieurs acteurs du même domaine. Ceux-ci bénéficient de fait de l'expertise des analystes pour le secteur d'activité concerné.
- La mutualisation des couts opérés par les acteurs MSSP leur permet de proposer des modèles de SOC moins chers que les versions internalisées.
- L'entente entre un acteur malveillant et un opérateur du SOC est moins probable car ces derniers sont moins exposés.
- Le MSSP met tout en œuvre pour se doter des expertises les plus pointues sur les outils de collecte et de traitement.

➢ **Inconvénients du SOC externalisé :**

- Les opérateurs distants ne connaitront jamais aussi bien les infrastructures et applicatifs que les opérateurs agissant au sein de l'Entreprise
- L'externalisation d'un service de sécurité essentiel comme le SOC peut avoir un impact négatif sur le « moral » des personnels IT de l'Entreprise
- Les données internes de l'Entreprise sont envoyées à l'extérieur sans contrôle possible a priori. Une erreur de manipulation est tout à fait probable

I.7 CONCEPTS ET FONDAMENTAUX

I.7.1 Journaux, événements, alertes et incidents

Pour éviter toute confusion dans la suite de ce document, les définitions des termes « journaux / enregistrements », « événements », « alerte » et « incident » sont proposées ci-dessous :

A. Journaux / Enregistrements

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

Constituant les logs d'un système actif, ces journaux sont généralement conservés à des fins d'exploitation ou d'investigation. Ils sont parfois les seuls éléments (à charge) qui peuvent être utilisés en cas de comportement anormal ou suspicieux d'un système. Ils sont donc généralement protégés voire séquestrés pour être utilisés en tant que preuve.

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

B. Evénement

Selon la norme ITIL v3, un « événement » correspond à un changement d'état suffisamment important pour être notifié à un gestionnaire du service. Ainsi, il peut s'agir d'un changement d'état normal ou, au contraire, d'un changement pour un état anormal (ex. une défaillance). Un événement peut être transcrit par un ou plusieurs enregistrements dans un journal.

Dans le cadre de ce document, nous préférerons la définition de la norme ISO 27000 (2.20) qui précise qu'un événement de sécurité est une occurrence identifiée de l'état d'un service, d'un système ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité. Alerte

Une alerte correspond à un événement ou à un groupe d'événements pondéré. Cette pondération est particulièrement importante puisqu'elle permet de classer les événements et de ne retenir que ceux qui atteignent ou dépassent un seuil de vigilance. Tout comme pour les enregistrements et journaux, le défi consiste à fixer correctement le seuil (ou à le retenir auprès d'un organisme tiers) pour ne conserver que les événements qui nécessitent une attention particulière. Parce que les mécanismes qui associent une pondération à l'événement peuvent être défaillants ou inadaptés, les alertes peuvent être classées en différentes catégories :

- Faux positif : la pondération a été positionnée de façon inadaptée, rendant un événement important à tort. Dans ce cas, le comportement du système est considéré défaillant à tort.

- Vrai positif : la détection a été correctement positionnée. Il s'agit d'une alerte qui correspond réellement à un événement redouté ou à comportement anormal du système.

- Faux négatif : le mécanisme de détection n'a pas correctement fonctionné et un événement qui aurait dû être identifié en tant qu'alerte n'a pas été repéré et classé. Le système est défaillant et aucune alerte n'appuie ce statut.

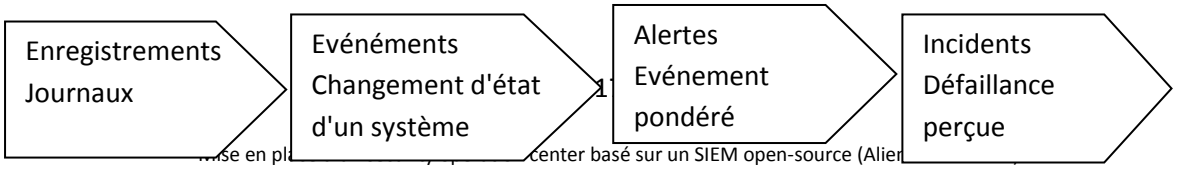
- Vrai négatif : le mécanisme de détection est adapté. Le comportement du système n'est pas défaillant et aucun événement n'est identifié en tant qu'alerte à tort.

C. Incident

Toujours selon la norme ITIL, un incident est une interruption non planifiée d'un service, une réduction de la qualité d'un service ou la défaillance d'un élément du système. Un incident est associé à un impact négatif (perçu ou non) sur la qualité de service globalement perçue par les utilisateurs du système. Un incident est généralement (mais pas toujours) caractérisé par une série d'alertes. Il est généralement enregistré, analysé et traité sur la base des éléments d'information le constituant. Un incident appelle une réponse.

Dans le contexte de la sécurité des systèmes d'information, la norme ISO 27000 (2.21) définit un incident comme un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information.

La chronologie suivante peut être établie :



Les incidents peuvent être catégorisés par le SOC ou le CSIRT, selon des critères propres à l'organisation, pour permettre un reporting à plus haut niveau de la sécurité des S.I. La catégorisation permet également de favoriser les comparaisons entre pairs. La norme ISO 27014 et les documents de travail de l'ETSI3 établissent à cet effet la catégorisation/taxonomie des indicateurs/catégories d'incidents de sécurité.

I.7.2 Le SIEM

La plateforme logicielle principale du SOC est le SIEM (Software Information Event Management). C'est un outil de gestion des évènements (ou logs) du système d'information Les SIEM (Security Information and Event Management – système de gestion des informations et des événements de sécurité) se sont imposés avec la démocratisation de la génération des journaux et des traces que produisent les différents systèmes et plus particulièrement ceux de sécurité. Il ne suffit plus, aujourd'hui, d'observer les traces produites par un composant de sécurité pour s'assurer du bienfondé du comportement du système complet. Il faut, à minima, considérer les traces des différentes briques essentielles du système.

Ces opérations d'observation et de recoupements, longues et fastidieuses, ont fait l'objet de plusieurs techniques et solutions de concentration et d'agrégation de traces. Ces systèmes de collecte et d'agrégation ont progressivement été enrichis de fonctionnalité de tri, de filtre et de statistiques produisant ainsi des rapports de journalisation sur tous les systèmes connectés. Par des mécanismes d'analyse statique des enregistrements, les SIEM sont désormais capables de détecter les enregistrements potentiellement générateurs d'événements voire même de qualifier certains d'entre eux en alertes.

Selon le système considéré, les traces, événements et alertes peuvent être rapprochés les uns des autres (géographiquement ou temporellement) pour permettre à un tiers (humain ou automatique) d'enregistrer/déclarer un incident

- **Le SIEM : un pilier pour le soc**

Le **SIEM** (pour **Security Information and Events Management**) essaie d'apporter un ensemble de moyens permettant d'agréger, normaliser, corréler, consolider, superviser, analyser, notifier et capitaliser les événements de sécurité de l'information

Le SIEM (Security Information and Event Management) est malheureusement souvent réduit à l'outil technique qui va permettre de gérer les logs générés par les différents équipements / applicatifs (de sécurité ou non) qui composent un système d'information.

Le SIEM est la réunion d'un SIM (Security Information Management) et d'un SEM (Security Event Management). Le SIM permet d'offrir un certain nombre de fonctionnalités pour collecter les logs dans le but d'analyser, de stocker, d'archiver l'ensemble des logs le forensic (investigation numérique), le reporting des données de log et surtout pour se conformer avec les normes. En effet, les législations obligent les entreprises à conserver toutes traces informatiques de tout équipement constituant le Système d'Informations (SI) et ceci avec une rétention différente en fonction du types de logs. Le SIM offre une visibilité sur l'ensemble des logs grâce à des outils d'indexation permettant d'améliorer la recherche et d'analyser les logs rapidement. Avec ce type de solution, il est également possible de générer des rapports et d'avoir un état de l'art des événements circulant dans un SI.

Quant au SEM, il permet la supervision temps réel ou quasi temps réel, la corrélation, la collecte, le **traitement et exploitation des événements** temps réel ou sur l'historique. L'ensemble des logs recueillis regorge d'une multitude d'informations qui sont aujourd'hui mal exploitées, voire pas du tout. Les logiciels SEM proposent de normaliser et catégoriser les logs afin de le rendre plus lisibles, plus exploitables. Ces solutions offrent également des outils de corrélations basés sur des règles prédéfinies et également sur des règles personnalisables. Ainsi le SIEM permet la détection des incidents de sécurité tels que les violations de politiques de sécurités, les tentatives d'exfiltrations de données, la détection d'un comportement anormal sur les réseaux (botnet, ver informatiques,..). Ce type de solution permet surtout de limiter le temps entre l'intrusion et la détection, un enjeu essentiel aujourd'hui.

En effet, l'enjeu aujourd'hui en termes de sécurité n'est plus vraiment de savoir comment bloquer les attaques ou les menaces parce que certains types de solutions permettent d'y répondre, notamment les solutions de type Firewall, WAF (Web Application Firewall), IPS (Intrusion Prevention System) ou encore anti-virus. Le réel enjeu est de savoir si ces attaques ou menaces ont réellement été bloquées, si elles ont été détectées uniquement dans une partie du réseau, si elles n'ont pas affecté les utilisateurs. Le SIEM va permettre de traquer ces comportements anormaux et ceci sur l'ensemble du SI. Ainsi, les entreprises auront de la visibilité sur les éléments qui auront pu être affectés ou parcourus par ces menaces. La complexité ou l'hétérogénéité de certains environnements rendent le partage d'informations difficile, c'est pourquoi ce genre de solution permet d'avoir une réelle visibilité en termes de sécurité sur l'ensemble de son environnement et non uniquement sur une partie du SI.

Cette visibilité peut se représenter sous forme d'alerte remontée sur un comportement anormale ou par des rapports quotidiens, hebdomadaires ou encore mensuel sur l'activité au sien d'un environnement. On peut également se servir de celle-ci pour rechercher une information et identifier des potentiels problèmes dans son SI puisque ces solutions de SIEM offrent des outils d'aide au diagnostic tels que la possibilité de faire des recherches par mots clés, de positionner des filtres sur certains types de logs ou encore de cibler sur une plage horaire.

L'objectif d'un SIEM est, notamment, de permettre aux équipes sécurité de détecter des attaques grâce à l'exploitation, le filtrage et à la corrélation de ces (millions) de logs provenant de multiples sources d'information (interne ou externe à l'organisation).

A fonctionnement d'un SIEM

En effet, derrière le mot SIEM, il y a un ensemble de moyens techniques qui permettent :

1. la collecte des événements
2. l'agrégation
3. la normalisation des événements
4. la corrélation des informations recueillies
5. le reporting
6. l'archivage des événements
7. le rejeu des évènements

***la collecte* :**

Les logiciels de SIEM prennent en entrée les événements collectés du SI, les journaux système des équipements : pare-feux, routeurs, serveurs, bases de données… Ils permettent de prendre en compte différents formats (syslog, Traps SNMP, fichiers plats, OPSEC, formats propriétaires, etc.) ou nativement le format IDMEF (*Intrusion Detection Message Exchange Format*), spécialement conçu et validé par l'IETF sous forme de RFC pour partager l'information qui intéresse un système de détection et protection aux intrusions.

La collecte peut être de façon passive en mode écoute ou active en mettant en place des agents directement sur les équipements ou à distance.

***L'agrégation** :*

Plusieurs règles de filtrage peuvent être appliquées. Ils sont ensuite agrégés selon les solutions, puis envoyés vers le moteur de corrélation

La normalisation :

Les traces brutes sont stockées sans modification pour garder leur valeur juridique. On parle de valeur probante.

Ces traces sont généralement copiées puis normalisées sous un format plus lisible. En effet, la normalisation permet de faire des recherches multi-critères, sur un champ ou sur une date. Ce sont ces évènements qui seront enrichis avec d'autres données puis envoyés vers le moteur de corrélation.

La corrélation des informations recueillies :

Les règles de corrélation permettent d'identifier un événement qui a causé la génération de plusieurs autres//un virus qui s'est introduit dans le système puis à causer tel incident// (un hacker qui s'est introduit sur le réseau, puis a manipulé tel équipement…). Elles permettent aussi de remonter une alerte via un *trap*, un *e-mail*, SMS ou ouvrir un ticket si la solution SIEM est interfacée avec un outil de gestion de tickets.

Le reporting :

Les SIEM permettent également de créer et générer des tableaux de bord et des rapports. Ainsi, les différents acteurs du SI, RSSI, administrateurs, utilisateurs peuvent avoir une visibilité sur le SI (nombre d'attaques, nombre d'alertes par jour…).

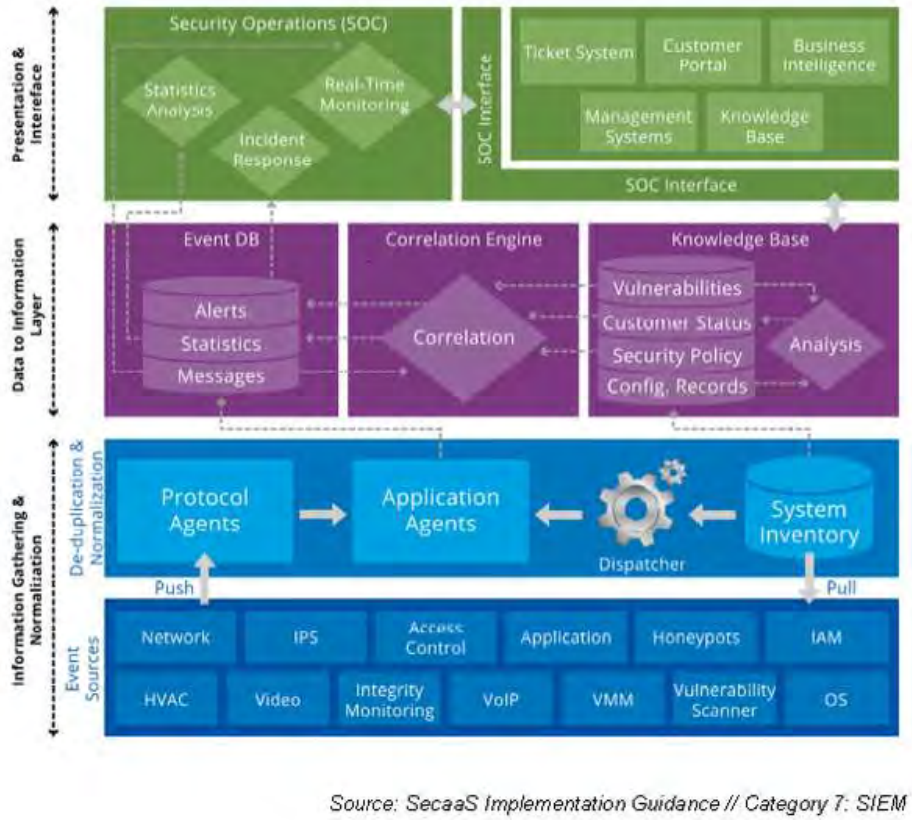
L'archivage des événements:

Les solutions SIEM sont utilisées également pour des raisons juridiques et réglementaires. Un archivage à valeur probante permet de garantir l'intégrité des traces.

Les solutions peuvent utiliser des disques en RAID, calculer l'empreinte, utiliser du chiffrement ou autre pour garantir l'intégrité des traces.

Le rejeu des événements :

La majorité des solutions permettent également de rejouer les anciens évènements pour mener des investigations post-incident. Il est également possible de modifier une règle et de rejouer les évènements pour voir son comportement.



Source: SecaaS Implementation Guidance // Category 7: SIEM

Fig2 : fonctionnement SIEM

B. L'ARCHITECHTURE D'UN SIEM

le schémas ci-dessous illustre l'architecture de référence SIEM.

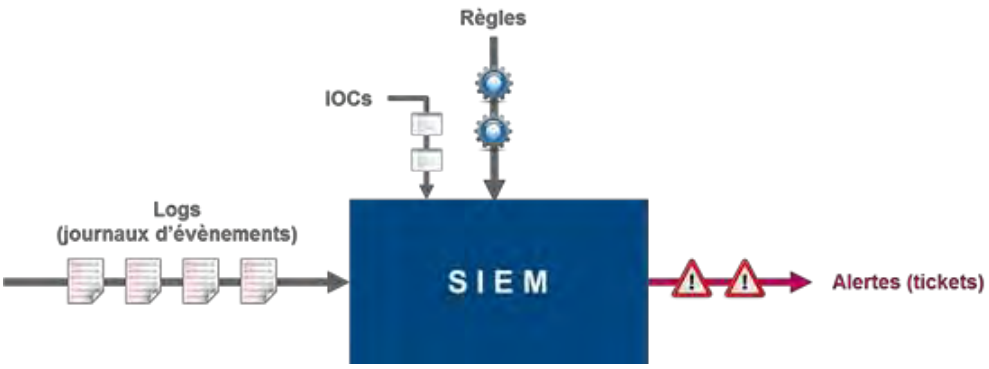


Fig 3 : Architecture d'un **siem**

Légende :

Les logs :
La détection se fait sur la base de journaux d'évènements (logs) provenant de divers équipements du système d'information surveillé (e.g. pare-feu, proxies, IDS, serveurs, applications, etc.).

Les règles :
Ceux sont elles qui décrivent les évènements que l'on souhaite détecter. Exemples : « Un administrateur X échoue son authentification plus de cinq fois en moins de 15 secondes » ou encore « Un compte administrateur réalise une action depuis un poste situé en-dehors de la zone d'administration ».

Les IOC (Indicator Of Compromise) :
Ce sont des indicateurs (noms de fichier, adresses IP, URL, etc.) permettant la création de nouvelles règles de détection plus fines et pertinentes. Exemple : « Présence d'une pièce-jointe de mail au format CAB » ou encore « Accès à l'URL *http://hackmeifyoucan1234.com/donotclickifyouwanttolive.htm* ».
Ici, les IOC sont : le fichier au format « .CAB » et l'URL http://hackmeifyoucan1234.com/donotclickifyouwanttolive.htm.
Si l'une de ces deux règles génère une alerte, une investigation (simple levée de doute dans un premier temps) devra être menée pour déterminer les raisons d'un tel évènement.

Les alertes :
Souvent illustrées sous forme de « ticket » (i.e. une alerte génère un ticket contenant l'ensemble des informations utiles à l'investigation), elles permettent d'indiquer qu'une des

règles implémentées dans le SIEM a été sollicitée (autrement dit, l'évènement redouté associé a eu lieu !).

Compte tenu de la complexité et de l'expertise pointue nécessaire à la gestion d'un tel outil, l'entreprise décide, la plupart du temps, de souscrire à un service auprès d'un prestataire spécialisé, autrement appelé « MSSP » (Managed Security Service Provider) ; ce dernier se chargera alors de toute la maintenance et l'exploitation de l'outil : un service « clef en main ».

C. Les Types de SIEM

Les types de solutions disponibles sur le marché actuel pour couvrir ce besoin sont multiples et peuvent avoir des philosophies différentes. En effet, on peut distinguer plusieurs types de produits. Certains fournissent des produits quasiment vierges en termes de règles de corrélations ou d'alertes et de rapports mais concentrent leurs forces sur la personnalisation, les performances des recherches et la capacité à s'adapter à n'importe quel environnement. Ainsi cette catégorie de solutions permet aux entreprises de créer leur propre SIEM afin de répondre exactement à leurs besoins et pour être le plus efficace possible puisque celui-ci sera façonné autour du SI de l'entreprise. Qui connait mieux le SI que les personnes l'ayant créé ou l'exploitant ? Ceci nécessite certes beaucoup d'investissement mais le bénéfice sera largement supérieur.

On peut avoir une autre catégorie de SIEM concentrant leurs valeurs sur leurs bases de règles de corrélation, d'alertes, de rapports et de parseurs (éléments permettant de catégoriser et normaliser les logs) prédéfinis. Cette catégorie offre également la possibilité d'approvisionner la base de connaissance de la solution afin d'avoir un maximum d'informations sur l'environnement dans lequel elle évolue comme par exemple renseigner les réseaux sensibles pour l'entreprise, les différents utilisateurs ou encore les différentes plateformes. Ces produits sont un peu plus difficiles à appréhender parce qu'ils permettent une multitude de fonctionnalités et de possibilités.

Enfin nous avons une dernière catégorie offrant une solution plus axée sur du « plug and play ».Celles-ci contiennent une base existante de règles de corrélations, parseurs (analyseur) et de rapports. Ces produits ne nécessitent que très peu d'investissement pour l'exploitation et sont généralement simples d'utilisation. Il est également possible de personnaliser les règles de corrélation et d'agrémenter le niveau de connaissance du produit par rapport à l'environnement pour améliorer la détection de menaces. Cependant, ces solutions semblent limitées en termes d'évolutivité et de fonctionnalités mais permettent de rapidement répondre aux besoins sans se noyer dans une solution complexe et difficilement gérable.

Cependant, toutes ces solutions de SIEM ont besoin de « connaître » l'environnement dans lequel elles évoluent. Plus la solution aura une connaissance approfondie de l'environnement et plus elle sera efficace pour détecter des anomalies. C'est notamment sur ces points que les éditeurs se démarquent.

Les Entreprises leaders dans l'édition de solution SIEM sont :

- Alcatel-Lucent *OA Safeguard*

- EMC2 *RSA Security*
- HP *ArcSight*
- IBM Qradar
- LogRhythm *SIEM 2.0*
- NetIQ *Security Manager*
- NitroSecurity *McAfee Enterprise Security Manager* (un produit McAfee)
- Novell *Sentinel*
- Q1 Labs *Qradar* (Groupe IBM)
- Splunk *Splunk Enterprise*
- Symantec *Security Information Manager*
- *USM Alien-vault*

- **Les solutions libres**

Il existe des solutions SIEM libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer PRELUDE de CS et OSSIM, ou Open-Source SIEM du SIEM Alienvault Unified Security Management

L'avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d'étudier et de modifier le code selon nos besoins et de le diffuser. De plus, il existe une communauté importante d'utilisateurs et de développeurs qui participent à l'amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations aux forums.

Chapitre II : les phases de déploiement d'un SOC

II.1 la phase de conception (design)

La plupart des SOC sont construits en réponse à un contexte réglementaire, une contrainte légale ou suite à une prise de conscience du contexte d'insécurité et de menaces ambiant (parfois même en écho à un sinistre passé qui aurait pu être prévenu par un dispositif SOC.
La mise en place d'un SOC est un projet d'envergure (donc généralement visible et suivi par les instances de direction) sur lequel viennent donc s'ajouter des contraintes de planning relativement fortes. Le SOC doit être mis en place, rendu opérationnel et efficace dès que possible pour pouvoir justifier les investissements (CAPEX/OPEX) et les changements d'organisation.
Ces contraintes de planning rendent difficile l'adoption d'une méthodologie réfléchie et partagée en termes de conception, de choix des outils, de recrutement des compétences pour construire et exécuter les services de SOC.
La phase de conception/design doit, a minima, traiter les sujets suivants :

- Définition du périmètre technique
  - Outils déjà mis en œuvre et périmètre déjà couvert
  - Procédures techniques existantes (infrastructures, applicatifs, sécurité ou non)
  - Processus organisationnels (gestion de crise, astreintes, escalades, …)
- Définition du périmètre organisationnel

- Définition de l'organisation cible

Si l'étude de cadrage est le point de départ de tous les travaux, ces réflexions préliminaires sont néanmoins particulièrement importantes et permettent de fédérer les acteurs principaux autours du projet.

II.1.1 l'étude de cadrage

En fonction du périmètre considéré et des activités/organisation de l'entreprise, une première phase de cadrage/opportunité peut être organisée.
Cependant, l'organisation d'un tel projet (pour une Entreprise, par définition, novice dans le domaine) se révèle généralement complexe et chronophage. La recommandation est alors de ne pas hésiter à se faire accompagner par une assistance à maitrise d'ouvrage pour cadrer les débats et préconiser les solutions techniques et organisationnelles pour faire avancer le projet.
La première étape est d'exprimer le besoin de mise en œuvre du SOC et de fixer ses objectifs :

- Pourquoi un SOC pour l'Entreprise ?
- Faut-il un unique SOC ou plusieurs SOC (un dans chaque branche/domaine/entité) ?
- Tout le périmètre doit-il être couvert ? Faut-il se concentrer sur certains périmètres sensibles ?
- Quelles sont les activités opérationnelles en plus de la supervision confiées au SOC ?
- Quelles sont les technologies utilisées et pressentie pour outiller le SOC ?
- Faut-il externaliser le service SOC ou l'internaliser ?
- Faut-il conduire un POC ou construire le SOC ex-nihilo ?

L'étude de cadrage est également l'occasion de répondre et de contrôler les prérequis :

- Existence d'une ou plusieurs PSSI accompagnée de directives de sécurité.
- L'identification des principaux risques et des menaces associées
- La mise en œuvre des mesures de sécurité de base (hygiène SSI).

La seconde étape de l'étude de cadrage se concentre sur les besoins SSI couverts par le SOC :

- Liste des « use cases » standards portés par le SOC
- Construction des scénarios de menaces métiers à couvrir
- Etude Spire ou autres analyses de risques
- Quel temps de rétention des différentes traces collectées ?

