REDSOCKS

malicious threat detection

惡意威脅的薩德預警系統

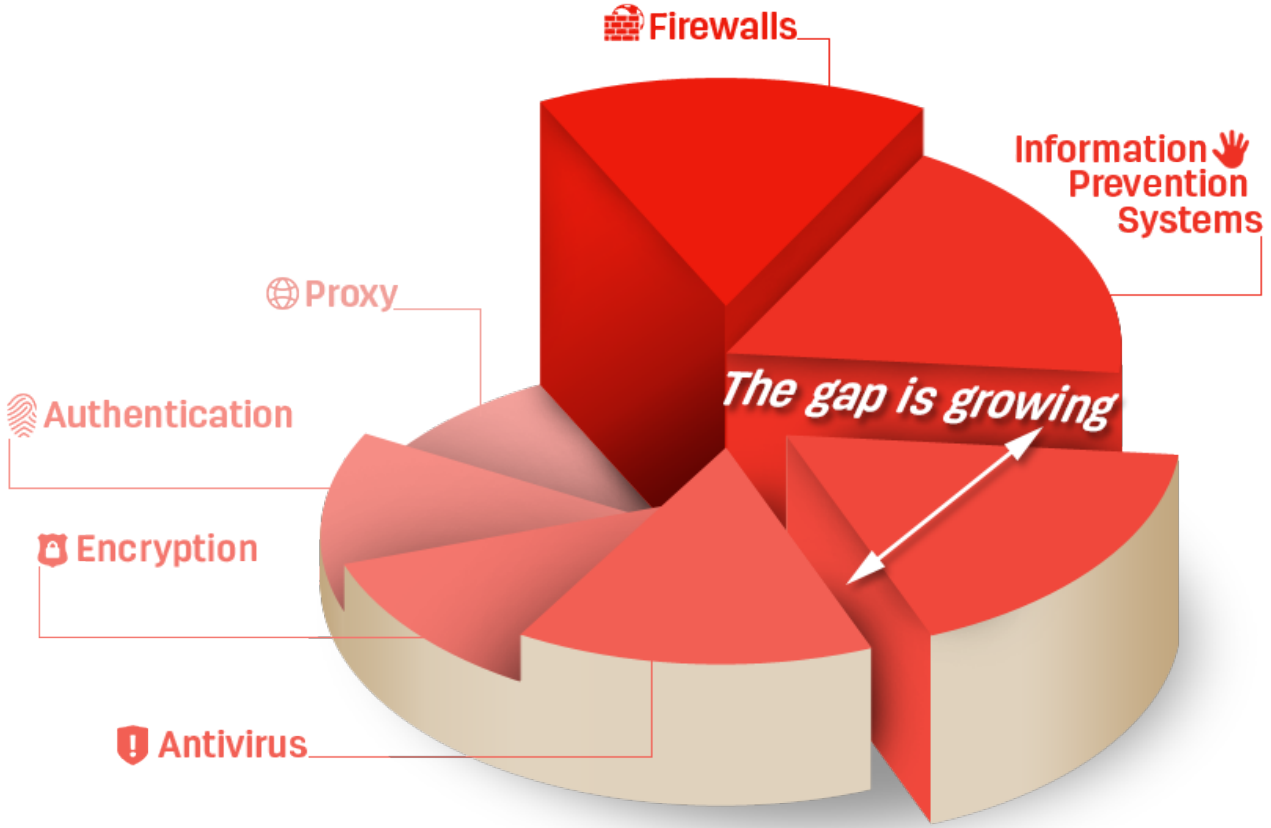
力悅資訊

彭國達

資訊安全的著眼點正在改變

許多資安專家聲稱防禦型的產品
已經快跟不上時代的變化。

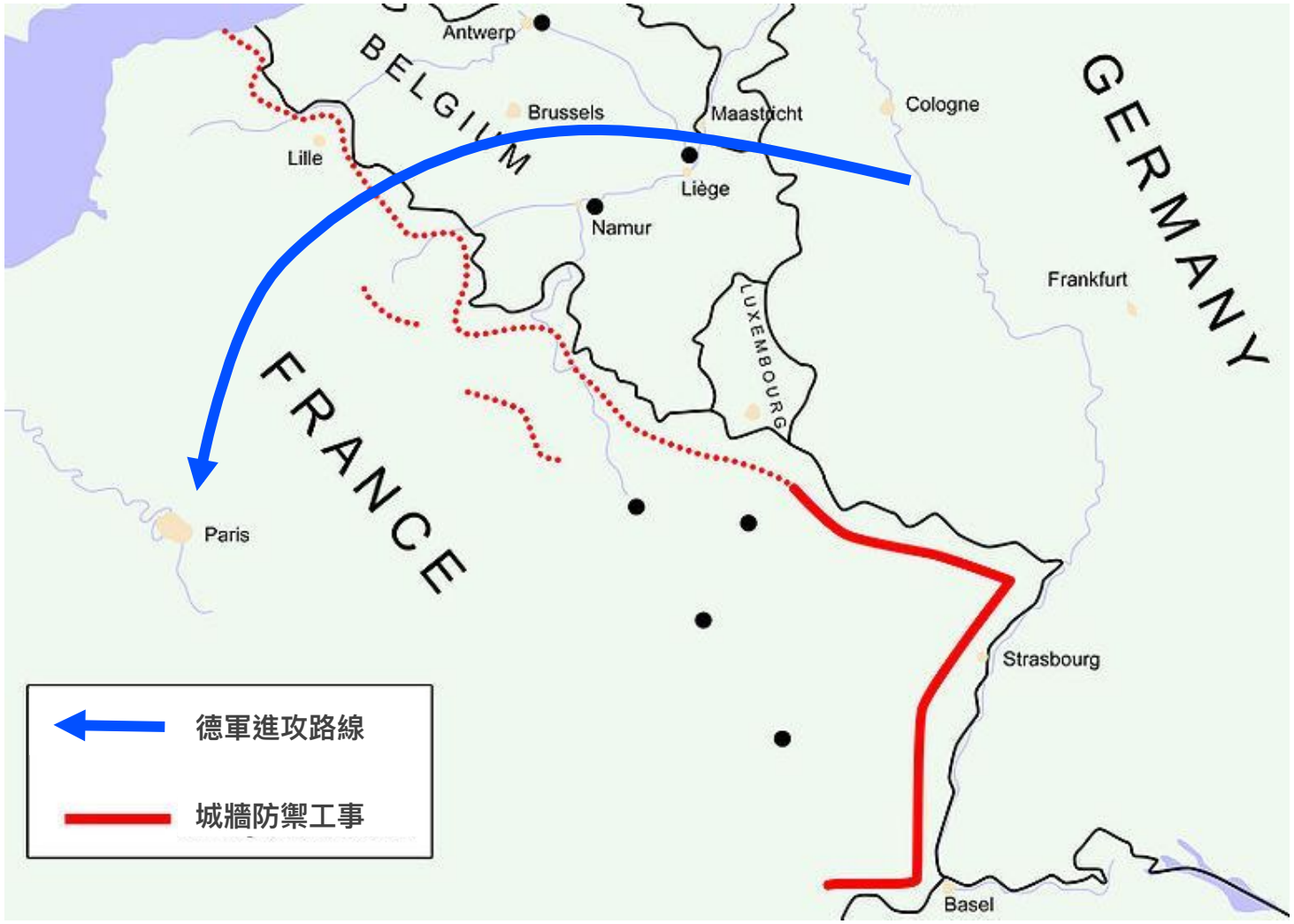
在資訊爆炸的商業環境中，
*網路犯罪者都會用許多**意料不到***
途徑達成他們的目標與目的



