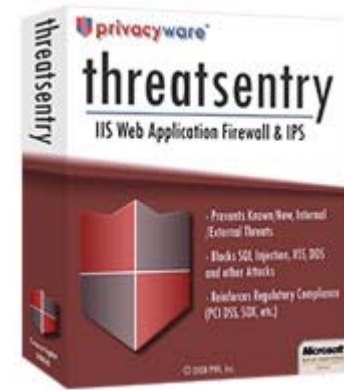


80 440

가

2

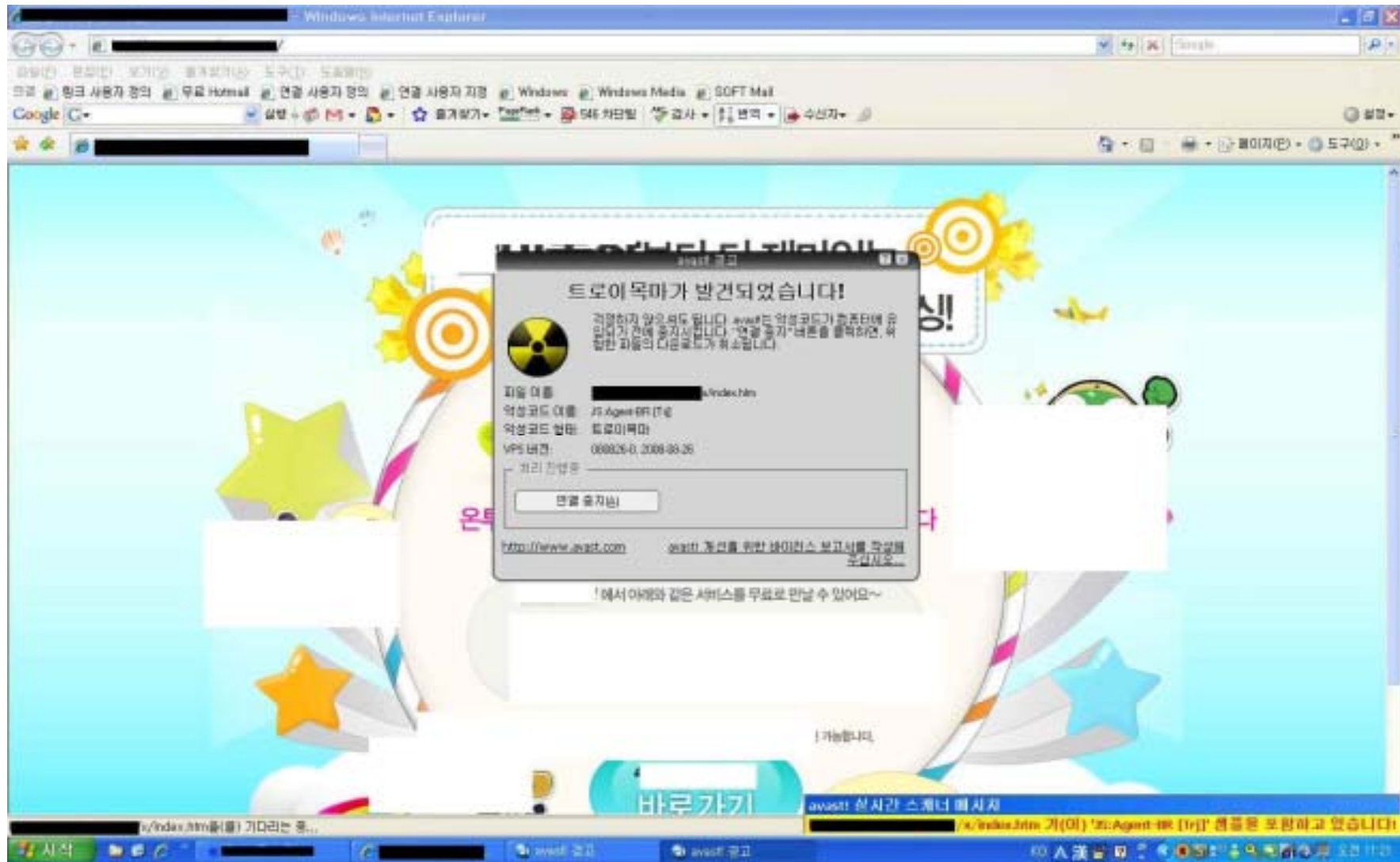
. (:)



(1)



(2)



VS

	TreatSentry()	
	가	- 가
	가 - Messenger - E-mail - - SMS (가)	
IP	가	
	/ - 가 - 가 - 가	- 가
	MMC 가	- WebKnight.XML
	MMC	- PIDx

DDoS

...

DDoS

'NetBot_Attack'

가

DDoS

'NetBot_Attack' VIP 4.7

DDoS

PC

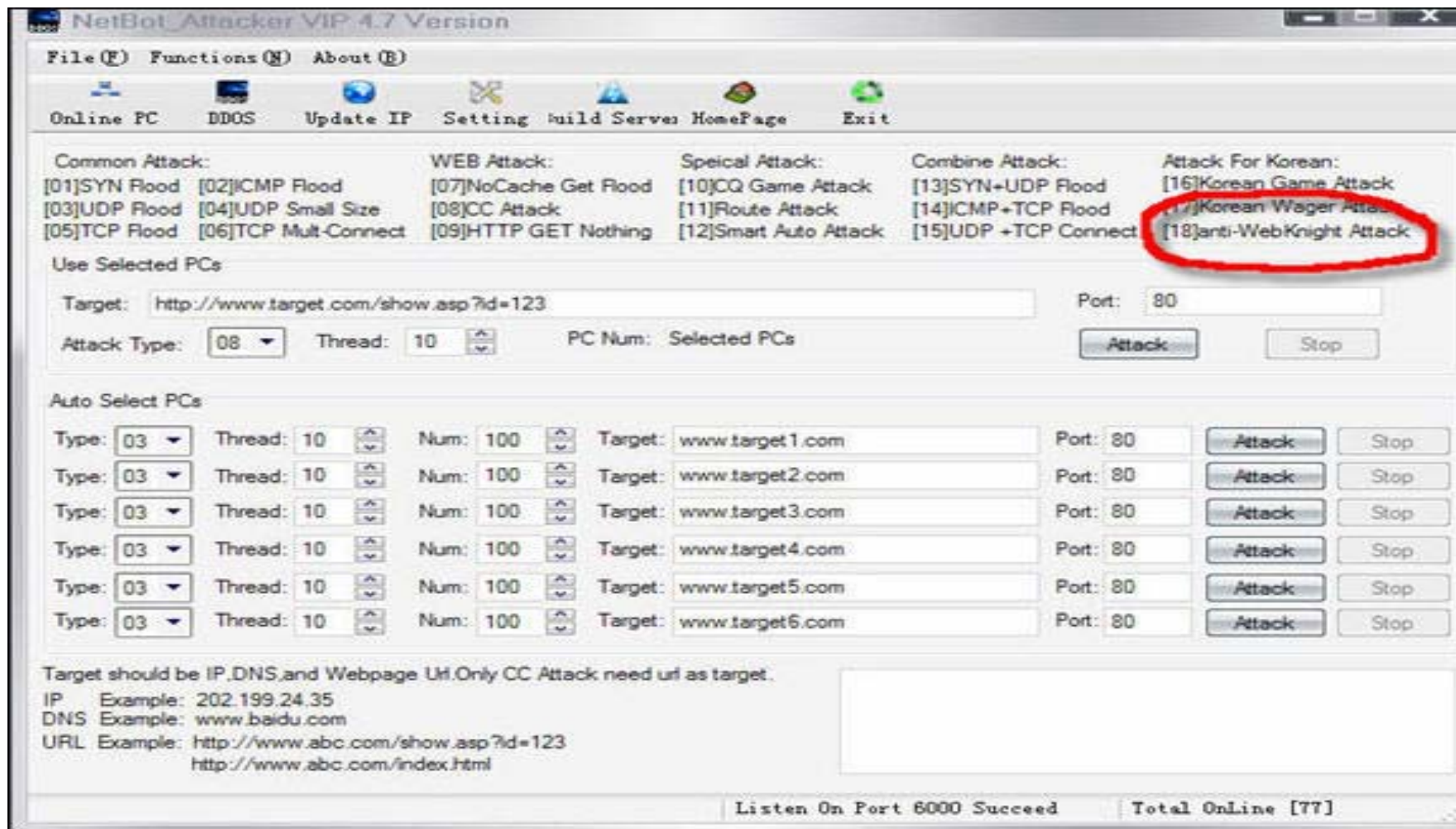
가

< > 2008 9 1

, NetBot

(Anti-WebKnight Attack)

NetBot_Attack



Netbot_Attacker VIP 4.7 최신 버전 화면

- IIS

.

