ISAC
校園資安服務平台

Efficient professional after-sales service
High-quality and rapid Security solution

Lastline
大中華區銷售總監　陳至彥

大綱

Agenda

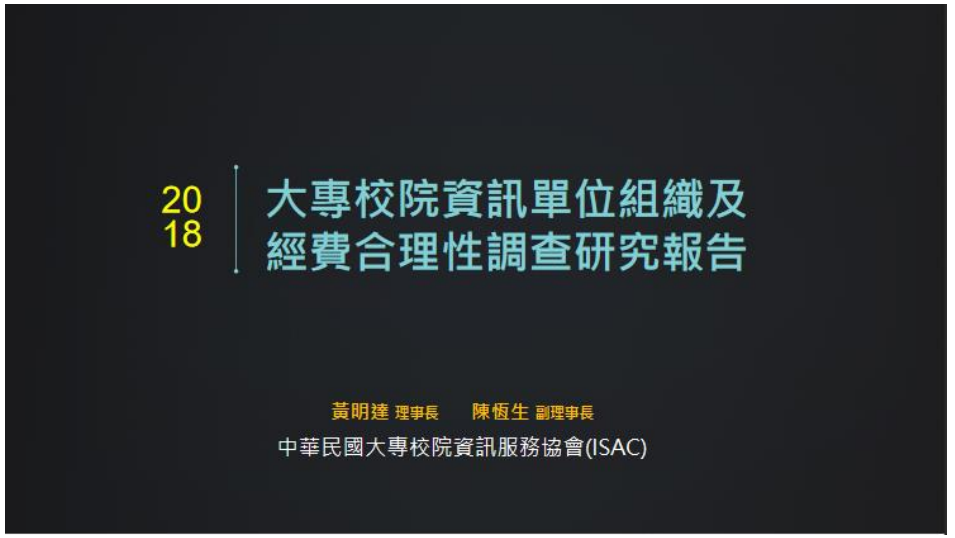
1. 緣起
2. 如何選商
3. PoC 結果分析
4. 資安服務平台介紹
5. 總結

