

網路障礙分析與資安事件監控軟體 N-Reporter 基礎介紹

台中區網中心 鄒珮甄

基礎畫面介紹

- 請輸入 <http://nfa.tcrc.edu.tw>
- 輸入帳號密碼
- 不要封鎖視窗



基礎畫面介紹

事件過濾設定 - Mozilla Firefox

nfa.tccrc.edu.tw/event/event_query.html?sno=AAwVA%3DIQAFJDgVPT86KGdiP3wlODY%2FBAZXCD1QUFEbB1QITVERURsBVA9F#complex

臺中區域網路中心 模擬畫面

nchu [中興大學]

事件 ▶ 事件查詢 ☒ 頁面自動更新 (118秒)

+ 查詢條件 進階條件 Show All 重新輸入

查詢時間區段 ☒ 選擇時間區段 5分鐘內 ☐ 過去 ☐ 起迄時間

報表製作依據 ☐ Syslog ☒ Flow

資料時間範圍: 2016/03/28 14:13:27 ~ 2016/03/28 14:13:42 總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port	目
2016/03/28 14:13:42	59.125.191.252		TW	43180		TCP	140.120.28.113	中興大學	TW	52782	目
2016/03/28 14:13:42	140.120.209.174	中興大學	TW	11369		TCP	60.174.145.152		CN	7463	目
2016/03/28 14:13:42	140.120.209.174	中興大學	TW	12063		TCP	114.46.167.167		TW	7567	目
2016/03/28 14:13:42	140.120.104.48	中興大學	TW	50012		TCP	210.200.25.110		TW	443	目
2016/03/28 14:13:42	125.227.216.237		TW	50099		TCP	140.120.113.19	中興大學	TW	36590	目
2016/03/28 14:13:42	223.136.64.166		TW	33513		TCP	140.120.53.153	中興大學	TW	80	目
2016/03/28 14:13:42	140.120.242.2	中興大學	TW	47869		TCP	106.3.74.131		CN	9001	目
2016/03/28 14:13:42	140.120.12.187	中興大學	TW	80	http	TCP	171.15.157.35		CN	52770	目
2016/03/28 14:13:42	140.120.209.194	中興大學	TW	53	dns	UDP	115.231.25.139		CN	53074	目
2016/03/28 14:13:42	140.120.28.114	中興大學	TW	27973		TCP	61.216.75.73		TW	27930	目
2016/03/28 14:13:42	140.120.55.138	中興大學	TW	51013		TCP	112.121.88.135		TW	2099	目
2016/03/28 14:13:42	140.120.136.52	中興大學	TW	9159		UDP	111.184.131.14		TW	63575	目
2016/03/28 14:13:42	1.162.82.103		TW	7048		UDP	140.120.13.180	中興大學	TW	8177	目

< First 1 2 3 4 5 6 7 8 9 10 Last >

每頁顯示: 50 目前所在頁面: 1 of 200

基礎畫面介紹



事件★



報表★



設備管理



系統管理★



收合功能視窗

基礎畫面介紹-事件



事件



🔍 事件查詢



📁 已儲存查詢條件



基礎畫面介紹-事件



事件 ▶ 事件查詢

☒ 頁面自動更新 (110秒)

+ 查詢條件

進階條件

Show All

重新輸入

查詢時間區段 ☒ 選擇時間區段 5分鐘內 ☐ 過去 ☐ 起迄時間

報表製作依據 ☒ Syslog ☐ Flow

資料時間範圍: 2016/03/28 14:25:42 ~ 2016/03/28 14:26:03 總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的
2016/03/28 14:26:03	203.133.9.69		TW	53	dns	UDP	1
2016/03/28 14:26:03	203.133.25.28		TW	80	http	TCP	1
2016/03/28 14:26:03	140.120.227.161	中興大學	TW	21620		TCP	1
2016/03/28 14:26:03	140.120.1.3	中興大學	TW	64595		UDP	2
2016/03/28 14:26:03	23.48.130.72		US	443	https	TCP	1
2016/03/28 14:26:03	118.161.189.164		TW	9516		UDP	1
2016/03/28 14:26:03	118.163.219.97		TW	1077		TCP	1
2016/03/28 14:26:03	140.120.13.180	中興大學	TW	8177		UDP	3
2016/03/28 14:26:03	140.120.32.236	中興大學	TW	1966		TCP	1