Une fois les besoins évalués, l'étude de cadrage se focalise sur la compatibilité technique et organisationnelle du S.I. existant avec la mise en œuvre d'un SOC. Les éléments suivants viennent donc compléter l'étude de cadrage :

- Revue de l'architecture sécurisée existante
- Existence et disposition des serveurs de temps
- Gestion des journaux d'événements et périmètre de collecte
- Volumétrie des journaux actuellement collectés / Durée de rétention.
- Vérification de la politique des logs (verbosité, chiffrement, signature)

D'un point de vue organisationnel, cette dernière partie de l'étude de cadrage se concentre sur :

- L'organisation du projet (RACI)
- La définition du périmètre métier adressé et couvert par le SOC (cf. première étape)
- Définition du socle de base des équipements supervisés :
  - Passerelles internet et de messagerie
  - Système de détection/prévention d'intrusions (IDS/IPS) de flux et de postes
  - Active Directory (et annuaires d'entreprises)
  - Anti-virus de flux et de poste

II.1.2 périmètre organisationnel

Les aspects organisationnels traités pendant la phase de conception concernent à la fois l'organisation de l'équipe de construction et d'exécution mais aussi les autres entités qui doivent être mobilisées pour la conduite du projet (pendant la phase de construction mais aussi pendant la phase d'exécution).
Le « noyau » de l'équipe du SOC et les principaux interlocuteurs du service doivent être identifiés fonctionnellement et nominativement. Généralement, ces acteurs sont :

- Le/les DSI
- Le/les RSSI
- Le/les responsables des risques & de l'audit
- Le/les architectes réseaux/système
- Le/les responsable du SOC
- Le/les responsables d'équipe opérationnelle
- Les analystes

En plus de l'identification précise des acteurs concernés par le projet, la conception doit proposer au moins une trajectoire de mise en place d'un SOC :

- périmètre technique et métier couvert,
- volumétrie collectée et traitée,
- agilité dans la supervision et la réaction,
- montée en efficacité.

Cette trajectoire, doit notamment permettre de convaincre et de justifier les investissements tout en fournissant une feuille de route pour les prochains mois/années d'activités du service.
La phase de conception est également le moment le plus indiqué pour communiquer auprès des équipes techniques et métier.

- Pour les personnels de l'IT, il faut communiquer sur l'évolution de l'organisation induite par la mise en œuvre d'un tel service. L'idée principale de cette communication est que : la mise en œuvre d'un SOC ne doit pas être vécue par les personnels de l'IT comme une perte de contrôle ou une observation à charge des opérations des équipes IT mais comme un complément et une aide.
- Pour les personnels métiers, et en fonction des RACI discutés pendant les ateliers de conception, il faut communiquer sur l'arrivée de ce nouvel acteur et sur les nouveaux circuits de communication (ou sur les modifications à venir). Là encore, le SOC ne doit pas être perçu comme un observateur à charge mais bien comme une aide complémentaire dans la supervision des activités.

Un projet de SOC de par sa nature de « transformation des activités » génère des frictions et des adhérences fortes avec les activités courantes. La communication est le remède et le catalyseur qui limite ces frictions.

II.1.3 périmètre technique

La conception technique du SOC doit se concentrer sur le choix des outils en fonction des équipements à surveiller. La collecte et les opérations de supervision doivent être considérées dans cette étude de conception.

Pour la collecte, la base du travail de conception est d'identifier et de localiser les outils déjà mis en œuvre sur le S.I. : IDS/IPS, pare-feu, détection de fuite de données, boitiers de chiffrement, antivirus, anti-spam, contrôles d'accès et d'identité… Chaque outil doit être associé à son/ses responsables et aux objectifs de sécurité poursuivis.

Cependant compte tenu des cas d'utilisations et des objectifs du SOC, il faut éviter à tout prix de noyer les opérations de collectes par un volume d'événements trop important et non pertinent.

Pour les opérations de supervision, l'étude de conception doit permettre de choisir l'outil majeur et les outils satellites(secondaires) permettant de recevoir, trier, qualifier/prioriser, suivre et traiter les incidents de sécurité. Ces outils doivent être adaptables et paramétrable par rapport aux contraintes de l'Entreprise. Sont notamment à prendre en compte :

- Compatibilité avec le ou les SIEM mis en œuvre ;
- Capacité à prioriser les incidents en rapport avec les échelles gravité/impact de l'Entreprise ;
- Echange et interactions avec d'autres SOC (entités de sécurité de l'Entreprise)

Pour faciliter les opérations de supervision, la liste des actifs critiques de l'Entreprise (serveurs, bases de données, annuaires, …) peut être constituée si elle n'existe pas déjà. Cette identification peut être pilotée/validée par les métiers en fonction de leur propre gestion des risques.

II.2 la phase de construction (buld)

La phase de construction se concentre dans un premier temps sur la collecte et le traitement des événements existant. Il s'agit du socle primaire. Sa construction est séquentielle :

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

En complément de ce socle, la construction considère :

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

Collecte

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

Dans le cadre de la mise en œuvre d'un SOC, la collecte des données doit être réalisée dans l'objectif d'alimenter le service de supervision. Les événements doivent ainsi être formatés pour être exploitables – il faut donc généralement les adapter pour les rendre compatibles avec les objectifs de sécurité du SOC (notez que le SIEM est généralement déployé bien avant les études ou la mise en œuvre d'un SOC dans l'Entreprise).

Dans un premier temps, la collecte concerne :

- les équipements de sécurité
- les applications
- les équipements réseaux

Déployer la collecte sur un périmètre complet est un projet ambitieux.
Compte tenu de la difficulté de la mission, la gestion de projet doit éviter à tout prix l'« effet tunnel » en privilégiant les « mini-succès ». Ce lotissement peut s'appuyer sur les besoins de détection exprimé dans le cadrage du SOC (identification des scénarios de menace, identification des sources concernées par les scénarios d'attaque, collecte des événements permettant la détection du scénario).
En complément de la collecte, le projet doit veiller à :

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

Traitement

Le traitement a pour objectif de s'attacher à la détection des risques les plus redoutés par la structure.
Cependant ce traitement des événements de sécurités produit souvent un nombre important de faux positifs.
Le traitement des événements de sécurité, pour être efficace et réduire le nombre de faux positifs, il est nécessaire de créer des scénarios métiers qui s'appuient sur des règles de corrélation issues des applications métiers et d'infrastructure (équipements).
Le traitement des règles se doit d'être un processus industriel afin de s'assurer qu'aucune menace ne soit oubliée. Le processus de traitement est basé sur la norme ISO 27035 (gestion des incidents de sécurité d'un SOC).

La structure de traitement est décomposée en niveaux 1/2/3. L'intérêt de ces niveaux est de s'assurer que tous les incidents sont traités par les personnes les plus compétentes sur le sujet. Ainsi le niveau 1 va traiter les incidents les plus simples et déclencher le N2 sur les incidents plus compliqués. Le N3 intervient sur les incidents complexes. Le passage d'un niveau à l'autre est appelé processus de triage.
Le processus de triage est basée sur le temps de traitement d'un incident, des
complexité ainsi que de sa criticité. L'objectif du triage est d'adresser les incidents aux personnes les plus compétentes pour les gérer et cela dans les meilleurs délais.

Temps de traitement de l'incident < 30mn **Complexité de faible à moyenne** **Criticité de faible à important**	**Temps de traitement de l'incident < 1 jour** **Complexité de moyenne à forte** **Criticité de important à fort**	**Temps de traitement de l'incident indéfini** **Complexité de forte à critique** **Criticité de fort à critique**

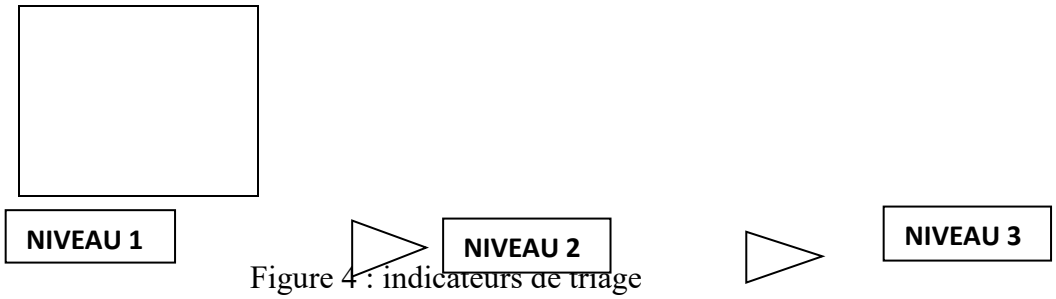


Figure 4 : indicateurs de triage

Le SOC apporte une protection inégale suivant les types de menaces. En ce qui concerne la fuite d'informations, la compromission de systèmes, la protection contre les malwares, les APT(advanced persistent threat) et les menaces ciblées, le SOC reste la meilleure des solutions pour la cyber-protection.

II.3 (Run) la phase de fonctionnement nominale d'un SOC

Un SOC, comme tout outil de sécurité, doit s'inscrire dans la roue vertueuse de Deming (ou PDCA : Plan Do Check Act). Pour ce faire il convient de prendre en compte le processus métier de gestion des incidents de sécurité.

Le schéma ci-dessous illustre une roue de Deming prenant en compte ces différents aspects :

Fig 5 : cycle PDCA roue de Deming

La mission première du processus d'amélioration continue reste le maintien en conditions opérationnelles du SOC par rapport aux objectifs de sécurité qu'il remplit.

Maintenir le fonctionnement nominal d'un SOC et le pérenniser est une tâche complexe et importante qu'il faut prendre en compte dès la conception du SOC. Elle doit être portée par

une volonté managériale forte sous l'exécution d'un manager fort et proche de ses équipes pour pouvoir être réalisée dans des conditions optimales.

II.4 l'évaluation de l'efficacité du SOC

La mesure de performance d'un SOC doit être faite en fonction des missions et de l'engagement du SOC. Ce dernier peut en effet avoir :

- Un engagement de résultats portant sur la détection et la réaction à des scénarios prédéterminés validés et testés. En complément, le SOC doit mettre à disposition les meilleurs efforts à la détection de nouveaux scénarios d'attaque. Cet engagement est le plus fréquemment mis en œuvre car il est facilement mesurable et induit l'obtention d'un niveau minimum de sécurité ;
- Un engagement de moyen portant sur la mise à disposition de ressources et de capacités d'analyse. Ce modèle est très rarement mis en œuvre bien que plus efficace dans la détection d'APTs car il repose avant tout sur la gestion et l'encadrement d'équipe.

Quelle que soit l'engagement choisi pour son modèle, un SOC doit pour démontrer son efficacité répondre à la question : « Comment garantir que l'Entreprise est mieux protégée ? ». Il dispose pour ce faire de plusieurs axes de réponse :

1. Démontrer sa conformité au contrat : Test des scénarios d'attaque convenus et dont la détection et le traitement ont été implémentés au niveau du SOC. Cette recette des scénarios prédéterminés se concentre sur le comportement adopté par le SOC face à la situation, depuis la collecte/détection jusqu'à la remédiation ;
2. Démontrer sa capacité opérationnelle de gestion d'incident au travers de simulations : Tests internes/externes sur les scénarios de menaces (contractuels et de l'état de l'art). Cette démonstration est effectuée en observant les réactions du SOC face aux stimuli non annoncés (pertinence de la détection, temps de détection et de traitement de bout en bout, envergure de la réaction, …) ;
3. Mettre en avant les retours d'expérience internes : Partage des conclusions des attaques déjouées ou subies ;
4. Se comparer avec les autres établissements SOC sur les indicateurs de performances.

L'évaluation par la conduite de test d'intrusion sur les scénarios de menaces couvert par le SOC est désormais une bonne pratique courante qui offre l'avantage d'alimenter le SOC en

nouveaux scénarios d'attaque au plus proche de la réalité. Cette approche en plus de s'inscrire dans la méthodologie ISO d'amélioration continue fournie des retours d'expérience en conditions quasi réelles permettant ainsi au SOC de s'évaluer de manière indépendante. Il ne faut néanmoins pas oublier que ce type de tests bien qu'au plus proche de la réalité, ne remplace pas une attaque réelle qui est souvent par nature complexe et qui implique parfois des contre-feux pour occuper le SOC.

II.4.1 Indicateurs de performance

Il est fortement conseillé d'utiliser des indicateurs standards de place qui en plus d'avoir été conçu par une communauté d'experts, permettent de comparer l'efficacité et l'efficience de son SOC par rapport au marché. De plus dans le cas d'un SOC info-géré, la capacité du prestataire à produire et traiter facilement ces indicateurs est un bon critère d'évaluation de maturité.

Les indicateurs de performances doivent être revus à minima mensuellement par le responsable en charge du SOC (ou SOC leader) pour lui permettre d'avoir une vision factuelle et objective du service fourni. Il doit ensuite restituer les plus pertinents avec son analyse dans les différents comités de pilotage.

Le tableau de bord qu'il produit est généralement constitué d'un transparent avec les indicateurs clés suivi d'un ou plusieurs transparents où sont mis en avant des indicateurs particuliers avec leur analyse. Les indicateurs clés de performance doivent permettre d'évaluer synthétiquement les capacités du SOC et leurs évolutions potentielles.

Vulnérabilités

Un SOC ne doit pas être un moyen aval de ne pas régler un problème de sécurité amont. Pour ce faire il doit participer autant à la correction des vulnérabilités et des faiblesses du SI. Cette participation doit se faire à minima dans le pilotage de l'analyse des causes racines des incidents majeurs ou des incidents répétitifs.

Il peut donc ainsi être également évalué par rapport au nombre de vulnérabilités qui sont corrigées au sein du SI, même si cette correction ne dépend pas directement de ses attributions.

Tickets

Un ticket d'incident peut se résumer comme étant une fiche de suivi de l'incident qui permet de lui attribuer un responsable de sa résolution et d'assurer sa résolution. Il est le livrable métier du SOC, et doit donc en ce sens être évalué.

Incidents

L'une des missions principales du SOC est d'assurer le pilotage de la résolution des incidents de sécurité. À ce titre, il est indispensable de s'assurer que l'ensemble des tickets d'incident

ont été clôturés avec les informations nécessaires pour comprendre les raisons de cette clôture. Ce suivi s'effectue au travers de l'indicateur du reste à faire et par échantillonnage sur les tickets fermés. Notons également que dans certaines circonstances l'entreprise à l'obligation de déclarer ses incidents de sécurité.
Parmi les législations en vigueur imposant la déclaration d'incident de sécurité, nous retiendrons les suivantes :

- France : Obligation de notification des incidents de sécurité informatique pour les OIV (Opérateur d'Importance Vitale) ;
- USA : Obligation de déclaration en cas de fuite de données contenant des informations personnelles ;
- Singapour : Obligation de notification auprès des clients ainsi que de l'autorité de régulation locale (le MAS : Monetary Authority Of Singapore) ainsi qu'à la police en cas de piratage et d'intrusion informatique.

Deuxième partie : réalisation

Chapitre III : étude de la solution OSSIM (open-source security information management)

III.1 Présentation générale de la solution

OSSIM, ou Open-Source SIEM est la version Open-Source du SIEM Alienvault Unified Security Management (USM), développé et commercialisé par la société Alienvault.
Cet outil est fourni sous la forme d'un système d'exploitation complet, basé sur un OS GNU/Linux Debian. Il intègre les applications qui forment le coeur du SIEM (nommé OSSIM), mais également de très nombreux systèmes de détection d'intrusions avec des configurations complètes pour assurer leur fonctionnement au sein du SIEM. En particulier, OSSIM installe par défaut les outils Snort et OSSEC (depuis la version 4 d'ossim, Snort est remplacé par Suricata)

OSSIM est un projet open source de « management 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.
Cette solution est née du constat selon lequel il est difficile encore à ce jour d'obtenir un instantané de son réseau et des informations qui y transitent avec un niveau d'abstraction suffisant pour permettre une surveillance claire et efficace.
Le but d'OSSIM est donc de combler ce vide constaté quotidiennement par les professionnels de la sécurité.

III.2 Principe technique de la solution

OSSIM est une solution fédérant d'autres produits open-source au sein d'une infrastructure complète de supervision de la sécurité (Plate-forme ou framework)
La plate-forme au sens d'OSSIM a pour objectif de centraliser, d'organiser et d'améliorer la détection et l'affichage pour la surveillance des événements liés à la sécurité du système d'information d'une entreprise.
La solution OSSIM fournit donc par le biais de son framework un outil administratif qui permet de configurer et d'organiser les différents modules natifs ou externes qui vont composer la solution.

III.3 ARCHITECTURE OSSIM

Le diagramme suivant fournit une vue de l'ensemble de l'architecture OSSIM.

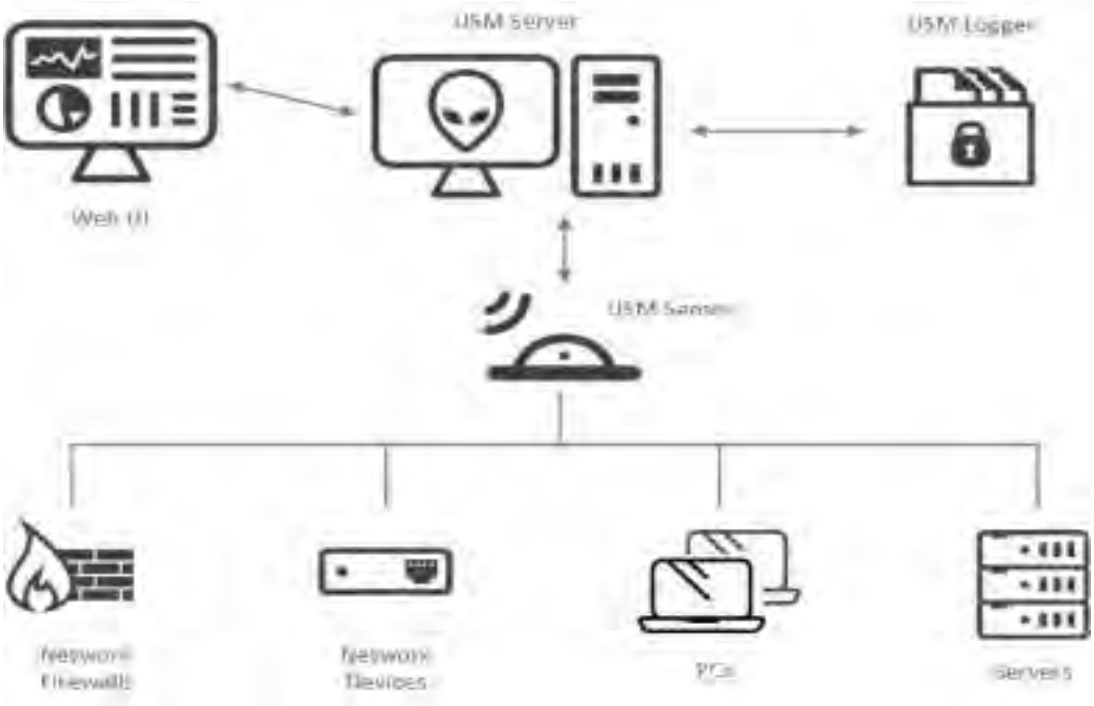


Fig 4 : Architecture OSSIM

L'architecture d'OSSIM d'AlienVault a les deux composantes principales:

- ✓ **OSSIM Sensor** (ou capteur) : Le sensor ou capteur est déployé tout au long du réseau, il permet d'assurer toute la collecte et la normalisation des événements de différents dispositifs sur le réseau.
- ✓ **OSSIM Server** : Le server assure l'analyse, l'agrégation et corrèle les informations recueillies par le capteurs OSSIM, et fournit une gestion unique de l'administration et les rapports.

La version commerciale d'OSSIM qui est USM Alienvault a une troisième composante appelé le **logger**, il permet d'archive en toute sécurité les données du journal (logs) des événements bruts pour les enquêtes judiciaires et des mandats de conformité.

Le capteur OSSIM recueille des données de logs sous leurs formes brutes et d'autres informations à partir de divers périphériques réseau, des serveurs hôtes et des applications ensuite normalise les données dans un format standard-événement, et envoie les événements sur le Server OSSIM. Pour traiter les fichiers log bruts et d'autres informations provenant de différents dispositifs du réseau, l'administrateur peut choisir d'utiliser parmi plus de 200 plugins de capteurs. Une fois que les événements arrivent au Server OSSIM, on peut utiliser l'interface Web de OSSIM pour afficher et analyser les événements, établir des règles de politique et de corrélation, de procéder à l'investigation des alertes, et effectuer d'autres opérations de sécurité sur le réseau.

III.4 LES FONCTIONS D'OSSIM

OSSIM est conçu principalement pour aider les organisations à se défendre efficacement contre les menaces avancées d'aujourd'hui. La plate - forme OSSIM offre cinq fonctions essentielles de sécurité dans une seule console, donnant ainsi la possibilité de gérer la conformité et les menaces.

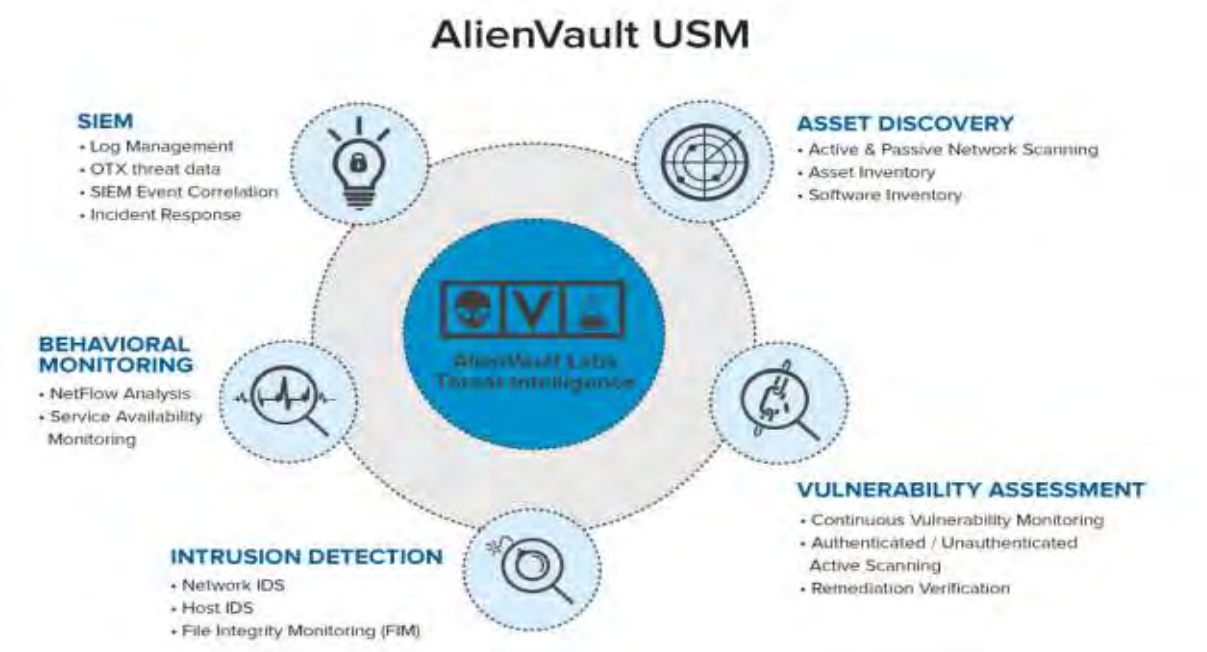


Fig 5 : Les fonctions d'OSSIM

Qu'est-ce qu'un actif ?

Dans OSSIM, un actif est un équipement sur le réseau de l'entreprise qui porte une adresse IP unique. Un actif peut être un serveur, un routeur, un pare - feu, une imprimante ou un PC individuel.

Un actif est contrôlé par au moins un Sensor (agent) OSSIM.

Voici une brève description des fonctions essentielles que fournit OSSIM:

- **Découverte d'actif** (Asset Discovery) : La découverte d'actifs est une capacité de sécurité essentielle d'OSSIM. OSSIM découvre les actifs présents dans votre environnement, détecte les changements opérés sur ces actifs, et découvre les actifs fictifs dans le réseau. La découverte d'actif utilise également le scan (ou balayage), qui peut être programmé pour être effectué périodiquement ou peut être effectuée manuellement.
- **L'évaluation de la vulnérabilité** (Vulnerability Assessment), identifie les vulnérabilités ou la conformité en comparant les programmes présents sur les actifs avec une base de données des vulnérabilités connues. Des Scans de vulnérabilité peuvent également être programmés pour être effectués périodiquement ou effectué manuellement.
- **La détection d'intrusion (Intrusion Detection)** pour les activités malveillantes surveille le trafic réseau, surveille les messages du journal du système, et surveille l'activité des utilisateurs. Sous OSSIM la détection d'intrusion se fait avec des composants de détection d'intrusion basée sur l'hôte (HIDS) et de détection d'intrusion basés sur le réseau (NIDS).
- **La surveillance comportementale (Bihavioral Monitoring)** offre une visibilité sur les tendances du trafic et des flux (données NetFlow), qui sont utilisés pour détecter les anomalies qui pourraient indiquer les violations de la politique de sécurité. Les données utilisées pour le suivi et l'analyse comportementale sont collectées à partir des périphériques réseau, et la surveillance de la disponibilité des actifs.
- **Le SIEM** (gestion des événements et informations de sécurité) combine des informations de sécurité avec les corrélations des journaux recueillies et d'autres données pour trouver des modèles malveillants dans le trafic réseau et au sein de l'activité.

L'architecture d'OSSIM peut être divisée en deux principales étapes :

1. Pré-processing, remontée d'événements des moniteurs et détecteurs dans une base de données commune

2. Post- processing, analyse centralisée

La figure illustre le fonctionnement en deux étapes (comme mentionné ci-dessus). Nous remarquons que ces deux étapes disposent de différentes bases de données permettant la sauvegarde des informations intermédiaires (corrélées).