Cyberview 力悦資訊

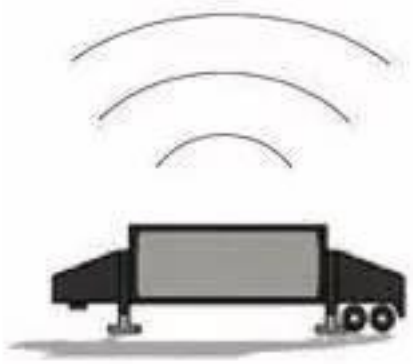
防禦機制真的越多越好嗎？

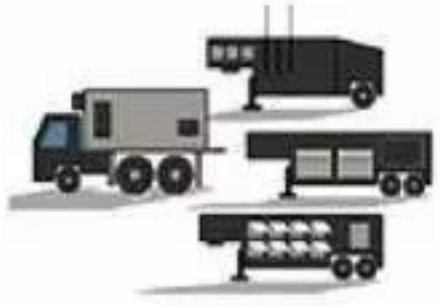
法國 馬其諾防線要塞



早期預警系統

incoming threat 飛彈威脅來襲





①雷達偵測到飛彈來襲

②指揮與射控系統
辨識與鎖定目標

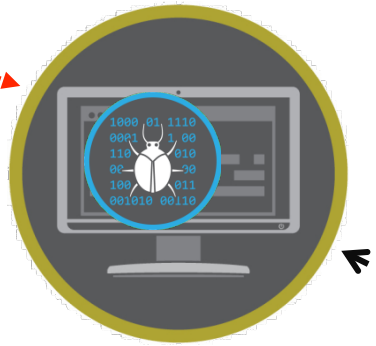
③車載發射器發射
攔截飛彈

Cyberview
力悅資訊

早期預警系統

惡意攻擊者

incoming threat 惡意威脅來襲



①早期預警系統偵測到
惡意威脅來襲

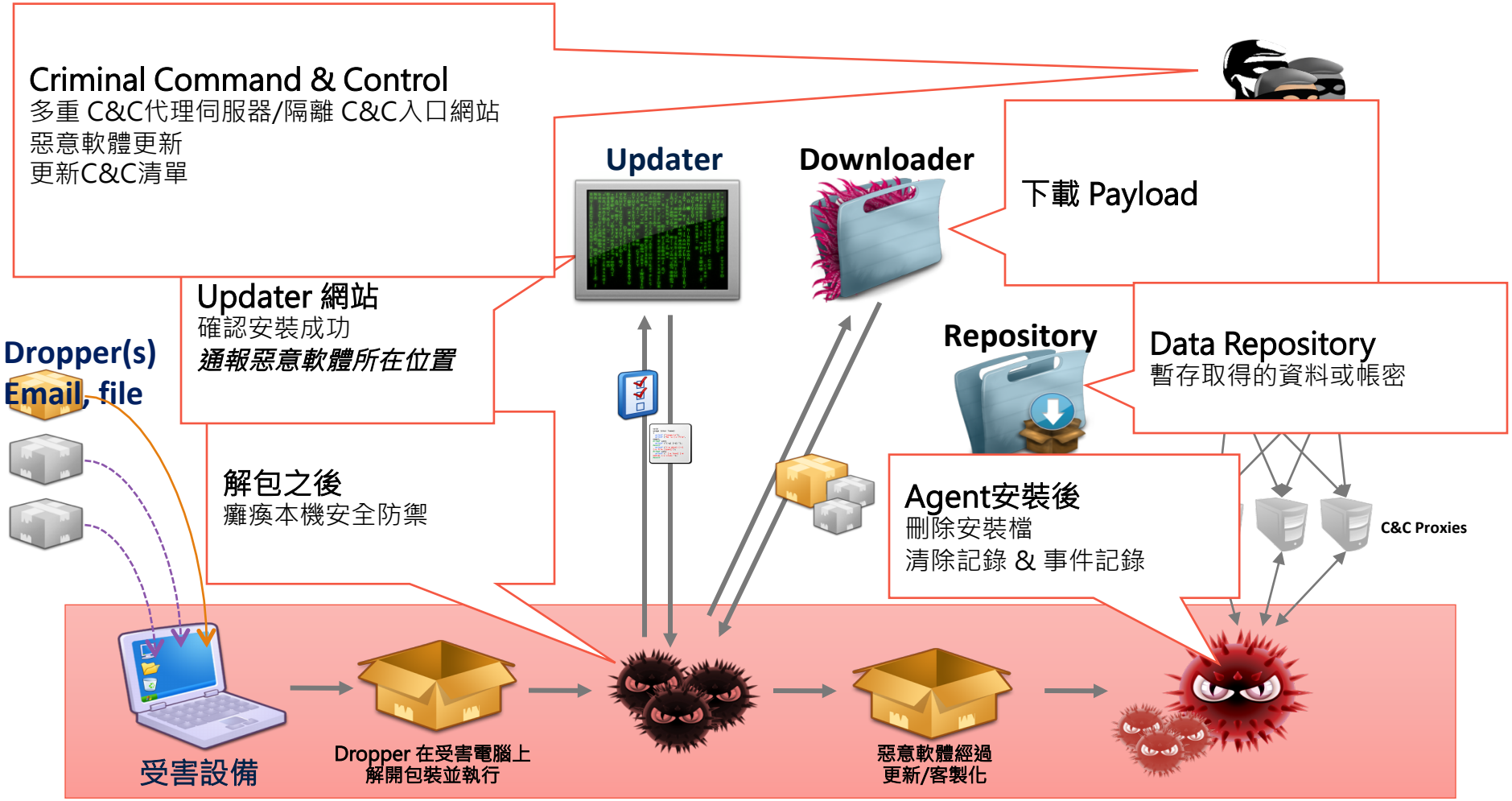
②辨識威脅等級與類別
提供建議處理順序

③專業人員按照順序於
惡意威脅尚未爆發前
好整以暇地解除危機