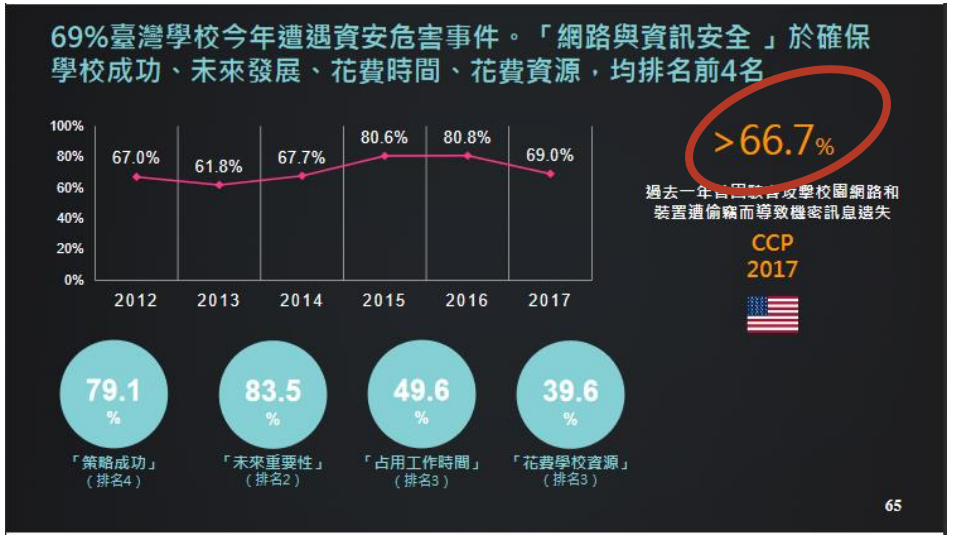
緣起

Initiative

2018 威脅情資

根據 2018/4/27 大專校院資訊單位組織及經費合理性調查研究報告



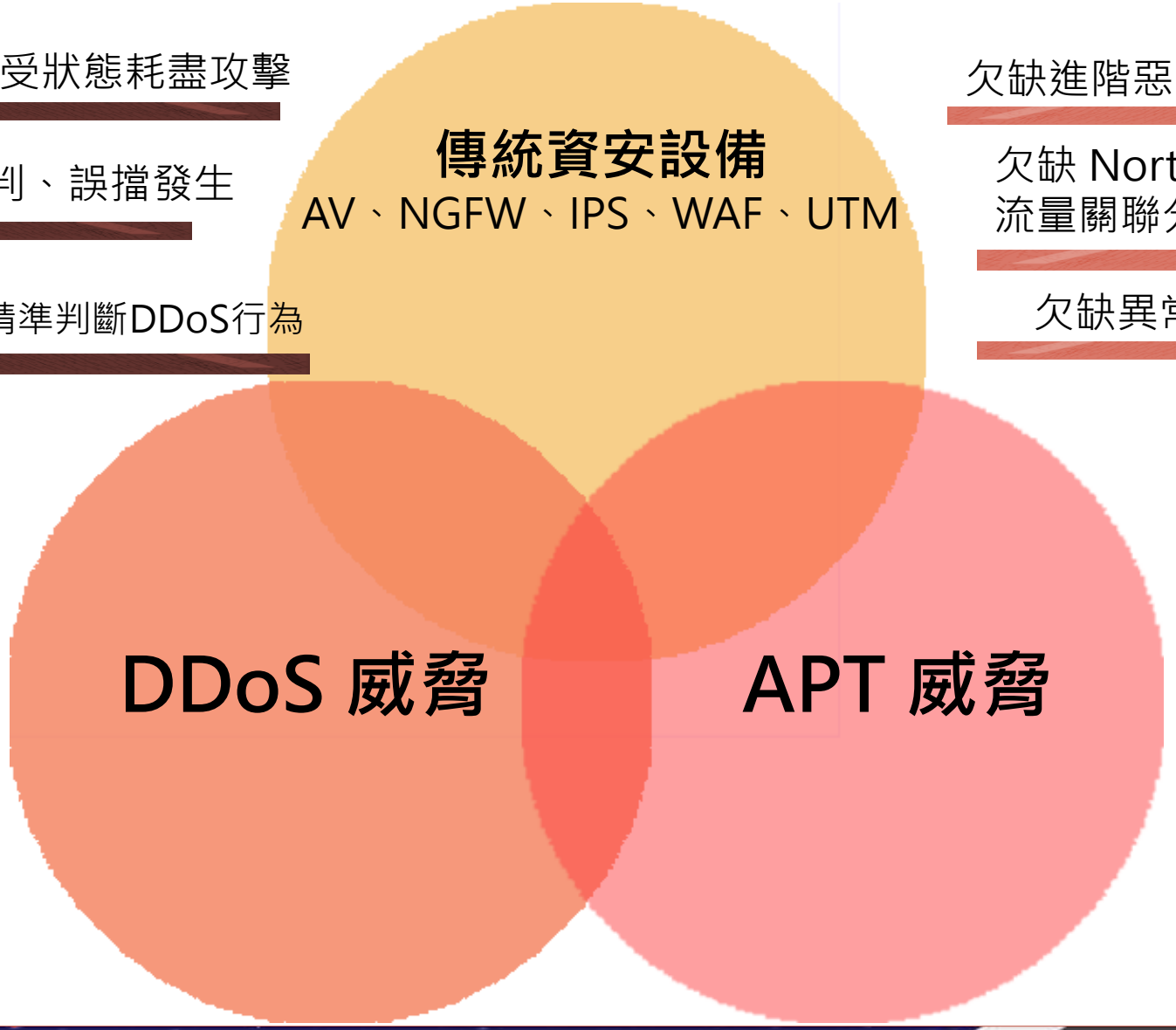


為何傳統設備無法有效防禦

狀態表架構，無法承受狀態耗盡攻擊

缺乏學習模式，易造成誤判、誤擋發生

靜態特徵碼比對方式，無法精準判斷DDoS行為



欠缺進階惡意程式靜/動態沙箱分析

欠缺 North-South 與 East – West 流量關聯分析

欠缺異常行為全景 Context 分析

如何選商

How To Choose

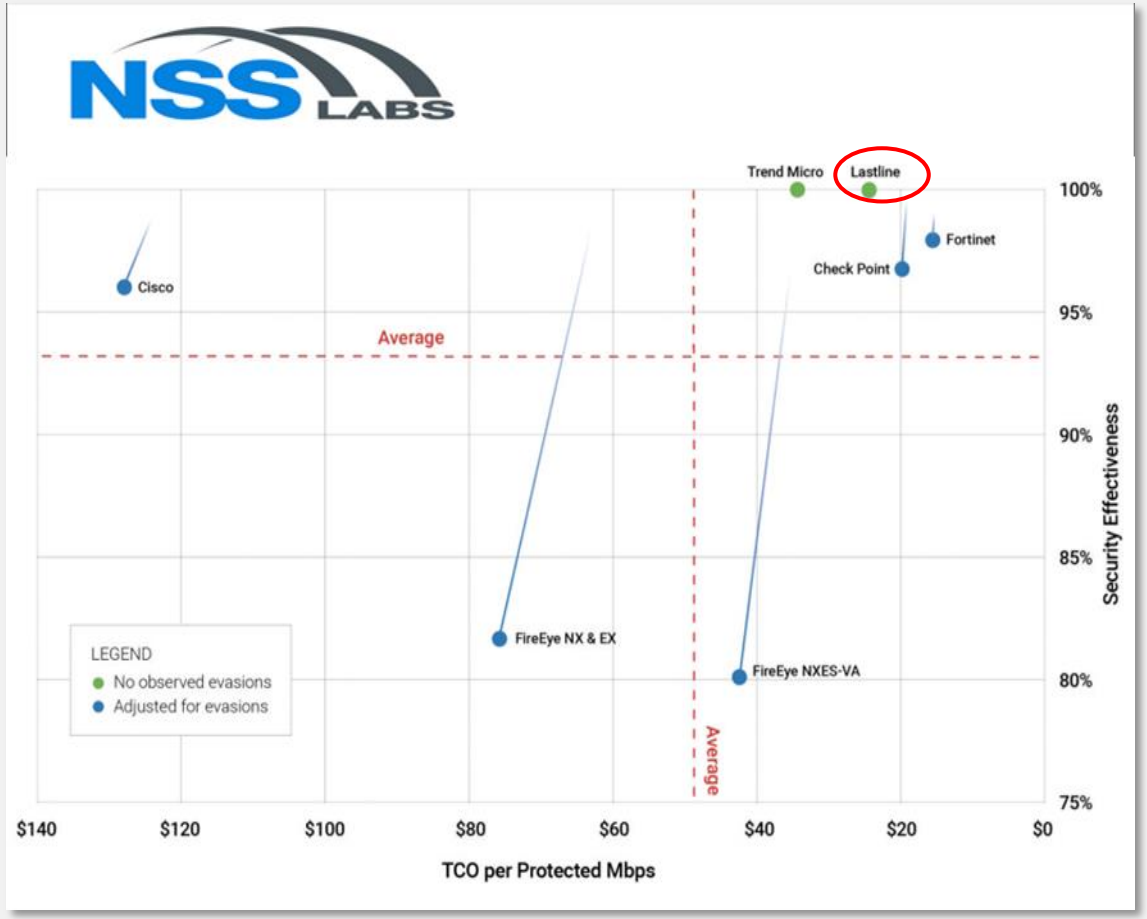
ISAC 選商原則

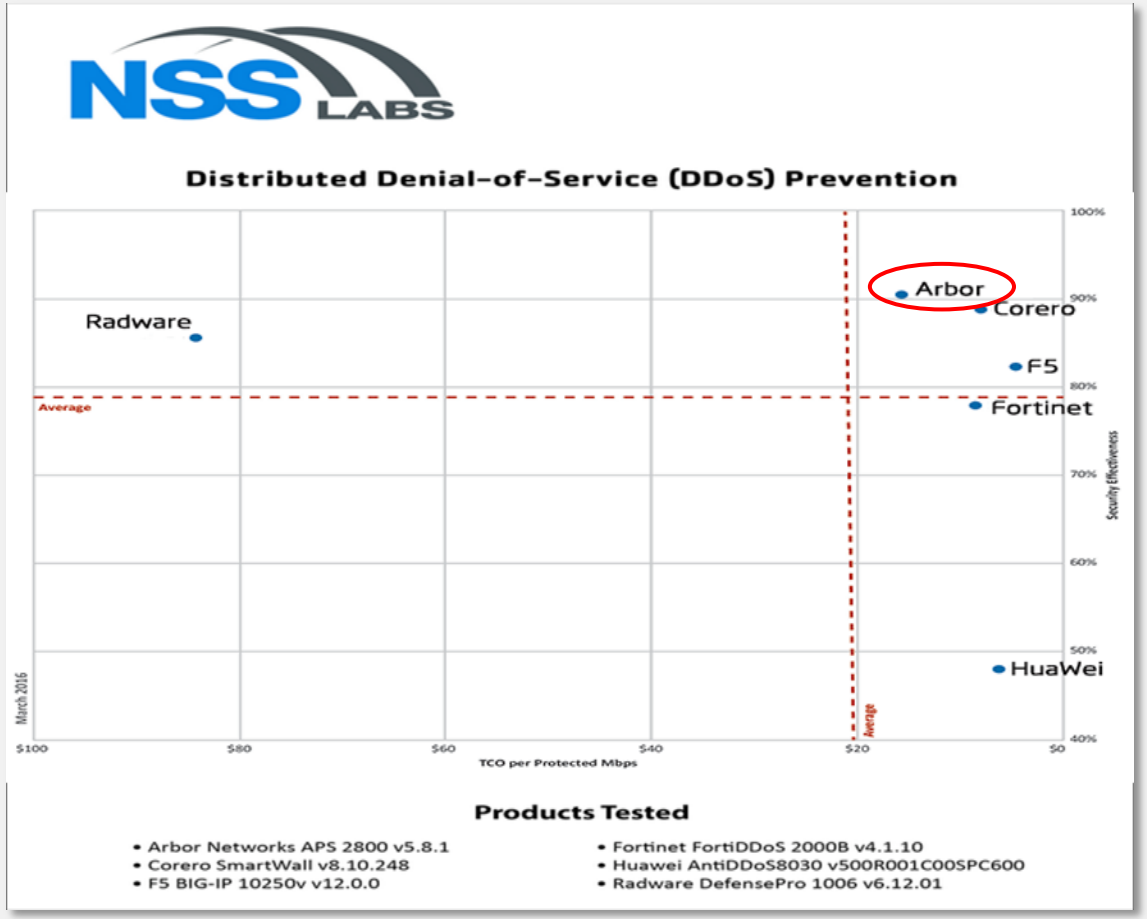
1.第三方權威研究機構評定為領導品牌

2.市場口碑

3.市場參考客戶名單

NSS-LAB評比

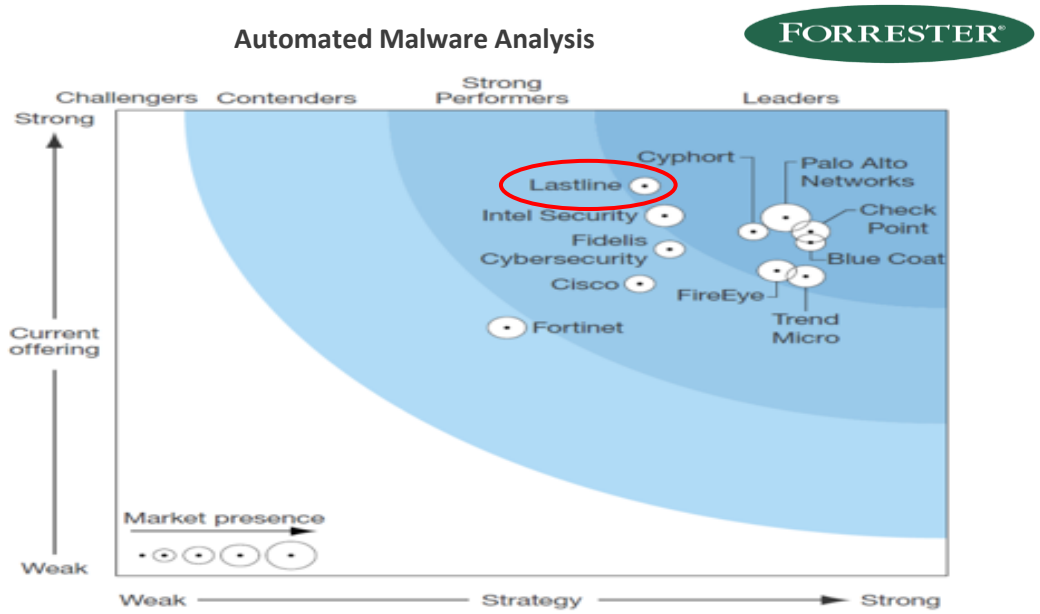


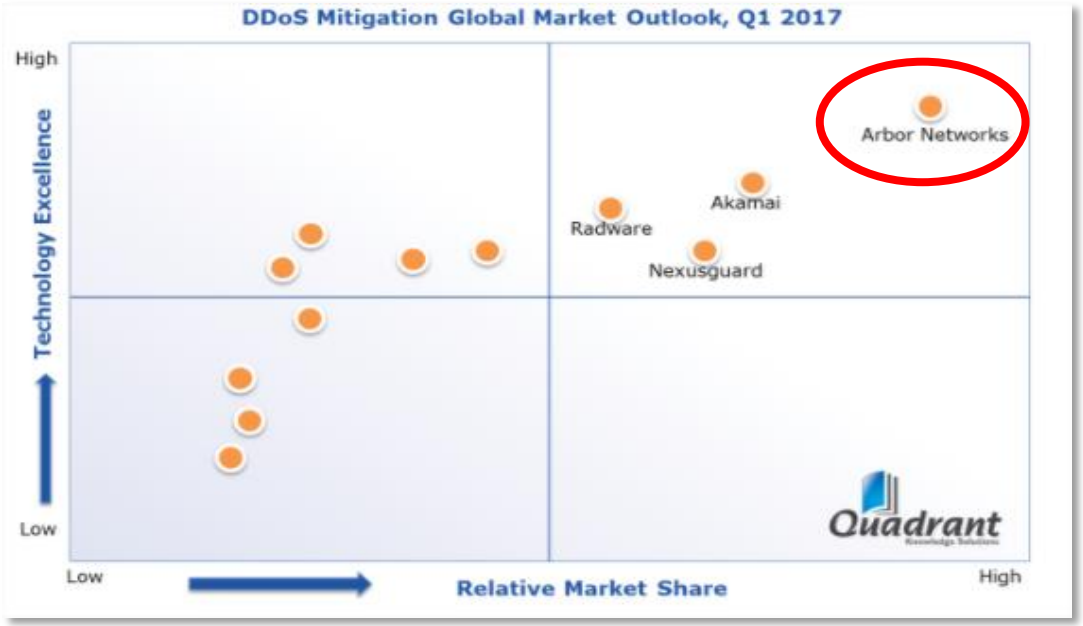


Lastline 是唯一一家具備 100% APT 檢測能力的廠商

Arbor 是唯一一家整體防禦力超過 90% 的DDoS 的廠商。

第三方權威研究機構一致認可 Arbor、LastLine 為世界領導品牌





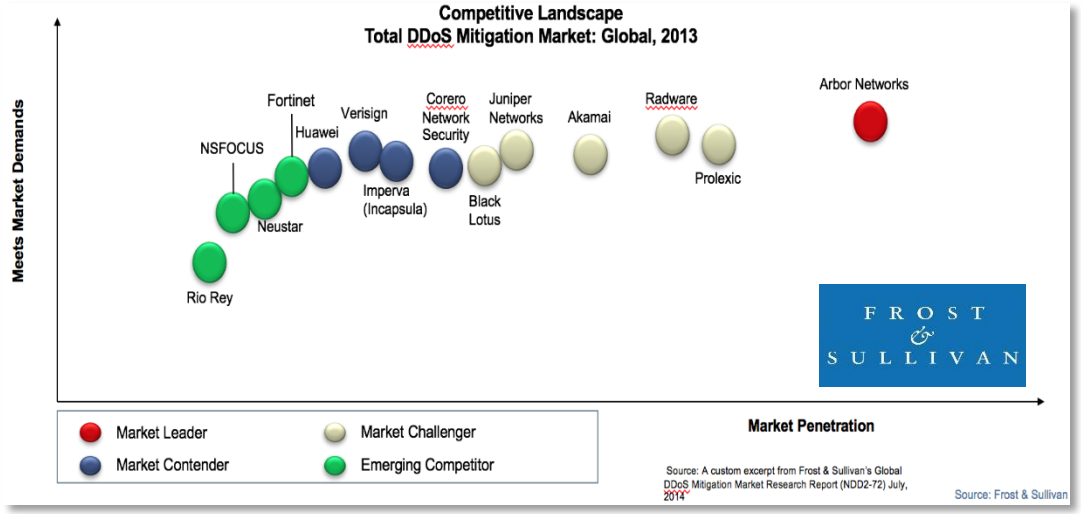
IHS Markit | DDoS Prevention Appliances: Biannual Market Tracker: Regional, H2 2017

The next table shows the three vendors in each of the deployment location segments we track in this report.

Exhibit 6 Worldwide DDoS prevention quarterly revenue market share by category

	2Q17	3Q17	4Q17	1Q18	CY16	CY17
Carrier transport and wired broadband						
Arbor	32.6%	35.2%	23.8%	31.8%	45.1%	33.9%
Radware	12.3%	11.3%	13.4%	12.1%	10.5%	11.8%
GenieNRM	11.1%	10.3%	12.5%	10.3%	9.7%	10.7%
Enterprise and carrier data centers						
Arbor	39.6%	41.5%	33.2%	37.8%	47.9%	40.9%
Huawei	6.6%	6.8%	8.5%	7.8%	2.5%	6.7%
Radware	7.4%	6.7%	8.3%	7.3%	6.9%	7.1%

