exaprotect Technology

Supervision de la sécurité et gestion du risque

Security Information Management

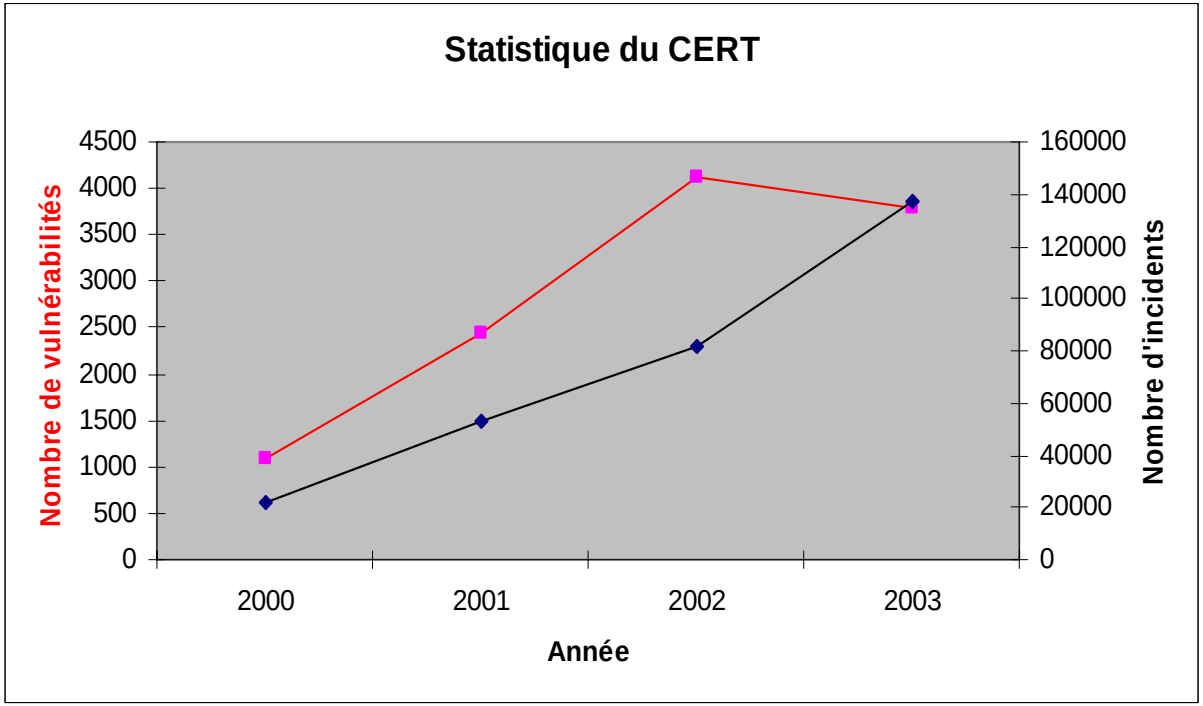
www.exaprotect.com

Plan de la présentation

1. La tendance en matière de SSI
2. Les enjeux de la supervision de la sécurité
3. La solution EAS

Menace croissante

- L'Internet est de moins en moins sûr !



- L'intelligence économique est omniprésente *

* http://www.bcarayon-ie.com/html/main_v2.html

Des budgets croissants pour les entreprises et administrations

- Des M€ dépensés en moyenne par an
- 90% utilisent des pare-feux ou des anti-virus
- 40% utilisent des systèmes de détection d'intrusions (IDS)
- Nombre croissant de dispositifs à protéger

Constats

- Chaque pare-feu peut produire **plus de 1 Go** de traces chaque jour
- Un IDS peut produire 10 Mo de messages par jour avec **99% de fausses alertes**
- Les équipes de sécurité **sont noyées** sous l'information
- Le RSSI est très souvent **aveugle** pour contrôler les effets de la **politique de sécurité** mise en oeuvre
- Le DG/DSI l'est tout autant lorsqu'il souhaite estimer un **ROI** sur ses **investissements** en sécurité

Principales problématiques

- **Sources hétérogènes** (filtrage, détection d'intrusion, détection de vulnérabilité, authentification ...)
- **Format « aléatoires »** (dépend de l'éditeur, varie d'une version à l'autre ...)
- **Différent moyen de transmission** (synchrone, asynchrone) et **destinataire multiple**
- **Visibilité parcellaire** (données distribuées sur les systèmes et multiplicité des consoles)

« Comment retirer la substantifique mœlle ?»

Quiz !

Cas concret : 100 serveurs, paramétrés pour bloquer l'accès et générer une alarme après 3 « *login failed* »

Question: *Combien d'alarme générera un attaquant chevronné pour pénétrer le S.I. ?*

- *A) aucune*
- *B) une seule*
- *C) 100*
- *D) …*

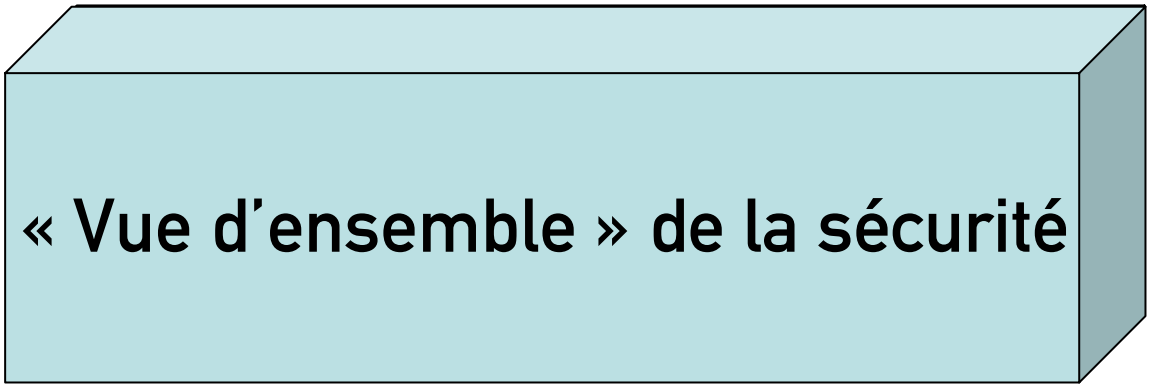
Réponse B: Seulement une seule, qui sera probablement noyée dans la masse

Explications …

- Etape 1: L'attaquant teste un serveur et identifie la politique (3 essais = 1 alarme)
- Etape 2: L'attaquant fait 2 tests en boucle sur chacun des 100 serveurs (procède suffisamment lentement pour ne pas être bloqué à nouveau).
- Plus aucune alarme ne sera générée et à un moment ou un autre il réussira !

