PARTIE 2 :

ADMINISTRATION ET SUPERVISION DES RESEAUX

DOSSIER PROJET MASTER 2 RESEAUX et TELECOMMUNICATIONS

Présenté par :

Habib BALE

Thillo TALL

TABLE DES MATIÈRES

INTRODUCTION

Depuis quelques années, les entreprises perçoivent l'intérêt d'exploiter les nombreuses *traces*, événements et autres données d'audit logicielles, pour obtenir une image plus objective de leur sécurité informatique.

A ce besoin, les éditeurs ont répondu par une gamme de produits communément appelés SIEM. Sans entrer dans le débat sémantique consistant à utiliser cette appellation générique ou une typologie plus pointue distinguant les SEM (Security Event Management) qui n'exploitent que des données événementielles (logs), des SIM (Security Information/Incident Management) qui prennent en compte d'autres sources (résultats de scans par l'antivirus, par exemple), le SIEM-type est une couche de collecte filtrant différentes sources pour ne conserver que les événements de sécurité informatique. C'est aussi une couche de stockage souvent centralisé, une couche de valorisation (corrélation, alerte, reporting) permettant d'exploiter les événements de sécurité et une couche de présentation.
Les SIEM ont une architecture souvent complexe, une centralisation fréquente des données qui n'est pas toujours compatible avec les contraintes d'utilisation d'une grande entreprise (organisation géographiquement distribuée) et une orientation trop SSI, limitant le ROI « à la source » (filtrage lors de la collecte), même si les SIEM ont trouvé un second souffle bienvenu, avec les grands projets de conformité de type SOX.
Ces critiques récurrentes ont conduit à l'émergence des solutions dites de « Log Management » ou Gestion des Logs, conciliant des possibilités de collecte beaucoup plus larges, des capacités de stockage ad hoc et des fonctionnalités basiques de requête et de reporting.

Ce nouveau marché s'articule aussi bien autour de pure players - LogLogic étant le plus connu d'entre eux - que d'éditeurs de SIEM ayant senti la tendance et complétant leur offre avec des composants dédiés au log management : ArcSight avec ArcSight Logger et ArcSight Connectors,CS-MARS avec certaines appliances de la série, Log One, etc.
Malgré cette effervescence marketing, les différents acteurs du marché semblent converger plus ou moins rapidement vers une architecture générique qui s'appuie sur des appliances plutôt que sur des composants logiciels (simplicité d'installation puis d'administration, réduction des coûts matériels et de fonctionnement).
Nous dans les lignes qui suivent allons faire une études comparative des differentes solution SIEM

1. LOGLOGIC

A. PRESENTATION

Loglogic, anciennement

F. GESTION DES ALERTES

Loglogic peut réaliser un « reporting » en fonction du type d

2. PRELUDE

A. PRESENTATION

Prelude est un SIEM issu d

D. AGREGATION

Prelude ne fait pas d

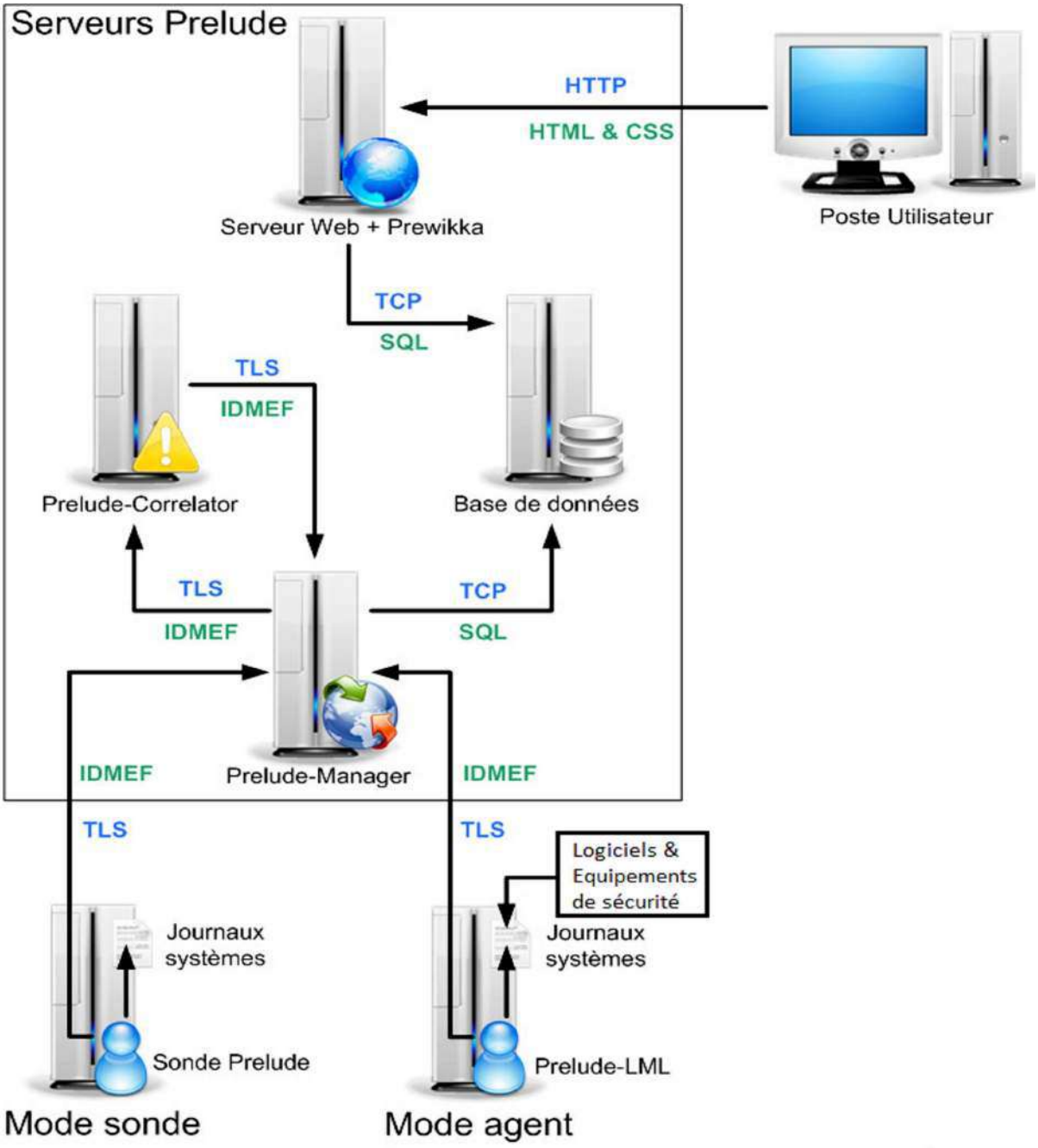

Figure 1 : Schéma du fonctionnement du SIEM Prelude

3. NET REPORT

A. PRESENTATION

La société Net Report a été crée en 2001 dans le but de fournir une solution globale à l

