5ème année
Réseaux et Télécommunications

Systèmes de détection d'intrusion

INSA de Toulouse

Rodolphe Ortalo
RSSI - CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Présentation du cours

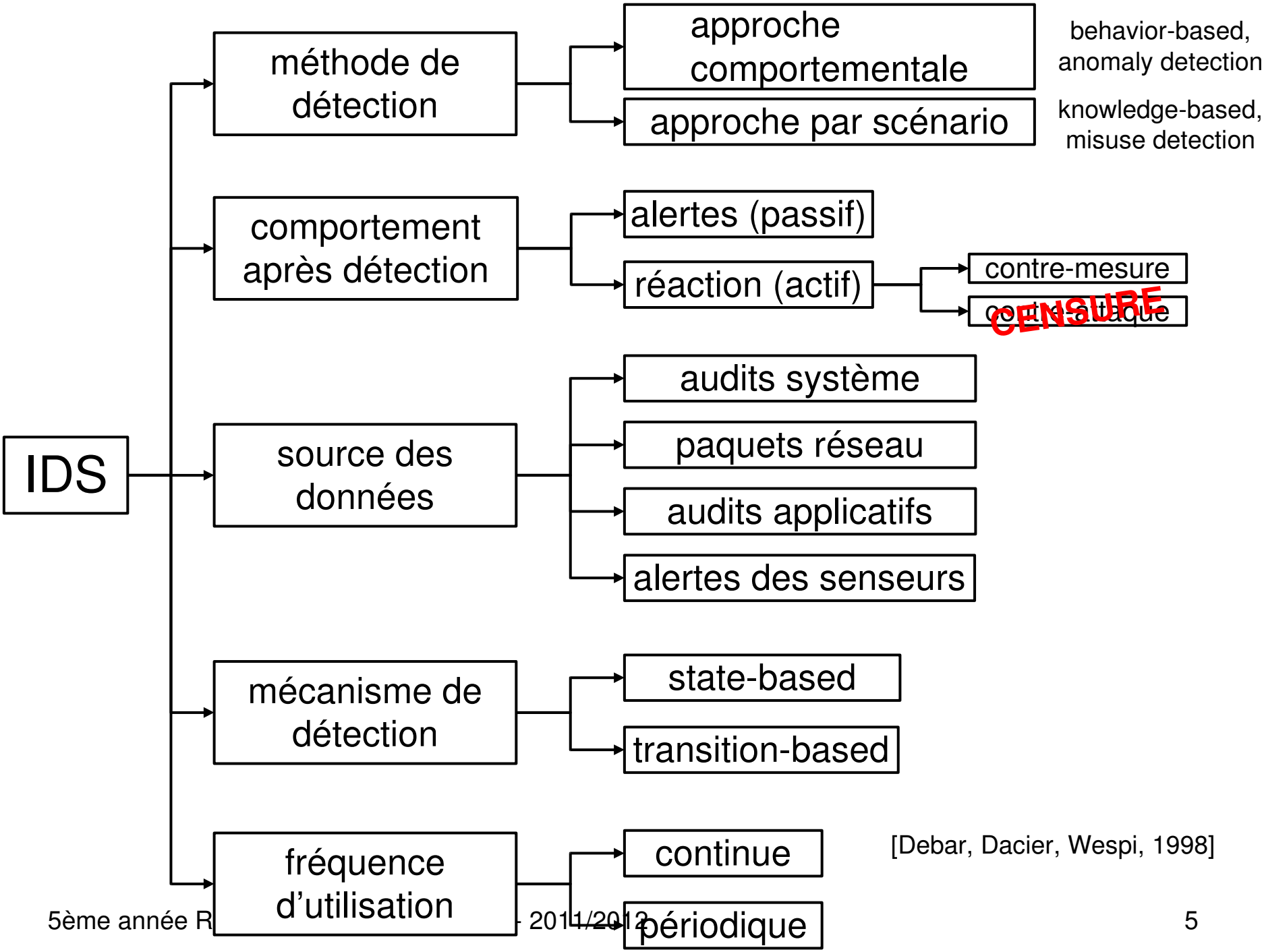
- Terminologie
- Détection d'intrusion
  - Approches étudiées et tendances
  - Mise en oeuvre
  - Architecture
  - Sondes réseau
    - Exemple de snort
    - Outils associés et consoles
  - Traitement des alertes (problèmes, corrélation)
- Lien avec des fonctions de protection courantes
  - Centralisation des traces
    - Syslog et volumétrie
    - Contrôleurs de domaine Windows
  - Système antivirus (exemple)
- Outils complémentaires
  - Analyse réseau
  - Contrôle d'intégrité des fichiers

Vulnérabilités – Attaques – Alertes

- Vulnérabilités
  - Grande variété : *buffer overflow*, CGI, droits d'accès permissifs, interception de sessions réseaux, transferts de privilèges, *social engineering*, cryptanalyse, etc.
- « Attaque »
  - Exploitation d'une vulnérabilité
  - Attaque élémentaire ou scénario d'intrusion
  - Action malveillante ou suspecte
- Alertes
  - Message résultant de la détection d'une attaque
  - *IDMEF (XML): Intrusion Detection Message Exchange Format défini par l'IETF/IDWG*

Génération d'alertes (efficacité)

	Pas d'alerte	Alerte
Pas d'attaque	Vrai négatif ☺	Faux positif ☹
Attaque en cours	Faux négatif ☹	Vrai positif ☺



[Debar, Dacier, Wespi, 1998]

Techniques utilisables

- Approche par scénario
  - Systèmes experts (ES)
  - Analyse de signatures (SA)
  - Réseaux de Petri (PN)
- Approche comportementale
  - Statistiques (ST)
  - Systèmes experts (ES)
  - Réseaux neuronaux (NN)
  - Approche immunologique (UII)

Beaucoup de techniques ont été explorées

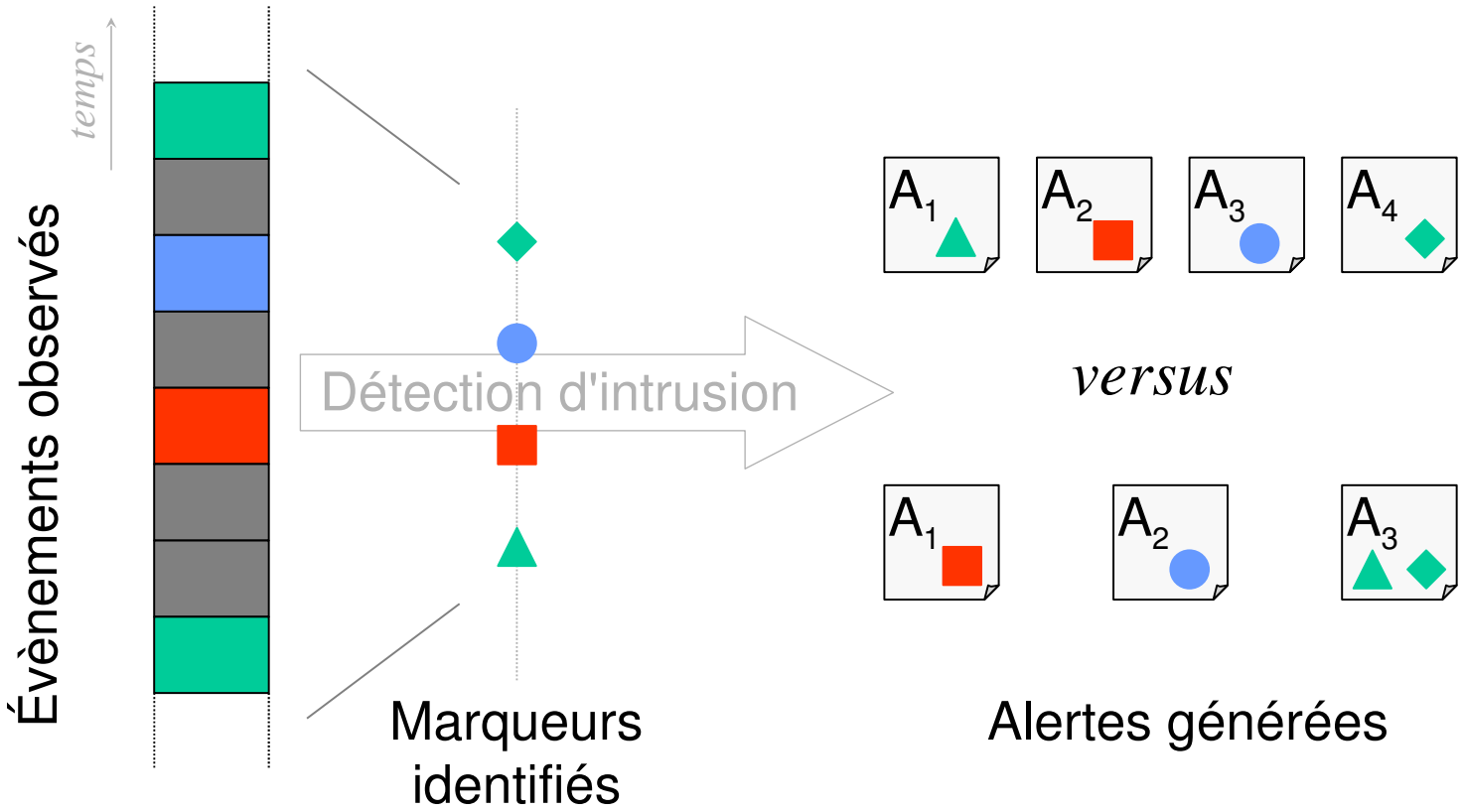
Origine	Nom	Période	Hôte	Réseau	Scénario				Comportemental			
					ES	SA	PN	STA	ST	ES	NN	UII
Université de Namur	ASAX	1990-97	■		■							
AT&T	ComputerWatch	1987-90	■							■		
USAF	Haystack	1987-90	■						■			
	DIDS	1989-95	■	■	■				■			
CS Telecom	Hyperview	1990-95	■		■				■		■	
SRI	IDES	1983-92	■		■				■			
	NIDES	1992-95	■		■				■			
	Emerald	1996-		■		■			■			
Purdue University	IDIOT	1992-97	■				■	■				
U.C. Davis	NSM	1989-95		■		■			■			
	GrIDS	1995-		■						■		
LANL	W&S	1987-90	■							■		
	Nadir	1990-	■		■					■		
Cisco/WheelGroup	NetRanger	1995-		■		■						
ISS	RealSecure	1995-	■	■		■						
Securenet Consortium	SecureNet	1992-96	■		■				■		■	■
Network Associates Inc.	Stalker	1995-	■			■						
	WebStalker CyberCop Server	1997-	■							■		
U.C. Santa-Barbara (UCSB)	STAT	1991-92	■					■				
	USTAT	1992-93	■					■				
Stanford University	Swatch	1992-93	■		■							
MCNC et NCSU	JiNao	1995-	?	■	■				■			

