Supervision Sécurité : IDS et analyse de logs

Yannick FOURASTIER
RESIST - CERT Onera - Mai 2002
yris@roots.org

Introduction :
Surveiller risques et intrusions logiques

- Surveillance des actions malveillantes et des menaces :
  - Supervision des moyens de protection des installations
  - Vigilance (critères I et C des DICP) par :
    - le contrôle des risques, fonctions des menaces et des vulnérabilités.
    - la réduction et le suivi de ces vulnérabilités,

    ↳ Capacité d'action
    - évaluation des besoins d'évolutions, priorités, plan d'action, etc.

- Constitution des Preuves (critère "P" des DICP).
  - Gestion des traces

    ↳ Capacité de réaction :
    - Forensic
    - Dépôt de plainte

    [Loi 88-15 du 05/01/1988, dite "Godfrain"]
    (Code Penal L2-Ch.III - Art.462-2 à Art.462-9)

- Attention : détection d'intrusion ≠ prévention d'intrusion

Introduction :
Outils de supervision

- Outils de supervision de la sécurité (I.C), entre autres :
  - les sondes (ou scanners) de vulnérabilités distribuées
    - exemple : Nessus, scanners ISS, etc.
  - les sondes de détection d'intrusion
    - exemple : Snort, Prelude, les produits PureSecure, ISS RealSecure, etc.
  - les outils de contrôle d'intégrité
    - exemple : Aide, les produits Le Cid, Tripwire, PureSecure, etc.

- Analyse de logs (P)
  - centralisation
    - exemple : syslog
  - consolidation / agrégation
    - exemple : produits Arcsight, etc.
  - corrélation (maturité faible, peu d'outils)
    - exemple : Psionic Logcheck (abstractions limitées), scripts spécialisés, etc.
  - console de supervision
    - exemple : ACID, demarc PureSecure, etc.

1. Généralités et Rappels

1 - Généralités / Rappels :
Intrusion Detection System

- Qu'est ce que c'est ?
  - IDS = Intrusion Detection System :
    - un composant logiciel ou “matériel” (logiciel embarqué)
  - NIDS vs HIDS :
    - Network IDS : écouter un segment du réseau
    - Host IDS : surveiller un système.
    - Technos à base de signatures, détection d’anomalies, hybrides

- A quoi ça sert ?
  - reconnaissance des tentatives d'intrusions :
    - par analyse des flux réseaux
    - par détection d’un comportement anormal
  - bloquer les tentatives d’intrusion
  - remonter des alertes lorsque des activités suspectes sont détectées

1 - Généralités / Rappels :
“Connais ton ennemi” - Sun Tzu

- Version “consciencieux” :
  - Etape 1 : Reconnaissance externe
    - exploitation des sources d’information publiques
    - cartographie des liens / points d’accès IP / plages CiX
  - Etape 2 : Reconnaissance “directe *in-situ*”
    - scans des plages téléphoniques
    - acquisition d’informations “techniques” (scans, walks snmp/web)
  - Etape 3 : Accès “direct” (misconf) ou exploit
  - Etape 4 : Appropriation
    - modification de l’intégrité du système (rootkit, backdoor, etc.)
  - Etape 5 : Profit - détournement de l’utilisation de la machine
    - rebond, détournement d’informations, etc.

- Version “kiddy” : Birthday Attack ou *exploit* au hasard

1 - Généralités / Rappels :
Stratégie de Supervision

- Quel est l'objectif de la supervision ?
  - Surveiller des menaces ?
  - Surveiller des risques ?
  - Agir sur incident ?
  - Réagir après incident (analyses *post-mortem*)
  - (… se faire plaisir ?)

↳ **Cohérence avec la Politique de Sécurité :**
  - Enjeux métiers
  - Tolérance aux intrusions

- Organiser un "Framework" de supervision :
  - par zones sensibles,
  - par technologies IDS (signature / anomalie)
  - par type NIDS / HIDS / modules Scanners

↳ **Cohésion et mise en œuvre rationalisée des éléments distribués, des relais et des plates-formes de supervision**

1 - Généralités / Rappels :
Implantation et configuration

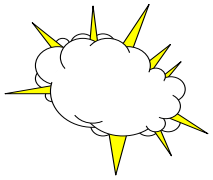
- Pré-requis :
  - Connaître les sensibilités :
    - zone d'implantation des ressources
    - criticité ("importance") de la ressource par rapport au métier
  - Analyse des risques en fonction :
    - des vulnérabilités spécifiques (génériques à minima),
    - des menaces génériques et spécifiques (profil d'attaquant, etc.)
- Mode d'implantation : à quoi faut-il faire attention ?
  - HIDS : impact sur les performances des systèmes hôtes. Bench impératif.
  - NIDS : quid des environnements switchés ? Multi-NICs ou SPAN port ?
- Définir les règles de configuration en fonction :
  - des vulns des plates-formes surveillées (systèmes, applis, etc.) :
  - des menaces à observer (pertinent /métier ou étude sociologique)
- La démarche n'est pas la même si les ressources sont :
  - un NT4 / IIS installé par défaut et non patché en frontal sur l'Internet (un honeypot ?)
  - un Sequent/Dynix au fin fond d'un réseau isolé

1 - Généralités / Rappels :
Implantation : exemple

Extérieur :
- Internet
- Extranet
- Réseau RTC
- etc.

HoneyNet - "Deception System"
honeypots, bridge HogWatch/Snort, etc.

Serveurs en DMZ
HIDS
AIDE, Snort 2.0, etc.



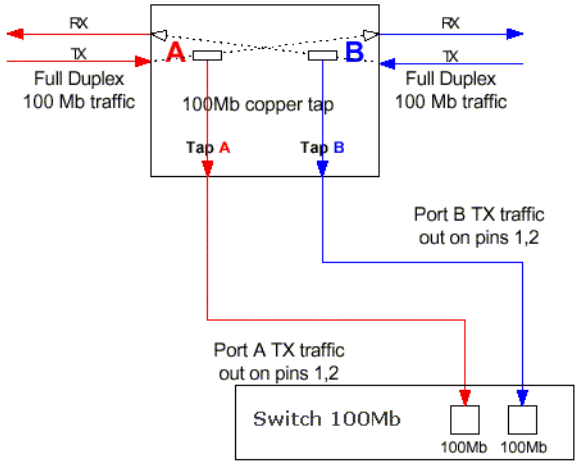
Routeur
ACL / Logs

Tap

Firewall

NIDS

Sonde
Analyse statistique du trafic
NIDS de vigilance



TAP : Duplication des trafics des brins ethernet
TX (emission) et RX (réception)

Classification de la sensibilité des zones :
- Stratégique
- Vital
- Sensible
- Public

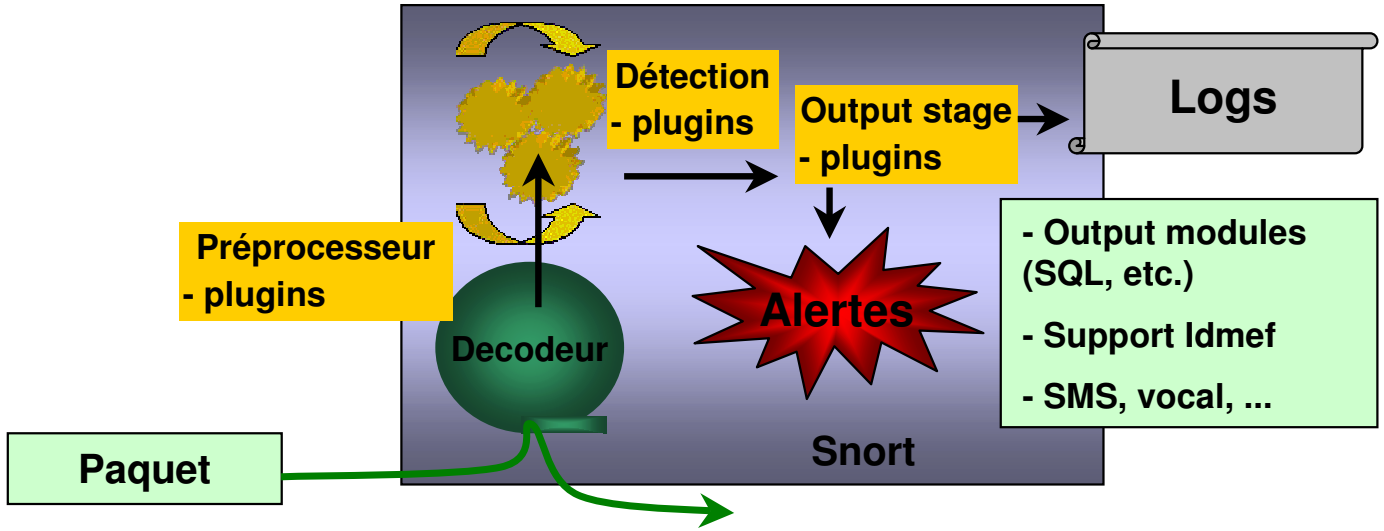
2. Supervision en Pratique : L'IDS Snort

2. Snort : Positionnement
Aide vs Snort : IDS système vs IDS réseau

- Advanced Intrusion Detection Environnment / GPL - Rami Lehti
  - Positionnement : HIDS
  - Technologie : détection d'anomalie système (v. 0.8)
  - Mécanisme :
    - système de contrôle d'intégrité multi hash, avec alerte (comme --> Le CID, TW)
    - apprentissage par constitution d'une base de scellés (p, i, n, u, g, s, m, a, c, S, algo de hash)
    - pas de reconnaissance d'attaque (≠ ISS RS OS Sensor, par exemple)
- Snort / GPL - Martin Roesh
  - Positionnement : NIDS
  - Technologie : base de signature (1.8.6) et prochainement hybride
  - Mécanismes :
    - écoute du réseau
    - détection sur signature (base de signatures >1400 / Snort 1.8.4)
    - modularité :
      - préprocesseurs : ports scans, décodages HTTP, fragments, etc.
      - postprocesseurs : alertes, TCP reset, log.