E. L

F. COLLECTE

La collecte se fait :

- A partir de périphériques hétérogènes
  Net Report supporte les principales catégories d

I. GENERATION DE TABLEAUX DE BORD

La génération des tableaux de bord peut être automatisée et planifiée dans le temps (tâche journalière, hebdomadaire ou mensuelle) Les tableaux de bord peuvent également être générés en temps réel.
Des fonctions avancées de Drill-Drown permettent une navigation intuitive et offrent la possibilité d

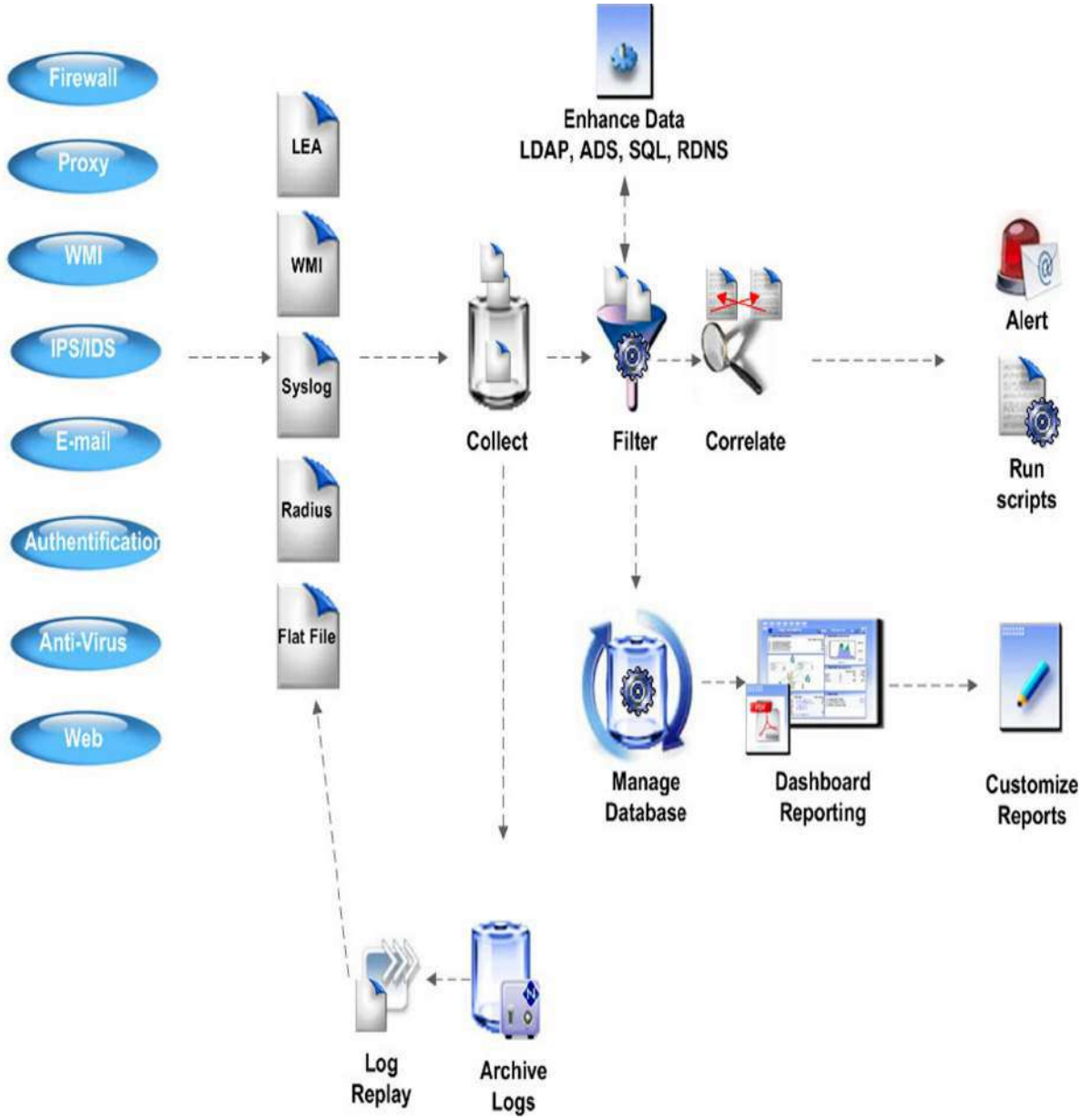

Figure 1 : schéma de fonctionnement du SIEM Net Report

4. LOG ONE DE NS ONE

A. PRESENTATION

Net Secure devenue NS One est un acteur spécialisé offrant une solution de sécurité globale personnalisable répondant à l´ensemble des besoins de sécurité applicative des entreprises mais également une solution de supervision globale de la sécurité.
NS One propose pour renforcer ce positionnement sur le marché et conforter la volonté de l´éditeur de devenir en 2008 l´un des acteurs majeurs de la sécurité applicative, NS One marque clairement sa volonté de changement en proposnt LOG One, une solution de supervision et d´interprétation des logs générés par l´ensemble des équipements installés sur le réseau de l´entreprise.