Infonetics RESEARCH



參考客戶

臺灣大學

證交所

台灣銀行

玉山金控

技服中心

中央大學

台湾大哥大

台灣中油

集保中心

中國信託

中華郵政

臺灣菸酒

PoC 結果分析

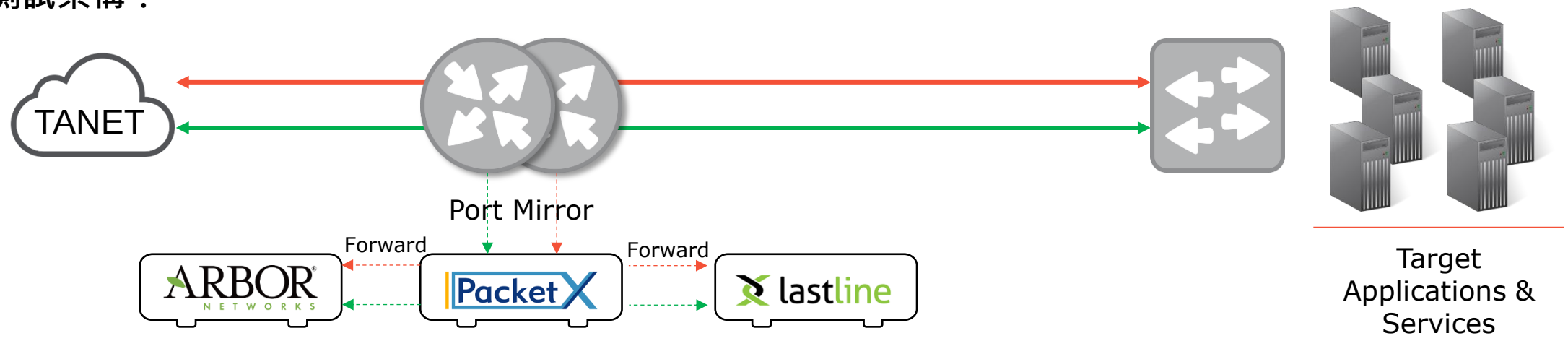
POC

測試摘要

測試地點：

學校名稱	A大學	B大學
測試期間：	7/17~8/29	
國/私立：	私立	國立
區域：	北區	南區
學校人數：	2萬人以上	2萬人以上

測試架構：



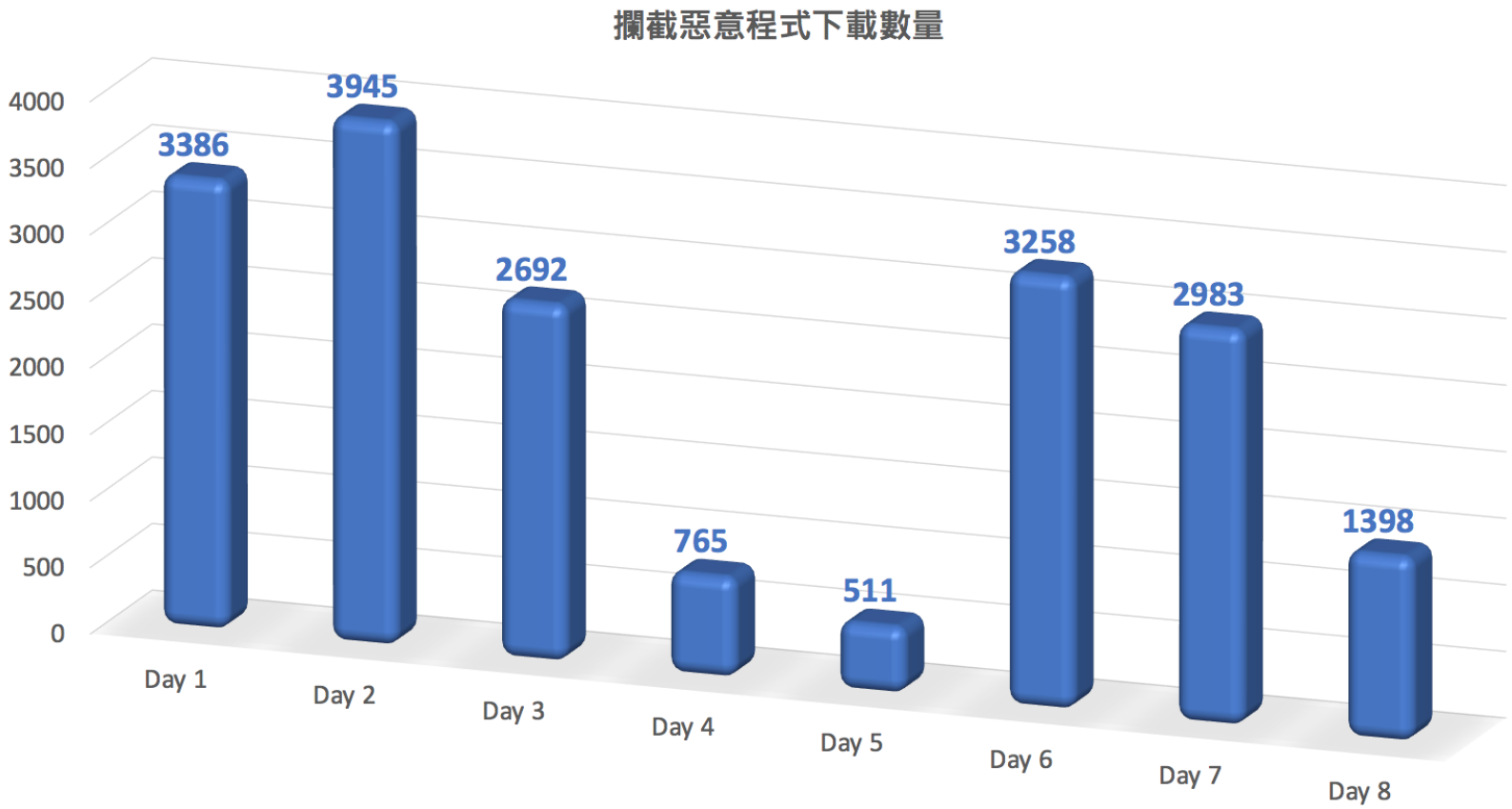
測試結果：前三大威脅

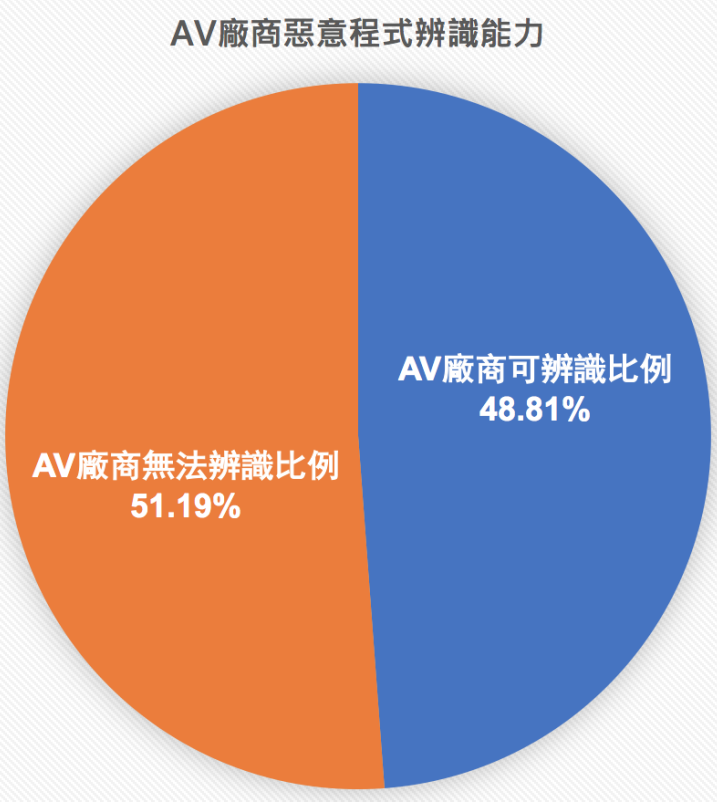
APT 威脅		DDoS 威脅	
威脅分類	造成影響	威脅分類	造成影響
Drive-By 偷渡式下載行為與惡意程式下載	駭客透過偷渡式下載(Drive-by)攻擊伴隨著零時差攻擊，進行惡意程式、勒索軟體、挖礦等惡意行為，進而對校園內主機進行攻擊。	機器人攻擊 (Botnet Prevention)	測試中發現來自國外IoT Botnet針對校園網路攝影機發出此類流量，試圖感染攝影機使其加入Botnet一環
Command & Control (C&C)	駭客入侵後可透過和命令與控制伺服器（中繼站）連線完成遠程控制。	無效或不符 RFC 定義封包 (應用程式攻擊） (Malformed HTTP Filtering & Block Malformed SIP Traffic)	
惡意程式感染活動	如 VPNFilter 等惡意程式可發起 IoT/DDoS 攻擊行為，利用校園網路設備或主機發起DDoS攻擊。	流量攻擊 / 狀態耗盡攻擊 (Filter List & Rate-based Blocking & Block Malformed DNS Traffic)	測試中發現來自各種不同手法的反射放大流量針對校園頻寬進行癱瘓，除了來自Internet不同國家的流量之外，也發現校園內有主機被入侵後，從校內對Internet IP發出巨量UDP封包試圖在校園內癱瘓網路。