Comment augmenter la visibilité ?

- Analyser chaque log (un *login failed* génère une entrée de log)
- Établir le lien entre les *logs* de tous les serveurs
- Alerter les administrateurs avant que l'attaque ne réussisse



Les administrateurs doivent gérer la menace dans son ensemble et pas uniquement des alarmes individuelles !

Problématiques techniques

- Comment collecter les logs depuis different équipements?
  - Installation d'agent (pas toujours possible)
  - Standard : Syslog, fichier texte, SNMP
  - Besoin de sécuriser les communications
- Performance de la solution ?
- Capacité à être déployée à grande échelle ?
- Comment corréler différents types d'alertes?
  - Besoin d'un format commun (normalisation)

Qu'est ce que la « corrélation de log » ?

- Plusieurs sens !
- Ce n'est pas seulement :
  - Centraliser les logs
  - Faire des rapports périodiquement (statistique …)
  - Prioriser et filtrer les événements de sécurité
- Mais c'est également :
  - Analyser en temps réel et en continue
  - Corréler les événements avec d'autre source (base de connaissance, base de vulnérabilité …)
  - Des règles personnalisables prenant en charge différentes sources et types d'informations

Les enjeux des technologies SIM*

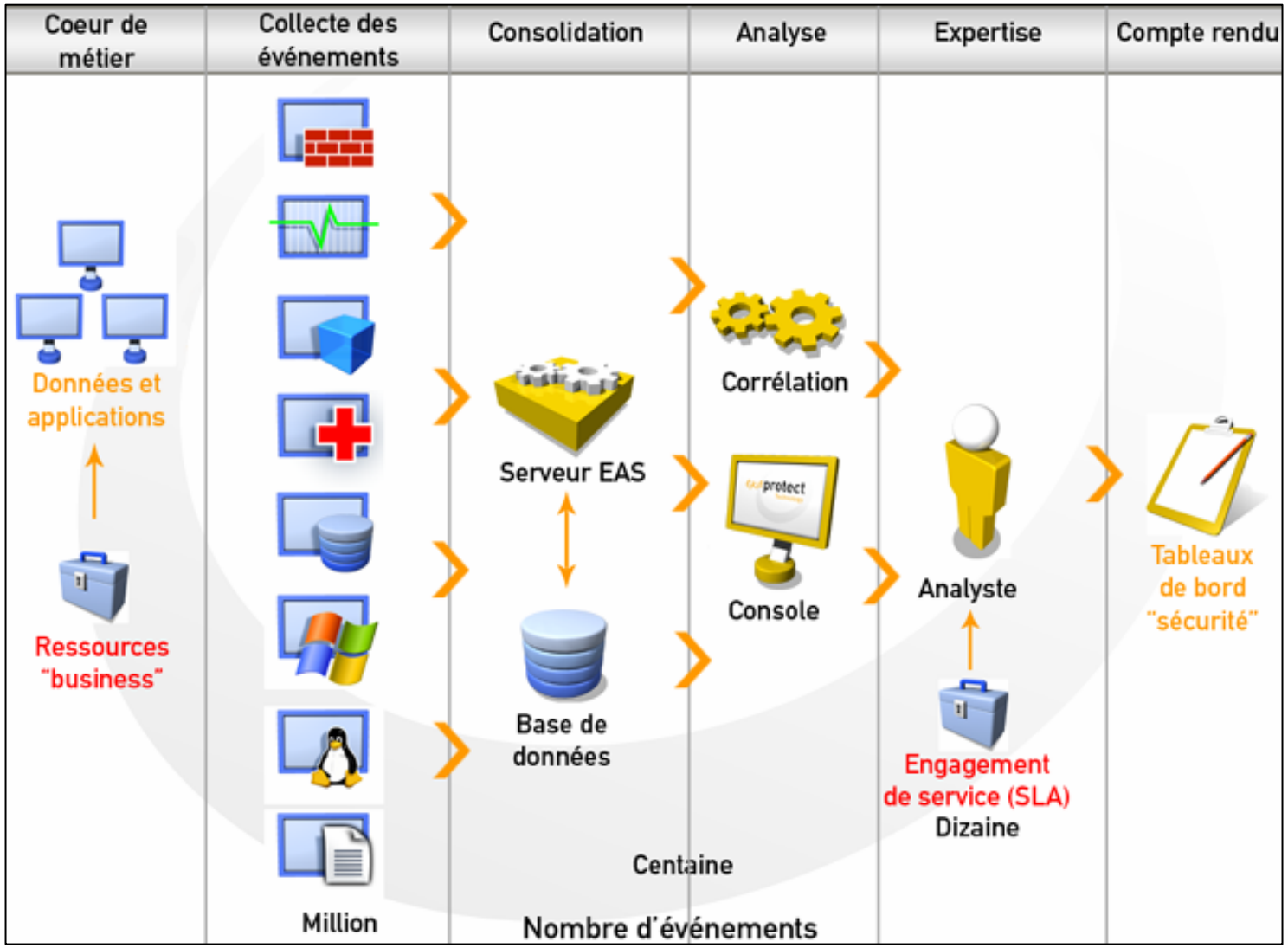
- Valoriser les investissements déjà réalisés
- Augmenter la productivité des équipes techniques et accroître l'intérêt des missions
- Diminuer les risques en visualisant le niveau de protection
- Formaliser le management de la SI (*tuning*, procédures)
- Répondre aux obligations réglementaires (LEN, BS7799-2 …)

* *Security Information Management*

Quelle Stratégie vis à vis des SIM ?