IIS가

(misuse)

.

- (rule), ,

SQL ,

XSS(

), , , ,

(parser evasion), , ,

IIS .

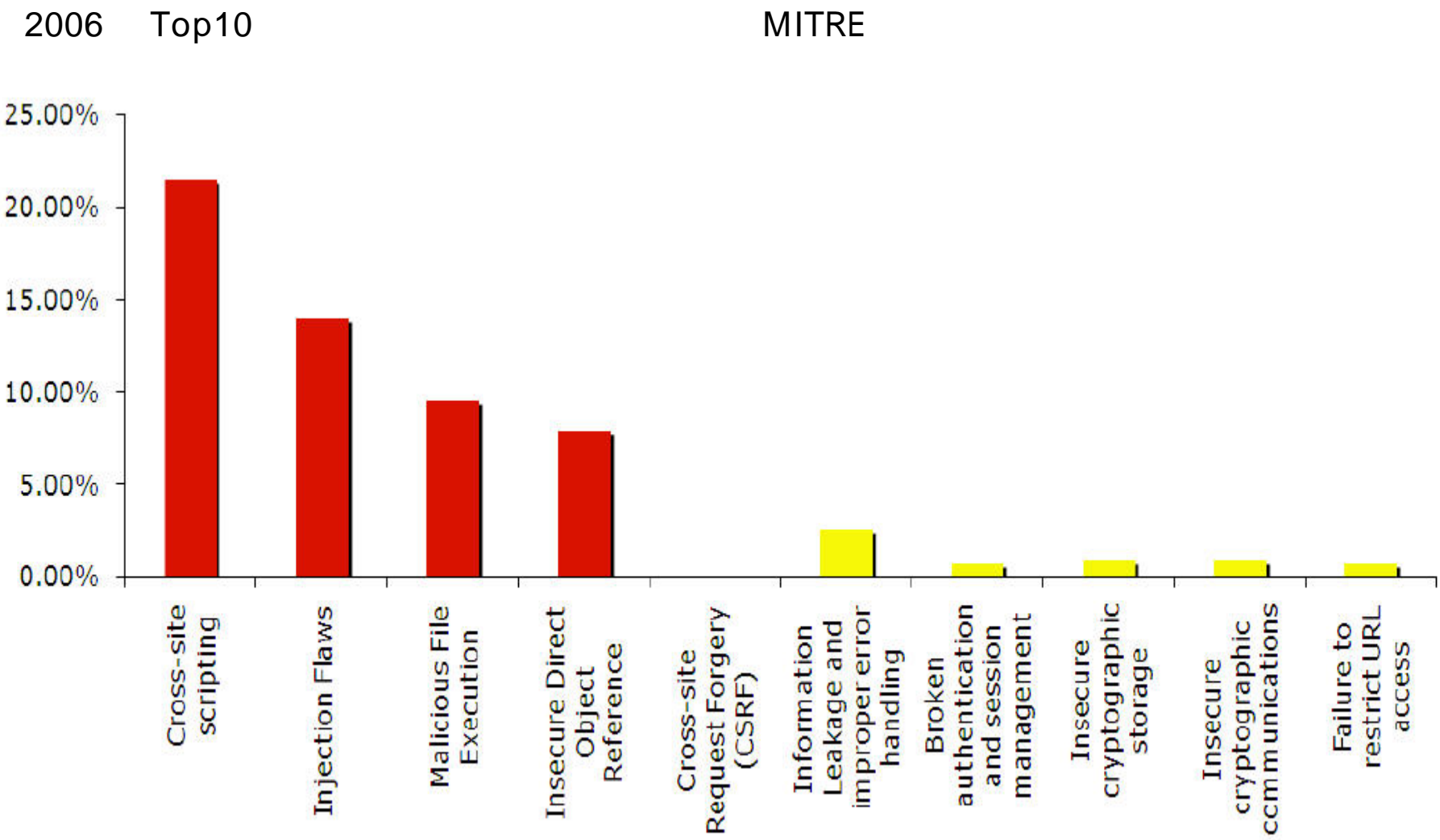
가

exploit

가

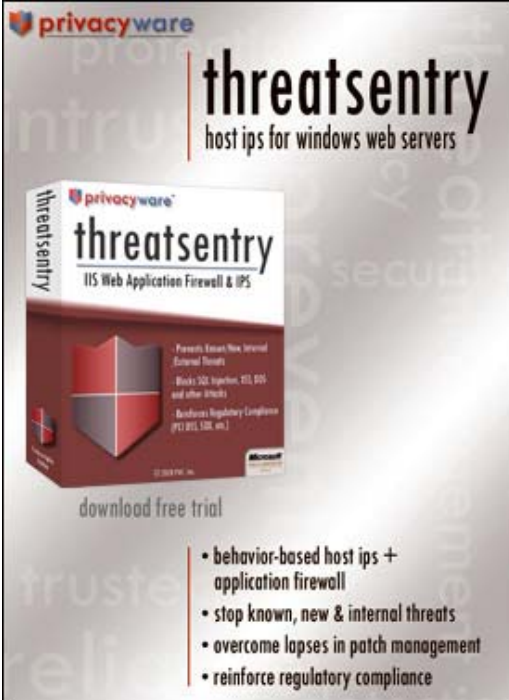
. ThreatSentry

- SQL Injection Cross-Site Scripting
- /
-
- IP
- /
- IIS
- () 가
- OWA



OWASP 10

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
10. URL



The advertisement features a central image of the ThreatSentry software box. The box is white and red, with the PrivacyWare logo at the top. The text on the box reads "threatsentry" in a large, bold font, followed by "IIS Web Application Firewall & IPS". Below this, there are several bullet points: "Prevents Known & New Internal External Threats", "Blocks SQL Injection, XSS, XSS, and other attacks", and "Reinforces Regulatory Compliance (PCI DSS, SOX, etc.)". The Microsoft logo is visible in the bottom right corner of the box. Below the box, the text "download free trial" is displayed. To the right of the box, there is a list of features: "behavior-based host ips + application firewall", "stop known, new & internal threats", "overcome lapses in patch management", and "reinforce regulatory compliance". The background of the advertisement is a light gray with faint, repeating words like "privacy", "security", "trust", and "reliability".

privacyware
threatsentry
host ips for windows web servers

privacyware
threatsentry
IIS Web Application Firewall & IPS

- Prevents Known & New Internal External Threats
- Blocks SQL Injection, XSS, XSS, and other attacks
- Reinforces Regulatory Compliance (PCI DSS, SOX, etc.)