Tendances actuelles

- Une seule technique par outil en général
- L'approche par signatures se généralise
  - Réalisation plus simple
  - Performances
- L'approche comportementale est peu utilisée par les outils commerciaux
- La réaction apparaît

- Entre 2003 et 2011 : légère évolution

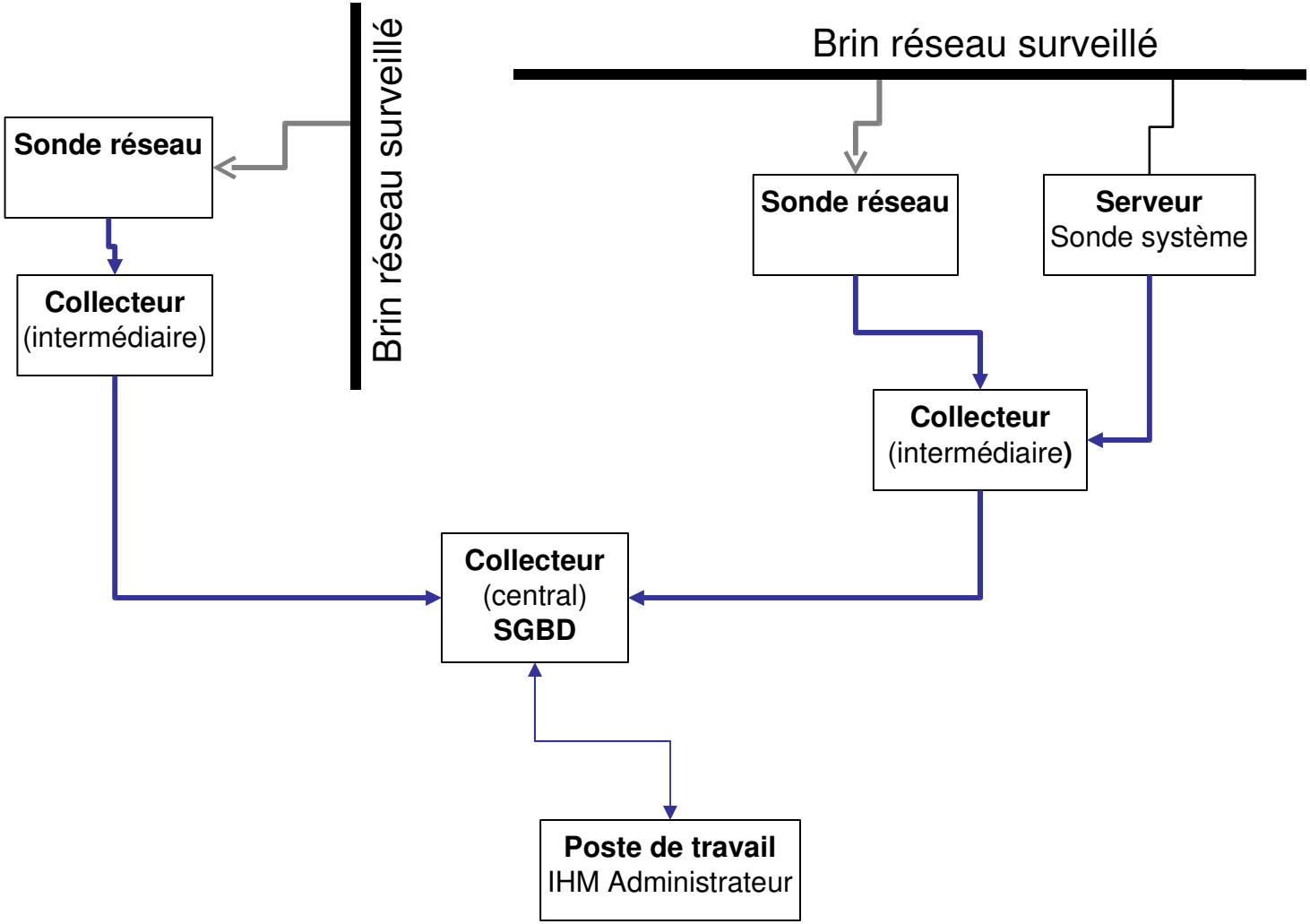
Analyse multi-évènements



Mise en oeuvre

- Sondes
  - Observation du trafic
    - Positionnement
    - Problème des environnements commutés (*mirroring* vs. *taps*)
  - Sondes système
  - Nombre des signatures (et impact CPU)
  - Pertinence des signatures
- Consolidation des alertes
  - Collecteurs
  - Protocole d'échange sécurisé
  - Format d'échange IDMEF: http://www.ietf.org/html.charters/idwg-charter.html

Architectures envisageables



Signatures – Snort (1)

SID	1800
Message	VIRUS Klez Incoming
Signature	alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"VIRUS Klez Incoming"; flow:to_server,established; dsize:>120; content:"MIME"; content:"VGhpcyBwcm9"; classtype:misc-activity; sid:1800; rev:3;)
Summary	This event is generated when an incoming email containing the Klez worm is detected.
Impact	System compromise and further infection of target hosts.
Detailed Information	W32/Klez.h@MM exploits the vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), enabling it to execute email attachments. Once executed, it can unload several processes including Anti-virus programs. The worm is able to propagate over the network by copying itself to network shares (assuming sufficient permissions exist). Target filenames are chosen randomly, and can have single or double file extensions.
Affected Systems	Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2)
Attack Scenarios	This virus can be considered a blended threat. It mass-mails itself to email addresses found on the local system, then exploits a known vulnerability, spreads via network shares, infects executables on the local system.
Ease of Attack	Simple. This is worm activity.
False Positives	Certain binary file email attachments can trigger this alert.
False Negatives	None known.
Corrective Action	Apply the appropriate vendor suppled patches. Block incoming attachments with .bat, .exe, .pif, and .scr extensions
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com>

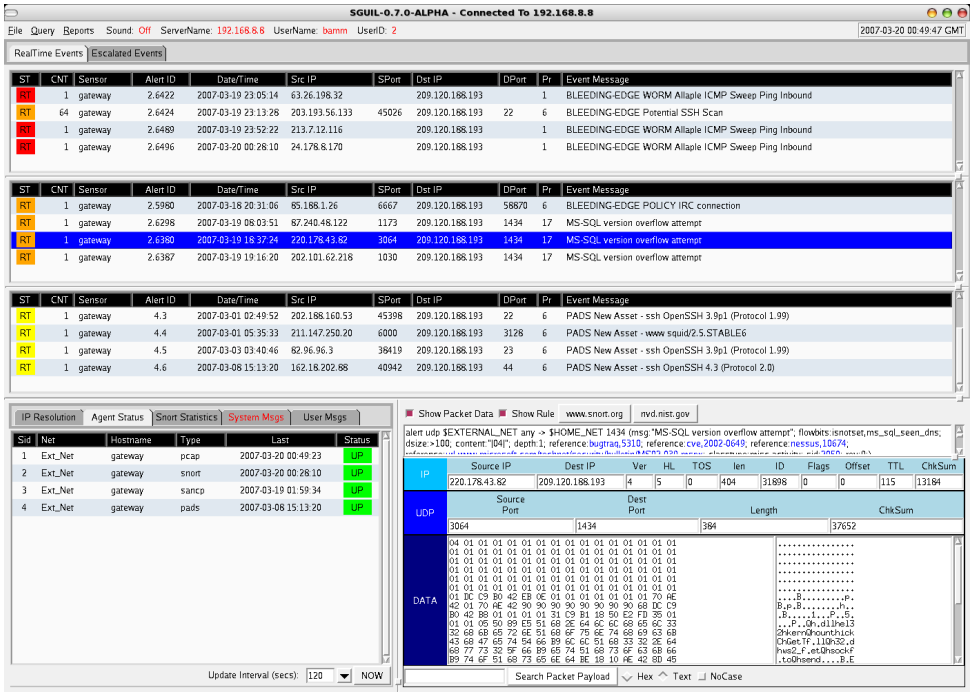
Signatures – Snort (2)

