Université Lumière Lyon 2
Faculté de droit et de science politique

Rapport de stage pour obtenir le diplôme
de Master Informatique, spécialité OPSIE
« Organisation et Protection des Systèmes d'Information dans les Entreprises »

Mise en oeuvre d'un prototype d'architecture OSSIM

Présenté par : Philippe Martinet

Maître de stage : M. Maxime Feroul
Tuteur de stage : M. David Pierrot

Année : 2005/2006

Sommaire

Remerciements,

A tous les membres de la société Kyos et plus particulièrement à M. Maxime Feroul, mon maître de stage. Merci pour leur accueil, le temps qu'ils ont su m'accorder, leur soutien et leurs conseils avisés.

Aux intervenants de la formation OPSIE et plus particulièrement à M. David Pierrot, mon tuteur pour ce stage. Merci pour la qualité des cours dispensés qui m'ont permis de mieux appréhender les multiples facettes de ce projet.

Présentation de l'entreprise

1. Kyos SARL

Kyos est une société de service (SSII) basée à Genève et spécialisée dans le domaine de la sécurité informatique.
Fondée en 2002, Kyos se positionne comme un opérateur global de la sécurité informatique, grâce à une expertise dans les métiers de conseil, d'ingénierie et d'infogérance.

Kyos accompagne ses clients dans la mise en œuvre d'une stratégie de sécurité complète, adaptée à leurs besoins, et surtout efficace dans le temps.

2. Les missions

Conseil

Kyos prend en charge la conception et le pilotage de la mise en oeuvre de solutions relatives à la sécurisation :

- des points d'accès à Internet
- des réseaux d'entreprises
- des plates-formes e-businness

Les prestations couvrent l'ensemble des phases suivantes :

- Définition de politique de sécurité
- Conception d'architecture de sécurité
- Conduite d'appel d'offre pour le choix de technologies et de fournisseurs
- Assistance à maîtrise d'ouvrage
- Sensibilisation / Formation

Ingénierie

Kyos met également à disposition des consultants experts en sécurité pour la réalisation en mode régie ou en mode forfaitaire des projets de ses clients.

De part son expérience, Kyos réalise ou accompagne ses clients durant les différentes phases du projet et leur apporte son expertise dans les domaines tel que :

- L'intégration Sécurisée
- Les audits de composants
- Les tests d'intrusion

- **Infogérance**

  Les entreprises soucieuses de maintenir un niveau de sécurité efficace sont confrontées aux obstacles suivants :

  - disposer de ressources spécialisées
  - une complexité croissante des technologies
  - un besoin fréquent de formation
  - un manque de temps et de moyens à consacrer au suivi quotidien

  S'affranchir de ces obstacles, se traduit par des coûts élevés et parfois exorbitants pour certaines entreprises en regard de leurs besoins de sécurité. On observe souvent dans ce cas l'abandon pur et simple de cette activité.

  Il existe pourtant une solution intermédiaire, l'infogérance (complète ou partielle) de sécurité.

  Afin de permettre un réel contrôle des coûts, Kyos propose une offre modulaire de services à ses clients.

  - Administration & supervision
  - Analyse de logs
  - Veille technologique
  - Tests d'intrusion récurrents

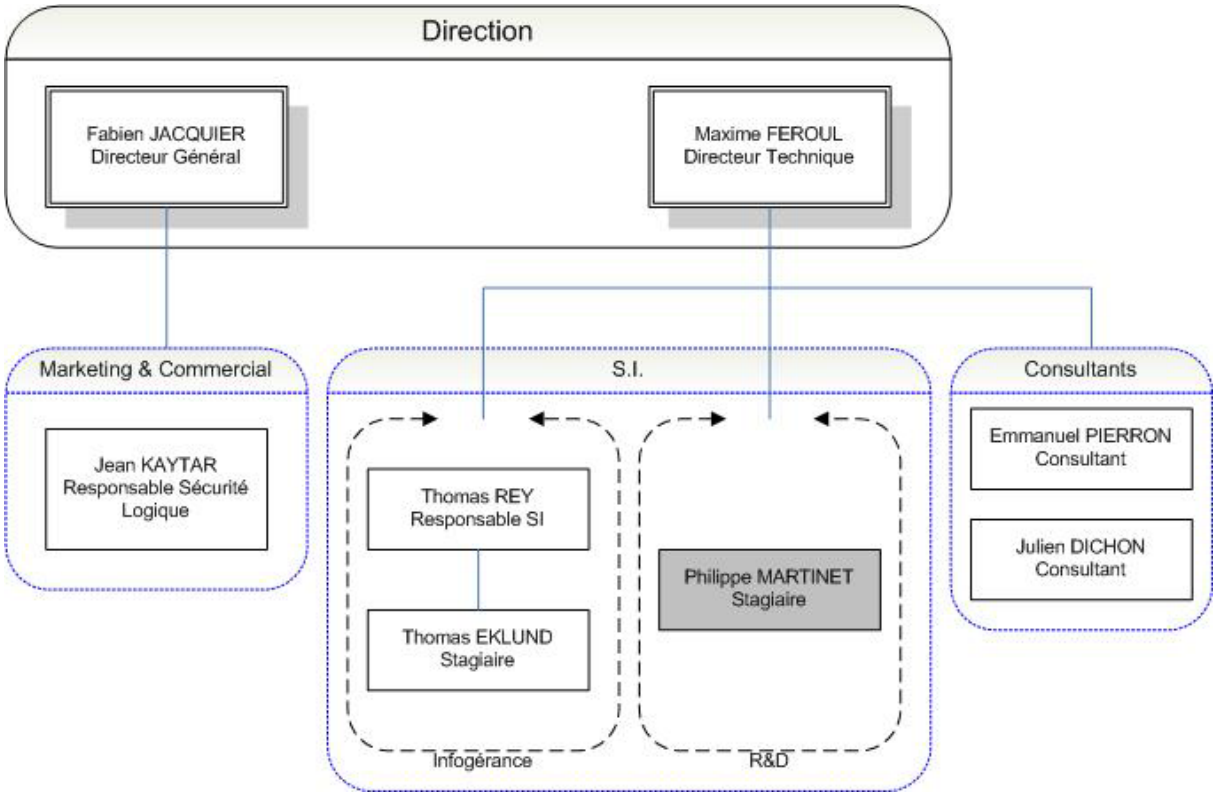
3. L'activité R&D

En parallèle de ses missions, Kyos attribue une part importante de son activité dans le domaine de la recherche et du développement (R&D) notamment au travers de participations à des projets de la Commission européenne.

Il s'agit pour Kyos d'une composante fondamentale du métier de la sécurité. La société doit être en mesure d'anticiper les évolutions des problématiques de sécurité sur les technologies émergentes du marché.

4. Organigramme

Fondée en 2002, Kyos est encore une jeune société en pleine expansion.
Lors de la rédaction de se rapport, elle comptait déjà 8 collaborateurs.



Le stage

1. Définition du besoin

Le cœur de métier de la société Kyos est avant tout et surtout la sécurité informatique. De part cette activité, la société a pu se forger une expérience concrète sur le terrain au contact des ses clients. De cette expérience la société Kyos en a dressé le bilan suivant.

De nos jours, le système d'information (S.I.) est devenu vital pour la majorité des entreprises. Garant de l'activité de l'entreprise pour certaines ou simple garant des données confidentielles pour d'autres, une interruption de service du S.I. induirait des risques majeurs pour l'entreprise

- Risque de perte financière
- Risque de perte d'image
- Risque d'impact juridique

Face à ces risques, les entreprises n'ont pas d'autre choix que d'investir dans une politique de sécurité. Cependant le coût de ces investissements est loin d'être négligeable et les entreprises sont souvent confrontées aux problèmes suivants :

- La multiplicité et la complexité croissante des technologies.
- L'émergence de nouvelles attaques (phishing, virus, etc …) sans cesses plus pertinentes qui imposent aux entreprises une veille permanente
- La spécificité. Chaque entreprise est différente, donc chaque entreprise à ses contraintes propres (au niveau stratégique comme au niveau technique)

C'est pour répondre à ces besoins que la société Kyos a été créée. Aujourd'hui la société souhaite renforcer sa position en articulant bien ses offres autour des problématiques de sensibilisation et de sécurisation des systèmes d'information de ses clients.

- La sensibilisation.
  « La sécurité est l'affaire de tous ».

Kyos souhaite assurer une mission de conseil auprès de ses clients pour les former et les sensibiliser à la sécurité.
Une politique de sécurité sera d'autant plus efficace si tous dans l'entreprise en sont les acteurs.

- L'action.
  « Un bon ouvrier travail avec les bons outils »

La mise en œuvre d'une politique de sécurité, c'est identifier les risques, savoir les mesurer et mettre en œuvre les outils pour diminuer ces risques.

Il existe de multiples solutions pour agir à différents niveaux de la sécurité du S.I..

- Solutions antivirales
- Solutions de type Firewall
- Solutions de détection d'intrusion

Ces solutions peuvent être soit matérielles, soit logicielles et peuvent intervenir sur un poste de travail, sur un serveur de production, sur une architecture de production etc …

Bref il n'existe pas vraiment de standard même si certaines solutions sortent du lot et s'imposent naturellement de part leur reconnaissance auprès des acteurs de la sécurité.

Autre inconvénient majeur. L'expérience montre que la mise en œuvre de telles solutions n'est valable que si les remontées d'informations sont suivies et traitées.
En sécurité informatique tout particulièrement, l'outil n'est utile que si les données remontées sont pertinentes et que celles-ci sont analysées et traitées.

2. Cahier des charges

En partant du postulat énoncé au paragraphe précédent, la société Kyos a décidé de réaliser une étude sur la solution OSSIM. Cette solution semblant répondre aux problématiques précédemment citées, permettant ainsi de gérer de manière centralisée les remontées d'information de différents outils, de les stocker et les traiter afin de faciliter l'administration et la gestion de la sécurité pour les administrateurs.

Après concertations avec les dirigeants de la société Kyos et aux vues des besoins, j'ai établi une liste des tâches à réaliser.

A. Etude de la solution OSSIM

    - Architecture de la solution
    - Analyse des fonctionnalités

B. Réalisation d'un prototype

    - Réalisation d'une maquette
    - Tests des fonctionnalités

C. Rédaction d'un compte rendu sur cette solution

    - Compte-rendu de l'étude
    - Compte-rendu des tests

D. Bâtir une offre de service intégrant la solution OSSIM

Le projet

Ce stage s'inscrit dans le cadre d'un projet de recherche et développement (R&D) pour le compte de la société Kyos (Réf INT12008/2).
En tant que tel, le stage a été géré comme tous les autres projets de la société.

J'ai abordé ce projet selon trois axes :

- L'objectif
- Les coûts
- Les délais

Le but étant de bien identifier les tâches de ce projet et d'établir un planning réaliste en fonction de ces trois contraintes.

1. L'objectif

L'objectif principal est de réaliser l'étude d'une solution technique OSSIM dans le cadre d'un projet R&D sur la sécurité des systèmes d'information. Cette étude est issue d'un constat énoncé par la société Kyos concernant les besoins passés, présents et futurs de ses clients.

Les détails du postulat de départ ont été définis dans la section « Stage » du présent document.

Dans un second temps, et en fonction des résultats, l'objectif est de bâtir une nouvelle offre de service basée sur cette solution.

2. Les coûts

Il est difficile de placer une notion de coûts dans le cadre d'un projet de R&D.
Les coûts associés au projet sont directement indexés aux coûts des intervenants sur ce projet.

Ce projet de R&D dans sa définition de départ n'ayant pas pour vocation de fédérer plusieurs profils de ressources. L'unique ressource associée à ce projet était moi-même.

Cependant dans un souci de bien discerner les étapes clés de suivi et de validation avec la direction technique de Kyos, j'ai ajouté un ressources générique nommée « Kyos » représentant le staff technique qui a participé au pilotage de ce projet (réunion de lancement, réunion d'avancement, etc …)

Les services de R&D ont très souvent pour vocation d'être des centres de coûts et non de profit ; les projets associés ne générant pas de profits directs pour la société.

Il en a été de même dans le cadre de mon stage, l'objectif étant d'effectuer une étude et de réaliser un prototype d'une solution technique afin de l'intégrer si cela était pertinent aux offres de service de la société Kyos.

Partant de ces constats, j'ai considéré que le coût associé à ce projet n'était pas une contrainte dans l'établissement de mon planning.

3. Les délais

Ce projet a été établit pour la durée de mon stage.
Les conventions de stage ont été signées pour un stage du 1er Mars 2006 au 30 Juin 2006.

Cependant, compte tenu de la localisation géographique de la société Kyos et compte tenu de ma situation professionnelle en France au début de ce stage, nous avons décidé d'un commun accord avec les dirigeants de la société Kyos que le projet ne démarrerait qu'au 1er Avril 2006. Le premier mois étant mis à profit pour mettre en œuvre toutes les démarches administratives (déclarations auprès du canton de Genève, Assurance, etc …), et nous permettre de nous organiser au niveau logistique (problème du logement, mise à disposition du matériel, etc …)

La durée effective de ce projet a donc été de 13 semaines (3 mois)

Dans le cadre de ce projet de R&D, l'unique contrainte de temps était liée à la livraison des livrables.

Les dates de restitution des livrables ont été fixées conjointement ainsi :

Livrables	Deadline
Etude de la solution OSSIM	09 Juin 2006
Offre de service OSSIM	30 Juin 2006

4. Définition du planning

En fonction des contraintes énoncées précédemment, j'ai établi le planning prévisionnel suivant :

N°	Tâches	Ressources	Durée (en J)	Date de début	Deadline
1	Réunion de lancement du projet	PMT, Kyos	1	03/04/2006	-
2	Etude de la solution OSSIM	PMT	20	04/04/2006	-
3	Réalisation du prototype	PMT	10	02/05/2006	-
4	Point sur l'avancement du projet	PMT, Kyos	1	15/05/2006	-
5	Rédaction CR sur la solution OSSIM	PMT	20	16/05/2006	09/06/2006
6	Présentation de la solution OSSIM	PMT,Kyos	5	13/06/2006	-
7	Réunion de suivi de projet	PMT,Kyos	1	20/06/2006	-
8	Réalisation d'une offre de service	PMT	10	20/06/2006	30/06/2006

PMT : Mon trigramme, me désigne comme ressource
Kyos : Ressource générique désignant le staff de la société Kyos

	Semaine 1	Semaine 2	Semaine 3	Semaine 4	Semaine 5	Semaine 6	Semaine 7
Réunion de lancement du projet							
Etude de la solution OSSIM							
Réalisation du prototype							
Point sur l'avancement du projet							
Rédaction CR sur la solution OSSIM							
Présentation de la solution OSSIM							
Réunion de suivi de projet							
Réalisation d'une offre de service							

	Semaine 8	Semaine 9	Semaine 10	Semaine 11	Semaine 12	Semaine 13
Réunion de lancement du projet						
Etude de la solution OSSIM						
Réalisation du prototype						
Point sur l'avancement du projet						
Rédaction CR sur la solution OSSIM						
Présentation de la solution OSSIM						
Réunion de suivi de projet						
Réalisation d'une offre de service						

A. Etude de la solution OSSIM

1. Présentation générale de la solution

OSSIM est un projet open source de « management de la sécurité de l'information ». Cette solution s'appuie sur une gestion des logs basées 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 se vide constaté quotidiennement par les professionnels de la sécurité.