LOG One centralise, analyse et corrèle les logs des équipements de sécurité, de réseau et des serveurs. Les évènements collectés sont corrélés en temps réel pour produire des alarmes pertinentes et enregistrées en parallèle pour une analyse ultérieure. Un système expert étudie en permanence l´historique des évènements collectés pour compléter l´analyse en temps réel par des rapports. La solution couvre le cycle méthodologique complet de la gestion d´incident : prévenir, dé-tecter, confiner, enquêter, corriger et documenter.
LOG One génère des alertes, définit des tableaux de bord paramétrables et génère automatiquement des rapports utilisés pour la mise en

La solution LOG One embarque le module Manager. Il assure :

- Le filtrage de tous les évènements considérés comme inutiles.
- La corrélation d

5. CISCO SECURITY MARS

A. PRESENTATION

Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) est un dispositif hautes performances évolutif d'administration et de surveillance, qui facilite la prise de décision en matière de sécurité.

CS MARS se positionne donc clairement comme une solution de type SIEM avec pour ambition d'apporter cette réponse non seulement aux infrastructures Cisco mais aussi dans des réseaux hétérogènes.

Attention cependant, il est important de se souvenir que le travail qu'il faudra fournir pour paramétrer CS MARS sera beaucoup plus important que sur une solution 100% Cisco. Cette remarque restera par ailleurs valable pour les produits Cisco trop récents pour que des scénarios aient été déjà intégrés (exemple le CUCM). Ce point est traité dans un des derniers paragraphes du document.

B. LES APPLIANCES CS MARS

CS MARS est livré sous forme d'appliance. Il arrive donc sous forme d'un produit pré packagé ayant une plateforme physique définie avec un OS et un produit livré par l'éditeur et non modifiable. Les utilisateurs n'auront en aucun cas accès aux fonctions sous sous-jacentes de l'OS. L'interface de gestion des appliances est accessible au travers des protocoles sécurisés HTTPS (TCP 443) et SSH (TCP 22). Ces protocoles sont sécurisés et offrent les fonctions d'authentification, de chiffrement et d'autorisation. HTTP et Telnet sont désactivés de façon permanente.

L'OS des serveurs est basé sur un linux renforcé. On trouvera par ailleurs une base Oracle et un serveur web de la famille Apache pour archiver les données et offrir une interface graphique (technologies web). Ces différents éléments sont mis à jour à chaque nouvelle version ou patch.
Les différents modèles d'appliances sont décrits dans le tableau de la Figure 2. Dans l'absolu, il sera préférable de placer le CS MARS derrière des firewalls et IPS ainsi que dans une zone réservée à l'administration pour lui éviter d'être la cible d'attaques externes auquel il peut être sensible comme tout serveur. N'oublions pas qu'une fois configurée, cette application contiendra de nombreuses informations sensibles sur le réseau qu'elle aide à protéger.

Cisco Part Number (Modèles Local Controller)	Événements/Sec*	NetFlows/Sec	Stockage	Unités de rack	Puissance
Cisco Security MARS 20R (CS-MARS-20R-K9)	50	1500	120 GB (non-RAID)	1 RU x 16 pouces	300W, 120/240V autoswitch
Cisco Security MARS 20 (CS-MARS-20-K9)	500	15,000	120 GB (non-RAID)	1 RU x 16 pouces	300W, 120/240V autoswitch
Cisco Security MARS 50 (CS-MARS-50-K9)	1000	30,000	240 GB RAID 0	1 RU x 25.6 pouces	300W, 120/240V autoswitch
Cisco Security MARS 100e (CS-MARS-100E-K9)	3000	75,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 pouces	500W redondante, 120/240V autoswitch
Cisco Security MARS 100 (CS-MARS-100-K9)	5000	150,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 pouces	500W redondante, 120/240V autoswitch
Cisco Security MARS 200 (CS-MARS-200-K9)	10,000	300,000	1 TB RAID 10 hot-swappable	4 RU x 25.6 pouces	500W redondante, 120/240V autoswitch
Cisco Part Number (Modèles Global Controller)	Surveillance distribuée				
	Modèles supportés	Connexions Maximum	Stockage	Unités de rack	Puissance
Cisco Security MARS GCm (CS-MARS-GCM-K9)	Cisco Security MARS 20/50 uniquement	5	1 TB RAID 10 hot-swappable	4 RU x 25.6 pouces	500W redondante, 120/240V autoswitch
Cisco Security MARS GC (CS-MARS-GC-K9)	Tous	Pas de restriction	1 TB RAID 10 hot-swappable	4 RU x 25.6 pouces	500W redondante, 120/240V autoswitch

Figure 1 : *Les différents modèles d'appliance*

C. LA GESTION DES PROBLEMATIQUES STM

La gestion des problèmes de sécurité détectés ou STM. Le STM permettra d'automatiser le travail portant sur les problématiques sécurité bien identifiées pour permettre aux équipes de se focaliser sur les nouvelles menaces et les réponses à trouver.

Les solutions STM se doivent d'être temps réels et de proposer des contre mesures de façon pro actives de manière à défendre le réseau en lui apportant les contre mesures nécessaires au moment les plus opportun.
Les technologies STM commencent au même en collectant les informations des différents équipements. Les algorithmes de corrélation détectent alors des points *chauds* ou une attaque se déroule sur le réseau. La réponse apportée se porte alors non seulement sur les équipements directement attaqués, mais aussi sur l'ensemble des éléments périphériques pouvant permettre de bloquer l'attaque en amont.

La plus value des technologies STM se résume essentiellement au travers des points suivants :

- Une connaissance approfondie de la topologie du réseau et de son adressage permettant de réduire le volume important de log générer aux éléments clés permettant de cibler un incident,
- Apport d'une interface graphique permettant d'identifier tous les éléments du réseau et leurs configurations mais aussi les emplacements d'incidents ou d'attaques,
- L'intégration de scénario permettant des audits amont de la solution permet de réduire le nombre de faux positifs et d'améliorer le paramétrage de la solution pour gagner en efficacité,
- L'apport d'une réponse en temps réel permettant de bloquer une attaque.

Remarque : CS MARS possède plusieurs méthodes d'apprentissage pour connaître la topologie d'un réseau:

- Découverte du réseau (SNMP, Telnet, SSH). Il faut deux heures pour environ 300 périphériques,

Intégration de fichiers de topologie externes (support HP OV ou Cisco works),

- Interprétation des logs,

Entrées manuelles.