- Acquérir un SIM en interne
  - Gérer sa mise en œuvre progressivement
  - Maîtriser l'outil sur un plan technique
  - Construire, diffuser et faire vivre les procédures d'exploitation et de reporting
  - Vérifier la pertinence des tableaux de bord
- Externaliser l'administration de la sécurité
  - Offre en pleine évolution
  - Réelle opportunité selon les contextes
  - Occasion de vérifier la politique de sécurité en interne
  - Obligation de suivi

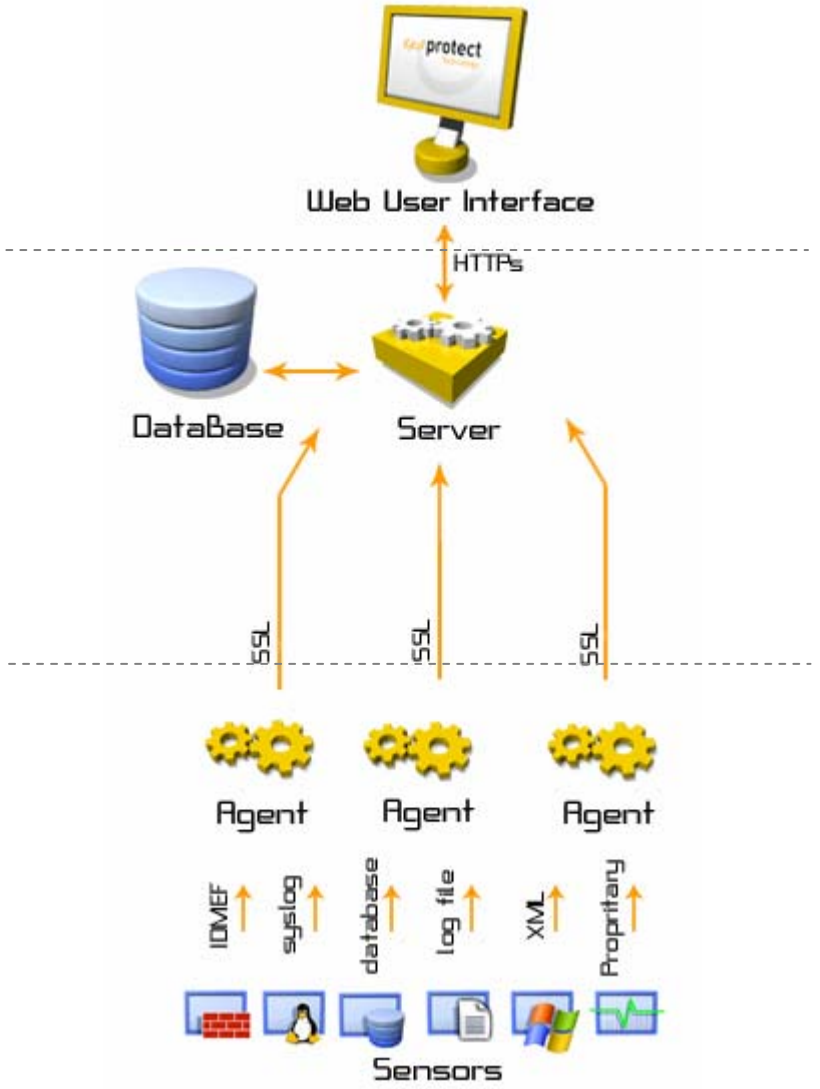
Le concept de la solution SIM ExaProtect



L'architecture à 3 niveaux

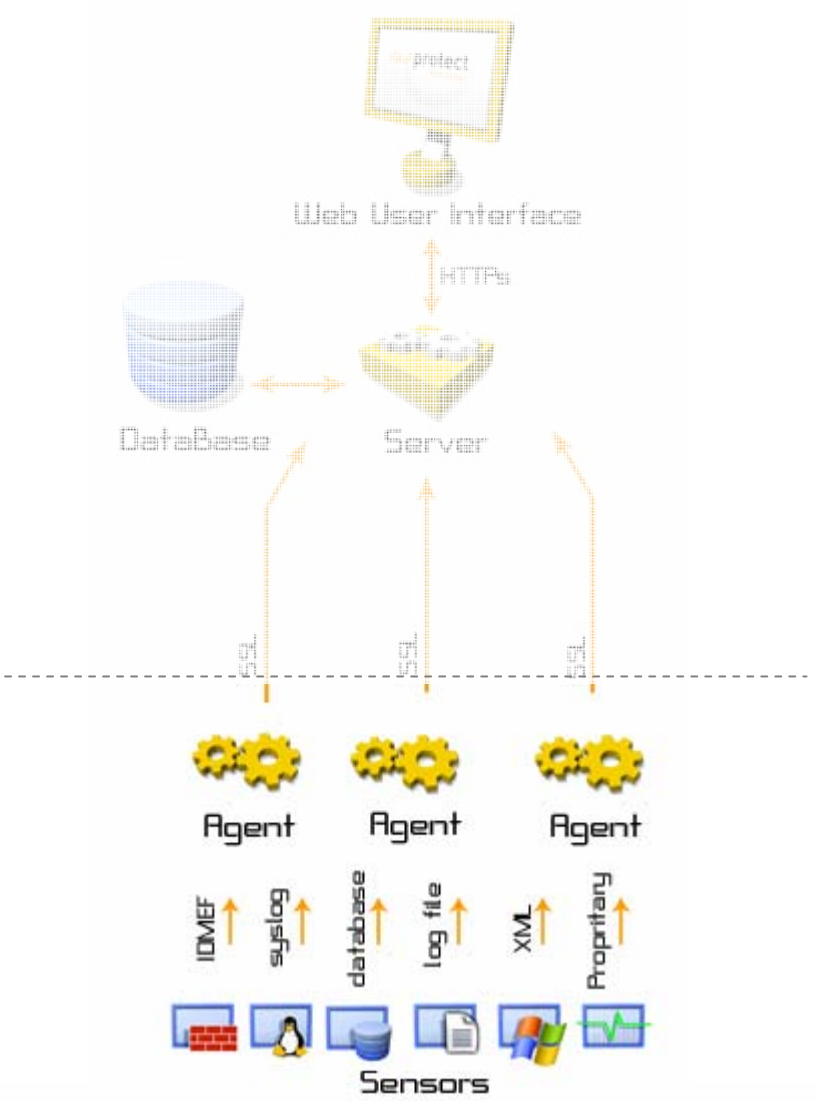
- EAS* basé sur des composants OpenSource
  - RedHat, MySQL, Apache / Tomcat, Prelude
- Technologie iCare
- *Appliance* dédié (Bi-Pro)