<

First

1

2

3

4

5

6

7

8

9

10

Last

>

每頁顯示: 50 目前所在頁面: 1 of 200

基礎畫面介紹-事件

發生資安通報!



發佈編號	ASOC-INT-201603-0633	發佈時間	2016-03-03 09:17:02
事件類型	對外攻擊	發現時間	2016-03-03 09:02:06
事件主旨	通報:[國立中興大學]140.120.90.81 Telnet.Login.Brute.Force		
事件描述	ASOC 發現貴單位(國立中興大學)所屬 140.120.90.81 疑似對外進行 Telnet.Login.Brute.Force 攻擊		

Telnet.Login.Brute.Force 攻擊

基礎畫面介紹-事件



發生資安通報II

發佈編號	ASOC-INT-201603-0621	發佈時間	2016-03-03 09:16:20
事件類型	對外攻擊	發現時間	2016-03-03 08:54:11
事件主旨	通報:[中興區網中心]163.28.82.5 utm: DNS		
事件描述	ASOC 發現貴單位(中興區網中心)所屬 163.28.82.5 疑似對外進行 utm: DNS 攻擊		

事件描述 ASOC 發現貴單位(中興區網中心)所屬 163.28.82.5 疑似對外進行 utm: DNS 攻擊

基礎畫面介紹-事件

事件過濾設定 - Mozilla Firefox

nfa.tcrc.edu.tw/event/event_query.html?sno=AgwSD%3DIXMQJDaDgCPTHe2diP3wIP2tsBAZXCD1XDQIbB1QITVEMAhscVAdI#complex

模 擬 畫 面

事件 ▾ 事件查詢 ☒ 頁面自動更新 (94秒)

+ 查詢條件

- 設備
- IP過濾
- Port 過濾

進階條件 Show All 重新輸入

☒ 選擇時間區段 5分鐘內 ☐ 過去 ☐ 起迄時間

☐ Syslog ☒ Flow

2016/03/28 14:29:43 ~ 2016/03/28 14:29:52 總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的
2016/03/28 14:29:52	140.120.209.174	中興大學	TW	51568		TCP	1
2016/03/28 14:29:52	140.120.49.88	中興大學	TW	53	dns	UDP	1
2016/03/28 14:29:52	140.120.47.149	中興大學	TW	80	http	TCP	1
2016/03/28 14:29:52	140.120.9.149	中興大學	TW	8690		UDP	1
2016/03/28 14:29:52	140.120.49.85	中興大學	TW	53	dns	UDP	4
2016/03/28 14:29:52	140.120.80.11	中興大學	TW	53	dns	UDP	6
2016/03/28 14:29:52	140.120.32.79	中興大學	TW	57009		UDP	1
2016/03/28 14:29:52	140.120.55.168	中興大學	TW	43285		UDP	2
2016/03/28 14:29:52	140.120.8.1	中興大學	TW	0		ICMP	5