2. Snort : Présentation

- Architecture



- Configuration des règles :

header **options**

Log	tcp	!192.168.1/24	any	->	172.16./16	25	(msg: “outside finger attempt”;)

proto port IP Dest. Option Option Argument
mot clef

action IP Source direction port ; séparateur

2 - Snort : Objets à connaître

Fichier de configuration et ligne de commande

- Fichier snort.conf :

```
var OURNET 192.168.0.0/24
var OTHERNET !$OURNET
var NIDSHOST 192.168.0.51
var PORTS 10
var SECS 3

#       Log rules
log tcp $OTHERNET any -> $OURNET 23
log tcp $OTHERNET any -> $OURNET 21
log tcp $OTHERNET any -> $OURNET 79
#       Alert Rules
alert udp any any -> $OURNET 53 (msg:"UDP IDS/DNS-version-query"; content:"version";)
alert tcp any any -> $OURNET 53 (msg:"TCP IDS/DNS-version-query"; content:"version";)
alert tcp any any -> $OURNET 80 (msg:"CGI attempt"; content:"/cgi-bin/";)
#       Load portscan pre-processor for portscan alerts
preprocessor portscan: $OTHERNET $PORTS $SECS /var/log/snort/pscan_alerts
preprocessor portscan-ignorehosts: $OURNET
#       Pass Rules (Ignore)
pass tcp $OURNET any -> $OTHERNET 80
pass udp any 1024:  <> any 1024:
pass tcp any 22 -> $NIDSHOST 22
```

- Ligne de commande (exemples sous Unix et sous Windows) :

```
snort -u snort -g snort -s -d -D -i eth0 -l /var/log/snort -c /etc/snort/snort.conf

D:\Snort\program\Binary\snort.exe -l D:\Snort\TEMP -c D:\Snort\Rules\12062k.rules.txt -i 4 -a -e -d -A full
```

2 - Snort 1.x : détails

Régles : sémantique - représentation interne

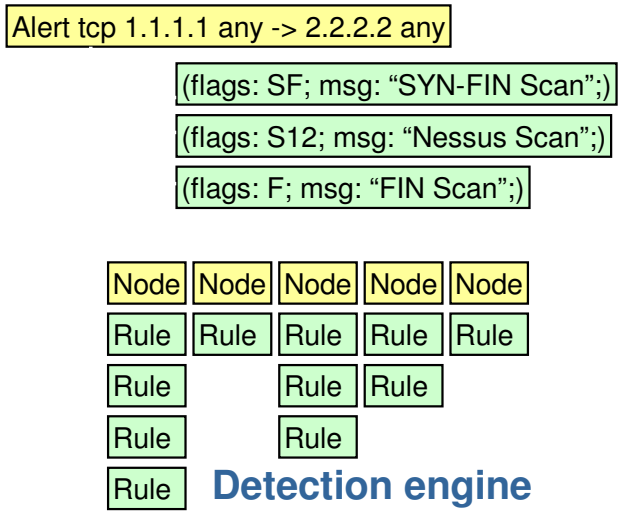
- Implémentation du moteur de détection : listes chaînées en 3D :
  - les dimensions 1 & 2 contiennent les données concernant les nœuds IP à évaluer par rapport au paquet capturé (origine libpcap)
  - la dimension 3 contient des listes chaînées de pointeurs sur fonctions pour tester les nœuds IP par rapport au paquet capturé.
  - tout le traitement est parcouru récursivement ⇒ rapidité / robustesse
  - choix d'implémentation "First exit" :
    - si détection (paquet ; node ; rule) alors la règle est appliquée ;
    - analyse du paquet suivant

- Illustration :

Fichier de configuration

Header de la règle	Options de la règle
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: SF; msg: "SYN-FIN Scan";)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: S12; msg: "Nessus Scan";)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: F; msg: "FIN Scan";)

Représentation interne



2 - Snort : Config. avancée

- Flexibilité de Snort :
  - utilisation des plug-ins :
    - *decoder stage* : préprocesseurs
    - *detection stage* : inclusion de bases de signatures externes
    - *output stage* : postprocesseurs (alerts, logs, modules d'interfaces, SQL, etc.)
  - syntaxe simple :
    - action de la règle : *alert, log, pass*
    - protocole : *tcp, udp, icmp*
    - adresses source et destination :
      - *src, dest, any* + opérateur *!*
      - domaines non supportés
    - port src / dest : *any, nb port*, plage de ports avec *p1:pn* + opérateur *!*
    - opérateur de direction : *-> unidirectionnel*, ou *<-> bidirectionnel*
    - syntaxe des options :
      - combinaison de règles avec le séparateur *;*
      - *séparation du mot clef / argument avec* :
      - mots clefs : *msg, logto, minfrag, ttl, id, dsize, content, offset, depth, flags, seq, ack, itype, idecode, nocase, session*
    - variables de substitution : *var Mon_Net 192.168.0/24*
    - inclusion de fichiers externes : *include : path/fichier*

2 - Snort : Config. avancée

- Faire ses propres règles (attention, case sensitive) :
  - Développer ses propres plugins préprocesseurs (➔ en C)
  - Règle vs plugin de préprocesseur :

```
alert tcp any any -> any any (minfrag: 256; msg: ”Fragmentation, possible activité hostile";)
preprocessor: minfrag 256 any
```

  - Règles surveillant des activités spécifiques :

```
alert tcp any any -> $SRV_Lotus 143 (content: "|90C8 C0FF FFFF|/bin/sh"; msg: "IMAP buffer overflow!";)
alert any any -> $NET_PRODUCTION any (flags: SF; msg: "Possible SYN FIN scan";)
alert TCP $EXTERNAL 6000:6005 -> $INTERNAL any (msg: ”Machine Rootée : Xterm sortant !!! "; flags:
      SA; classtype: system-success;)
```

  - Créer de nouveaux types de règles (en plus de log / alert)

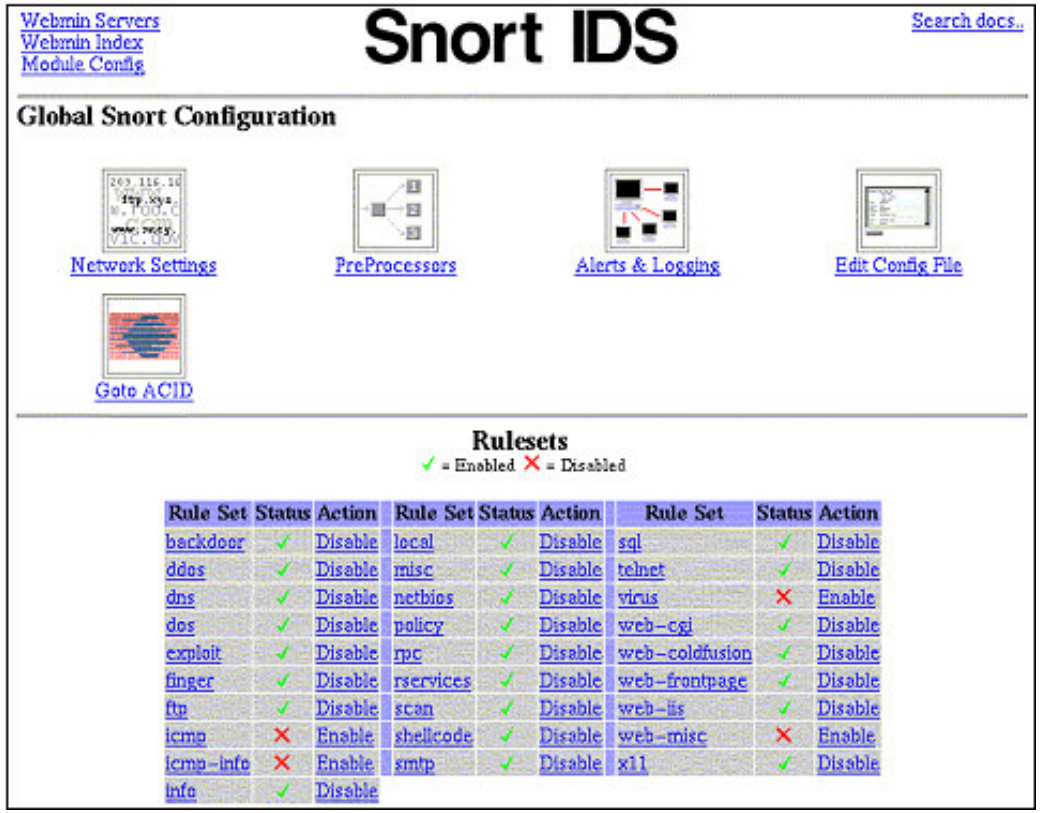
```
ruletype redalert
{
type alert
output alert_syslog: LOG_AUTH LOG_ALERT
output database: log, mysql, user=snort dbname=snort host=localhost
}
```

- Programmer des actions spécifiques :
  - HogWatch, Snort2Iptables ...