Cyberview
力悅資訊

惡意威脅是可以預警的？

如果您知道要找什麼行為跡證



網路攻擊鍊 - 無法防禦的40%

Cyberview 力悅資訊

一旦防禦失敗，後續的修復將會和時間賽跑

專家這麼說，但有限的資源應該放在1天、187天、49天？

<1 day

187 days

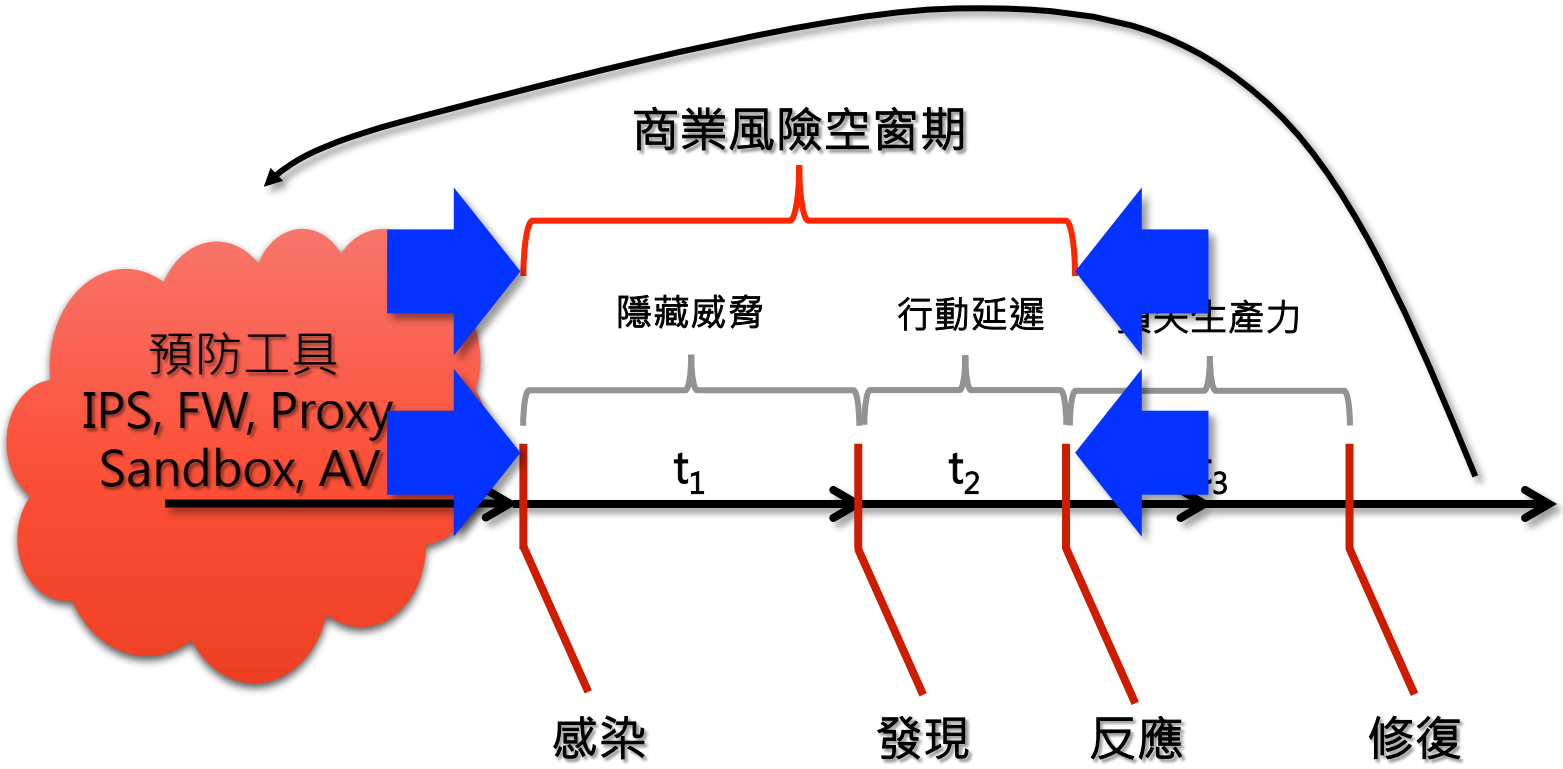
49 days

潛伏的威脅是可以被預警的，如果你知道要找什麼行為跡證

Sources: Ponemon Institute, "2016 Global Report on the Cost of Cyber Crime"
Ponemon Institute, "2016 Cost of Cyber Crime Study;" Verizon 2016 "Data Breach Investigations Report"

Cyberview 力悅資訊