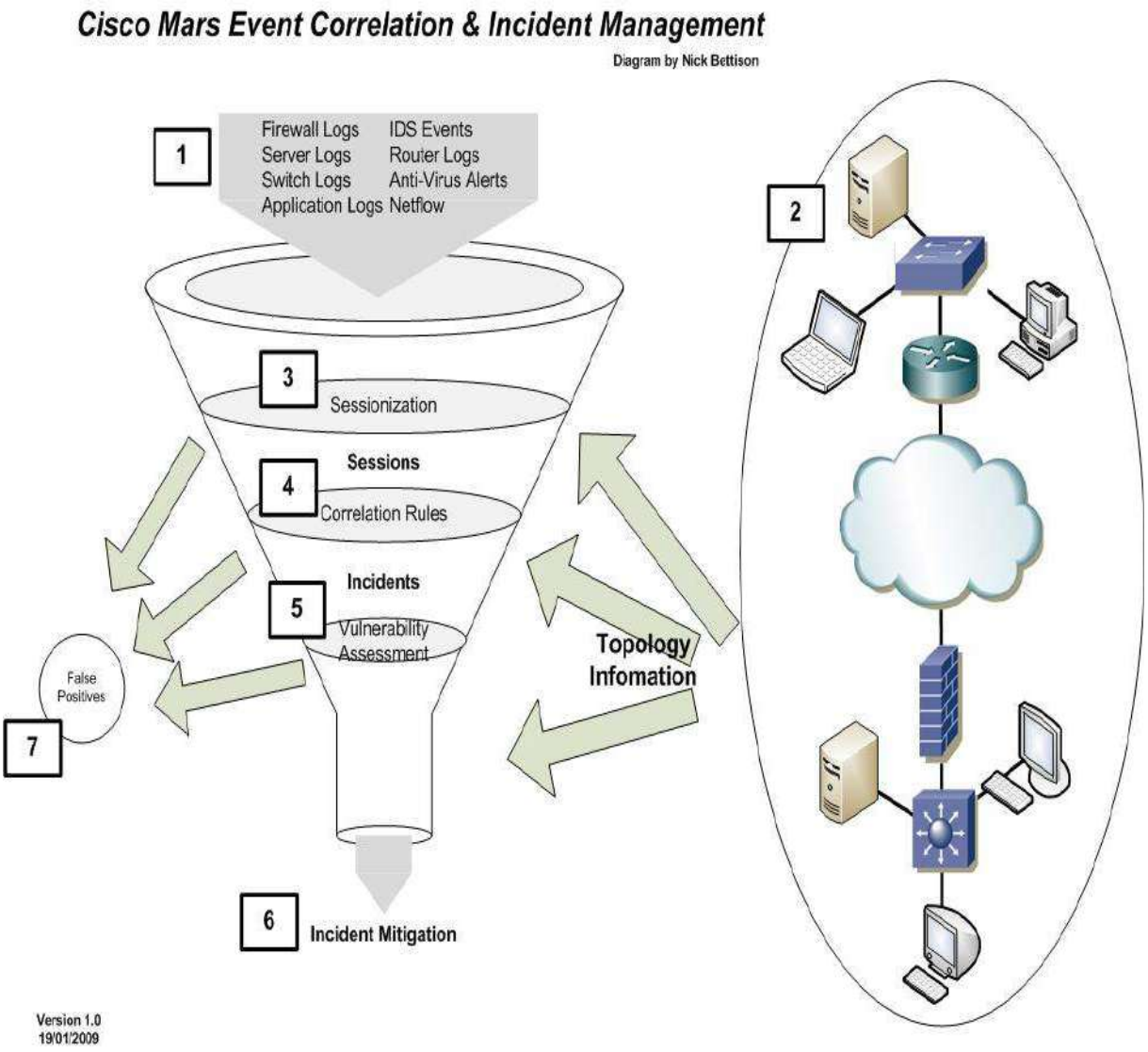

Figure 3. *La gestion d'un événement au sein de CS MARS*

D. LA GESTION DES ALARMES AVEC CS MARS

Par alarme, on parle du cycle d'action déclenché par une remontée d'incident. On prendra par exemple le blocage d'un paquet suspect par un IPS et la trap SNMP qui est déclenchée suite à cette action au système de supervision. La liste ci-dessous donnera une indication sur les protocoles supportés pour assurer les remontées d'alarmes.

Avec un CS MARS, au lieu d'avoir une simple remontée d'alarme, une corrélation d'évènement (mécanisme sommairement présenté en Figure 3) sera réalisée en amont de l'alarme envoyée à l'administrateur permettant ainsi de réduire les faux positifs, de qualifier très précisément le problème et de se concentrer directement sur les points essentiels, des actions correctives pouvant déjà être enclenchées en fonction du paramétrage. La Figure 4 présente un rapport remontant un premier niveau d'information suite à des évènements anormaux détectés par CS MARS. Protocoles utilisées pour les remontées d'alarmes : Syslog, SNMP, RDEP, OPSEC-LEA (Clear and encrypted), POP, SDEE, HTTPS, HTTP, JDBC, RPC, SQLNet.
La gestion de ces alarmes pourra se faire au travers de différentes méthodes suivantes : SNMP, Mail, Syslog, Messages texte, SMS, Signal sonore.
La gestion des incidents détectés se ferra soit de façon pro active soit sous réserve de validation par un administrateur au travers d'éléments comme ceux-ci :

- Envoi de TCP reset,
- Fermeture de ports,
- Mise en place d'access-list,
- Isolation de VLAN,
- Politique de sécurité plus globale pour le réseau,
- ...

Ces modifications porteront en premier lieu sur les équipements impactés. Les modifications concernant un écosystème élargi (voir le diagramme de l'attaque en Figure 3) seront soumises comme des alternatives complémentaires et nécessiteront une approbation. On se reportera à la Figure 5 comme exemple concret.
La connexion aux équipements devant être modifiés se fera au travers de SNMP, telnet ou SSH.
C'est cette possibilité de provoquer une réaction temps réel et adaptée à l'incident qui place le produit CS MARS comme un brique importante du concept de Self Defending Network (réseau se défendant seul) poussée en avant par Cisco.