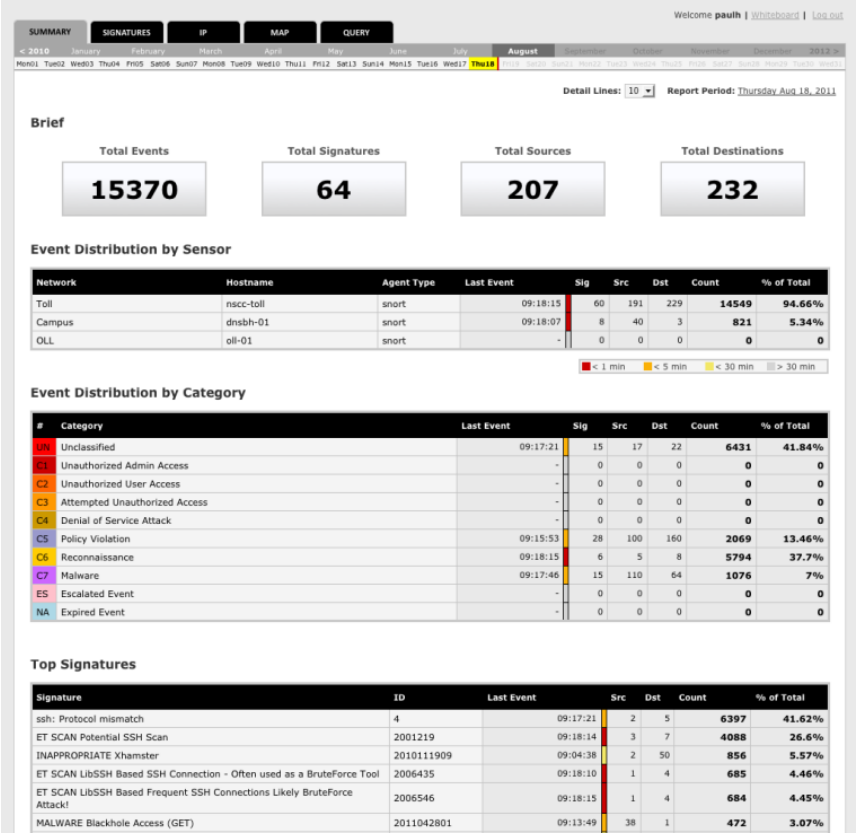
SID	2251
Message	NETBIOS DCERPC Remote Activation bind attempt
Signature	alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation bind attempt"; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57|"; distance:29; within:16; reference:cve,CAN-2003-0352; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/bulletin/MS03-026.asp; reference:cve,CAN-2003-0715; sid:2251; rev:1;)
Summary	This event is generated when an attempt is made to exploit a known vulnerablity in Microsoft RPCSS service for RPC.
Impact	Denial of Service. Possible execution of arbitrary code leading to unauthorized remote administrative access.
Detailed Information	A vulnerability exists in Microsoft RPCSS Service that handles RPC DCOM requests such that execution of arbitrary code or a Denial of Service condition can be issued against a host by sending malformed data via RPC. The Distributed Component Object Model (DCOM) handles DCOM requests sent by clients to a server using RPC. A malformed request to the host running the RPCSS service may result in a buffer overflow condition that will present the attacker with the opportunity to execute arbitrary code with the privileges of the local system account. Alternatively the attacker could also cause the RPC service to stop answering RPC requests and thus cause a Denial of Service condition to occur.
Affected Systems	Windows NT 4.0 Workstation and Server Windows NT 4.0 Terminal Server Edition Windows 2000 Windows XP

Outils complémentaires

- Oinkmaster
  - Récupération automatique des signatures
- Barnyard
  - Insertion des alertes dans une base de données
    - Modèle de données
    - Efficacité
- Consoles de visualisation
  - Principale valeur ajoutée des offres commerciales
  - Plusieurs générations
  - Exemples
    - ...
    - Sguil+Squert
    - Snorby
    - …

Console(s) de gestion





Sguil + Squert

Console(s) de gestion

Snorby

Firefox

Snorby - Dashboard

http://demo.snorby.org/users/login

Snorby "All About Simplicity"

Welcome Demo | Settings | Log out

Dashboard | My Queue (0) | Events | Sensors | Search | Administration

Dashboard

More Options

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 12/20/11 11:00:00 AM

4 HIGH SEVERITY 4 / 61

30 MEDIUM SEVERITY 30 / 61

27 LOW SEVERITY 27 / 61

Sensors | Severities | Protocols | Signatures | Sources | Destinations

Event Count vs Time By Sensor

Snorby
Weaksum
Sagan

Event Count

20 15 10 5 0 -5

11 12 13 14 15 16 17 18 19 20 21 22 23 0 1 2 3 4 5 6 7 8 9 10 11

Last 24 Hours

TOP 5 SENSOR

Snorby	222939
Weaksum	197986
Sagan	2173

TOP 5 ACTIVE USERS

Dustin Webber	18
Demo	0
Champ Clark	0

LAST 5 UNIQUE EVENTS

Data on SYN packet	2
stream5: TCP window cl...	8
http_inspect: NON-RFC ...	22
[OPENSSH] Invalid or i...	1
Snort Alert [1:396:0]	2

ANALYST CLASSIFIED EVENTS

False Positive	252028
Unauthorized Root Access	25553
Reconnaissance	11480
Attempted Unauthorized...	3705
Policy Violation	1412
Denial of Service Attack	345
Unauthorized User Access	333
Virus Infection	222

Traitement et qualification des alertes

Firefox

Snorby - High Severity Events

http://demo.snorby.org/results?search[severity]=1&search[time_end]=1324397928&search[time_start]=1

Snorby "All About Simplicity"

Welcome Demo | Settings | Log out

Dashboard | My Queue (0) | Events | Sensors | Search | Administration

High Severity Events 4 events found

Hotkeys | Classify Event(s)

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011
1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011
1	Snorby	CA 208.87.23.173	US 173.255.236.165	Demo classified event as Attempted Unauthorized Access	12/19/2011
1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011

Snorby 2.3.11 - http://www.snorby.org © 2011 Dustin Willis Webber

[PREWIKKA] - Windows Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Favoris | Galerie de composants ...

[PREWIKKA] | Page | Sécurité | Outils

Prewikka

Prelude management

Alerts | Heartbeats | Filters | admin on Tuesday December 20 20 1 | logout

- Events
- Agents
- Users
- About

Classification	Source	Target	Sensor	Time
2 x User authentication via su successful (**succeeded**)	user: 0	user: process: su (9548)	PAM	15:17:48 - 15:17:45
User login successful (**succeeded**)	.46.50:54647/tcp	user: process: sshd (9536)	sshd	15:17:40
34 x DNS SPOOF query response with TTL of 1 min. and no authority	9.30:53/udp	7.49:65095/udp	snort ( )	15:17:17 - 14:19:13
6 x Server recognition (failed)	147.35:tcp	process: sshd (9528)	sshd	15:16:07 - 14:21:37
18 x VIRUS OUTBOUND bad file attachment	20.12:57056/tcp	0.10:25/tcp	snort ( )	15:10:52 - 15:08:49
4 x Server recognition (failed)	.145.201:tcp	process: sshd (9496)	sshd ( )	15:09:21 - 14:22:48
2 x **WEB-PHP Pajax arbitrary command execution attempt**	.15.200:35658/tcp	0.100:8080/tcp	snort ( )	14:58:56 - 14:58:26
WEB-CLIENT QuickTime Object ActiveX CLSID access	100.40:8080/tcp	53.100:53847/tcp	snort ( )	14:58:16
1 x **WEB-CLIENT Microsoft wmf metafile access** 1 x **WEB-CLIENT Outlook EML access**	53.100:52268/tcp	00.40:8080/tcp	snort ( )	14:44:57 - 14:27:26
NETBIOS SMB-DS Trans unicode Max Param/Count DOS attempt (vendor-specific:url, vendor-specific:url, vendor-specific:url, cve:2002-0724, bugtraqid:5556)	3.68:65373/tcp	7.14:445/tcp	snort ( )	14:41:09
5 x MISC Visio version number anomaly	5.20:8080/tcp	00:58131/tcp	snort ( )	14:36:01 - 14:36:00
DNS SPOOF query response with TTL of 1 min. and no authority	.30:53/udp	26:64876/udp	snort ( )	14:35:50

Delete

Filter:

Step: 1 Hours

Tz: Frontend localtim

Limit: 50 apply

2011-12-20 14:18:11

2011-12-20 15:18:11

+01:00

prev | current | next

<< | < | > | >>

1 ... 12 (total:12)

Internet | Mode protégé : activé | 125%

Limites actuelles de la détection d'intrusion

- Faible taux de détection
  - Faux négatifs
- Trop d'alertes
  - Fausses alertes : Faux positifs
  - Plusieurs milliers d'alertes générées en une semaine
- Le niveau de granularité d'une alerte est trop faible
  - Pas de vision globale
  - Difficile de détecter une attaque distribuée
- Difficile de détecter les attaques nouvelles
  - C'est un avantage des approches comportementales

Granularité trop fine

Exemple : alertes générées par Dragon

[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
[**] [1:1
07/20-1
[**] [1:1
07/20-1

SID	1256
Message	WEB-IIS CodeRed v2 root.exe access
Signature	alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase; classtype:web-application-attack; reference:url,www.cert.org/advisories/CA-2001-19.html; sid:1256; rev:7;)