* ExaProtect Advanced Software



Les agents ExaProtect

- **Collection et normalisation** des événements
- **Tolérance aux pannes** (mode hors ligne, redondance de serveur)
- **Priorisation** des événements dans la file d'attente
- **Flux sécurisés** (chiffrés en SSL et authentifiés par certificat)
- Émission de "***heartbeats***"



La normalisation des messages

- Analyse sémantique (lexicale)
  - Uniformisation du **contenu**
  - Un même événement, différents messages !

Checkpoint : « *Port Scanning* »
NetASQ : « *Possible port scan* »
Snort : « *Portscan detected* »

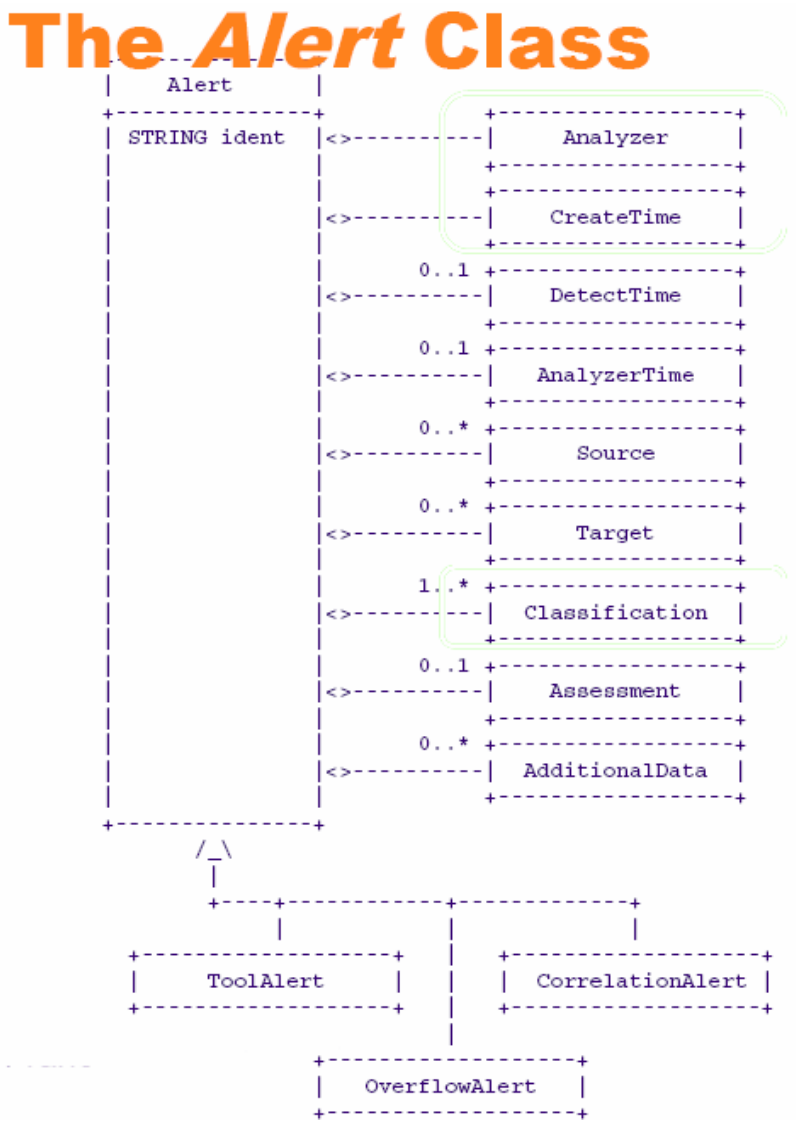
- Analyse syntaxique
  - Uniformisation de la **forme**
  - Conversion en IDMEF* de chaque message

Permet un traitement optimisé des messages

* Intrusion Detection Message Exchange Format

L'IDWG pousse le future standard IDMEF

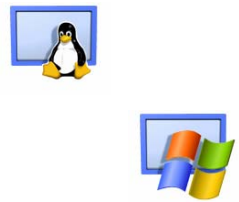
- **Consensus sur la nécessité d'un format unique et non ambigu des messages de sécurité : besoins d'exploitabilité et de cohérence**
  - **Modèle de données orienté objet : classes et attributs :**
  - **Échange de messages IDMEF via XML sur TCP ou IDXP/BEEP**
  - **Richesse du format**
  - **IDXP-BEEP, RFC 3080 et 3195 : transport TCP et profils (gestion des canaux, sécurité du transport par TLS, authentification par SASL)**
  - **IDMEF supporté par les acteurs du marché**



exaprotect Technology

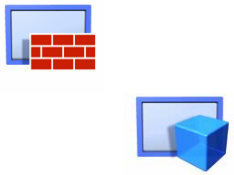
La solution ExaProtect

Liste non exhaustive …



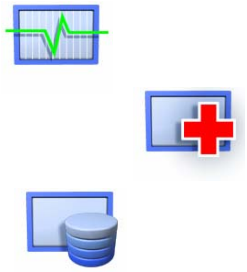
debian · redhat · hp invent · SOLARIS · Microsoft Windows Server

Système d'exploitation



Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet. · NETASQ Secure Internet Connectivity · ARKOON NETWORK SECURITY® · NETSCREEN · NOKIA CONNECTING PEOPLE · CISCO SYSTEMS · ZyXEL TOTAL INTERNET ACCESS SOLUTION · astaro internet security

Pare-feu et routeur



network ASSOCIATES · TREND MICRO · Nessus · SNORT · symantec.