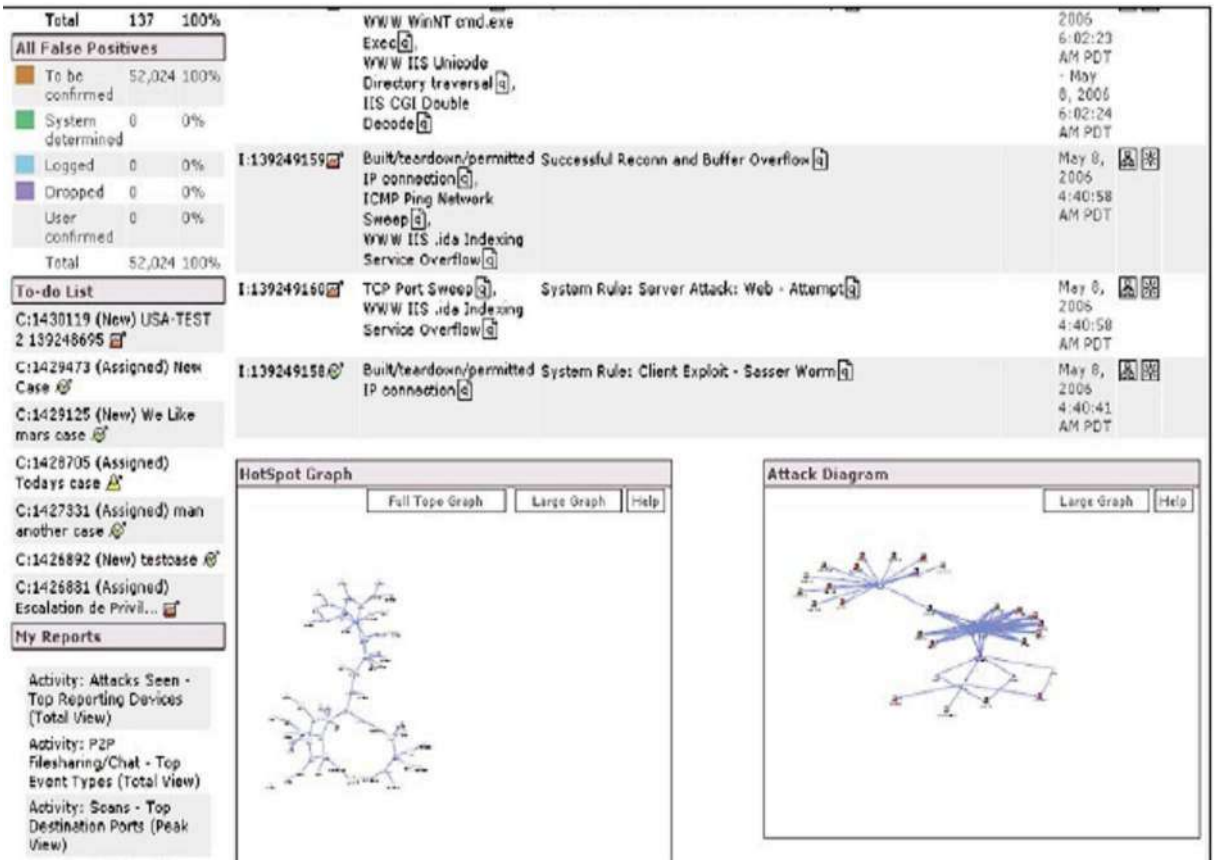

Figure 2 : Premier niveau d'information d'une alerte

E. GESTION DE L'ARCHIVAGE AVEC CS MARS

CS MARS est basé sur une base Oracle. Celle-ci est bien sur correctement configurée pour l'ensemble des opération du produit et ne demandera pas de compétence particulière pour l'administrée. Par conséquent, l'ensemble des systèmes de connexion traditionnels de ce produit ont été désactivés et seules les opérations réalisées par l'interface d'administration ou les services de CS MARS seront autorisées. La structure de la base n'est pas publiquement divulguée par Cisco.
On notera que le produit possède des mécanismes d'export et de sauvegarde de la base vers des NAS permettant éventuellement de restaurer le système avec une perte minimum de données si un problème devait survenir sur le système.

F. LES RAPPORTS SOUS CS MARS

Pour un outil de type STM, les problématiques de création de rapports et de requêtes sont un point absolument essentiel à regarder. En effet, si ces éléments ne sont pas bien traités, le produit perdra beaucoup de sa valeur car l'essentiel de l'information ne parviendra pas aux administrateurs en temps et heure.

CS MARS intègre un choix important de rapport déjà construits qui permettront de traiter la plupart des cas rencontrés classiquement dans la vie d'un réseau. Ces derniers permettent

de partir d'informations globales et de relativement haut niveau pour arriver aux éléments très détailler (voir Figure 5).

CS MARS propose désormais des rapports prenant en compte les spécificités des référentiels SOX, PCI et GLBA. Il est indéniable que l'intégration de rapports concernant ces référentiels devrait fortement facilité le travail des administrateurs devant montrer les conformités. Les personnes souhaitant plus de détails pourront se connecter à l'url suivante : *https://cisco.hosted.jiveso ftware.com/docs/DOC-2302 (l'enregistrement est gratuit*).

Les méthodologies d'audit COBIT sont elles aussi intégrées. Il est intéressant de constater que même si l'accès à la base de donnée n'est pas accessible, un moteur de création de requêtes existe, permettant ainsi de modifier ou de créer des rapports prenant en compte les particularités d'un environnement donné.
Le moteur chargé d'exécuter les différentes requêtes et de générer les rapports pourra être paramétré pour travailler en temps réel ou différé si l'on souhaite éviter d'accaparer trop de ressources pour cette tache à certaines périodes. Intégration d'un périphérique tierce.