2. Principe technique de la solution

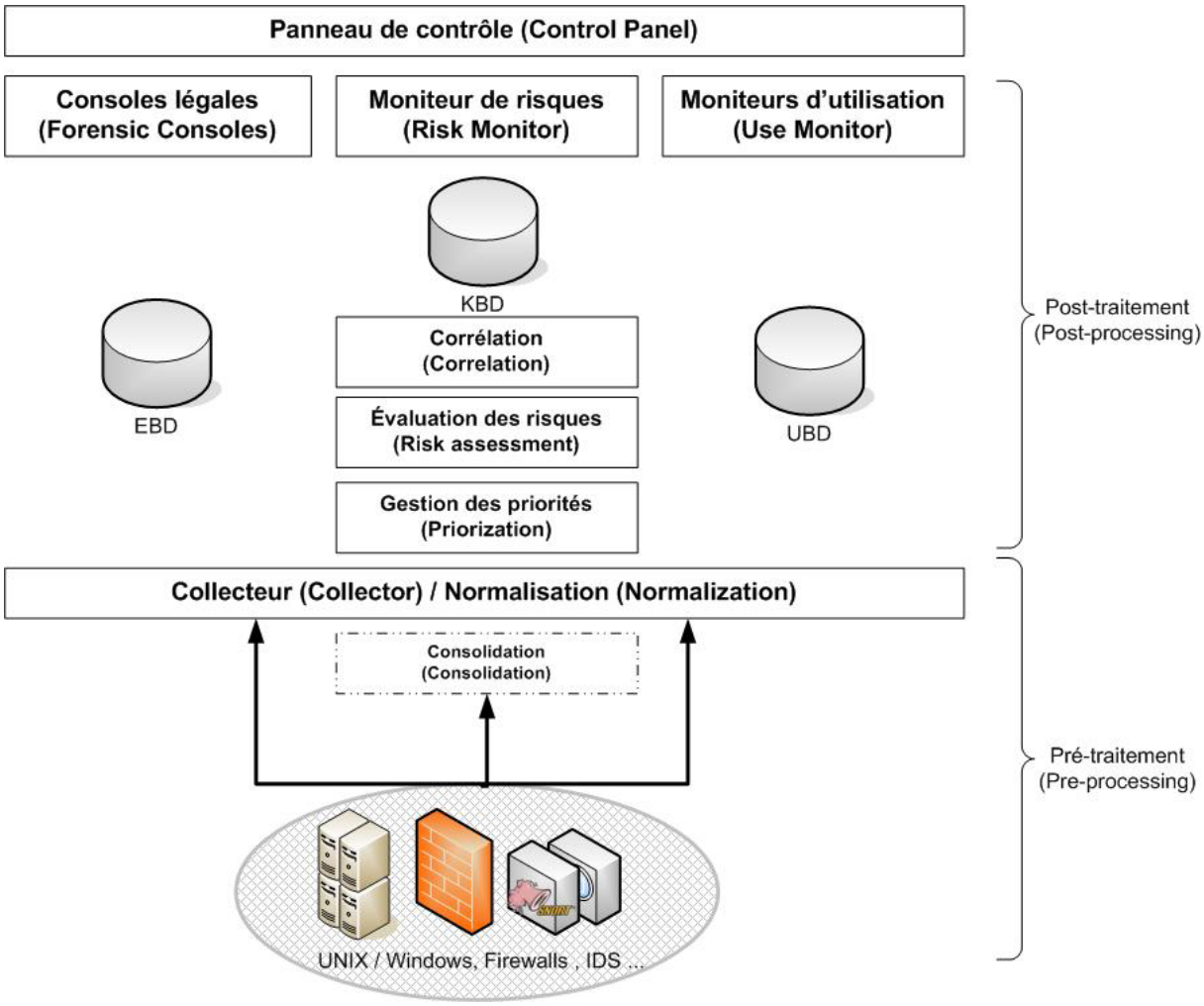
OSSIM est une solution fédérant d'autres produits open-source au sein d'une infrastructure complète de supervision de la sécurité (framework[1])

Le framework au sens d'OSSIM à 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.
La framewok est ainsi constitué des éléments de supervision suivants

- Un panneau de contrôle
- Des moniteurs de supervision de l'activité et des risques.
- Des moniteurs de supervision réseau et des consoles d'investigation (Forensic[2])

[1] Framework : Littéralement Cadre d'applications
Pour OSSIM le framework représente l'interface d'administration qui permet de fédérer les différents produits open-source associés.
[2] Forensic : Légal. Souvent traduit par Console d'investigation.



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

3. Architecture

En terme de développement, la solution OSSIM est donc architecturée autour de deux éléments.

- Le kernel[3]
- Les logiciels tiers

[3] Kernel : littéralement le noyau. Il représente le « cœur » de la solution.

- Le kernel

Le kernel est le premier niveau de développement d'OSSIM. Il permet de définir les structures de données.

Il fournit les interfaces qui permettent de communiquer avec les différents produits et travail sur les mécanismes de post-traitement.

Ces post-traitements assurés par la solution OSSIM s'appuient en fait sur des processus de post-traitement d'agents connus comme

- La détection des signatures des sondes de détection d'intrusion (IDS)
- La détection d'anomalie
- Les firewall

Le fonctionnement d'OSSIM se peut donc se décliner en deux étapes. Chaque étape correspondant à une partie bien distincte de l'architecture technique de la solution.

a) Prétraitement (ossim-agent)

Le prétraitement de l'information qui est assuré par les moniteurs d'événements et autres éléments de détection.

Les équipements qui prennent en charge ce prétraitement peuvent être déployés en même temps qu'OSSIM ou bien faire partie de l'architecture existante.
On retrouve parmi ces équipements, les sondes de détections d'intrusion (IDS), les Firewall[4], les syslog[5], etc …

Le prétraitement de l'information, assuré au niveau de ces équipements, consiste en la collecte des informations de logs ainsi que la normalisation des celles-ci afin de les stocker de manière uniforme et de pouvoir les traiter efficacement durant l'étape de post-traitement.

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.

b) Post-traitement (ossim-server)

Le post-traitement est constitué de l'ensemble des processus interne à la solution OSSIM qui vont prendre en charge l'information brute telle qu'elle a été collectée (puis normalisée), pour ensuite l'analyser, la traiter et enfin la stocker.

Les différents traitements appliqués aux informations recueillies dépendent des outils activés au sein de la solution mais aussi de politiques définies par le biais du panneau de contrôle. Les informations sont priorisées. Les risques sont évalués en fonction de la politique définie, et enfin les informations sont corrélées avant d'être stockées dans la base des événements (EDB).

[4] Firewall : Pare-feu.
[5] Syslog : Gestionnaire de log système sur les systèmes *NiX. Par abus de langage, définit généralement les système de gestion des logs sur tous les systèmes / appliances.

En parallèle de ces actions, certaines informations comme la supervision réseau sont directement remontées par le biais de consoles.

Le kernel permet également d'obtenir cette notion de framework au sein d'OSSIM qui assure le lien avec tous les autres systèmes.

- Les logiciels tiers

L'autre niveau de développement de la solution consiste à assurer l'interconnexion de logiciels tiers avec le kernel.

Il existe actuellement deux types de logiciels tiers pris en charge par OSSIM

- Les produits open-source qui peuvent être modifiés et/ou patchés au besoin et qui sont généralement fournis dans le package[6] OSSIM

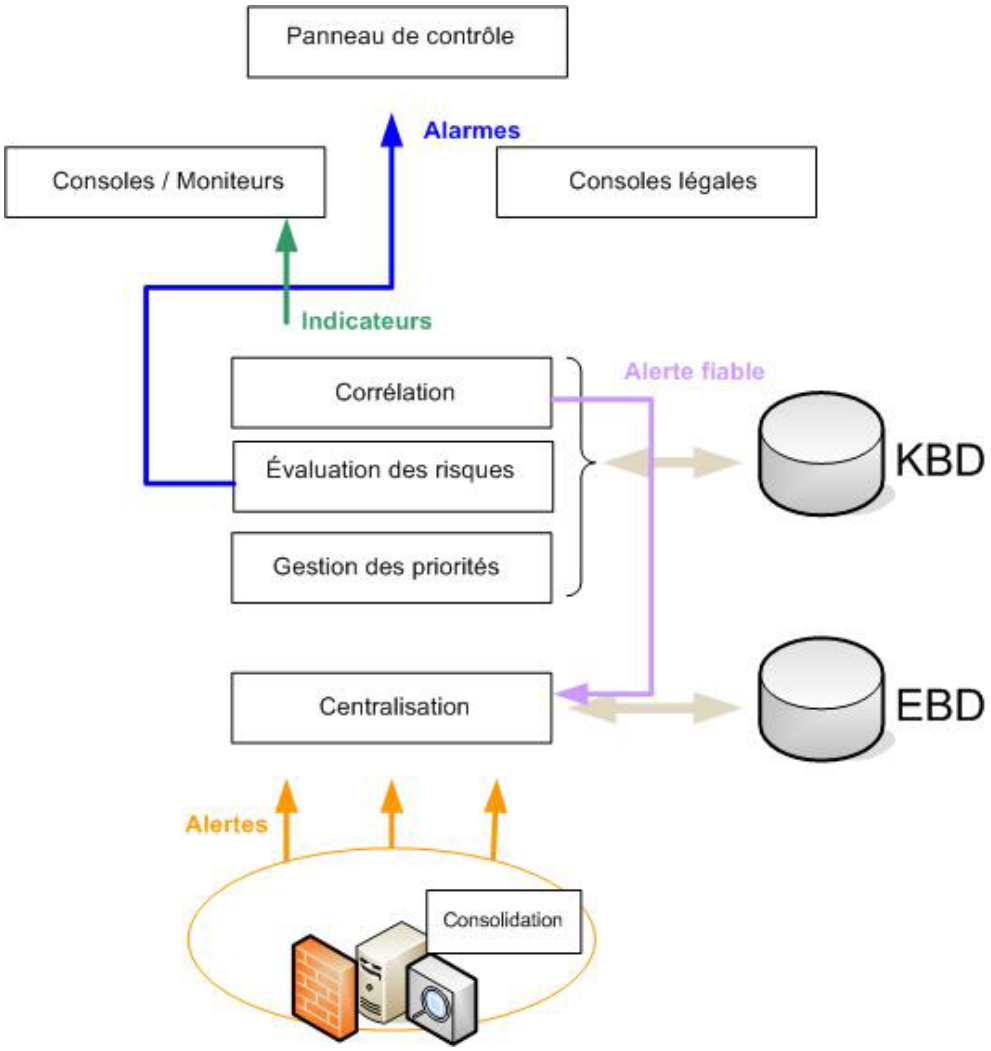
- Les produits commerciaux qui ne peuvent être modifiés et/ou patchés pour les adapter à la solution et qui ne sont donc pas inclus dans le package OSSIM.

Remarque :
L'adaptation des produits à OSSIM est effectivement un élément fondamental, dans le cas d'un produit qui ne prend pas en charge les standards utilisés par OSSIM, puisque la solution tente justement de fédérer toutes les sources d'information qu'elle ingère.

[6] Package : anglicisme définissant souvent un ensemble de programmes réunis dans un seul paquetage.

4. Les flux de fonctionnement d'OSSIM

Pour bien comprendre le fonctionnement interne d'OSSIM, voici un schéma type reprenant le flux d'information au travers de la solution.



Principe de cheminement du flux d'information

- 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 disponibles (SNMP, etc …)

- Le parser[7] normalise ces alertes et les stocke dans la base de donnée des événements (EDB)

- Le parser se charge également de f'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[8] (Compromise and Attack Level Monitor)

- Le panneau contrôle quand a lui remonte les alarmes 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.

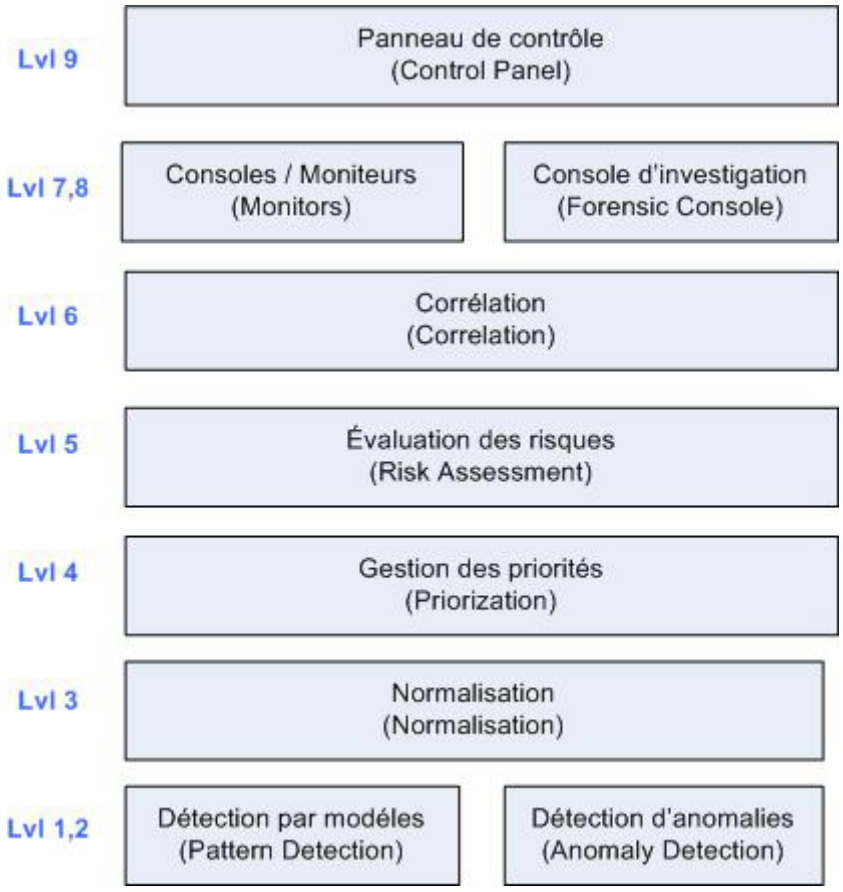
- L'administrateur peut enfin vérifier l'état de la machine impliquée en utilisant les consoles d'utilisation, de profil ou de session.

5. Les fonctionnalité d'OSSIM

Dans cette partie, j'ai essayé de présenter 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 :

[7] Parser : littéralement l'analyseur. Le parser défini souvent un outil (script) qui parcours des fichiers en vue d'y effectuer certaines actions.
[8] CALM est un algorythme d'évaluation. Cet algorythme sera détaillé un peu plus loin dans ce document.



1) La Détection 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.

Le pattern matching est une technique « ancienne » qui identifie une intrusion par le seul examen d'un paquet et la reconnaissance dans une suite d'octets du paquet d'une séquence caractéristique d'une signature précise. Très simpliste elle entraîne de nombreux « faux positifs » et « faux négatifs ». De plus elle est très facilement éludable via la fragmentation de paquet.

Rappel

a) *Faux positifs*

Un faux positif est un événement remonté par un dispositif de détection d'intrusion mais qui ne correspond par 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 firewall 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.

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).

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 œuvre un processus d'agrégation.

La normalisation exige quand 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[9]. 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.