[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:33.969027 64.165.187.170:4582 -> 193.54.194.111:80
[**] [1:1288:2] WEB-FRONTPAGE /_vti_bin/ access [**]
07/20-13:59:34.434017 64.165.187.170:4587 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:34.817953 64.165.187.170:4593 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80
[**] [1:1
07/20-1
[**] [1:1
07/20-1

SID	1002
Message	WEB-IIS cmd.exe access
Signature	alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; flow:to_server,established; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:5;)

Granularité trop fine

Exemple : alertes générées par Dragon

- [**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
  07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:33.059882 64.165.187.170:4533 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59
  [**] [1:1002:
  07/20-13:59
  [**] [1:1288:
  07/20-13:59
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:34.817955 64.165.187.170:4593 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
-

Attaque *Nimda* de 64.165.187.170
vers 193.54.194.111

Sémantique trop pauvre

Exemple : alertes générées par Dragon

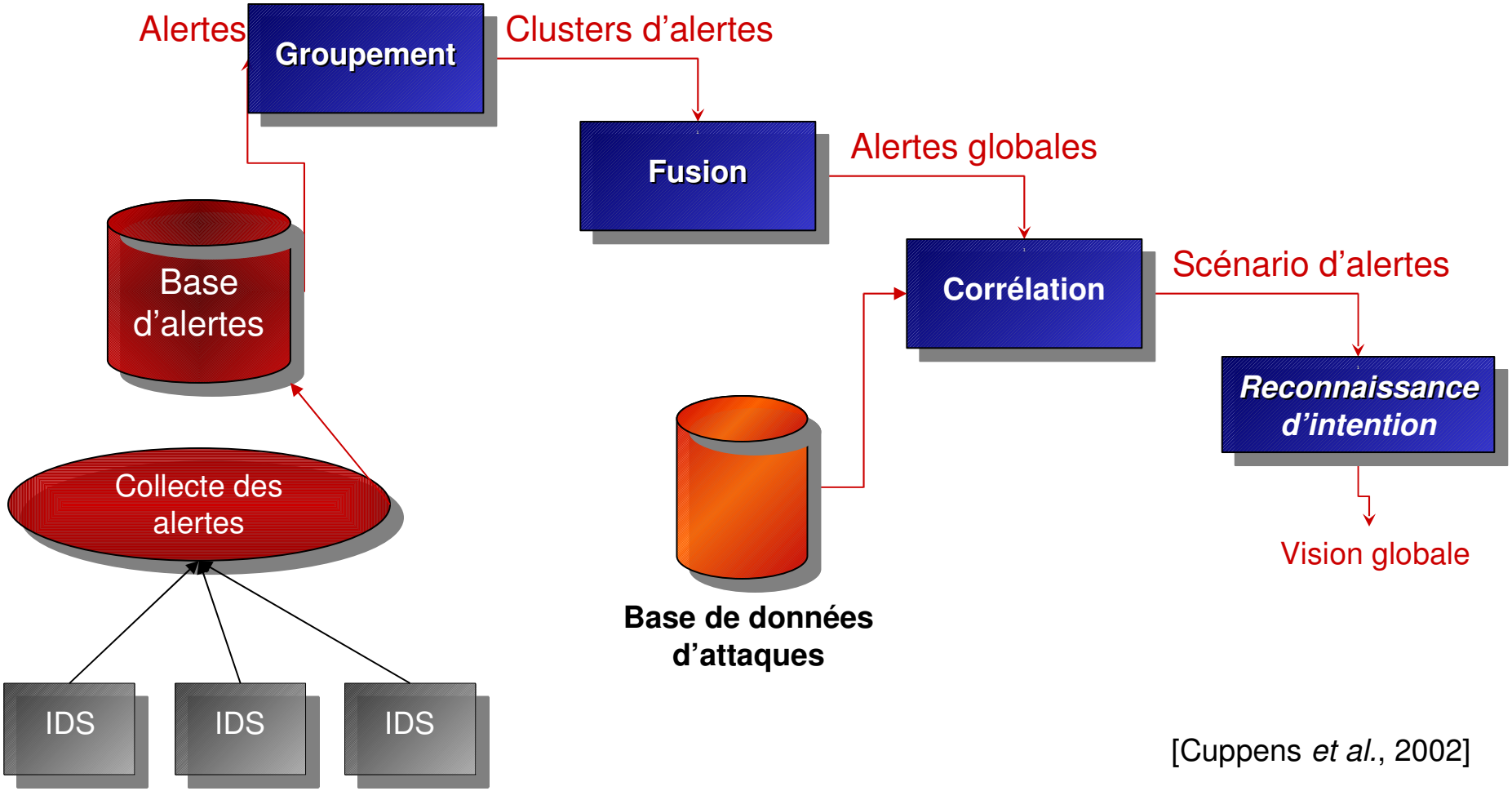
- [**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
  07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:33.0[illegible]882 64.165.187.170:4533 -> 193.54.194.111:80
  [**] [1:1002:[illegible]
  07/20-13:59[illegible]
  [**] [1:1002:[illegible]
  07/20-13:59[illegible]
  [**] [1:1288:[illegible]
  07/20-13:59[illegible]
  [**] [1:1002:[illegible]
  07/20-13:59:34.817[illegible]53 64.165.187.170:459[illegible] -> 193.54.194.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:[illegible]5.219711 64.165.187.170:4601 -> 19[illegible].54.194.111:80
  [**] [1:100[illegible]:2] WEB-IIS cmd.exe access [**]
  07/20-[illegible]3:59:35.607048 64.165.187.170:4603 -> 193.54.[illegible]4.111:80
  [**] [1:1002:2] WEB-IIS cmd.exe access [**]
  07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
- [illegible]

Attaque *Nimda* de 64.165.187.170 vers 193.54.194.111, 193.54.194.111 non-vulnérable

Corrélation d’alertes

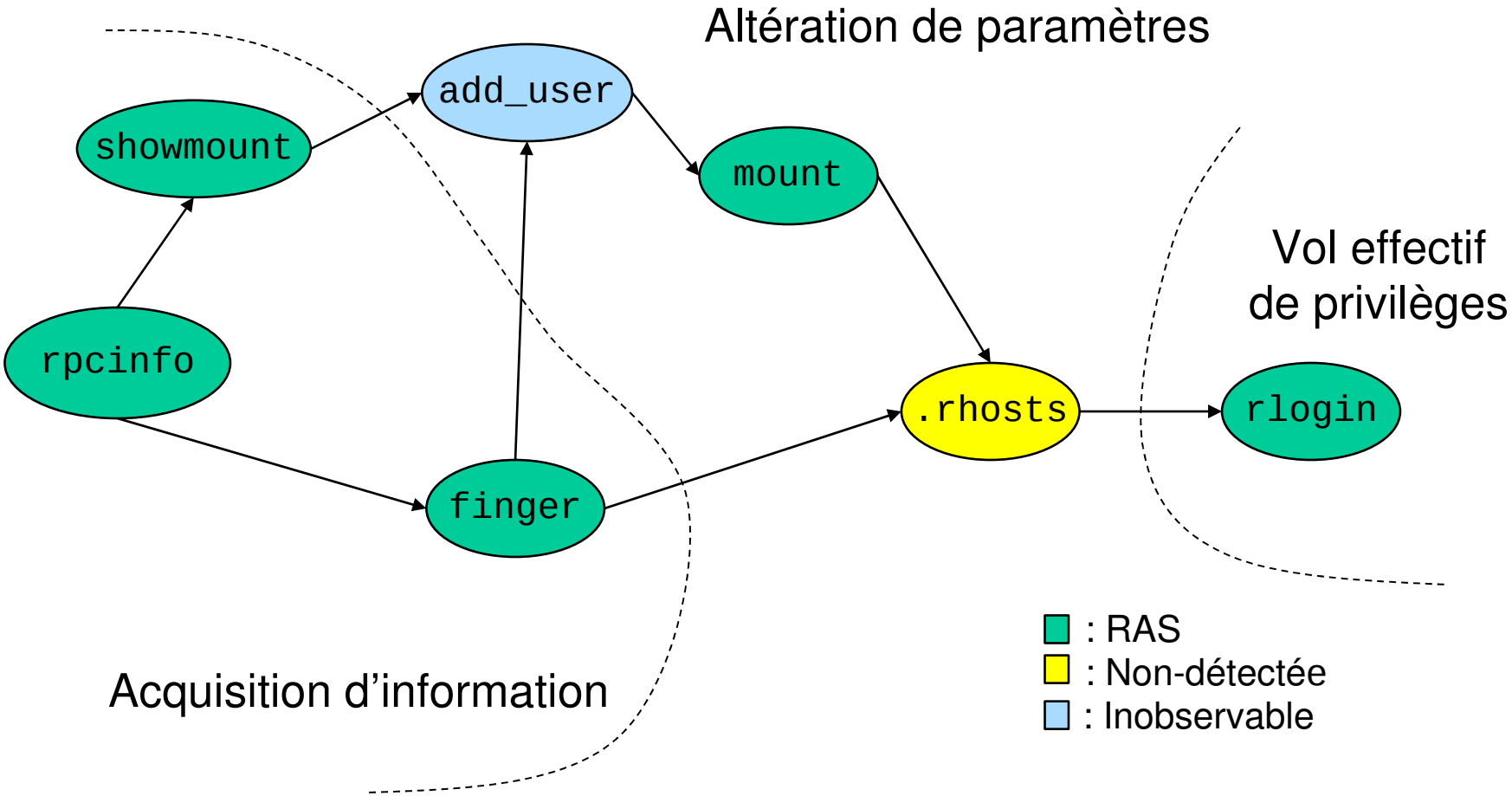
- Développement des méthodes utilisables pour la corrélation
- Prise en compte d’information de cartographie
- Intégration de notions de groupement puis de fusion dans des outils existants ?