2 - Snort : Config. avancée

IDS Management : Fronts ends

- Et pour les récalcitrants du shell et de Vi (ou W32/notepad :) ...:
  - différents front-ends : *demarc PureSecur*, etc.
  - webmin



2 - Snort : Journalisation

- Exemples de logs standard
  - Sous Unix :
    - un fichier par type d'attaque dans /var/log/snort
    - exemple

```
[**] spp_http_decode: IIS Unicode attack detected [**]
05/07-11:10:40.910903 192.168.1.3:3607 -> 192.168.0.1:80
TCP TTL:249 TOS:0x0 ID:22898 IpLen:20 DgmLen:1022 DF
***AP*** Seq: 0x552997B8  Ack: 0xE39D7CB1  Win: 0x4470  TcpLen: 20

[**] IDS198/SYN FIN Scan [**]
05/07-11:38:45.254726 192.168.1.3:53 -> 192.168.0.1:53
TCP TTL:23 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x4D622A79  Ack: 0x7EEF29AF  Win: 0x404  TcpLen: 20
```

  - Sous Windows :
    - adresses des noeuds *src/dest* en sous dossiers de $TEMP\
    - exemples :
      - fichier d'alerte dans le dossier D:\Temp\

```
[**] IDS05 - SCAN-Possible NMAP Fingerprint attempt [**]
05/07-10:05:07.959989 0:60:97:8A:F5:31 -> 0:50:BA:A4:EA:97
 type:0x800 len:0x4A
192.168.1.3:42856 -> 192.168.0.1:139 TCP TTL:51 TOS:0x0 ID:4196
**SF*P*U Seq: 0xA5757576   Ack: 0x0   Win: 0x1000
```

      - fichiers de traces (dump TCP en ASCII) dans des sous dossiers de $Temp\ nommés selon l'IP source (ici 192.168.1.3) et destination (ici 192.168.0.1)

2 - Snort : Compléments

- Richesse fonctionnelle complémentaire, par composants développés pour Snort (plug-ins, librairies, etc.).

- Exemples :
  - LibIDMef : normalisation du format des sorties (logs, alertes, etc.)
  - SGBD :
    - mySQL -./configure --with-mysql
    - Oracle
    - Postgresql
    - unixODBC
  - Spade (*Statistical Packet Anomaly Detection engine*)
  - FlexResp (*Session response/closing*)
  - XML output
  - TCP streams (*stream single-byte reassembly*) : permet de constituer certaines contre-mesures à des outils d'évasions comme *wiskler.pl, fragroute*, etc.
  - snort-panel (Xato) : front-end de management pour Windows.

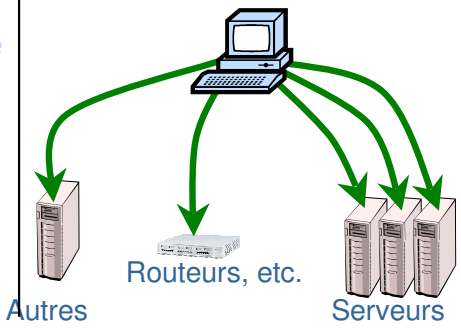
3. Traitement des logs

3 - Traitement des alertes
Centralisation vs Répartition

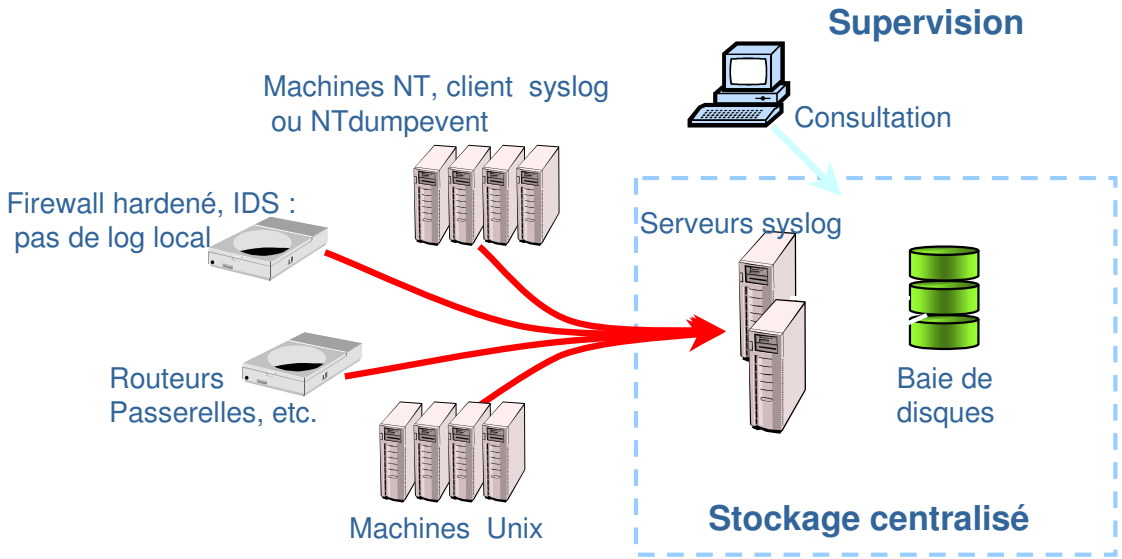
- Type de stockage des traces :
  - Fichier ASCII (par exemple syslog)
  - Fichier binaire d'enregistrements formatés (par exemple, en techno NT : le journal des évènements)

- Mode de stockage :
  - local : sur la machine où l'événement se produit
  - distant : sur une machine dédiée à l'enregistrement des traces

- Exemple :



Stockage local des logs
lorsque possible



3 - Traitement des alertes
Consolidation des évènements

- Des informations d'origines diverses, décrivant un seul et même événement. Par exemple :

Check Point:
"14" "15May2002" "12:10:29" "eth-s1p4c0" "ip.of.firewall" "log"
"accept" "www-http" "65.65.65.65" "10.10.10.10" "tcp" "4" "1355" ""
"" "" "" "" "" "" "" "" "firewall" " len 68"

Cisco Router:
May 15 12:10:27: %SEC-6-IPACCESSLOGP: list 102 permitted tcp
65.65.65.65(1355) -> 10.10.10.10(80), 1 packet

Snort:
[**] [1:971:1] WEB-IIS ISAPI .printer access [**]
[Classification: Attempted Information Leak] [Priority: 3]
05/15-12:10:29.100000 65.65.65.65:1355 -> 10.10.10.10:80
TCP TTL:63 TOS:0x0 ID:5752 IpLen:20 DgmLen:1234 DF
AP Seq: 0xB13810DC Ack: 0xC5D2E066 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 493412860 0
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0241]
[Xref => http://www.whitehats.com/info/IDS533]

- Problème :
  - Schéma de descriptions différents, Stockage important
  - Traitement automatisé difficile, manuel “impossible”

3 - Traitement des alertes
Normalisation des évènements loggués

- Objectifs :
  - simplifier le traitement des logs
  - rendre plus efficient les traitements automatisés

- Moyens :
  - décrire les informations de log selon un modèle standardisé,
  - stocker les résultats de la normalisation dans un dépôt sur lequel l'extraction sera aisé (fichier à plat , SGBD ?)

Exemple : résultat d'une normalisation sur les infos précédentes

Date	Nom_Evt	IP_Src	IP_Dst	Port	Eqt_Orig	Details
15-May-02	Accept	65.65.65.65	10.10.10.10	80	CheckPoint	
15-May-02	List 102 permitted tcp	65.65.65.65	10.10.10.10	80	Cisco Router	
15-May-02	WEB-IIS ISAPI .printer access	65.65.65.65	10.10.10.10	80	Snort	TCP TTL:63 TOS:0x0 ID:5752 IpLen:20 DgmLen:1234 DF ***AP*** Seq: 0xB13810DC Ack: 0xC5D2E066 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 493412860 0

3 - Traitement des alertes
Correlation

- analyse des masses de logs pour attirer l'attention du superviseur sur un événement qui autrement serait passé inaperçu