Microsoft

download free trial

- behavior-based host ips + application firewall
- stop known, new & internal threats
- overcome lapses in patch management
- reinforce regulatory compliance

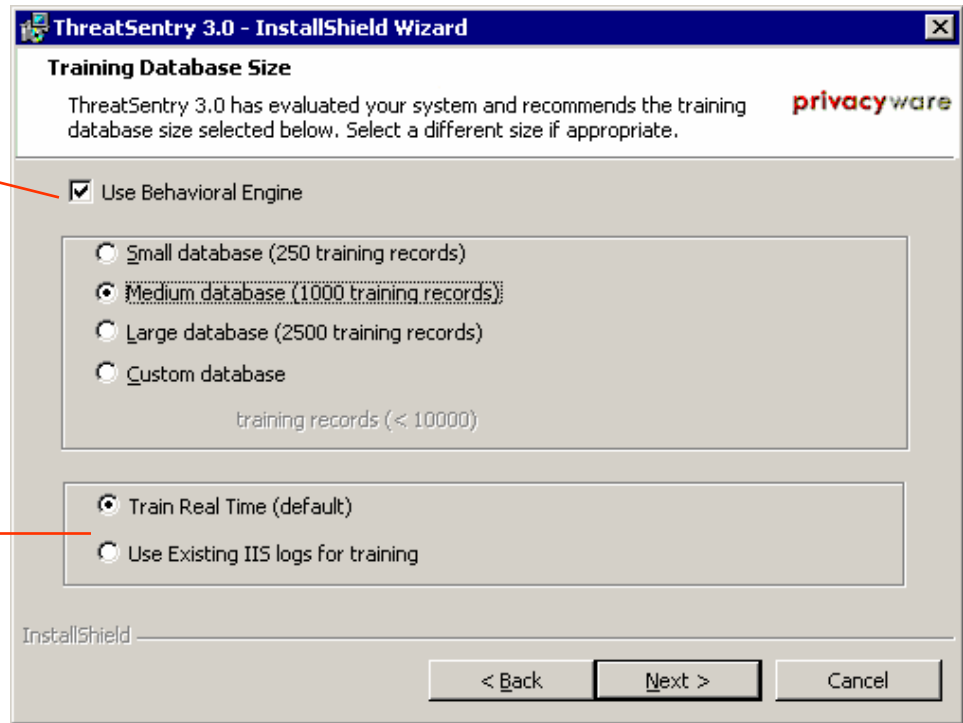
—

(active)

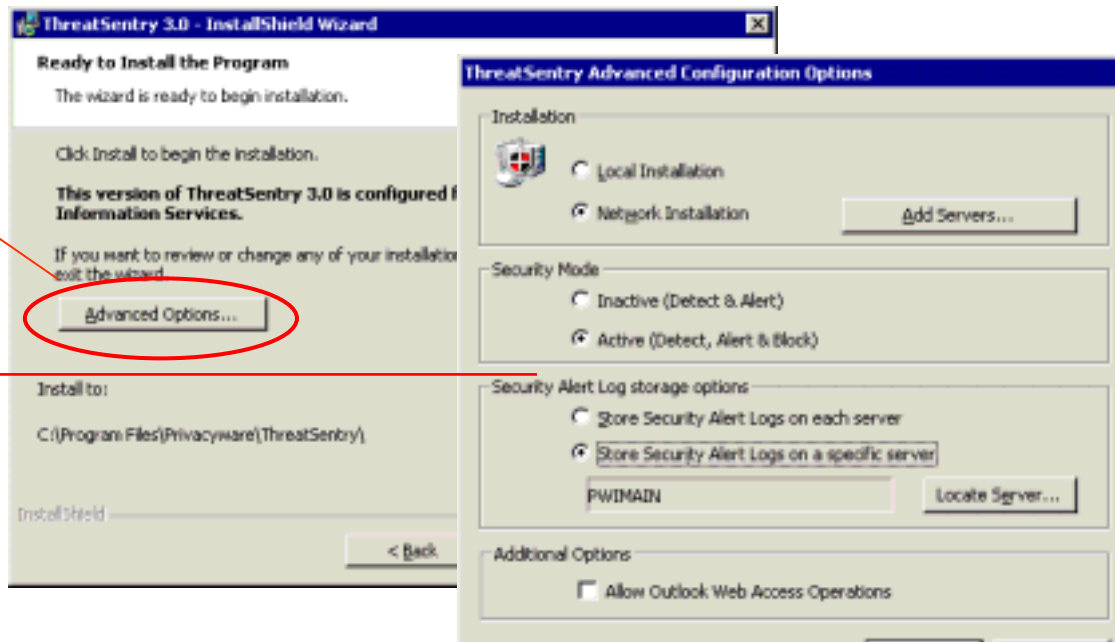
(inactive)

(Baseline)

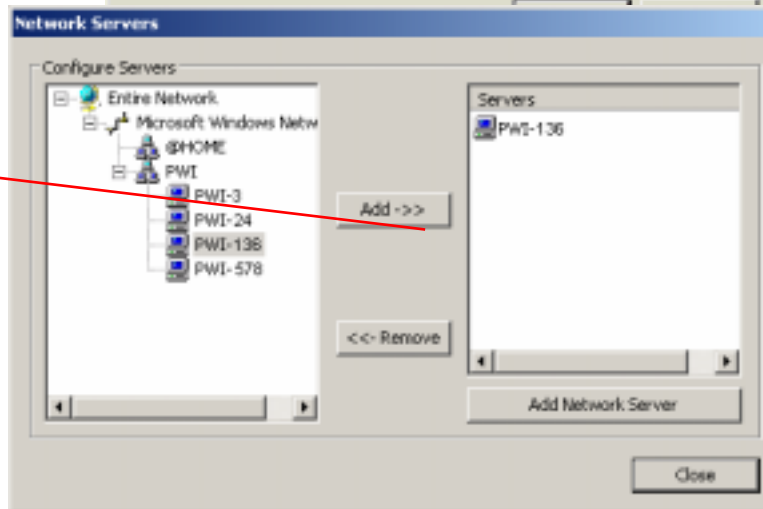
IIS 가



(Advanced options)

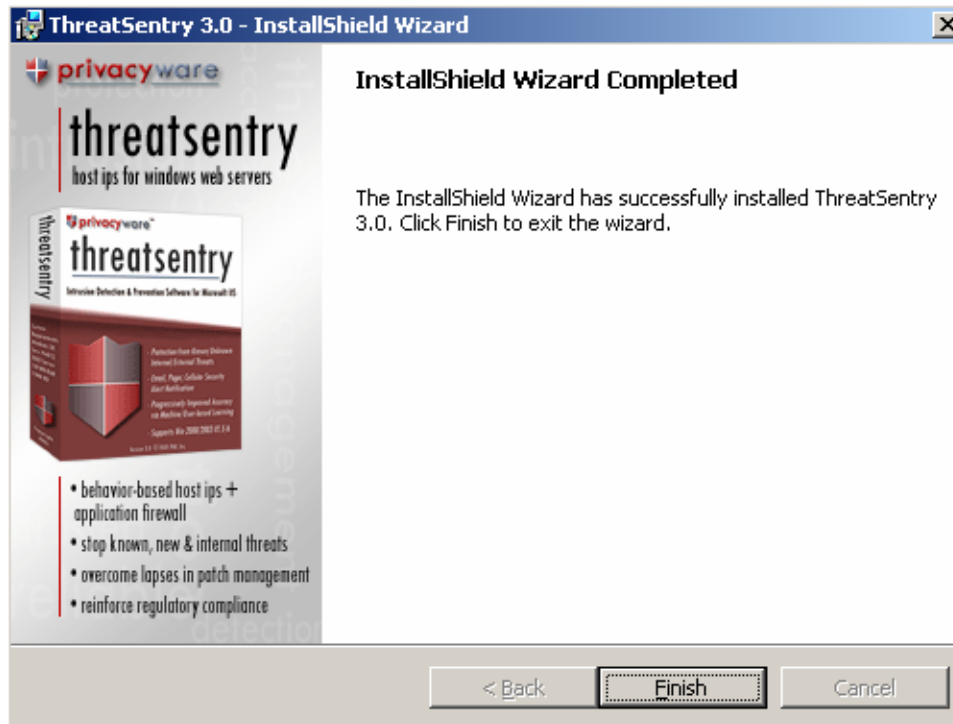


OWA
가 .