Les étapes du diagnostic

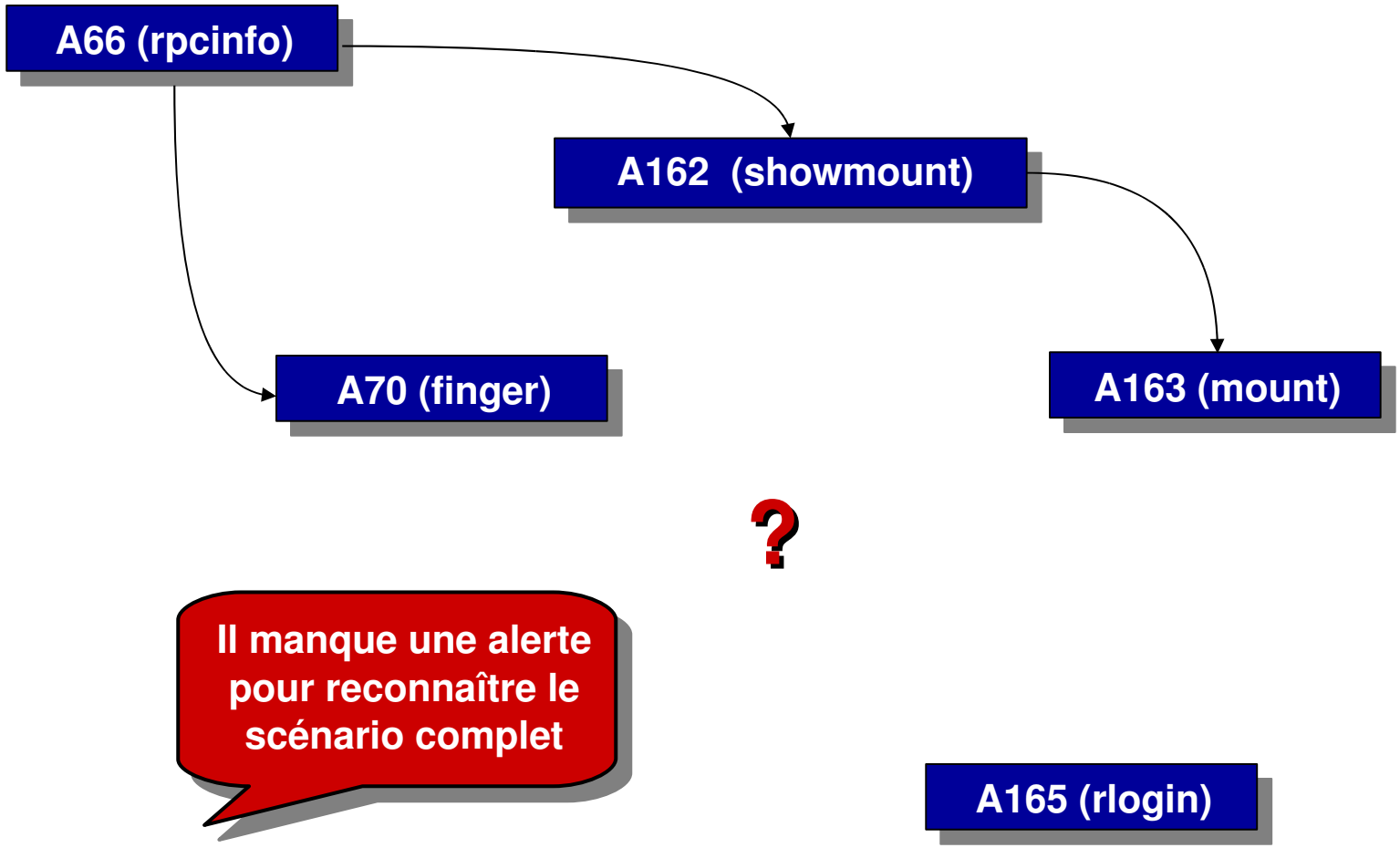


[Cuppens *et al.*, 2002]

Scénario non-linéaire (exemple)



Exemple de corrélation

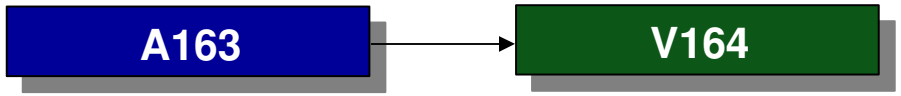


Génération d'hypothèse

- On cherche une attaque appropriée

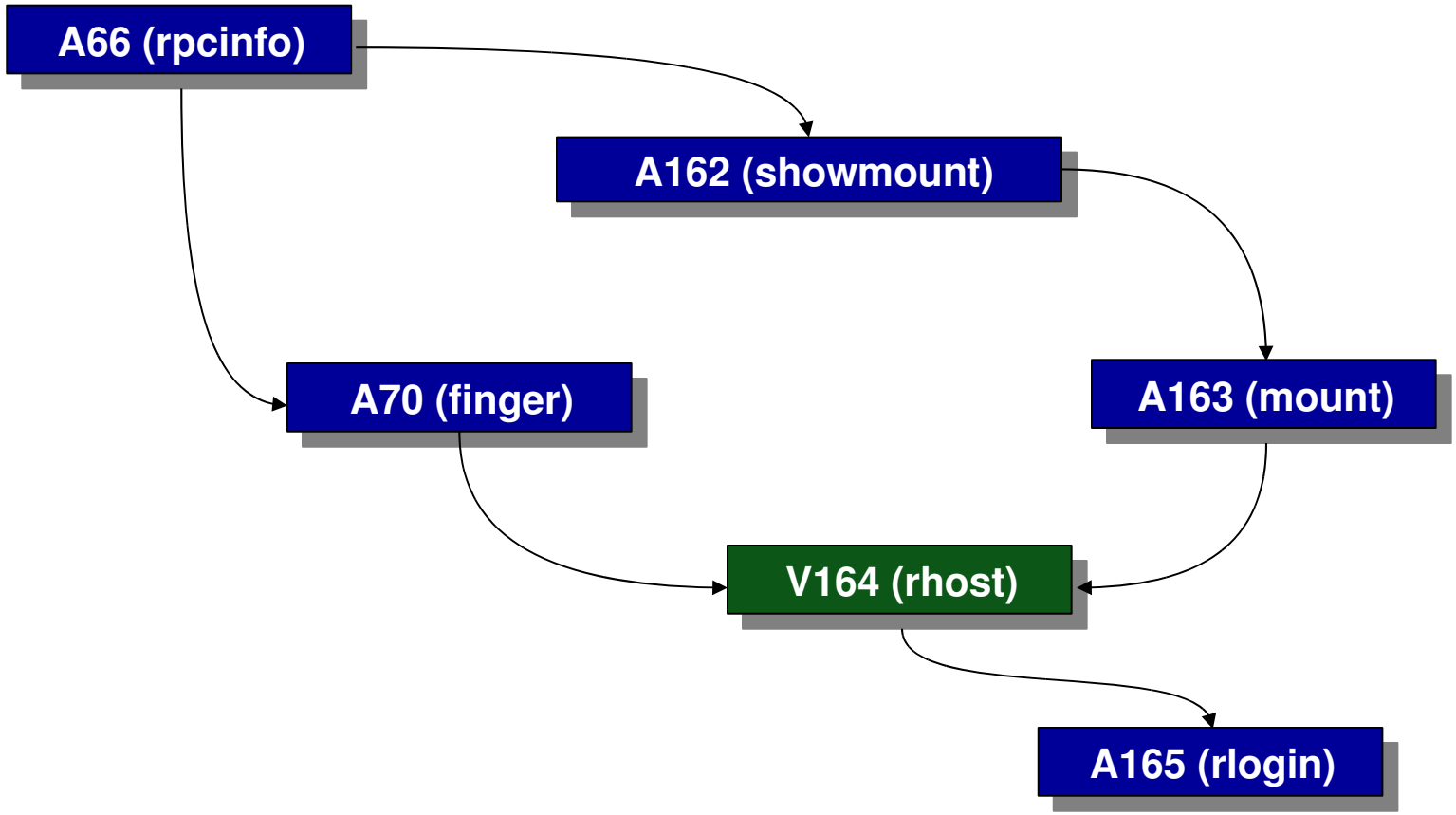
- Création d'une alerte en tant qu'instance de cette attaque