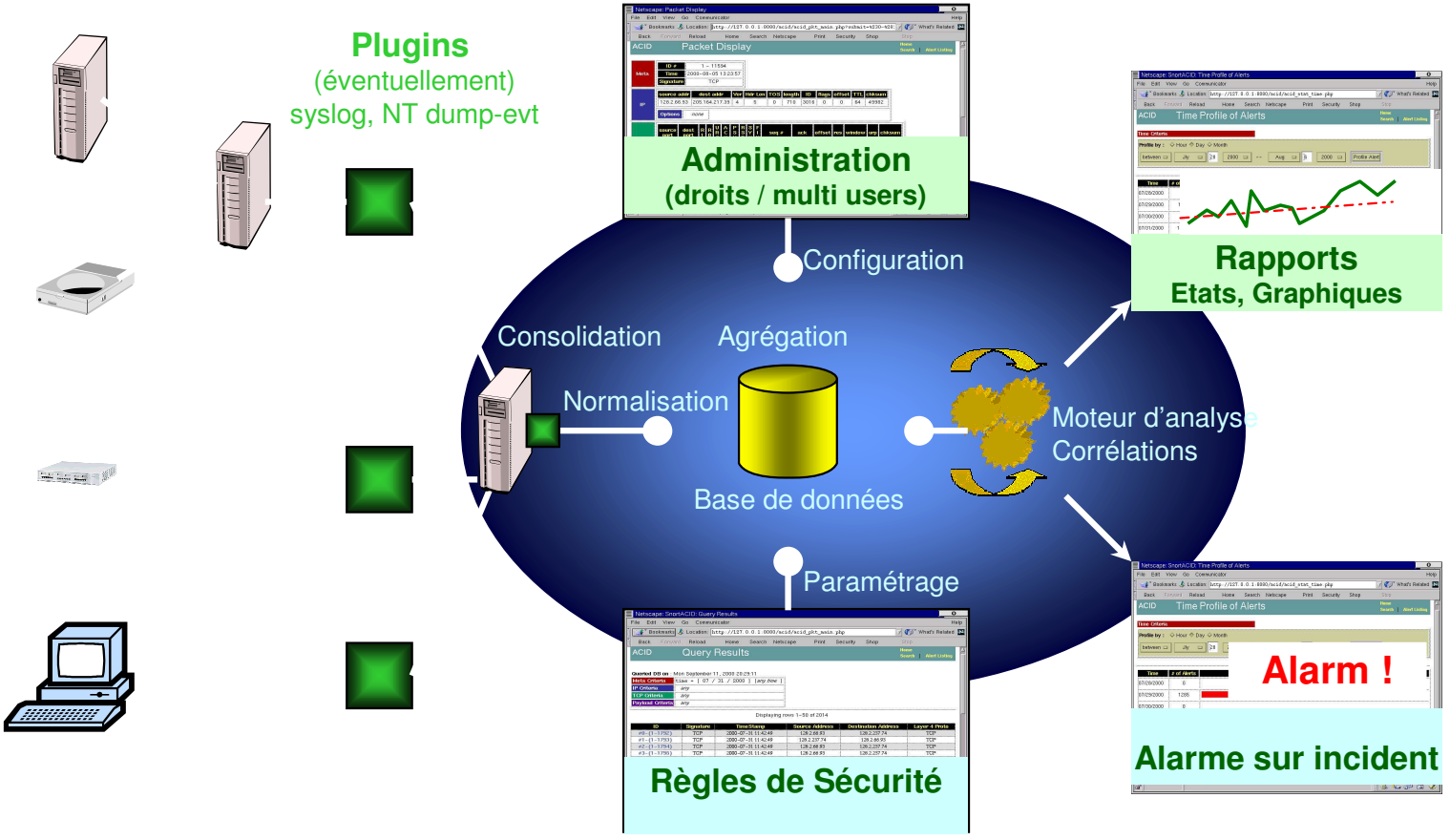
- génération de macro-information par la mise en relation d'attributs décrivant des événements émanant de plusieurs sources :
  - extraction d'informations normalisées
  - analyse des informations de même nature (ex : adresses IP sources, évènements, etc.)
  - mise en relations
  - génération d'une alerte

Date	Nom_Evt	IP_Src	IP_Dst	Port	Eqt_Orig	Details
15-May-02	Accept	65.65.65.65	10.10.10.10	80	CheckPoint	
15-May-02	List 102 permitted tcp	65.65.65.65	10.10.10.10	80	Cisco Router	
15-May-02	WEB-IIS ISAPI .printer access	65.65.65.65	10.10.10.10	80	Snort	TCP TTL:63 TOS:0x0 ID:5752 IpLen:20 DgmLen:1234 DF ***AP*** Seq: 0xB13810DC Ack: 0xC5D2E066 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 493412860 0

3 - Traitement des alertes

Architecture des plates-formes de supervision

Sommaire

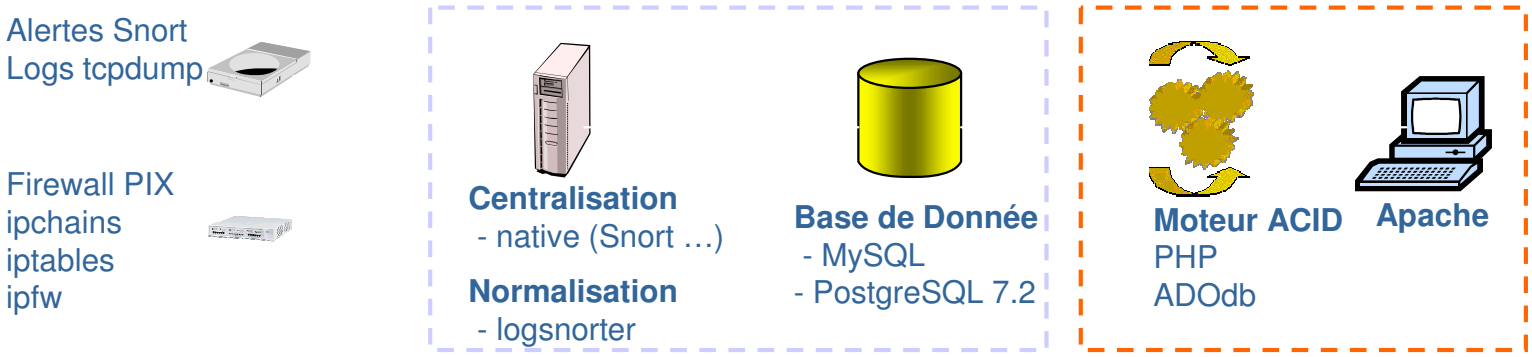


3 - Traitement des alertes

ACID : Présentation générale

- Analysis Console for Intrusion Database
  - AirCert Project - CERT CC - licence GPL
  - moteur d'extraction et d'analyse d'évènements de sécurité:
    - requêteur et interface de recherche
    - éditeur de paquets (décodeur) :
      - affichage des infos layer-3 et 4 des paquets / alertes logguées
    - alert management
      - groupage logique d'alerte pour générer un incident
      - suppression des alertes acquittées et des falses positives identifiées
      - exports, archivages, etc.
    - Graphiques et statistiques

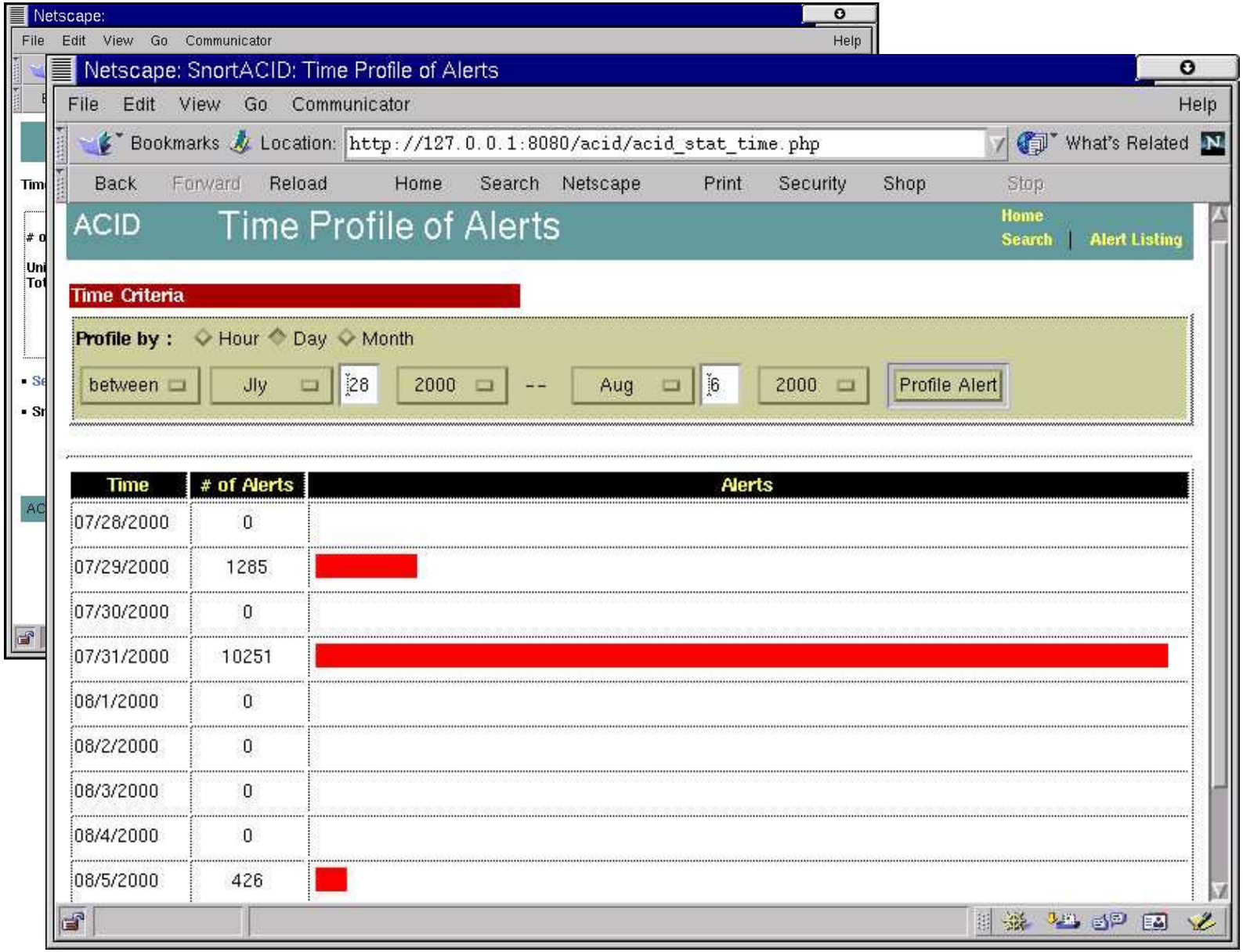
- Architecture de la plate-forme ACID :