Antivirus, scanner, sonde IDS

Nagios® · ActivCard · RSA SECURITY · TRIPWIRE

Monitoring et authentification

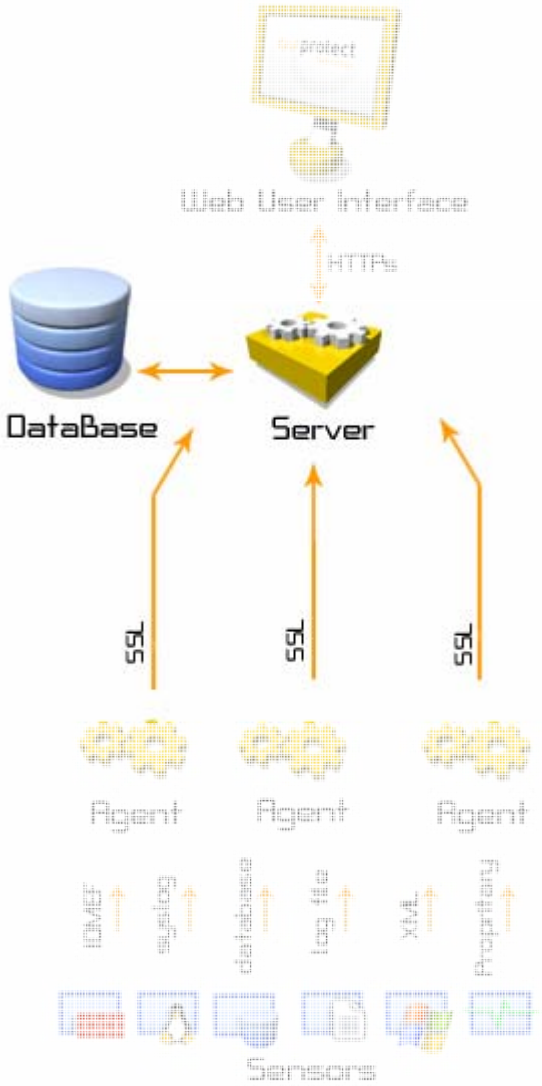
Agent universel (Fichiers logs « à plat »)

Autres applications …

Le serveur ExaProtect

- Technologie iCare *
  - Analyse et corrélation des événements
  - Supervision temps réel
  - Génération de tableaux de bord

- Stockage et archivage des données
  - Sauvegarde / restauration
  - Purge



* Labellisé par ANVAR

Agrégation d'événements

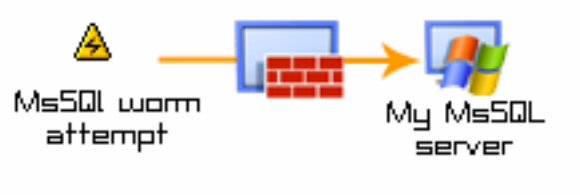
- Regroupement des alertes entre elles
  - Même source (IP, utilisateur …)
  - Même destination
  - Même signature d'événements
  - …

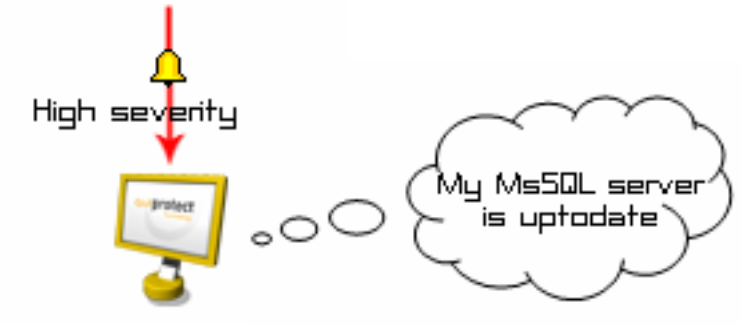
- Sélection des critères suivant le type de message
  - Ex:
    - *Exploit* (IP source, IP destination, port destination)
    - *Attack response* (IP source, port source)

Réduit le nombre d'alertes à expertiser

Évaluation du risque

- Chaque alerte est évaluée suivant la valeur et le niveau de vulnérabilité de la cible
- Prise en compte des critères *business* (SLA, info *corporate* …)
- Utilisation d'une base de connaissance





1. Augmente la pertinence des alertes
2. Enrichit la description de l'événement

La base de connaissance « Asset Database »

- **Modélisation préalable du périmètre surveillé**
- **Alimentation semi automatique**

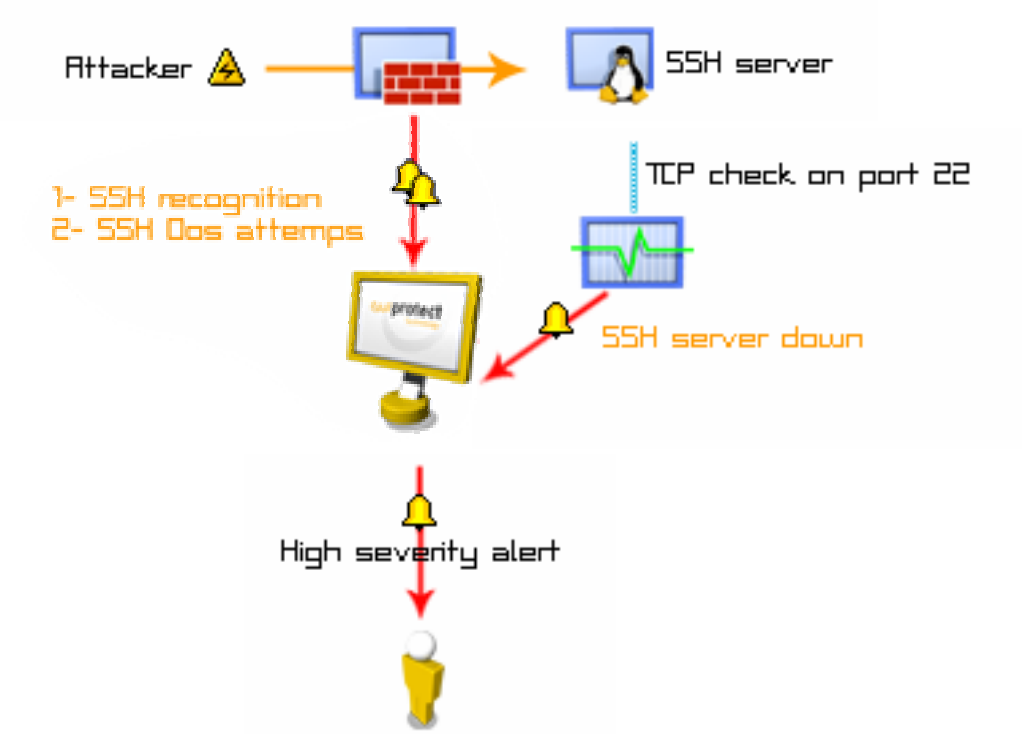
Host & Service
Business Asset
SLA, Criticité
Vulnérabilité
Plan de réponse