早期預警系統的商業價值何在?



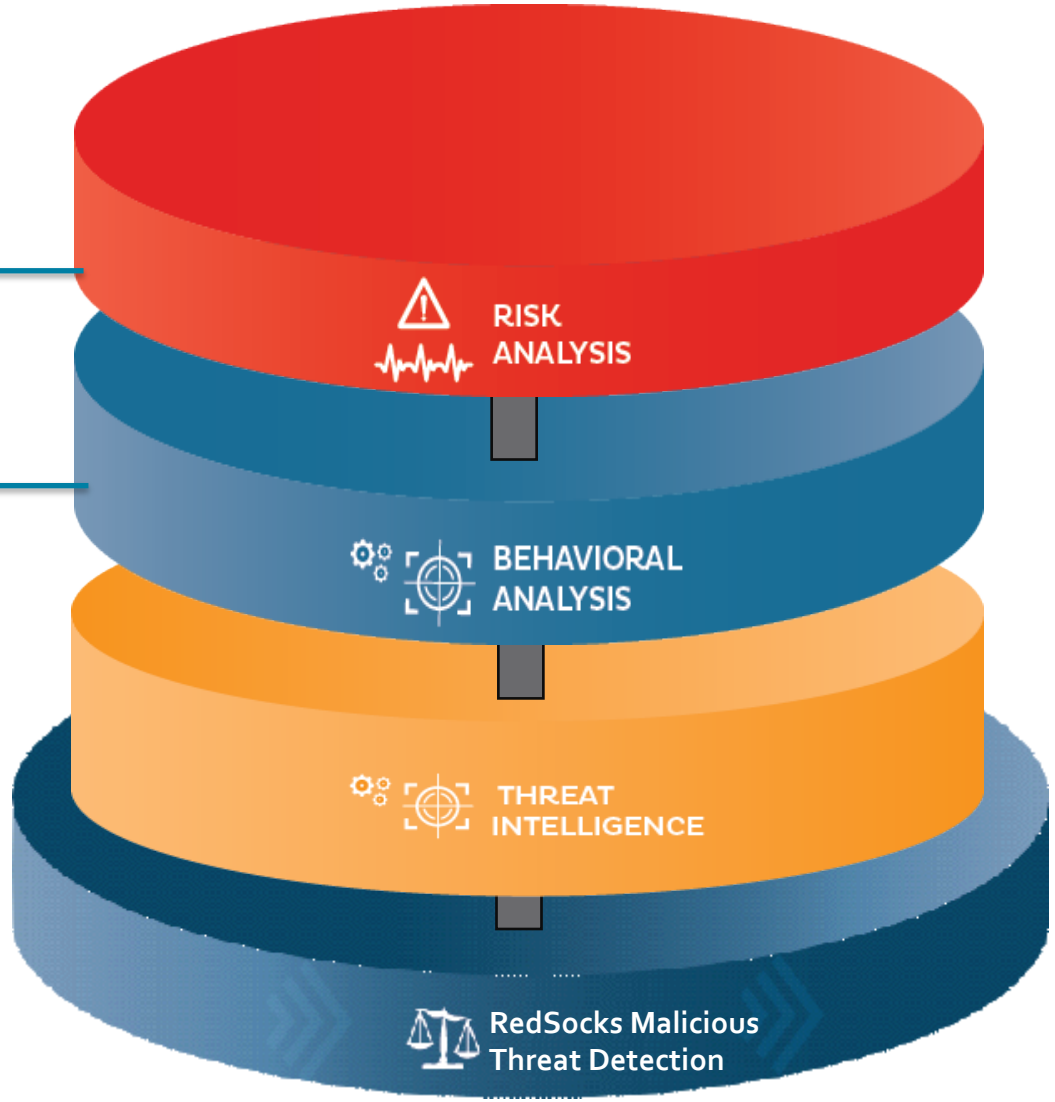
1. 阻止惡意威脅於未然

2. 依”現況”正確擬定資安策略

早期預警雷達

9種
風險等級

39+類
網路行為
雷達偵測



①
- ✓ Blacklisted hostnames and URLs
- ✓ Botnet Controller
- ✓ Malware-specific behavioral heuristics
- ✓ Sinkhole
- ✓ TOR Network

②
- ✓ Disguised executable file
- ✓ Experimental
- ✓ Mining Pool
- ✓ Miscellaneous
- ✓ Path traversal
- ✓ Periodic heartbeat
- ✓ Port scan
- ✓ Web shells