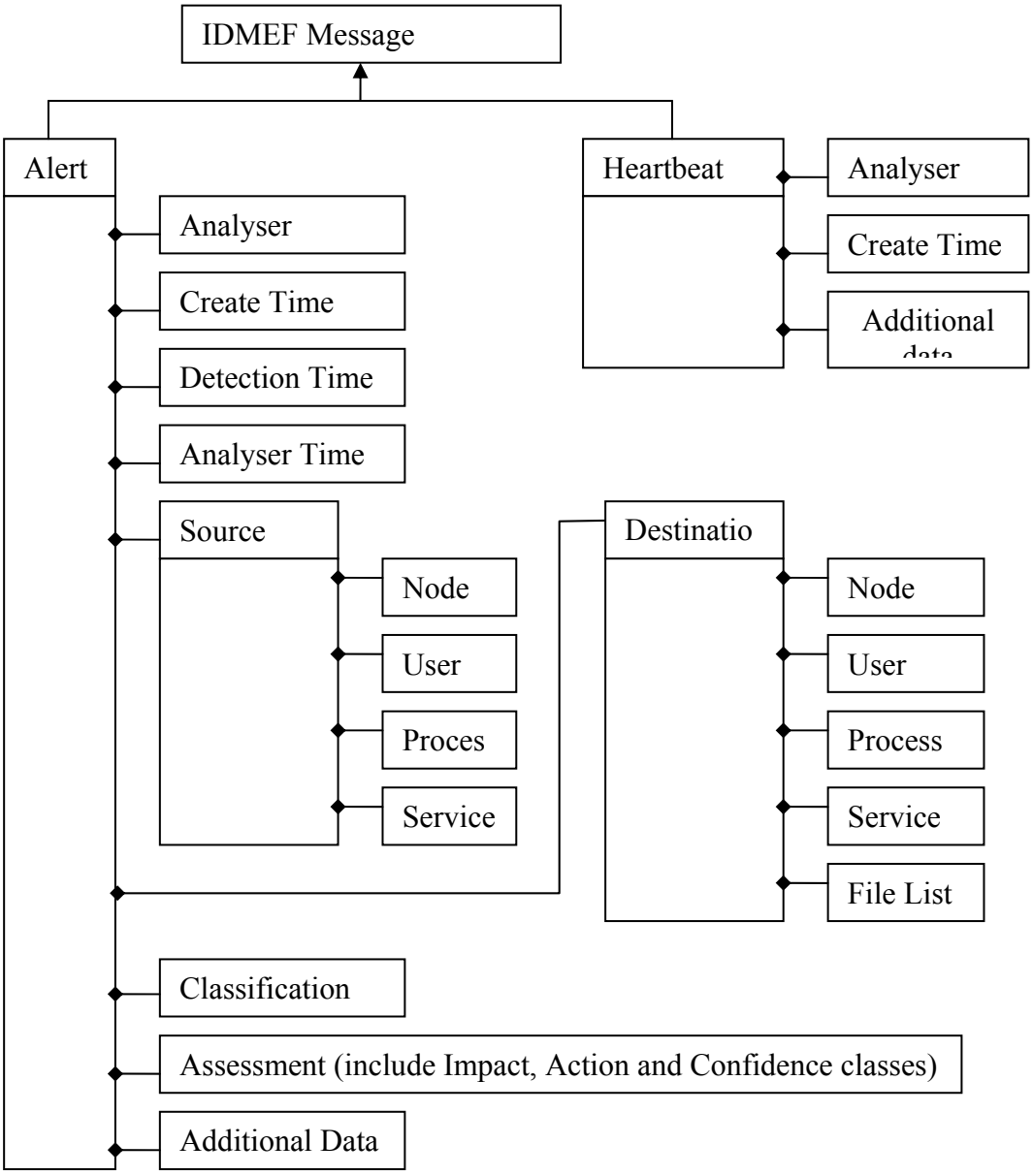
L'IDMEF est un standard établit par l'IETF[10]. Le modèle de données de l'IDMEF est une représentation orientée objet au format XML des alertes envoyées par les équipements de détection vers OSSIM.

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.

[9] IDMEF : Intrusion Detection Message Exchange Format
[10] IETF : Internet Engineering Task Force



Modèle de donnée IDMEF[11]

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.

[11] Extrait du draft publié par l'IETF

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 de 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.

5) Evaluation des risques – Level 5

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

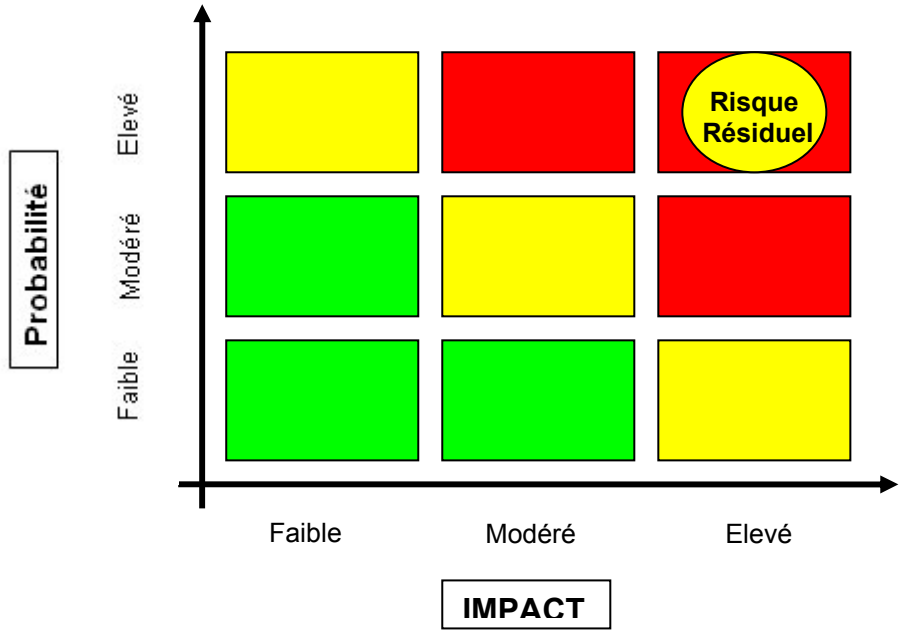
Dans OSSIM, l'importance donnée à un événement dépend de trois facteurs :

- la valeur des équipements associée à l'événement
- La menace représentée par l'événement (Impact)
- Le degré d'occurrence

a) Risque intrinsèque / Risque inhérent

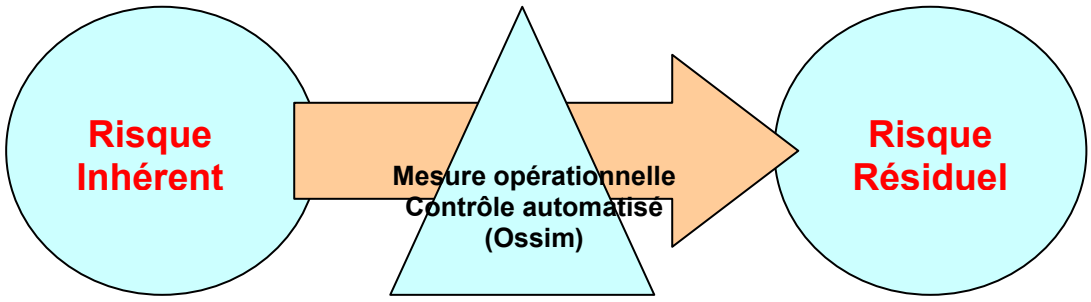
Communément admise, la définition traditionnelle du risque est la suivante :

Le risque est caractérisé par son impact et son degré d'occurrence



Traditionnellement l'évaluation des risques est concernée par des risques intrinsèques, ou des risques latents, en d'autres termes, des risques qu'une entreprise assume en vertu à la fois des équipements qu'elle possède afin de développer ses affaires mais également des menaces circonstancielles liées à ces équipements.

Le poids d'un risque peut être corrigé par un dispositif de maîtrise des risques (DMR). OSSIM tient lieu ici de DMR.



b) Risque immédiat

Grâce aux possibilités de contrôle en temps réel qu'offre OSSIM, il est possible de mesurer le risque lié à la situation actuelle en temps réel.

Dans ce cas-ci la mesure du risque est pondérée par les dommages qu'il produirait et la probabilité que la menace se produise au moment présent.

Cette probabilité est en fait un dérivé de l'imperfection des sondes et s'avère n'être rien de plus que le degré de fiabilité des sondes qui détectent une potentielle intrusion en cours.

Le risque immédiat peut donc être définit par l'état de risque produit quand une alerte est reçue et évaluée instantanément comme une mesure des dommages qu'une attaque pourrait produire, pondérée par la fiabilité du détecteur qui a remonté l'information.

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

6) Corrélation – Level 6

La corrélation est au cœur de la solution OSSIM.

Remarque :
La fonction de corrélation peut être définie comme un algorithme qui exécute une opération sur des données en entrée et renvoie des données en sortie.

Les informations collectées par les détecteurs et les moniteurs sont spécifiques et encore partielles. Elles ne représentent qu'une petite partie de la quantité d'information que nous souhaiterions obtenir au final.

Le mécanisme de corrélation peut donc être vu comme la possibilité d'utiliser les informations remontées par les détecteurs et, en utilisant un nouveau niveau de traitement, de compléter et d'améliorer le niveau d'information.
Le but étant de rendre cette remontée d'information le plus efficace possible par rapport à l'étendue de la quantité d'information disponible sur le réseau d'entreprise.

Le mécanisme de corrélation est en quelque sorte un moyen de gommer un certain manque de fiabilité ou un sensibilité insuffisante au niveau des détecteurs.

En fait, si l'on voulait obtenir un maximum d'efficacité au niveau des détecteurs, il faudrait imaginer un détecteur capable de capter tous les événements disponibles sur le réseau. Il lui faudrait ensuite les stocker et les afficher.
Etant donné le volume des informations qui transitent sur un réseau d'entreprise, cette solution n'est tout simplement pas envisageable !

- Principe technique de la corrélation sous OSSIM

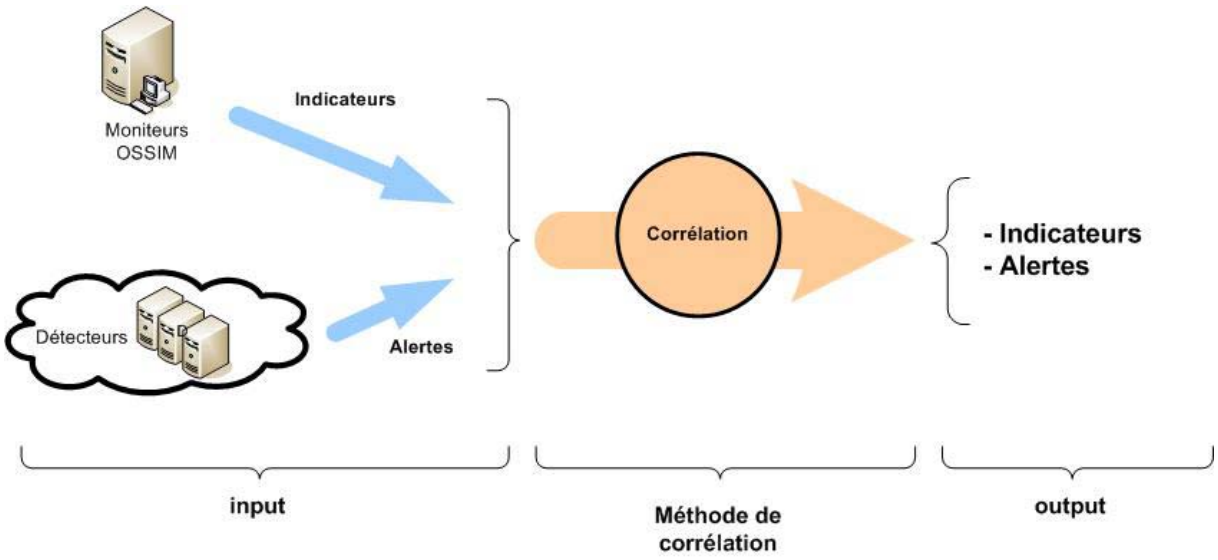
a) En entrée (input) :

Deux éléments bien définis fournissent des informations aux fonctions de corrélation :

- Les moniteurs, qui fournissent normalement des indicateurs
- Les détecteurs, qui fournissent normalement des alertes

b) En sortie (output) :

On retrouve également l'un de ces deux éléments : alertes ou indicateurs.
Les fonctions de corrélation deviennent en fait de nouveaux détecteurs et moniteurs. (cf flux de fonctionnement OSSIM - §4 de cette étude).



Le modèle de corrélation d'OSSIM a pour objectif de :

- Développer des modèles spécifiques pour détecter le connu et le détectable.
- Développer des modèles non spécifiques pour détecter l'inconnu et l'indétectable
- Fournir une machine d'inférence qui peut être configurée en utilisant des règles en corrélation et qui a la capacité de décrire des modèles plus complexes
- Fournir la capacité de lier des détecteurs et des moniteurs de manière récursive pour créer des objets plus détaillés et plus utiles
- Développer les algorithmes pour montrer une vue générale de la situation de la sécurité

Pour atteindre ces objectifs, OSSIM utilise deux méthodes de corrélation très différentes, basées sur les deux principes suivants :

- Corrélation en utilisant des séquences d'événements

  Concentrées sur des attaques connues et détectables qui relie les modèles et les comportements connus qui définissent une attaque en utilisant des règles mises en application par un état de référence.

- Corrélation en utilisant des algorithmes heuristiques.

  Cette méthode utilise une approche opposée, mettant en application des algorithmes qui essayent de détecter des situations risquées en utilisant l'analyse heuristique.

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

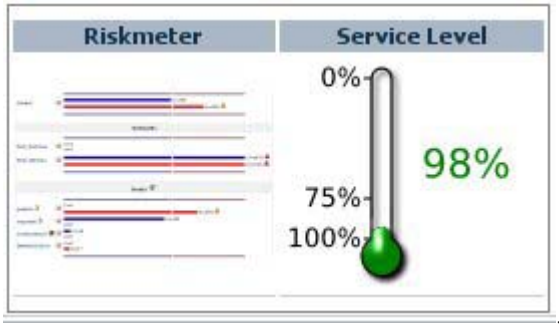
Détails des mécanismes de corrélation

a) Méthode 1 : Corrélation en utilisant des algorithmes heuristiques

Pour cette méthode, OSSIM met en application un algorithme heuristique simple en utilisant l'accumulation d'événements (CALM[12]) afin d'obtenir un indicateur ou un instantané de l'état général de la sécurité du réseau.

Dans ce processus l'objectif premier est d'obtenir le risque immédiat tout d'abord puis une valeur que l'on pourrait définir comme le risque accumulé.

En fait cette méthode de corrélation permet d'obtenir une sorte de « thermomètre » des situations à risque, et ce, sans jamais connaître aucun détail au sujet des caractéristiques du problème.



Cet indicateur permet donc de montrer le risque accumulé sur une période donnée.

[12] CALM : Compromise and Attack Level Monitor. Cet algorithme sera détaillé un peu plus loin dans ce document.

Pour reprendre l'exemple du « thermomètre », la valeur de l'indicateur va *monter* proportionnellement à la quantité des événements reçus récemment et en fonction de leur criticité.
Cette valeur *baissera* par contre si au bout d'un certain temps, aucun nouvel événement n'est survenu.

Cette méthode de corrélation complète la corrélation par séquences d'événements avec une approche opposée. Dans cette dernière nous essayons donc de caractériser des attaques possibles avec le plus haut niveau de détail possible.