Utilisateur
Fichier à plat (import)
Nessus / Nmap
OSVDB, ICAT

Prendre en compte l'environnement

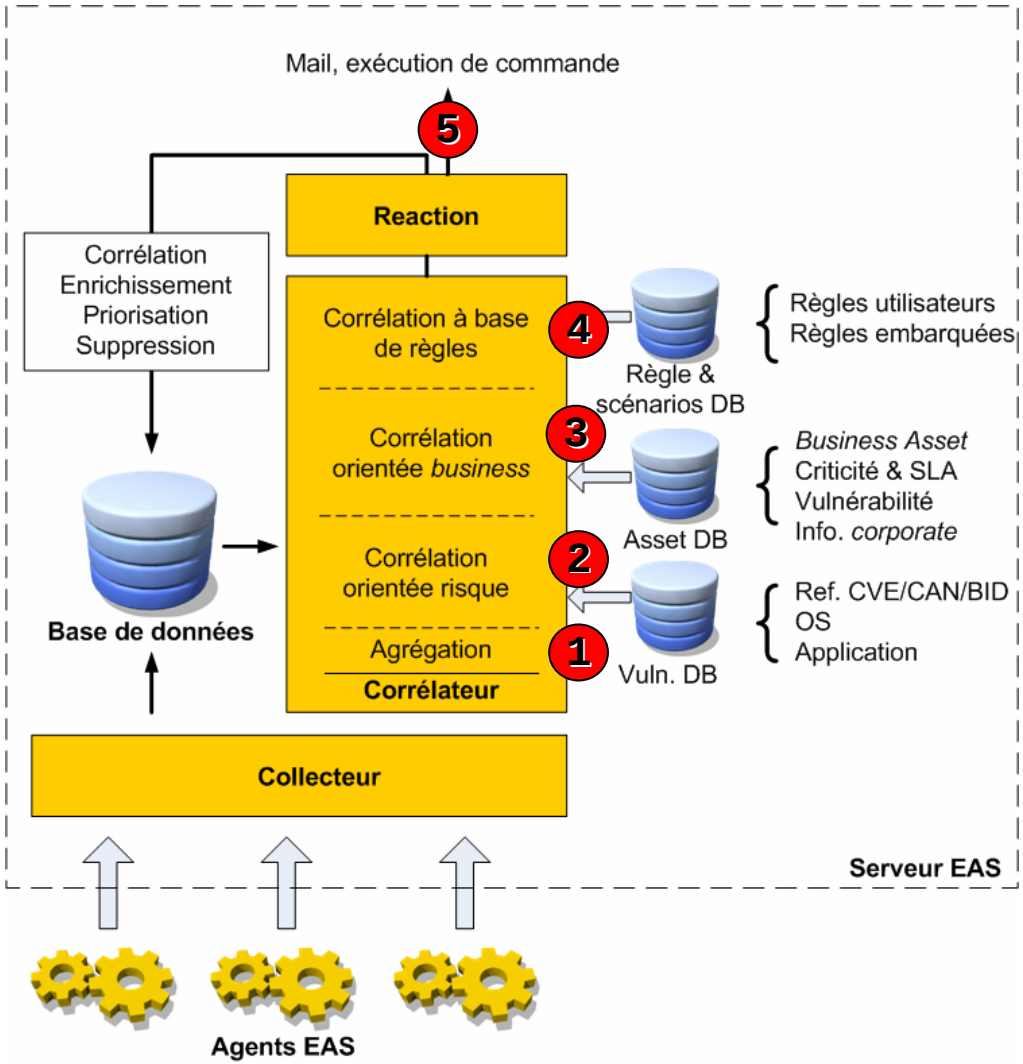
Corrélation avec une base de règles

- Basée sur des règles utilisant des scénarii prédéfinis (si… alors… sinon…)
- Personnalisable par l'utilisateur



1. **Détection d'incident potentiel**
2. **Réduction du nombre d'alertes en les regroupant en fonction de scénarii prédéfinis**