< First 1 2 3 4 5 6 7 8 9 10 Last >

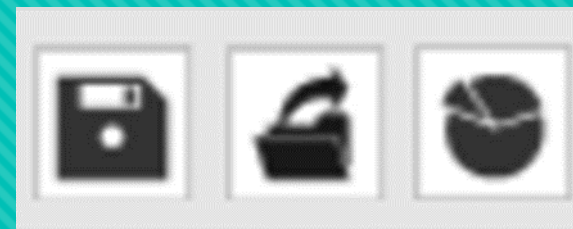
每頁顯示: 50 目前所在頁面: 1 of 200

Step 1: 查詢條件

Step 2: IP過濾

Step 3: 啟動查詢

基礎畫面介紹-事件-查詢事件



事件 ► 事件查詢 ☐ 頁面自動更新

+ 查詢條件 進階條件 Show All 重新輸入

查詢時間區段 ☐ 選擇時間區段 5分鐘內 ☐ 過去 ☒ 起迄時間 2016/3/3 00:00 ~ 2016/3/3 05:37

報表製作依據 ☐ Syslog ☒ Flow

IP過濾 ► ☒ 同時判定來源與目的IP ☐ 判定來源或目的IP 來源IP: 140.120.90.81

資料時間範圍: 2016/03/03 05:00:07 ~ 2016/03/03 05:28:52 總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	48784		TCP	6.170.201.117		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	36992		TCP	6.170.201.34		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	45100		TCP	6.170.201.119		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	41744		TCP	6.170.201.45		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	53293		TCP	6.170.201.49		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	59966		TCP	6.170.201.42		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	33579		TCP	6.170.201.55		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	46148		TCP	6.170.201.62		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	37771		TCP	6.170.201.67		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54718		TCP	6.170.201.70		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	36798		TCP	6.170.201.120		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54661		TCP	6.170.201.75		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	38583		TCP	6.170.201.79		US	23

基礎畫面介紹-事件-儲存事件結果

事件過濾設定 - Mozilla Firefox

nfa.tsrc.edu.tw/event/event_query.html?sno=AgwSD%3DIXMQJDaDgCPTHe2diP3wlP2tsBAZXCD1XDQIbB1QITVEMAhscVAdI#complex

模 擬 畫 面

nchu [中興大學]

事件 ► 事件查詢 ☐ 頁面自動更新

+ 查詢條件 進階條件 Show All 重新輸入

查詢時間區段 ☐ 選擇時間區段 5分鐘內 ☐ 過去 ☒ 起迄時間 2016/3/3 00:00 ~ 2016/3/3 05:37

報表製作依據 ☐ Syslog ☒ Flow

IP過濾 ☒ 同時判定來源與目的IP ☐ 判定來源或目的IP 來源IP: 140.120.90.81

資料時間範圍: 2016/03/03 05:00:07 ~ 2016/03/03 05:28:52 總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	48784		TCP	6.170.201.117		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學					6.170.201.34		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學					6.170.201.119		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學					6.170.201.45		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學					6.170.201.49		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學					6.170.201.42		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	33579		TCP	6.170.201.55		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	46148		TCP	6.170.201.62		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	37771		TCP	6.170.201.67		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54718		TCP	6.170.201.70		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	36798		TCP	6.170.201.120		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54661		TCP	6.170.201.75		US	23
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	38583		TCP	6.170.201.79		US	23