En conséquence de quoi, la valeur de la corrélation employant des algorithmes heuristiques est doublée au sein d'OSSIM.

Cette méthode fournit donc une vue globale de la situation. Elle permet également de détecter les modèles possibles que d'autres systèmes de corrélation pourraient ne pas voir, soit parce que les attaques sont inconnues, soit à cause d'une certaine imperfection.

Algorithme CALM

CALM (Compromise and Attack Level Monitor) est un algorithme d'évaluation qui emploie l'accumulation d'événements et leur rétablissement dans le temps.

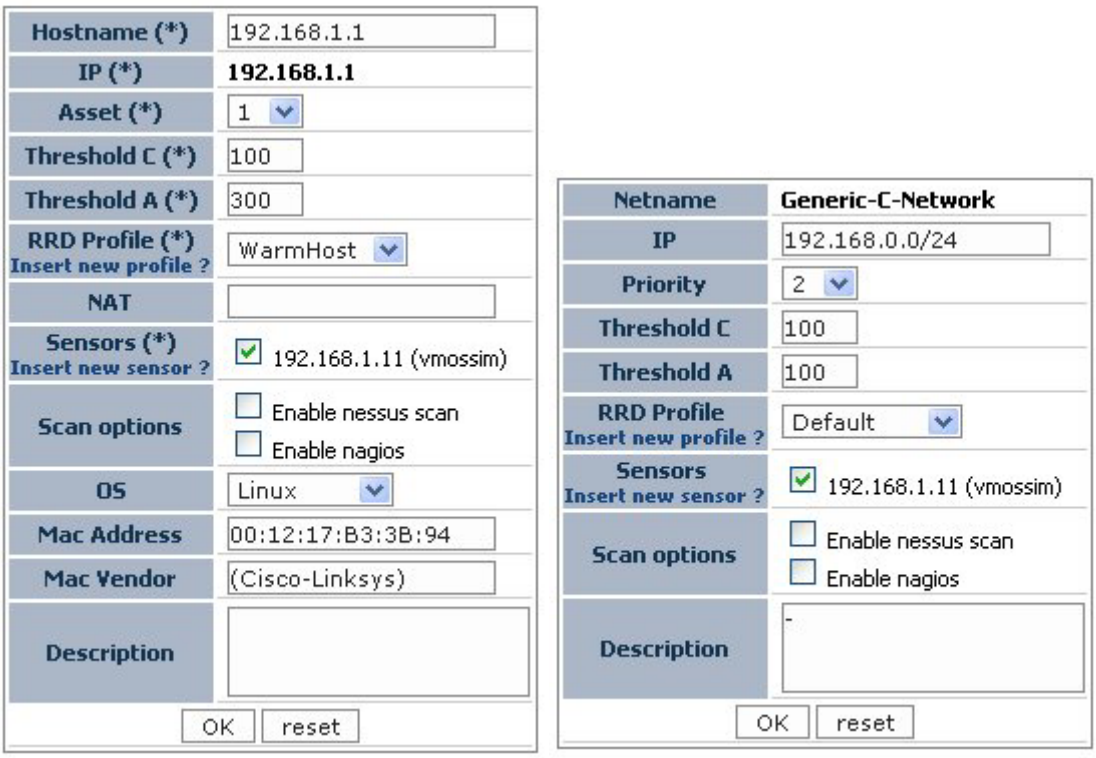
En entrée, il récupère un volume élevé d'événements, et en sortie il fournit un indicateur unique de l'état général de la sécurité.

Cette accumulation est valable pour n'importe quel objet sur le réseau (n'importe quelle machine, groupe de machines, segment de réseau, etc.) que l'on souhaite surveiller.

Accumulation d'événements (Event Accumulation)

L'accumulation est calculée simplement par la somme de deux variables d'état qui représentent le risque immédiat de chaque événement :

- « C » ou le niveau de la compromission, qui mesure la probabilité qu'une machine est compromise
- « A » ou le niveau de l'attaque à laquelle un système est soumis, qui mesure le risque potentiel dû aux attaques lancées



Exemple de configuration des seuils C et A pour un host ou un réseau

Ces deux variables ont été séparées pour la surveillance parce qu'elles caractérisent deux situations :

Le niveau de l'attaque indique la probabilité qu'une attaque ai été lancée, une attaque qui peut ou peut ne pas être réussie ; tandis que le niveau du compromission fournit l'évidence directe qu'il y ai eu une attaque et qu'elle ai réussie.

De plus, l'importance des deux variables dépend de la situation des machines.

Par exemple, en raison de l'exposition de réseaux en DMZ[13], qui peuvent être exposés à un énorme nombre d'attaques, la plupart d'entre elles automatisées, une valeur A (niveau d'attaque) sera considérée comme une situation « normale ».
Par contre, n'importe quel signe de compromission ou d'utilisation qui pourrait nous mener à penser qu'un attaquant ai pénétré le réseau devrait être immédiatement remonté et traité.

D'une autre manière, il y a des cas dans lesquels une machine produit des anomalies dans le réseau dû à la nature de sa fonction (telles que les scanners de sécurité, un service avec des ports passifs aléatoires, développement, etc.) et ceux-ci auront normalement une valeur élevée de C et une valeur de A plus basse.

[13] DMZ : Zone démilitarisée ou zone sacrifiable.

En fait, la valeur assignée à la variable C ou A pour une machine sur le réseau se fera selon trois règles :

- N'importe quelle attaque possible lancée de la machine 1 sur la machine 2 augmentera le A (niveau des attaques éprouvées) de la machine 2 et le C (niveau de compromission, ou des actions suspectes normalement commises par un hacker) de la machine 1.
- Quand il y a une réponse d'attaque (une réponse qui pourrait indiquer le succès de l'attaque), la valeur de C augmentera pour les deux machines 1 et 2.
- Si les événements sont internes, la valeur de C montera seulement pour la machine de commencement.

CALM est donc prévu pour la surveillance en temps réel, de ce fait l'algorithme doit accorder de l'importance aux événements les plus récents et jeter les plus vieux.
Pour ce faire, l'implémentation actuelle utilise une variable unique pour le rétablissement dans le temps.
Le système abaissera en fait périodiquement les niveaux de C et de A pour chaque machine par une valeur constante.

b) Méthode 2 : Corrélation en utilisant des séquences d'événements

L'idée de base pour la détection d'une séquence par modèle est simple. Il suffit juste de créer une liste de règles de façon a établir un scénario tel que :
« Si réception de l'événement A et puis B et puis C, alors effectuer l'action D. »

Rules (Directive 14)										
	Name	Priority	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Plugin ID	Plugin SID
-	Rare dest connection		1		1	ANY	ANY	!20,139	ANY	spp_anomsensor (1104)	ANY
-	Too many rare connections (15) against same ip		3	300	15	1:SRC_IP	1:DST_IP	1:SRC_PORT	ANY	spp_anomsensor (1104)	ANY
-	Too many rare connections (300) against same ip		5	1200	300	1:SRC_IP	1:DST_IP	1:SRC_PORT	ANY	spp_anomsensor (1104)	ANY
-	Too many rare connections (2000) against same ip		10	1800	2000	1:SRC_IP	1:DST_IP	1:SRC_PORT	ANY	spp_anomsensor (1104)	ANY
	Too many rare connections (20000) against same ip		10	43200	20000	1:SRC_IP	1:DST_IP	1:SRC_PORT	ANY	spp_anomsensor (1104)	ANY

Exemple de directive OSSIM

C'est dans cette optique qu'il est nécessaire de définir des listes de règles pour chaque séquence d'événements que nous voulons surveiller.

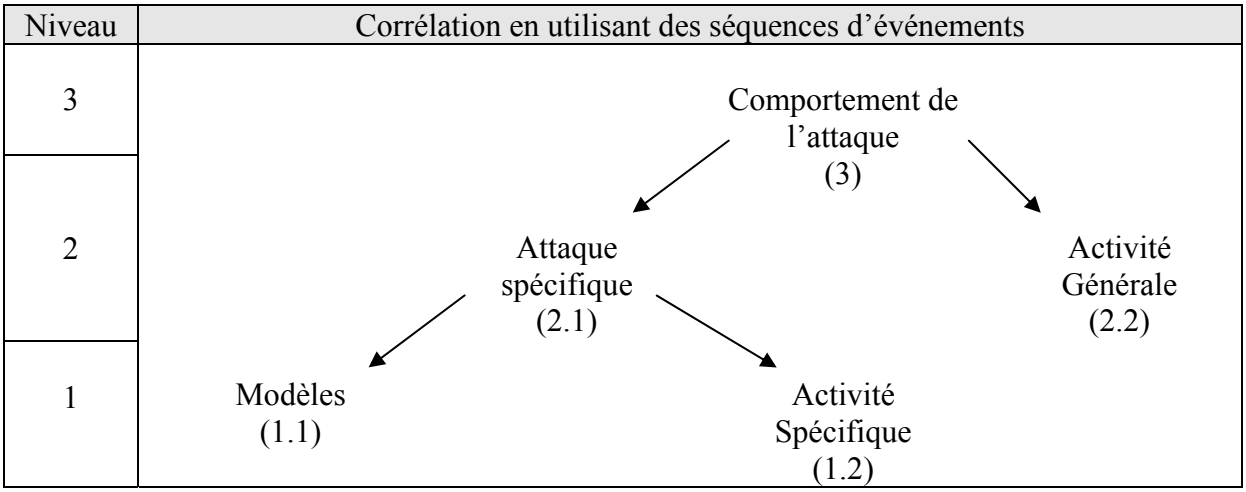
A cet effet, OSSIM intègre un éditeur de règles pour ajouter ou affiner de nouvelles séquences d'événements.

Cet outil permet notamment d'exécuter des séquences avec les caractéristiques suivantes :

- La capacité de définir des origines et des destinations variables
- Accepte en entrée à la fois les modèles des détecteurs et les indicateurs des moniteurs
- Définit la priorité et la fiabilité de nouvelles alertes
- Utilise des variables « élastiques », ou variables qui peuvent mesurer un événement pour définir la priorité ou la fiabilité (par exemple déni de service total - > priorité haute, déni de 50% - > priorité moyenne, déni de 15% - > priorité basse)
- Architecture récursive. Il est possible de créer des objets par des règles de corrélation qui fonctionnent ensuite comme des détecteurs ou des moniteurs pour de nouvelles règles

Les niveaux de corrélation

La nature récursive du modèle permet la création d'une hiérarchie presque infinie des niveaux de corrélation, mais pour bien comprendre le processus dans un exemple simple j'ai détaillé une hiérarchie sur trois niveaux suivant les indications du diagramme ci-dessous :



Chacun de ces trois niveaux est expliqué plus en détail ci-après, mais dans un souci de clarté les niveaux seront traités dans le désordre.

- ✓ Niveau 2.1 : Attaque spécifique

Ce niveau dépend directement des détecteurs et des moniteurs. Le but est d'inclure à la fois les signatures et l'activité liées aux attaques concrètes, par exemple les attaques avec un nom connu, comme identifié par le détecteur (exemple : «compromised by ftp cwd overflow»).

L'objectif principal du niveau d'attaque spécifique est d'améliorer la fiabilité de détection. Ceci signifie qu'au lieu d'être satisfait d'une signature d'attaque possible, nous recherchons plus d'évidence démontrant que l'attaque est en cours ou a échoué.

Cette évaluation permet de faire la différence en limitant les « faux positifs » et en donnant la priorité à de vraies attaques dans le système de détection. Cette évaluation est importante car comme cela a été évoqué dans la partie « évaluation du risque », la fiabilité d'un événement affecte directement le calcul du risque.

Rappel

c) Faux positifs

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

d) Faux Négatifs

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

Pour bien comprendre, prenons un exemple simple de corrélation entre un détecteur de modèle (pattern detector) et un moniteur :

En utilisant une signature IDS, on détecte une possible attaque par déni de service par synflood. On envoie alors une alerte déclenchant une requête au moniteur de service pour voir s'il a constaté une chute en terme de disponibilité et si oui à quel degré.
En fonction du retour, on peut donc assigner à notre alerte « denial of service via synflood » un degré plus élevé de fiabilité.

OSSIM utilise évidemment des séquences plus complexes dans lesquelles sont corrélées les alertes produites par des signatures avec le comportement caractéristique d'une attaque spécifique.
Si l'on prend l'exemple de la détection d'un cheval de Troie (Trojan Horse). L'utilisation de signatures IDS permet de détecter différentes opérations :

- *Connect, active*
- *get info*
- *access*
- *server2client_flow*
- *client2server_flow*
- *response*
- *traffic_detect*

La détection d'une tentative de connexion n'est en soit pas une information très utile toute seule.
Il y en a en effet des douzaines chaque jours dans les environnements DMZ, mais si l'on détecte par contre n'importe quelle autre opération (notamment une réponse à une attaque), il devient alors nécessaire d'envoyer une alerte à priorité élevée.

- ✓ Niveau 1.2 : Détection en utilisant une activité spécifique

Pour expliquer le concept de l'activité spécifique, je reprendrai ici l'exemple de Trojan.
Après une tentative de connexion, si le Trojan utilise le port P, il suffit d'examiner ce port pour contrôler l'activité spécifique du Trojan, c'est-à-dire la transmission de données.
Si l'on détecte une activité, cela confirme donc que la tentative de connexion a probablement réussie. La différence, c'est que cette fois l'identification s'est faite en surveillant l'activité du Trojan elle-même au lieu d'employer une signature IDS.

- ✓ Niveau 1.1 : Détection en utilisant des modèles (pattern)

La détection par modèles ayant déjà été expliquée dans la présentation du « Level 1 » des fonctionnalités d'OSSIM (§5 de ce document), je ne développerai pas ici.

Cependant, il semble intéressant de compléter ces explications avec la notion de « réponses aux attaques ».

En se basant sur les deux points précédents, on s'aperçoit que les réponses aux attaques sont importantes parce qu'elles permettent de vérifier l'existence d'un événement, ce qui équivaut directement à une augmentation de la fiabilité de l'alerte.

Le moteur de corrélation d'OSSIM est donc conçu pour rechercher de manière permanente ces réponses aux attaques, et les signes d'attaques éventuelles. Le but étant de trouver la confirmation que l'attaque est vraiment en cours. Cela permet notamment de différencier les attaques échouées des attaques réussies.

Si l'on reprend encore l'exemple du Trojan, le principe est le suivant :

On distingue deux étapes dans l'événement.

Etape 1 : Compromission par le Trojan ou tentative de connexion.

L'événement est détecté et une alerte est remontée, caractérisée par :

- La signature.
  Connection, client2server, access, getinfo

- L'activité spécifique
  Flux détecté entre l'attaquant et la victime.

La fiabilité associée à cette alerte sera donc faible.

Etape 2 : Détection d'une réponse typique à une attaque aboutie ou d'une réponse aux actions du Trojan.

L'alerte sera cette fois caractérisée par :

- La signature.
  server2client

- L'activité spécifique
  Flux détecté entre la victime et l'attaquant.

De par ces nouvelles informations, l'alerte sera cette fois qualifiée comme élevée.