3 - Traitement des alertes

ACID : Fonctionnement

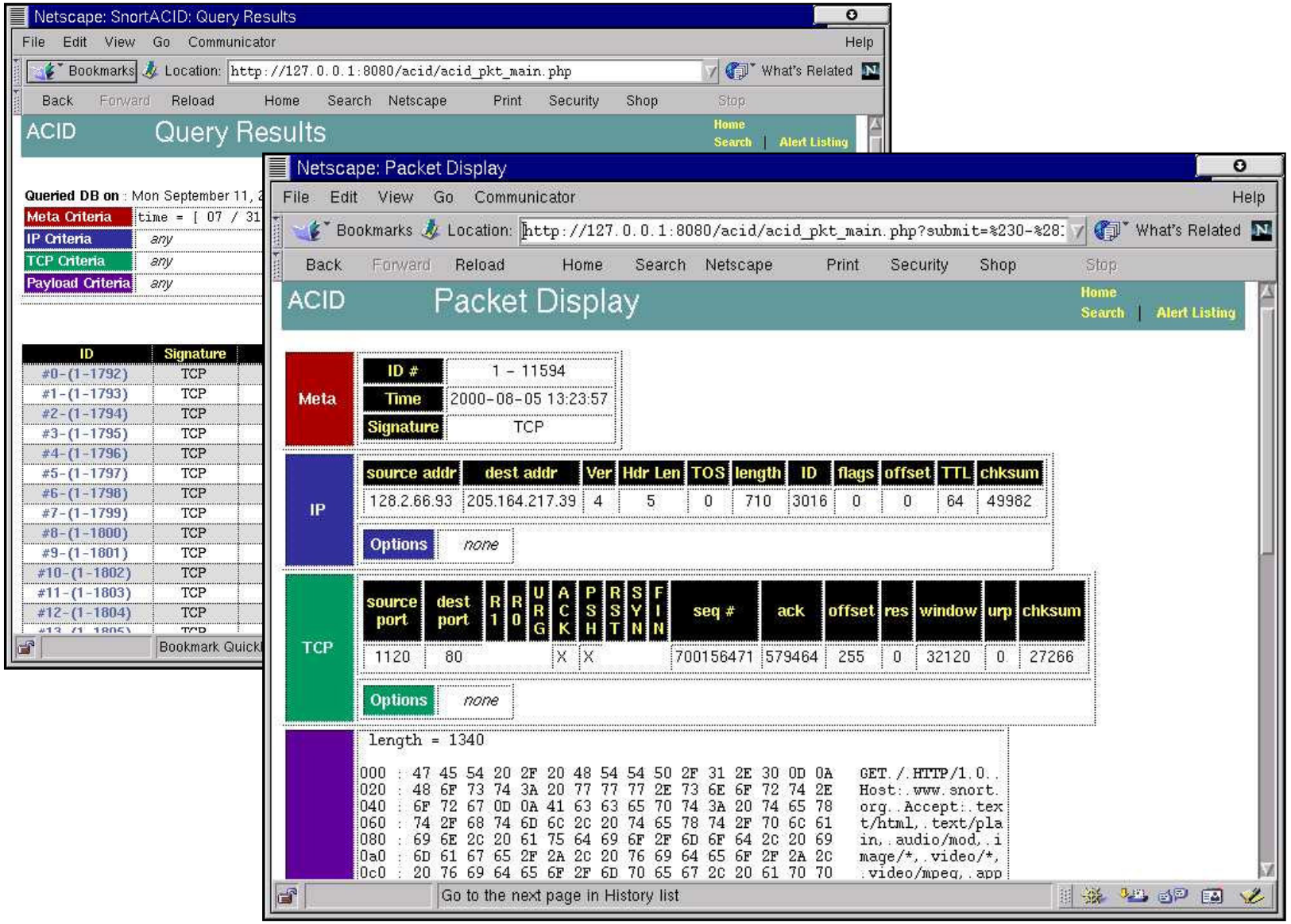
Sommaire



3 - Traitement des alertes

ACID : Mise en œuvre

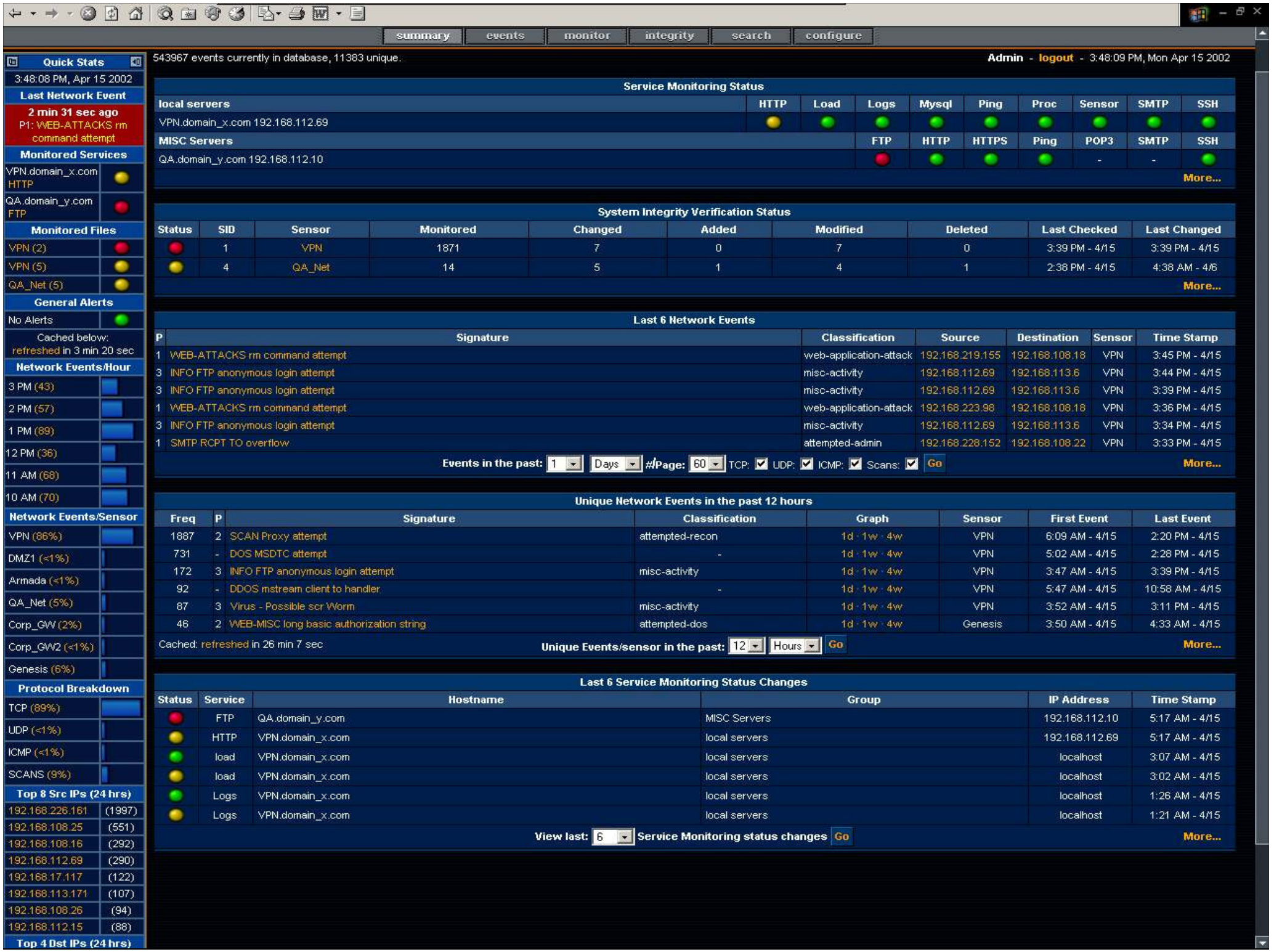
Sommaire

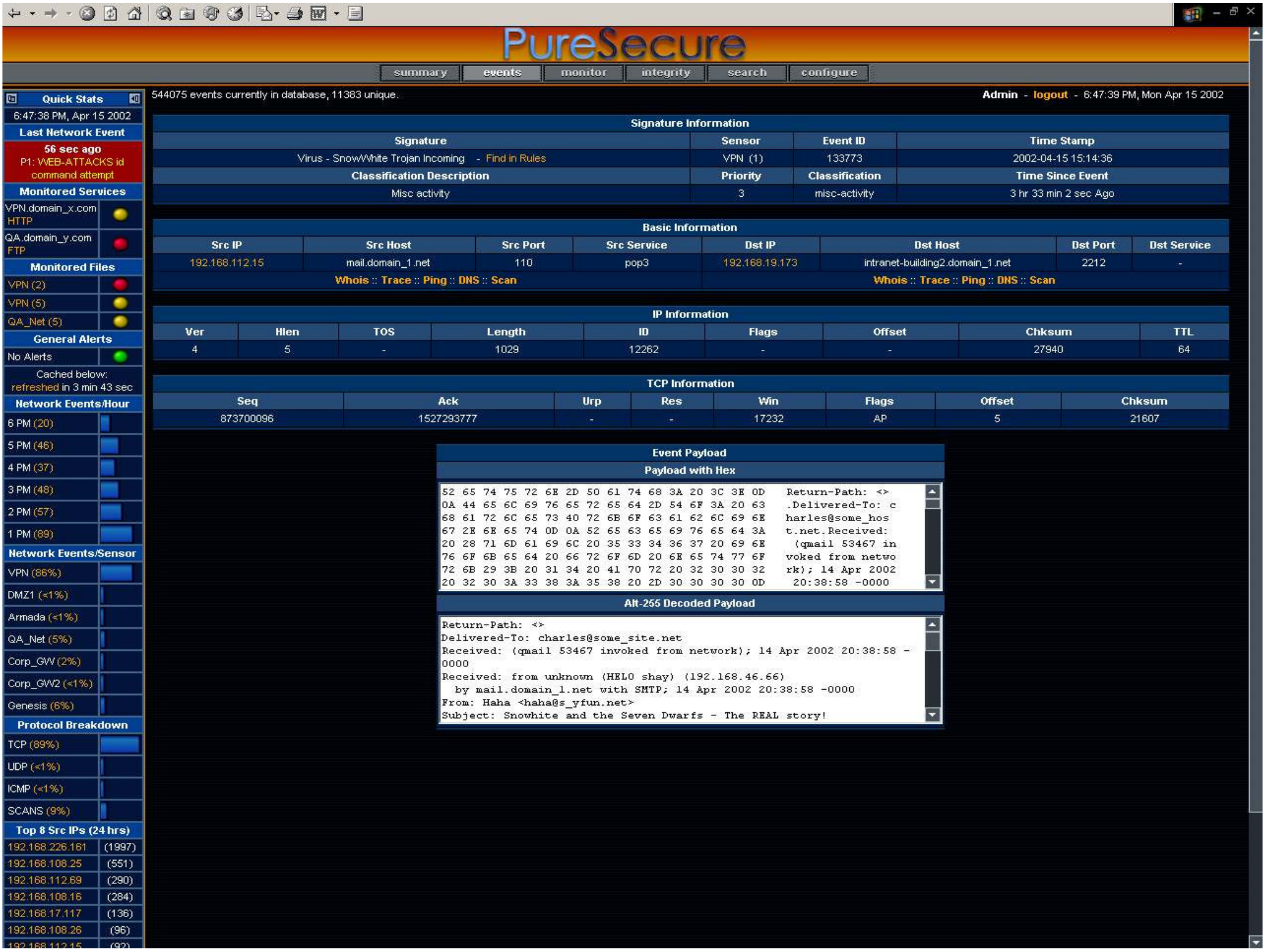


3 - Traitement des alertes
Demarc PureSecure : Présentation

- Pure Secure - Total Intrusion Detection System
  - Produits sous licence propriétaire Demarc :
    - NIDS basé Snort 1.8.6, en appliance rackable 1U
    - Système de contrôle d'intégrité
    - Management front-end
  - Installation simple sous Unix / Windows :
    - de tous les composants nécessaires
    - configuration des éventuels composants externes (mySQL, Apache, etc.)

- Plate-forme complète de supervision de la sécurité :
  - configuration des IDS PureSecure / Snort
  - moteur d'extraction et d'analyse d'èvènements de sécurité:
  - centralisation des alertes de différentes sources de sécurité
  - éditeur de paquets (décodeur) : infos layer-3 et 4 des paquets / alertes logguées
  - alert management - monitoring des équipements
  - Graphiques et statistiques
  - plug-ins : interface perl, etc.


summary
events
monitor
integrity
search
configure
Quick Stats
3:48:08 PM, Apr 15 2002
Last Network Event
2 min 31 sec ago
P1: WEB-ATTACKS rm command attempt
Monitored Services
VPN.domain_x.com HTTP
QA.domain_y.com FTP
Monitored Files
VPN (2)
VPN (5)
QA_Net (5)
General Alerts
No Alerts
Cached below: refreshed in 3 min 20 sec
Network Events/Hour
3 PM (43)
2 PM (57)
1 PM (89)
12 PM (36)
11 AM (68)
10 AM (70)
Network Events/Sensor
VPN (86%)
DMZ1 (<1%)
Armada (<1%)
QA_Net (5%)
Corp_GW (2%)
Corp_GW2 (<1%)
Genesis (6%)
Protocol Breakdown
TCP (89%)
UDP (<1%)
ICMP (<1%)
SCANS (9%)
Top 8 Src IPs (24 hrs)
192.168.226.161 (1997)
192.168.108.25 (551)
192.168.108.16 (292)
192.168.112.69 (290)
192.168.17.117 (122)
192.168.113.171 (107)
192.168.108.26 (94)
192.168.112.15 (88)
Top 4 Dst IPs (24 hrs)
543967 events currently in database, 11383 unique.
Admin - logout - 3:48:09 PM, Mon Apr 15 2002
Service Monitoring Status
local servers HTTP Load Logs Mysql Ping Proc Sensor SMTP SSH
VPN.domain_x.com 192.168.112.69
MISC Servers FTP HTTP HTTPS Ping POP3 SMTP SSH
QA.domain_y.com 192.168.112.10
More...
System Integrity Verification Status
Status SID Sensor Monitored Changed Added Modified Deleted Last Checked Last Changed
1 VPN 1871 7 0 7 0 3:39 PM - 4/15 3:39 PM - 4/15
4 QA_Net 14 5 1 4 1 2:38 PM - 4/15 4:38 AM - 4/6
More...
Last 6 Network Events
P Signature Classification Source Destination Sensor Time Stamp
1 WEB-ATTACKS rm command attempt web-application-attack 192.168.219.155 192.168.108.18 VPN 3:45 PM - 4/15
3 INFO FTP anonymous login attempt misc-activity 192.168.112.69 192.168.113.6 VPN 3:44 PM - 4/15
3 INFO FTP anonymous login attempt misc-activity 192.168.112.69 192.168.113.6 VPN 3:39 PM - 4/15
1 WEB-ATTACKS rm command attempt web-application-attack 192.168.223.98 192.168.108.18 VPN 3:36 PM - 4/15
3 INFO FTP anonymous login attempt misc-activity 192.168.112.69 192.168.113.6 VPN 3:34 PM - 4/15
1 SMTP RCPT TO overflow attempted-admin 192.168.228.152 192.168.108.22 VPN 3:33 PM - 4/15
Events in the past: 1 Days #/Page: 60 TCP: UDP: ICMP: Scans: Go
More...
Unique Network Events in the past 12 hours
Freq P Signature Classification Graph Sensor First Event Last Event
1887 2 SCAN Proxy attempt attempted-recon 1d · 1w · 4w VPN 6:09 AM - 4/15 2:20 PM - 4/15
731 - DOS MSDTC attempt - 1d · 1w · 4w VPN 5:02 AM - 4/15 2:28 PM - 4/15