- Initialisation des champs de l'alerte grâce aux règles de corrélation



- Tentative de corrélation des deux dernières alertes

Résultat de la génération d'hypothèses

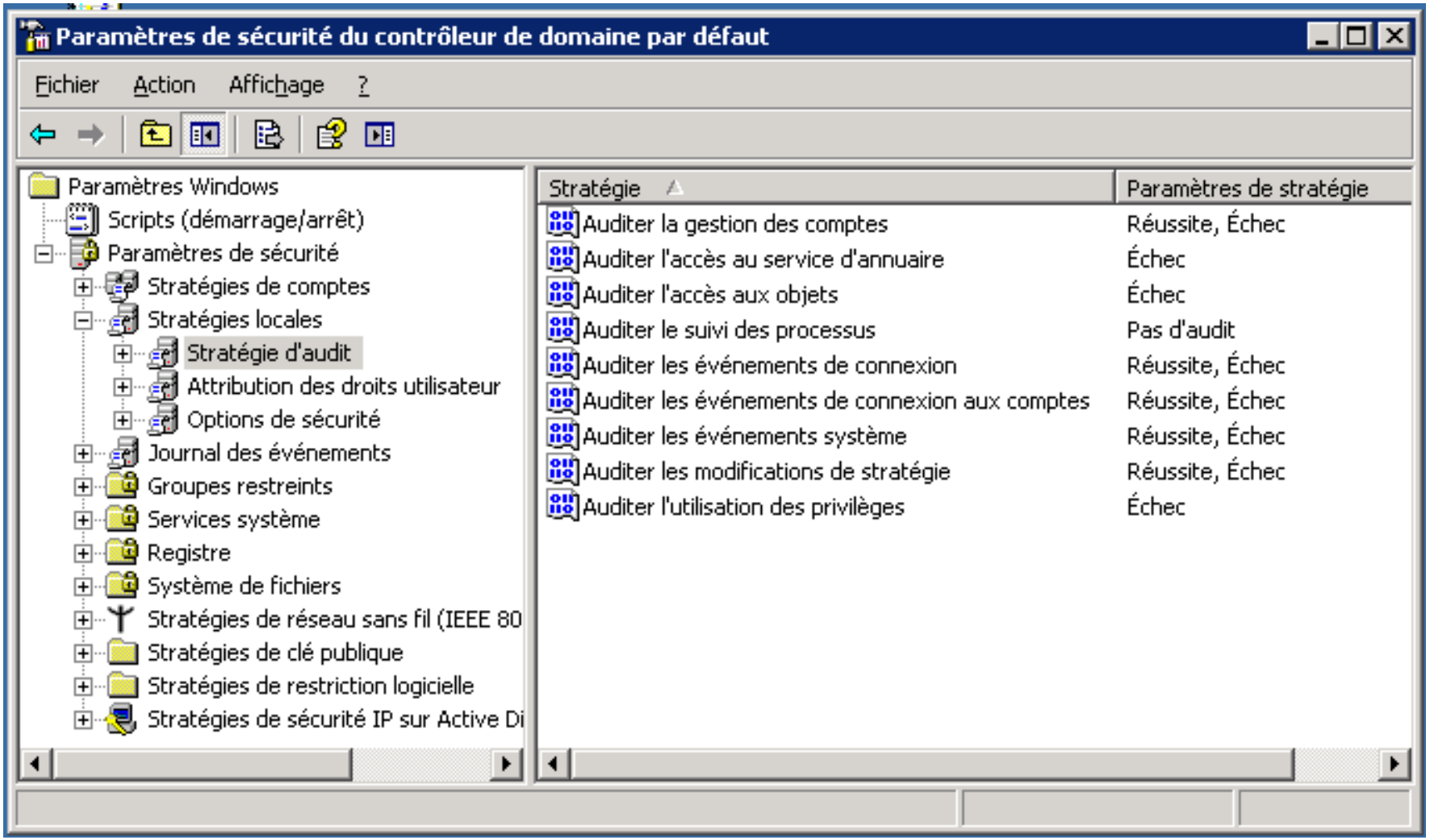


Centralisation des traces

- Solutions propriétaires
- Syslog
- CNIL

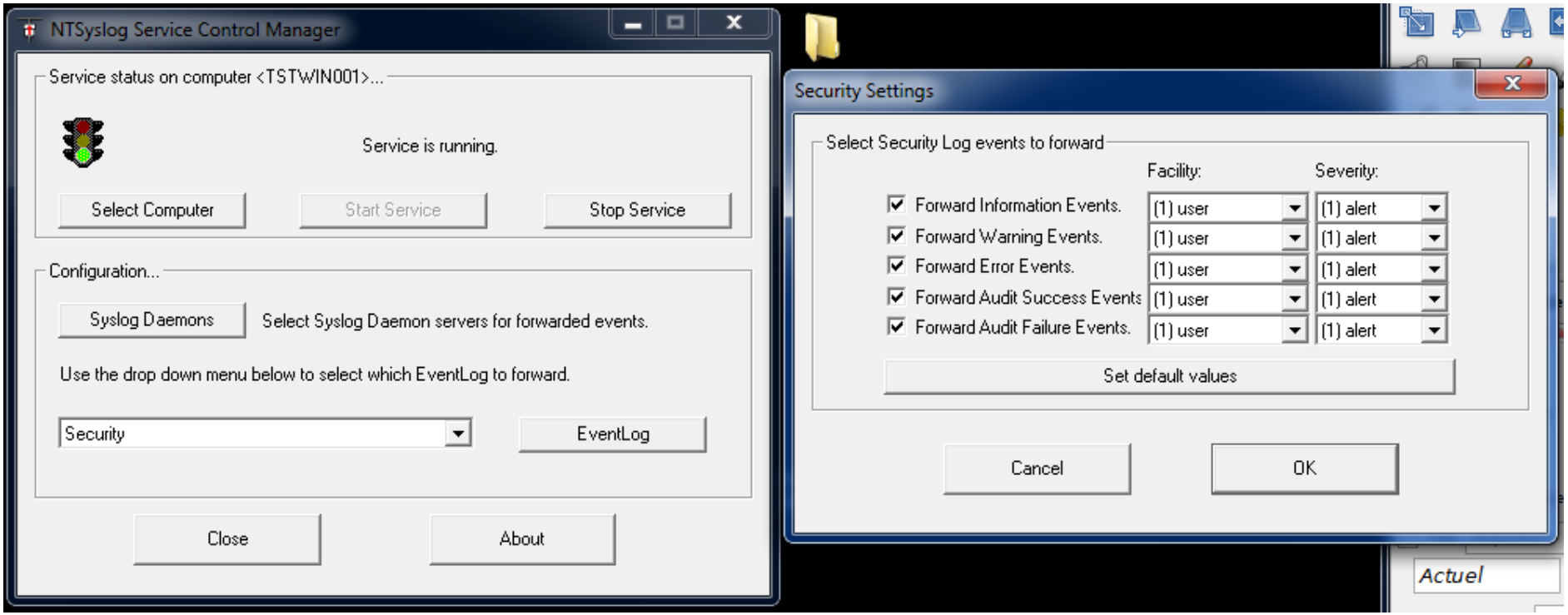
```
ortalo@[redacted]: /home/ortalo
Nov 27 10:02:02 [redacted] postgres[23600]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:02 [redacted] postgres[23600]: [2] LOG:  connection authorized: user=postgres database=phpgroupware
Nov 27 10:02:08 [redacted] postgres[23608]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:08 [redacted] postgres[23608]: [2] LOG:  connection authorized: user=postgres database=prelude
Nov 27 10:02:12 [redacted] postgres[23613]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:12 [redacted] postgres[23613]: [2] LOG:  connection authorized: user=postgres database=template1
Nov 27 10:02:34 [redacted] nagios: SERVICE ALERT: [redacted];PING;OK;SOFT;3;PING OK - Packet loss = 0%, RTA = 117.51 ms
Nov 27 10:03:04 [redacted] nagios: SERVICE ALERT: [redacted];PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 2
53.35 ms
Nov 27 10:04:04 [redacted] nagios: SERVICE ALERT: [redacted];PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 59.94 ms
Nov 27 10:05:01 [redacted] /USR/SBIN/CRON[24114]: (www-data) CMD (php4 /usr/share/cacti-0.8.3a/cmd.php > /dev/null 2>&
1)
Nov 27 10:05:23 [redacted] syslog-ng[198]: STATS: dropped 0
Nov 27 10:07:44 [redacted] nagios: HOST ALERT: [redacted];DOWN;SOFT;1;CRITICAL - Plugin timed out after 10 seconds
Nov 27 10:07:44 [redacted] nagios: HOST ALERT: [redacted];UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 54.46 ms
Nov 27 10:07:44 [redacted] nagios: SERVICE ALERT: [redacted];PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA =
 379.32 ms
Nov 27 10:08:01 [redacted] /USR/SBIN/CRON[24687]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a -f /etc/exim/exim.conf
]; then /usr/lib/exim/exim3 -q ; fi)
Nov 27 10:08:35 [redacted] nagios: SERVICE ALERT: [redacted];PING;CRITICAL;SOFT;2;PING CRITICAL - Packet loss = 0%, RTA
 = 605.51 ms
Nov 27 10:08:54 [redacted] nagios: SERVICE ALERT: [redacted]:PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 2
06.12 ms
:
```