On peut résumer ce fonctionnement dans le tableau suivant :

<table>
<tr><th>Succession des événements</th><th>Type d'alerte</th><th>Fiabilité</th></tr>
<tr><td rowspan="2">Compromission par le Tojan ou tentative de connexion</td><td>Signature : connection client2server, access, getinfo</td><td rowspan="2">Faible</td></tr>
<tr><td>Activité spécifique :
Flux attaquant → victime</td></tr>
<tr><td rowspan="2">Détection d'une réponse typique à une attaque aboutie ou d'une réponses aux actions du Trojan</td><td>Signature : response, server2client</td><td rowspan="2">Elevée</td></tr>
<tr><td>Activité spécifique :
Flux victime → attaquant</td></tr>
</table>

- ✓ Niveau 2.2 : Détection en utilisant l'activité général

Par détection utilisant l'activité générale il faut comprendre l'utilisation de règles visant à détecter des attaques inconnues ou indétectables, car les signatures ou les modèles qui les caractérisent ne sont pas disponibles.

Ces attaques peuvent être identifiée grâce à l'activité anormale produite par l'attaquant. Cette activité est détectée en surveillant les indicateurs d'activité générale d'un utilisateur (tels que des ports ou des services, le trafic, les horaires, etc.) pour tous les utilisateurs.

Parfois il est possible de caractériser des attaques avec un bon niveau de détails en utilisant cette technique. Mais le plus souvent, la détection de ces comportements suspects est moins précise que dans le cas d'une détection d'attaque spécifique

Voici quelques exemples de détection possibles en surveillant l'activité générale :

- Détection d'un ver inconnu qui produit du trafic anormal et un certain nombre de connexions atypiques sur des ports et des destinations normalement inutilisés.
- Détection d'un accès suspect, tel qu'un utilisateur établissant une connexion persistante sur un port d'administration pour la première fois
- Trafic excessif, avec des destinations et des utilisations anormales.

- ✓ Niveau 3 : Comportement de l'attaque

Le troisième niveau est justement la corrélation de diverses attaques spécifiques ou d'activités générales identifiées aux niveaux précédents.

Rappel :
L'architecture de la corrélation dans OSSIM est récursive, et les règles peuvent inclure les nouveaux objets qui fonctionnent cette fois comme des détecteurs (qui envoient les alertes) ou comme des moniteurs (qui fournissent les valeurs) et qui sont compris dans un ensemble de règles du niveau précédent.

Cependant, il ne faut pas uniquement définir ce niveau par le fait que les objets des précédents niveaux agissent comme point d'entrée car ce n'est pas toujours le cas ! OSSIM peut en fait mélanger ou associer les méthodes en fonction des besoins.

Chaque niveau correspond en réalité à un certain degré d'abstraction, et donc ce niveau doit permettre l'identification des modèles de comportement, sensés aider à identifier l'objet, le chemin pris, le comportement et la méthode de l'attaquant.
Le comportement d'attaque se définit donc comme les séquences de l'attaque ainsi que l'activité générée par un utilisateur sur une ou plusieurs machines compromises.

Voici quelques exemples de comportements d'attaques :

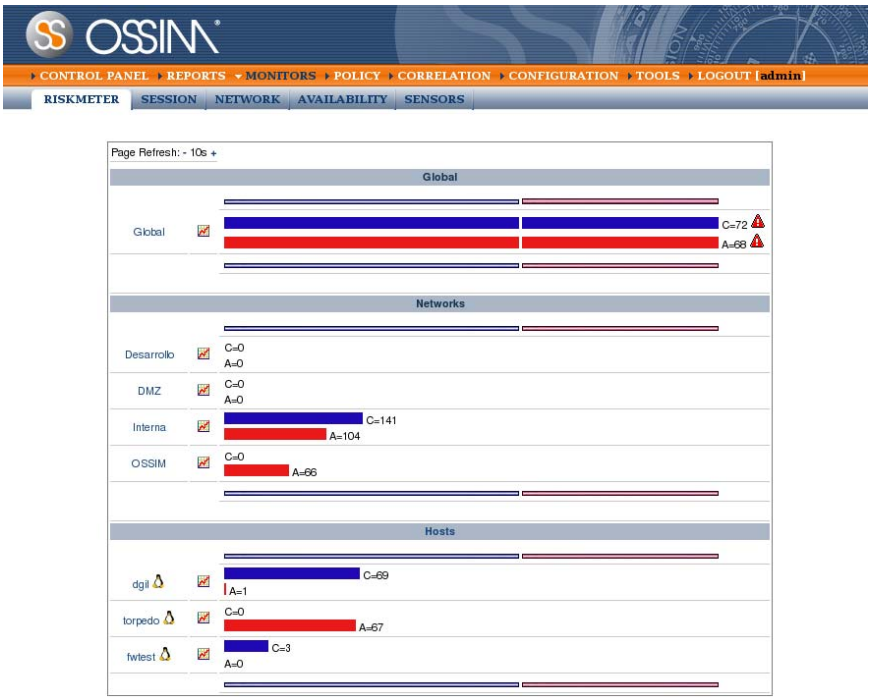
- Les attaques distribuées, caractérisées par la relation entre les différents attaquants et attaques éprouvées.
- Accès à un réseau critique depuis l'Internet par rebonds en utilisant les flux provenant d'une DMZ
- Compromission interne d'un utilisateur malveillant, identifié par les diverses activités anormales détectées pour cet utilisateur.

7) Console / Moniteurs – Level 7

Ces consoles ne sont pas à proprement parlé des fonctionnalités puisque ce sont en fait de simples représentations des processus précédemment expliqués, 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 montre les valeurs 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 ai été compromise.

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

Comme expliqué dans la section sur « la détection d'anomalies » (§5-2 de ce document), 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.

c) Moniteur de chemin (Path monitor)

Ce moniteur peut tracer en temps réel les chemins utilisés par les différentes machines sur le réseau au niveau des communications ou des liens.
Ce diagramme est régénéré à un certain intervalle de temps, créant un graphique dont les branches apparaissent et disparaissent dans le temps.

Ce moniteur reçoit des données de deux autres moniteurs :

- Le moniteur de session qui identifie tous les liens en cours sur le réseau
- Le moniteur de risque qui envoie le niveau de risque de toutes les machines

Deux modes d'utilisation sont disponibles :

Hard Link Analysis (TCP Link Analysis)

En utilisant cette méthode le graphique représente seulement les connexions persistantes de type TCP.
Le but de cette méthode est d'identifier les attaques réseaux impliquant l'intrusion simultanée de différentes machines.

Soft Link Analysis

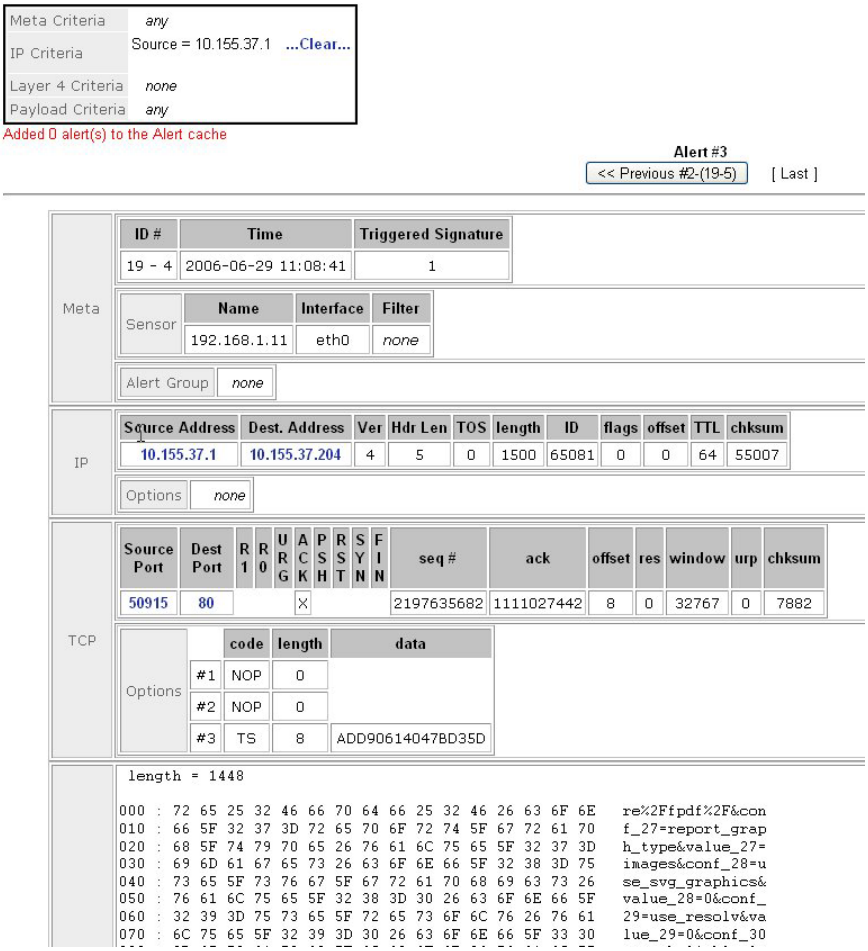
OSSIM utilise le « soft link analysis » pour représenter graphiquement tous les liens perçus sur le réseau. UDP mais aussi TCP ou encore ICMP.
Il en résulte souvent une représentation chaotique de la cartographie du réseau.

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

La console d'investigation permet d'accéder à toute 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.

À 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



Exemple de remontée d'événement
Affichage détaillé disponible dans la console d'investigation

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 quel 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

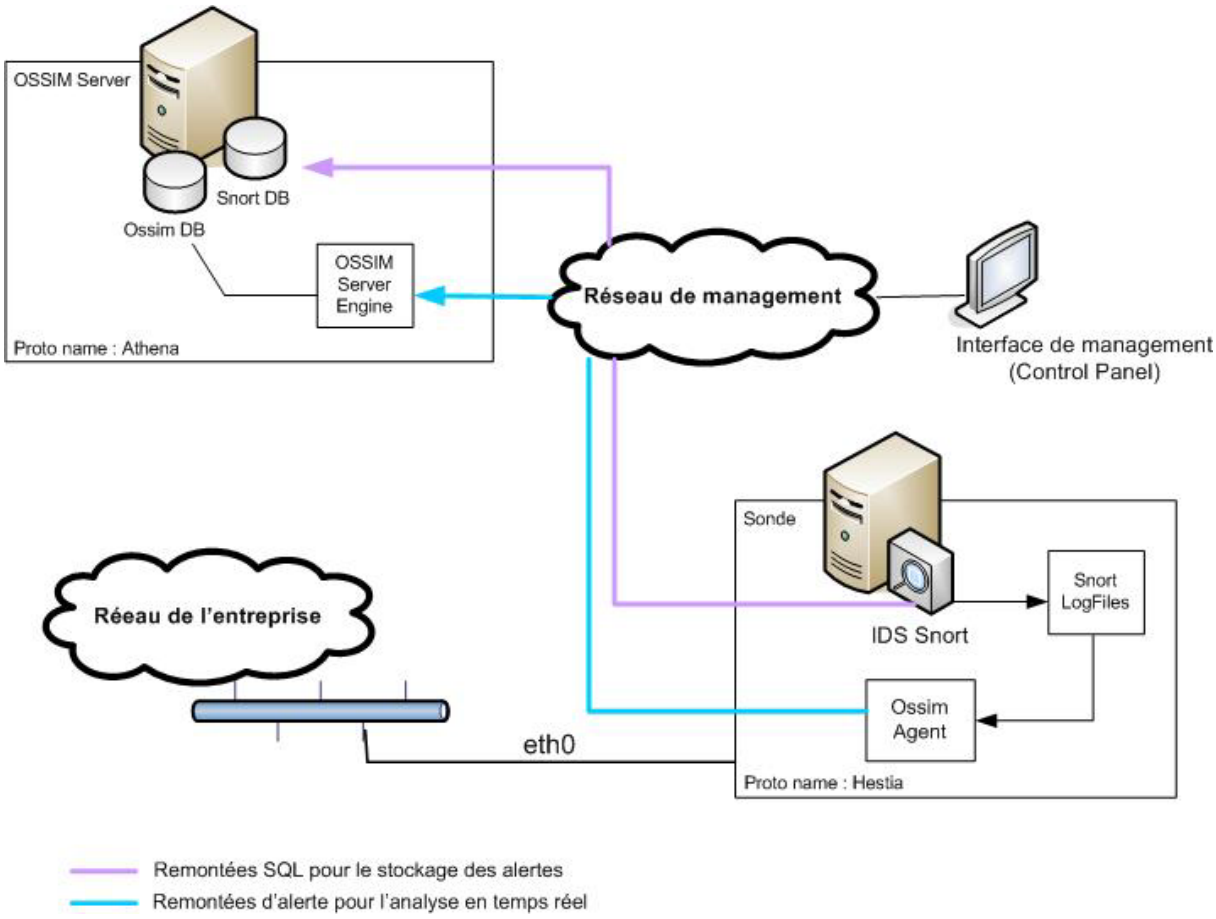
Remarque :
Le panneau de contrôle est totalement adaptable aux besoins du client.
À la différence de toutes les autres fonctions, il inclura seulement un échantillon personnalisé en fonction des besoins.

B. Le prototype

Le prototype a été réalisé en complément de l'étude préalable de la solution. C'est en fonction des résultats obtenus sur le prototype en regard de l'étude préalable que j'ai pu rédiger ce document.

Les fonctionnalités ayant déjà été traités et illustrées précédemment, je vais surtout dans cette partie expliquer le contexte technique du prototype. L'architecture choisie et réalisé, en expliquant mes choix.

1. Architecture cible



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.

Mon choix s'est donc porté sur une architecture basée sur un NIDS Snort.

Snort est un système de détection d'intrusion réseau, capable d'effectuer l'analyse du trafic en temps réel et de la journalisation de paquets sur des réseaux IP
Il peut effectuer de l'analyse de protocoles, de la recherche / correspondance de contenu et peut être utilisé pour détecter une variété d'attaques et de scans, tels que des débordements de tampons, des scans de ports furtifs, des attaques CGI, des scans SMB, des tentatives d'identification d'OS, et bien plus.

Snort utilise un langage de règles flexible pour décrire le trafic qu'il devrait collecter ou laisser passer, ainsi qu'un moteur de détection qui utilise une architecture modulaire de plugins.
Snort possède aussi des capacités modulaires d'alertes temps réel, incorporant des plugins d'alerte et de journalisation pour syslog, des fichiers textes en ASCII, des sockets UNIX, des messages WinPopup à des clients Windows en utilisant smbclient de Samba et des base de données.

Snort est assez complet en terme de détection d'intrusion réseau et largement reconnu par les professionnels de la sécurité informatique.
Son architecture axée autour de sa propre base de donnée m'a semblée intéressante à mettre en œuvre au sein de la solution OSSIM.

a) 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 exprimé par la société Kyos d'avoir un prototype à présenter à ses clients lors de la présentation de son offre de service.

Le prototype a été divisé en deux machines virtuelles

- Athena
  Qui correspond à la partie « server » de la solution et qui héberge le cœur d'OSSIM, son framework et les bases de données.

- Hestia
  Qui correspond à la partie « agent » de la solution et qui héberge donc la sonde Snort et tous les mécanismes de collecte d'OSSIM.

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 quelque soit son OS.

b) Environnement applicatif

Le choix de l'OS pour le prototype a été édicté par les contraintes suivantes
Le choix s'est porté sur une installation basée sur Linux Debian 3.2 Etch/Testing pour trois raisons.

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

Après plusieurs tentatives d'installation depuis les sources (ossim 0.9.8), 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

Au moment des tests, il semblerait que les packages OSSIM (0.9.8) disponibles pour Debian (dans sa version Etch/Testing) étaient les plus à jour et largement utilisés.