III.5 LE TRAITEMENT DU FLUX DES ÈVÈNEMENTS

Le traitement du flux est un fonctionnement interne d'OSSIM, voici un schéma type reprenant le flux d'information au travers de la solution.
L'illustration suivante détaille le flux des événements et d'autres informations à partir de l'environnement du réseau tel qu'il est collecté ou généré par le capteurs OSSIM (sensor) et livré au Server OSSIM pour traitement

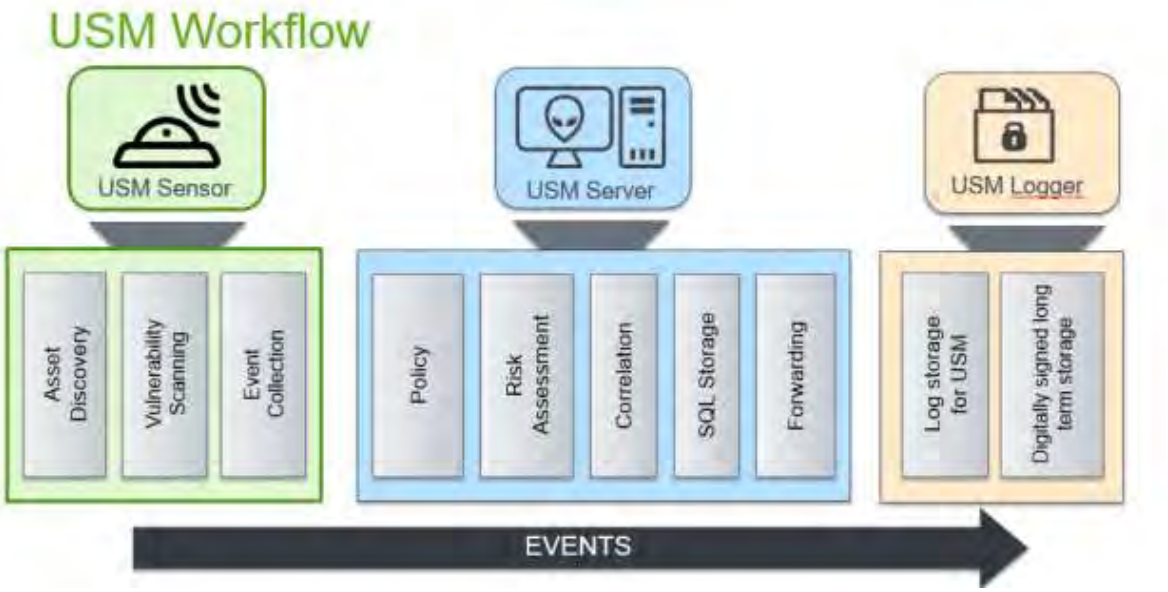


Fig 7 : Flux des événements

- **Principe de traitement du flux d'événement sous OSSIM**

Le traitement du flux peut être divisé en deux principales étapes :

- Prétraitement (ossim-sensor)
- Post-traitement (ossim-server)

Le prétraitement est assuré par **OSSIM-Sensor (capteur ou agent)** qui combine la découverte de l'actif, l'évaluation de la vulnérabilité, la détection des menaces et la surveillance comportementale pour fournir une connaissance de la situation. Le senseur OSSIM est le module de sécurité de premier niveau dans la plate – forme OSSIM et offre une visibilité détaillée dans votre environnement, des vulnérabilités, des cibles, des vecteurs d'attaque et de services.

Le Sensor OSSIM assure la collecte des informations de logs ainsi que la normalisation de celles-ci dans un format d'événement standard afin de les stocker de manière uniforme et de pouvoir les traiter efficacement durant l'étape de post-traitement.

Ces événements normalisés sont ensuite envoyés au composant OSSIM-serveur.

Le post-traitement assuré par le **Server OSSIM** fournit une interface de gestion unifiée à travers l'interface Web d'OSSIM qui combine l'automatisation de la sécurité, et OTX (programme d'échange des menaces de Alienvault) pour corréler des données, réduire les risques et améliorer l' efficacité opérationnelle.

Le **Server OSSIM** reçoit des événements du **Sensor OSSIM** (capteur ou agent) et effectue l'évaluation des politiques. C'est la politique qui définit ce qui se passera avec les événements. Par défaut, les événements sont envoyés au moteur de corrélation, à partir du module d'évaluation des risques, puis stocké dans une base de données SQL interne. Les événements peuvent également être transférés vers un autre Server OSSIM, si nécessaire. Ce flux est entièrement configurable en utilisant les politiques d'OSSIM.

La Corrélation peut être faite logique, où les événements peuvent être comparés à des modèles et de multiples conditions peuvent être connectés en utilisant des opérateurs logiques tels que OR et AND. La corrélation peut être calculée au moyen de la corrélation croisée, où les événements sont corrélés avec les données de vulnérabilité. Après que les événements soient traités et corrélés, le Server OSSIM effectue des analyses de risque et déclenche une alarme si le risque de l'événement est assez élevé.

Le **Logger** qui est la composante propre à la version commerciale USM-Alienvault permet l'archivage sécurisé des données de la plate – forme. Il stocke une copie de toutes les données d'événement USM qui peut être utilisé pour les rapports de conformité, ou récupérée plus tard pour forensics (l'investigation) et enquêtes sur les incidents passés.

Remarque :
Les logs peuvent être centralisées et/ou consolidées au préalable avant d'être collectées par les agents OSSIM. Ceci afin de diminuer l'utilisation de la bande passante du réseau.
Les détecteurs (quels qu'ils soient) traitent les événements jusqu'à ce qu'une alerte soit identifiée soit par signature, soit par la détection d'une anomalie.

Remarque
Les alertes peuvent être préalablement traitées par un outil de consolidation avant d'être envoyées au collecteur OSSIM. Ceci permettant de limiter l'utilisation de la bande passante du réseau.

- Le collecteur reçoit les alertes au travers des différents protocoles disponible (SNMP, etc …)
- Le parser(l'analyseur) normalise ces alertes et les stocke dans la base de donnée des événements (EDB)
- Le parser se charge également d'affecter des priorités aux alertes en fonction des politiques définie dans le panneau de contrôle ainsi que de toutes les informations systèmes dans les inventaires des équipements attaqués.
- Le parser 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 complète ou plus fiable. Ces nouvelles alertes sont renvoyées au parser pour être à nouveau stockées, priorisées et évaluées par rapport aux politiques de risques et ainsi de suite …
- Le moniteur 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 alertes les plus récentes, met à jour l'état de tous les métriques qu'il compare à leurs seuils, et envoie alors de nouvelles alarmes ou effectue les actions appropriées selon les besoins.

- Depuis le panneau de contrôle, l'administrateur peut également voir et/ou établir un lien entre tous les événements 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.

III.6 Les fonctionnalités d'OSSIM

Dans cette partie, on présente au mieux les différentes possibilités offertes par la solution OSSIM.
Les fonctionnalités d'OSSIM peuvent être représentée de manière simple et graphique en un découpage sur 9 niveaux tel que le montre le schéma suivant :

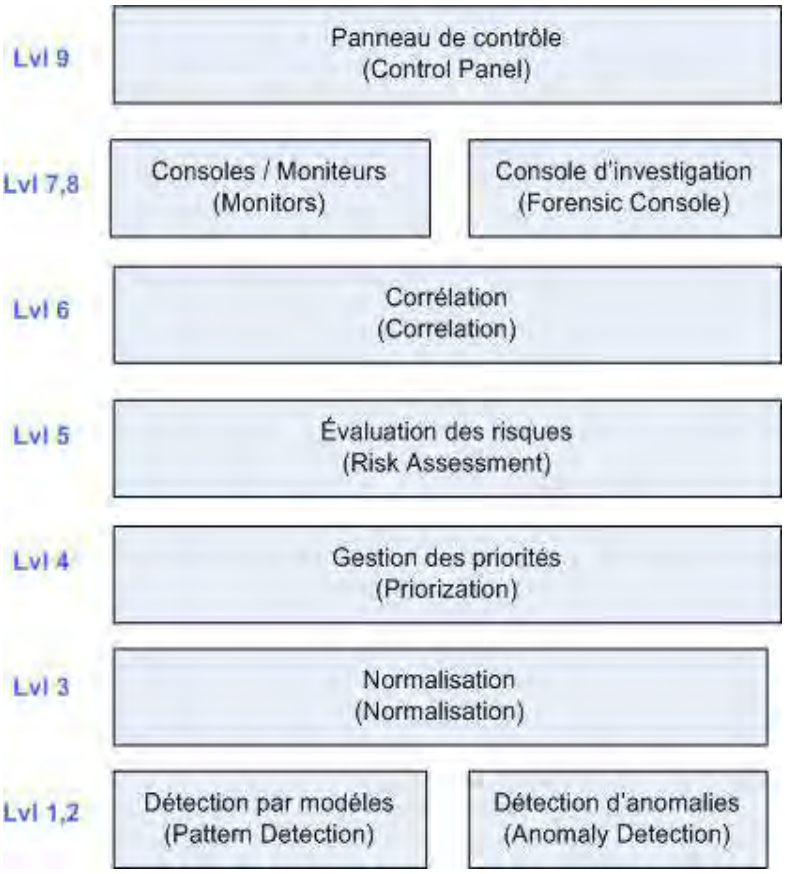


Fig 9 : les fonctionnalités d'OSSIM

6.1) La Détection par signature ou par modèles (Pattern Detector) – Level 1

La plupart des détecteurs traditionnels fonctionnent en utilisant des modèles, le meilleur exemple étant les systèmes de détection d'intrusion (IDS), qui sont capables de détecter un modèle d'attaque défini en utilisant des signatures ou des règles.
Lorsqu'une intrusion connue est repérée lors de l'utilisation du système, une alerte est levée.

La détection par signatures a des limites. Elle ne connait pas l'objectif de l'activité correspondant à une signature et va donc déclencher une alerte même si le trafic est normal. De plus, la détection par signature exige de connaitre préalablement l'attaque afin de générer la signature précise correspondante (fonctionnement par liste noire, exemple : antivirus). Ceci implique qu'une attaque encore inconnue ne pourra pas être détectée par signature. C'est le cas des attaques de type « **Zeroday** »qui est l'exploitation d'une nouvelle vulnérabilité avant l'apparition de la mise à jour

Rappel

a) Faux positifs
Un faux positif est un événement remonté par un dispositif de détection d'intrusion mais qui ne correspond pas réellement à une attaque ou une vulnérabilité. Il s'agit d'une erreur de détection faite par l'équipement.

b) Faux Négatifs
Un faux négatif est une attaque ou une vulnérabilité valide non découverte par le dispositif de détection d'intrusion.

La plupart des dispositifs comme les routeurs et les firewalls incluent également des mécanismes de détection par modèle. Ils sont ainsi capables de détecter, par exemple, les scans de port, les tentatives de spoofing, et les attaques par fragmentation.
Il y a également des détecteurs pour les événements de sécurité dans les systèmes d'exploitation. Ils sont capables d'envoyer des alertes pour d'éventuels problèmes de sécurité, et presque tous incluent leur propre enregistreur, comme le syslog pour les nix.
En fait, n'importe quel élément dans le réseau, tel qu'un routeur, un poste de travail, un firewall, etc., a une certaine capacité pour la détection. Et le but d'OSSIM est justement de rassembler les événements de tous les systèmes critiques afin d'atteindre un des principaux objectifs : obtenir une vue complète du réseau.

6.2) La détection d'anomalies (Anomaly Detector) – Level 2

La capacité à détecter des anomalies est plus récente que la détection par modèles. 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.
Cette nouvelle fonctionnalité opposée au principe de détection par modèles fournit un point de vue différent mais complémentaire 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.
De même, dans le cas d'un ver qui aurait été introduit sur le réseau de l'entreprise, une attaque de Spamming, et même l'utilisation des programmes de P2P qui produiraient un certain nombre de connections anormales qu'il est facile de détecter
La détection d'anomalies permettrait également de détecter :

- Une utilisation des services dont la source ou la destination ne serait pas normale
- Une utilisation à des heures anormales
- Une utilisation excessive du trafic ou des connections

- Une copie anormale de fichiers sur le réseau interne
- Un changement de système d'exploitation sur une machine
  Etc …

La remontée de ces informations est prise en tant qu'information additionnelle qui complète les alertes traditionnelles par modèles, cela permet de mieux évaluer les alertes et donc de différencier celles qui pourraient avoir des conséquences plus importantes (plus risquées).

6.3) Centralisation et Normalisation – Level 3

La normalisation et la centralisation (ou l'agrégation) ont pour objectif d'unifier les événements de sécurité de tous les systèmes critiques de l'entreprise dans un format simple et sur une seule console.
Cela permet notamment d'obtenir une vue considérablement complète de ce qui se passe partout sur le réseau. 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.
Tous les produits de sécurité ont normalement une capacité de gestion centralisée en utilisant des protocoles standard. C'est pour cela qu'OSSIM, en se basant sur ces protocoles, met en oeuvre un processus d'agrégation.
La normalisation exige quant à elle un parser (analyseur) ou un traducteur au courant des types et des formats d'alertes venant de différents détecteurs. La base de données est organisée et la console d'investigation adaptée afin d'homogénéiser le traitement et l'affichage de tous ces événements.
De cette façon il est donc possible d'observer tous les événements 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 également vivement encouragée par la communauté de développeur d'OSSIM et bon nombre d'acteurs de la sécurité en général.
L'IDMEF est un standard établit 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. Ils n'ont malheureusement pas toujours accès aux mêmes informations systèmes et n'ont pas non plus le même niveau de détails.
C'est pour cela que le standard a été mis au point en se basant sur un modèle de données flexible, à savoir un modèle objet. Le modèle objet, en effet, permet facilement l'extension des détails des informations via l'agrégation et l'héritage.
En fait, si l'on considère une alerte remontée à OSSIM par un équipement.
Si cet équipement étend par agrégation ou héritage le modèle de base de l'alerte, et qu'OSSIM ne sait pas interpréter toutes les informations, OSSIM pourra malgré tout traité la partie d'information qu'il est capable d'interpréter.

Remarque :
Il faut bien garder à l'esprit que ce standard doit permettre à des équipements de détection d'être plus ou moins précis mais ne doit pas produire d'informations contradictoires. Les éléments de base communs à deux alertes provenant d'un même événement mais remontés par deux équipements différents doivent absolument rester identiques.

6.4) Gestion des priorités (Priorization) – Level 4

Soit une machine qui tourne sous UNIX avec un serveur web Apache.
Si OSSIM reçoit une alerte pour cette machine au sujet d'une attaque sur Microsoft IIS, l'alerte devrait se voir attribuer une priorité basse.
Autre exemple, si un utilisateur établit une connexion suspecte à un serveur, le système devrait

- Lui accorder une priorité maximum si l'utilisateur est externe au réseau et attaque la base de données de client.
- Lui accorder une priorité basse si l'utilisateur est interne au réseau et attaque une imprimante réseau.
- Ignorer si l'utilisateur est quelqu'un qui test normalement des serveurs de développement.

On s'aperçoit ici que la priorité d'une alerte dépend donc de la topologie et de l'inventaire des systèmes de l'entreprise.
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, et d'où à où) :

Les processus de gestion des priorités dans OSSIM sont définis au niveau du framework dans lequel il est possible de configurer les éléments suivants :

- La politique de sécurité, ou l'évaluation des équipements selon la topologie et des flux de données.
- Inventaire
- Évaluation des équipements
- Évaluation des risques (Gestion de la priorité des alertes)
- Évaluation de la fiabilité de chacun alerte
- Définition d'alarme

Remarque :
La gestion des priorités est l'une des étapes les plus importantes dans le filtrage des alertes reçues par les détecteurs. Elle doit être exécutée en utilisant un process continu d'amélioration et de retour d'expérience de l'entreprise

6.5) Evaluation des risques – Level 5

//Rappel : Les risques sont souvent la contrepartie des enjeux dans une entreprise.

Le risque peut être défini comme étant la probabilité de menace de l'événement. En d'autres termes, cette étape tente de définir si la menace est réelle ou pas.
L'importance à donner à un événement dépend principalement de trois facteurs :

- La valeur du bien attaqué
- La menace représentée par l'événement
- La probabilité que l'événement apparaisse

Les trois facteurs vus ci-dessus sont la base du calcul du risque intrinsèque.

Dans OSSIM , tous les actifs et le réseau ont une valeur allant de 0 à 5, 0 étant le moins important et 5 le plus important. Pour décider de la valeur de l'actif, le système vérifie d' abord si une valeur a été affectée manuellement. Dans le cas contraire, le système utilise la valeur du réseau où appartient l'actif. Si le réseau ne dispose pas d'une valeur d'actif, OSSIM attribue l'actif la valeur par défaut de

OSSIM utilise la valeur de l'actif pour calculer le risque d'événement. OSSIM calcule la valeur du risque pour chaque événement après son arrivée au Server. Le système utilise la formule suivante pour calculer le risque:

Risque = (valeur de l'actif * priorité de l'événement * Fiabilité de l'événement) / 25

Où:

- La valeur de l'actif est 0-5.
- une priorité de l'événement va de 0 à 5.
- Fiabilité de l'événement est comprise entre 0 et 10.

Par conséquent, la valeur du risque est de 0 à 10. Les décimales sont toujours arrondies vers le bas. Par exemple, si la valeur est 3, la priorité de l'événement est 3, et la fiabilité de l'événement est de 5, vous obtiendrez 3 * 3 * 25/05 = 1,8. Dans ce cas, le risque pour l'événement est 1.

Dans OSSIM , tout événement avec une valeur de risque supérieur ou égal à 1 génère une alarme (alerte).

AlientVault recommande de ne pas modifier la valeur de l'actif OSSIM. L'OSSIM génère ses propres événements, dont la plupart sont d'information. Par conséquent, augmenter la valeur de cet actif (qui augmente le risque de ces événements) va générer un plus grand nombre de fausses alarmes.

Etant donné qu'OSSIM offre un traitement temps réel des alertes, le calcul du risque immédiat peut être associé à la situation courante.
Ce risque offre une vision de l'évaluation des dégâts qu'une alerte reçue pourrait engendrer. Cette évaluation prendra aussi en compte la fiabilité du capteur ayant émis cette alerte. Le risque immédiat est donc calculé pour chaque alarmes reçues et indique l'importance de l'alarme en terme de sécurité.

6.6) Corrélation – Level 6

Ce procédé permet notamment de retrouver certaines relations entre différentes alertes indépendantes.
Ceci permettra par exemple de découvrir des attaques noyées dans le flot des alertes ou encore de discréditer des alertes (découverte de faux positifs).
La corrélation peut être simplement définie comme un procédé traitant des données (inputs) et retournant un résultat (outputs). OSSIM utilise deux types d'inputs :

- ✓ Informations du moniteur (qui fournit normalement des indications à l'administrateur)
- ✓ Informations des détecteurs (qui fournissent normalement des alarmes)

Le résultat de ce traitement sera lui aussi d'un des deux genres cités ci-dessus (du moniteur ou des détecteurs).

Les modèles de corrélations utilisés par OSSIM ont les objectifs suivants :

– Utilisation de méthodes par signatures, pour la détection d'événements connus et détectables
– Utilisation de méthodes sans signature, pour la détection d'événements non connus
– Utilisation d'une machine d'états configurable par l'utilisateur, pour la description de signatures complexes
– Utilisation d'algorithmes évolués, pour l'affichage général de la sécurité.

Méthodes de corrélation

OSSIM met en oeuvre plusieurs méthodes de corrélation complémentaires :

- Corrélation utilisant des séquences d'événements, basées sur les signatures connues et détectables
- Corrélation utilisant des algorithmes heuristique (Technique consistant à apprendre petit à petit, en tenant compte de ce que l'on a fait précédemment pour tendre vers la solution d'un problème), utilisée pour la détection d'attaques non connues
- Cross-corrélation (corrélation croisée) permettant la recherche de relations entre les scans **Nessus** effectués et des alertes détectées

Corrélation par heuristique OSSIM implémente un algorithme d'heuristique comme un accumulateur d'événements (CALM) (Compromise and Attack Level Monitor), offrant une indication de l'état général du réseau. L'objectif de ce traitement est d'obtenir en premier lieu, le risque immédiat (définit ci-dessus) puis, le risque accumulé.

- Le risque immédiat offre un haut niveau de monitoring temps réel. Celui-ci peut être assimilé à un "thermomètre" des situations critiques, sans même connaitre les détails des caractéristiques du problème.
- Le risque accumulé offre quant à lui un haut niveau de monitoring sur une certaine fenêtre temporelle (risque accumulé et non plus temps réel).

Le second algorithme heuristique utilisé par OSSIM permet la prévision des statistiques réseaux (paquets émis et reçus) en fonction des valeurs précédentes (***Holt-Winter)***. Ceci permettra la détection automatique d'anomalies réseaux.

Par conséquence, la corrélation par heuristique offre :

- ✓ Une vue globale et rapide de la situation
- ✓ Une détection possible d'attaques, non relevées par les autres méthodes de corrélation (se basant sur des signatures)

CALM (Compromise and Attack Level Monitor), est un algorithme (algorithme utilisé dans OSSIM) utilisant les événements accumulés et fournissant une valeur indicative du niveau de sécurité global. L'accumulation d'événements est effectuée indépendamment pour tous les

éléments du réseau. Celle-ci est simplement calculée par la somme de deux variables d'état représentant le risque immédiat de chaque événement :
1. Variable "C" ou niveau de fiabilité d'une machine ou d'un réseau, mesure la probabilité qu'une machine ou un réseau soit compromis (source d'une attaque effectué par un ver ou troyen installé sur une machine à surveiller).
2. Variable "A" indique la probabilité que la machine ou réseau à surveiller soit la cible d'attaques.
La variable "A" représente la probabilité qu'une attaque a été lancée et qu'elle est réussie, alors que la variable "C" fournit l'évidence qu'il y a eu une attaque et qu'elle a réussi.
Chaque machine du réseau a donc une variable "A" et "C" associée, fluctuant de la manière suivante :
1. Toute attaque possible d'une machine 1 (source) vers une machine 2 (cible) incrémentera le niveau
"A" de la machine 2 et le niveau "C" de la machine 1.
2. Lorsqu'une réponse à une attaque est détectée (signifiant que l'attaque est réussie), le niveau "C" des deux machines sera incrémenté.
3. Lorsque l'événement est interne (source interne), seul le niveau "C" de la machine source est incrémenté.
CALM fonctionne d'une manière temps réel (accumulation temps réel des événements). Il peut aussi être intéressant d'observer ces statistiques dans une fenêtre temporelle (accumulation sur le temps). En effet, ceux-ci varieront grandement en fonction de la fenêtre utilisée puisqu'un fonctionnement temps réel (accumulation continue d'événements) aura pour effet de noyer certaines alarmes critiques dans la masse d'information. Nous pourrions assimiler le fonctionnement d'accumulation sur le temps à un zoom sur les statistiques temps réel.

Holt-Winter Algorithme, algorithme heuristique implémenté dans le moteur de corrélation temps réel d'OSSIM, permettant la découverte de comportements anormaux sans l'utilisation de seuils.

Corrélation par diagramme d'états (séquence d'événements) Ce genre de corrélation fait appel à la détection par signatures. Ceci permettra à l'utilisateur (administrateur réseau en charge de la sécurité), de définir des règles de corrélation à l'aide des signatures disponibles.
Exemple : Si l'alerte A, B et C est levée, il faut exécuter l'action D.
Le moteur de corrélation d'OSSIM a les caractéristiques suivantes :

- Capacité de définir des variables d'origines et de destination.
- Utilisation des alarmes des détecteurs (détection par signature) et/ou des informations des moniteurs (monitoring) comme input pour la corrélation.
- Utilisation de variables élastiques (accumulant des informations au cours du temps)
- Architecture récursive (possibilité d'utiliser des règles précédemment définie dans de nouvelles règles)

6.7) Console / Moniteurs – Level 7

Les consoles de monitoring utilisent les différentes données produites par les procédés de corrélation (décrit ci-dessus) pour la construction d'un affichage efficace et/ou résumé.
Ces consoles ne sont pas à proprement parlé des fonctionnalités puisque ce sont en fait de simples représentations des processus précédemment expliqués, Le monitoring consiste en l'affichage des informations fournies.

Mais il me semble important de les présenter pour bien comprendre leur intérêt au sein de la solution OSSIM.

a) Moniteur de risque

OSSIM possède un moniteur de risque appelé RiskMeter qui permet l'affichage des données produites par l'algorithme CALM.
Ces valeurs mesurent le niveau de compromission (C) et le niveau d'attaque (A).
Ces indicateurs de risque sont dérivés des alertes et indiquent la possibilité qu'une machine ait été compromise.

b) Moniteurs d'utilisation, de session et de profils

Comme expliqué dans la section sur « la détection d'anomalies »,
OSSIM place beaucoup d'importance dans la surveillance détaillée de chaque machine et profil.
Il y a trois types de consoles pour ce genre de surveillance :

- Le moniteur d'utilisation qui fournit des informations générales au sujet de la machine, telle que le nombre de bytes transmis par jour.
- Le moniteur de profil qui fournit des informations spécifiques au sujet de l'activité d'utilisateur, permettant d'établir un profil. Par exemple, l'utilisation de SMTP, POP et http constitue un profil d'utilisateur « normal ».
- Le moniteur de session qui fournit un affichage en temps réel des sessions associées à un utilisateur, ainsi qu'un instantané de cette machine sur le réseau.