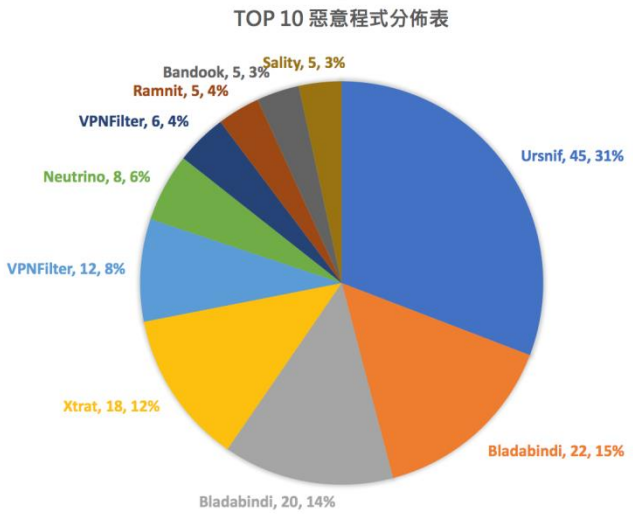
在測試過程中，我們發現了

- **APT 與 DDoS 威脅已經造成特定主機應用效能下降**
- **校內電腦已被駭客潛伏利用，成為攻擊第三方的中繼站**

效益關鍵數據 – 進階惡意程式辨識能力



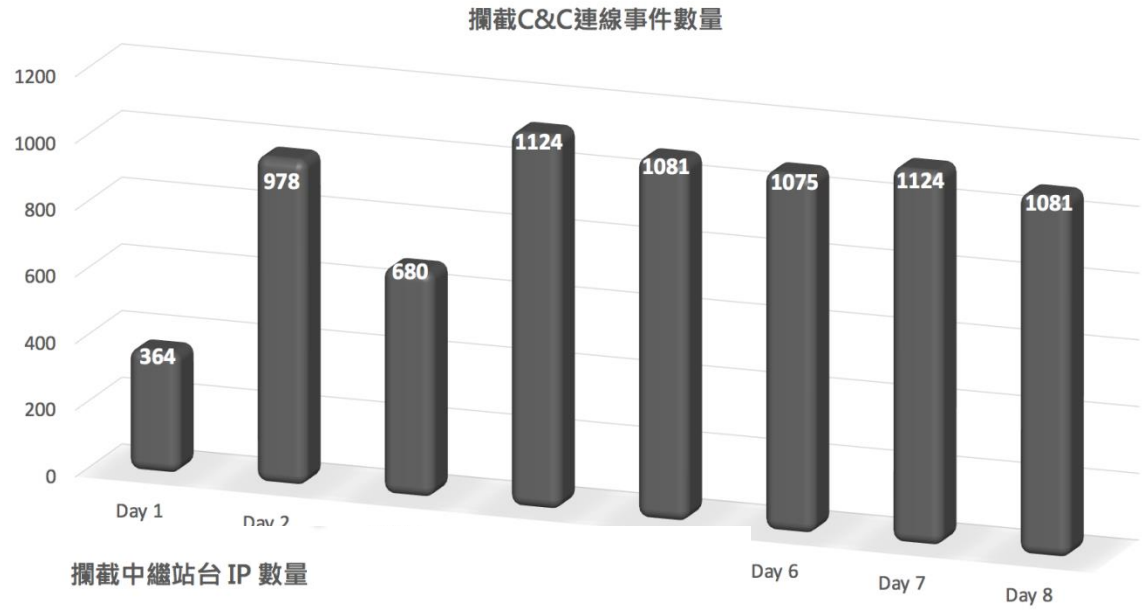


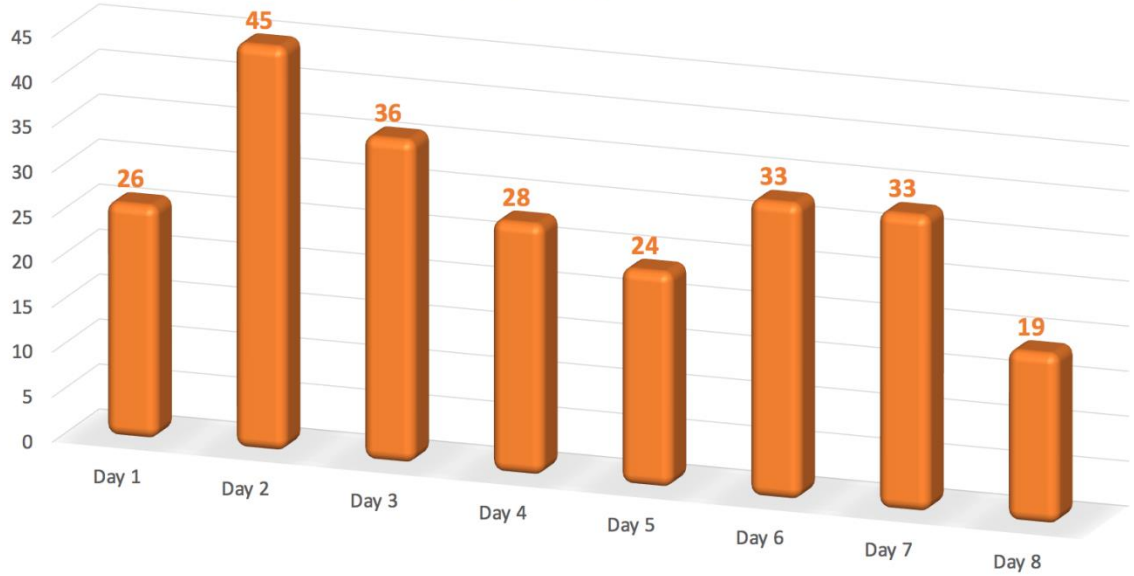


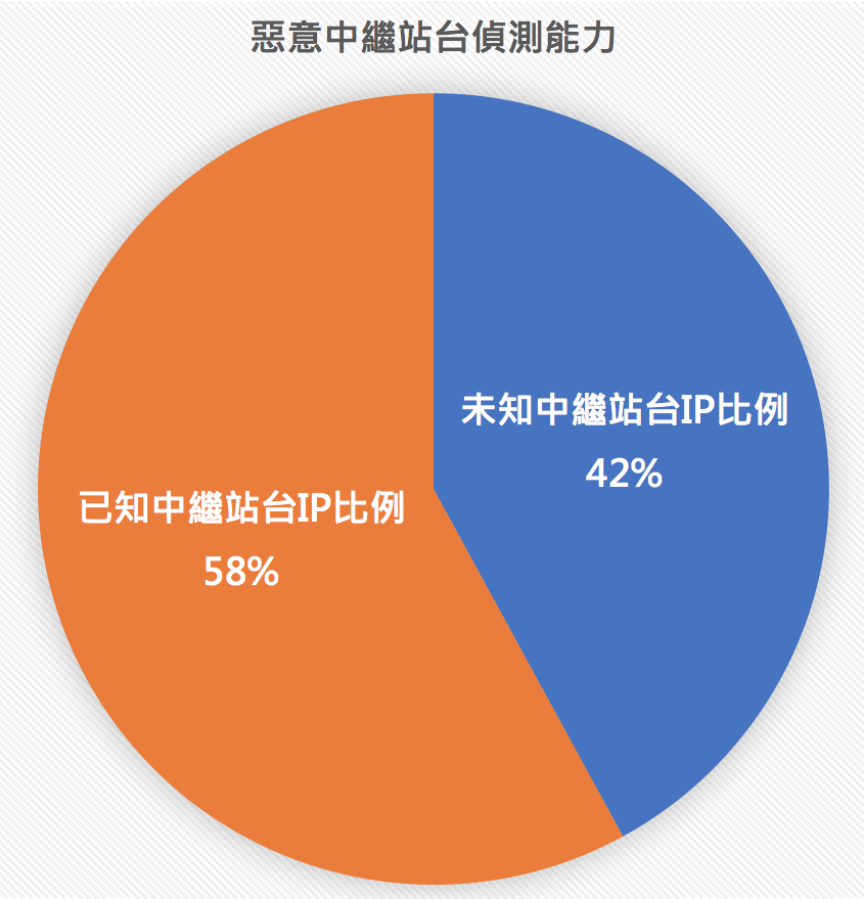
在測試過程中，我們攔截了超過18,900個惡意程式下載，其中

- Lastline 檢測出的惡意程式有高達 51.19% 是AV廠商無法辨識
- Lastline 無需特徵碼即可提早約 32天 辨識出進階惡意程式

效益關鍵數據 – 中繼站台惡意行為偵測能力





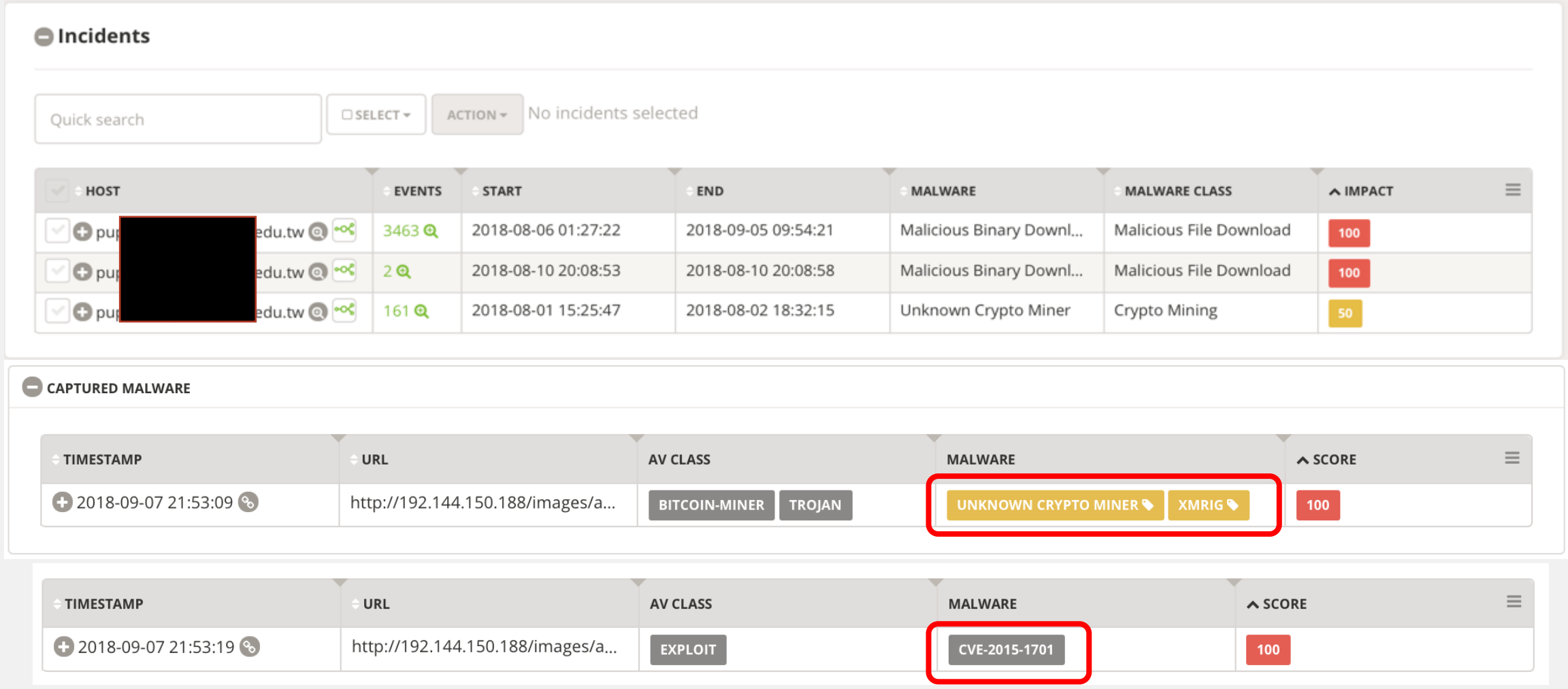


在測試過程中，我們阻擋了超過7,500次的中繼台連線行為，其中

- Lastline 檢測出的中繼站台 IP與行為有高達 42% 是既有資安設備無法檢測

APT實例(1)：校園主機遭入侵感染

- 檢測出校內主機遭入侵感染挖礦惡意程式與Windows CVE-2015-1701提權擴張漏洞利用。



APT實例(1)：校園內主機下載多重惡意程式

Evidence

FIRST SEEN	LAST SEEN	MALWARE	MALWARE CLASS	IMPACT	EVIDENCE	SUBJECT	REFERENCE
2018-08-26 07:16:...	2018-08-26 07:16:35	Malicious Binary Do...	Malicious File Downl...	100	FILE DOWNLOAD	714c78823625001019499c3f...	Network event
2018-08-26 07:16:...	2018-09-03 21:54:12	Malicious Binary Do...	Malicious File Downl...	100	CONFIRMED EXECUTION		Network event
2018-08-10 20:08:...	2018-08-10 20:08:53	Malicious Binary Do...	Malicious File Downl...	100	FILE DOWNLOAD	9fe988dc33ac0010196c8661...	Network event
2018-08-10 20:08:...	2018-08-10 20:08:58	Malicious Binary Do...	Malicious File Downl...	100	FILE DOWNLOAD	6e0faf5b40ed001012143b29...	Network event
2018-08-26 07:16:...	2018-08-26 07:16:24	Malicious Binary Do...	Malicious File Downl...	99	FILE DOWNLOAD	2ca341926c8b00101d63772...	Network event
2018-08-06 01:56:...	2018-09-05 09:53:48	XMRig	Crypto Mining	40	SIGNATURE		Network event
2018-08-06 02:56:...	2018-09-05 08:48:45	XMRig	Crypto Mining	40	REPUTATION	pool.minexmr.com	Network event
2018-08-06 01:56:...	2018-09-05 09:53:48	Unknown Crypto Mi...	Crypto Mining	45	SIGNATURE		Network event
2018-08-06 01:56:...	2018-09-05 09:49:18	Unknown Crypto Mi...	Crypto Mining	45	SIGNATURE		Network event
2018-08-06 01:27:...	2018-09-05 09:54:21	Unknown Crypto Mi...	Crypto Mining	45	SIGNATURE		Network event

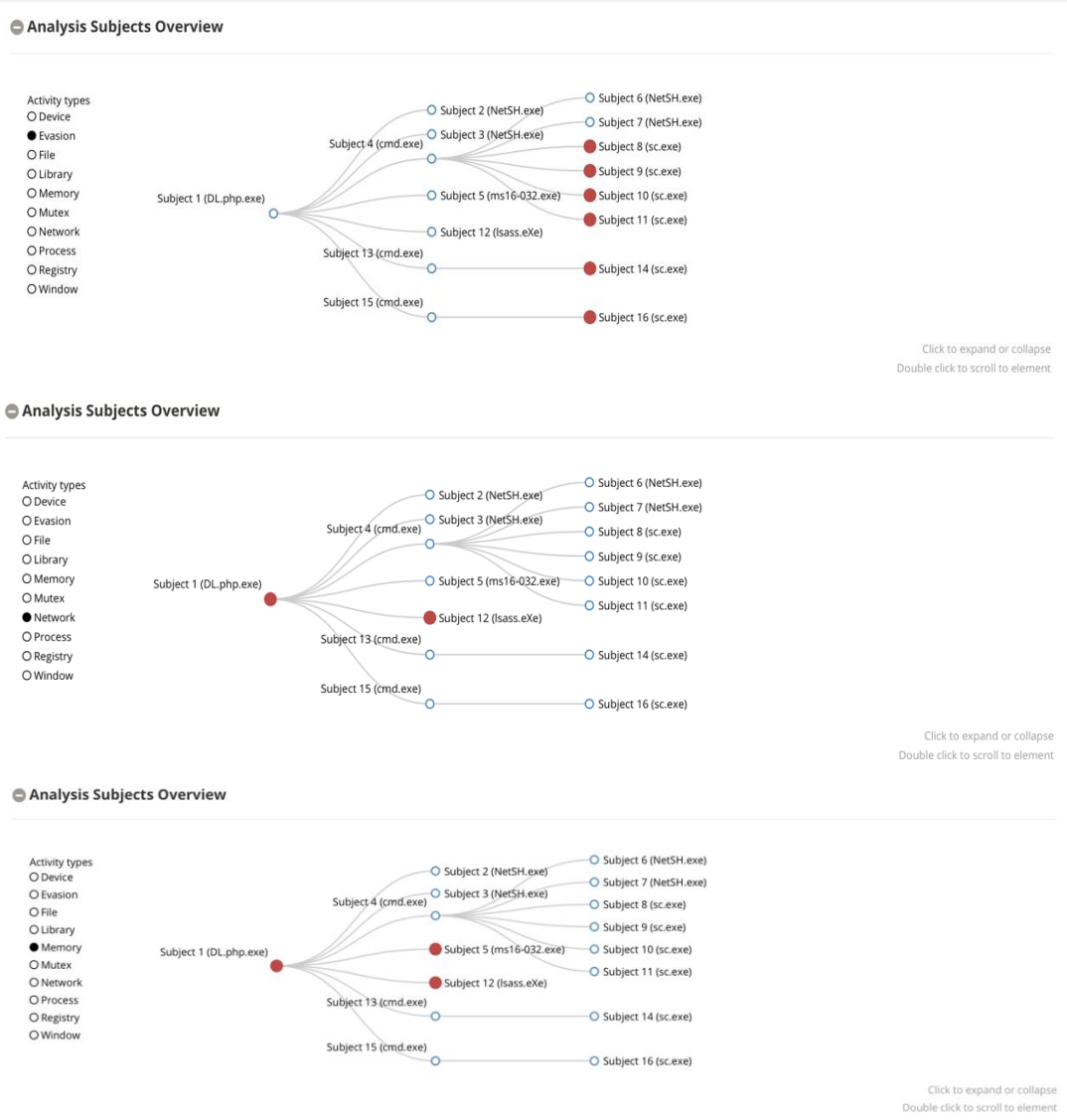
Files downloaded

Quick search

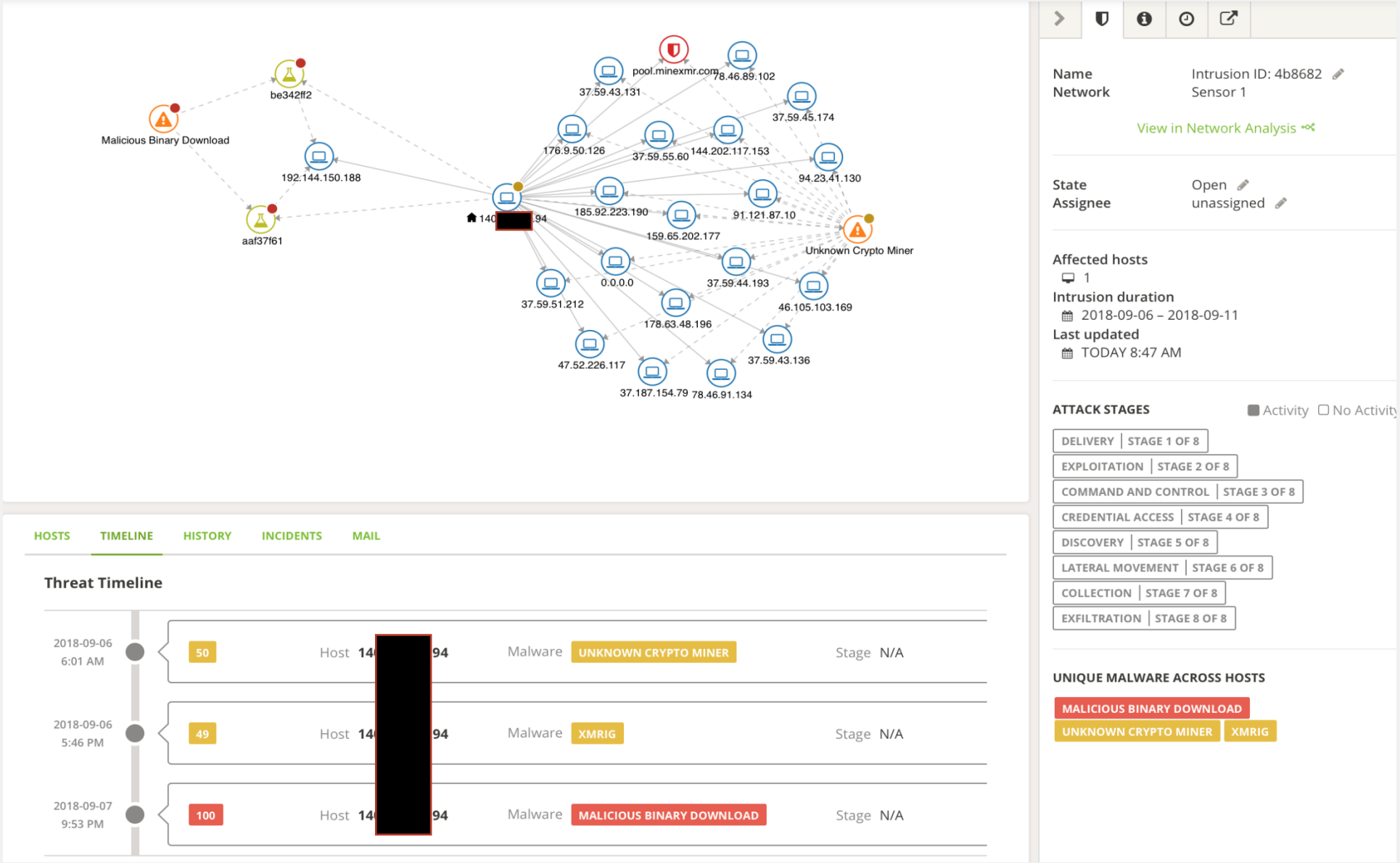
TIMESTAMP	CONTACTED IP	LOCATION	MD5	TYPE	AV CLASS	MALWARE	SCORE
2018-08-26 07:16:...	192.[redacted]:80	http://192.144.150.1...	dbc90a81308e19561...	Executable	EXPLOIT	CVE-2015-1701	100
2018-08-10 20:08:...	192.[redacted]:80	http://192.144.150.1...	dbc90a81308e19561...	Executable	EXPLOIT	CVE-2015-1701	100
2018-08-10 20:08:...	192.[redacted]:80	http://192.144.150.1...	673e9ecd9db107174...	Executable	BITCOIN-MINER TROJAN	UNKNOWN CRYPTO MINER XMRIG	100
2018-08-26 07:16:...	192.[redacted]:80	http://192.144.150.1...	673e9ecd9db107174...	Executable	BITCOIN-MINER TROJAN	UNKNOWN CRYPTO MINER XMRIG	99