172 3 INFO FTP anonymous login attempt misc-activity 1d · 1w · 4w VPN 3:47 AM - 4/15 3:39 PM - 4/15
92 - DDOS mstream client to handler - 1d · 1w · 4w VPN 5:47 AM - 4/15 10:58 AM - 4/15
87 3 Virus - Possible scr Worm misc-activity 1d · 1w · 4w VPN 3:52 AM - 4/15 3:11 PM - 4/15
46 2 WEB-MISC long basic authorization string attempted-dos 1d · 1w · 4w Genesis 3:50 AM - 4/15 4:33 AM - 4/15
Cached: refreshed in 26 min 7 sec
Unique Events/sensor in the past: 12 Hours Go
More...
Last 6 Service Monitoring Status Changes
Status Service Hostname Group IP Address Time Stamp
FTP QA.domain_y.com MISC Servers 192.168.112.10 5:17 AM - 4/15
HTTP VPN.domain_x.com local servers 192.168.112.69 5:17 AM - 4/15
load VPN.domain_x.com local servers localhost 3:07 AM - 4/15
load VPN.domain_x.com local servers localhost 3:02 AM - 4/15
Logs VPN.domain_x.com local servers localhost 1:26 AM - 4/15
Logs VPN.domain_x.com local servers localhost 1:21 AM - 4/15
View last: 6 Service Monitoring status changes Go
More...


PureSecure
summary
events
monitor
integrity
search
configure
544075 events currently in database, 11383 unique.
Admin - logout - 6:47:39 PM, Mon Apr 15 2002
Quick Stats
6:47:38 PM, Apr 15 2002
Last Network Event
56 sec ago
P1: WEB-ATTACKS id command attempt
Monitored Services
VPN.domain_x.com HTTP
QA.domain_y.com FTP
Monitored Files
VPN (2)
VPN (5)
QA_Net (5)
General Alerts
No Alerts
Cached below: refreshed in 3 min 43 sec
Network Events/Hour
6 PM (20)
5 PM (46)
4 PM (37)
3 PM (48)
2 PM (57)
1 PM (89)
Network Events/Sensor
VPN (86%)
DMZ1 (<1%)
Armada (<1%)
QA_Net (5%)
Corp_GW (2%)
Corp_GW2 (<1%)
Genesis (6%)
Protocol Breakdown
TCP (89%)
UDP (<1%)
ICMP (<1%)
SCANS (9%)
Top 8 Src IPs (24 hrs)
192.168.226.161 (1997)
192.168.108.25 (551)
192.168.112.69 (290)
192.168.108.16 (284)
192.168.17.117 (136)
192.168.108.26 (96)
192.168.112.15 (92)
Signature Information
Signature
Virus - SnowWhite Trojan Incoming - Find in Rules
Sensor
VPN (1)
Event ID
133773
Time Stamp
2002-04-15 15:14:36
Classification Description
Misc activity
Priority
3
Classification
misc-activity
Time Since Event
3 hr 33 min 2 sec Ago
Basic Information
Src IP
192.168.112.15
Src Host
mail.domain_1.net
Src Port
110
Src Service
pop3
Dst IP
192.168.19.173
Dst Host
intranet-building2.domain_1.net
Dst Port
2212
Dst Service
-
Whois :: Trace :: Ping :: DNS :: Scan
Whois :: Trace :: Ping :: DNS :: Scan
IP Information
Ver
4
Hlen
5
TOS
-
Length
1029
ID
12262
Flags
-
Offset
-
Chksum
27940
TTL
64
TCP Information
Seq
873700096
Ack
1527293777
Urp
-
Res
-
Win
17232
Flags
AP
Offset
5
Chksum
21607
Event Payload
Payload with Hex
52 65 74 75 72 6E 2D 50 61 74 68 3A 20 3C 3E 0D Return-Path: <>
0A 44 65 6C 69 76 65 72 65 64 2D 54 6F 3A 20 63 .Delivered-To: c
68 61 72 6C 65 73 40 72 6B 6F 63 61 62 6C 69 6E harles@some_hos
67 2E 6E 65 74 0D 0A 52 65 63 65 69 76 65 64 3A t.net.Received:
20 28 71 6D 61 69 6C 20 35 33 34 36 37 20 69 6E (qmail 53467 in
76 6F 6B 65 64 20 66 72 6F 6D 20 6E 65 74 77 6F voked from netwo
72 6B 29 3B 20 31 34 20 41 70 72 20 32 30 30 32 rk); 14 Apr 2002
20 32 30 3A 33 38 3A 35 38 20 2D 30 30 30 30 0D 20:38:58 -0000
Alt-255 Decoded Payload
Return-Path: <>
Delivered-To: charles@some_site.net
Received: (qmail 53467 invoked from network); 14 Apr 2002 20:38:58 -0000
Received: from unknown (HELO shay) (192.168.46.66)
by mail.domain_1.net with SMTP; 14 Apr 2002 20:38:58 -0000
From: Haha <haha@s_yfun.net>
Subject: Snowhite and the Seven Dwarfs - The REAL story!