Ces trois moniteurs sont essentiels pour un système de sécurité. En leur absence l'administrateur de sécurité serait aveugle aux événements passés et ne pourrait pas distinguer une activité normale d'une activité anormale.
Ce secteur de la sécurité coïncide avec l'administration de réseau, mais un certain chevauchement est inévitable puisque, par exemple, la saturation d'un réseau ou le comportement anormal d'une machine pourrait indiquer un problème de réseau ou un problème de sécurité.
OSSIM offre à travers ces trois consoles de surveillance la capacité, en s'appuyant sur des produits, d'agir en tant que sniffers et de la situation du réseau au degré de détail le plus élevé.

a) Moniteur de chemin (Path monitor)

Ce moniteur offre un affichage temps réel des chemins de l'information empruntés par des données émises par différentes machines sur le réseau. Il utilise les informations fournies par le moniteur de session (identifiant chaque lien présent sur le réseau) et par le moniteur de risque (fournissant le niveau de risque de chaque machine) afin de construire un affichage agréable (à l'aide de différentes couleurs).

Deux méthodes d'affichage et d'analyse sont disponibles.

- ***Hard link analysis*** (Analyse des liens TCP)

Cette méthode affiche uniquement les sessions TCP courantes. Le but de celle-ci est de pouvoir observer la propagation d'une attaque ou d'un ver afin de déterminer un périmètre de sécurité.

- ***Soft link analysis***

Cette méthode d'analyse offre l'affichage de tous les liens perçus sur le réseau (UDP, TCP, ICMP inclus).

6.8) Console d'investigation (Forensic Console) – Level 8

La console d'investigation permet d'accéder à toutes informations recueillies et stockées par les collecteurs.
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 événements de sécurité par rapport à tous les éléments critiques du réseau a posteriori et d'une façon centralisée. A la différence du moniteur de risque détaillé dans la section précédente, cette console permet d'explorer chaque événement qui se produit dans le système avec un maximum de détails

6.9) Panneau de contrôle (Control Panel) – Level 9

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 qu'elle a décidé de mettre en œuvre.
Le panneau de contrôle permet de définir une série de seuils ou d'objectifs que l'entreprise devrait rencontrer.
Ces seuils sont définis en tant que valeurs absolues ou relatives comme par exemple le degré d'anomalie.
Il est possible également d'assigner pour des alarmes des processus pour envoyer une alerte à l'administrateur ou exécuter n'importe quel processus automatique, quand des seuils définis sont dépassés.

Remarque :
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.

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 que problème qui a été identifié.

A titre d'exemple, le panneau de contrôle peut remontrer les informations suivantes :

- La surveillance constante du niveau de risque pour les réseaux principaux de l'entreprise.
- La surveillance des machines ou des sous réseaux qui dépassent le seuil de sécurité
- La surveillance constante du réseau global, des hosts, et des niveaux de paramètre des services :
  - ✓ Sortie et trafic sur les réseaux principaux
  - ✓ Ressources principales de base de données
  - ✓ Latence des services critiques
  - ✓ Nombre de transactions des services critiques

- La surveillance des réseaux ou des niveaux de paramètres des services qui surpassent un seuil établi :
  - ✓ Nombre d'email, de virus, et d'accès externes

- ✓ Latence des services, et leur utilisation du trafic
- La surveillance des profils qui surpassent les seuils pour :
  - ✓ Utilisation du trafic
  - ✓ Utilisation des services critiques
  - ✓ Utilisation des services anormaux
  - ✓ Changements de configuration
  - ✓ Toute autre activité anormale

Remarque :
Le panneau de contrôle est totalement adaptable aux besoins du client.
À la différence de toutes les autres fonctions, il inclura seulement un échantillon personnalisé en fonction des besoins.

4) Fonctionnement du flux d'information dans OSSIM (Data flow)

Afin d'aider à la compréhension, nous allons détailler le cheminement d'une alerte dans l'architecture d'OSSIM. Le schéma de la figure ci-dessous, illustre le fonctionnement d'OSSIM d´ecrit ci-dessus :

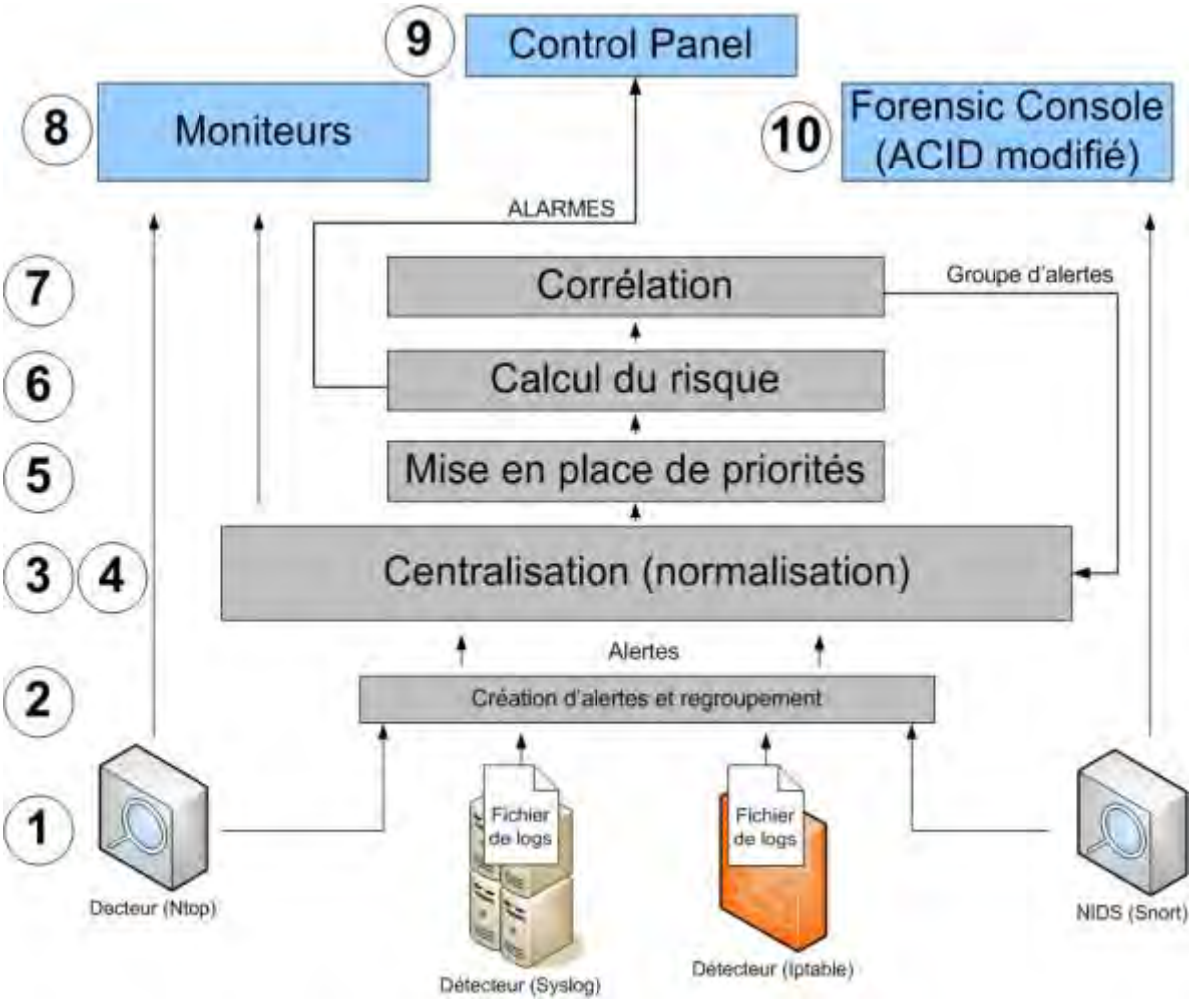


Fig 10 : DATA FLOW DU SERVER OSSIM

1. Détection d'un événement suspect par un détecteur (par signatures ou par l'heuristique).

2. Si nécessaire, des alertes sont regroupées (par le détecteur) afin de diminuer le trafic réseau

3. Le collecteur reçoit la/les alerte(s) via différents protocoles de communications ouverts

4. Le parser (l'analyseur) normalise et sauve les alarmes dans la base de données d'événements (EDB)

5. Le parser assigne une priorité aux alertes reçues en fonction de la configuration des politiques de sécurités définies par l'administrateur sécurité

6. Le parser évalue le risque immédiat représenté par l'alerte et envoie si nécessaire une alarme interne au Control panel

7. L'alerte est maintenant envoyée à tous les processus de corrélation qui mettent à jour leurs états et envoient éventuellement une alerte interne plus précise (groupe d'alerte provenant de la corrélation) au module de centralisation.

8. Le moniteur de risque affiche périodiquement l'état de chaque risque calculé par CALM.

9. Le panneau de contrôle affiche les alarmes les plus récentes et met à jour les indices des états qui sont comparés aux seuils définis par l'administrateur. Si les indices sont supérieurs aux seuils configurés, une alarme interne est émise.

10. Depuis le panneau de contrôle, l'administrateur a la possibilité de visualiser et rechercher des liens entre les différentes alarmes à l'aide de la console forensic

Chapitre IV **: Mise en œuvre de la solution OSSIM**

Les fonctionnalités d'OSSIM ayant déjà été traités et illustrées précédemment, on va surtout dans cette partie expliquer le contexte technique de la topologie choisie et réalisé, en expliquant mes choix.

OSSIM peut intégrer les composants logiciels de sécurités open-source suivants:

- PRADS , utilisés pour identifier les hôtes et services par la surveillance passive du trafic réseau. Ajouté dans laversion v4.0
- OpenVAS , utilisée pour l'évaluation de la vulnérabilité et de corrélation croisée des (système de détection d'intrusion (IDS) des alertes et Scanneur de vulnérabilité) informations.
- Snort , utilisé comme un système de détection d'intrusion (IDS), et également utilisé pour la corrélation croisée avec Nessus.
- Suricata , utilisé comme un système de détection d'intrusion (IDS), à partir de la version 4.2 ce sont les IDS utilisés dans la configuration par défaut
- Tcptrack, utilisée pour les informations de données de session qui peut accorder des informations utiles pour l'attaque corrélation.
- Nagios , utilisé pour surveiller les informations d'hôte et la disponibilité de service basé sur une base de données d'inventaire d'accueil.
- OSSEC , un système de détection d'intrusion basé sur l' hôte (HIDS).
- Munin , pour l'analyse du trafic et le service watchdogging.
- Nfsen / NFDump, utilisé pour recueillir et analyser les NetFlow informations.
- Fprobe, utilisé pour générer NetFlow données de trafic capturé.

Note: Suricata et Snort ne peuvent pas être utilisés en même temps.

➢ A propos des systèmes de détection d'intrusion

Un système de détection d'intrusion (IDS) surveille les réseaux et les hôtes dans la recherche d'activités malveillantes ou de violations de règles telles que le compromis de confidentialité, la sécurité du système ou l'intégrité. Certains systèmes IDS peuvent être capables d'arrêter une tentative d'intrusion, mais ceci n'est ni nécessaire ni attendu d'un système IDS. Les systèmes IDS se concentrent principalement sur l'identification d'intrusions possibles, l'enregistrement d'informations à leur sujet et les tentatives de rapports, que les analystes de sécurité peuvent analyser plus tard.
Les firewalls de réseau classiques analysent les en-têtes de couche réseau et de transport, tels que l'adresse IP source et de destination, le protocole et les ports source et de destination. Cependant, les attaques de nos jours ne visent plus seulement les couches de réseau et de transport, puisque les firewalls de réseau les protègent bien; Au lieu de cela, ils se concentrent sur l'exploitation des vulnérabilités dans les systèmes d'exploitation, les applications et les protocoles. Les pare-feu réseaux ne peuvent pas détecter de telles attaques. Par conséquent, vous avez besoin de systèmes de sécurité supplémentaires, tels que les IDS, afin de les détecter. D'autres exemples d'attaques que l'IDS peut détecter, mais le pare-feu ne peuvent pas inclure:

- Les attaques qui utilisent le tunneling, également connu sous le nom "port forwarding", à l'intérieur du trafic légitime ou le cryptage
- Attaques dans les réseaux internes

Les systèmes IDS se répartissent généralement en deux catégories:

- Network IDS (NIDS) - Placé à des points stratégiques d'un réseau pour surveiller le trafic entre les périphériques et les hôtes du réseau.

- IDS basé sur l'hôte (HIDS) - Fonctionne sur des systèmes hôtes individuels et surveille le trafic depuis et vers le système hôte ainsi que sur les activités du système lui-même.

OSSIM fournit à la fois des capacités de détection d'intrusion basées sur le réseau et l'hôte.

✓ À propos du système de détection d'intrusion réseau (NIDS)

Vous placez habituellement un système de détection d'intrusion de réseau (NIDS) à un point stratégique du réseau, tels qu'au niveau pare-feu où il peut surveiller le trafic entre tous les dispositifs. De cette façon, le NIDS détecte les activités malveillantes qui tombent à travers le pare-feu réseau. Un NIDS fonctionne généralement en mode promiscuité, en surveillant une copie du trafic réseau. Il analyse le trafic en le comparant à une base de données d'attaques connues, également appelées signatures, ou en détectant des anomalies dans les modèles de trafic. Lorsqu'il est identifié, un événement NIDS est généré et signalé à la station de gestion.

Avantages des NIDS:
- Il surveille le trafic du réseau tout entier s'il est placé correctement dans un réseau.
- Il n'a aucune incidence sur les performances et le débit du réseau car il analyse uniquement la copie du trafic réseau.
- Il n'a pas d'impact sur la disponibilité du réseau, car il n'est pas en ligne avec le trafic réseau.

Limites de NIDS:
- Il ne peut pas analyser les informations cryptées.
- Elle nécessite des mises à jour de signatures continues.
- Elle nécessite une configuration réseau spécifique pour recevoir une copie du trafic.
- Il ne peut pas bloquer les attaques.

✓ À propos du système de détection d'intrusion de l'hôte (HIDS)

Un système de détection d'intrusion basé sur l'hôte (HIDS) surveille le comportement et l'état d'un système informatique, ainsi que les paquets réseau que le système envoie et reçoit. Un HIDS s'exécute en tant qu'agent sur un système, qui envoie des événements détectés à une station de gestion. L'agent HIDS surveille généralement quels programmes accèdent à ces ressources et détermine si une application a effectué une modification non autorisée de la mémoire, d'un fichier ou d'une base de données. Un HIDS peut également examiner l'état d'un système et surveiller des journaux spécifiques au système afin de détecter tout changement significatif sur le système.
Alors qu'un NIDS détecte les attaques envoyées sur un réseau que le NIDS surveille, un HIDS détecte celles contre les hôtes sur le réseau. NIDS ne peut pas détecter les événements dans les flux de paquets qui utilisent le cryptage, mais HIDS peut après décrypte l'hôte du trafic. Idéalement, un HIDS devrait travailler côte à côte avec un NIDS. Vous pouvez corréler les événements détectés par les deux systèmes pour déterminer si une attaque a réussi. Par exemple, une attaque réseau détectée suivie de la création d'un compte administrateur sur un serveur peut signifier que l'attaque a réussi.
Avantages de HIDS:
- Il peut détecter si une attaque a réussi ou non.
- Il surveille les activités du système.
- Il peut détecter les changements dans les fichiers, la mémoire et les applications.
- Il peut détecter les attaques que NIDS ne parvient pas à détecter, telles que les modifications à partir d'une console système.

Limites de HIDS:

- Vous devez déployer un agent pour chaque hôte que vous souhaitez surveiller.
- Il ne détecte pas les analyses réseau ou les attaques de reconnaissance.
- L'hôte sur lequel il réside est susceptible d'attaque et d'invalidation.

I. Architecture

1) Architecture :

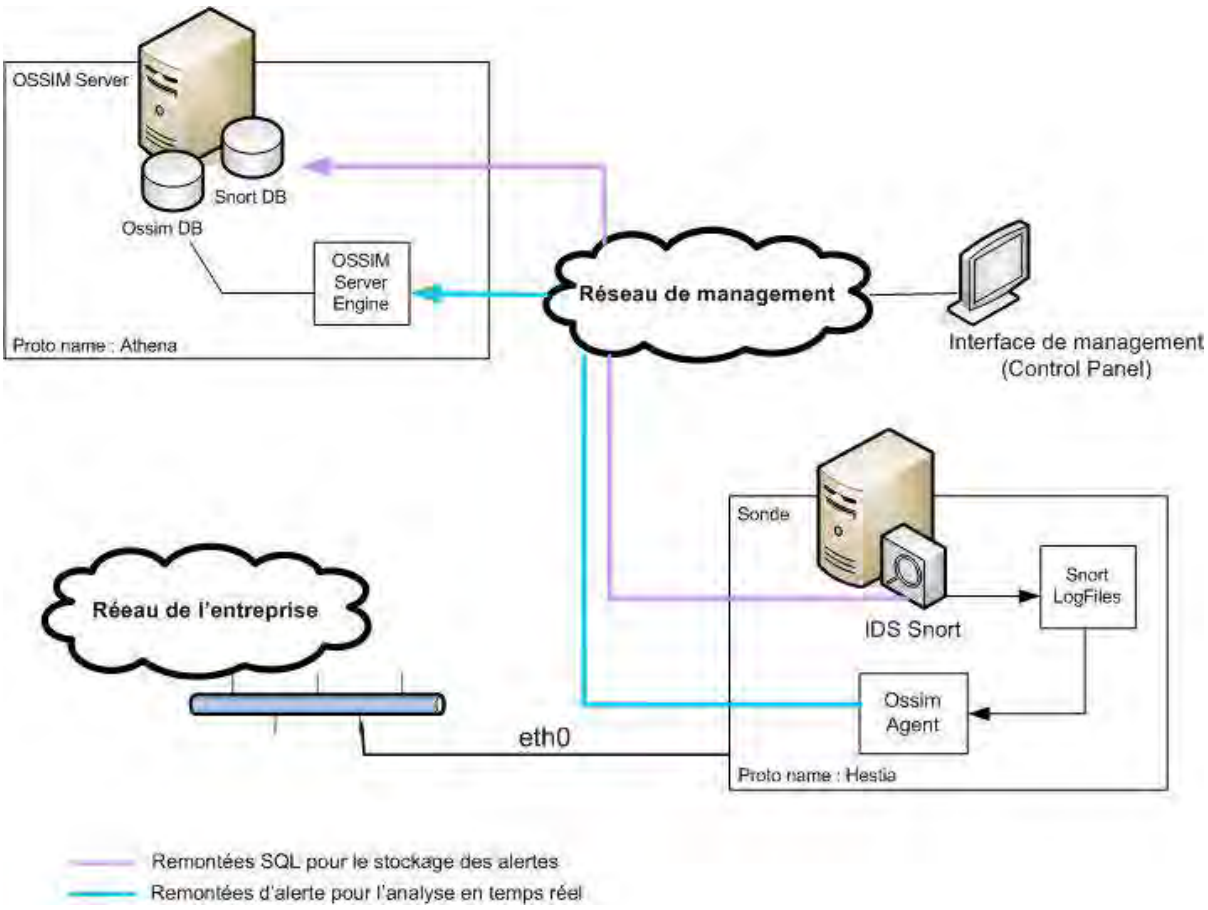


Fig 11 architecture applicatif

La solution OSSIM est découpée selon trois axes (Server, Framework et Agent). Etant donné le nombre de logiciels tiers pouvant être couplé à un agent OSSIM, il existe un certain nombre d'architecture possible aux interactions aussi diverses que variées.

Pourquoi deux flux d'informations ?

- Le flux nommé « Requêtes SQL pour le stockage des alertes » est utilisé afin de déposer directement les alertes dans la base de données du serveur. Ceci permettra l'archivage de celles-ci et leur consultation via ACID (Analysis Console for Intrusion Databases, interface Web intégrée à OSSIM permettant l'interrogation d'une base de données permettant ainsi l'analyse précise de chaque alertes.

- Le flux nommé « remonter des alertes pour l'analyse temps réel » est quant à lui nécessaire pour le procédé d'analyse et de corrélation temps réel opéré sur le serveur d'OSSIM.

Ces deux flux d'informations redondants sont indispensables si l'on ne veut pas redéfinir le protocole d'envoi des informations dans la base de données "Snort DB". En effet, le plugin de sortie Mysql ne serait pas suffisant pour un traitement temps réel puisque le stockage des informations dans une base de données "casse" le procédé temps réel. Un tel fonctionnement impliquerait l'interrogation continuelle de la base de données afin de découvrir les nouvelles données insérées. Les concepteurs d'OSSIM ont donc préféré utiliser deux flux d'informations plutôt que de créer un nouveau plugin de sortie pour Snort permettant d'envoyer les alertes dans un seul flux structuré au serveur. Dans ce mode de fonctionnement, c'est le serveur qui se chargerait ensuite du traitement temps réel et de l'insertion des informations dans une base de données.
Pour l'analyse et la corrélation, le serveur Ossim utilise uniquement les alertes provenant de l'agent Ossim.

2) **Environnement technique**

Au niveau de l'environnement de test, mon choix s'est porté sur des machines virtuelles de type VMWare.
Ce choix a été motivé par le souhait d'avoir un prototype à présenter lors de la présentation des services d'**ossim**.
Le prototype a été divisé en trois machines virtuelles

- la partie Serveur de la solution qui héberge le coeur d'OSSIM, son framework et les bases de données.
- Machine Windows sur laquelle on a installé un agent Ossec
- Machine Ubuntu sur laquelle on a installé un agent Snort

La solution VMWare permet donc d'obtenir une certaine mobilité en offrant la possibilité par le biais de « player » d'exécuter le même prototype sur n'importe quelle machine quelques soit son OS.

3) Environnement applicatif

Le choix s'est porté sur une installation basée sur l'iso car la dernière version (5.3.2) du programme OSSIM n'est pas encore disponible dans les dépôts *apt-get* et une installation depuis les sources n'as pas réussi pour les raisons suivantes :

- Problème sur les fichiers sources disponible sur le site officiel d'OSSIM

Après plusieurs tentatives d'installation depuis les sources (ossim 5.3), il semblerait que certains fichiers soient manquants. Notamment un script python qui assure la collecte au niveau des agents.

Les sources ainsi endommagées ne permettaient pas l'installation complète de la solution.

- Stabilité des packages et niveau de mise à jour

Par contre pour la procédure d'installation habituelle des packages d'OSSIM :

L'avantage notable du système Debian est l'utilisation des commandes « *apt et dpkg»* pour l'installation et la configuration des packages.
OSSIM a été parfaitement porté sous Debian et propose des packages spécifiques à chacune de ses briques. On trouve ainsi les packages :

- *Ossim-mysql* : pour l'installation des composants relatif à la base de donnée mysql
- *Ossim-server* : pour l'installation du moteur d'OSSIM
- *Ossim-framework* : pour l'installation du Framework
- *Ossim-agent* : pour l'installation des composants de l'agent OSSIM

Chaque package peut être installé séparément et possèdent ses propres paramétrages.

Il faut au préalable Configuration le fichier sources.list pour définir le dépôt officiel OSSIM pour une installation via APT.

[-- /etc/apt/sources.list --]
deb http://data.alienvault.com/debian/ binary/
deb http://ftp.debian.org/debian/ wheezy main contrib
deb http://secure.debian.org/wheezy/updates main contrib
deb http://www.ossim.net/download/ debian64/

❖ Installation des bases de données

Il faut au préalable créer la base de données. La structure de la base est fournie dans la solution OSSIM et dépend du choix de la base de donnée (mysql) et des éventuels plugins installés
(snort). La base de données est modifiée pour s'interfacer avec Snort.

```
# apt-get install ossim-mysql
# mysqladmin -u root password mon_mot_de_passe
# mysql -u root –p
```

❖ Création des bases

```
mysql> create database ossim;
mysql> create database ossim_acl;
mysql> create database snort;
mysql> exit;
```

Import des structures et modification de structure pour Snort

```
# zcat /usr/share/doc/ossim-mysql/contrib/create_mysql.sql.gz \
/usr/share/doc/ossim-mysql/contrib/ossim_config.sql.gz \
/usr/share/doc/ossim-mysql/contrib/ossim_data.sql.gz \
/usr/share/doc/ossim-mysql/contrib/realsecure.sql.gz | \
mysql -u root ossim -p
# zcat /usr/share/doc/ossim-mysql/contrib/create_snort_tbls_mysql.sql.gz \
/usr/share/doc/ossim-mysql/contrib/create_acid_tbls_mysql.sql.gz \
```

| mysql -u root snort –p

- **Installation de la partie « Server »**

apt-get install ossim-server
La configuration se fait par l'intermédiaire de l'interface debconf.
Le fichier de configuration d'OSSIM server se trouve dans */etc/ossim/server/config.xml*

- **Installation de la partie « Framework »**

Cette étape permet également d'ajouter la partie phpgacl qui permet la gestion des contrôles d'accès à OSSIM.

apt-get install phpgacl
apt-get install apache2 ossim-framework
Pour reconfigurer le framework OSSIM, il est conseillé d'utiliser les interfaces debconf (*dpkg-reconfigure ossim-utils* et *dpkg-reconfigure ossim-framework*)
Le fichier de configuration est situé dans */etc/ossim/framework/ossim.conf*

A partir de là, OSSIM devra est accessible depuis un navigateur Internet en indiquant l'adresse du server

IV. 3 installation et Configuration d'OSSIM :

A. Procédure d'Installation d'OSSIM :

1) Télécharger le support d'installation : Vous pouvez télécharger la dernière version d'AlienVault OSSIM de http://communities.alienvault.com

2) Démarrez le système d'installation et sélectionnez le mode "Installation automatique"

Fig 12 : page d'accueil d'OSSIM

3) A ce stade, vous devrez configurer votre carte réseau. Vous devez utiliser une adresse IP avec accès à Internet pendant le processus d'installation. Cette adresse IP sera utilisée par l'interface de gestion. Entrez l'adresse IP et cliquez sur "Continuer".