③
- ✓ Adware
- ✓ Bad Internet Neighbourhood
- ✓ BitTorrent tracker
- ✓ Cloud Storage Service
- ✓ File sharing
- ✓ File sharing Tool
- ✓ Instant Messaging
- ✓ Public Proxy
- ✓ Remote Administration
- ✓ Geofence (Syrian, Iran, Nigeria, Romania, Ukraine, Indonesia, China…)

④
- ✓ Domain Parker (DGA)
- ✓ Dynamic DNS domains
- ✓ Free hosting domains
- ✓ IP Self Check Service

... More…

Cyberview 力悅資訊

RedSocks Malicious Threat Detection 運作方式

RedSocks 威脅情資實驗室

>39+ 種網路行為分析
>100.000 每小時持續更新

BARE METAL LAB
HIGH VOLUME MALWARE ANALYSES
LONG TERM MALWARE ANALYSES
OPEN SOURCE INTELLIGENCE
MALWARE THROTTLE LAB
GEOFENCE
HEURISTICS

STIX - TAXII
情資檔匯入

7x24 惡意威脅
情報更新

公司內部網路

導入 RedSocks Malicious Threat Detection

SIEM
資安事件前因後果
關聯彙整

儀表板
快速檢視

即時與追蹤歷史
惡意威脅感染

PROBE
MNGT & FLOW DATA / IPFIX

IPFIX DATA

MIRRORED TRAFFIC

SWITCH

Malicious Threat Detection
(MTD)

資訊安全管理員

數位鑑識儲存庫
網路行為長期保留備查

公司資產
個人電腦, 筆記型電腦,
伺服器, 行動裝置

網際網路

熱門網站
惡意電子郵件

感染

INTERNET

黑客

租用

犯罪網絡

Cyberview 力悅資訊

REDSOCKS

malicious threat detection

實務案例的探討分析

案例探討分析① – Domain Parker

Domain Parker – 5 Infected device

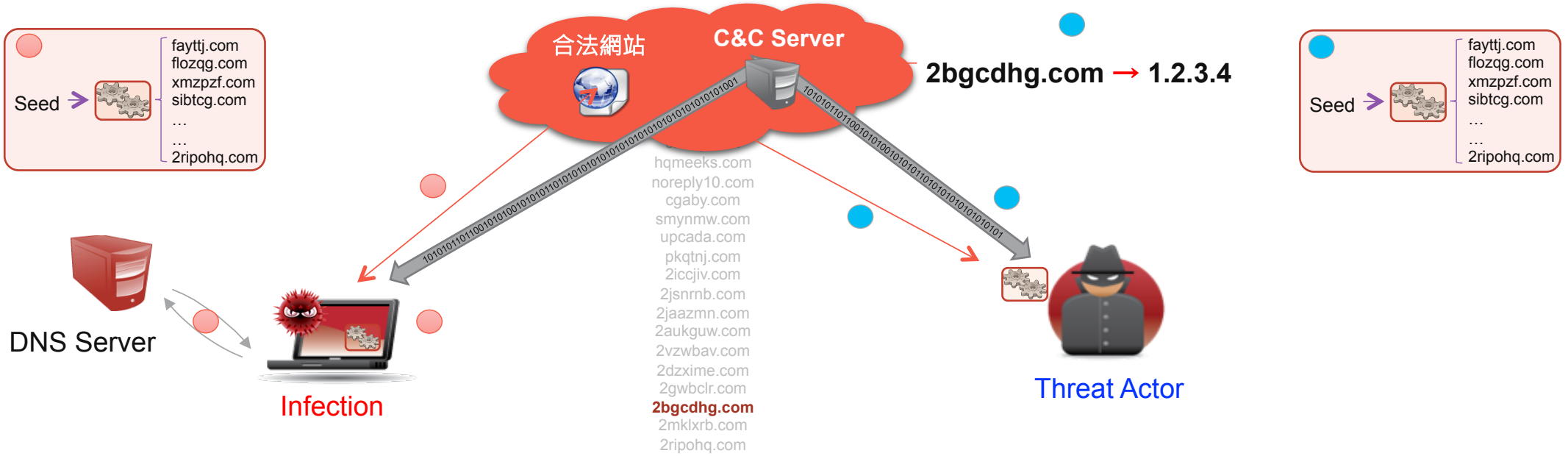
Domain parkers are IP's which host expired domains. Recurring connections to domain parkers can indicate infection with malware.

端點	感染類別 Level 5
10.80.1.113 172.16.121.171 10.80.199.122 10.80.142.46 10.80.80.56	Domain Parker

Timestamp (GMT+0800)	TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Wed Dec 20 2017 15:45:44	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.1.113	3699	184.168.221.40	27433	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 15:21:16	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.121.171	49548	5.39.99.50	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 15:20:29	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.121.171	49540	204.11.56.48	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:45:10	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.199.122	54152	50.63.202.91	80	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:32:04	5	Domain Parker	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.142.46	63683	185.53.179.8	443	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:32:04	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.142.46	63684	185.53.179.8	443	TCP	RSMIT - Expired Domain Parking IP
Wed Dec 20 2017 14:29:54	5	Domain Parker	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.80.56	52087	209.99.40.223	80	TCP	RSMIT - Expired Domain Parking IP

Cyberview 力悦資訊

DGA(Domain Fluxing) and Domain Parker



- Infection seeks a ‘Seed’ (e.g. cnn.com for date)
- Seed is entered into DGA, generating pseudo-random domains (e.g. 1000 domains)
- Infection queries Domains, seeking one with an IP
- Infection connects to domain with an IP, communicates with threat actor
- Cycle begins again

- Threat Actor seeks a ‘Seed’ (e.g. cnn.com for date)
- Seed is entered into DGA, generating pseudo-random domains (e.g. 1000 domains)
- Threat actor registers one domain, with an IP
- Infection connects to domain with an IP, threat actor communicates with infection
- Cycle begins again