Pour intégrer un périphérique inconnu dans CS MARS, il sera nécessaire de créer un parser personnalisé. Ceci sera réalisé en trois grandes étapes (Figure 6) :

- Définition du nouveau type de périphérique

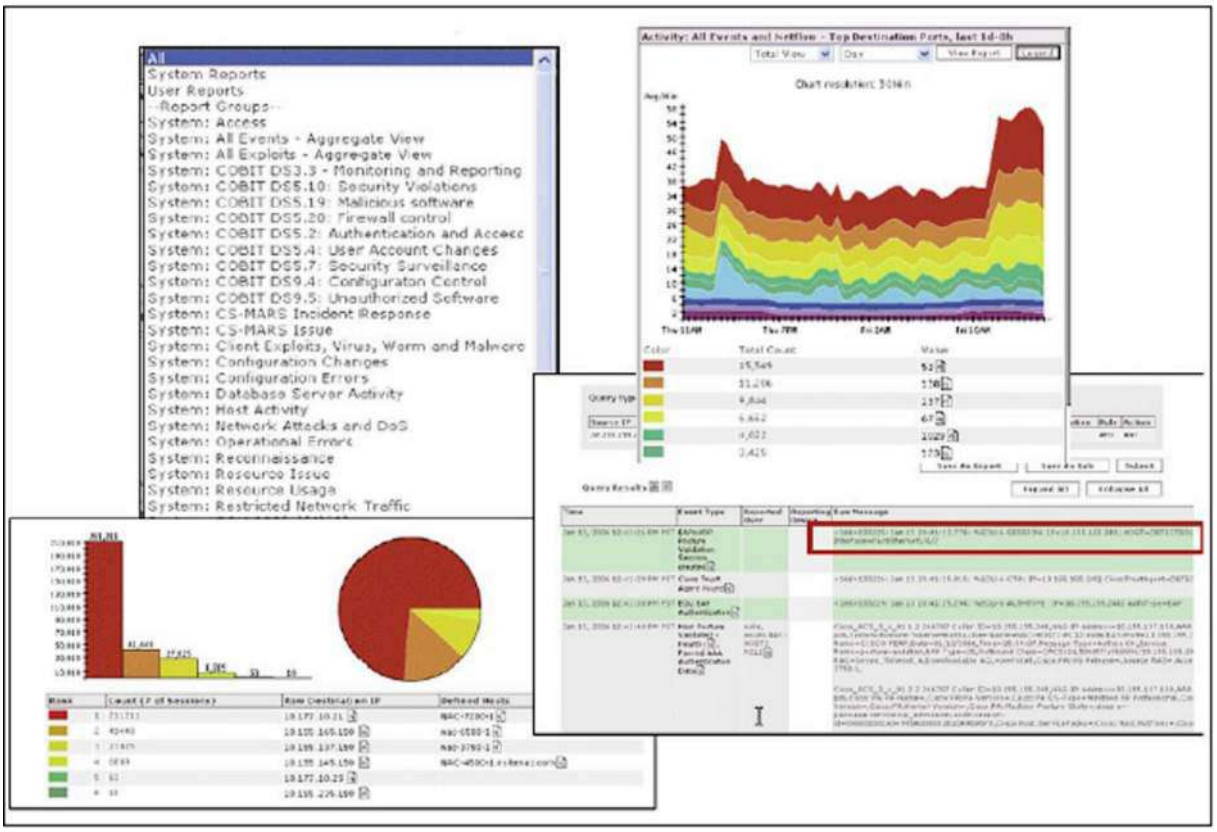

Figure 5. *Exemple de rapports*

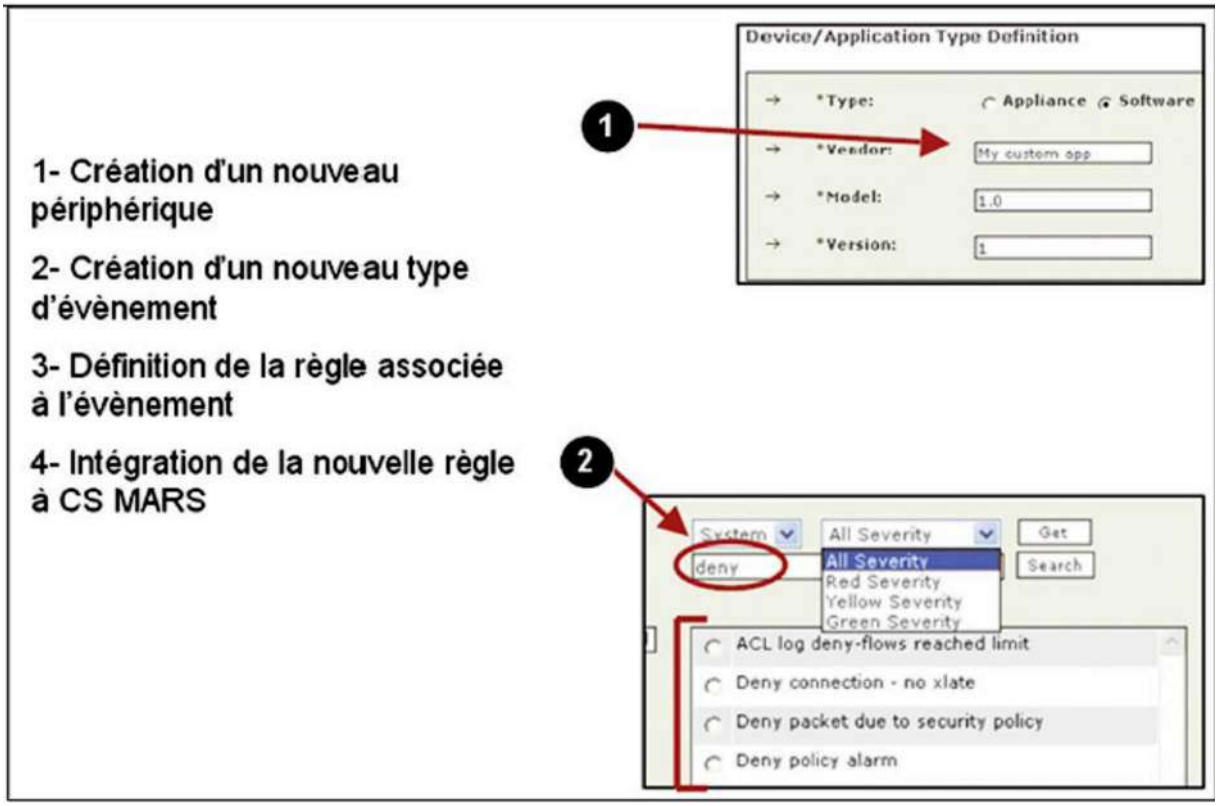

Figure 6. *Intégration d*

G. QUELQUES CONSIDERATIONS D'ARCHITECTURE

La façon la plus simple de travailler avec la solution CS MARS est de déployer un seul contrôleur, soit une seule appliance collectant l'ensemble des logs générés par les périphériques réseaux ou les serveurs et assurant l'analyse des données.