Fig 13 : configuration de la carte réseau

3) Entrez le masque de réseau et l'adresse de la passerelle cliquez sur "Continuer".

Fig 14 : configuration du masque réseau

4) Pour les besoins d'authentification entrez le mot de passe de l'administrateur « root » , et cliquez sur "Continuer".

Fig 15 : configuration du mot de passe de l'administrateur

5) Une fois que l'installation est terminée, la fenêtre suivante s'invite et vous demande d'entrer votre login **ROOT** et votre mot de passe pour accéder à l'interface web d'OSSIM :

.

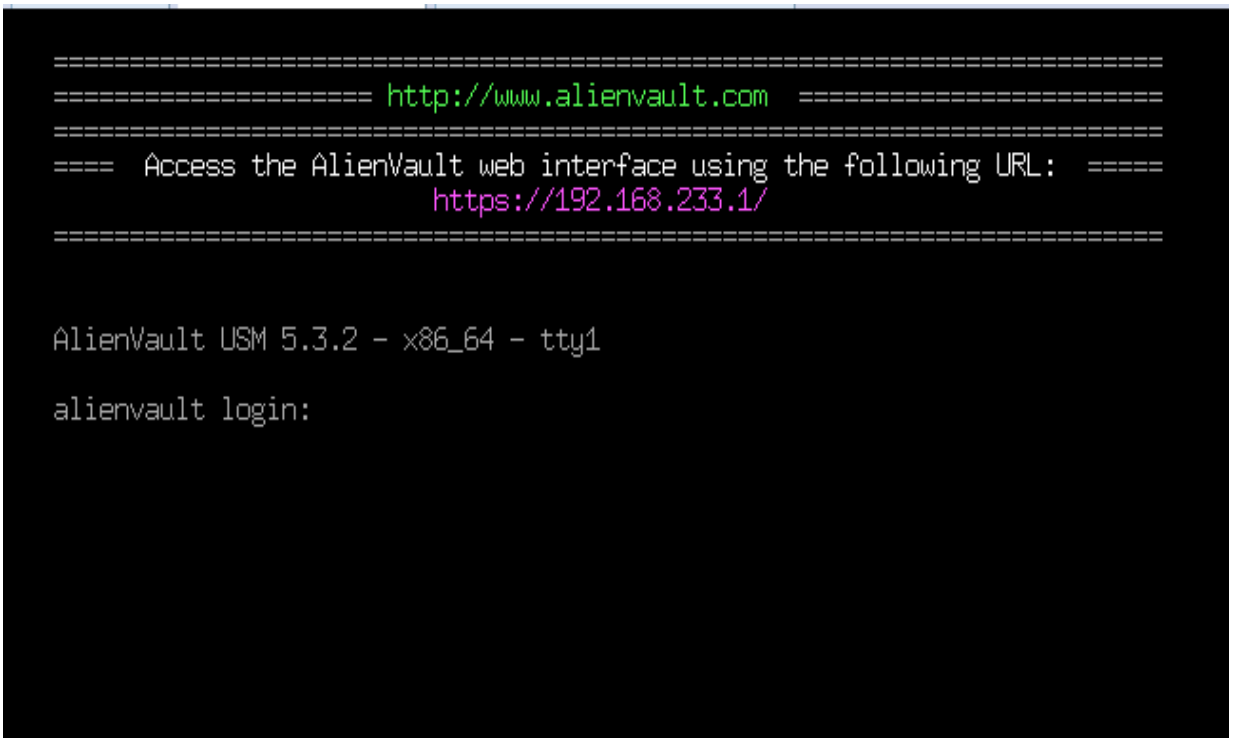


Fig 16 : la page d'authentification du server OSSIM

Maintenant, on Sélectionne les plugins dont nous voulons activés pour effectuer des scans de machines depuis différents outils

Apache
IIS
Syslog
Ossec
Piége
Renifler
OpenVas
Nessus
Nagios
Nmap

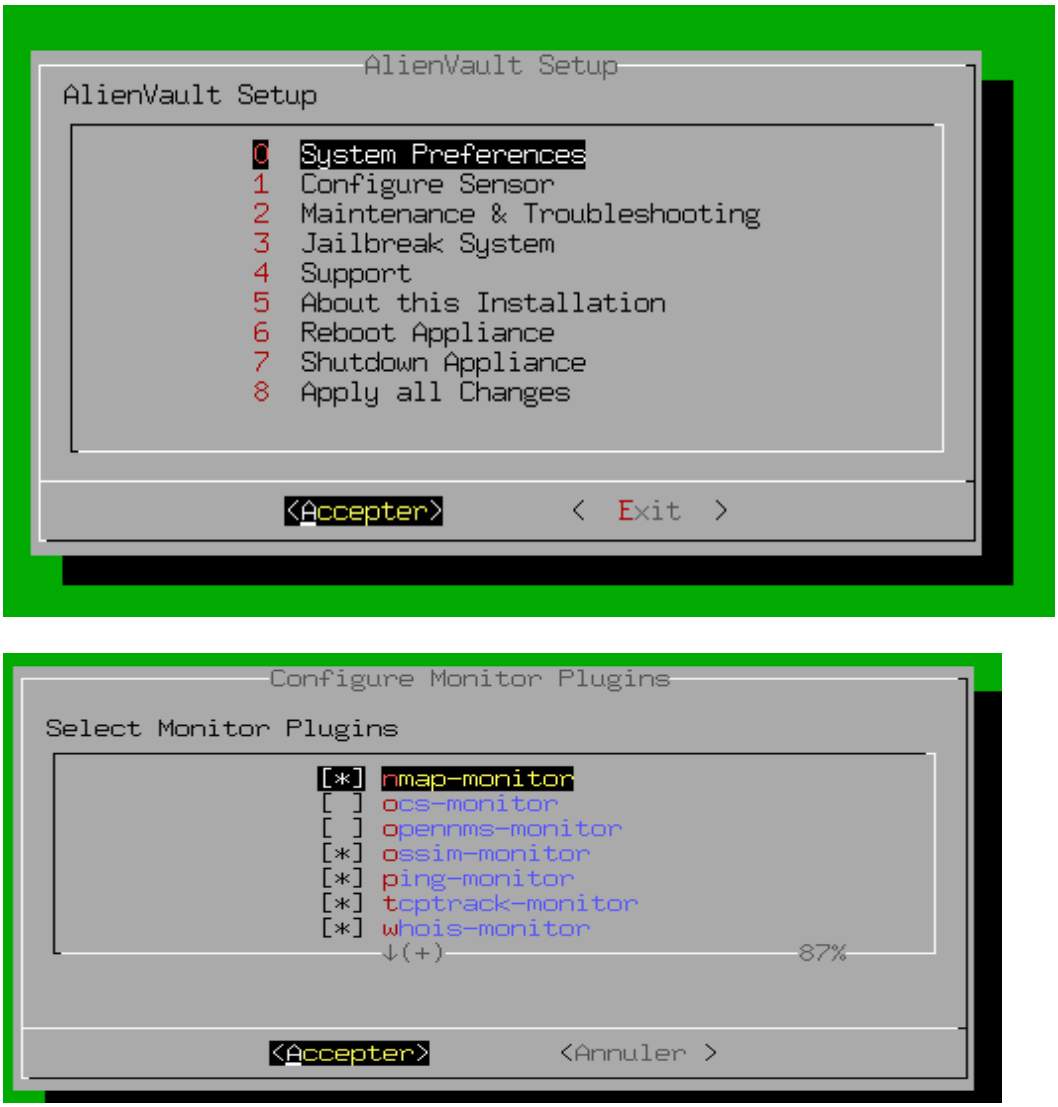


Fig 17 : la selection des plugins à utiliser

6) Pour ouvrir l'interface graphique, tapons l'adresse IP de notre server OSSIM (192.168.233.1) dans le navigateur : Dans le cas de chrome le navigateur vous informera qu'il ne s'agit pas d'un certificat de confiance parce que OSSIM utilise un certificat auto-signé

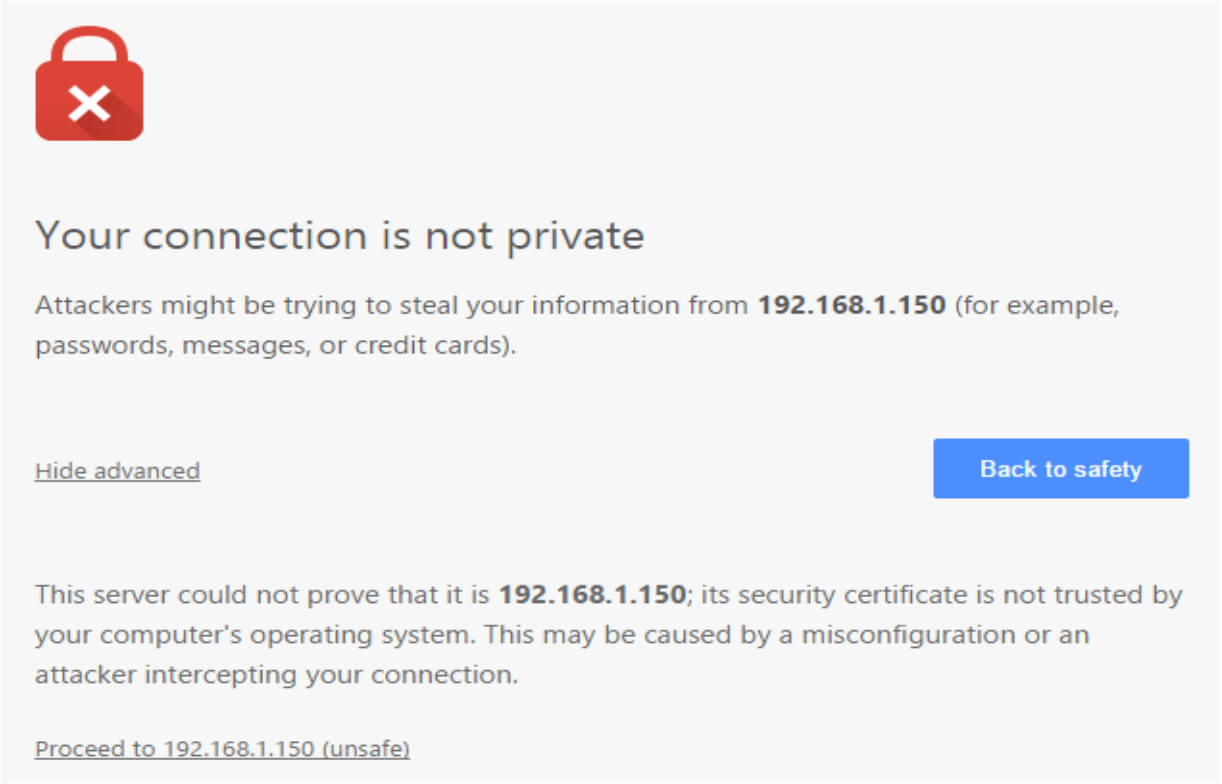


Fig 18 : notification du certificat auto-signé d'OSSIM

Après l'acceptation de l'exception ci-dessus, Ossim requière les informations suivantes sur l'administrateur du server. Remplissez cette formulaire pour la création de votre compte administrateur.

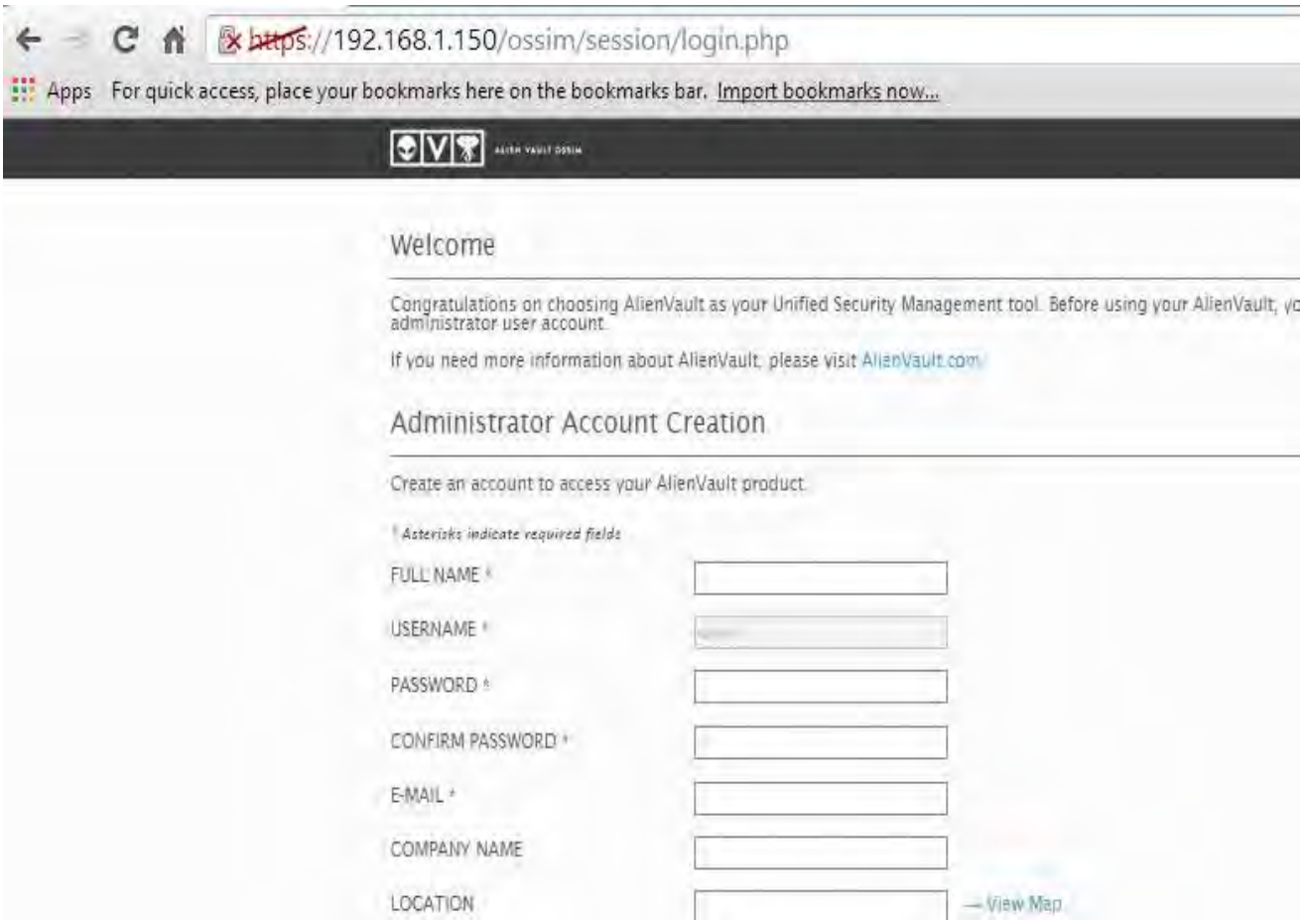


Fig 19 : les informations pour la création du compte admin

Les fenêtres suivantes apparaîtront après la création du compte admin. entrez votre nom d'utilisateur ainsi que votre mot de passe administrateur pour accéder à l'interface web du server Ossim

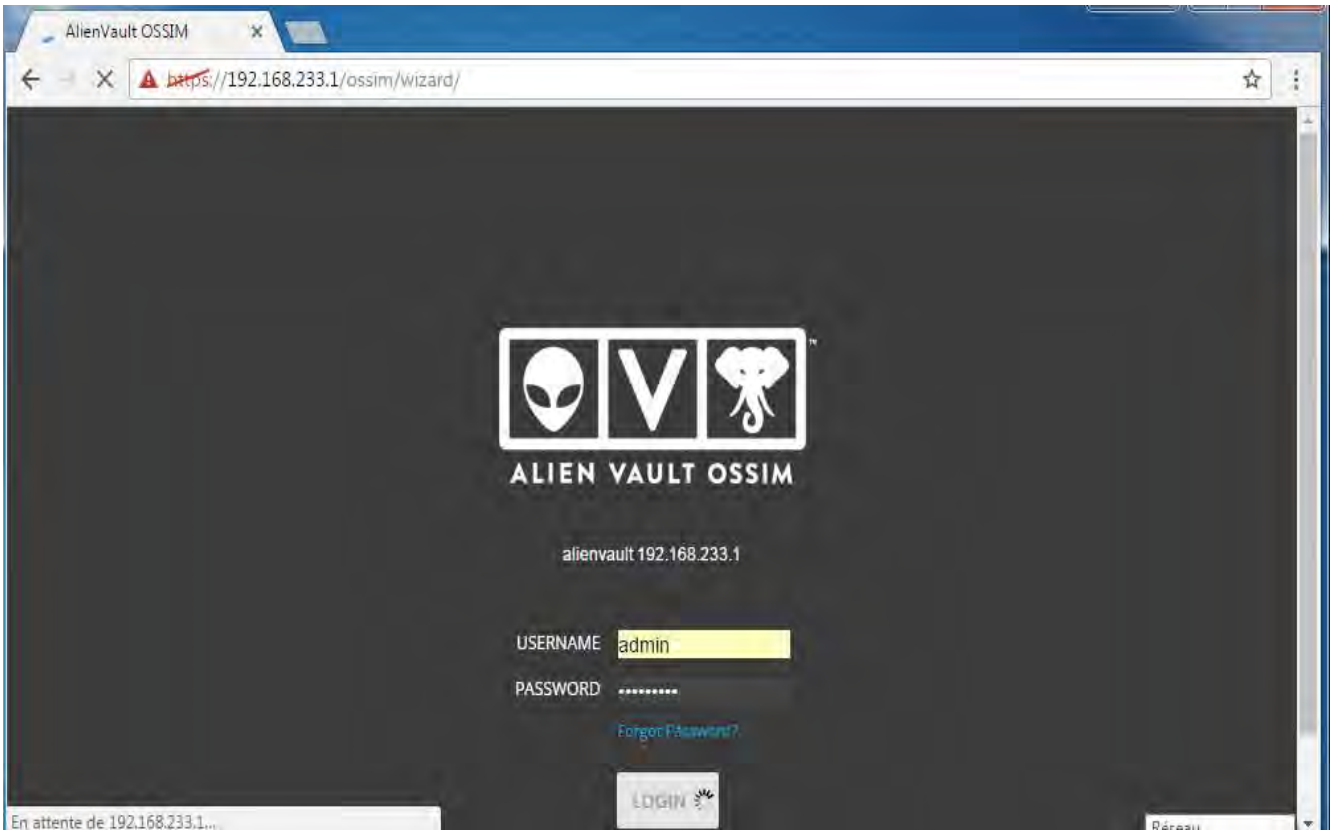


Fig 20 : l'authentification de l'admin

Après connexion réussi dans l'interface web , l'assistant de configuration suivant apparaîtra pour une configuration initiale du server Ossim

Fig 21 : assistant de configuration d'ossim

Cet assistant propose les trois options suivantes disponibles avec le server OSSIM :

1. Monitor Network : qui permet la configuration des interfaces et moniteurs pour la surveillance du trafic réseau par le server OSSIM
2. Discover Asset : qui permet la découverte automatique des périphériques réseau présents dans l'organisation

3. Collect Logs & Monitor Asset : qui permet la collecte des journaux à partir des nœuds du réseau et la surveillance des activités suspectes

Ensuite cliquez sur démarrer de la figure ci-dessus pour configurer le server OSSIM.
La première option nous ouvre une fenêtre pour la configuration des interfaces réseau (eth) pour la collecte et la surveillance logs du server

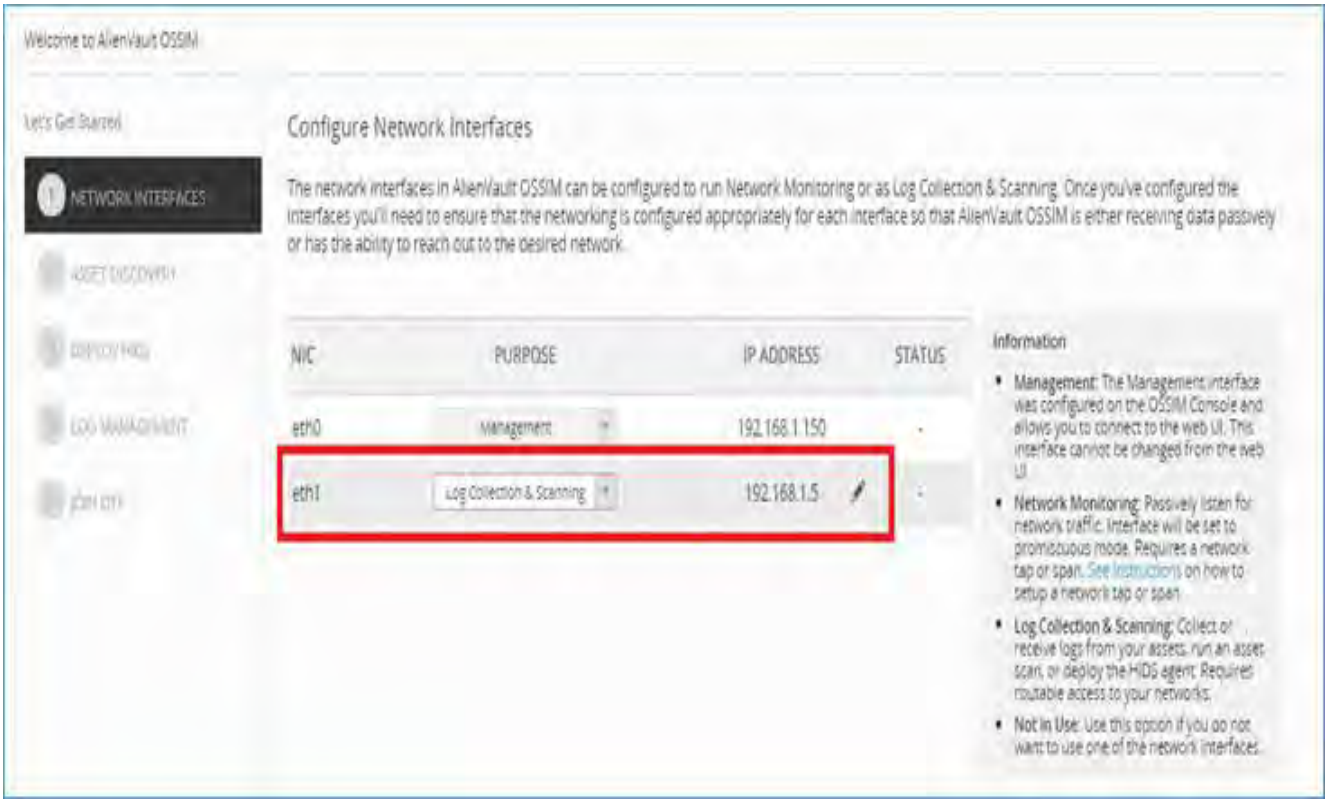


Fig 22 : configuration des interfaces eth du sever ossim

Dans la deuxième étape, OSSIM effectuera la découverte automatique des actifs du réseau.
Sélectionnez l'option (2) ASSET DISCOVER pour préciser les types d'actifs (périphériques) découverts dans le réseau ;
Le type de l'actif peut être :

- Un système windows
- Un système linux
- Un dispositif réseau (routeur, firewall, imprimante, etc …)

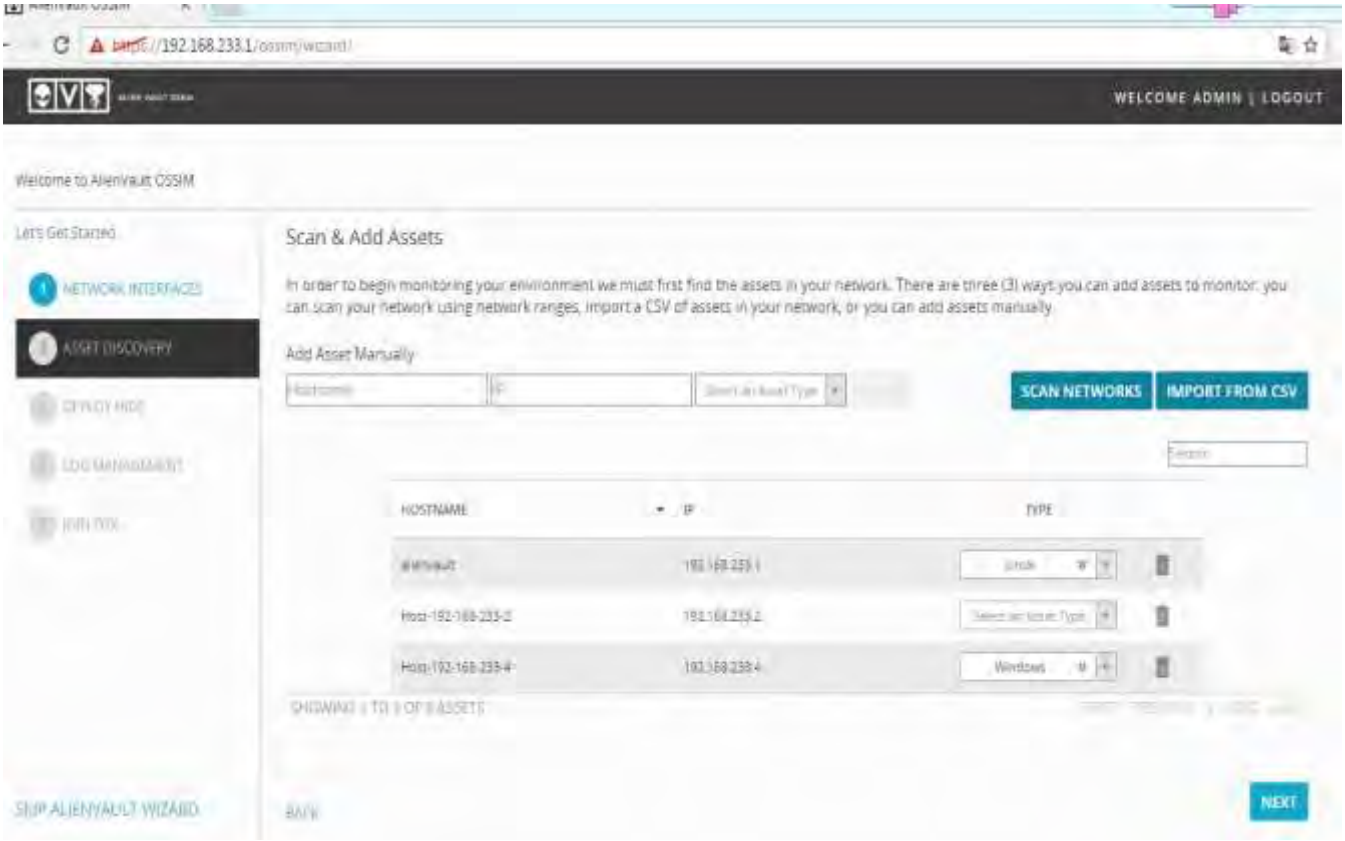


Fig 23 : la découverte des actifs (périphériques) du réseau

Après la configuration du réseau et de découverte de l'actif, l'étape suivante (l'option 3) est « DEPLOY HIDS » le déploiement de l'agent HIDS (l'agent Ossec) sur les machines pour effectuer la surveillance , la détection de rootkit et la collecte des journaux (log)

d'événements . Entrer le nom d'utilisateur / mot de passe de la machine (de l'actif) sur laquelle on doit déployer le HIDS.