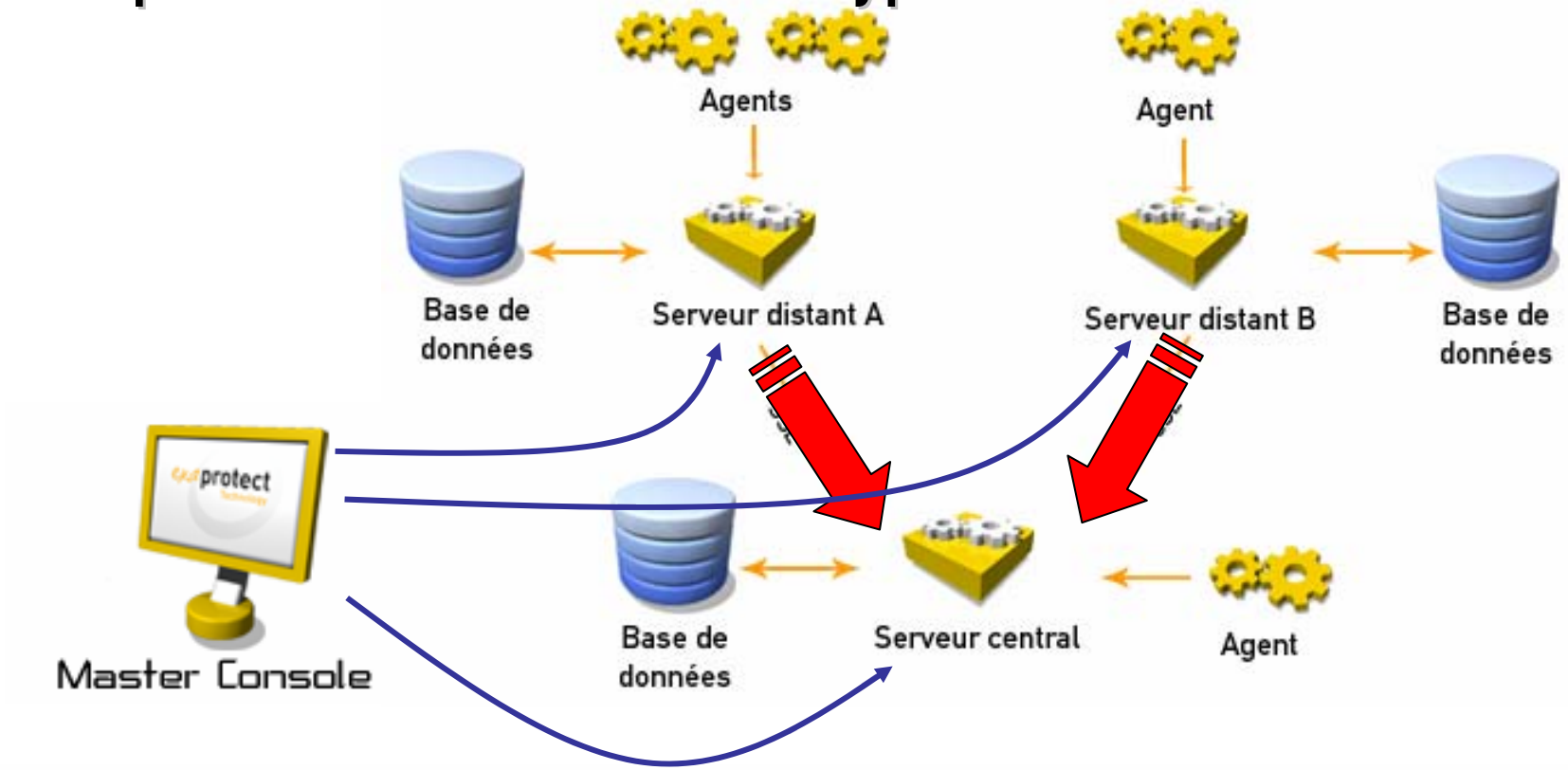
L'architecture interne du serveur



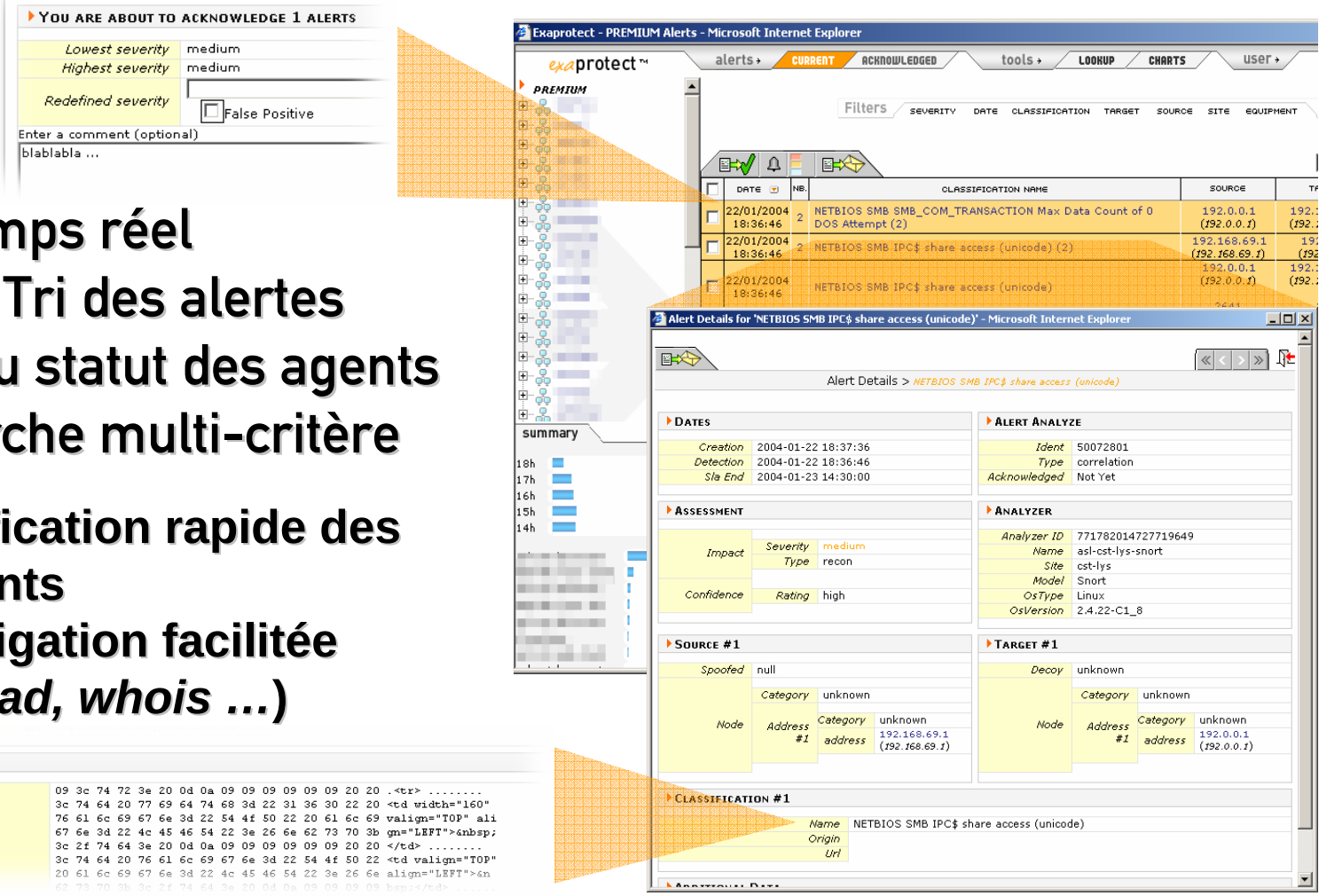
1. Regroupement d'événements
2. Évaluation de l'événements
3. Enrichissement
4. Condition et exception
5. Action