Cyberview 力悅資訊

案例探討分析② – Sinkhole

Sinkhole – 4 Infected device

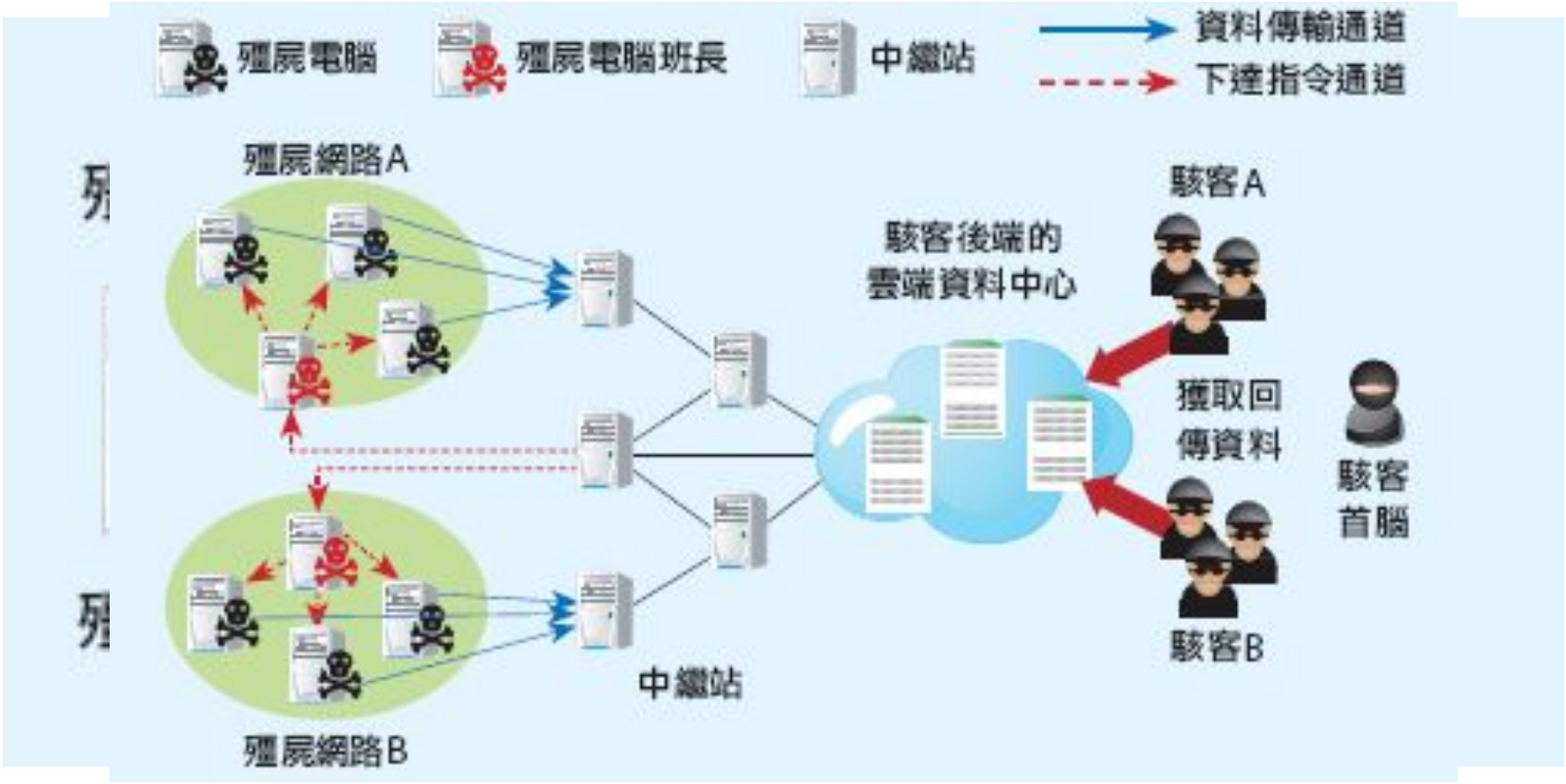
Malware is active on your client's system, but the controller IP has been seized or diverted in order to disable the botnet. The infected client still tries to connect to it and, therefore, a breach and an infection occurred in the past.

端點	感染類別 Level 1
10.80.153.128 10.80.130.59 10.80.148.63 10.80.239.10	Sinkhole

Timestamp (GMT+0800)	TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Thu Dec 21 2017 10:24:19	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.153.128	1315	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...
Thu Dec 21 2017 10:23:49	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.153.128	1314	23.253.126.58	41801	UDP	RSMIT - Arbor Networks Malware Sinkhole
Thu Dec 21 2017 10:15:58	1	Sinkhole	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	10.80.130.59	4067	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...
Thu Dec 21 2017 10:15:28	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.130.59	4031	23.253.126.58	41801	UDP	RSMIT - Arbor Networks Malware Sinkhole
Thu Dec 21 2017 10:14:12	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.148.63	49502	204.95.99.243	3720	TCP	RSMIT - Malware Sinkhole (Microsoft DDNS Take...
Thu Dec 21 2017 10:12:50	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.239.10	50396	204.95.99.109	80	TCP	RSMIT - Malware Sinkhole (Microsoft DDNS Take...
Thu Dec 21 2017 10:08:27	1	Sinkhole	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	10.80.130.59	3925	193.166.255.171	41801	UDP	RSMIT - FitSec Malware Sinkhole (sinkhole.fitsec.c...