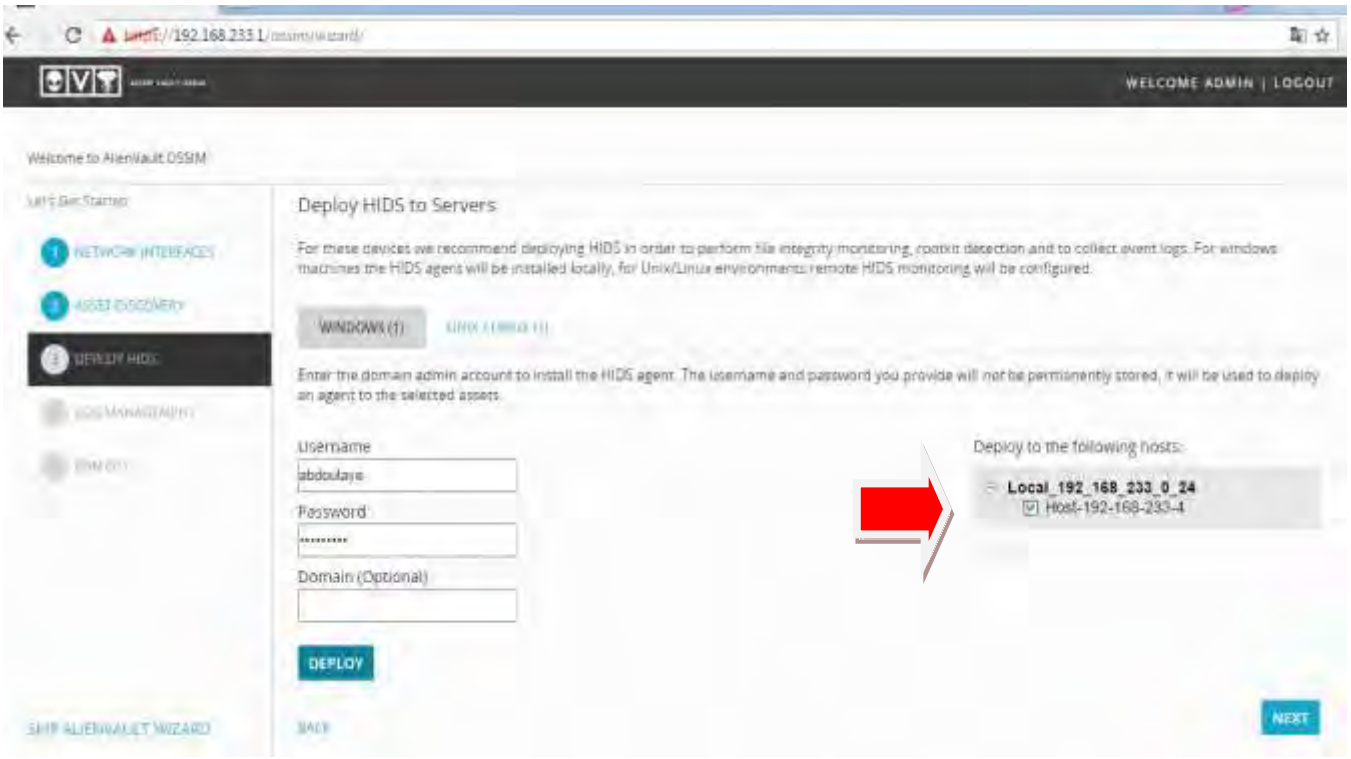
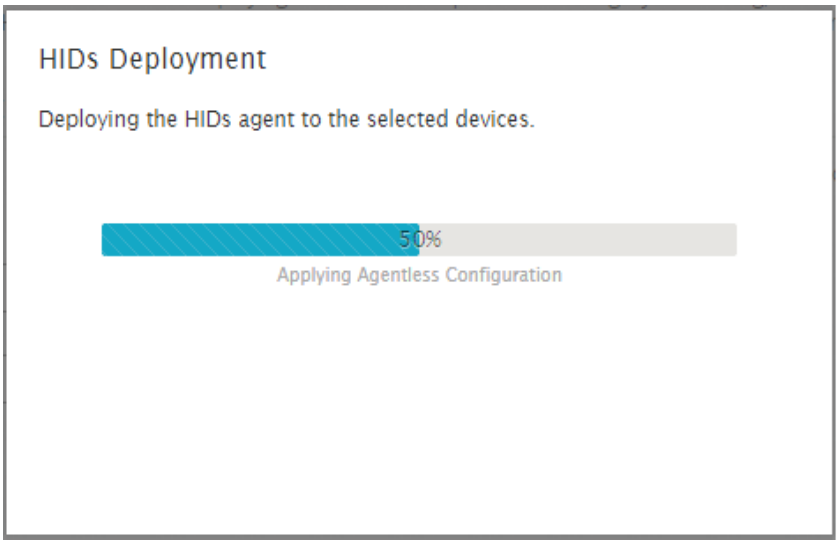


Fig 24 : déploiement de l'agent ossec

Sélectionner l'Hôte désiré dans la liste à droite ci-dessus et cliquer sur DEPLOY pour le déploiement HIDS. Encore un fois cliquer sur le bouton « Continuer » pour lancer le processus de déploiement qui est représenté sur la figure. Ce processus prendra quelques minutes pour déployer le HIDS (ossec) sur l'hôte sélectionné.



Après déploiement de HIDS, l'étape suivante (l'option 4) « LOG MANAGEMENT » permet de configurer l'actif précédemment découvert pour la gestion des différents journaux d'événements (logs).

Fig 25 :configuration de l'actif

La dernière étape dans l'assistant de configuration est de rejoindre le OTX (Open Threat Exchange) qui est le programme d'échange des menaces dans AlienVaul (optionnel). Terminer l'étape de configuration en cliquant sur « Finish ».

Le principal tableau de bord du server OSSIM est illustré ci-dessous :

Fig 26 : tableau de bord du server ossim

L'INTERFACE WEB de OSSIM :

L'interface web du server Ossim se compose des cinq menus suivants sur l'interface principale :

- DASHBOARDS (tableaux de bord)
- ANALYSIS (analyse)
- ENVIRONMENTS
- REPORTS
- CONFIGURATION

- DASHBOARDS :

Il montre une vue d'ensemble de toutes les composantes du serveur OSSIM comme la gravité de la menace, la vulnérabilité des hôtes dans un réseau, l'état du déploiement, niveaux de risques , et les états OTX.

Les sous-menus du Dashboard (tableau de bord) sont illustrés sur la figure suivantes :

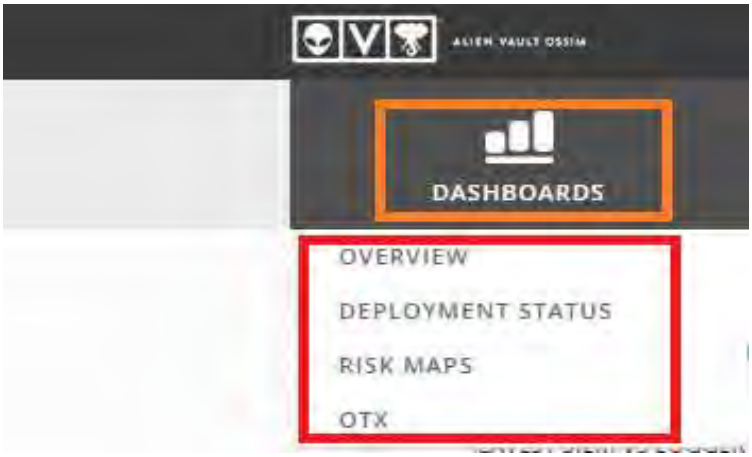


Fig 27 : les sous menus du menu **dashbords**

- ANALYSIS

L'analyse est un composant très important dans tout dispositif SIEM. Le server OSSIM analyse les hôtes en fonction de leurs journaux (logs). Ce menu affiche les alertes (ALARMS), les événements de sécurité (siem), les journaux brutes (raw logs) et les Tickets. Ces sous-menus sont illustrés sur la figure:

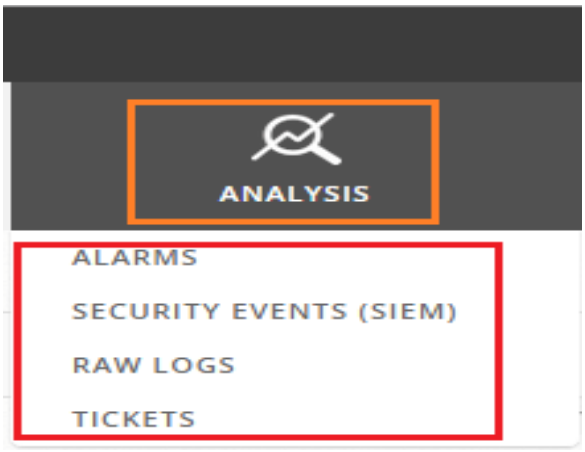


Fig 28 : les sous-menu du menu **analysis**

- ENVIRONMENTS

Dans ce menu du server OSSIM, les réglages sont liés aux actifs de l'organisation. Il montre les actifs (ASSETS), les paramètres et groupes réseaux (GROUPS NETWORKS), les vulnérabilités, Netflow et détection .les sous menus sont représentés ci-dessous sur la figure :

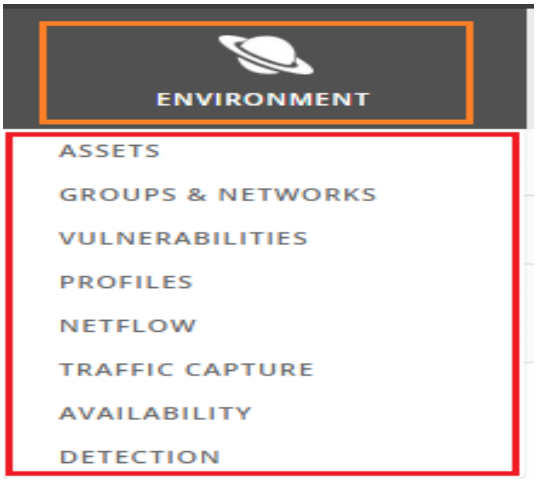


fig 29 : les sous-menus du menu **environment**

- REPORTS

Le reporting est une partie très importante de toute exploitation forestière server. Le server OSSIM génère des rapports qui sont très utiles pour l'enquête détaillé (Forensic) de tout hôte spécifique.

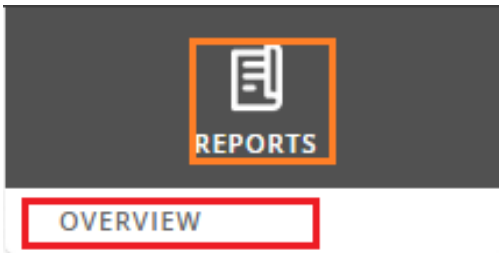


Fig 30 : le menu **reports**

- CONFIGURATION

Dans ce menu de configuration d'AlienVault OSSIM, l'utilisateur peut modifier le réglage du server OSSIM telle que changer l'adresse IP de l'interface de gestion, ajouter plus d'hôte pour le suivi et l'exploitation forestière et ajouter /supprimer des différents capteurs / plugins. Les sous-menus pour ces services sont représentés ci-dessous

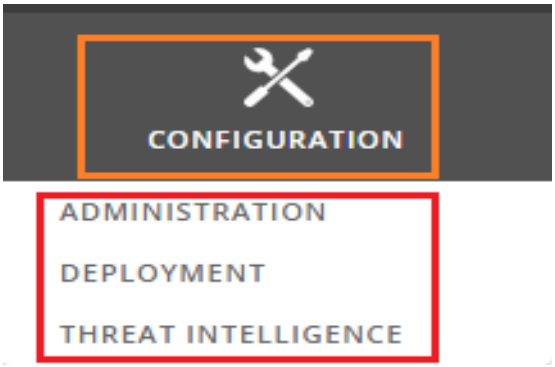


fig 31 : les sous-menus du menu **configuration**

B. SUIVIE ET ANALYSE DE SÈCURITÈ PAR OSSIM

Cette section donne un aperçu des principales options, menus et sous-menus de l'interface Web utilisateur de OSSIM et les opérations utilisés principalement pour l' affichage, la surveillance et l'analyse des activités et des événements de sécurité réseau.

Cette section couvre les sous-thèmes suivants:

- Affichage des tableaux de bords OSSIM
- Analyse d'alarmes, événements, journaux et billets (ticket)
- Gestion de l'environnement OSSIM
- Administration et configuration d'OSSIM

1. Affichage du Tableau de Bords d'OSSIM

La première sélection de menu de l'interface Web d'OSSIM qui joue un rôle important dans la surveillance de la sécurité et de l'analyse d'un environnement de réseau est le menu **Dashboards (Tableau de bord)**. Il offre une visibilité globale sur l'activité du réseau, et affiche divers paramètres de sécurité réseau.

Lorsque vous lancez d'abord l'interface Web utilisateur d'OSSIM, il ouvre son tableau de bord : le **Dashboards** > **Aperçu (overview)** pour l'affichage de la page.

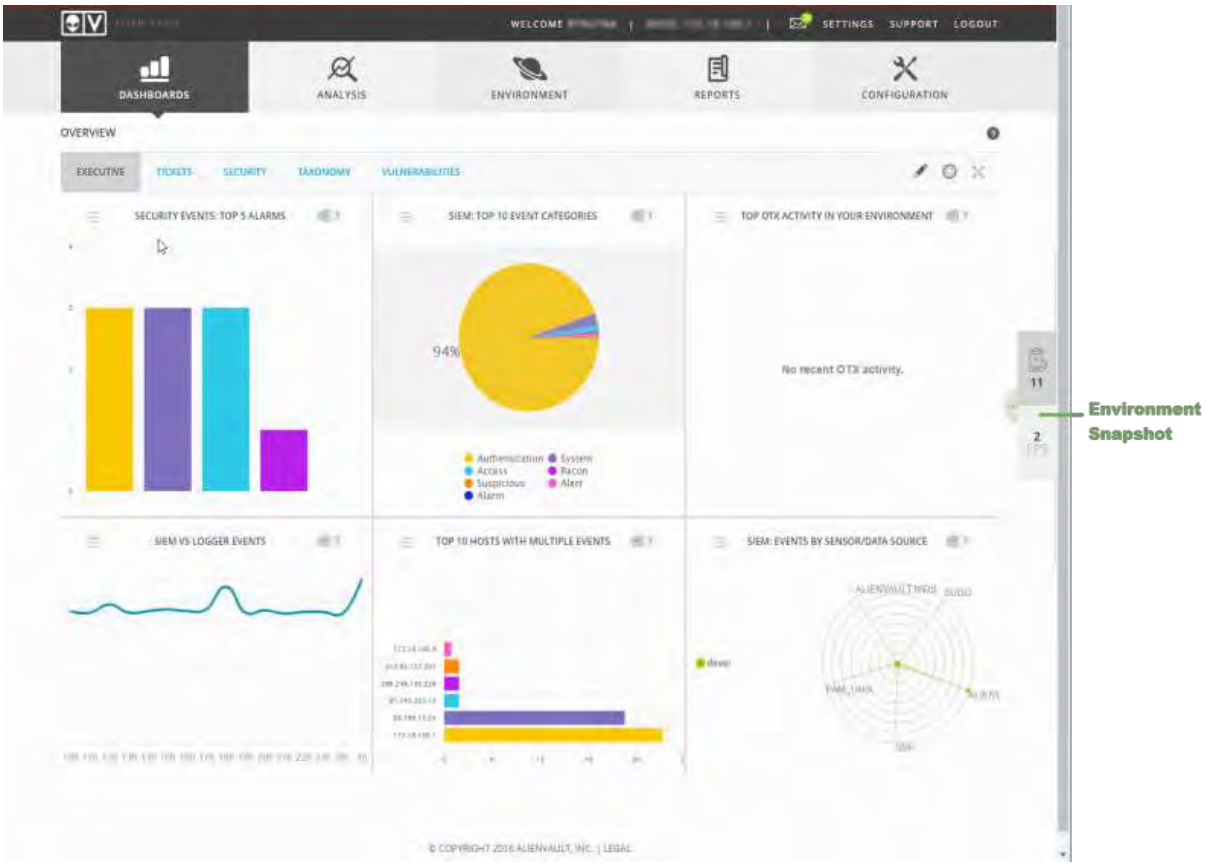


Fig 32 : tableau de bord d'ossim

Ce point de vue sommaire de l'information montre l'état général du réseau, de sorte que vous pouvez obtenir une indication immédiate des niveaux d'événements et d'alarmes qui se produisent dans votre environnement.

En plus de l'écran **OVERVIEW (aperçu)**, la sélection du menu principale **Dashboards** fournit également plusieurs autres sélections du sous-menu :

- **Statut de déploiement** : Fournit une vue globale sur la surveillance en place pour les actifs, les réseaux et les emplacements.

  Certains de ces services de surveillance sont activés par défaut , alors que d'autre ont été activés dans l'Assistant de configuration initiale (en analyse d'inventaire actif), et d'autre (scan de vulnérabilité) doivent être activés manuellement. Vous pouvez vérifier quels services sont activés pour un réseau en sélectionnant le réseau, puis en regardant les services dans la partie droite de l'écran. La couleur verte indique que le service est activé, tandis que la couleur rouge indique qu'un service est désactivé. Vous pouvez activer un

service en cliquant sur le carré rouge indiquant un service désactivé. Vous pouvez également consulter les statistiques pour les services activés sur tous les réseaux dans un endroit en examinant la partie visibilité du réseau de l'écran. Les cercles indiquent le nombre de réseaux dans lesquels un service spécifique est activé.

- **Cartes des risques** - Affiche une carte des risques qui montre l'état de l'actif au sein d'une carte sélectionnée et offre la possibilité de gérer les cartes.
- **OTX** - permet de visualiser graphiquement les menaces dans une carte. La carte permet de visualiser les adresses IP qui appartiennent à des hôtes qui sont des attaques ou qui ont un comportement malveillant. Ces adresses IP sont fournies par OTX (programme d'échange des menaces), qui comprend une communauté membres de l'équipe d'AlienVault et les utilisateurs d'OSSIM et USM dans le monde entier.

D'autres options de la page de Présentation du tableau de bord affichent les tickets, Sécurité, Taxonomie, et vulnérabilités.

- **Tickets** - Fournit des métriques sur les tickets créés dans le propre système de ticket d'OSSIM. Les tickets offrent le suivi des flux de travail de l'activité liée aux alarmes (alertes) détectées ou toute autre question que vous voulez garder la trace.

- **Sécurité** - Fournit des états sur les différentes mesures de sécurité dans l'environnement, par exemple, les hôtes actifs, les alarmes (alertes) les plus fréquentes, et des rapports des événements de sécurité.
- **Taxonomie** - Fournit des métriques sur les événements basés sur différentes classifications d'événements de taxonomie OSSIM, par exemple, la détection de virus, les connexions réussies et échouées, les logiciels malveillants, et les types d'événements exploités.
- **Vulnérabilités** - Fournit des paramètres sur les caractéristiques de vulnérabilité tels que la gravité et les hôtes les plus touchés. Affiche également les détails de disponibles des rapports d'analyse.

L'**environnement Snapshot** est affiché sur le côté droit de l'interface Web OSSIM. L'état par défaut affiche les alarmes en cours et les événements par seconde (EPS). Vous pouvez étendre le Plateau de la notification pour afficher l'instantané de l'environnement en cliquant sur la petite flèche sur le côté gauche de l'affichage résumé de l'**Environnement Snapshot.**

Fig 33 : le menu **snapshot**

L'environnement **Snapshot** montre les tickets ouverts, les alarmes non résolues, la santé du système, la dernier activité de l'événement, et le nombre de périphériques surveillés.

2. Analyse d'Alarmes, d'Èvénements et de Tickets

On aura probablement passé le plus de temps à examiner et à analyser la sécurité du réseau de notre environnement en utilisant diverses options proposées dans le Menu Analyse de l'interface Web utilisateur OSSIM. Le menu d'analyse fournit les sélections de sous - menu suivantes:

- **Alarmes** - Affiche toutes les alarmes générées dans l'OSSIM. (Tout événement avec une valeur de risque calculée égale à 1 ou supérieure génère une alarme). Vous pouvez également rechercher des alarmes en utilisant des filtres.
- **Les événements de sécurité (SIEM)** - Affiche tous les événements qui ont été traitées ou générées par le Server OSSIM. Vous pouvez également rechercher et filtrer les événements qui apparaissent à l'écran, ainsi que de visualiser les détails des événements spécifiques.
- **Tickets** - Permet d'accéder aux systèmes de gestion de tickets OSSIM. Les tickets offrent le suivi des flux de travail de l'activité liée aux alarmes détectées ou toute autre question que vous voulez garder la trace.

✓ **Visualisation des alarmes (alertes) :**

Lorsque vous sélectionnez le menu **Analyse** > option **Alarmes** OSSIM affiche la page suivante :

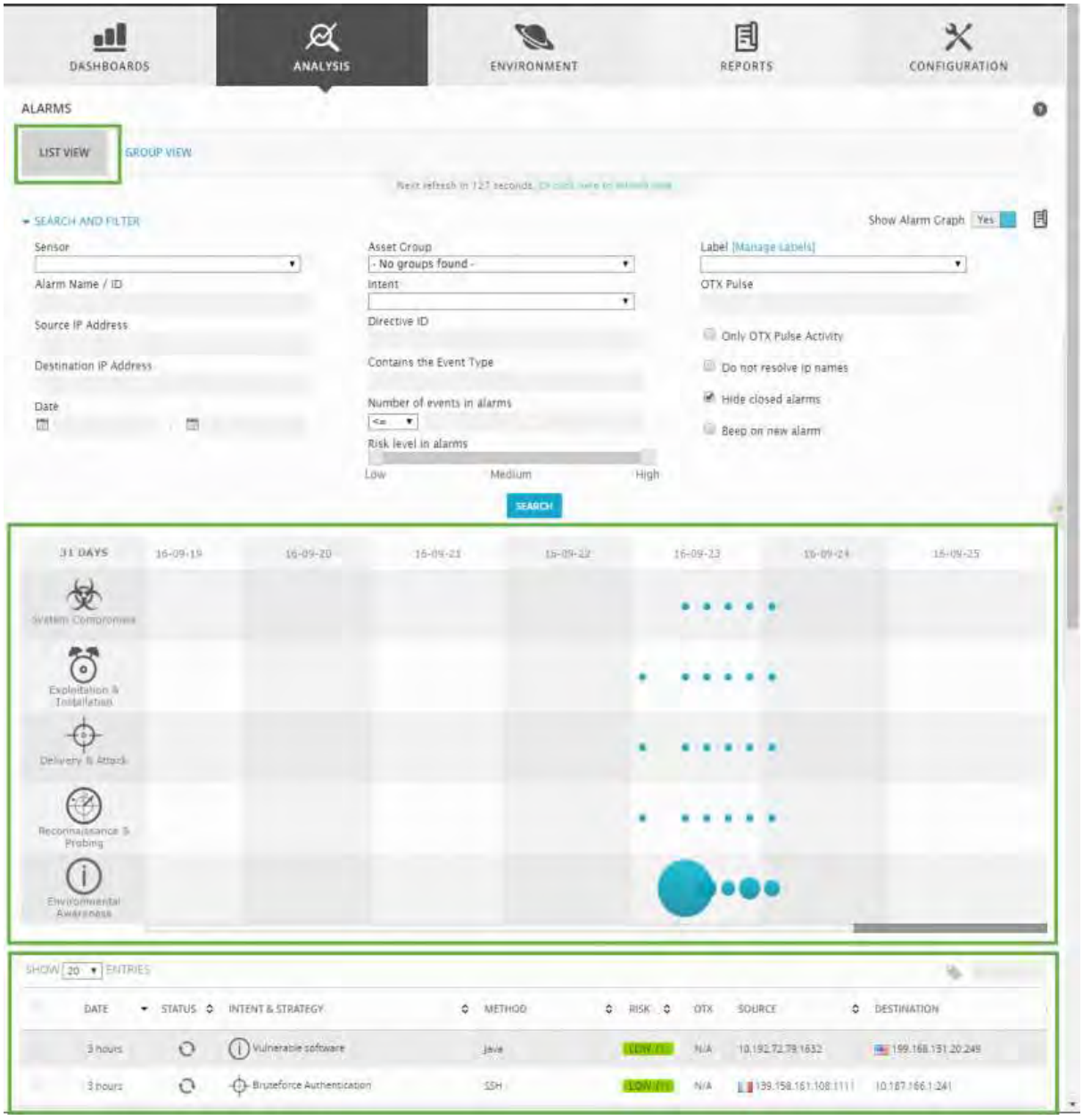


Fig 34 : les alertes

Par défaut, l'affichage s'ouvre dans **List View**, qui énumère simplement les alarmes dans l'ordre chronologique inverse (la dernière des alarmes émis est affichée en premier). Vous pouvez également modifier l'affichage **Groupe View**, qui permet de grouper les alarmes par différentes clés telles que le nom de l'alarme, la source et adresse IP de destination, ou le type d'alarme.