L'architecture distribuée

- Adaptée pour les environnements complexes
- Routage des événements
- Supervision centralisée / Hypervision



La console temps réel



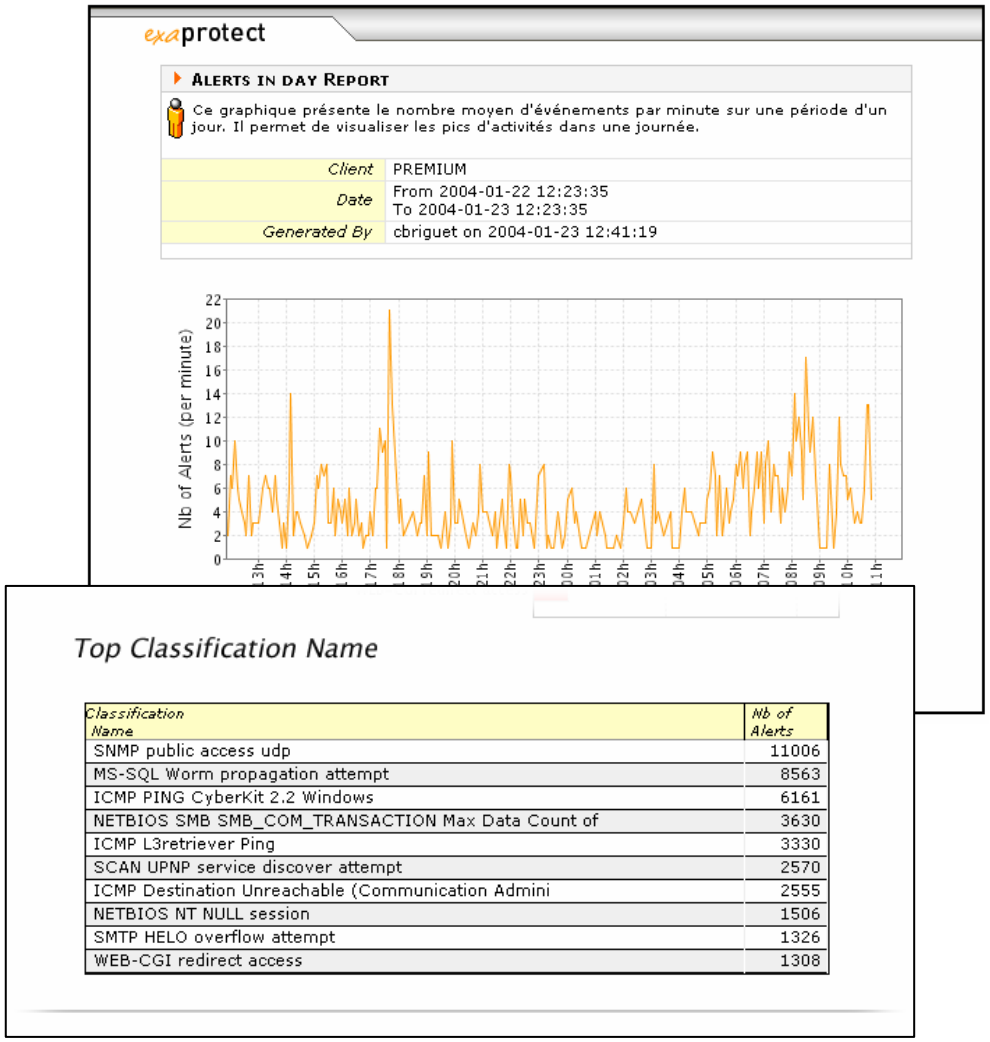
- Vue temps réel
- Filtre / Tri des alertes
- Suivi du statut des agents
- Recherche multi-critère

→ **Identification rapide des incidents**

→ **Investigation facilitée (*payload, whois ...*)**

Les tableaux de bord sécurité

- Rapports dynamiques et pré-générés
- Orientés “administrateur sécurité” et “management/RSSI”
- Personnalisables
- Exportables sur un intranet



exaprotect

ALERTS IN DAY REPORT

Ce graphique présente le nombre moyen d'événements par minute sur une période d'un jour. Il permet de visualiser les pics d'activités dans une journée.

Client	PREMIUM
Date	From 2004-01-22 12:23:35 To 2004-01-23 12:23:35
Generated By	cbriguet on 2004-01-23 12:41:19

Top Classification Name

Classification Name	*Nb of Alerts*
SNMP public access udp	11006
MS-SQL Worm propagation attempt	8563
ICMP PING CyberKit 2.2 Windows	6161
NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of	3630
ICMP L3retriever Ping	3330
SCAN UPNP service discover attempt	2570
ICMP Destination Unreachable (Communication Admini	2555
NETBIOS NT NULL session	1506
SMTP HELO overflow attempt	1326
WEB-CGI redirect access	1308

Les points forts

- Premier logiciel SIM 100% au standard IDMEF
- Génération de tableaux de bord orientés « service »
- Corrélation temps réel et « automatique »
- Architecture adaptée à tout type d'entreprise
- Composants clients Open Source

Face à la concurrence…

- Simplicité d'utilisation
- Coûts d'acquisition, de mise en œuvre et d'exploitation
- Moteur de corrélation temps réel, mis à jour en continu
- Évaluation CC en cours

Les bénéfices d'une telle solution

- Diminue les coûts de supervision de la sécurité
- Augmente le niveau de sécurité
- Fournit une vision continue et globale
- Valorise les investissements déjà réalisés

Merci de votre attention …

Île de France :

20, rue Heinrich
92100 BOULOGNE

Siège de Lyon :

Le Palais d'Hiver
149, Boulevard Stalingrad
69100 VILLEURBANNE

Pour plus de détails > http://www.exaprotect.com