APT實例(1)：主機下載並執行惡意程式

SEVERITY	TYPE	DESCRIPTION
100	Signature	Identified trojan code
70	Disable	Disabling installed firewalls (Microsoft)
54	Network	Suspicious traffic observed
50	Stealth	Creating executables masquerading as system files
30	Family	Potentially unwanted application/program (XMRigMiner)
25	Autostart	Registering a new service at startup
20	Network	Connecting to server using hard-coded IP address
20	Network	Attempting to download executable from remote location
20	File	Modifying executable in Temporary System directory
15	Settings	Adding a Windows Firewall exception
15	Execution	Executing command-line shell with anomalous arguments
10	Packer	Packer signature (non install-builder or archive-builder packer)
10	Network	Listening for incoming connection over a specific port
5	Evasion	Trying to get information about the operating system from WMI
5	Evasion	Trying to detect virtual environment by checking processor's information from WMI
1	Settings	Granting rights to debug or read memory of another process (SeDebugPrivilege)
1	Search	Enumerates running processes
1	Execution	Ability to use cryptography API
1	Execution	Ability to iterate through running processes

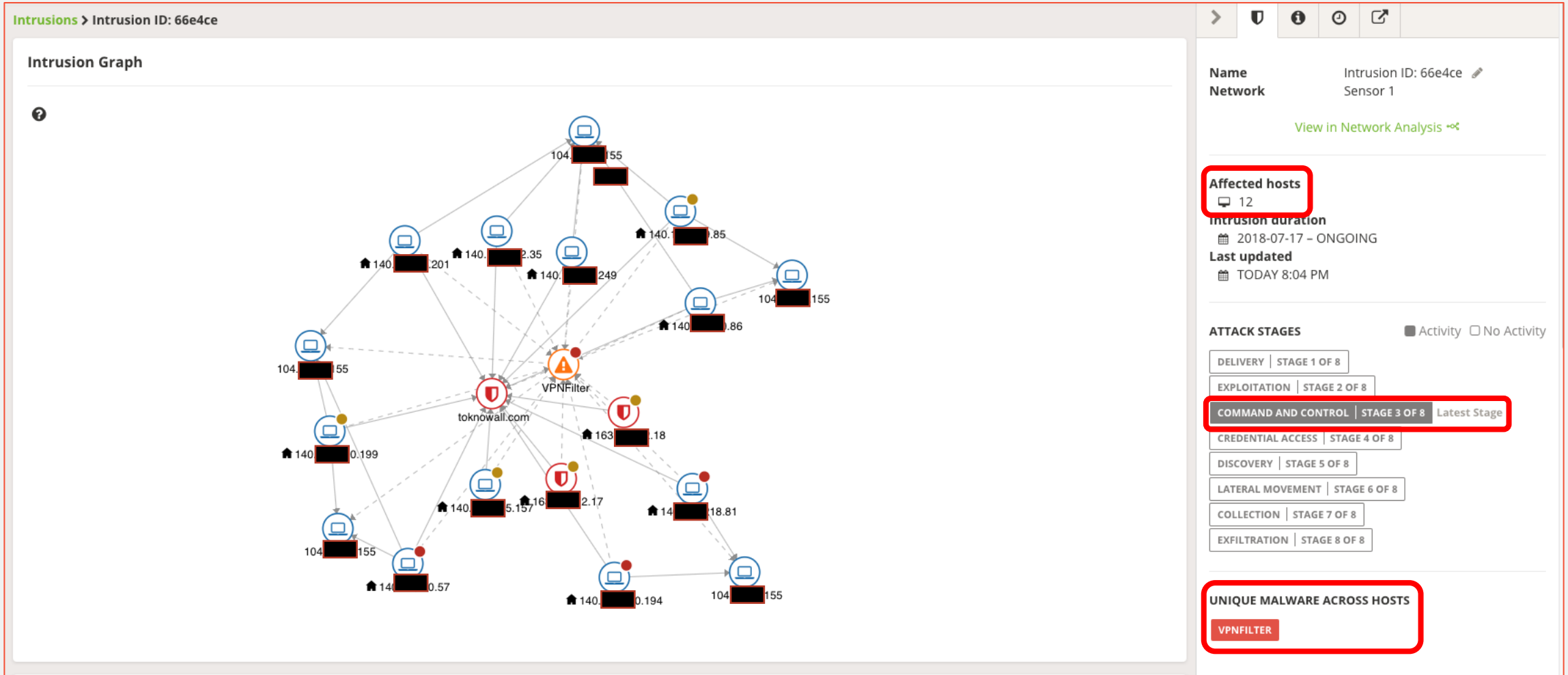


APT實例(1)：校園內主機遭受攻擊關聯示意圖



APT實例(2)：VPNFilter惡意程式感染活動

- 校園內有多台主機感染 VPNFilter 惡意程式且遭到控制，作為攻擊跳板對外發動攻擊或監控裝置流量、竊取網站憑證，或切斷裝置的連網能力或讓裝置無法使用，擁有強大的破壞力。



APT實例(2)：校園內主機亦遭受感染，並持續連線至外部C&C中繼站

HOST	SENSOR	EVENTS	START	END	MALWARE	MALWARE CLASS	IMPACT
www.h[redacted]edu.tw	Sensor 1	144	2018-07-17 15:15:32	2018-07-25 13:39:30	NetwiredRC	command&control	100

Events

TIMESTAMP	HOST	SENSOR	CONTACTED IP	CONTACTED HOST	MALWARE	MALWARE CLASS	IMPACT
2018-07-20 14:40:14	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	100
2018-07-23 22:22:02	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	100
2018-07-20 15:22:04	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	118.184.85.102	NetwiredRC	command&control	99
2018-07-20 21:24:35	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	118.184.85.102	NetwiredRC	command&control	99
2018-07-20 11:18:48	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	118.184.85.102	NetwiredRC	command&control	99
2018-07-23 22:56:37	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	118.184.85.102	NetwiredRC	command&control	99
2018-07-24 19:25:43	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	25
2018-07-19 03:04:39	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	25
2018-07-23 06:55:29	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	25
2018-07-20 12:26:05	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	25
2018-07-24 16:20:45	www.h[redacted]du.tw	Sensor 1	118.184.85.102:8080	www.openmd5.com	NetwiredRC	command&control	25

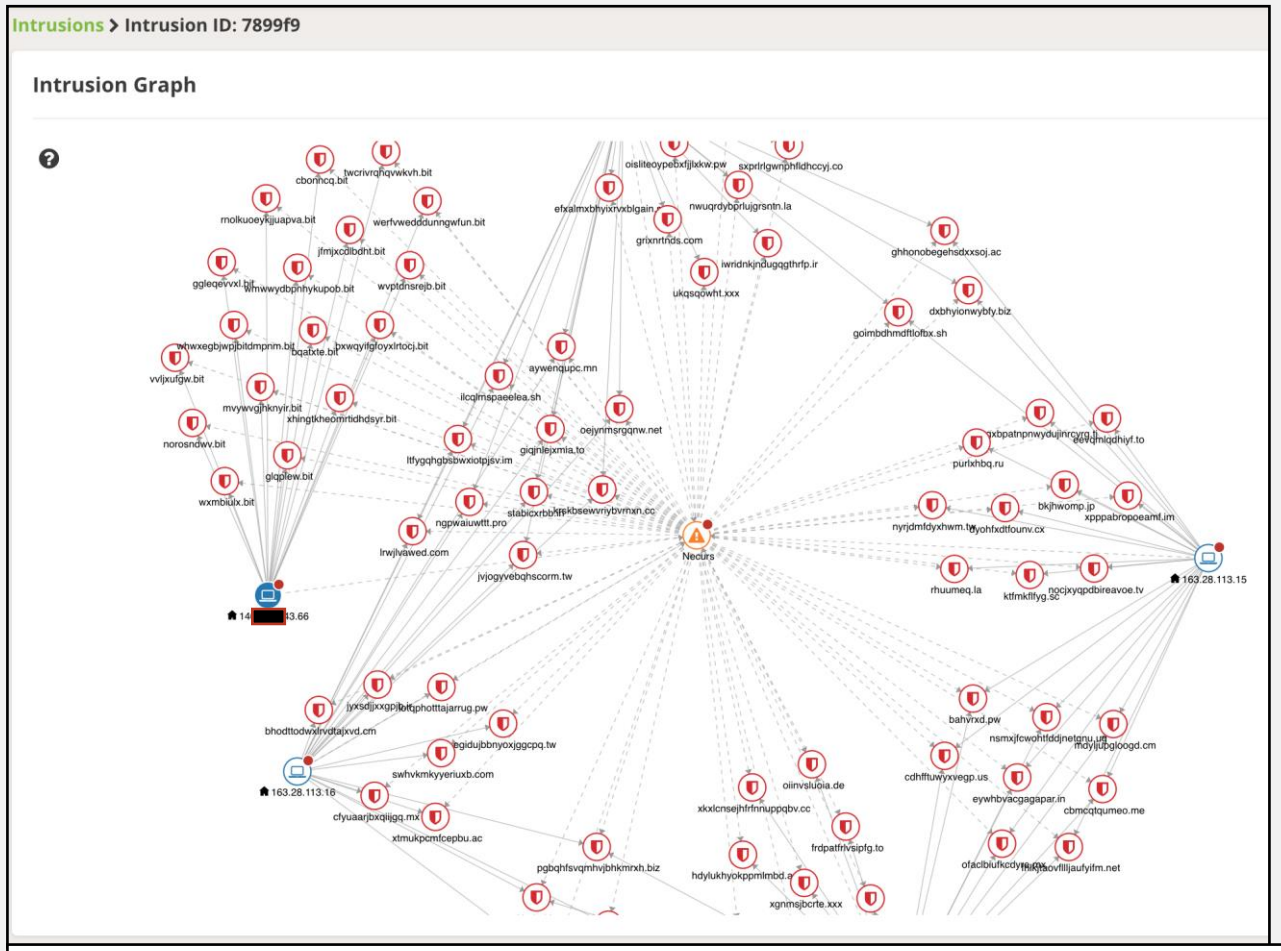
APT實例(2)：校園內特定主機下載多重惡意程式

- Sality + Gamarue + Ramnit
- 惡意程式以botnet為主，主要控制受害主機藉以當做攻擊跳板或直接發動攻擊

HOSTS	MALWARE	ATTACK STAGES	LATEST ACTIVITY
140.[redacted].52	SALITY GAMARUE SINKDNS SINKHOLE RAMNIT SINKHOLE HOST + 22	DELIVERY COMMAND AND CONTROL	2018-07-25 4:19 PM
140.[redacted]36	SALITY GAMARUE SINKHOLE HOST RAMNIT SINKDNS SINKHOLE + 22	DELIVERY COMMAND AND CONTROL	2018-07-20 10:08 AM
140.[redacted]135	SALITY GAMARUE RAMNIT SINKDNS SINKHOLE SINKHOLE HOST + 22	DELIVERY COMMAND AND CONTROL	2018-07-25 11:02 AM

HOST	SENSOR	EVENTS	START	END	MALWARE	MALWARE CLASS	IMPACT
140.1[redacted]93	Sensor 1	54	2018-07-17 19:16:51	2018-07-24 21:55:23	Ramnit	command&control	99
140.1[redacted]93	Sensor 1	9	2018-07-18 07:13:16	2018-07-24 19:50:31	CoinHive Monero Miner	Crypto Jacking	53
140.1[redacted]93	Sensor 1	1	2018-07-21 14:57:36	2018-07-21 14:57:36	Malicious Binary Downl...	Malicious File Dow...	34
140.1[redacted]93	Sensor 1	1	2018-07-24 09:54:41	2018-07-24 09:54:41	unescape of long unico...	drive-by	53
140.1[redacted]93	Sensor 1	1	2018-07-25 10:57:32	2018-07-25 10:57:32	Malicious Binary Downl...	Malicious File Dow...	66

APT實例(2)：主機感染垃圾郵件惡意程式，可被利用對外發動攻擊



- 檢測出Necurs惡意程式連線行為， Necurs除了用來傳送大量的垃圾郵件，並且夾帶惡意軟體之外，還具備了發動DDoS攻擊的能力

HOSTS	MALWARE	ATTACK STAGES	LATEST ACTIVITY
140.[redacted]44	NECURS QUANT LOADER	DELIVERY	2018-07-24 11:06 AM
140.[redacted]66	NECURS	DELIVERY COMMAND AND CONTROL	2018-07-25 10:30 AM

DDoS實例-外部攻擊：癱瘓校園網路

- 使用方式：Botnet Prevention
- 攻擊來源國家：
  - Russia (俄羅斯聯邦)
  - Egypt (阿拉伯埃及共和國)
  - Vietnam(越南社會主義共和國)
  - Nigeria (奈及利亞聯邦共和國)
  - USA(美利堅合眾國)
  - France(法蘭西共和國)
  - Italy(義大利共和國)
  - Kazakhstan (哈薩克共和國)
  - Japan(日本國)
  - Botswana (波札那共和國)
- 攻擊IP數：8221
- 針對學校的Web Cam發動攻擊, 以取得控制權, 以利作為攻擊跳板

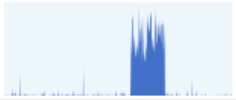
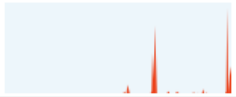
Results

Found **8221** blocked hosts affected by Protection Group **Class Camera**, blocked by Attack Category **Botnet Prevention**, from **Mon Aug 6 11:55:00 2018** to **Tue Aug 28 12:55:00 2018**.