Paramétrage d'un DC Windows

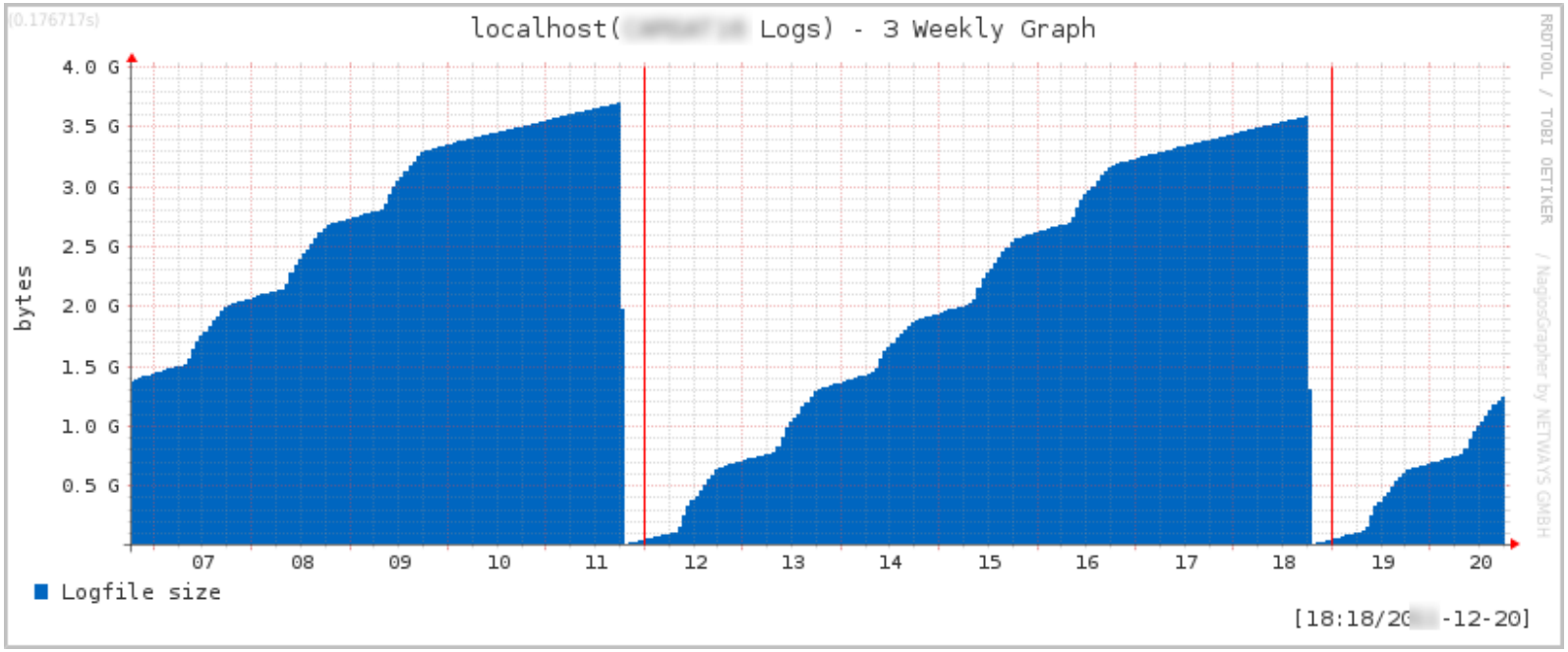


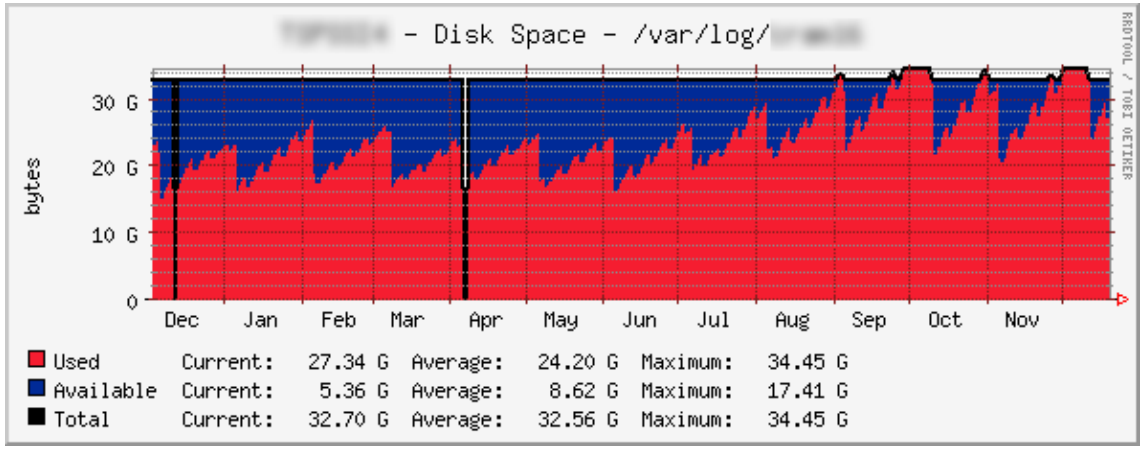
Déport de trace (simple)

Outil : NTsyslog



Éléments de volumétrie





Antivirus sur le poste (1)

Symantec Endpoint Protection

Etat

Aide et support

Etat
Rechercher les menaces
Changer les paramètres
Afficher la quarantaine
Afficher les journaux

LiveUpdate

Votre ordinateur est protégé.

Aucun problème détecté.

Technologies de protection

Les technologies de protection Symantec suivantes sont installées sur votre ordinateur :

Protection antivirus et antispyware — Activé — Options

Protège contre virus, chevaux de Troie, logiciels espions.

Définitions : mardi 20 décembre 2011 r20

Protection proactive contre les menaces — Activé — Options

Assure une protection immédiate contre les menaces inconnues.

Définitions : mardi 20 décembre 2011 r5

symantec.

Antivirus sur le poste (2)

Symantec Endpoint Protection

Aide et support

Rechercher les menaces

Etat
Rechercher les menaces
Changer les paramètres
Afficher la quarantaine
Afficher les journaux

LiveUpdate

Active Scan

Analyser uniquement les zones les plus communément infectées.

Durée : **1 a 2 minutes**

Exécuter Active Scan

Analyse complète

Analyser l'ensemble de l'ordinateur.

Durée : **30 a 120 minutes**

Exécuter une analyse complète

Analyses

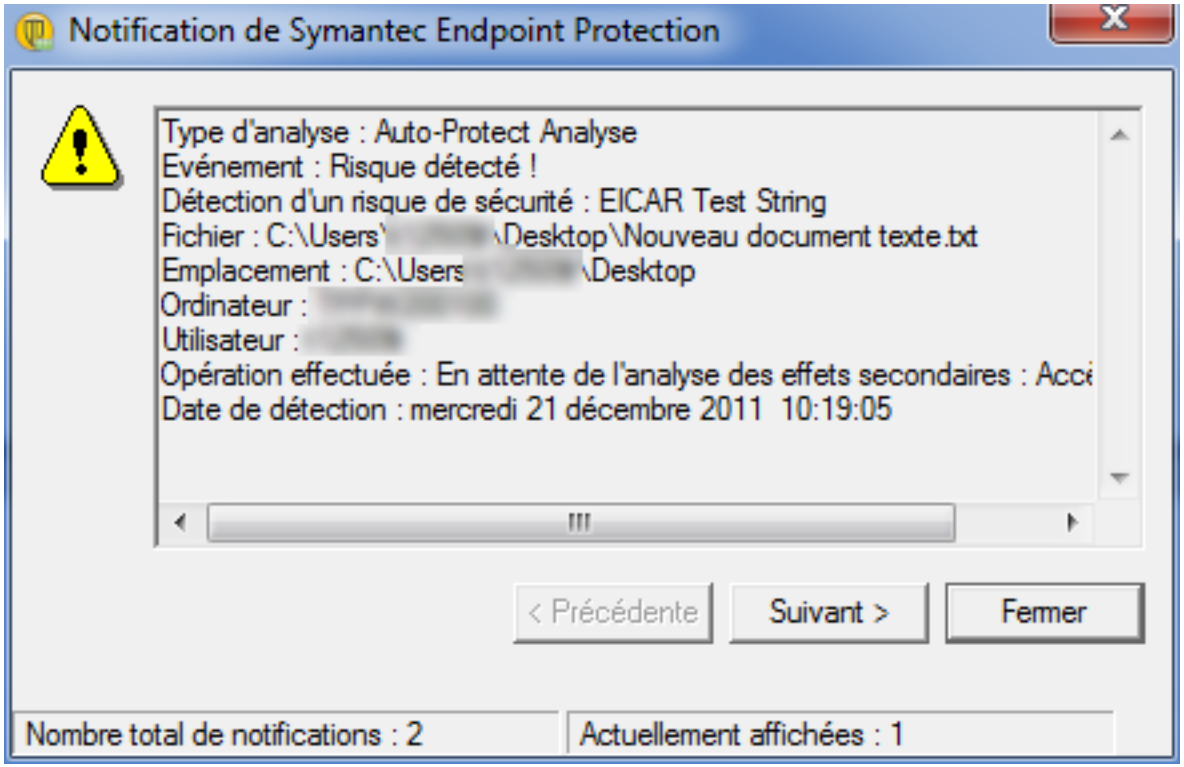
Analyses configurées pour cet ordinateur.

Créer une analyse

Nom de l'analyse	Activé	Type	Moment de l'analyse	Dernière analyse
Analyse planifiée chaque semaine	Oui	Analyse com...	Hebdomadaire	lundi 19 décembre 2011 22.

symantec.

Antivirus sur le poste (3)



Console Antivirus (1)

Console Symantec Endpoint Protection Manager

Symantec™ Endpoint Protection Manager

Actualiser | A propos de | Aide | Déconnexion

Page démarrage

Contrôles

Rapports

Administrateur

Etat de la sécurité

Préférences

Etat de la sécurité - Bon

Infos supplém.