La seconde possibilité nécessite l'utilisation de deux briques appelées contrôleur global et local. Dans ce cas, des contrôleurs locaux sont placés sur différents sites. Les périphériques intégrés pour travailler avec CS MARS envoient les logs vers ces derniers. Les périphériques supervisés ne pourront jamais envoyer directement des données au contrôleur global. La supervision de la solution complète est effectuée depuis le contrôleur global. Chaque contrôleur local n'ayant qu'une vision limitée à son périmètre. L'utilisation du modèle utilisant deux types de contrôleur devra prendre en compte les éléments suivants :

- Le volume de log total généré par les périphériques supervisés ne peut être absorbé par un seul serveur (20 000 logs/s et 600 000 netflows/s). Le listing 3 donnera quelques chiffres indicatifs permettant de calculer le volume généré par un réseau. Il est couramment considéré que si 60% de la capacité d'EPS du serveur est atteinte, il devient nécessaire d'envisager une mise à jour pour assurer le bon fonctionnement,
- L'architecture réseau comprend des sites distants reliés à l'aide de liens WAN. Dans ce cas, le contrôleur global demande uniquement les informations nécessaires au contrôleur local et évite ainsi de saturer le lien WAN,
- La société est composée de nombreux départements ou filiales avec des besoins spécifiques. Les contrôleurs locaux permettront à chaque département de répondre à ses propres exigences tandis que le contrôleur global amènera une vision globale et pourra être placé dans un SOC.

Il sera absolument nécessaire par ailleurs de calculer l'espace disque nécessité pour archiver l'ensemble des logs qui seront générés par l'installation supervisée. On pourra considérer que la taille moyenne d'un log sera de 300 octets. La formule suivante permettra alors un premier calcul : Nbre de jour archivés = Taille réservée à l'archivage / (Taille du log (donc ici 300 en moyenne) * EPS * 86,400).

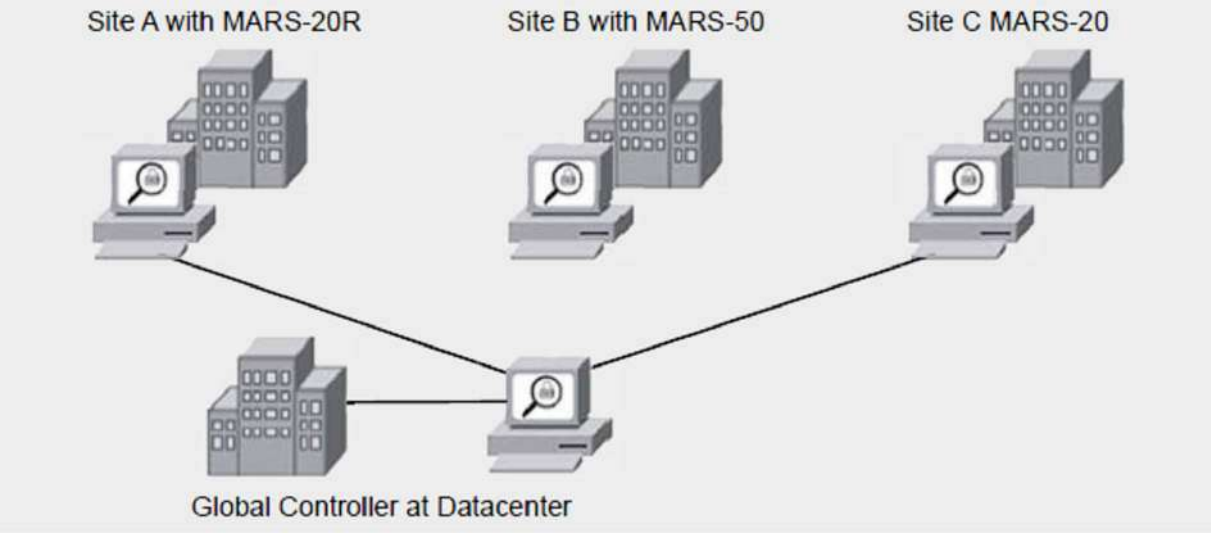

Figure 7. *Synoptique d'architecture avec les deux types de contrôleurs*

6. ARCSIGHT ESM

A. PRESENTATION:

ArcSight, une société HP, a été fondée en 2000 et est une société technologique qui fournit des informations de sécurité et de gestion des événements (SIEM) des solutions.

ArcSight est en pole position du Quadrant magique de Gartner concernant les principaux éditeurs de solutions **SIEM** pour Mai **2010**
ArcSight Enterprise Security Manager (ESM): moteur d'analyse de base pour gérer les menaces et les risques au sein de la plate-forme ArcSight constituée de :

* ArcSight Logger: stockage des journaux de la plateforme et la solution de recherche
* ArcSight Express: la corrélation et la gestion des logs
* ArcSight IdentityView: suivi des activités des utilisateurs
* Connecteurs ArcSight: la collecte des données provenant de diverses sources de données
* Applications vérificateur ArcSight: surveillance continue des contrôles automatisés

La plate-forme ArcSight supporte également la virtualisation, les environnements informatiques mobiles et de nuages

ArcSight ESM assure l

- corrélation tridimensionnelle : informations de sécurité des différents produits, informations de vulnérabilité, caractéristiques d