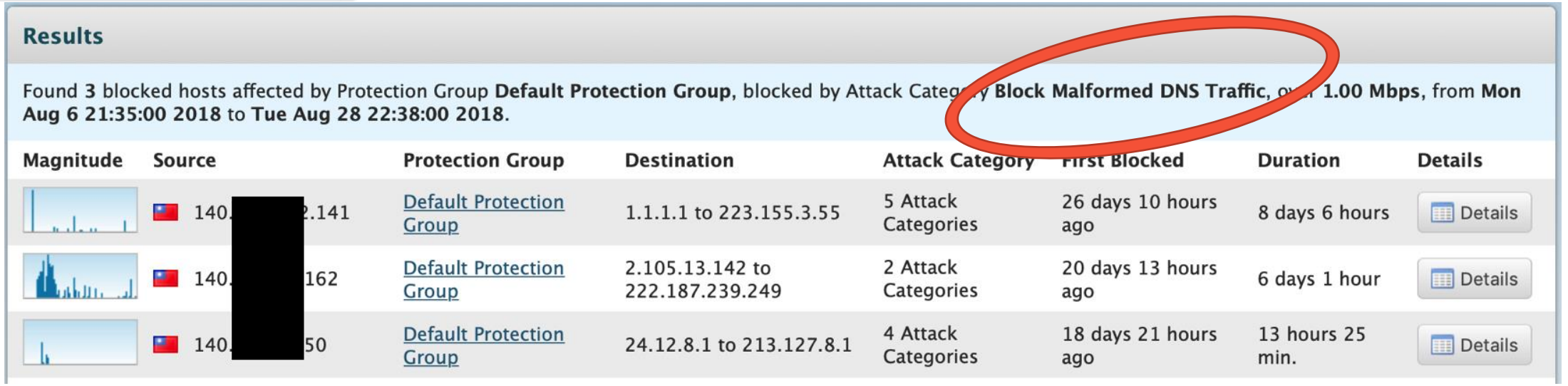
Magnitude	Source	Protection Group	Destination	Attack Category	First Blocked	Duration	Details
	31.163.132.46	6 Protection Groups	140. 140. to .32	Botnet Prevention	5 days 8 hours ago	3 hours 4 min.	Details
	178.47.117.123	5 Protection Groups	140. 140. to .53	Botnet Prevention	3 days 12 hours ago	2 hours	Details
	197.33.58.249	Class Camera	140. 88	Botnet Prevention	8 hours 48 min. ago	1 min.	Details
	41.45.55.96	Class Camera	140. 191	Botnet Prevention	6 hours 15 min. ago	1 min.	Details
	183.80.43.89	2 Protection Groups	140. 140. 110 to 159	Botnet Prevention	17 hours 36 min. ago	7 min.	Details
	41.184.250.175	2 Protection Groups	140. 140. 204 to 124	Botnet Prevention	2 days 4 hours ago	2 min.	Details
	58.187.99.187	2 Protection Groups	140. 140. 2 to 36	Botnet Prevention	1 day 18 hours ago	8 min.	Details
	118.71.7.222	3 Protection Groups	140. 140. 61 to .152	Botnet Prevention	1 day 21 hours ago	5 min.	Details
	94.50.25.129	2 Protection Groups	140. 140. 32 to 156	Botnet Prevention	23 hours 36 min. ago	6 min.	Details
	94.50.145.160	5 Protection Groups	140. 140. 5 to .38	Botnet Prevention	6 days 8 hours ago	3 hours 33 min.	Details
	42.116.186.243	Class Camera	140. 195	Botnet Prevention	7 hours 47 min. ago	2 min.	Details
	58.187.95.169	3 Protection Groups	140. 140. 64 to .38	Botnet Prevention	1 day 17 hours ago	9 min.	Details
	41.237.88.57	2 Protection Groups	140. 140. 64 to .63	Botnet Prevention	1 day ago	2 min.	Details
	41.235.213.95	Class Camera	140. 151	Botnet Prevention	15 hours 1 min. ago	1 min.	Details
	31.163.61.251	6 Protection Groups	140. 140. to .3	2 Attack Categories	4 days 20 hours ago	2 hours 46 min.	Details

DDoS實例-外部攻擊：癱瘓校園網路

- 各種反射放大攻擊, 尤其瞬間產生巨大流量, 將導致學校網路正常運作

Filter List		692.20 GB
Block Malformed DNS Traffic		115.75 GB
Block Malformed SIP Traffic		69.40 GB
Rate-based Blocking		417.63 GB
TCP Connection Limiting		108.91 GB
UDP Flood Detection		105.50 GB

DDoS實例-內部攻擊：來自校園內部的巨量攻擊



Results

Found **3** blocked hosts affected by Protection Group **Default Protection Group**, blocked by Attack Category **Block Malformed DNS Traffic**, over **1.00 Mbps**, from **Mon Aug 6 21:35:00 2018** to **Tue Aug 28 22:38:00 2018**.

Magnitude	Source	Protection Group	Destination	Attack Category	First Blocked	Duration	Details
	140.[redacted].141	Default Protection Group	1.1.1.1 to 223.155.3.55	5 Attack Categories	26 days 10 hours ago	8 days 6 hours	Details
	140.[redacted]162	Default Protection Group	2.105.13.142 to 222.187.239.249	2 Attack Categories	20 days 13 hours ago	6 days 1 hour	Details
	140.[redacted]50	Default Protection Group	24.12.8.1 to 213.127.8.1	4 Attack Categories	18 days 21 hours ago	13 hours 25 min.	Details

Source	140.[redacted]41
Country	Taiwan
Destination	1.1.1.1 to 223.155.3.55
Protocol	tcp (6) – udp (17)
Port	3 – 65530
First Time Blocked	12:24:01 PM 08/02/18
Last Time Blocked	1:35:00 PM 09/03/18
Total Time Blocked	10 days
Total Blocked	318.64 GB, [redacted] M packets
Rate Blocked	[redacted] Mbps, 634 pps
Protection Groups	Default Protection Group

Source	140[redacted]162
Country	Taiwan
Destination	2.105.13.142 to 222.187.239.249
Protocol	udp (17)
Port	3 – 65527
First Time Blocked	9:27:01 AM 08/08/18
Last Time Blocked	11:05:00 AM 09/03/18
Total Time Blocked	6 days 13 hours
Total Blocked	105.57 GB, [redacted] M packets
Rate Blocked	[redacted] Mbps, 461 pps
Protection Groups	Default Protection Group

Source	140[redacted]50
Country	Taiwan
Destination	1.1.1.1 to 223.252.195.133
Protocol	icmp (1) – udp (17) (tcp)
Port	1 – 65535
First Time Blocked	4:30:01 PM 08/09/18
Last Time Blocked	1:37:00 PM 09/03/18
Total Time Blocked	13 days 1 hour
Total Blocked	226.12 GB, [redacted] M packets
Rate Blocked	[redacted] Mbps, 518 pps
Protection Groups	Default Protection Group

- 受駭客控制的主機瞬間發出的巨量內對外攻擊, 將影響校園的網路服務及造成頻寬壅塞

DDoS實例-內部攻擊：來自校園內部的巨量攻擊

- 內部IP在發動攻擊前均有連線到已知惡意網址的行為，經第三方單位比對，確實有C&C行為

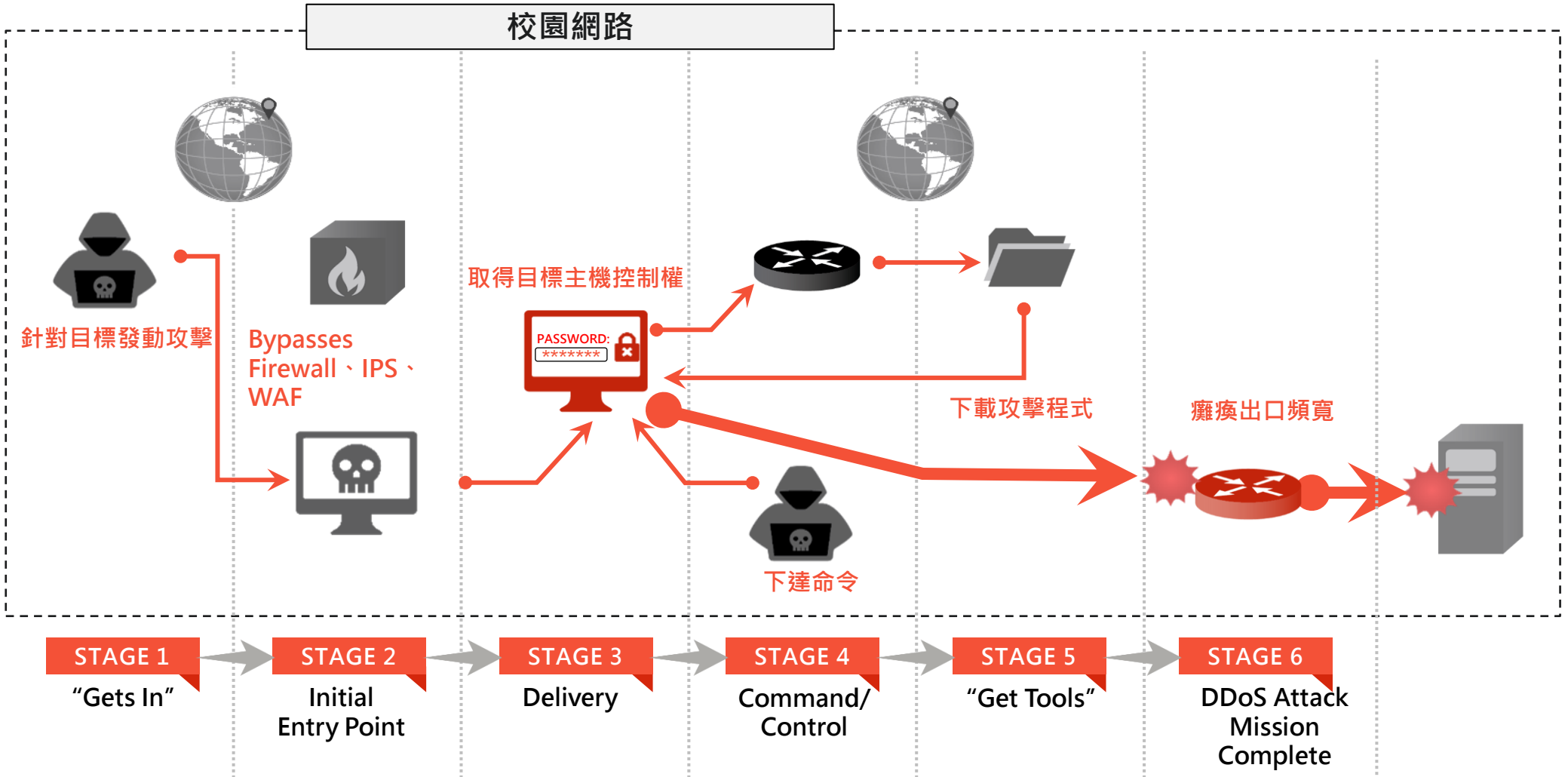
☐	Aug 09 2018, 04:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 09 2018, 03:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 09 2018, 02:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 09 2018, 01:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 09 2018, 00:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 08 2018, 23:15:00	vertical_high_tech	sonic4us.ru	NL
☐	Aug 08 2018, 16:15:00	vertical_high_tech	.electricbridge.net	US
☐	Aug 07 2018, 23:15:00	vertical_high_tech	.electricbridge.net	US
☐	Aug 06 2018, 12:15:00	vertical_high_tech	.weatherclear.net	US
☐	Aug 03 2018, 16:15:00	vertical_high_tech	.weatherclear.net	US
☐	Aug 03 2018, 15:15:00	vertical_high_tech	.weatherclear.net	US
☐	Aug 03 2018, 14:15:00	vertical_high_tech	.weatherclear.net	US
☐	Aug 03 2018, 10:15:00	vertical_high_tech	.weatherclear.net	US
☐	Aug 03 2018, 09:15:00	vertical_high_tech	.weatherclear.net	US