summary
events
monitor
integrity
search
configure
543970 events currently in database, 11383 unique.
Admin - logout - 3:50:52 PM, Mon Apr 15 2002
Quick Stats
3:50:51 PM, Apr 15 2002
Last Network Event
49 sec ago
P2: ATTACK RESPONSES command completed
Monitored Services
VPN.domain_x.com HTTP
QA.domain_y.com FTP
Monitored Files
VPN (2)
VPN (5)
QA_Net (5)
General Alerts
No Alerts
Cached below: refreshed in 37 sec
Network Events/Hour
3 PM (43)
2 PM (57)
1 PM (89)
12 PM (36)
11 AM (68)
10 AM (70)
Network Events/Sensor
VPN (86%)
DMZ1 (<1%)
Armada (<1%)
QA_Net (5%)
Corp_GW (2%)
Corp_GW2 (<1%)
Genesis (6%)
Protocol Breakdown
TCP (89%)
UDP (<1%)
ICMP (<1%)
SCANS (9%)
Top 8 Src IPs (24 hrs)
192.168.226.161 (1997)
192.168.108.25 (551)
192.168.108.16 (292)
192.168.112.69 (290)
192.168.17.117 (122)
192.168.113.171 (107)
192.168.108.26 (94)
192.168.112.15 (88)
Top 4 Dst IPs (24 hrs)
Service Monitoring Status
domain_1 DNS Servers
Dad
Disks
DNS
IMAP4
Load
Ping
POP3
Sensor
TCP
192.168.0.1 (192.168.0.1)
QA_Net.domain_1.com (192.168.113.10)
local servers
HTTP
Load
Logs
Mysql
Ping
Proc
Sensor
SMTP
SSH
VPN.domain_x.com (192.168.112.69)
MISC Servers
FTP
HTTP
HTTPS
Ping
POP3
SMTP
SSH
Corp_GW.domain_1.org (192.168.117.102)
QA.domain_y.com (192.168.112.10)
vulcan.domain_1.com (192.168.113.6)
Other Servers
Disks
Load
Logs
NNTP
Ping
Proc
Sensor
192.168.17.117 (192.168.17.117)
news.domain_1.com (192.168.90.101)
Genesis.domain_1.com
routers
Ciscocpu
Disks
Ping
Telnet
genesis.domain_1.com (192.168.112.1)
20 Most Recent Service Status Changes
Status
Service
Hostname
Group
IP Address
Time Stamp
FTP QA.domain_y.com MISC Servers 192.168.112.10 5:17 AM - 4/15
HTTP VPN.domain_x.com local servers 192.168.112.69 5:17 AM - 4/15
load VPN.domain_x.com local servers localhost 3:07 AM - 4/15
load VPN.domain_x.com local servers localhost 3:02 AM - 4/15
Logs VPN.domain_x.com local servers localhost 1:26 AM - 4/15
Logs VPN.domain_x.com local servers localhost 1:21 AM - 4/15
Logs VPN.domain_x.com local servers localhost 9:16 PM - 4/14
Logs VPN.domain_x.com local servers localhost 9:09 PM - 4/14
Logs VPN.domain_x.com local servers localhost 9:08 PM - 4/14
Logs VPN.domain_x.com local servers localhost 9:03 PM - 4/14
Logs VPN.domain_x.com local servers localhost 8:48 PM - 4/14
Logs VPN.domain_x.com local servers localhost 8:43 PM - 4/14
Ping 192.168.17.117 Other Servers 192.168.17.117 7:06 PM - 4/14
ciscocpu genesis.domain_1.com routers localhost 7:01 PM - 4/14
ciscocpu genesis.domain_1.com routers localhost 6:56 PM - 4/14
Ping 192.168.17.117 Other Servers 192.168.17.117 6:27 PM - 4/14
Logs VPN.domain_x.com local servers localhost 3:48 AM - 4/14
Logs VPN.domain_x.com local servers localhost 3:43 AM - 4/14
Logs VPN.domain_x.com local servers localhost 3:34 AM - 4/14
HTTP VPN.domain_x.com local servers 192.168.112.69 3:29 AM - 4/14
View last: 20 Service Monitoring status changes Go

summary | events | monitor | integrity | search | configure

543970 events currently in database, 11383 unique.

Admin - logout - 3:51:38 PM, Mon Apr 15 2002

Quick Stats

3:51:36 PM, Apr 15 2002

Last Network Event

1 min 34 sec ago
P2: ATTACK RESPONSES command completed

Monitored Services

VPN.domain_x.com HTTP	
QA.domain_y.com FTP	

Monitored Files

VPN (2)	
VPN (5)	
QA_Net (5)	

General Alerts

No Alerts	

Network Events/Hour

3 PM (46)	
2 PM (57)	
1 PM (89)	
12 PM (36)	
11 AM (68)	
10 AM (70)	

Network Events/Sensor

VPN (86%)	
DMZ1 (<1%)	
Armada (<1%)	
QA_Net (5%)	
Corp_GW (2%)	
Corp_GW2 (<1%)	
Genesis (6%)	

Protocol Breakdown

TCP (89%)	
UDP (<1%)	
ICMP (<1%)	
SCANS (9%)	

Top 8 Src IPs (24 hrs)

192.168.226.161	(1997)
192.168.108.25	(551)
192.168.108.16	(292)
192.168.112.69	(290)
192.168.17.117	(122)
192.168.113.171	(107)
192.168.108.26	(96)
192.168.112.15	(88)

Top 4 Dst IPs (24 hrs)

192.168.103.26	(470)
192.168.113.6	(299)

System Integrity Verification

Status	SID	Sensor	Monitored	Changed	Added	Modified	Deleted	Last Checked	Last Changed
	1	VPN	1871	7	0	7	0	3:39 PM - 4/15	3:39 PM - 4/15
	2	DMZ1	21	0	0	0	0	4:03 PM - 1/13	4:03 PM - 1/13
	3	Armada	207	0	0	0	0	7:46 AM - 4/14	7:46 AM - 4/14
	4	QA_Net	14	5	1	4	1	2:38 PM - 4/15	4:38 AM - 4/6
	5	Corp_GW	176	0	0	0	0	6:31 PM - 4/1	6:31 PM - 4/1

Confirm All Changes

1 - VPN (1871 files currently being monitored)

/etc/master.passwd — **Last Change Observed:** 5:37 AM - 4/15

Description: System Master Passwd File (w/shadow passwords)

MODIFIED FILE

	Expected	Observed
INODE:	79670	79668
MTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002
CTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002

/etc/passwd — **Last Change Observed:** 5:37 AM - 4/15

Description: System Password file

MODIFIED FILE

	Expected	Observed
INODE:	80380	80382
MTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002
CTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002

/etc/master.passwd — **Last Change Observed:** 5:37 AM - 4/15

Description: System Config Files

MODIFIED FILE

	Expected	Observed
INODE:	79670	79668
MTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002
CTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002