儲存查詢條件

輸入查詢條件名稱: 140.120.90.81監測情形

確定 取消

First 1 2 3 4 5 6 7 8 9 10 Last 每頁顯示: 50 目前所在頁面: 1 of 200

基礎畫面介紹-報表

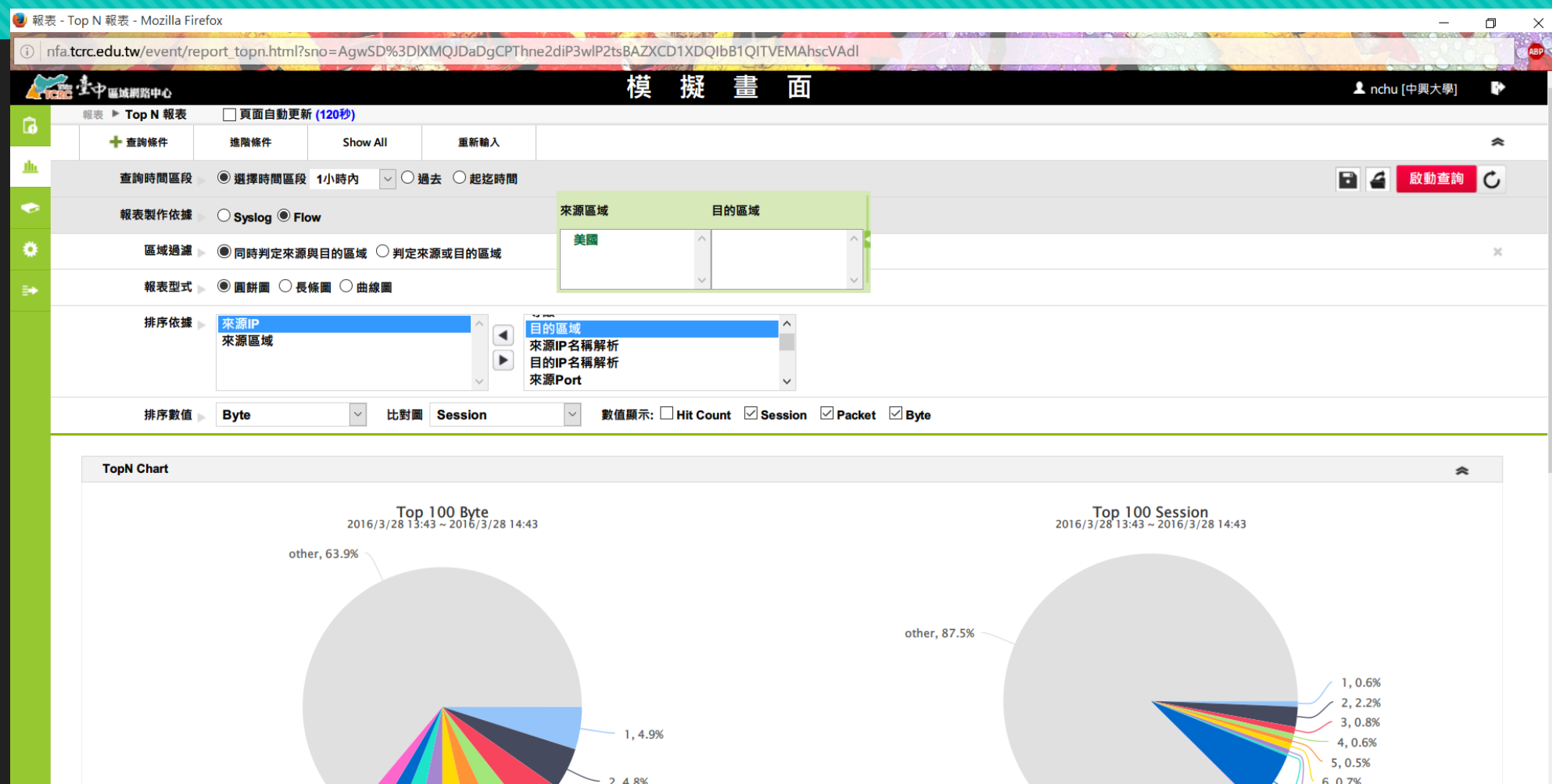


基礎畫面介紹-報表-TOP N



報表	
Top N	Top N 報表
分時監控報表	已儲存報表
趨勢分析	
異常IP阻擋 	
Flow 專屬報表	
2016/03/28 14:17:33	21

基礎畫面介紹-報表-TOP N-查詢美國到校流量



基礎畫面介紹-報表-分時監控報表

The screenshot displays the TCRS (臺中區域網路中心) web interface. The browser address bar shows the URL: `140.120.150.224 - 遠端桌面連線` and `nfa.tcrc.edu.tw/event/report_filter.html?sno=Aw0eA%3DIXEQIDa`. The page title is '報表' (Reports). The main content area shows a list of reports with the following options:

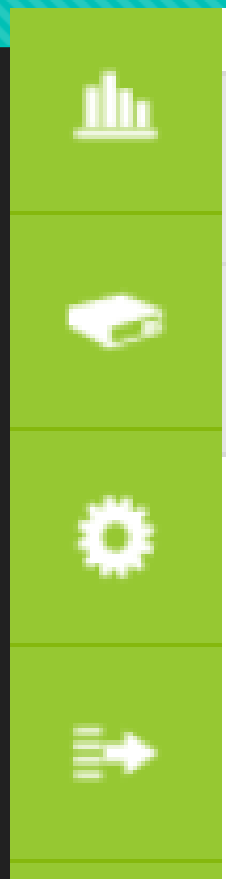
- 報表
- Top N
- 分時監控報表 (Selected)
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

The '分時監控報表' option is highlighted in green. A dropdown menu is visible, showing the following options:

- 訂製分時監控報表
- 查看分時監控報表
- 分時監控報表群組
- 分時監控異常列表

The interface also includes a sidebar with navigation icons (bar chart, graduation cap, gear, and a right-pointing arrow) and a footer section with the text '介面過濾' and '同時'.

基礎畫面介紹-報表-分時監控報表- 訂製分時監控報表-DNS監控



140.120.150.224 - 遠端桌面連線

nfa.tccrc.edu.tw/event/report_filter.html?sno=Aw0eA%3DIXEQIDaDgCb1hneWdiP311P2tu8AZXCW1XDQA6b1QHVEMAbscVAdQ

模 擬 畫 面

nchu [中興大學]

報表 ▶ 訂製分時監控報表

+ 查詢條件 進階條件 Show All 重新輸入

報表製作依據 ☐ Syslog ☒ Flow

Protocol ▶ N/A

IP過濾 ☐ 同時判定來源與目的IP ☐ 判定來源或目的IP

Port 過濾 ☒ 同時判定來源與目的Port ☐ 判定來源或目的Port

區域過濾 ☐ 同時判定來源與目的區域 ☐ 判定來源或目的區域

介面過濾 ☐ 同時判定流入與流出介面 ☐ 判定流入或流出介面

流量過濾 ☐ 流量(bytes) > [] ☐ 封包(packets) > []

封包大小 [] - [] (0-1500) (byte / packet)

時間範圍 []

設備 []

來源Port

Port 過濾

協定: Any

單一Port: []

Port 區段: [] - []

Port 名稱解析: Port Domain

+

dns

確定 取消

Copyright © 2009 N-Partner. All rights reserved.

下午 10:43
星期一
2016/3/28

基礎畫面介紹-報表-分時監控報表群組

140.120.150.224 - 遠端桌面連線

nfa.tsrc.edu.tw/event/report_filter_group_list.html?sno=Aw0eA%3DIXEQIDaDgCbThneWdiP3TTP2tuBAZXCWTXDQAbBTQJHVEMABscVAdQ

臺中區域網路中心 模擬畫面 nchu [中興大學]

報表 ▶ 分時監控報表群組 ☒ 頁面自動更新 (00:55)

總筆數: 2

操作	領域	報表名稱	報表製作依據	報表建立時間	最近修改時間	瀏覽
	中興大學	123	Flow	2016-03-18 14:49:00		
	中興大學	網站回應與訪問網站				