Communicating Files ⓘ

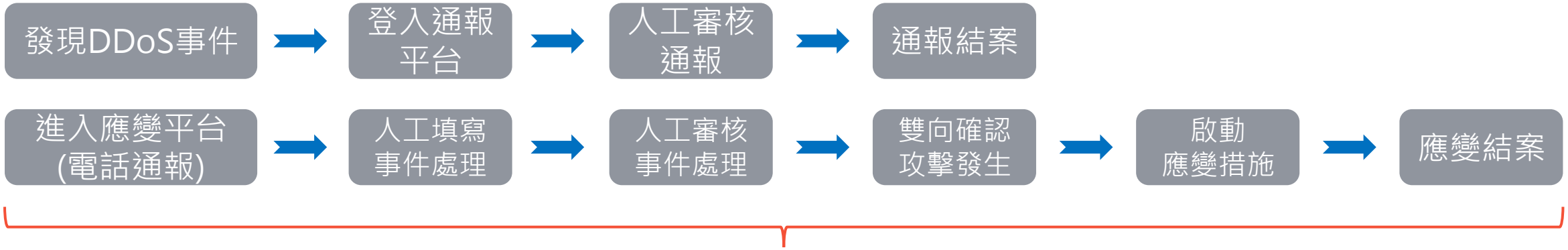
Date scanned	Detections	File type	Name
2018-08-28	55/67	Win32 EXE	bayrob-nivdort.exe
2018-08-28	55/67	Win32 EXE	a04e5250c158e731df449cce49830e81073521e600a1ccbc051847a7f605e4d6
2018-06-27	54/68	Win32 EXE	9175c0e232955d877efb415b0a2ef35dda3a4c1f326d2ae97b84b066018b022a
2018-07-16	50/67	Win32 EXE	8c560fca15f6121ab6d97be3ef414bbe74bb91c08f13933b6955e89bdd89a3b4
2018-08-25	56/67	Win32 EXE	923d64fb6541e7ab3e0c6da5133e9700.virus
2018-06-27	52/68	Win32 EXE	a19aec246c1e728866a70b8a0d56ad41.virus
2018-08-24	48/68	Win32 EXE	7f8fdf93b81f7cb5de777bc81091abf9
2018-09-03	53/68	Win32 EXE	117416a41b449df5d568b5ff5ec233dc.virus
2018-08-28	53/68	Win32 EXE	92016c775446336645b29ec599c1b499
2018-08-29	54/67	Win32 EXE	515211c9da9bffaace62f931a8759450.vir
2018-08-29	53/67	Win32 EXE	2b13808a6aa2b7dc896b425794efc968.vir
2018-07-09	53/67	Win32 EXE	4eoCFaNg1f
2018-08-29	56/68	Win32 EXE	4d47bea173789adbe91d2b69211f4010.virobj
2018-07-07	54/68	Win32 EXE	b2c49773d50184db59662c7dbd408600.virus
2018-08-29	55/68	Win32 EXE	6b6181829231f7f9b5165cfeb344d181.vir

DDoS實際案例：來自內部的巨量攻擊

- DDoS Botnet攻擊鍊的形成

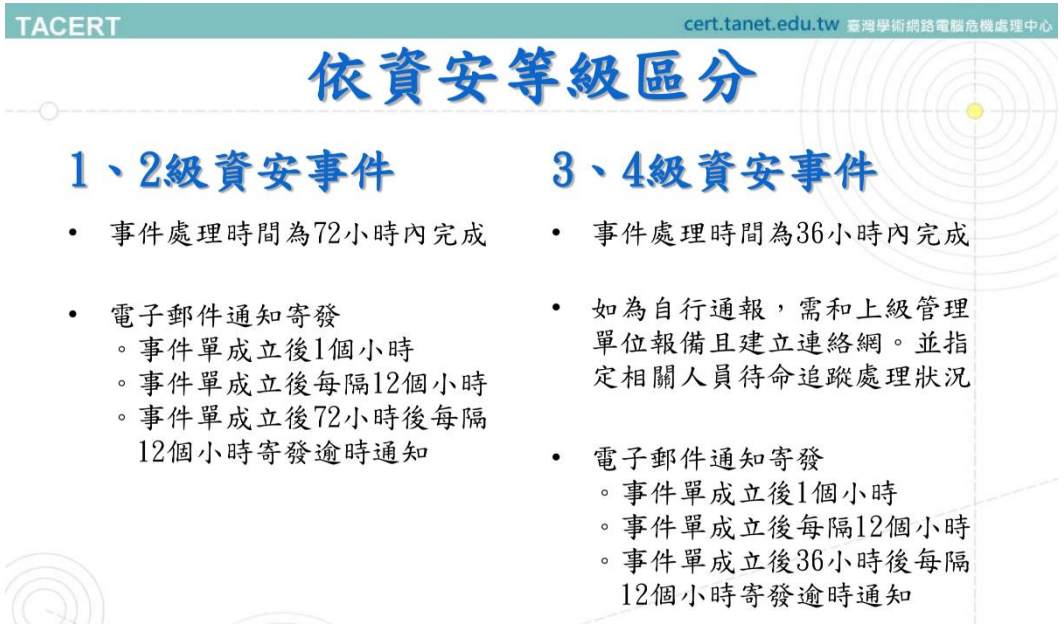


目前TANET DDoS攻擊對應流程



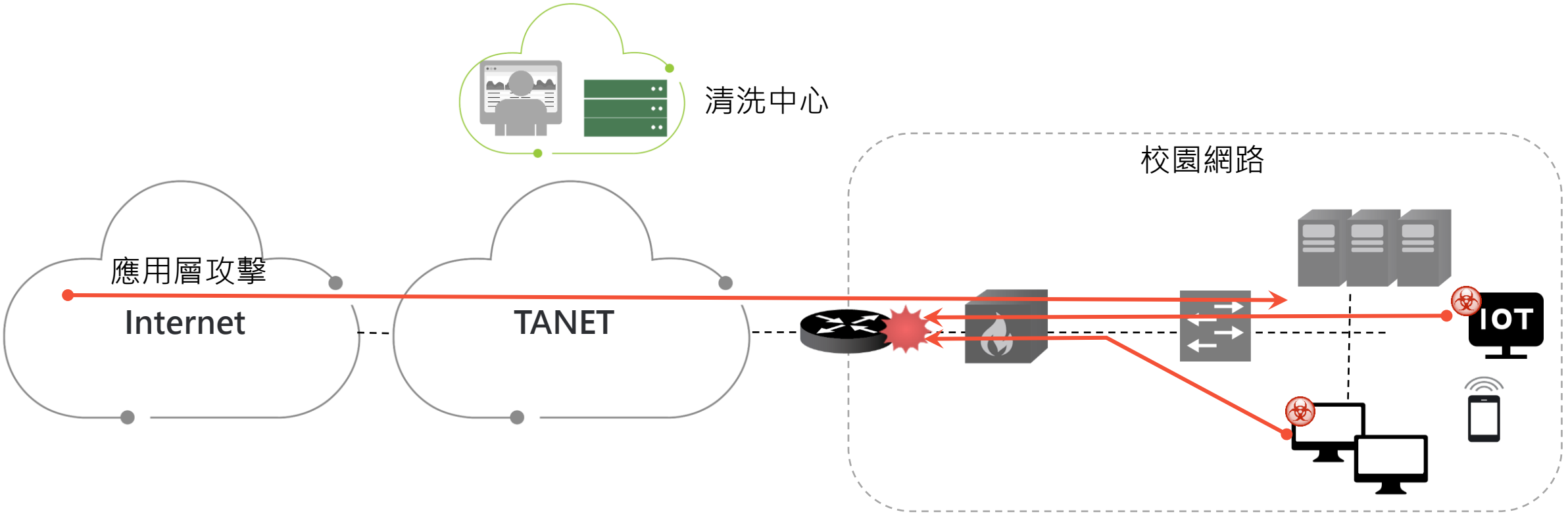
- 審核與應變過程需花費至少一小時才能完成
- 應變起始到結案需人工確認才啟動清洗機制
- 清洗設備需位於網路骨幹中，處理流量過大無法針對Layer7流量進行防禦

如果沒有Always on的即時偵測及快速清洗機制, 目前的通報及應變流程將緩不濟急.



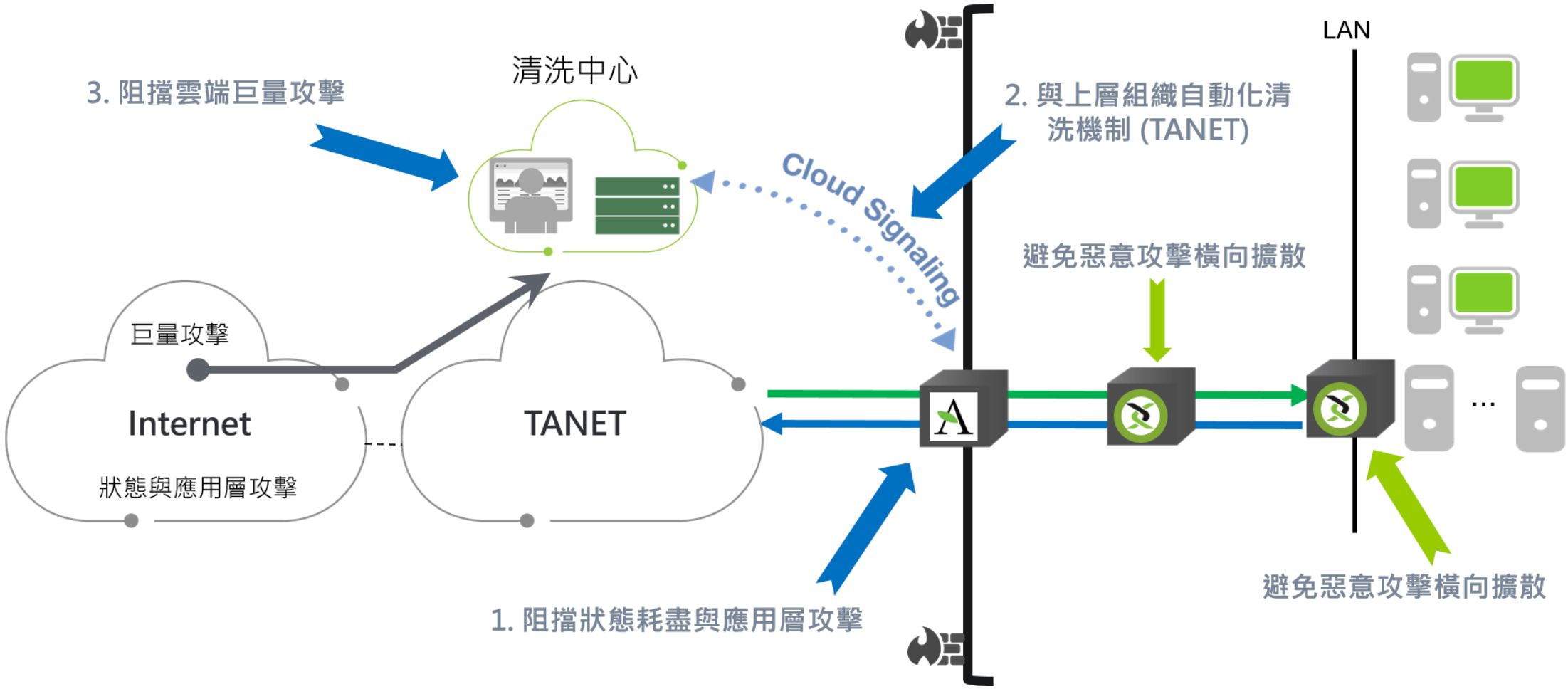
目前DDoS攻擊對應流程

- 清洗中心無法防止來自校園內部的攻擊
- 校園缺少內到外連線阻斷與DDoS防禦機制



PoC 總結建議

- 為避免惡意攻擊橫向擴散，必須監控內部網路，及早建立內網預警機制
- 針對 Inside Out、Outside In 的流量，皆須防範威脅攻擊發生



ISAC
校園資安服務平台

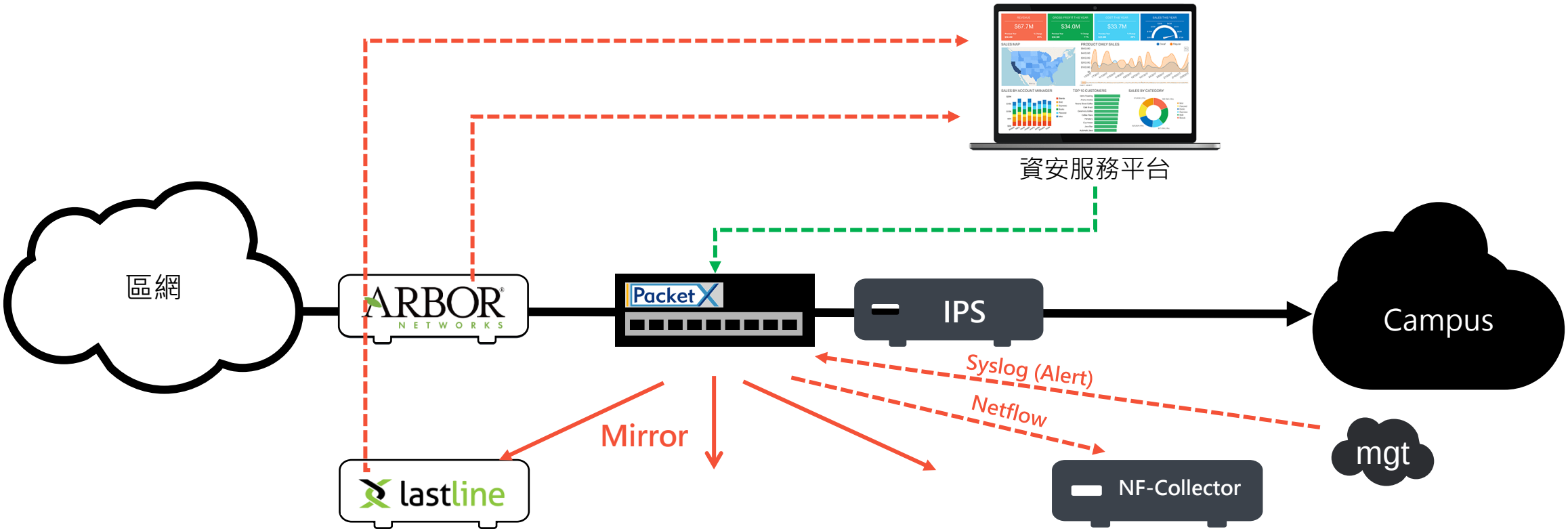
Efficient professional after-sales service
High-quality and rapid Security solution