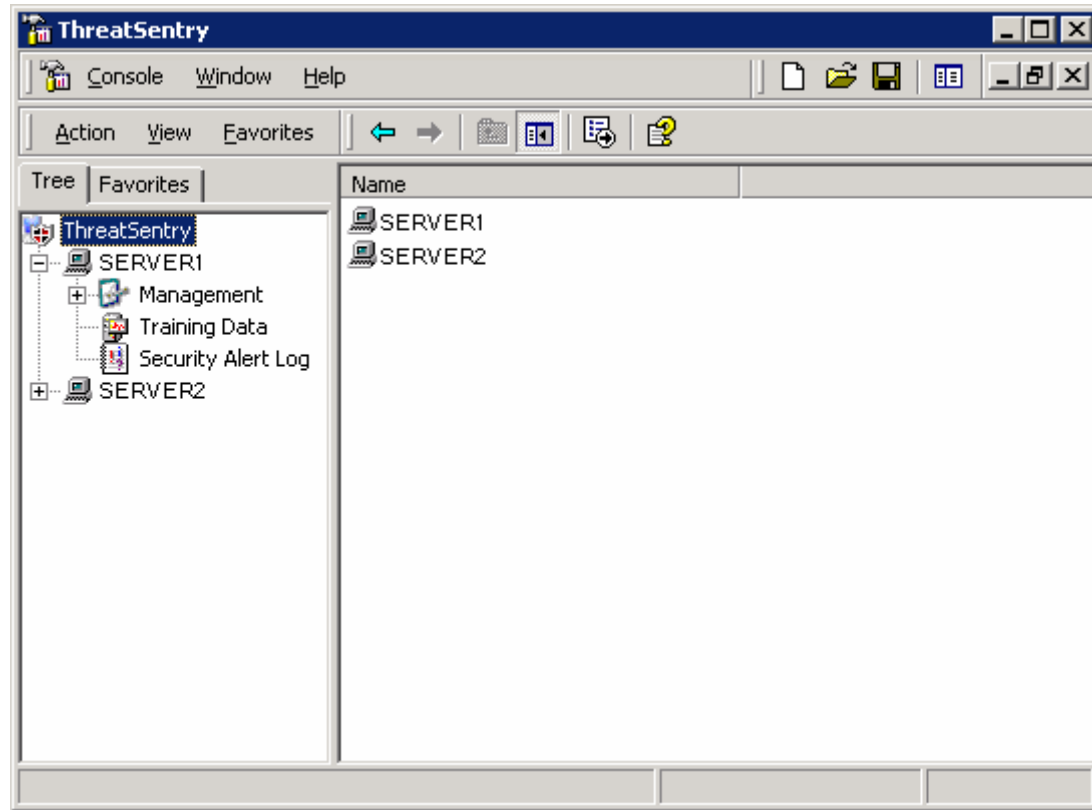


가
가 .

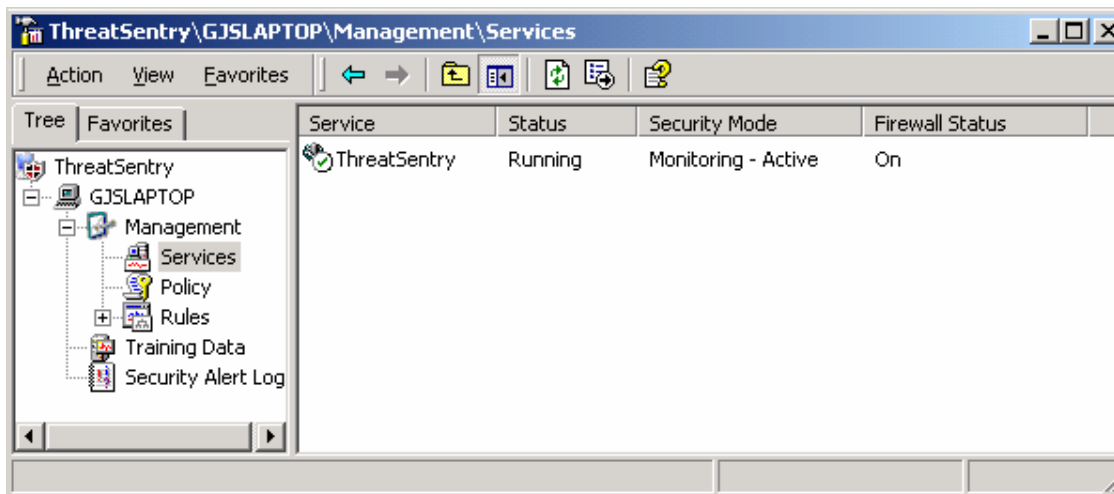
가

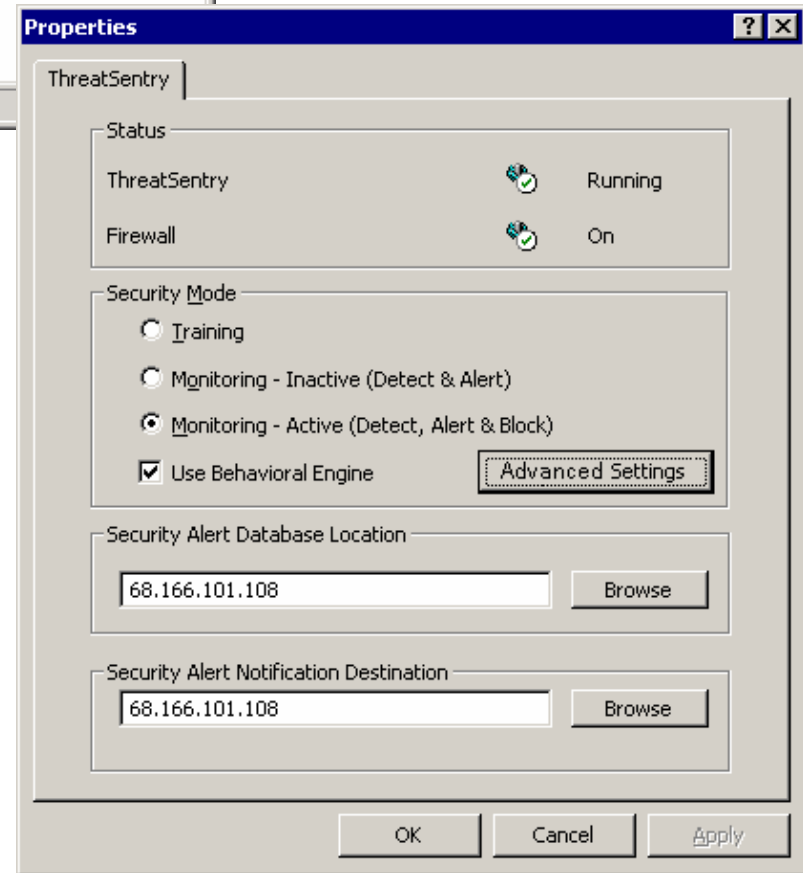
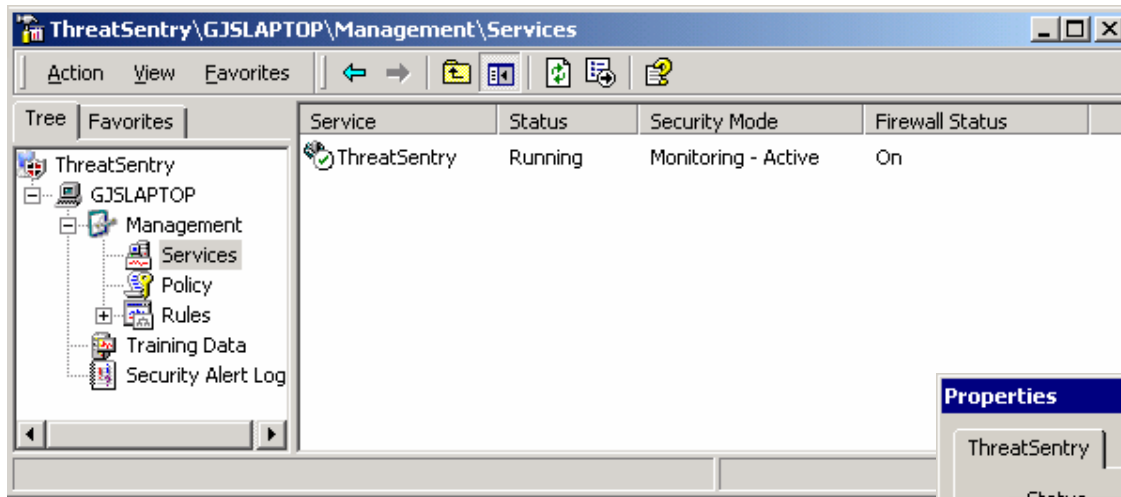


- MMC
 가 , 가
 .
 가
 가
 가 :
 (Management),
 (Training Data),
 (Security Alert Log).



(Management) – 가 ; (Service),
 (Policy), (Rules).
 , (running/down), - (Training, Monitoring
 – Inactive, Monitoring Active), (On/Off) .