- Facilité d'installation et de configuration

L'avantage notable du système Debian est l'utilisation des commandes « *apt et dpkg»* pour l'installation et la configuration des packages.

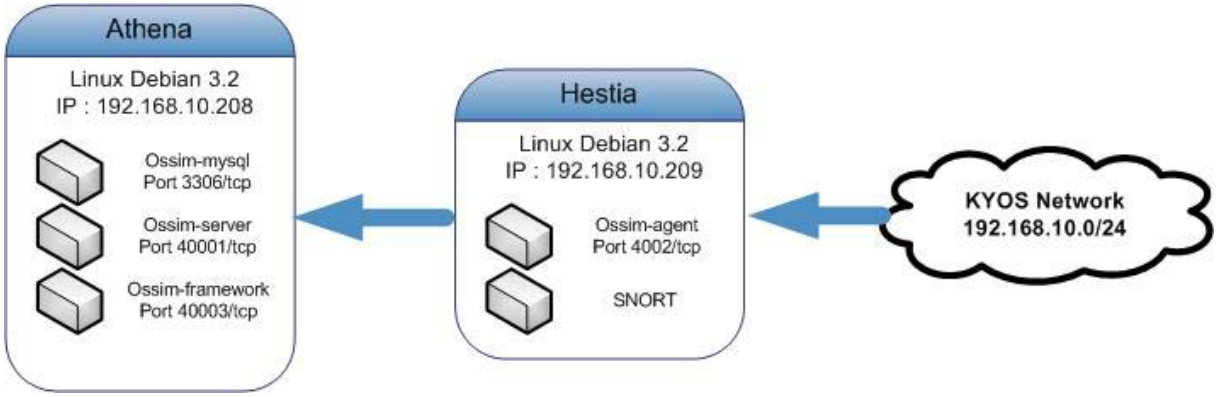
OSSIM a été parfaitement porté sous Debian et propose des packages spécifiques à chacune de ses briques. On trouve ainsi les packages :

- *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 composant de l'agent OSSIM

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

Les packages se chargent d'installer la solution OSSIM dans son ensemble en installant les versions nécessaires des applicatifs tiers tel que mysql (en version 4) pour la base de donnée, php (en version 4) pour l'interface HTTP, ou encore apache pour le moteur web …

Remarque
Pour le serveur web apache, j'ai choisi d'utiliser la version 2, plutôt que la 1.3, pour son architecture et ses fonctionnalités. Par contre pour faciliter les choses je n'ai pas pris en charge l'HTTPS.



2. Procédure d'installation du prototype

Configuration du fichier sources.list pour définir le dépôt officiel OSSIM pour une installation via APT.

```
[ -- /etc/apt/sources.list -- ]
deb http://ftp.debian.org/debian/ testing main
deb http://secure-testing.debian.net/debian-secure-testing testing/security-updates main
deb http://www.ossim.net/download/ debian/
```

- Installation des bases de données

Il faut au préalable créer la base de donnée. 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 donnée 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 conseiller 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 est accessible depuis un navigateur Internet à l'adresse
http://athena/ossim/

Remarques:

- *Dans le cas d'une installation avec apache2, il installer obligatoirement le package libapach2_mod_php4 pour la prise en charge de php par apache2. Dans le cas contraire, les scripts php ne seront pas interprétés et le framework d'OSSIM inutilisable.*

- *Lors de l'installation du framework OSSIM, j'ai rencontré l'erreur suivante.*

```
dpkg: error processing ossim-framework (--configure)
subprocess post-installation script returned error exit status 1
…
```

Le problème est lié au package ossim-framework-daemon.deb, package qui a été corrigé mais qui n'a pas encore été mis à jour dans sa dernière version lors de l'installation par apt-get du package ossim-framework

Pour contourner ce problème, il faut exécuter le code suivant

```
# Start Script
#!/bin/sh
apt-get install -u ossim-framework
mkdir -p /tmp/ossim_daemon
cd /tmp
wget http://www.ossim.net/download/debian/ossim-framework-daemon_0.9.8-13_i386.deb
dpkg -x ossim-framework-daemon_0.9.8-13_i386.deb ossim_daemon/
cp /tmp/ossim_daemon/etc/default/ossim-framework /etc/default/ -rf
cp /tmp/ossim_daemon/etc/init.d/ossim-framework /etc/init.d/ -rf
cp /tmp/ossim_daemon/usr/bin/ossim-framework /usr/bin/ -rf
cp /tmp/ossim_daemon/usr/share/ossim-framework/ /usr/share/ -rf

# Reinstall OSSIM Framework
apt-get install -u ossim-framework
# End Script
```

- Installation de la partie « Agent »

Il faut au préalable installer Snort.

```
# apt-get install snort-mysql
```

Ici, il ne faut pas configurer les paramètres de base de donnée Snort via l'utilitaire debconf car on veut utiliser Snort avec OSSIM. La configuration se fera donc manuellement après l'installation dans le fichier */etc/snort/snort.conf*

```
…
var HOME_NET [192.168.1.0/24]
var EXTERNAL_NET !$HOME_NET
..
# splitted in two lines for readability
output database: alert, mysql, user=root password=yourdbpass dbname=snort
host=yourdbhost sensor_name=your_sensor_ip logfile=alert
..
#  if you want spade support obtain a valid spade.conf file
#  (for example from ossim source or from ossim-contrib package)
include spade.conf
…
```

On récupère les dernières règles pour Snort et on les charge dans la base OSSIM.

```
# cd /etc/snort/rules/
# wget http://www.bleedingsnort.com/bleeding-all.rules
# echo "include \$RULE_PATH/bleeding-all.rules" >> /etc/snort/snort.conf
# /usr/share/ossim/scripts/create_sidmap.pl /etc/snort/rules | \
    mysql -u root ossim -p
```

Ensuite on installe la partie « Agent »

```
# apt-get install ossim-agent
```

Le fichier de configuration d'OSSIM agent se trouve dans */etc/ossim/agent/config.xml*

Remarque
Il est nécessaire de passer l'interface eth0 de la machine en mode « promiscuous » pour la collecte des informations. Pour VMWare il faut exécuter la ligne suivante

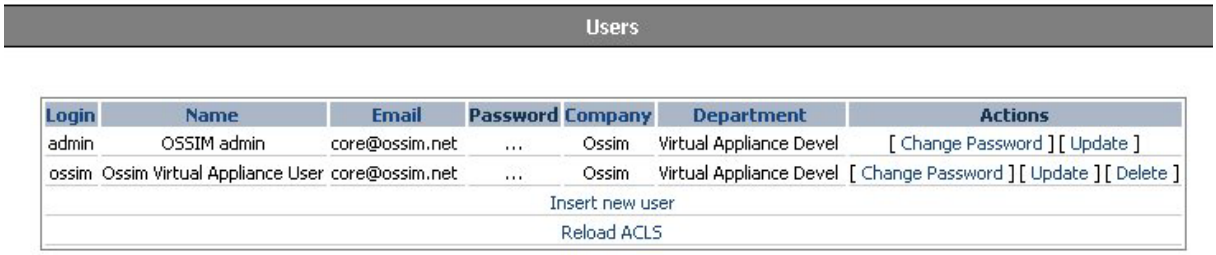
```
chmod a+rw /dev/vmnet0
```

3. Mode opératoire

A partir de là, on peut considérer le prototype comme installé.
Pour qu'il soit véritablement opérationnel, il reste à déclarer la sonde au sein de la solution et à configurer les différents outils et moniteurs.

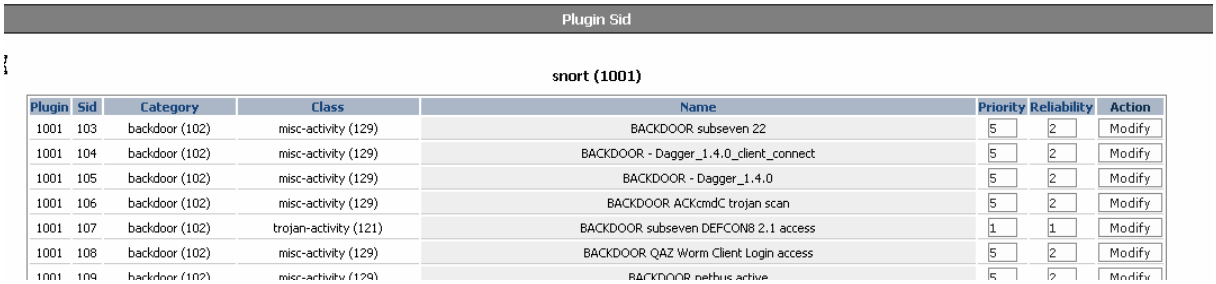
Dans la section « Configuration » il est possible d'agir sur les paramètres suivants :

- Vérifier la configuration générale d'OSSIM et de Snort (Chemins, comptes de connexion, etc)
- Gérer les ACL du framework OSSIM.



Remarque :
Par défaut le compte d'administration d'OSSIM est admin:admin
Pour des raisons de sécurité, il est conseillé de changer le mot de passe.

- Modifier les paramètres de fiabilité et de priorité des plugins installés



- Déclarer les profils pour les graphiques RRDtool des moniteurs

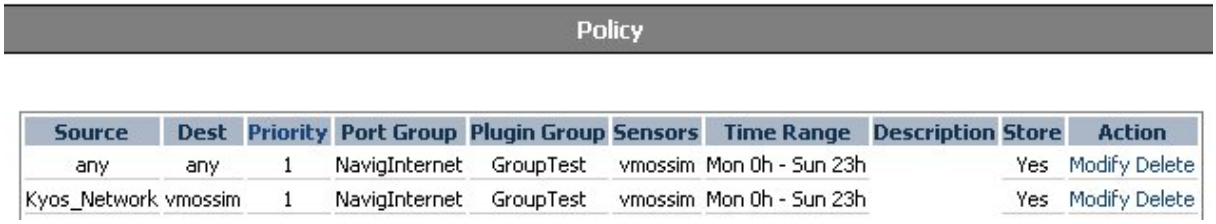
- Effectuer des scans de machines depuis différents outils (nessus, nmap, etc…), à condition que les outils soient préalablement installés sur le server OSSIM.

- Définir les actions qui seront tracées pour les utilisateurs du framework (exemple : connexion, déconnexion, suppression d'un utilisateur etc …)

- Définir le modèle HTML des mails remontés aux administrateurs sécurité.

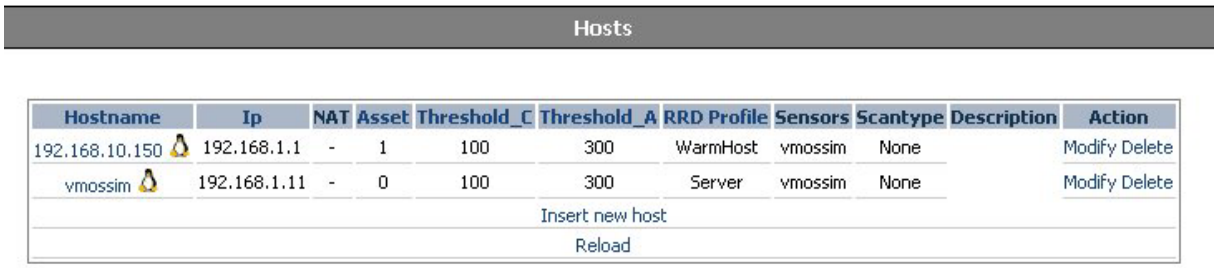
Dans la section « Policy » il est possible d'agir sur les paramètres suivants :

- Définir les politiques



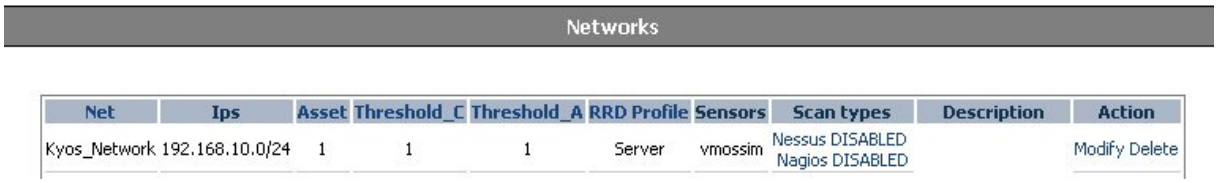
La politique est caractérisée par :
- La source (host ou réseau)
- La destination (host ou réseau)
- Les groupes de ports
- Sa priorité (1 à 5 avec 5 comme valeur la plus importante)
- Les groupes de plugins
- La sonde qui lui est associée

- Définir les hosts



La machine est caractérisée par :
- Son hostname
- Son adresse ip
- Sa priorité (1 à 5 avec 5 comme valeur la plus importante)
- Les seuils A et C pour l'évaluation des risques
- Le profil de graphique RRDTool
- La sonde qui lui est associée

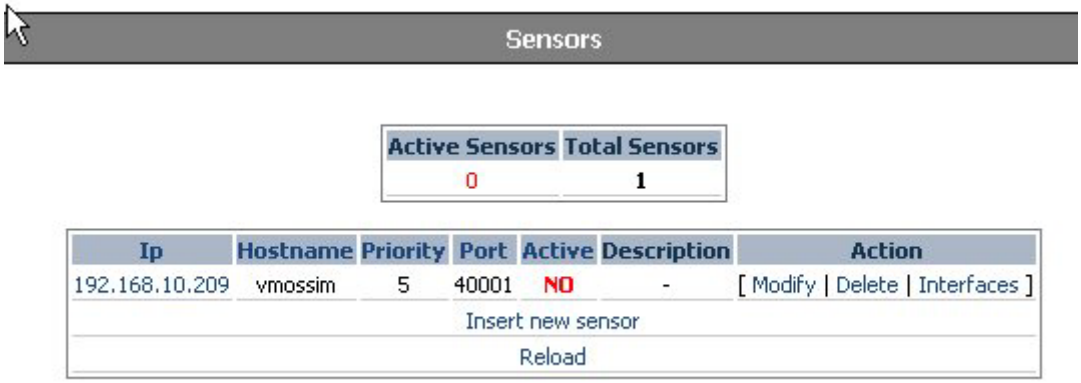
- Définir les réseaux et groupes de réseaux



La réseau est caractérisée par :

- Son nom
- L'adresse ip du reseau
- Sa priorité (1 à 5 avec 5 comme valeur la plus importante)
- Les seuils A et C pour l'évaluation des risques
- Le profil de graphique RRDTool
- La sonde qui lui est associée

- Définir les sondes



La sonde est caractérisée par :

- Son nom
- Son adresse ip
- Sa priorité (1 à 5 avec 5 comme valeur la plus importante)

- Définir les ports et groupes de ports (à gérer ensuite dans les politiques)

- Définir les actions à mener et les règles de réponses en fonction des alarmes.

- Définir les groupes de plugins (à gérer ensuite dans les politiques)

Pour commencer, le mode opératoire est le suivant.

- Déclarer la sonde.
- Déclarer les réseaux et groupes de réseaux
- Déclarer les ports et groupes de ports qui nous serons utiles dans les politiques.
- Ajustement des paramètres de fiabilité et de priorité des plugins installés
- Déclarer un host
- Déclarer ses politiques

C. Offre de service OSSIM

1. Introduction

L'objectif final de cette étude de R&D était d'établir un prototype fonctionnel basé sur la solution OSSIM et de bâtir, si la solution était intéressante pour la société, une nouvelle offre de service pour Kyos.