Cyberview 力悅資訊

殭屍網路與 Sinkhole



案例探討分析③ – Bad Internet Neighbourhood & Ming Pool

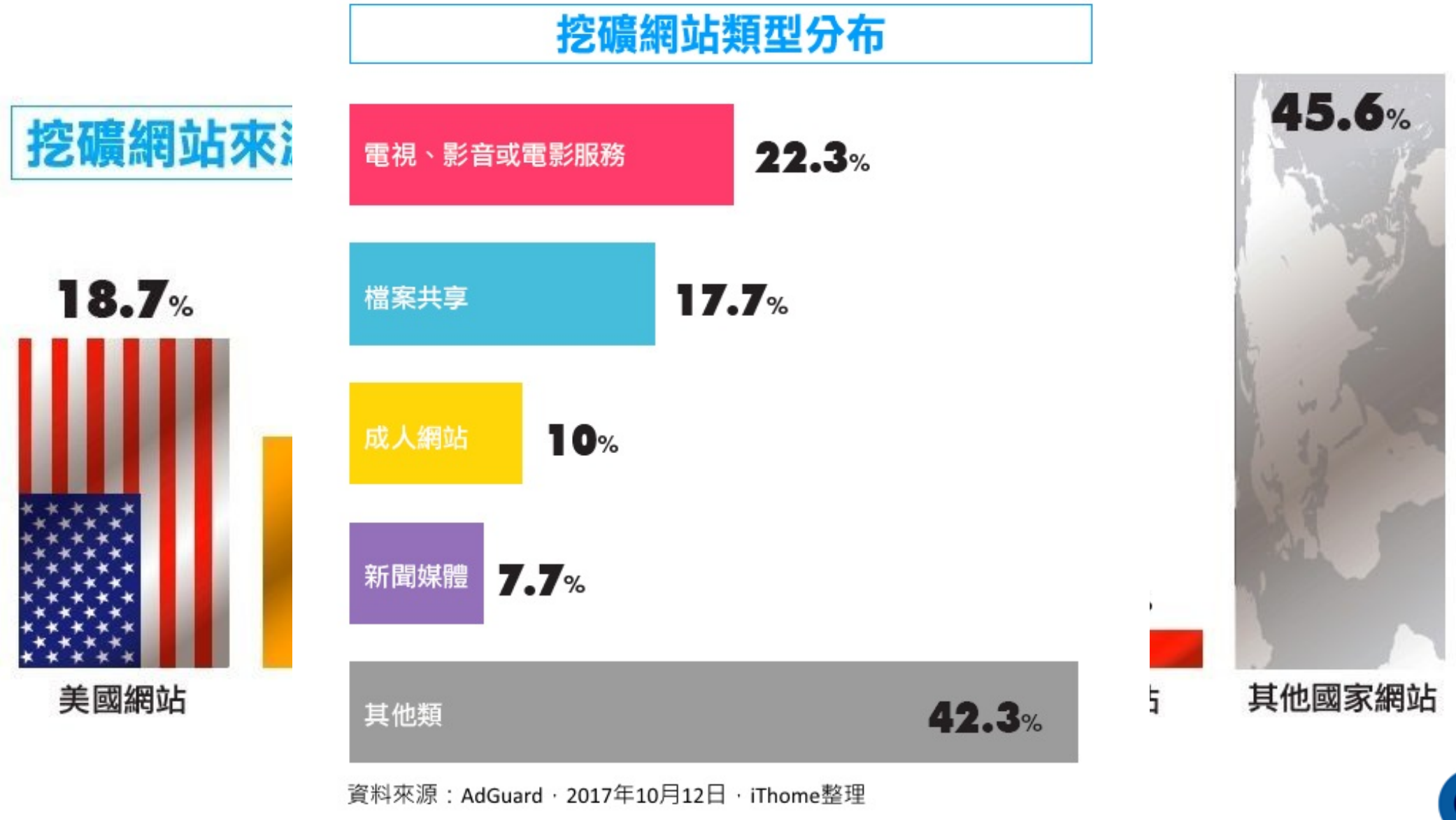
Bad Hood & Ming Pool – 3 Infected device

These IP-addresses are frequently used in targeted attacks, phishing/pharming campaigns or as Botnet Controllers.
Cryptocurrencies are generated by users who offer their CPU or GPU power to calculate complex algorithms
A mining pool occurs when multiple people combine computing resources to produce cryptocurrencies. Malware writers are always looking for ways to make money and illicitly using your computer to generate cryptocurrencies pays off. In addition to malware, mining can also be done by personnel who uses resources for personal benefit. An alert in this category should warrant further investigation.

端點	感染類別 Level 3
172.16.36.19 172.16.142.28 172.16.134.108	Bad Hood Ming Pool

Timestamp (GMT+0800)	TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Thu Dec 21 2017 10:15:21	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	43110	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 09:51:10	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.142.28	39526	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 09:31:59	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42676	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 09:00:02	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.134.108	50014	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 08:59:59	3	Bad Hood	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.134.108	44125	49.4.20.52	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 08:44:09	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42608	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...
Thu Dec 21 2017 07:57:40	3	Bad Hood	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.36.19	42590	49.4.20.230	8443	TCP	RSMIT - Connection on Backdoor or Trojan Defau...

盜用電腦資源挖礦



資料來源：AdGuard，2017年10月12日，iThome整理

Cyberview 力悅資訊

案例探討分析④ – TOR Network

TOR Network – 2 Infected device

The Tor Network is designed to offer anonymous Internet access to its users and can also be used to hide a Botnet Controller. Anonymous access could be a used as a means to subvert company usage policy or even engage in illicit activity. Since mid-2013, the Tor Network has been used by an increasing number of operators to hide communications with Botnet Controllers. If not initiated by an employee, then an infection is present within your network. An alert in this category should be investigated at all times.