PacketX
技術長　王騰嶽

資安服務平台介紹

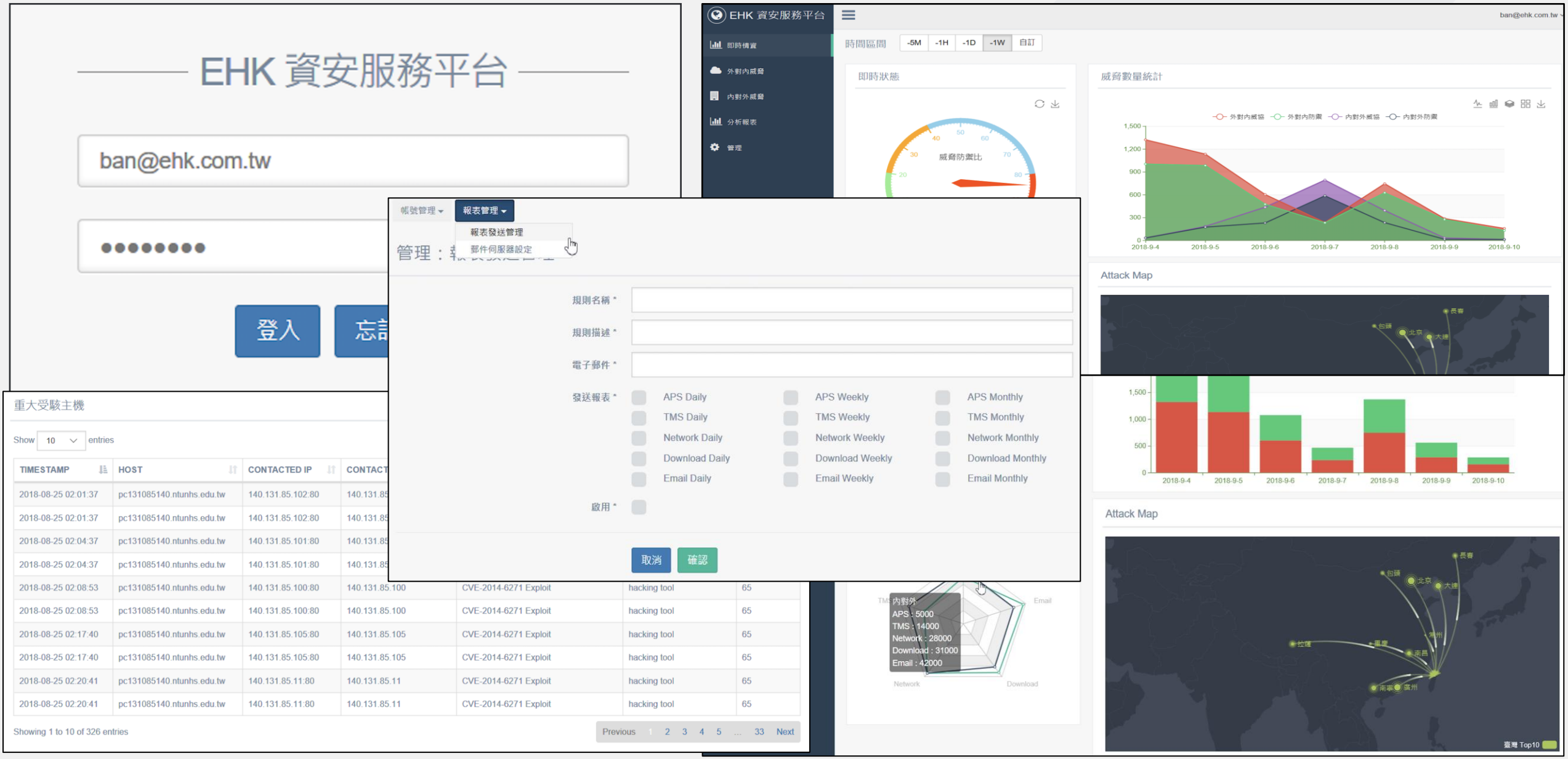
Managed Cyber Security Platform

資安服務平台介紹

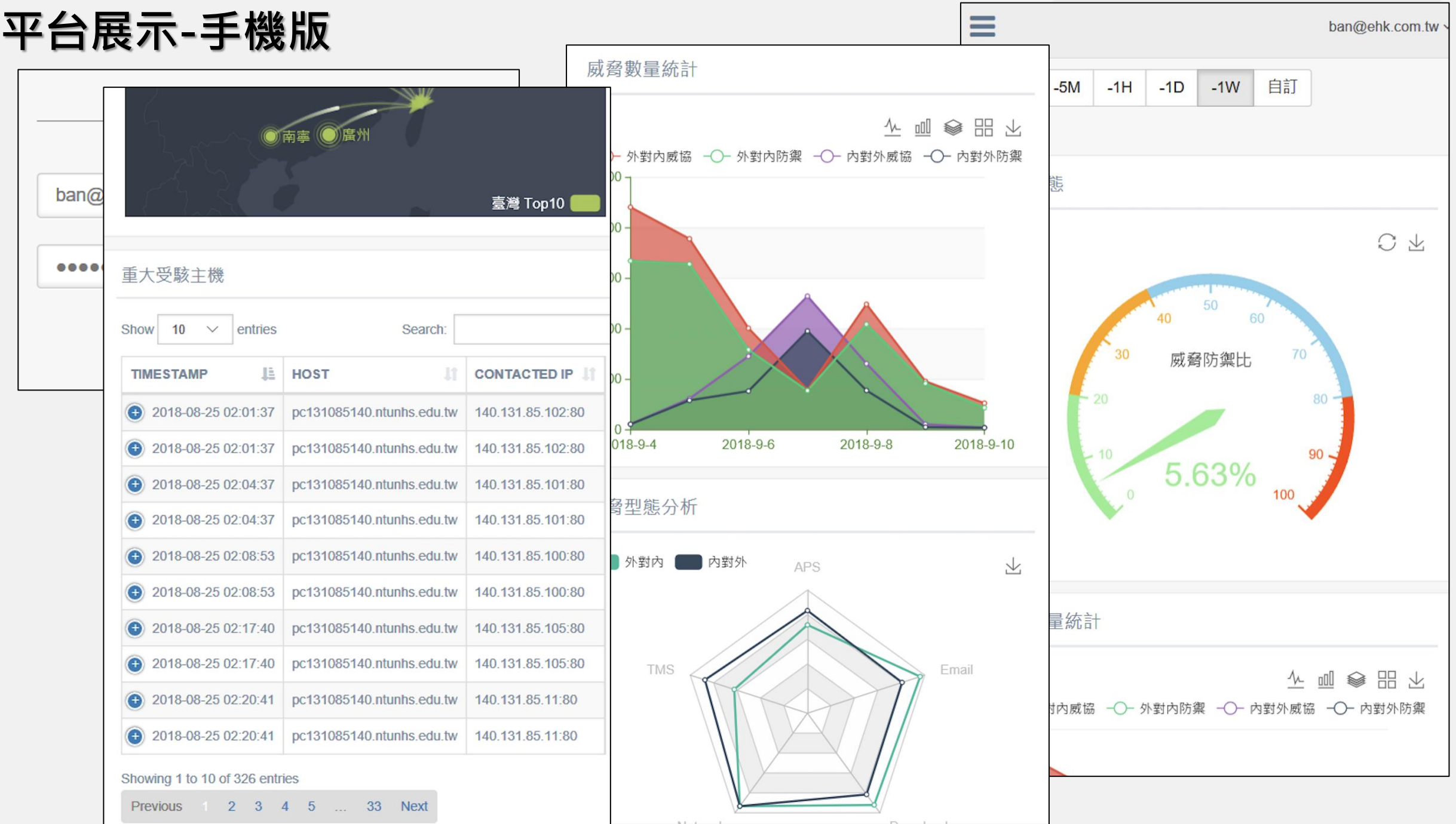


1. 除第一線的 Arbor 外所有 in-line 設備均改成 sniffer mode 接在 PacketX 上，避免 SPoF
2. 藉由 PacketX 過濾流量，提升資安設備效能，投資成本降低
3. 由 PacketX 產生 1:1 NetFlow ，降低路由器負載
4. 利用 PacketX 採擷多網段流量，產生 Out of Band 複製流量給資安分析工具
5. 導入 ISAC 資安服務平台，以有效掌握單位資安風險 (報表、告警、阻擋政策)

平台展示-電腦版


EHK 資安服務平台
ban@ehk.com.tw
登入
EHK 資安服務平台
即時情資
外對內威脅
內對外威脅
分析報表
管理
時間區間
-5M
-1H
-1D
-1W
自訂
即時狀態
威脅防禦比
威脅數量統計
外對內威脅
外對內防禦
內對外威脅
內對外防禦
帳號管理
報表管理
報表發送管理
郵件伺服器設定
規則名稱 *
規則描述 *
電子郵件 *
發送報表 *
APS Daily
APS Weekly
APS Monthly
TMS Daily
TMS Weekly
TMS Monthly
Network Daily
Network Weekly
Network Monthly
Download Daily
Download Weekly
Download Monthly
Email Daily
Email Weekly
Email Monthly
啟用 *
取消
確認
Attack Map
重大受駭主機
Show 10 entries
TIMESTAMP
HOST
CONTACTED IP
2018-08-25 02:01:37 pc131085140.ntunhs.edu.tw 140.131.85.102:80
2018-08-25 02:04:37 pc131085140.ntunhs.edu.tw 140.131.85.101:80
2018-08-25 02:08:53 pc131085140.ntunhs.edu.tw 140.131.85.100:80 140.131.85.100 CVE-2014-6271 Exploit hacking tool 65
2018-08-25 02:17:40 pc131085140.ntunhs.edu.tw 140.131.85.105:80 140.131.85.105 CVE-2014-6271 Exploit hacking tool 65
2018-08-25 02:20:41 pc131085140.ntunhs.edu.tw 140.131.85.11:80 140.131.85.11 CVE-2014-6271 Exploit hacking tool 65
Showing 1 to 10 of 326 entries
Previous 1 2 3 4 5 ... 33 Next
內對外
APS : 5000
TMS : 14000
Network : 28000
Download : 31000
Email : 42000
Attack Map
臺灣 Top10

平台展示-手機版


南寧
廣州
臺灣 Top10
重大受駭主機
Show 10 entries
Search:
TIMESTAMP
HOST
CONTACTED IP
2018-08-25 02:01:37 pc131085140.ntunhs.edu.tw 140.131.85.102:80
2018-08-25 02:01:37 pc131085140.ntunhs.edu.tw 140.131.85.102:80
2018-08-25 02:04:37 pc131085140.ntunhs.edu.tw 140.131.85.101:80
2018-08-25 02:04:37 pc131085140.ntunhs.edu.tw 140.131.85.101:80
2018-08-25 02:08:53 pc131085140.ntunhs.edu.tw 140.131.85.100:80
2018-08-25 02:08:53 pc131085140.ntunhs.edu.tw 140.131.85.100:80
2018-08-25 02:17:40 pc131085140.ntunhs.edu.tw 140.131.85.105:80
2018-08-25 02:17:40 pc131085140.ntunhs.edu.tw 140.131.85.105:80
2018-08-25 02:20:41 pc131085140.ntunhs.edu.tw 140.131.85.11:80
2018-08-25 02:20:41 pc131085140.ntunhs.edu.tw 140.131.85.11:80
Showing 1 to 10 of 326 entries
Previous 1 2 3 4 5 ... 33 Next
威脅數量統計
外對內威協
外對內防禦
內對外威協
內對外防禦
2018-9-4
2018-9-6
2018-9-8
2018-9-10
外對內
內對外
APS
TMS
Email
ban@ehk.com.tw
-5M
-1H
-1D
-1W
自訂
威脅防禦比
5.63%
0
10
20
30
40
50
60
70
80
90
100
外對內防禦
內對外威協
內對外防禦

總結

Conclusion

總結

天禦慧資安服務平台是學校資安最堅強後盾

強化資安防禦能力，建立**高延展整合性服務平台**

全面

5x8 Always On 訂閱服務+自動即時監控、通報、客製化告警報表系統，**高CP值一站式服務**

優惠

天禦慧智提供佈建及維運管理服務，學校不需投資設備維運人力**快速無痛導入**

無痛

攜手國際資訊安全領導品牌大廠，打造**最優值及最嚴密等級**防禦服務

信任

天禦慧智

THANKS

Efficient professional after-sales service
High-quality and rapid E-solution