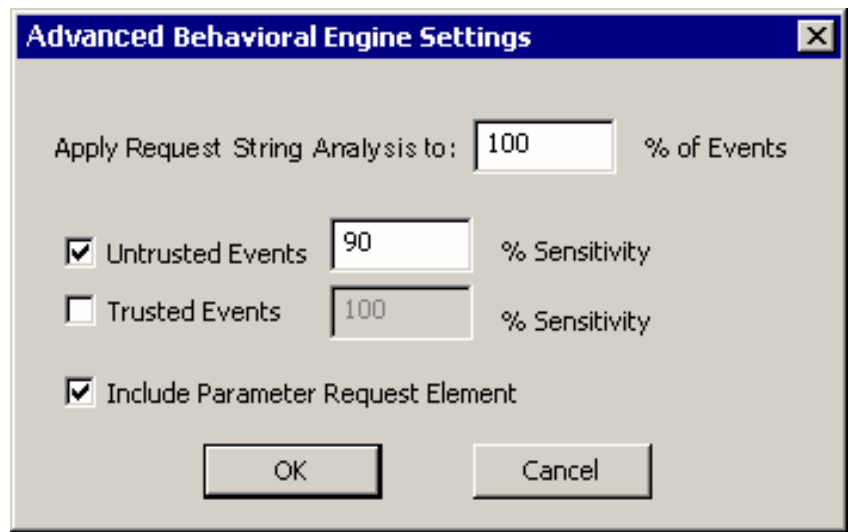




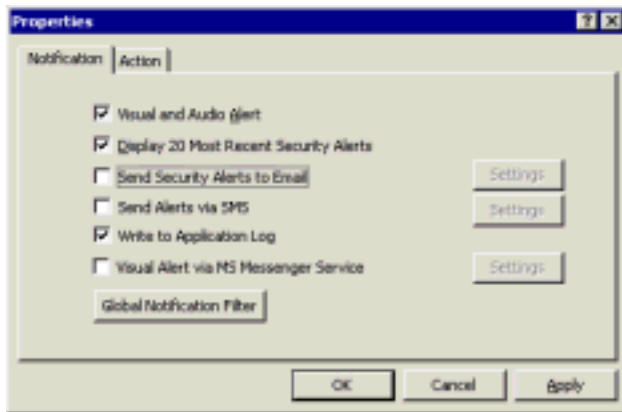
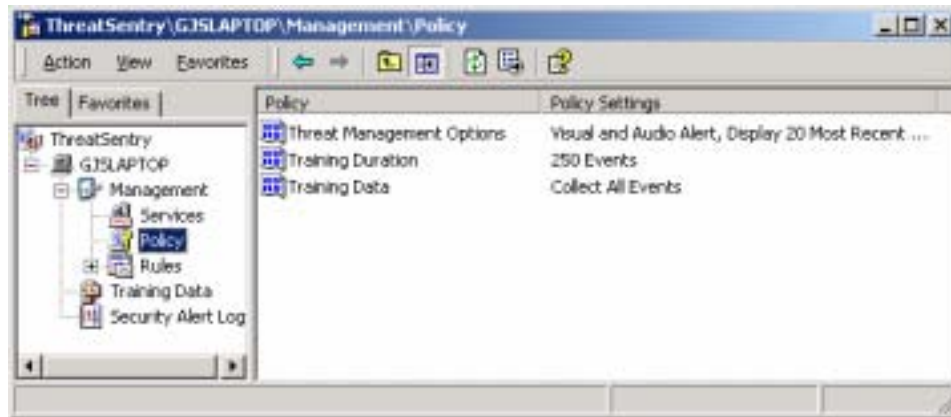
Properties) : (Services 가
/
()
가 .
(properties) .

URL : IIS 14
 (Advanced Settings) URL

100%
 URL ()
 /
 100%
 50%
 5%
 URL
 90%
 URL 가
 90%



- 가 (Policy): 가
, 가

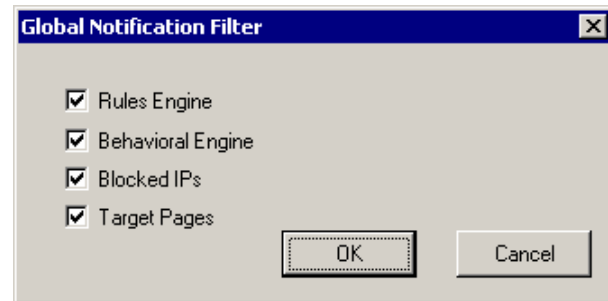


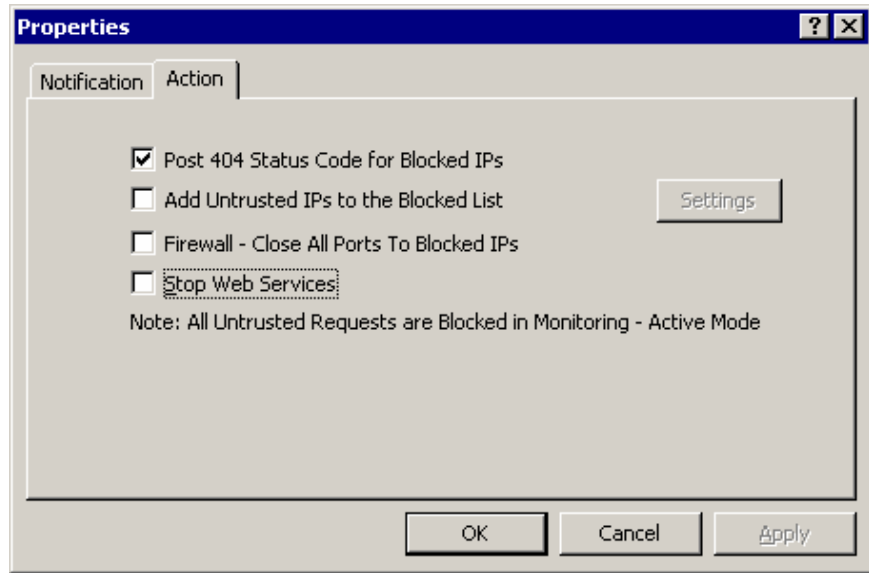
- - (Threat Management Options): 가

(Notification) (Action).
가

가 가

(Global Notification Filter):





(Threat Management Options):

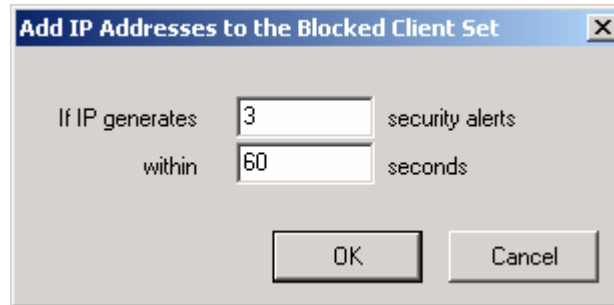
-404 : IP
404 .