Avantages et inconvénients majeurs de la solution OSSIM

Avantages	Inconvénients
▪ Solution open-source avec une communauté active ▪ 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 open-source). La solution la plus proche est Prelude mais la solution est beaucoup moins modulaire qu'OSSIM. ▪ Fonction d'apprentissage qui permet à la solution d'accroître la fiabilité des ses remontées d'information. ▪ Interface intuitive grâce à la modularité du panneau de contrôle qui s'adapte aux besoins du client.	▪ Solution open-source. Pas de possibilité de souscrire un support auprès d'une société. Support communautaire uniquement. ▪ Solution complexe à mettre en œuvre. 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 part le grand nombre de paramètres pouvant rentrer en jeu

Compte tenu de ce tableau et après avoir étudié et testé les différentes fonctionnalités de cette solution il a donc été décidé, d'un commun accord avec la direction de la société, d'établir cette offre de service.

2. Le cadre de cette offre

Au vue des possibilité de la solution et compte tenu de la complexité de mise en œuvre, je considère que cette offre n'a de sens qu'au sein de la mise en œuvre d'une réelle politique de sécurité au sein du SI. C'est donc dans ce sens que j'ai essayé d'articuler cette offre.

a) Le contexte

« Gouverner c'est prévoir, prévoir c'est s'informer ! »
L'information est fondamentale que ce soit à l'intérieur mais aussi et surtout à l'extérieur de l'entreprise. L'information est cœur de la stratégie d'entreprise.

b) Les enjeux

Un des enjeux majeurs, aujourd'hui, pour les entreprises est donc de se prémunir de la fuite d'information, car ces dernières années le poids relatif à la malveillance a augmenté.
La malveillance est désormais aussi importante en externe qu'en interne (50/50). Elle a de nouvelles finalités mais surtout de nouvelles formes.

- Spamming
- Agressions virales
- Intrusions multiples
- Moteurs d'extraction de données
- Analyses comportementales indues…

Parallèlement, les contrôles du respect des réglementation s'est durcit.

- Protection des logiciels (piratage)
- Protection des données…
  - personnes physiques (CNIL)
  - stratégiques (intelligence économique)
- Respect des normes et réglementations (ISO 17799, BS 7799-1, etc ....)

c) Les risques

Le système d'information est pour l'entreprise un outil facteur de productivité et de rentabilité. Il est à la fois un outil de maîtrise des risque (DMR) mais intrinsèquement un facteur de risque de part sa complexité.
Pourtant le système d'information se doit de répondre aux certains impératifs (DICA), à savoir qu'il se doit de garantir :

- **D**isponibilité
- **I**ntégrité
- **C**onfidentialité
- **A**uditabilité (Tracabilité)

d) La démarche

Le risque informatique n'est pas une nouveauté mais il a évolué dans le temps.

Face à ces risques les entreprises sont dans une logique de protection.
C'est-à-dire qu'elles ont une approche technique sécuritaire, qu'elles s'orientent vers la sécurisation de l'outil informatique. Le tout dans une logique basée sur les moyens.

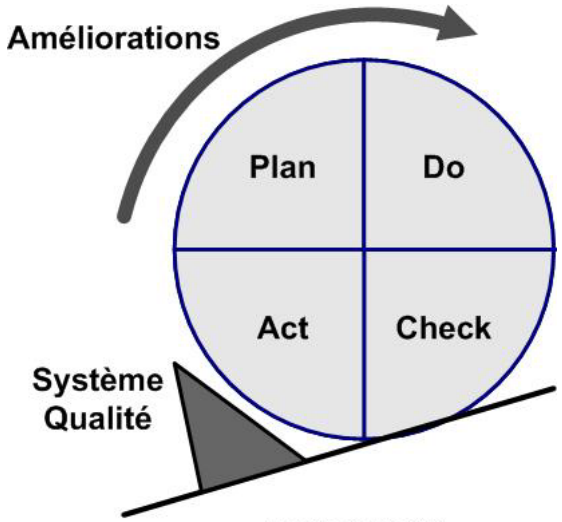
Tout ceci rend le suivi et la représentation difficilement abordables par les directions générales. Ces mêmes directions qui doivent prendre des orientations stratégiques pour l'entreprise.

L'orientation que devrait prendre ces entreprises serait plutôt d'aller vers une approche de la maîtrise des risques.
Il faut arriver à bien définir les risques et les enjeux.
Il ne faut pas décorréler la stratégie du système d'information de la stratégie d'entreprise.

e) La méthode

Cette démarche qui a pour objectif la maîtrise des risques peut être obtenue en adaptant la méthode qualité PDCA (Plan Do Check Act)

Si l'on reprend le principe de la *roue de Deming*. La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service...



-- La roue de Deming --

- **P**lan : ce que l'on va faire
- **D**o : production
- **C**heck : mesure, vérification
- **A**ct : décision amélioration, corrective

Plan, consistera à analyser les risques en regard des enjeux afin d'établir les axes précis de la politique de sécurité du système d'information de l'entreprise.
Do, consistera à mettre en œuvre un dispositif de maîtrise des risques.
Check, consistera à contrôler au moyen d'indicateurs pertinents le niveau de sécurité du système d'information et le niveau des risques résiduels.
Act, consistera à affiner le dispositif de maîtrise des risques en vue de réduire le de risques résiduels

f) OSSIM

La solution OSSIM est un parfait outil au niveau de l'administration du système d'information. C'est un outil de management de la sécurité de l'information (SIM) qui peut être considéré comme une approche proactive dont le but est d'assurer un bon niveau de sécurité, au bon moment, sur des informations pertinentes et pour un coût raisonnable.

Accessible aux différents niveaux d'interlocuteurs, la solution s'intègre parfaitement à une analyse de risque au niveau du système d'information et va permettre d'apporter les métriques nécessaires pour suivre l'évolution et éventuellement agir de manière proactive pour minimiser certains risques.

OSSIM est une solution centralisée qui s'appuie sur d'autres solutions de sécurité.
Articulée autour d'un framework, OSSIM permet de piloter ces produits afin de collecter tous les événements liés à la sécurité de manière centralisée et normalisée.
Les informations sont ensuite stockées dans une base de donnée des événements.

Par son framework, la solution OSSIM permet d'afficher les alertes en temps réel par le biais de consoles de supervision ou sur une fenêtre de temps donnée grâce à sa base de donnée des événements.

Basé sur l'algorithme de corrélation CALM, et sa méthode d'évaluation des risques, la solution OSSIM accroît la fiabilité des informations remontées. OSSIM est ainsi capable « d'apprendre » et d'affiner jusqu'à l'infini le niveau de pertinence de ces alertes.

En ce sens, la solution OSSIM fait partie intégrante des moyens à mettre en œuvre dans un dispositif de maîtrise des risques (DMR).

3. La présentation

Pour finaliser cette offre de service, j'ai également rédigé une présentation power-point comme support de présentation.
Ce support reprend en quelques slides[14] le cadre de l'offre de service définit dans le paragraphe précédent. Il permettra à la société Kyos de présenter dans le futur la solution OSSIM à ses clients.

Le contenu de la présentation est disponible en *Annexe 3*.

[14] Slides : Diapositives

Conclusion

L'étude réalisée dans le cadre de ce projet de R&D, au sein de la société Kyos, m'a permis de découvrir une solution de management de la sécurité de l'information.

OSSIM 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
  Qui regroupe les consoles d'administrations et les outils de configuration et de pilotage. Le framework assure également la gestion des droits d'accès.

Cette solution offre une grande modularité de part 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 corrélation (basé notamment sur l'algorithme CALM), 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 données grâce à ses bases de données (EDB et KDB).
Son panneau de contrôle complètement modulaire s'adapte très bien aux besoins spécifiques de chaque client. 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 n'a de sens (à mon avis) qu'inscrit 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.

OSSIM en tant que simple outil de surveillance n'a pas vraiment de sens. Si l'on ne sait pas exactement ce que l'on attend de la solution, sa mise en œuvre et sa configuration en fait un outil particulièrement complexe qui demandera un temps fou pour le paramétrage et l'apprentissage. Dans ce cas de figure, on retombe à mon sens dans les travers des solutions actuelles, à savoir que la remontée d'information est telle qu'il faut beaucoup d'énergie et de temps pour arriver à en extraire une information pertinente. (*« Trop d'information tue l'information »).*

.

Annexe 1 : Sources documentaires

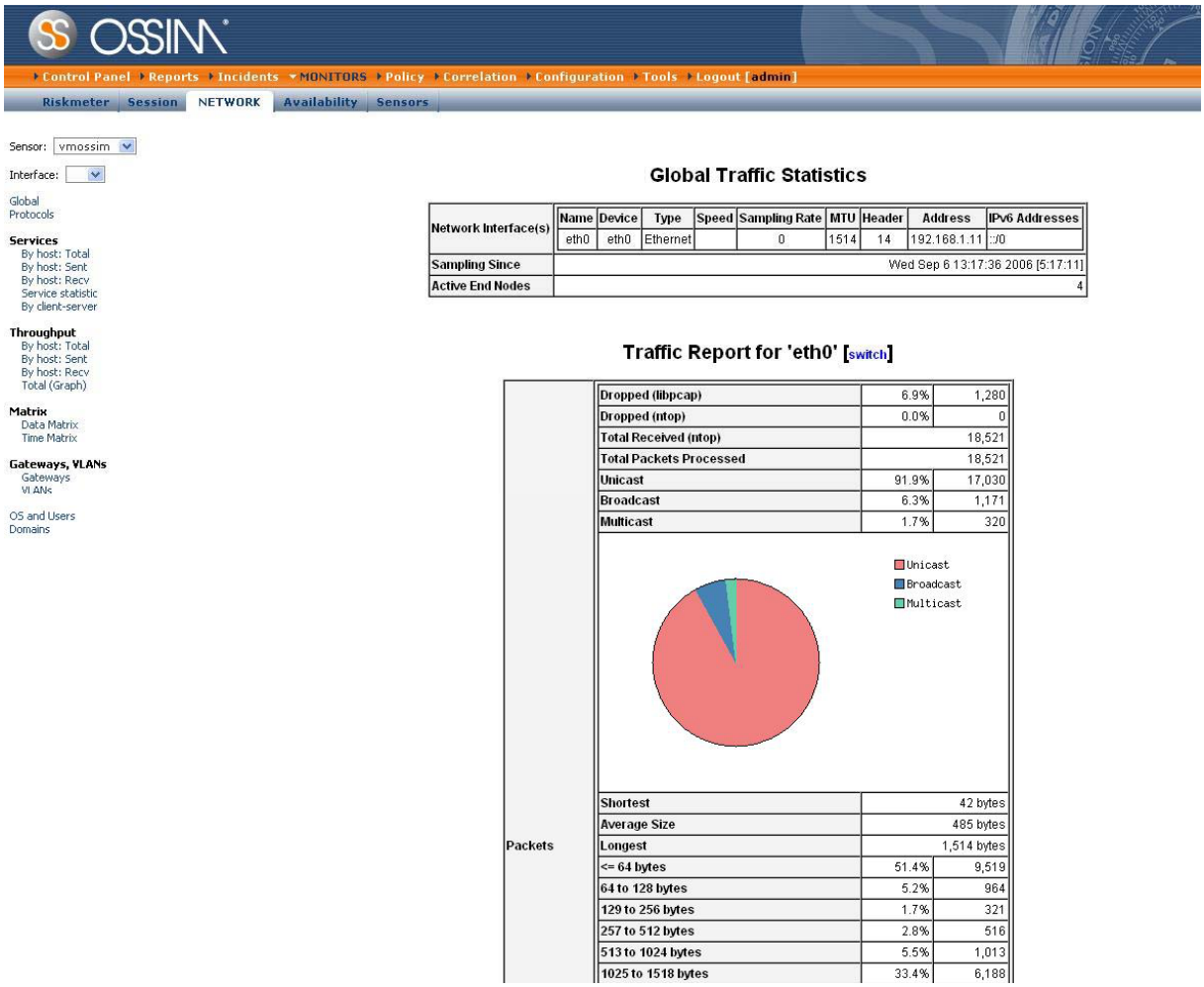
La principale source de documentation utilisée pour la rédaction de ce rapport a été Internet donc voici les principaux sites.

IDMEF : http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt
IETF : http://www.ietf.org/home.html
Clusif : https://www.clusif.asso.fr
OSSIM : http://www.ossim.net
ISO : http://www.iso.org/iso/fr/ISOOnline.frontpage
BSI : http://www.bsonline.bsi-global.com/server/index.jsp
VmWare : http://www.vmware.com/
Clusif / Clusis : https://www.clusif.asso.fr/index.asp et http://www.clusis.ch/
Debian : http://www.debian.org
Kyos : http://www.kyos.ch
Snort : http://www.snort.org
SSI : http://www.ssi.gouv.fr/fr/index.html

En plus des informations recueillies sur Internet, je me suis appuyé sur les cours OPSIE :

- *Analyse et Gestion des Risques (M. Caubère)*
- *Sécurité (M. Pierrot)*
- *Gestion de projet (M. Chettouh)*

Annexe 2 : Screenshots OSSIM



Moniteur résau (basé sur Ntop)