La partie centrale de l'écran comprend une table qui fournit une représentation graphique agrégée des alarmes qui se sont produites au cours des 31 derniers jours; chaque colonne représente un autre jour. Les cercles bleus indiquent le nombre de fois qu'une alarme dans une catégorie est apparue. Un cercle plus grand indique un nombre plus élevé d'alarmes qui ont

été générées. Vous pouvez poser la souris sur chacun des cercles pour obtenir le nombre réel de différents types d'événements qui se sont produits, ainsi que la liste Top5 des remèdes possibles pour chaque type d'alarme.

Les alarmes sont classées en cinq catégories différentes, qui sont représentées par les icônes graphiques dans l'affichage. Ceux-ci sont:

- Compromis du système ()
- Exploitation et l'installation ()
- Livraison et d'attaque ()
- Reconnaissance et sondage ()
- Sensibilisation à l'environnement ()

Ces catégories d'alarmes sont également susceptibles d'être la séquence ou les étapes d'événements qu'un attaquant pourrait suivre pour infiltrer avec succès un réseau, obtenir un accès non autorisé aux données, ou accomplir un acte malveillant. Ces catégories d'alertes sont également compatibles avec le modèle d'attaque détaillé par Lockheed Martin appelé la chaîne **Cyber kills**.

En-dessous de l'affichage par catégorie des icônes d'alarme, OSSIM affiche par défaut une liste tabulaire des alarmes individuelles, dans l'ordre chronologique inverse. En outre, si vous cliquez sur l'un des cercles bleus, OSSIM affichera uniquement les alarmes correspondant au cercle sélectionné. Dans la liste d'alarmes, vous pouvez cliquer sur une ligne d'alarme individuelle pour développer l'affichage des informations sur l'alarme. Vous pouvez ensuite cliquer sur le **Détails**, ou cliquez sur le bouton **Détails** (icône ), pour afficher plus d' informations sur l'alarme sélectionnée, y compris les événements individuels qui effectivement déclenchent l'alarme.

La partie supérieure de la page de l'affichage des Alarmes vous permet de rechercher et de filtrer les alarmes qui sont affichés sur la page. Vous pouvez filter les alarmes par des attributs d'événements tels que l'emplacement du capteur, groupe d'actifs ou le niveau de risque.

- ✓ **Visualisation des événements de sécurité**

Lorsqu'on sélectionne le menu **Analyse** > option **événements de sécurité (SIEM)**, OSSIM affiche la page suivante.

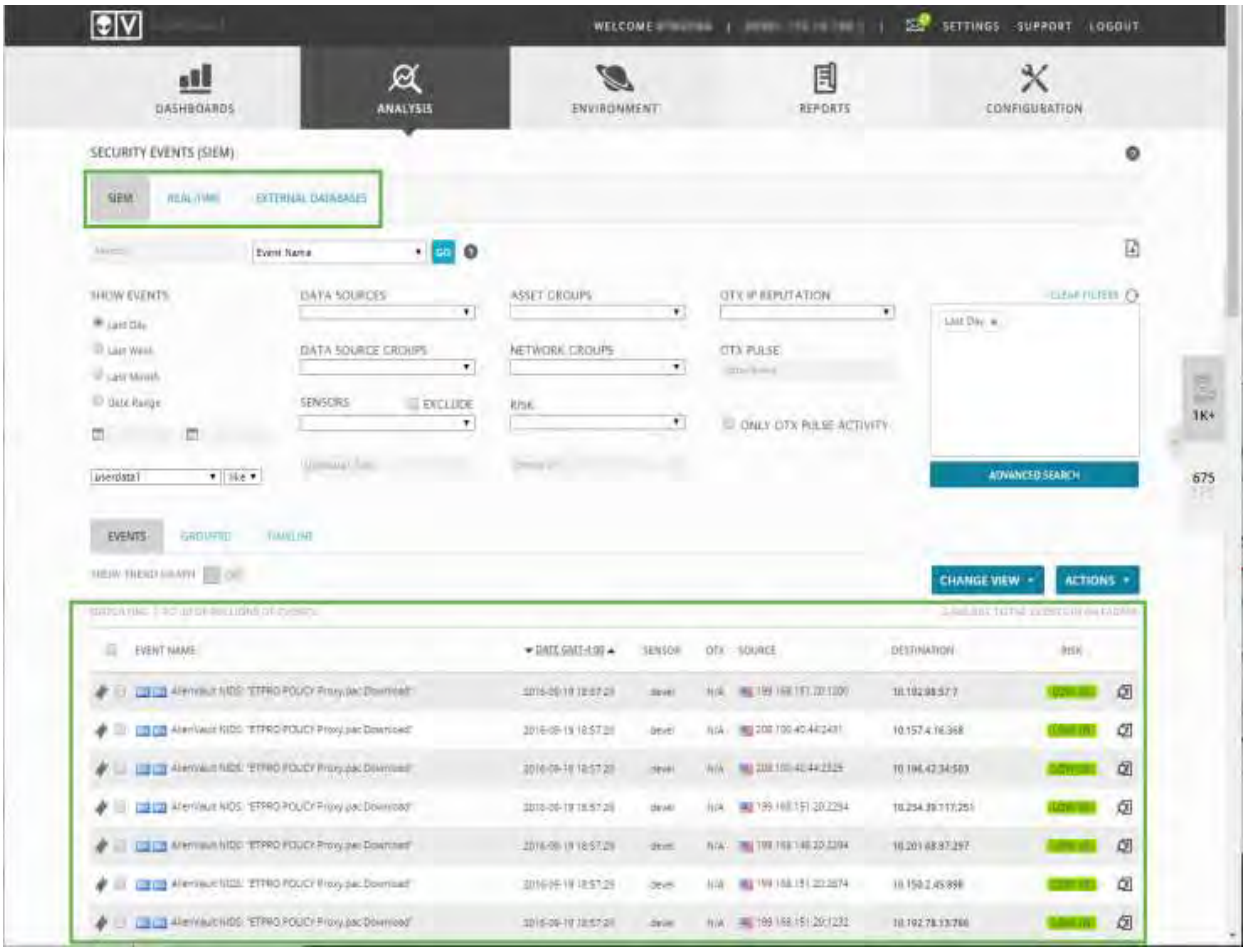


Fig 35 : les événements de sécurité générés

Par défaut, la page **Security Events (SIEM)** affiche une vue des événements OSSIM. L'interface Web fournit également deux autres options pour l'affichage des événements de sécurité:

- **Real-Time** – la page qui affiche les événements en cours dans notre réseau.
- **External DataBases (Bases de données externes)** - Affichage des événements de sécurité à partir d'une base de données AlienVault externe qui est associée à une autre installation d'OSSIM AlienVault.

Depuis l'option **view** (vue) SIEM, vous pouvez rechercher et filtrer les événements à l'aide de plages (intervalle) de temps et d'autres critères attribués à l'événement.

En dessous de la section du filtre de la page de recherche, OSSIM fournit un affichage de tous les événements, ou des événements filtrés (si vous avez spécifié les critères de recherche pour les événements). Tout événement de log (journal) normalisé, ou tout autre événement reçu ou généré par un capteur OSSIM depuis une application, du système ou du réseau apparaîtront à l'écran.

Du tableau de la liste récapitulatif des événements, on peut cliquer sur une ligne d'événement spécifique pour voir plus de détails sur cet événement dans une fenêtre contextuelle. Vous pouvez également cliquer sur l'icon **Plus de détails** ( ) dans une ligne d'événements pour afficher sur une nouvelle page les détails de l'événement, qui vous permet également de choisir d'autres mesures à prendre avec l'événement en cours.

✓ **Affichage des Tickets**

Lorsque vous sélectionnez **Analyse** > option **Tickets** affiche la page suivante.

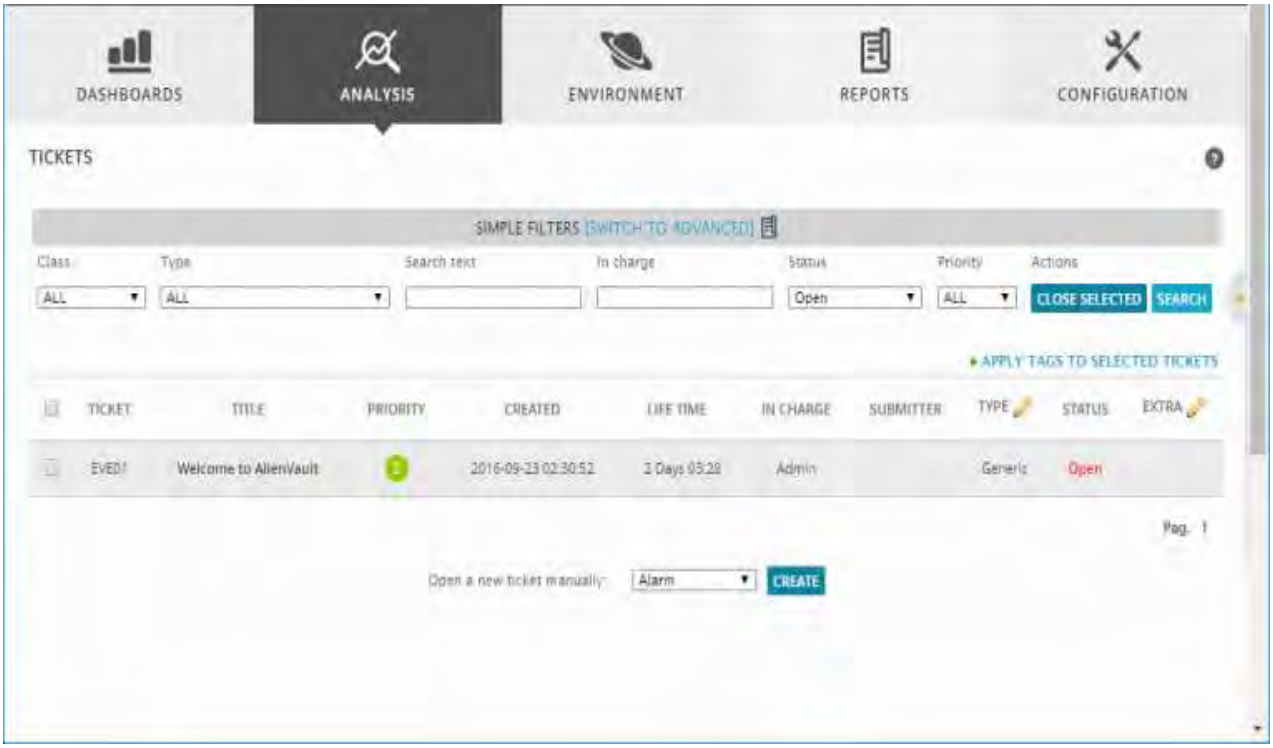


Fig 36 : les tickets

Cette page donne accès au système d'assainissement des tickets. Les **Tickets** offrent le suivi des flux de travail de l'activité liée aux alarmes détectées ou toute autre chose que vous voulez garder la trace. Par défaut, l'interface Web d'OSSIM affiche une liste de tous les Tickets. En outre, vous pouvez cliquer sur le bouton **Créer** pour créer un nouveau Ticket d'un type ou d'une catégorie spécifique.

Dans la section des filtres en haut de la page des Tickets, vous pouvez choisir des critères pour filtrer les résultats des Tickets. Vous pouvez choisir des critères supplémentaires pour filtrer les résultats des Tickets en cliquant sur l'option **Switch To Advanced**.

Dans la liste sommaire des Tickets, vous pouvez cliquer sur un ticket spécifique pour l'ouvrir et afficher l'ensemble des détails du ticket. Sur cet écran de détail des tickets, vous pouvez effectuer différentes actions telles que la modification des champs attribués à un ticket, en ajoutant des notes, et en changeant le statut et la priorité d'un ticket, selon quelle méthode ou processus vous souhaitez utiliser pour suivre la résolution des problèmes.

3. Gestion de l'Environnement d'OSSIM

En plus de surveiller et d'analyser les événements et alarmes, il y a d'autres aspects de la sécurité comme surveiller et mettre à jour l'environnement réseau. Le menu Environnement donne accès à ces autres domaines de la sécurité du réseau grâce à diverses options de sous-menu, qui comprennent les éléments suivants:

- **Actifs et groupes** - Cette option vous permet de visualiser et de gérer les actifs, les réseaux, les groupes d'actifs, et les groupes de réseau.
- **Vulnérabilités** - Cette option vous permet de visualiser et d'effectuer des balayages ou scan de vulnérabilité. L'analyse de la vulnérabilité peut fonctionner à partir d'un ou plusieurs capteurs AlienVault.
- **NetFlow** - Cette option offre la possibilité de surveiller et de travailler avec des flux de données.
- **Traffic capture** - Cette option permet à l'utilisateur de mettre en œuvre et gérer la capture du trafic à distance via le capteur AlienVault. Il existe plusieurs options de capture telles que timeout, la taille du paquet, le nom du capteur, et la source et la destination des paquets.
- **Disponibilité** - Vous pouvez utiliser cette option pour afficher et configurer la surveillance de la disponibilité.
- **Détection** - Cette option est utilisée pour gérer la détection d'intrusion pour la plupart des systèmes d'exploitation. Cette option affiche également l'analyse du journal, le contrôle d'intégrité, la surveillance du registre Windows, la détection de rootkit, alerte en fonction du temps, et la réponse active.
- **Rapports** - Listes tous rapports OSSIM disponibles et vous permet d'effectuer des opérations telles que Supprimer, Export, Copier, Modifier, Exécuter personnalisé et Exécuter le rapport.

✓ Visualisation des actifs et groupes d'actifs

Lorsque vous sélectionnez **Environnement** > option **Actifs et groupes** OSSIM affiche la page suivante.

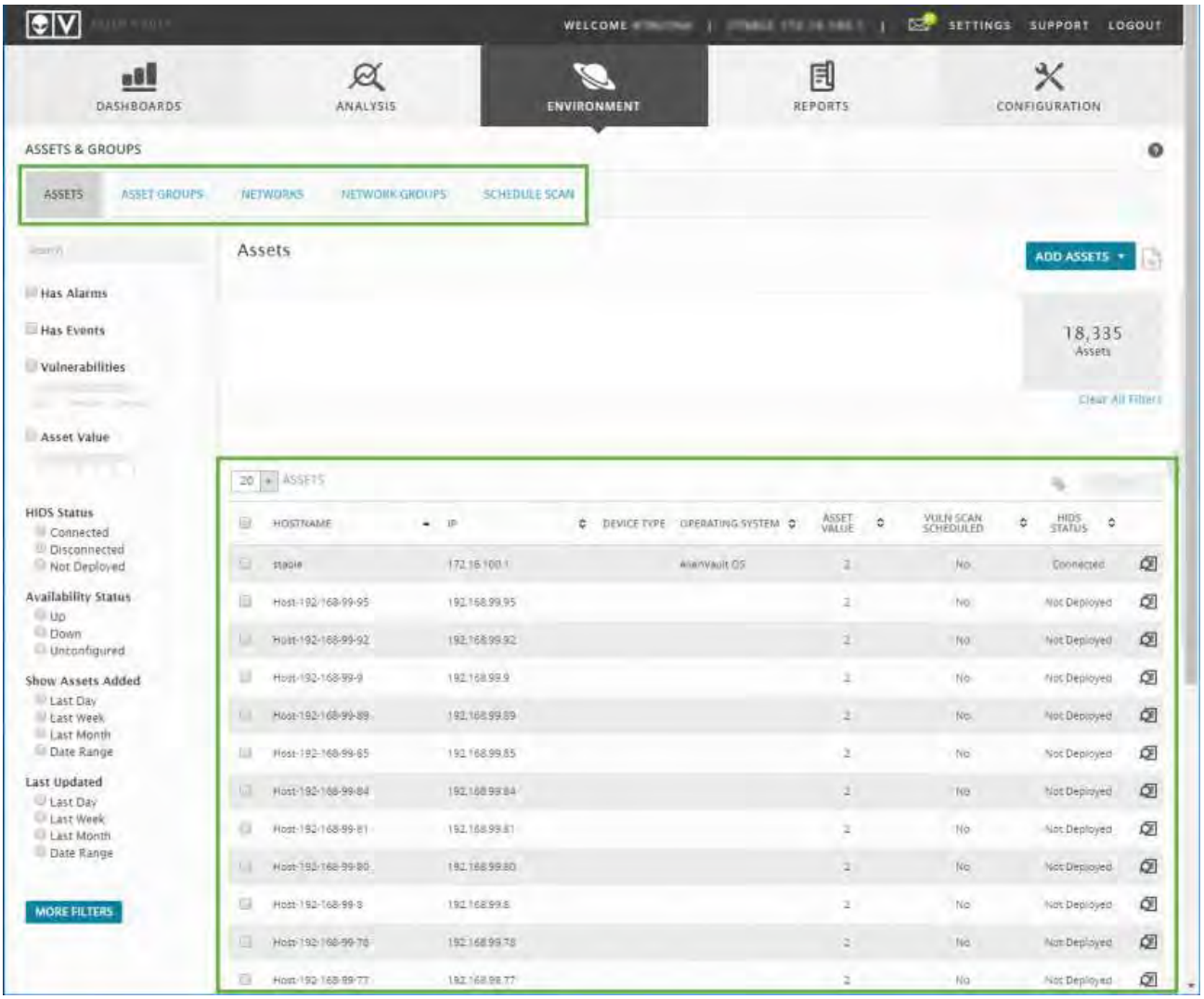


Fig 37 : les actifs présents dans le réseau

L'affichage de la page **Environnement> Actifs et groupes** indique le nombre d'actifs et affiche également une liste tabulaire de tous les actifs de votre environnement réseau qui ont été ajoutés manuellement ou créés à l'aide de découverte d'actifs (effectuée par des analyses de réseau). Vous pouvez cliquer sur le bouton **Add actif** pour ajouter des actifs, en choisissant des options telles que Add Host, Importer à partir de CSV, Import de SIEM, et Scan pour les nouveaux actifs. La sélection de la case à cocher à côté d'un actif spécifique permet grace au bouton **Actions** d'effectuer des opérations telles que l'exécution de balayages (ou découverte) d'actifs ou de vulnérabilité, le déploiement d'un agent HIDS, et permettant la surveillance de la disponibilité.

Dans l'affichage des actifs par défaut, le panneau **Recherche** de gauche vous permet de filtrer les actifs figurant dans la liste des actifs en sélectionnant des attributs spécifiques d'actifs. OSSIM maintient un inventaire intégré des actifs qui peuvent stocker des informations supplémentaires sur les actifs, en plus des informations récupérées en utilisant des méthodes et des outils de numérisation passives et actives.

En cliquant sur un actif spécifique dans la liste tabulaire des actifs, cela élargit les informations affichées pour l'élément sélectionné. Il comprend des informations connexes telles que le nombre de vulnérabilités, les alarmes et les événements relatifs à l'actif.

Fig 38 : les informations sur l'actif sélectionné

Vous pouvez également trier les actifs dans la liste en cliquant sur les titres des tableaux qui reflètent les valeurs d'attribut maintenues pour chaque actif. Cliquer sur l'icône ( ) à côté pour afficher tous les détails enregistrés ou suivis pour cet actif sur une nouvelle page.

Sur la page Détail de l'actif, outre le nom, l'adresse IP, et la description de l'actif, vous pouvez également voir l'emplacement de l'actif, et les informations détaillées telles que les vulnérabilités, les alarmes, les événements, et ainsi de suite.

L'interface Web d'OSSIM fournit également les options d'affichage suivantes:

- **Asset Groups (groupe d'actifs)** - Affiche des informations organisées par groupes d'actifs dans votre environnement réseau. En outre, vous pouvez créer de nouveaux groupes et ajouter des actifs à partir de ces groupes.
- **Network (Réseaux)** Affiche des informations d'actifs organisées par des réseaux ou sous - réseaux définis par votre organisation. En outre, vous pouvez ajouter ou définir de nouveaux réseaux ou sous - réseaux à des actifs du groupe. Les actifs sont organisés en réseaux basés sur l'adressage IP.
- **Network group (Groupes réseau)** - Affiche des informations d'actifs organisée par groupes de réseaux vous permettent de les définir au sein des réseaux ou sous - réseaux. De ce point de vue, vous pouvez également ajouter de nouveaux groupes de réseau ou de modifier ceux qui existent déjà.
- **Scheduled scan (Planifier une analyse)** - Fournit des options pour afficher les analyses planifiées existantes et planifier de nouveaux scans de découverte des actifs et des analyses WMI (windows management instrumentation) sur les hôtes Windows.

✓ L'affichage des Vulnérabilités :

Lorsque vous sélectionnez le menu **Environnement** > option **Vulnérabilités** OSSIM affiche la page suivante.

Par défaut la page **Environnement**> **Vulnérabilités** affiche une vue graphique des vulnérabilités les plus importantes dans votre environnement, par gravité, ou par services.

A partir de cet écran, vous pouvez également afficher les résultats du scan de vulnérabilité des actifs (au format HTML ou PDF), ou planifier une nouvelle tâche de scan.