- IP 가:
IP
가 . 가 IP

- (Firewall): 가 IP

- (Stop Web Services): 가 IIS

IP 가(Add Untrusted IPs to the Blocked List)
IP가



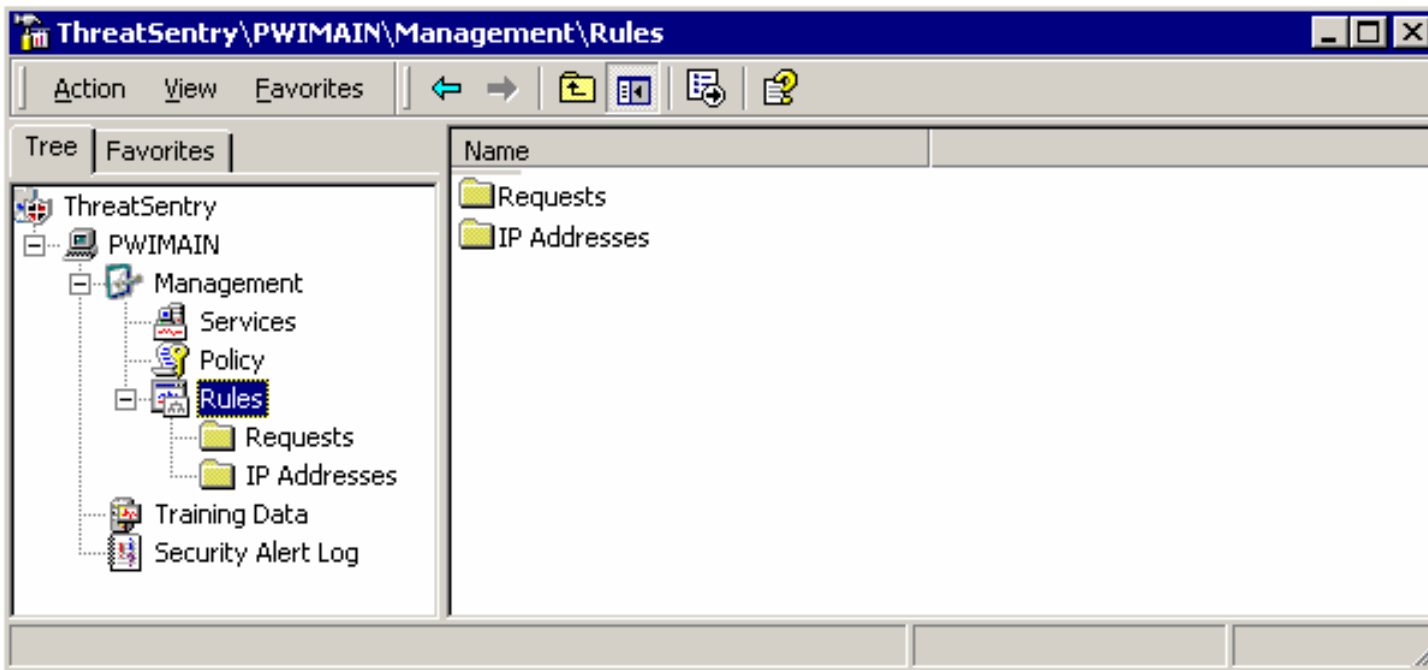
— (Rules) -
 (Application Firewall)

(knowledgebase)

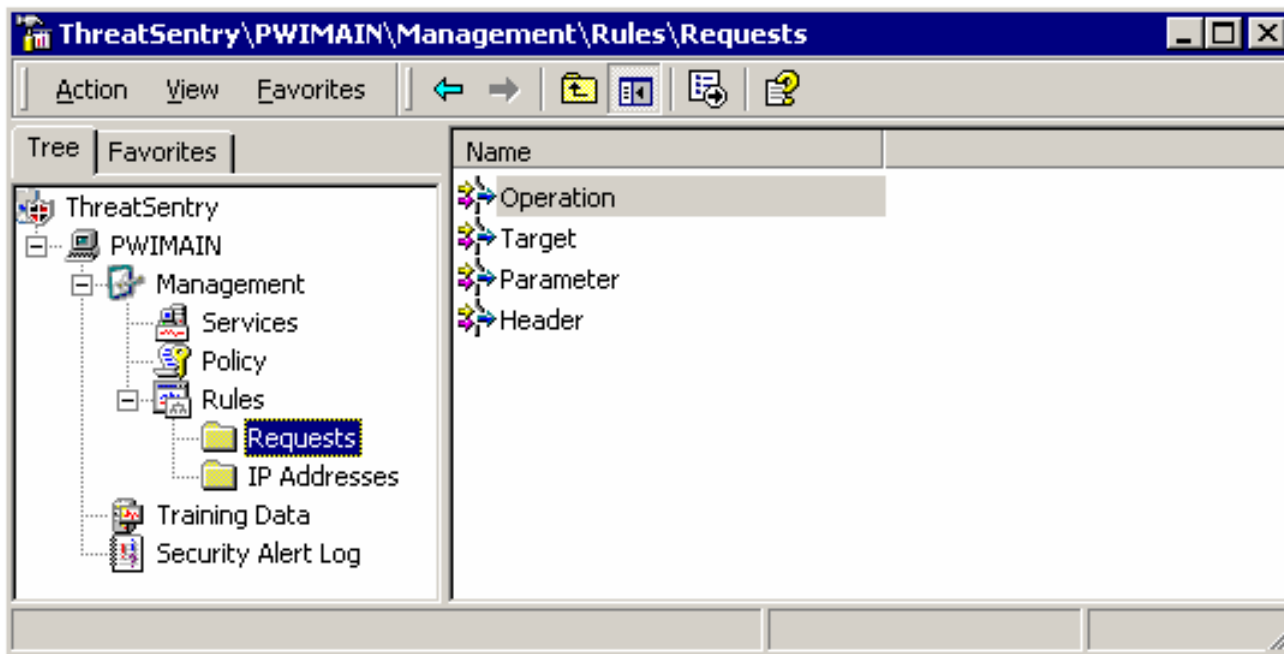
가 가 :

1) (Requests):

2) IP (IP Addresses):
 / IP



가 HTTP (Multi Digital Vector) 가 Requests (Operation, Target, Parameter, Header)



(Target):

. ()

가 , , 가 가

가

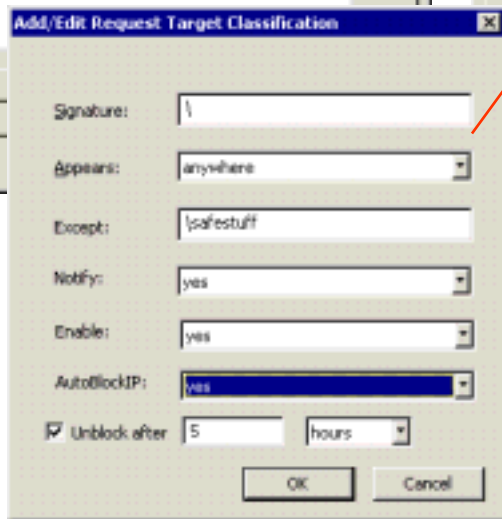
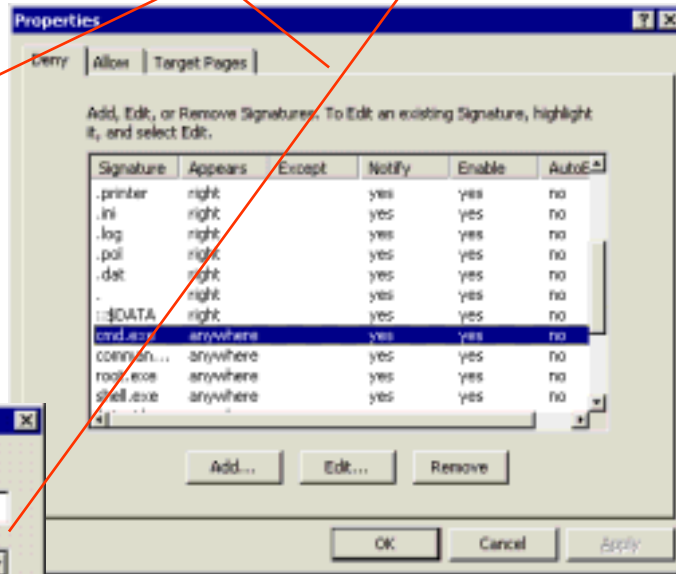
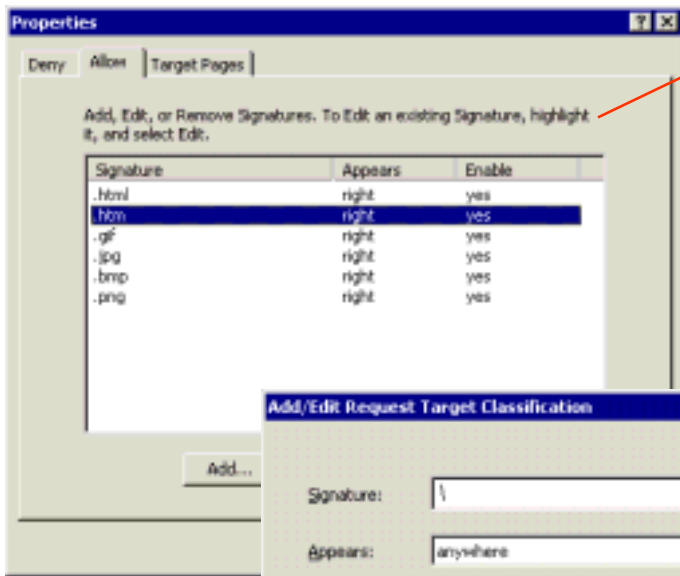
가