Résumé des actions par nombre de détections

Opération	Virus	Risques de sécurité
Nettoyé	0	0
Suspect	0	0
Bloqué	0	0
Mis en quarantaine	0	0
Supprimé	0	0
Nouvellement infecté	0	0
Encore infecté	1	0

Risques par heure : 12 dernières heures

Afficher : Risques

0

Résumé de l'état

	Ordinateurs
Moteur antivirus arrêté	0
Auto-Protect arrêté	0
Protect contre intervent. désactiv	0
Redémarrage requis	1
Intégrité de l'hôte défaillante	0
Etat élément n'effectu. pas rappo.	0

Aucune notification non acquittée dans les 24 dernières heures

Distribution des définitions de virus : 12 dernières heures

Afficher : Distribution des définitions de virus

Définitions	Ordinateurs
2011-12-20 rev. 020	725
2011-12-20 rev. 002	1
2011-12-19 rev. 020	3
2011-12-18 rev. 009	1
tous les autres	11

Dernière version Symantec : 2011-12-20 rev. 038

Dernière version du gestionnaire : 2011-12-20 rev. 020

Security Response

Dernière mise à jour : 21/12/2011 07:38:55

Men princip

Dernier change. propa. : 09/10/2010 00:56:01

» Aucun article à afficher

Dernières menaces

» Aucun article à afficher

Il n'y a actuellement pas de menaces de catégorie 3 ou plus en circulation.

Symantec ThreatCon

Level 1: Normal

- Alerte de sécurité
- Symantec
- Définitions
- Dernières menaces
- Security Focus

Résumé des applications surveillées

	Occurrences
Détection d'application commerciale	0
Détect. proactive forcée menaces TruScan	0

Rapports sur les favoris

Principales sources d'attaques

Corrélation des principaux risques

Distrib. ds menaces protect TruScan

Console Antivirus (3)

Téléchargements les plus récents de LiveUpdate

Affiche les téléchargements les plus récents de contenu LiveUpdate sur ce site. L'affichage n'affiche pas les téléchargements LiveUpdate sur les clients. Il n'affiche pas non plus les téléchargements des paquets d'installation de client.

Type de contenu	Révision	Moment du téléchargement
Catalogue de contenus de Symantec Endpoint Protection Manager 11.0	2011-05-19 rev. 701	21 septembre 2011 07:14:25 CEST
Définitions antivirus et contre les logiciels espions Win64 11.0 MicroDefs...	2011-12-20 rev. 020	21 décembre 2011 07:26:23 CET
Définitions antivirus et contre les logiciels espions Win32 11.0 MicroDefs...	2011-12-20 rev. 020	21 décembre 2011 07:39:04 CET
Decomposer Win32 et Win64 11.0	2008-02-17 rev. 000	24 septembre 2009 14:30:05 CEST
Moteur d'analyse proactive des menaces TruScan Win64 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:43 CEST
Données d'analyse proactive des menaces TruScan 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:34 CEST
Moteur d'analyse proactive des menaces TruScan Win32 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:48 CEST
Liste blanche d'analyse proactive des menaces TruScan Win32 11.0	2011-12-20 rev. 005	21 décembre 2011 07:46:23 CET
Liste des applications commerciales d'analyse proactive des menaces Tr...	2011-12-20 rev. 005	21 décembre 2011 07:47:53 CET
Moteur d'application commerciale d'analyse proactive des menaces TruS...	2008-09-29 rev. 016	24 septembre 2009 14:29:56 CEST
Liste blanche d'analyse proactive des menaces TruScan Win64 11.0	2011-12-20 rev. 005	21 décembre 2011 07:47:11 CET
Liste des applications commerciales d'analyse proactive des menaces Tr...	2011-12-20 rev. 005	21 décembre 2011 07:46:15 CET
Signatures de prévention d'intrusions Win32 11.0	2011-12-20 rev. 001	21 décembre 2011 07:20:54 CET
Signatures de prévention d'intrusions Win64 11.0	2011-12-20 rev. 001	21 décembre 2011 07:47:03 CET
Signatures de contrôle des transmissions 11.0	2010-12-01 rev. 096	3 décembre 2010 06:29:22 CET

Fermer

Console Antivirus (2)

Symantec™ Endpoint Protection Manager

Actualiser | A propos de | Aide | Déconnexion

Page démarrage
Contrôles
Rapports
Politiques
Clients
Administrateur

Afficher les clients

- Ma société
  - Groupe par défaut
  - ajout fonctionnalites
  - Clients spécifiques (
  - deploiement
  - Hébergeurs Hyper-V
  - PC quarantaine
  - PC Standard
  - PC W2K Nomade ave
  - Serveur Notes
  - Serveurs
  - Serveurs GED
  - Serveurs Oracle
  - Sharepoint de dev vi

Tâches

- Ajouter un groupe...
- Ajouter un compte d'ordinate
- Ajouter un compte d'utilisate
- Importer une unité ou un con
- Importer les utilisateurs Activ
- Exécuter la commande sur le
- Effectuer une recherche par
- Définir le filtre d'affichage
- Rechercher les ordinateurs

PC Standard

Clients | Politiques | Détails | Paquets d'installation

Affichage : Etat du client

Ce groupe contient les clients suivants : Page 1 sur 35 < Précédente Suivant >

Nom	Client d'ouverture de session	Adresse IP	Version de client	Dernier contrôle	Redémarra
			11.0.5002.333	20/12/11 16:59	Non
			11.0.5002.333	19/12/11 17:11	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	02/12/11 14:31	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	20/12/11 16:35	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	13/12/11 08:34	Non
			11.0.5002.333	16/12/11 16:59	Non
			11.0.5002.333	16/12/11 16:19	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	25/11/11 11:11	Non
			11.0.5002.333	13/12/11 15:35	Non
			11.0.5002.333	08/12/11 17:59	Non
			11.0.5002.333	20/12/11 16:39	Non
			11.0.5002.333	09/12/11 15:59	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	20/12/11 17:03	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	16/12/11 16:59	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:24	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	20/12/11 17:47	Non
			11.0.5002.333	21/12/11 10:24	Non

Console Antivirus (3)

Symantec™ Endpoint Protection Manager

Actualiser | A propos de | Aide | Déconnexion

Page démarrage
Contrôles
Rapports
Politiques
Clients

Afficher les politiques

- Antivirus et antispyware
- Pare-feu
- Prévention d'intrusion
- Contrôle des applications et des
- LiveUpdate
- Exceptions centralisées
- Composants de politique

Tâches

- Ajouter une politique antivirus et
- Importer une politique antivirus et
- Rechercher des applications

Politiques antivirus et antispyware

Nom	Description	Compte de l'utilisat...
Politique antivirus et antispyware	Politique recommandée pour la plupart des environnements, offrant ...	0
Politique antivirus et antispyware - Haut...	Politique haute sécurité, pouvant affecter les performances d'autres...	0
Politique antivirus et antispyware - Haut...	Politique offrant de meilleures performances mais une sécurité inféri...	0
Politique antivirus et antispyware Test s...	Politique Test	0
V1 - Politique antivirus et antispyware p...	Politique par défaut pour les serveurs	10
Sans scan planifiés - Politique antivirus ...	Politique sans scan	0
V2 - Politique antivirus et antispyware	Politique par défaut pour les clients standards	11
V2 - Serveurs Citrix - politique antivirus ...	Politique pour serveurs Citrix	1
V2 - Politique antivirus et antispyware - ...	idem politique livrée pour clients standards mais avec analyse planifi...	4
Test BM Exclusion	Test Exclusion	0

Les modifications récentes sont répertoriées ci-dessous :

Description	Heure	Administrateur

Console Antivirus (3)

http://localhost:8014/ - Reporting - Nouveaux risques détectés dans le réseau - Windows Internet Explorer

Symantec Endpoint Protection

symantec.

Nouveaux risques détectés dans le réseau

20 Septembre 2011 11:00 PM à 21 Décembre 2011 11:59 PM

Imprimer | Enregistrer | Fermer

15 entrées

Nom du risque Categorie / Type Découvert	Première occurrence Détecté par	Domaine Serveur Groupe	Ordinateur Utilisateur
Infostealer 1 / Viral (Fichier) 08/12/1997	15/12/2011 08:07:15 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]
Backdoor.Cycbot 1 / Viral (Fichier) 30/10/2010	15/12/2011 08:07:06 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]
Trojan.Malscript 1 / Viral (Fichier) 27/10/2010	14/12/2011 11:23:31 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]
Spyware.Netobserve Non spécifié / Logiciel espion (Fichier) Inconnue	06/12/2011 09:54:33 Analyse planifiée	Par défaut [illegible] Ma société\PC Standard	[illegible]
Trojan.Gen.2 1 / Viral (Fichier) 20/08/2010	28/11/2011 09:03:30 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]
CainAbel Non spécifié / Risque de sécurité (Fichier) Inconnue	23/11/2011 10:59:38 Analyse Auto-Protect	Par défaut [illegible] Ma société\ajout fonctionnalites	[illegible]
Adware.InetAntiSpy Non spécifié / Logiciel de publicité (Fichier) Inconnue	17/11/2011 11:36:03 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]
Bloodhound.Olexe 1 / Viral (Fichier) 20/12/2006	17/11/2011 09:31:38 Analyse Auto-Protect	Par défaut [illegible] Ma société\PC Standard	[illegible]

Outils complémentaires

- Analyse d'un flux réseau
  - Wireshark
- Contrôle de l'intégrité d'un système de fichiers
  - Outils disponibles
    - md5sum, sha1sum, *sha3sum* (2012+)
    - Samhain, AIDE
  - Problématiques de la famille « Tripwire »
    - Protection des empreintes de référence
      - Stockage externe ou hors ligne
      - Signature
    - Mise en oeuvre sur systèmes de fichiers réels
      - Fichiers spéciaux (/dev, etc.)
      - Traces
      - Binaires et mises à jour