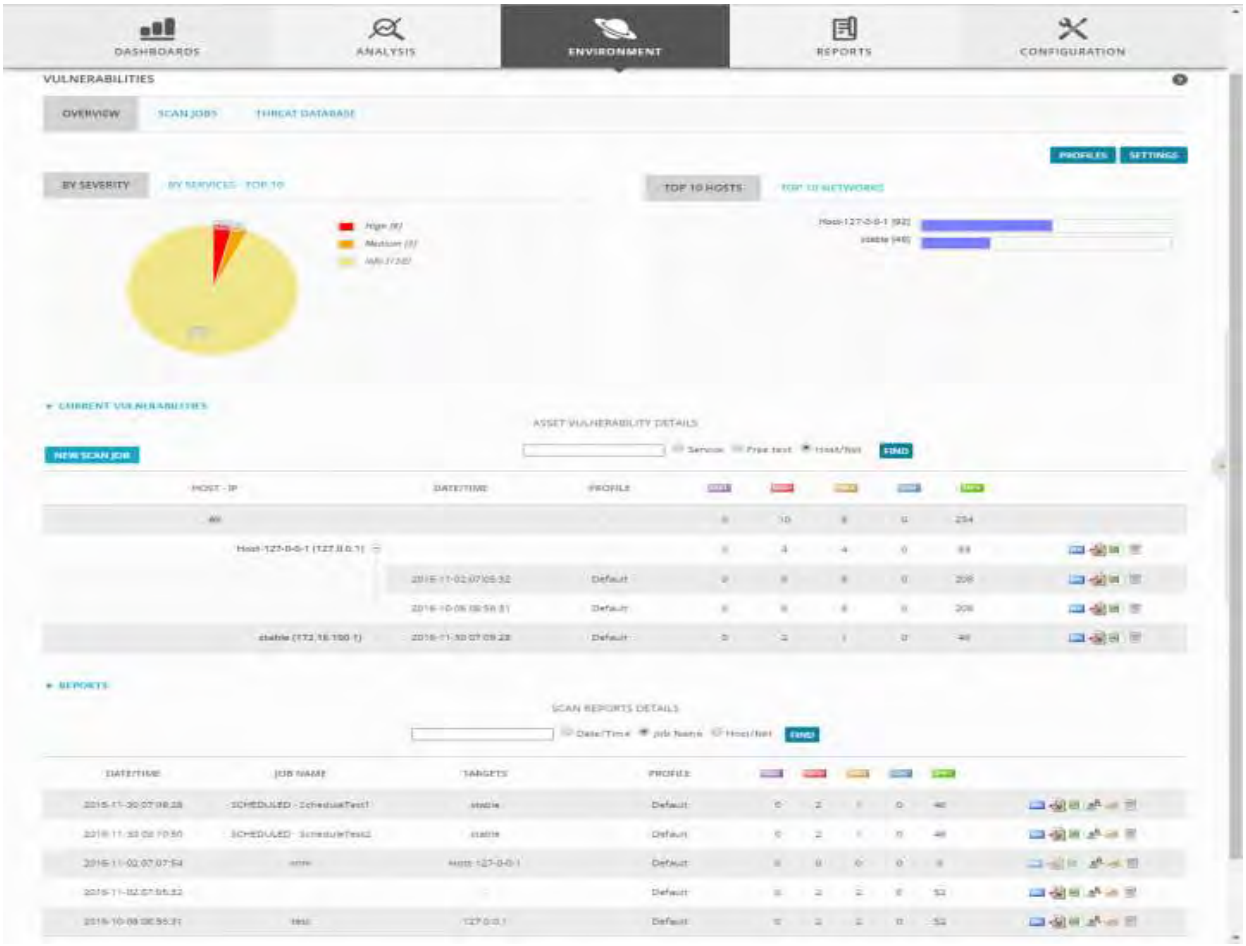


Fig 39 : les vulnérabilités sur l'actif

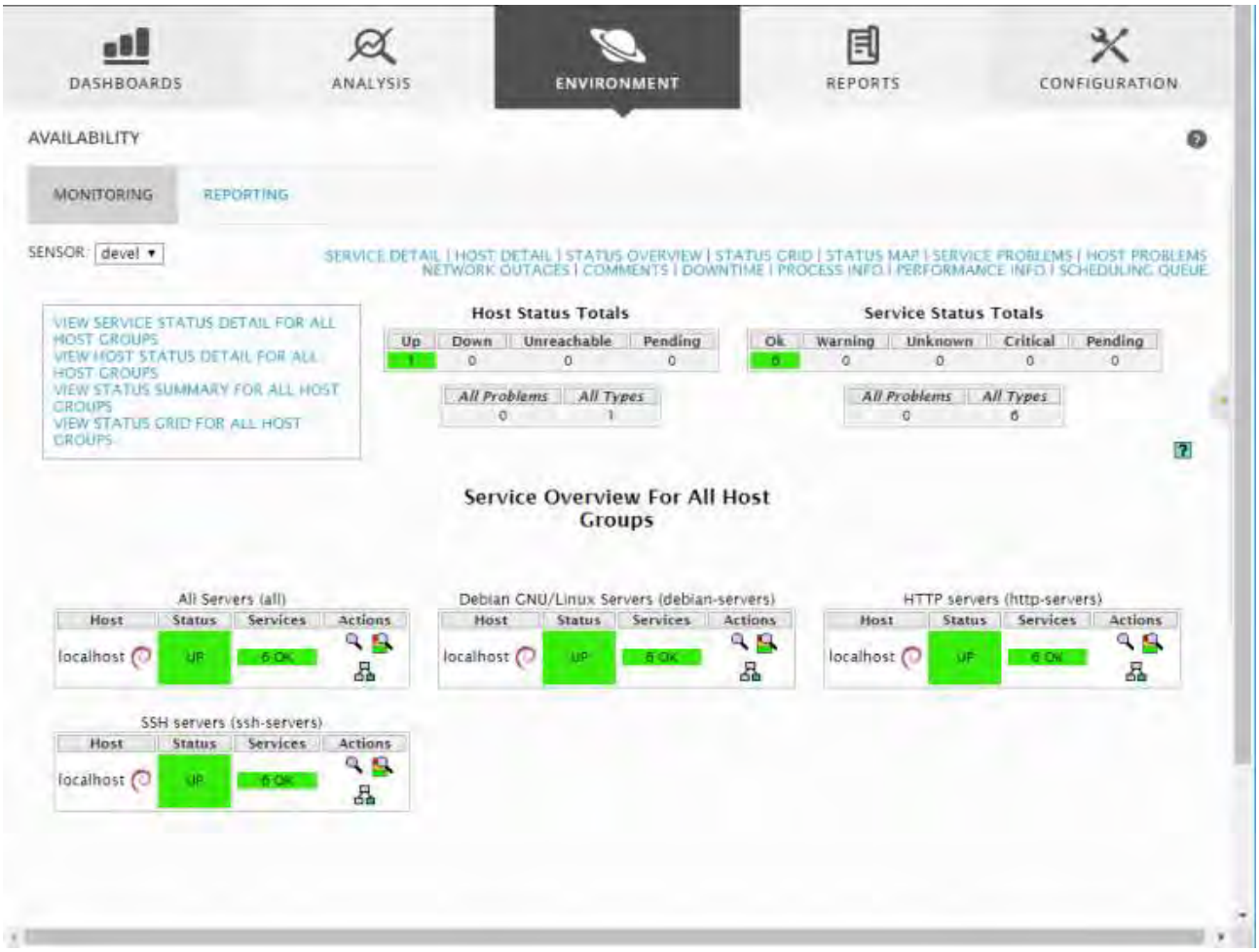
En outre, vous pouvez créer ou modifier des profils (décrivant le type des analyses qui peuvent être effectuées), et définir ou modifier les informations d'identification à utiliser pour les analyses (en cliquant sur le bouton **Paramètres**).

En plus de l'affichage **Overview** (Aperçu) des Vulnerabilités, l'interface Web OSSIM fournit également les options suivantes:

- **Jobs scan (Travaux d'analyse)** - Fournit la capacité de voir les scans en cours, l'importation d'évaluation de la vulnérabilité, des rapports d'analyse, et de créer ou de planifier de nouveau scan de vulnérabilité.
- **Threat DataBase (Base de données des menaces)** - Fournit la capacité de rechercher et afficher les menaces actuelles.

✓ **L'affichage de la disponibilité :**

Lorsque vous sélectionnez **Environnement** > puis l'option **Disponibilité** OSSIM affiche la page suivante.



La page affiche l'état des actifs et d'autres informations opérationnelles sur différents serveurs, applications et des services en cours d'exécution dans votre environnement réseau. Dans la vue de la page de suivi, vous pouvez sélectionner différentes options pour voir les détails de l'état sur les hôtes et les services individuels, ainsi que des groupes d'actifs. Vous pouvez également sélectionner les options pour afficher des détails tels que les problèmes sur les services et les hôtes, des pannes de réseau, les temps d'arrêt, et la performance.

En plus de l'affichage de la page de suivi, OSSIM fournit également une page d'option de déclaration qui vous permet de sélectionner et de générer des rapports pour un grand nombre de détails.

- ✓ **La Detection :**

Lorsque vous sélectionnez E**nvironnement** >puis l'option **Détection** OSSIM affiche la page suivante.

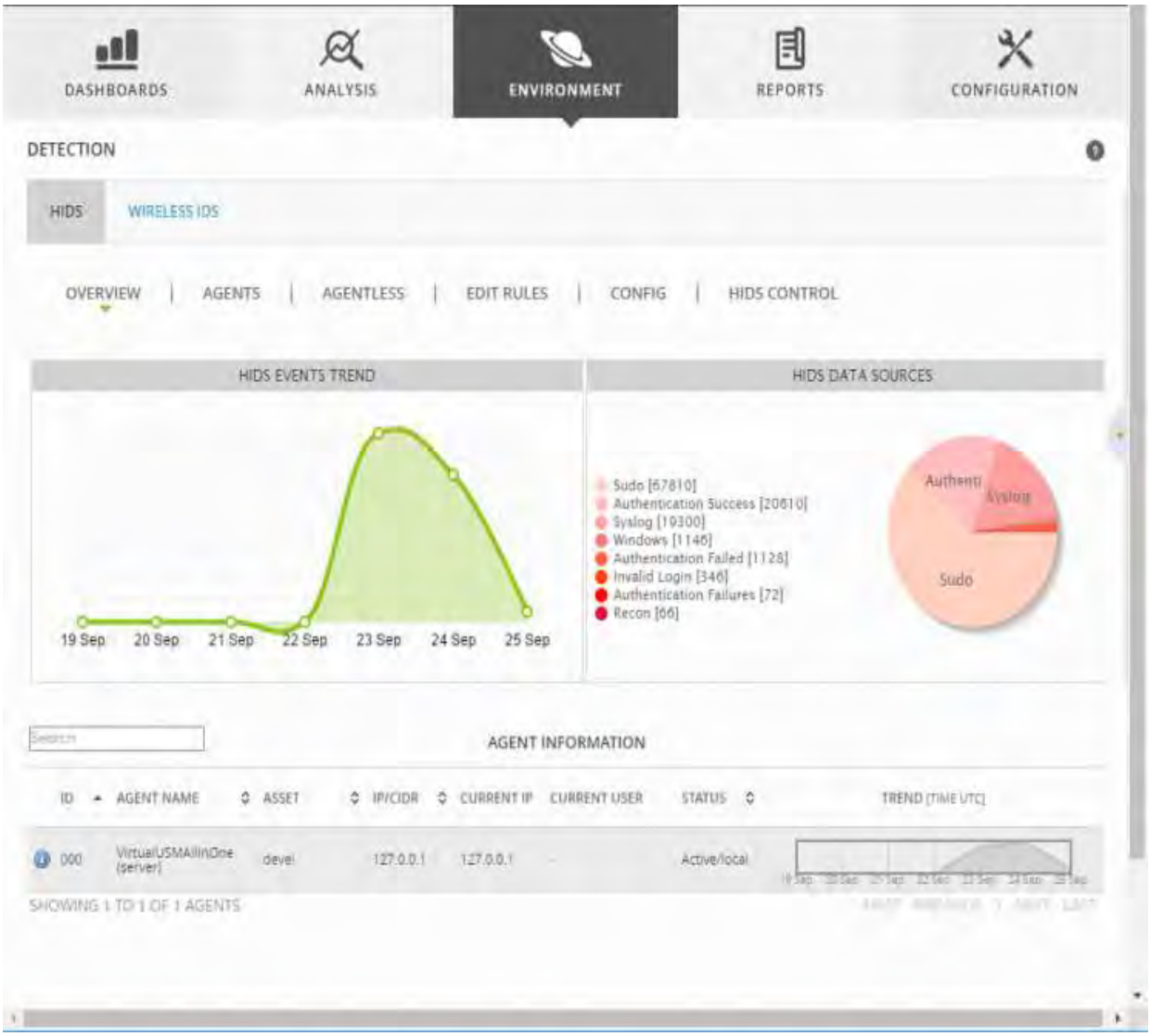


Fig40 : la détection d'intrusion

L'affichage de la page de détection fournit des options pour gérer la détection d'intrusion pour la plupart des systèmes d'exploitation. Vous pouvez également afficher l'état et d'autres résultats sur la détection d'intrusion, tels que les tendances de l'événement, l'analyse des journaux, des contrôles d'intégrité, la surveillance du registre Windows, et la détection de root kit.

Sur la page HIDS par défaut (Aperçu), vous pouvez également choisir des options pour afficher l'état et les détails de configuration du HIDS pour les éléments suivants:

- **Agents** : permet une révision et mise à jour des paramètres pour l'Agent de contrôle HIDS, Syschecks et agents.conf, ou ajouter de nouveaux agents.
- **Agentless** : pour les paramètres de mise à jour pour la détection d'intrusion sans agent sur un hôte.
- **Modifier les règles** : règle la mise à jour de fichiers XML et des règles individuelles pour le HIDS.

- **Config** - Examen et mise à jour des règles de fichiers XML qui sont soit activées ou désactivées, définir les options Syschecks, modifier le fichier de configuration XML utilisé pour le HIDS.
- **HIDS contrôle** - Définir des actions de contrôle du HIDS, redémarrez les services du HIDS, et vue les alertes journaux.

✓ La génération de rapport :

Alors que le menu Dashboards offre une visibilité et l'affichage des différents paramètres de sécurité réseau pour votre environnement réseau, l' USM fournit également plus de 200 rapports différents que vous pouvez planifier ou générer à la demande, qui fournissent des détails sur les différents aspects de l' USM sécurité du réseau.

Les rapports Page Display

Lorsque vous sélectionnez les **rapports** > **Tous les rapports** option de menu, USM affiche la page suivante.

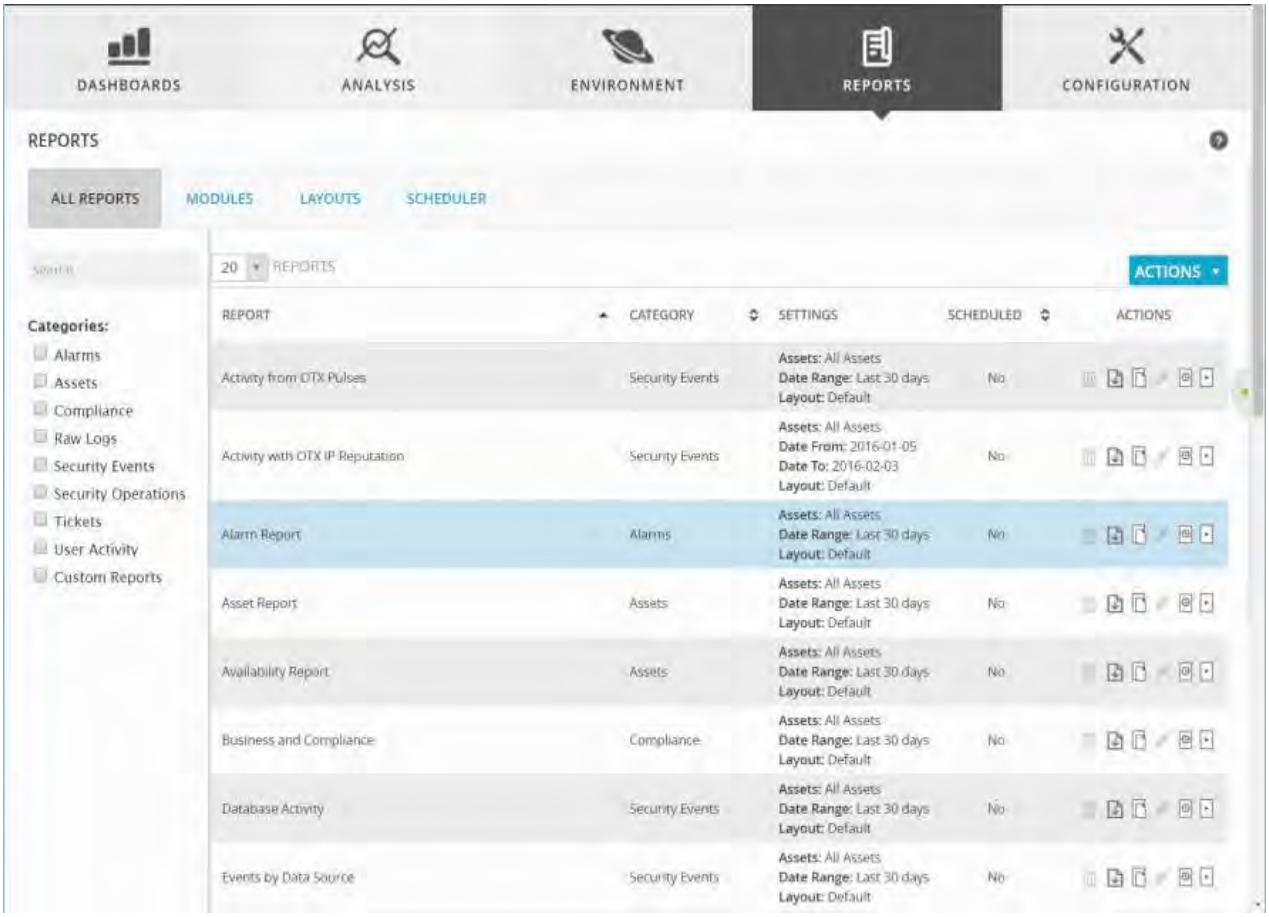


Fig 41 : génération de rapports

Cette page affiche l'ensemble de la collection de rapports disponibles dans l' OSSIM , indiquant le nom de chaque rapport, ses catégories, les paramètres de rapport, et si le rapport

est prévu pour être généré. Depuis cette page, vous pouvez également sélectionner les cases à cocher dans le panneau de recherche de gauche pour restreindre l'affichage pour afficher uniquement les rapports appartenant à des catégories sélectionnées.

Chacune de ces catégories de rapports est également disponible comme une option de sous - menu de rapport, par exemple, vous pouvez sélectionner **Rapports** > **Alarmes** pour afficher une liste qui contient seulement des rapports relatifs aux alarmes.

La dernière colonne dans la liste des rapports décrit les actions disponibles pour un rapport sélectionné. Ceux-ci comprennent Effacer, Export, Copier, Modifier, Exécuter personnalisé et Exécuter le rapport. Vous pouvez générer ou exécuter un rapport, à la demande, ou de créer un planificateur de tâches à exécuter périodiquement un rapport. Après avoir exécuté les rapports, vous pouvez les enregistrer en format PDF pour l'impression ou la distribution par courrier électronique.

En cliquant sur le bouton **Actions**, fournit des options pour créer ou importer un nouveau rapport.

En plus des pages d'affichage par défaut à partir de laquelle vous pouvez accéder et exécuter des rapports, OSSIM offre l'affichage des pages alternatives pour ce qui suit:

- **Modules** - Fournit la sélection de plus de 2600 composants de rapport à inclure dans les rapports. Vous pouvez définir des requêtes pour récupérer des données utilisées pour générer des graphiques et des tableaux inclus dans les rapports.
- **Layouts** - Fournit des options pour définir les aspects graphiques des rapports en définissant l'en- tête et pied de page, des couleurs et des icônes qui signalent les documents utilisés.
- **Scheduler** - Fournit des options pour spécifier la génération périodique de rapports, désignant également qui peut voir un rapport et qui les rapports sont envoyés.

C. AVANTAGES et LIMITES (ou inconvénients) d'OSSIM

➢ Avantages :

- OSSIM est une solution open-source
- Solution basée sur des outils de sécurité open-source. Permet une grande modularité et offre un panel de fonctionnalité conséquent.
- Pas de solution vraiment concurrente à ce jour (commerciale ou opensource). La solution la plus proche est **Prelude** mais la solution est beaucoup moins modulaire qu'OSSIM.
- Interface intuitive grâce à la modularité du panneau de contrôle qui s'adapte aux besoins du client.

➢ Inconvénients ou limites :

- Solution complexe à mettre en oeuvre. Nécessite une démarche d'audit et d'évaluation des risques pour être pertinent dans la configuration de la politique de sécurité souhaitée.

- Configuration difficile de par le grand nombre de paramètres pouvant rentrer en jeu

CONCLUSION

Mettre en œuvre un SOC peut être une tâche monumentale. Le SOC n'est plus un simple monitoring des événements se produisant sur le périmètre d'une entreprise mais une surveillance de tous les évènements qui peuvent survenir sur la globalité de l'infrastructure. Bien que les points les plus fins de déploiement SOC soient très spécifiques au réseau, il y a trois éléments majeurs que chaque organisation doit comprendre : personnes (employés), processus et technologies. Les trois existent dans toute gestion de la sécurité et devraient être considérés comme tout aussi critique.

La détection des menaces complexes, en temps réel et 24h/24h, est un enjeu crucial pour toutes les entreprises et par conséquent pour l'économie. Disposer d'une intelligence collective globale sur les menaces potentielles est un élément essentiel pour la mise en place d'un SOC avec un monitoring efficace permettant de réagir rapidement à des situations de danger.

Pourtant, encore trop peu d'organisations sont équipées d'un tel dispositif. Les raisons d'un tel manque peuvent se lister en 3 points :

- Les organisations n'ont pas toujours les compétences en interne pour piloter un SOC.
- La mise en place d'un SOC coûte cher et les entreprises n'ont pas forcément les moyens financiers.
- Certaines organisations n'ont ni les outils, ni les méthodes pour piloter un SOC.

Les SOC sont généralements basés autour d'un SIEM (gestion d'événements et informations de sécurité).

OSSIM est le SIEM open-source de AlienVault, c'est une solution composée de trois briques.

- une partie serveur

Qui contient les différents moteurs d'analyse, de corrélation et les bases de données.

- une partie agent

Qui prend en charge la collecte et la mise en forme des événements

- une partie framework (ou interface web)

Qui regroupe les consoles d'administrations et les outils de configuration et de pilotage.

Cette solution offre une grande modularité de par sa capacité à s'appuyer sur des outils de sécurité open-source. OSSIM est en quelque sorte le chef d'orchestre des différentes solutions déjà existante et permet de fédérer, d'agréger, d'analyser et de stocker les informations de manière centralisée et normalisée.
OSSIM s'appuie sur des mécanismes de corrélations, de gestion des priorités et d'évaluation des risques pour qualifier les alertes.
OSSIM traite les informations soit en temps réel soit sur une fenêtre de temps donnée.
Son interface web complètement modulaire s'adapte très bien aux besoins spécifiques de chaque utilisateur. OSSIM offre ainsi des informations essentielles et concises.
Tout ceci fait d'OSSIM une solution globale de management de la sécurité.
Cependant, les mécanismes mis en œuvre au sein d'OSSIM sont tout aussi complexes à configurer que précis dans leur utilisation.

En fait, la solution OSSIM ne peut être efficace (à mon avis) qu'au sein de la mise en œuvre d'une réelle politique de sécurité au sein du SI. Cela passe par des audits techniques et des évaluations des risques afin de bien identifier les métriques à surveiller.
Ce n'est qu'à cette condition que la solution OSSIM sera véritablement efficace.

Webographie :

La principale source de documentation utilisée pour la rédaction de ce mémoire a été Internet dont voici les principaux sites.

: https://fr.wikipedia.org/wiki/Security_Operations_Center (consulter le 5 mars 2019)

: https://www.alienvault.com/products/ossim (consulter en mars 2019)

: http://www.snort.org (consulter le 15 mars 2019)

: https://fr.wikipedia.org/wiki/IDMEF_:_Intrusion_Detection_Message_Exchange_Format (consulter avril 2019)

: https://www.src-solution.com/comment-reussir-le-deploiement-dun-soc-security-operatio-center/ (consulter en avril 2019)

: https://www.solutions-numeriques;com/articles/partage-dexperience-la-problematique-du-soc-porte-essentiellement-sur-la-gouvernance-et-la-federation/ (consulter en avril 2019)

: https://www.orange-business.com/fr/blogs/securite/securite-organisationnelle-et-humaine/securite-siem-ou-pas-siem- (consulter en avril 2019)

: https://www.oracle.com/fr/cloud/soc-security-operations-center.html (consulter avril 2019)

: http://www.vmware.com/
: http://www.debian.org

Bibliographie :

http://download.velannes.com/Ossim_doc.pdf (consulter en mars 2019)

https://www.alienvault.com/docs/OssimJWinteregg.pdf (consulter en mars 2019)

GLOSSAIRE

SOC	Security operation center (centre d'opération de sécurité)
IT	Technologie de l'information
CERT/C-SIRT	Computer Emergence Response Team /Computer Security Incident Response Team (l'équipe d'intervention en cas d'incident de sécurité informatique)
S.I	Système d'Information
MSSP	Managed Security Service Provider
DSI	Direction des Sytèmes d'Information
SSI	Sécurité des Systèmes d'Information
PCI-DSS	Payment Card Industry Data Security Standard (norme de sécurité de l'industrie des cartes de paiement)
ISO	International Organisation Standardization (organisation internationale de normalisation)
RGPD	Règlement Général sur la Protection des Données
PSSI	Politique de Sécurité du Système d'information
SMSI	Security Management System Information
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
ITIL	Information Technology Infrastructure Library
ETSI	European Telecommunications Standards Institute
WAF	Web Application Firewall
IPS	Intrusion Prevention System
SNMP	Simple Network Management Protocol
SYSLOG	Protocole de journaux d'événements d'un système informatique
OPSEC	Sécurité opérationnelle : méthode pour se prémunir des risques si des informations sensibles sont acquises par des adversaires
IDMEF	Intrusion Detection Message Exchange Format

IETF	Internet Engineering Task Force : élabore les normes qui composent la suite de protocoles Internet (TCP/IP).
RFC	Publication de référence portant sur le réseau Internet
RSSI	Responsable de Sécurité des Systèmes d'Information
RAID	Redundant Array of Independent/Inexpensive Disks
IOC	Indicator Of Compromission (indicateur de copromission)
URL	Uniform Resource Locator
IP	Internet Protocol
OSSIM	Open Source Security Information Management
RACI	responsible, accountable, consulted et informed
APT	Advanced Persistent Threat
PDCA	Plan, Do, Check et Act = planifier, réaliser, vérifier et agir
OIV	Opérateur d'Importance Vitale
OSSEC	Open Source HIDS SECurity
WEB	World Wide Web
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
POP	Post Office Protocol
http	HyperText Transfer Protocol
Syslog	un protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.
SNMP	Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
IDMEF	(Intrusion Detection Message Exchange Format / En français, Format d'Échange de

	Messages de Détection d'Intrusion) est un format de données servant à échanger des informations de sécurité collectées par les logiciels de détection d'intrusion et de prévention d'intrusion avec les systèmes de management qui communiquent avec eux.
IETF	Internet Engineering Task Force, Un des groupes de travail de l'IAB chargé de résoudre les problèmes techniques du réseau. C'est par son biais que les standards Internet sont préparés et élaborés.
TCP/IP	Transmission Control Protocol/ Internet Protocol". Série d'instructions définissant la façon dont les paquets de données sont envoyés sur les réseaux. C'est le langage de communication entre tous les ordinateurs connectés à Internet.
RFC	Publication de référence portant sur le réseau Internet et rédigée par les experts du réseau