分時監控報表群組

名稱: 網站回應流量與訪問網站流量比較

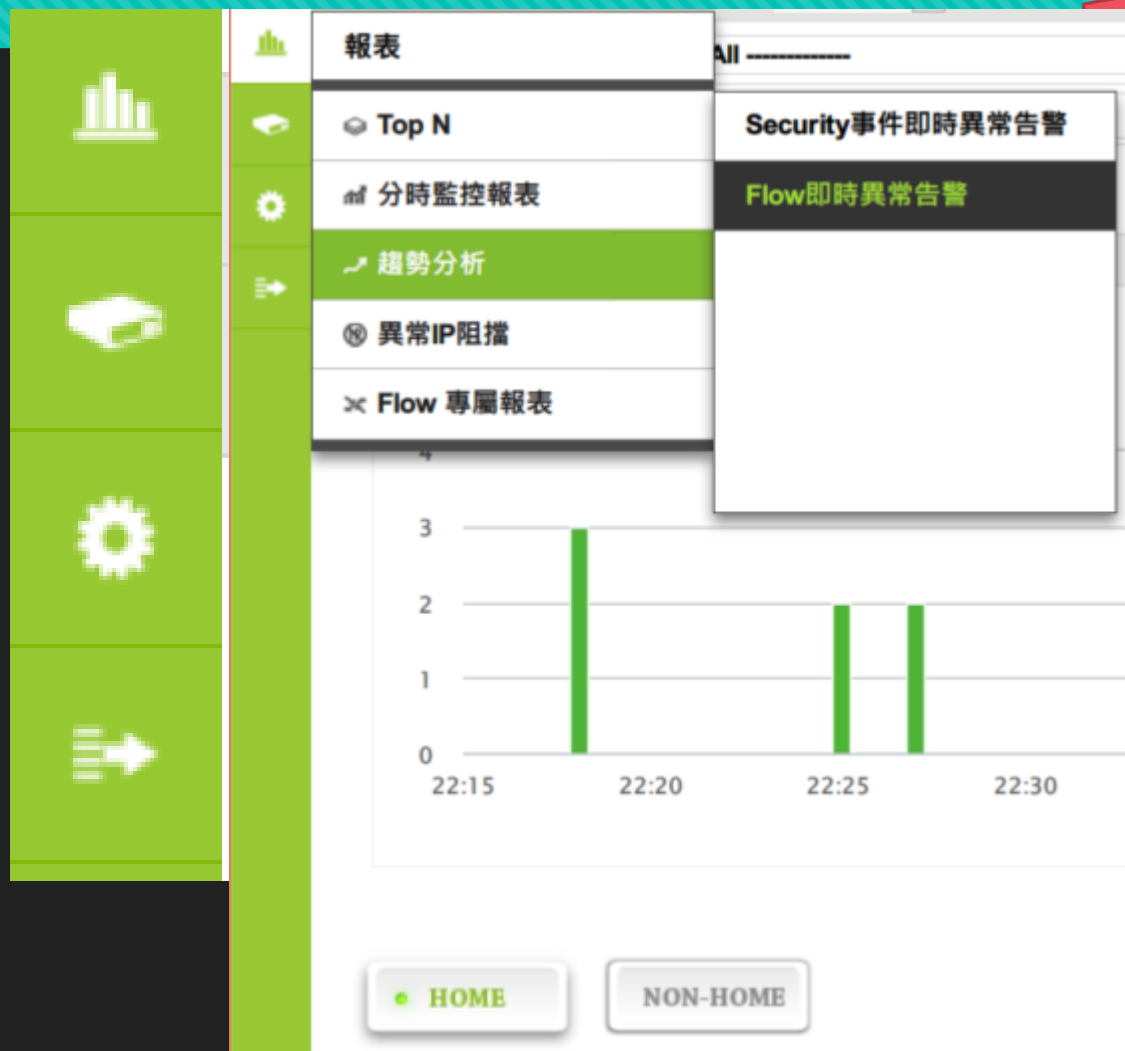
類型: ☐ Syslog ☒ Flow

In:

Out:

確定 取消

基礎畫面介紹-報表-趨勢分析



HOME NON-HOME

總筆數: 3

所屬領域	異常項目	攻擊者IP
中興大學	Burst Session on Source	140.120.239.1 (中興大學)
中興大學	Host Scan	140.120.236.7 (中興大學)
中興大學	Burst Session on Source	140.120.240.5 (中興大學)

基礎畫面介紹-設備管理



基礎畫面介紹-系統管理