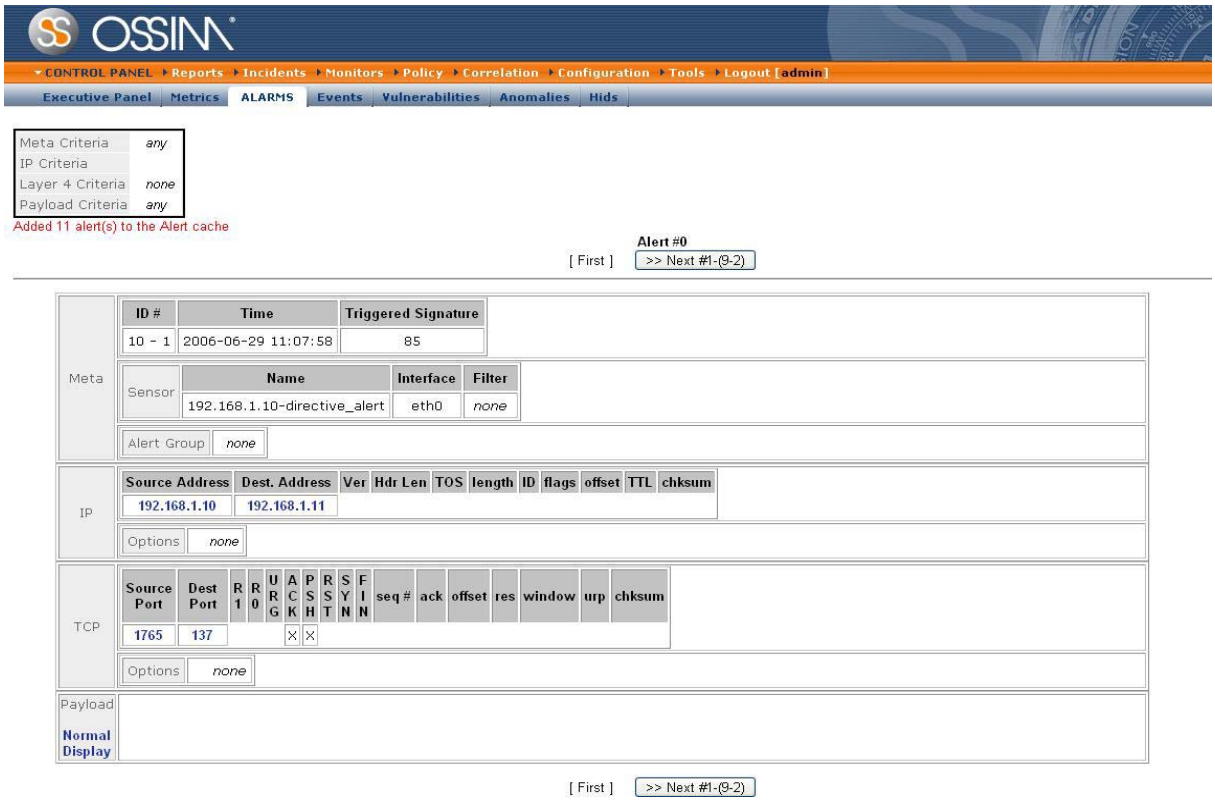


Fig 1

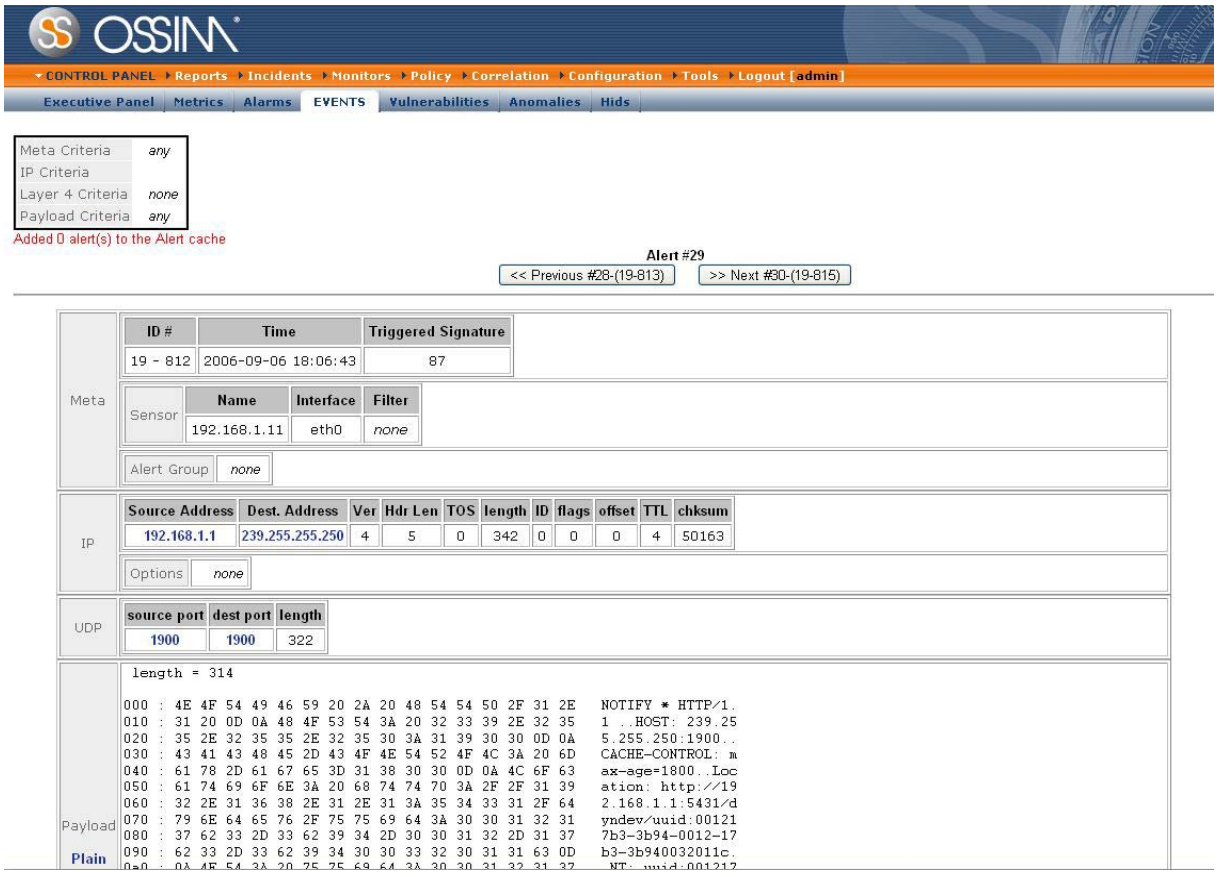
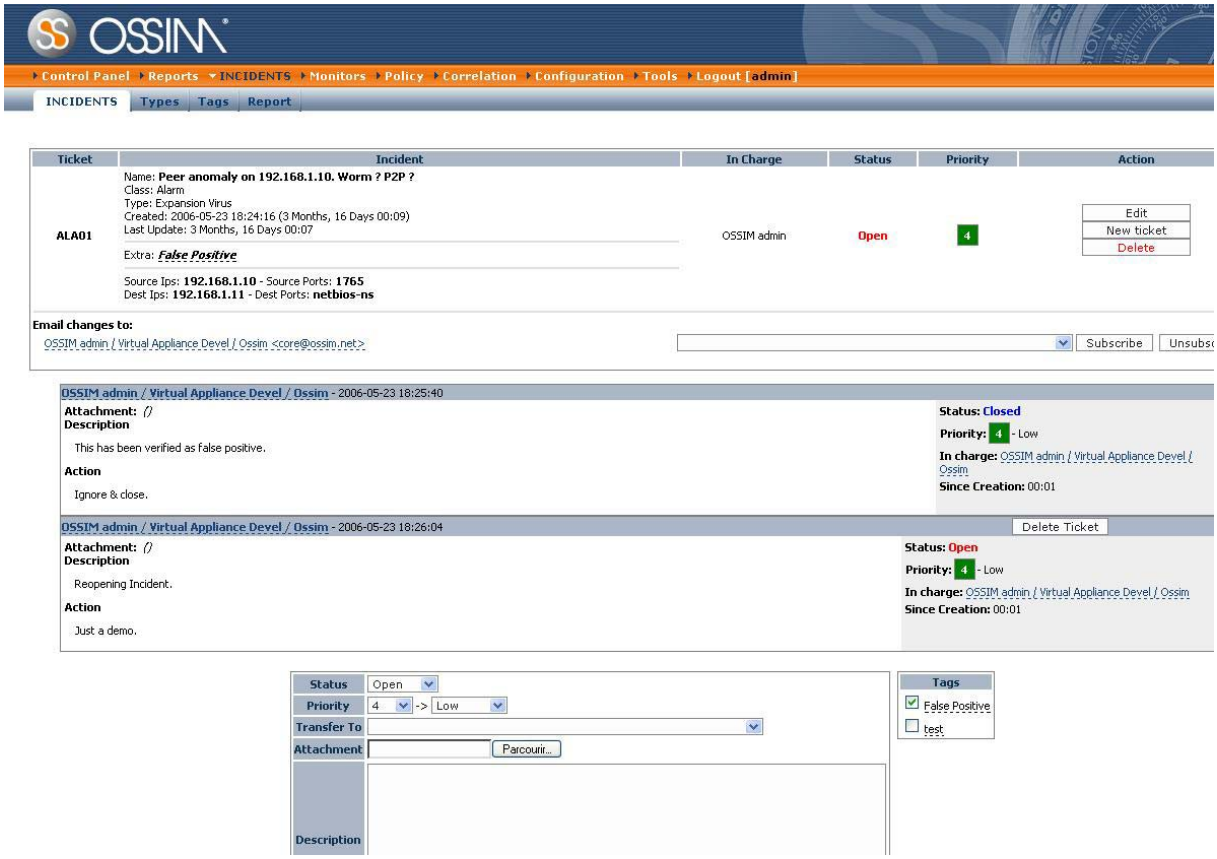
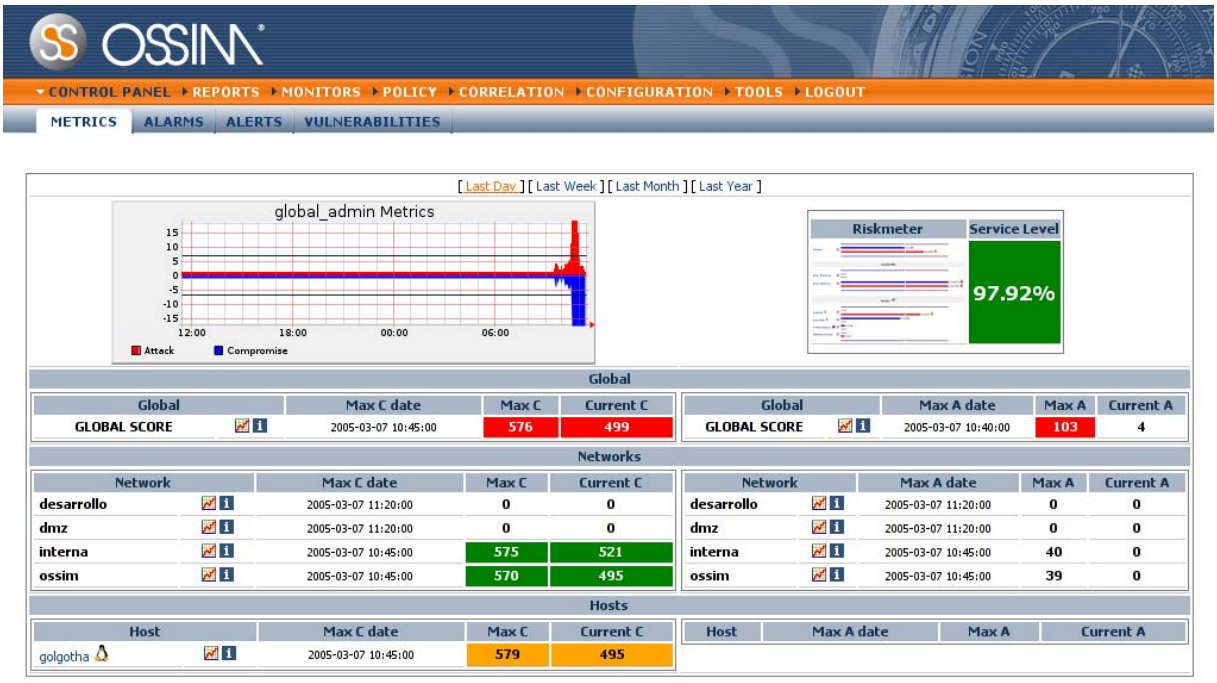


Fig 2

Détail d'une alarme dans la console d'investigation (fig 1 & 2)



Exemple d'un ticket d'incident



Exemple d'affichage

Annexe 3 : Présentation offre OSSIM

Sommaire

> OSSIM
- Présentation d'OSSIM
- Les fonctionnalités
- L'architecture

> OSSIM dans l'entreprise
- Les enjeux et les risques du SI
- Vers une solution globale de sécurisation

> L'offre de service KYOS OSSIM

Présentation OSSIM

> OSSIM c'est

- Un projet Open-Source de SIM
- Un framework qui fédèrent d'autres produits open-source
- Des agents qui collecte les informations des sondes
- Un serveur qui traite et stocke les alertes

> Le framework OSSIM

- Centralise
- Organise
- Améliore la détection
- Améliore l'affichage

Fonctionnalités (1)

> Détection

- Par modèles (type IDS)
- D'anomalies (p/r à un système de référence)
- Détections complémentaires

> Centralisation / Normalisation

- Collecte
- Consolidation
- Mise en forme (IDMEF)

Fonctionnalités (2)

> Gestion des priorités

- Priorisation des événements

> Evaluation des risques

- Pondération des alertes en fonction du risque
- Risque : Impact / Degré d'occurrence

> Corrélation

- C.A.L.M – Algorithme basé sur l'accumulation d'événements
- Améliore la détection / Requalifie les alertes pour détecter des comportements

Fonctionnalités (3)

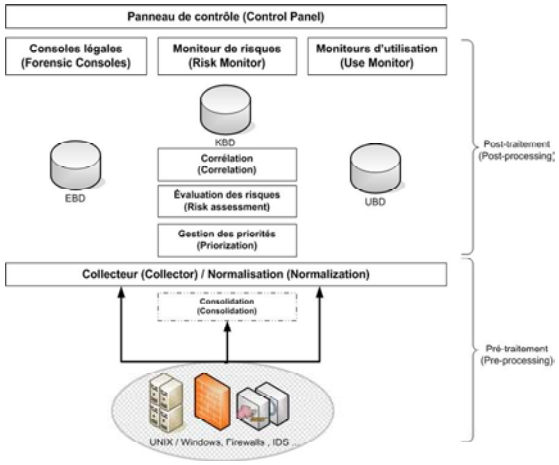
> Consoles / Moniteurs

- Remontées d'information Temps Réel
- Console d'investigation

> Panneau de contrôle

- Affichage personnalisé
- Accessible à différents niveaux d'interlocuteurs (techniques ou non)
- Accès gérés par ACL

Architecture interne d'OSSIM



Risques & enjeux (1)

> Les enjeux des entreprises

- Sécurisation du S.I (DICA)
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Auditabilité
- Protéger l'information

> Les causes de ces enjeux

- Augmentation du poids de la malveillance
- Obligation de respect des réglementations

Risques & enjeux (2)

> Les risques pour l'entreprise
- Perte d'image
- Pertes financières
- Impact Juridique

> Le S.I. est à la fois un DMR mais également un facteur de risque de part sa complexité

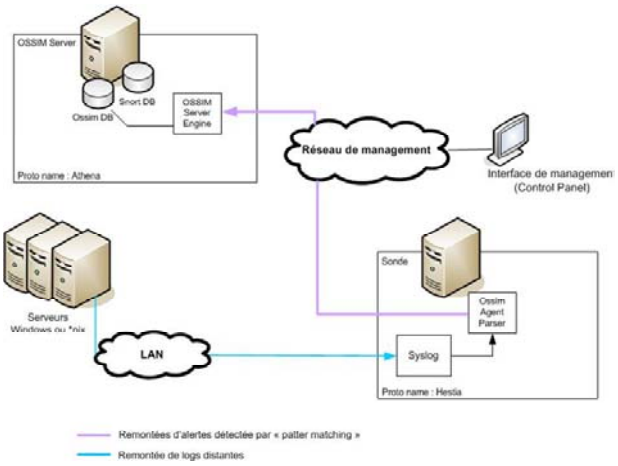
> Le risque informatique n'est pas une nouveauté mais il a évolué dans le temps

La solution OSSIM

> Actuellement : approche technique sécuritaire
- Logique basée sur les moyens

> OSSIM participe à une solution globale de sécurisation …
- Dispositif de Maitrise des Risques
- Définition des risques et enjeux
- Corrélation entre stratégie du S.I. et stratégie d'entreprise

Architecture OSSIM dans l'entreprise



Démarche

> OSSIM est une solution complète mais complexe à mettre en œuvre

> OSSIM s'inscrit dans une démarche globale de sécurisation

> Cette solution nécessite

- Une analyse complète des risques p/r aux enjeux
- Une maîtrise de l'activité
- Une politique de sécurité bien définie

L'offre KYOS OSSIM

> Dans cette optique KYOS propose d'établir un projet global de sécurisation avec

- Un accompagnement dans les phases d'audit et de cartographie des risques
- Du conseil pour établir une politique de sécurité réaliste et fonctionnelle
- L'intégration de la solution OSSIM au sein de l'entreprise
- La formation du personnel de sécurité pour l'utilisation d'OSSIM
- Un contrat de support pour assurer le suivi des paramétrage

> Une offre complète pour une solution complète.