가

가

가

가 IP



. IP

(AutoBlockIP)

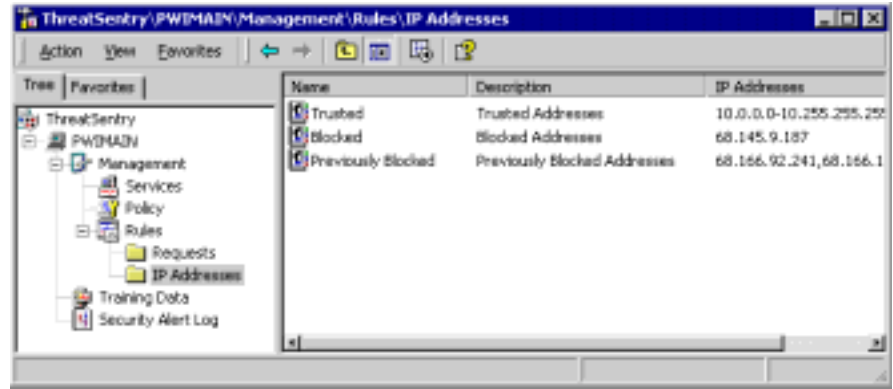
IP

IP

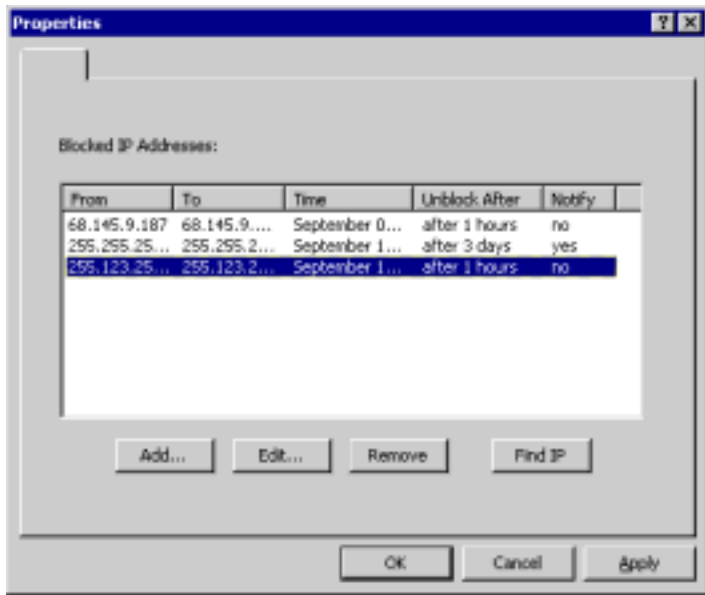
가 IP

— IP : The IP
(Thrustrd),
(Blocked) IP

IP
(Previously
Blocked)



IP . IP
IP 가 ,



IP IP
From and To
IP
IP가
가
(Notify)
/

(Training Data) –

가
(Training Data)

가
“Untrusted()”()

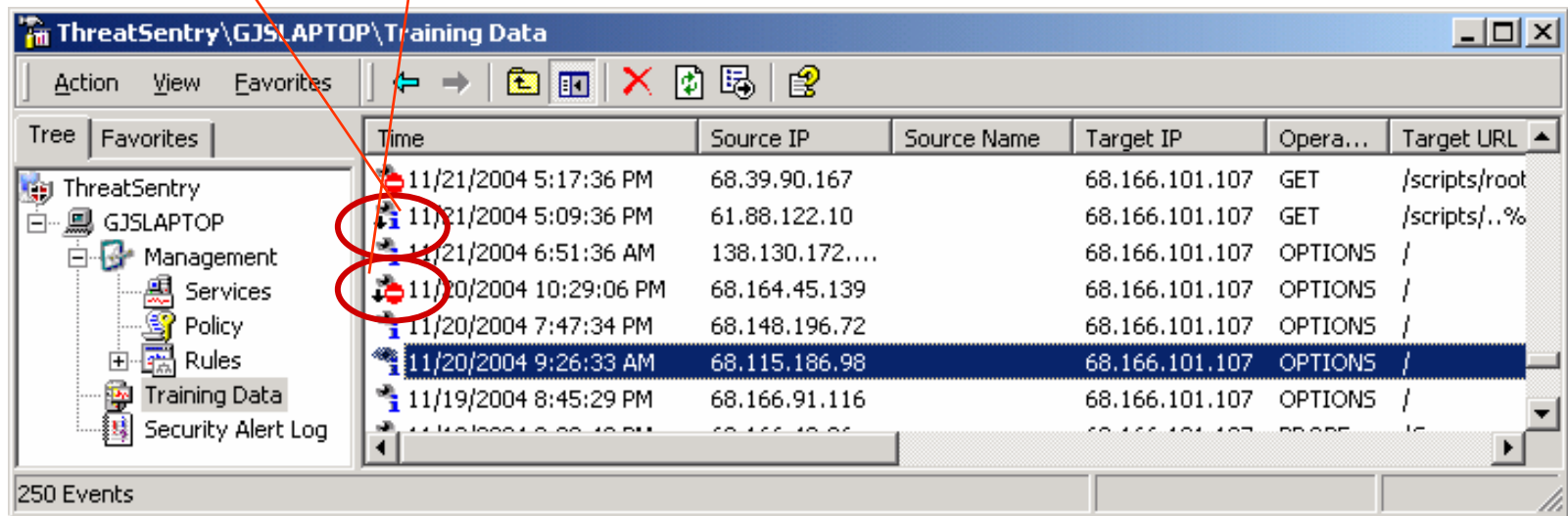
가 가
“Trusted()”()

: Time, Source IP, Source Name, Target IP, Operation, Target URL, Parameter, HTTP Status, Win32 Status, Bytes Sent, Bytes Received, Processing Time, Type, Security

The screenshot shows a window titled "ThreatSentry\PWIMAIN\Training Data" with a table of training events. The table has columns for Time, Source IP, Source Name, Target IP, Operation, Target URL, and Parameter. The left sidebar shows a tree view with folders like ThreatSentry, PWIMAIN, Management, Services, Policy, Rules, Training Data, and Security Alert Log. The bottom status bar indicates "117 Events".

Time	Source IP	Source Name	Target IP	Operation	Target URL	Parameter
8/10/2005 8:39:32 PM	68.166.207.101		68.166.101.108	OPTIONS	/	
8/10/2005 8:48:09 PM	68.166.31.252		68.166.101.108	OPTIONS	/	
8/31/2005 7:56:56 PM	68.166.80.154		68.166.101.108	OPTIONS	/	
8/3/2005 1:27:23 AM	172.208.127.97		68.166.101.108	GET	/	
8/3/2005 1:41:21 AM	203.192.201.22		68.166.101.108	GET	/cgi-bin/openwebmail/...	
8/3/2005 1:53:35 AM	68.55.86.237		68.166.101.108	GET	/	
8/3/2005 3:08:37 AM	68.33.88.205		68.166.101.108	GET	/	
8/3/2005 3:11:34 AM	68.51.132.124		68.166.101.108	GET	/	

가



ThreatSentry\GJSLAPTOP\Training Data

Action View Favorites

Tree Favorites

Time	Source IP	Source Name	Target IP	Opera...	Target URL
11/21/2004 5:17:36 PM	68.39.90.167		68.166.101.107	GET	/scripts/root
11/21/2004 5:09:36 PM	61.88.122.10		68.166.101.107	GET	/scripts/..%
11/21/2004 6:51:36 AM	138.130.172....		68.166.101.107	OPTIONS	/
11/20/2004 10:29:06 PM	68.164.45.139		68.166.101.107	OPTIONS	/
11/20/2004 7:47:34 PM	68.148.196.72		68.166.101.107	OPTIONS	/
11/20/2004 9:26:33 AM	68.115.186.98		68.166.101.107	OPTIONS	/
11/19/2004 8:45:29 PM	68.166.91.116		68.166.101.107	OPTIONS	/

250 Events

(Security Alerts) –
가

가

()가 , ()




OK

가

IIS

Security Alert Detail and Management Options [X]

 GJSLAPTOP

Stop IIS

To Stop Web services, select the <Stop IIS> button below. To acknowledge the event without additional action, select <OK>.