B. ARCSIGHT MANAGER

Le gestionnaire ArcSight est le c

D. ARCSIGHT BASE DE DONNEES

La base de données est une base de données ArcSight relationnelle Oracle optimisée pour le stockage de tous les événements du journal. Une indexation efficace et efficiente des données fournit un accès rapide à des événements historiques dans l'analyse des journaux de sécurité, ou lors de la génération de rapports. Outre le stockage des événements du journal est stocké dans la base de données et la configuration de l'ESM ArcSight ArcSight - tels que Les utilisateurs, groupes, les paramètres d'autorisations, règles, filtres, tableaux de bord, la modélisation des réseaux, rapports, etc

FONCTIONNALITES CLES

* Référentiel central pour tous les événements du journal normalisé
* Stockage efficace par compression, partitionnement et l'archivage
* Base de données relationnelle basée sur Oracle 10g
* Fournir des données en fonction du volume DB-volume et de données dans la plage allant jusqu'à plusieurs mois

E. ANALYSE DE LA SECURITE AVEC LA CONSOLE ARCSIGHT

La console ArcSight fournit l'interface globale pour tous les utilisateurs d'ArcSight ESM alors que l'utilisation de la zone de la console ArcSight comprend l'exploitation d'une exploitation COS (Centre d'Opération de Sécurité) qui se concentre sur le suivi des indicateurs d'alerte et le signalement des incidents est, ainsi que les Création de contenu ArcSight (telles que le filtrage, les règles de corrélation, tableaux de bord, rapports, etc) pour l'analyse de la sécurité en aval. La console ArcSight est également l'outil central pour gérer et administrer le dar ESM ArcSight.

FONCTIONNALITES CLES

* une interface basée sur Java, conçu pour Operation Center de sécurité
* Fournit des outils pour la définition des filtres, règles, rapports, affiche, alarmes, etc..
* Permet de contrôler l'accès basé sur les rôles, à partir d'un tableau de bord simple de créer des règles de corrélation complexes

F. GESTION DES ALERTES

ArcSight produit de log management, ArcSight Logger, est un appareil autonome pour stocker, gérer et rapports contre les données du journal d'entreprise. Un seul appareil peut effectivement stocker jusqu'à 35 To de données journal, sans besoin de réglage ou d'optimisation. ArcSight Logger offre de recherche et de reporting, ainsi que d'alerte par e-mail, SNMP ou d'une console Web.
Contrairement aux autres produits de gestion des logs, ArcSight Logger fournit drill-down à partir des alertes et des rapports sur les événements source derrière l'alerte ou de rapport.
En conséquence, même les clients qui n'ont besoin que simple bénéfice d'alerte et de reporting de «Forensics à la voléesont servis.

G. CORRELATION

- Corrélation avancée

ESM utilise une variété de techniques sophistiquées pour passer au crible millions des événements pour trouver les incidents qui peuvent avoir un impact véritable sur l

H. AUTOMATISATION DE CONFORMITE

ArcSight conformité Forfaits Insight est un moyen idéal pour lancer un projet de conformité ou d'automatiser le suivi du manuel existant contrôles de conformité. Installable sur le dessus de la plate-forme ArcSight SIEM,
Ces modules fournissent de pré-emballés règles, rapports, tableaux de bord et alertes mappés à des réglementations spécifiques. Grâce à l'automatisation et la meilleure pratiques, ArcSight conformité Forfaits Insight peut réduire considérablement le coût et les efforts de conformité.

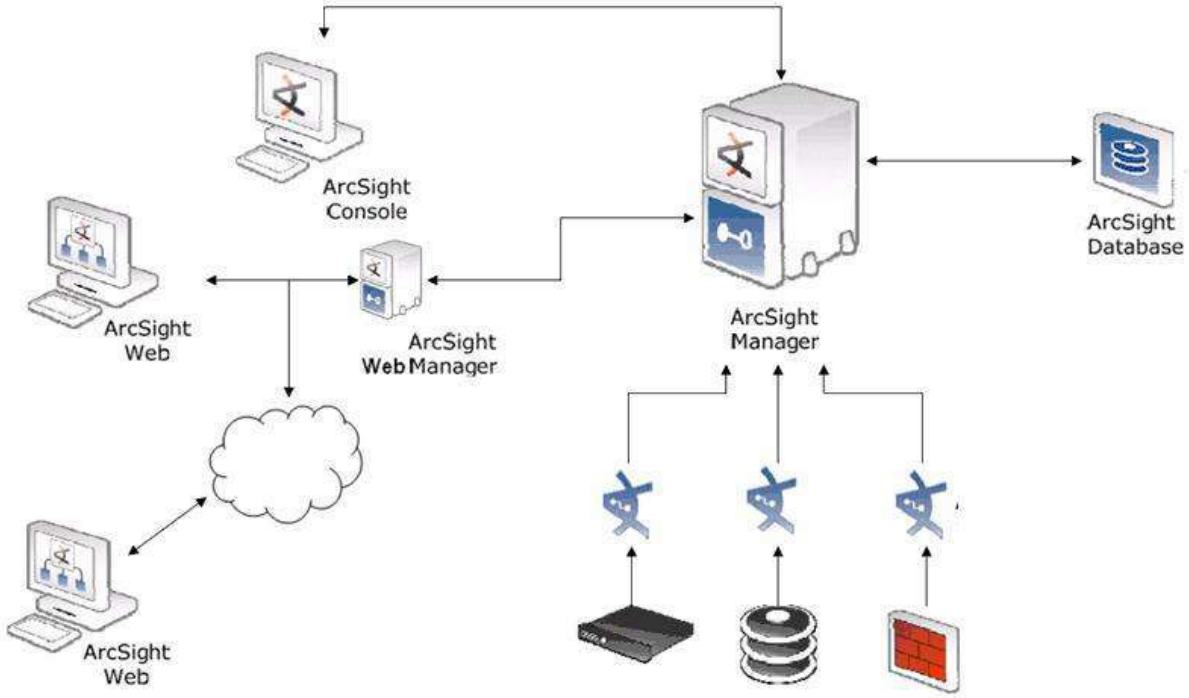

Figure 1 : Scema de fonctionnement du package ArcSight ESM

CONCLUSION :

L