/etc/spwd.db — **Last Change Observed:** 5:37 AM - 4/15

Description: System Config Files

MODIFIED FILE

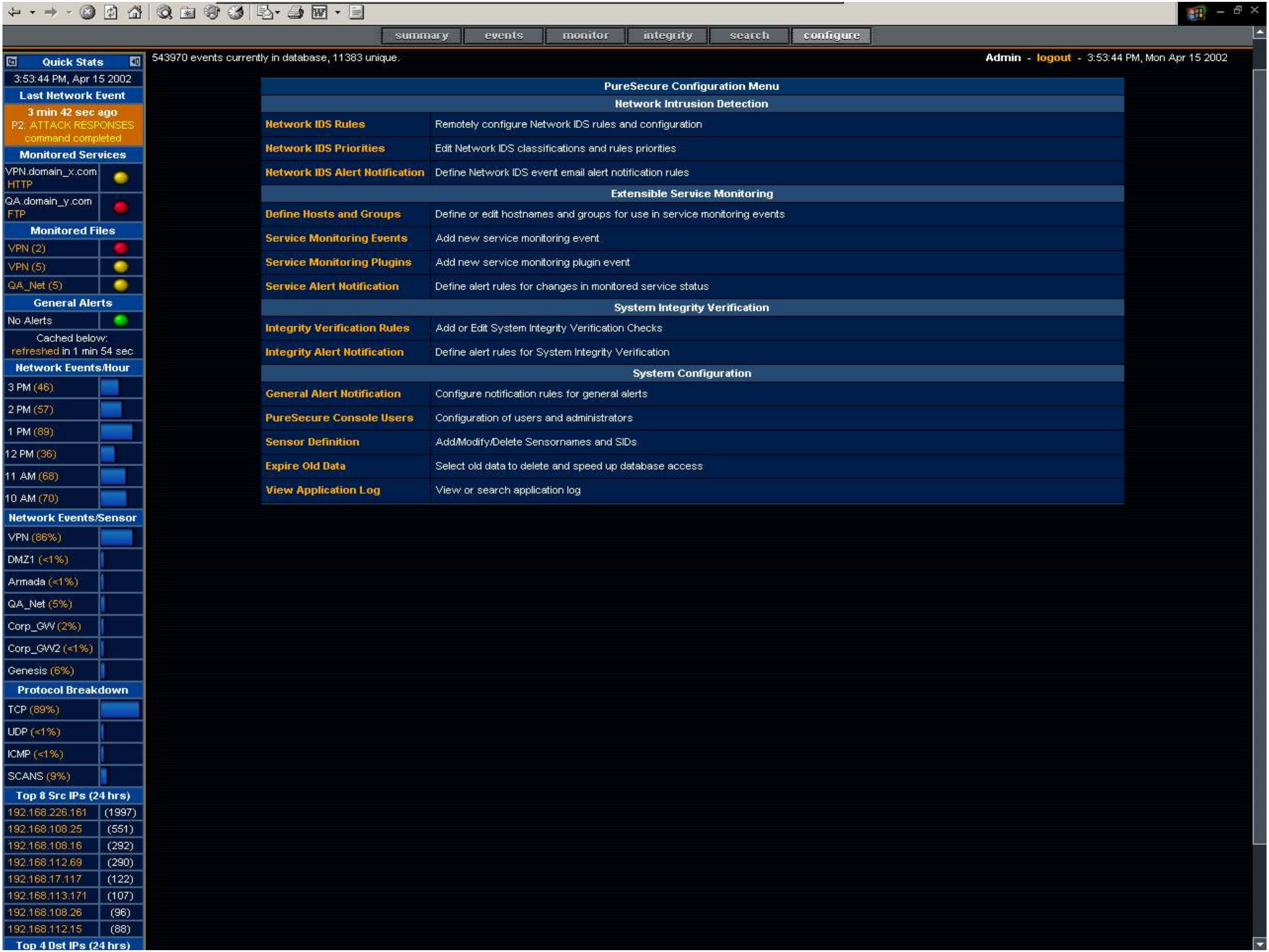
	Expected	Observed
INODE:	80379	80381
MTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002
CTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002

/etc/passwd — **Last Change Observed:** 5:37 AM - 4/15

Description: System Config Files

MODIFIED FILE

	Expected	Observed
INODE:	80380	80382
MTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002
CTIME:	Tue Apr 9 00:44:57 2002	Mon Apr 15 04:34:36 2002


summary
events
monitor
integrity
search
configure
Quick Stats
3:53:44 PM, Apr 15 2002
Last Network Event
3 min 42 sec ago
P2: ATTACK RESPONSES command completed
Monitored Services
VPN.domain_x.com HTTP
QA.domain_y.com FTP
Monitored Files
VPN (2)
VPN (5)
QA_Net (5)
General Alerts
No Alerts
Cached below: refreshed in 1 min 54 sec
Network Events/Hour
3 PM (46)
2 PM (57)
1 PM (89)
12 PM (36)
11 AM (68)
10 AM (70)
Network Events/Sensor
VPN (86%)
DMZ1 (<1%)
Armada (<1%)
QA_Net (5%)
Corp_GW (2%)
Corp_GW2 (<1%)
Genesis (6%)
Protocol Breakdown
TCP (89%)
UDP (<1%)
ICMP (<1%)
SCANS (9%)
Top 8 Src IPs (24 hrs)
192.168.226.161 (1997)
192.168.108.25 (551)
192.168.108.16 (292)
192.168.112.69 (290)
192.168.17.117 (122)
192.168.113.171 (107)
192.168.108.26 (96)
192.168.112.15 (88)
Top 4 Dst IPs (24 hrs)
543970 events currently in database, 11383 unique.
Admin - logout - 3:53:44 PM, Mon Apr 15 2002
PureSecure Configuration Menu
Network Intrusion Detection
Network IDS Rules
Remotely configure Network IDS rules and configuration
Network IDS Priorities
Edit Network IDS classifications and rules priorities
Network IDS Alert Notification
Define Network IDS event email alert notification rules
Extensible Service Monitoring
Define Hosts and Groups
Define or edit hostnames and groups for use in service monitoring events
Service Monitoring Events
Add new service monitoring event
Service Monitoring Plugins
Add new service monitoring plugin event
Service Alert Notification
Define alert rules for changes in monitored service status
System Integrity Verification
Integrity Verification Rules
Add or Edit System Integrity Verification Checks
Integrity Alert Notification
Define alert rules for System Integrity Verification
System Configuration
General Alert Notification
Configure notification rules for general alerts
PureSecure Console Users
Configuration of users and administrators
Sensor Definition
Add/Modify/Delete Sensornames and SIDs
Expire Old Data
Select old data to delete and speed up database access
View Application Log
View or search application log

3 - Traitement des logs
Organisation de la gestion d'alerte

- La gestion des logs a des implications :
  - légale : CNIL, jurisprudence sur la surveillance en entreprise, etc.
  - organisationnelle : durée, qui fait quoi, qui décide, etc.

- Que faire en cas d'alerte ?
  - … rester calme et identifier la réalité de l'attaque
  - enregistrer toute l'activité provenant de la source attaquante
    - ↳ utiliser les fonctions d'enregistrement filtré des NIDS ou un sniffer portable
  - isoler la cible attaquée (utilité d'une bonne correlation !)
    - ↳ dans les limites des contraintes de disponibilité (qui peut être fonction d'un SLA)
  - prévenir le responsable de la sécurité (RSSI) a minima,
  - bloquer ou laisser continuer l'attaque ?
    - ↳ la détourner sur un honeypot en agissant sur les règles de routage ?
  - déposer plainte le cas échéant
    - ↳ attention : les lois du Far West ne s'appliquent pas en France, aussi ne pas agresser (attaque logique) l'attaquant !….
    - ↳ ne rien faire contribue à laisser se répandre un sentiment d'impunité que l'on paiera plus tard : l'attaquant aura développé ses compétences et sa confiance !

Synthèse et Bilan

Conclusion
Bilan

- Implantation en fonction :
  - des besoins réels, rationnalisés par rapport aux enjeux métiers
  - des possibilités techniques de l'environnement
- Snort un NIDS performant et multifonctions mais qui n'échappe pas complètement aux limites des IDS :
  - les techniques d'évasion (par fragmentation, rejeux, flood, etc.)
  - les falses positives : attention à la configuration fine / contexte !
- Ecueils à éviter (rappels)
  - les IDS ne dispensent pas de …patcher, configurer les plates-formes, les suivre correctement (administrer ?) !
  - ne pas considérer les IDS comme des "produits" sur étagère
  - implanter des IDS, sans réflexion préalable, ni organisation pour les exploiter ne sert à rien !
- Organiser l'administration de la Sécurité

Conclusion
Tendances technologiques et évolutions

- Globalement les technologies IDS sont mûres :
  - peu d'évolutions majeures sur les implémentations à base de signature :
    - le modèle de détection de snort est considéré comme le plus efficace et performant par les majors du secteur (ISS, Cisco, etc.)
    - A noter : l'usage de plus en plus fréquent d'IDMef pour la normalisation des logs, et la normalisation des modèles de classification des risques.

- Les tendances :
  - détection d'anomalie
    - intégration de fonctionnalités nouvelles, prêtes sur le plan théorique depuis 2 ans (*A strict anomalie detection model for IDS* par sasha et beetle, *Phrack 56* - volume \0xa, issue \0x38 du 5 janvier 2000)
    - les implémentations consistent aujourd'hui à travailler sur des techniques d'IA d'apprentissage à base de réseaux neuronaux (neural net)
    - Stide : IDS capable de reconnaitre des attaques non connues ou déguisées
  - correlation d'évènements
    - adaptation des principes mis en œuvre dans les outils de *datamining* et de *business intelligence*

Conclusion

Ressources ... *"Si vis pacem, para bellum"*

Jules Cesar

- www.snort.org/dl/snort-1.8.6.tar.gz (tarball sources)
- www.snort.org/dl/binaries/ (packages *BSD, Solaris, RPMs, et Win32 sources et exe)
- www.snort.org/docs/writing_rules/
- www.nessus.org
- www.cert.org/kb/acid
- www.whitehats.com (base de signatures, ArachNIDS)
- www.incidents.org/snortdb (base de signatures)
- www.securityfocus.com (base de signatures, whitepapers)
- cve.mitre.org (base de signatures)
- www.psionic.com/ (logcheck + hostsentry + portsentry)
- www.demarc.com (PureSecure)

- proxy.11a.nu/papers_gsec_2001.html (howto pour construire et manager un cluster de NIDS Snort sous FreeBSD avec ACID/MySQL (+ssh, rsync, etc.)
- www.infosys.tuwien.ac.at/Staff/chris/doc/2002_03.ps (*Service Specific Anomaly Detection for Network Intrusion Detection*)
- www.infosys.tuwien.ac.at/Staff/chris/doc/2002_04.ps （*Stateful Intrusion Detection for High-Speed Networks*)
- www-2.cs.cmu.edu/afs/cs.cmu.edu/user/maxion/www/pubs/TanMaxion02.pdf (*dernières évolutions de l 'IDS à détection d'anomalie stide et résultats empiriques)*
- www.sdl.sri.com/papers/o/a/oakland02/oakland02.pdf (exemple de mise en œuvre des principes de tolérance d'intrusion dans « Enclaves », environnement supportant des groupes sécurisés d'application).