Event Details

Time: 11/17/2004 9:20:27
Most Recent Un-reviewed Alert: 11/15/2004 13:32:03
Originator IP Address: 222.182.6.112
Server IP Address: 68.166.101.107
Request: GET
HTTP Status: 0
Time for processing: 0
Bytes Received: 0
Bytes Sent: 0

Target <http://www.ebay.com/>

Stop IIS OK

가 가

: Time, Source IP, Source Name, Target IP, Operation, Target URL and Parameter, Parameter, HTTP Status, Win32 Status, Bytes Sent, Bytes Received, Processing Time, Type, Security Mode and Event Source.

The screenshot shows the ThreatSentry Security Alert Log window. The title bar reads 'ThreatSentry\PWIMAIN\Security Alert Log'. The window contains a table with the following columns: Time, Source IP, Source Name, Target IP, Operation, Target URL, and Parameter. The table lists several events from 9/3/2005. The left sidebar shows a tree view with 'ThreatSentry' expanded to 'PWIMAIN', which includes 'Management', 'Training Data', and 'Security Alert Log'. The status bar at the bottom indicates '160 Events'.

Time	Source IP	Source Name	Target IP	Operation	Target URL	Parameter
9/3/2005 5:03:38 PM	68.145.9.187		68.166.101.108	OPTIONS	/	
9/3/2005 4:25:47 PM	68.166.121.130		68.166.101.108	GET	/scripts/..%25f../winnt/system32/...	/c+dir
9/3/2005 4:25:44 PM	68.166.121.130		68.166.101.108	GET	/scripts/..%25%35%63../winnt/sys...	/c+dir
9/3/2005 4:25:32 PM	68.166.121.130		68.166.101.108	GET	/scripts/..%35c../winnt/system32...	/c+dir
9/3/2005 4:25:30 PM	68.166.121.130		68.166.101.108	GET	/scripts/..%35%63../winnt/syste...	/c+dir
9/3/2005 4:25:25 PM	68.166.121.130		68.166.101.108	GET	/scripts/..%c1%9c../winnt/system3...	/c+dir

ThreatSentry\PWIDEMO\Security Alert Log

Action View Favorites

Tree Favorites

Time	Source IP	Source Name	Target IP
11/29/2004 4:08:10 PM	69.141.135.251		68.1
11/29/2004 4:08:10 PM	69.141.135.251		68.1
11/29/2004 4:08:10 PM	69.141.135.251		68.1
11/29/2004 4:08:07 PM	69.141.135.251		68.1
11/29/2004 4:08:07 PM	69.141.135.251		68.1
11/29/2004 4:08:07 PM	69.141.135.251		68.1

155 Events

Event Details and Management

Untrusted Event

General

Time: 11/17/2004 9:20:27 AM
Bytes Sent: 0
Bytes Received: 0
Processing Time: 0
HTTP Status: 0
Win32 Status: 0
Type: Predefined rules, target

Target

Server: 68.166.101.107
Request: GET
URL: http://www.ebay.com/
Parameters:

Originator

IP Address: 222.182.6.112
User:
DNS Lookup:

WHOIS Lookup:

OrgName: Asia Pacific Network Information Centre
OrgID: APNIC

Start Lookup Copy to Clipboard

Classify Event as Trusted Close

가

IP

가

IP

가

ThreatSentry - [ThreatSentry\PWDMAIN\Security Alert Log]

Console Window Help

Action View Favorites

Tree Favorites

ThreatSentry
PWDMAIN
Management
Training Data
Security Alert Log

Time	Source IP	Target URL	Target IP	Parameter	Type
10/28/2005 3:50:24 PM	69.141.255.167	/nullida	68.166.101.108	NNNNNNNNNNNNNNNN...	Predefined rules, target (.ida)
10/28/2005 3:50:24 PM	69.141.255.167	/scripts/..%255c..%2550vwnnt/syst...	68.166.101.108	(c+md+c)EXPLOIT_DETE...	Predefined rules, target (..)
10/28/2005 3:50:24 PM	69.141.255.167	/listart.asp	68.166.101.108		Predefined rules, header (translate:F)
10/28/2005 3:50:24 PM	69.141.255.167	/listart.asp::\$DATA	68.166.101.108		Predefined rules, target (::\$data', \')
10/28/2005 3:50:24 PM	69.141.255.167	/listart.asp	68.166.101.108		Predefined rules, header (translate:F)
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp::\$DATA	68.166.101.108		Predefined rules, target (::\$data', \')
10/28/2005 3:50:23 PM	69.141.255.167	/msadc/msadcs.dll/AdvancedDataFa...	68.166.101.108		Predefined rules, target (.msadc)
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp	68.166.101.108		Predefined rules, header (translate:F)
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp::\$DATA	68.166.101.108		Predefined rules, target (::\$data', \')
10/28/2005 3:50:23 PM	69.141.255.167	/scripts/..%cd%af.._jwinnt/system3...	68.166.101.108	(c+md+c)EXPLOIT_DETE...	Predefined rules, target (..)
10/28/2005 3:50:23 PM	69.141.255.167	/null.htm	68.166.101.108	C:\Webhitsfile\listart.as...	Predefined rules, target (.htm)
10/28/2005 3:50:23 PM	69.141.255.167	/SOME_SITE/global.asa+.htm	68.166.101.108		
10/28/2005 3:50:23 PM	69.141.255.167	/null.htm	68.166.101.108		
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp	68.166.101.108		
67		/scripts/..%cd%af.._jwinnt/system3...	68.166.101.108		
67		/null.htm	68.166.101.108	C:\Webhitsfile=)listart.as...	Predefined rules, target (.htm)
67		/scripts/EXPLOIT_BAT.bat"+&+d+e+...	68.166.101.108		Predefined rules, target (.script)
67		/nullida	68.166.101.108	NNNNNNNNNNNNNNNN...	Predefined rules, target (.ida)
10/28/2005 3:50:23 PM	69.141.255.167	/msadc/msadcs.dll/AdvancedDataFa...	68.166.101.108		Predefined rules, target (.msadc)
10/28/2005 3:50:23 PM	69.141.255.167	/msadc/msadcs.dll/AdvancedDataFa...	68.166.101.108		Predefined rules, target (.msadc)
10/28/2005 3:50:23 PM	69.141.255.167	/msadc/msadcs.dll/AdvancedDataFa...	68.166.101.108		Predefined rules, target (.msadc)
10/28/2005 3:50:23 PM	69.141.255.167	/null.htm	68.166.101.108	C:\Webhitsfile=)listart.as...	Predefined rules, target (.htm)
10/28/2005 3:50:23 PM	69.141.255.167	/SOME_SITE/global.asa+.htm	68.166.101.108		Predefined rules, target (.htm)
10/28/2005 3:50:23 PM	69.141.255.167	/null.htm	68.166.101.108	C:\Webhitsfile=)listart.as...	Predefined rules, target (.htm)
10/28/2005 3:50:23 PM	69.141.255.167	/scripts/..%cd%af.._jwinnt/system3...	68.166.101.108	(c+md+c)EXPLOIT_DETE...	Predefined rules, target (..)
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp::\$DATA	68.166.101.108		Predefined rules, target (::\$data', \')
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp	68.166.101.108		Predefined rules, header (translate:F)
10/28/2005 3:50:23 PM	69.141.255.167	/listart.asp	68.166.101.108		Predefined rules, header (translate:F)
10/28/2005 3:50:23 PM	69.141.255.167	/SOME_SITE/global.asa+.htm	68.166.101.108		Predefined rules, target (.htm)
10/28/2005 3:50:23 PM	69.141.255.167	/scripts/..%cd%af.._jwinnt/system3...	68.166.101.108	(c+md+c)EXPLOIT_DETE...	Predefined rules, target (..)

16709 Events

.ida

IIS ISAPI HTR



: 02)717-9431
: 02)717-9404
: www.rovermoot.co.kr
: info@rovermoot.co.kr



NTFAQ
: 010-5241-1860
: www.ntfaq.co.kr
: ntfaq@ntfaq.co.kr



Tel : 02-3486-9220
Fax: 02-3486-9331
<http://www.softmail.co.kr>