端點	感染類別 Level 1
172.16.126.71 172.16.126.14	TOR

Timestamp (GMT+0800)	TL	Category	Exporter IP address	ODID	Source MAC	Source IP	Port	Destination IP	Port	Protocol	Alert detail
Wed Dec 20 2017 12:39:26	1	Tor	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.126.71	51238	62.210.244.146	9001	TCP	RSMIT - Tor Connecting IP - Country FR - hxxp://6...
Wed Dec 20 2017 11:54:09	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.71	51230	136.243.243.6	1444	TCP	RSMIT - Tor Connecting IP - Country DE - hxxp://t...
Wed Dec 20 2017 11:54:09	1	Tor	::ffff:ac8:c8c8	3	84:78:ac:22:8d:c1	172.16.126.71	51227	146.0.77.50	443	TCP	RSMIT - Tor Connecting IP - Country NL
Wed Dec 20 2017 10:06:42	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.71	49447	178.16.208.57	443	TCP	RSMIT - Tor Connecting IP - Country SE - hxxp://b...
Mon Dec 18 2017 18:43:41	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	52722	77.68.11.42	9001	TCP	RSMIT - Tor Connecting IP - Country GB
Mon Dec 18 2017 13:54:11	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	50238	91.121.23.100	9001	TCP	RSMIT - Tor Connecting IP - Country FR - hxxp://0...
Mon Dec 18 2017 13:41:55	1	Tor	::ffff:ac8:c8c8	4	84:78:ac:21:91:c1	172.16.126.14	55805	128.31.0.39	9101	TCP	RSMIT - Tor Connecting IP

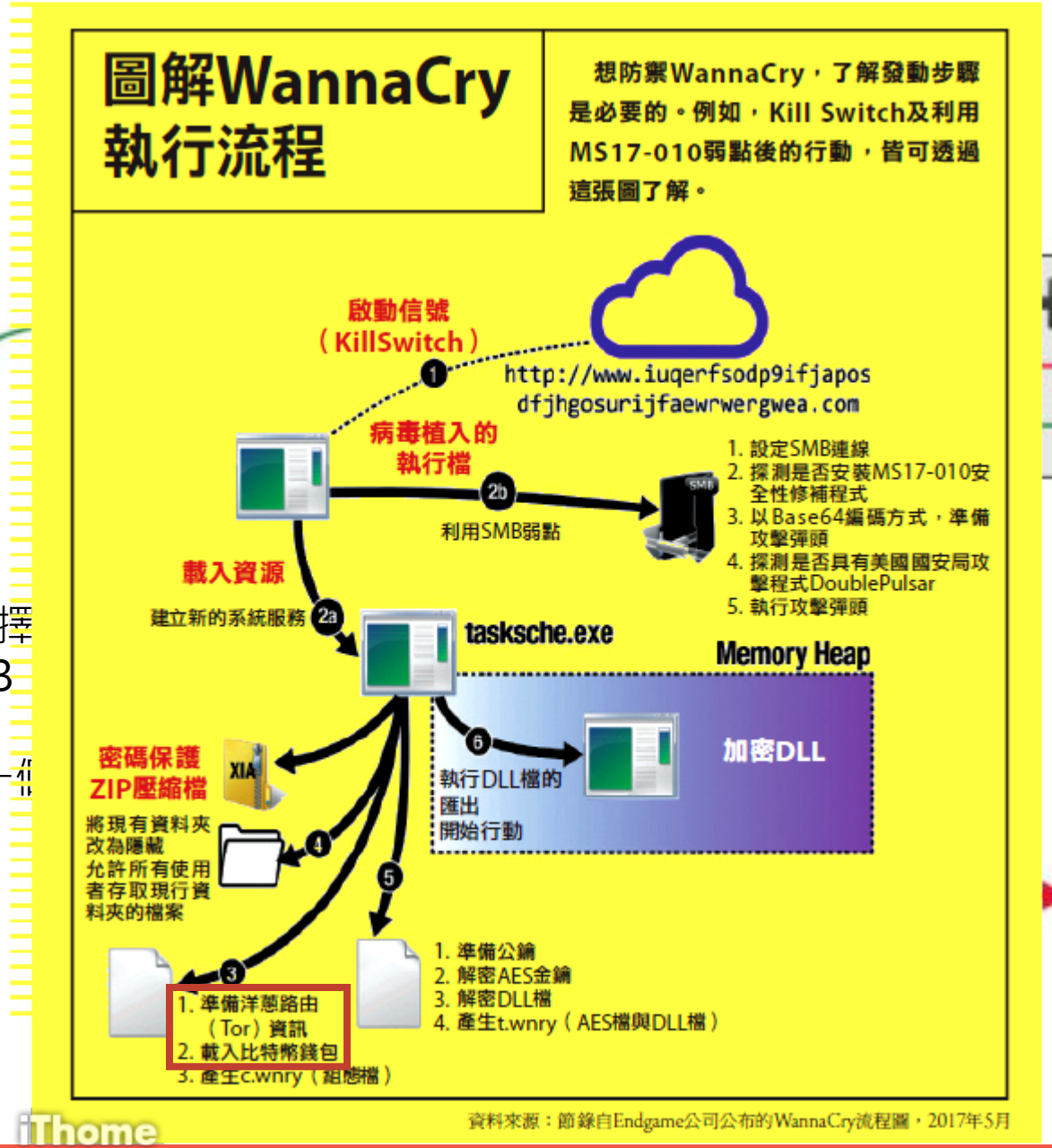
Cyberview 力悅資訊

TOR (洋蔥路由)網絡運作原理

A

A 的 TOR 軟體會自動選擇隨機路徑並抵達伺服器 B

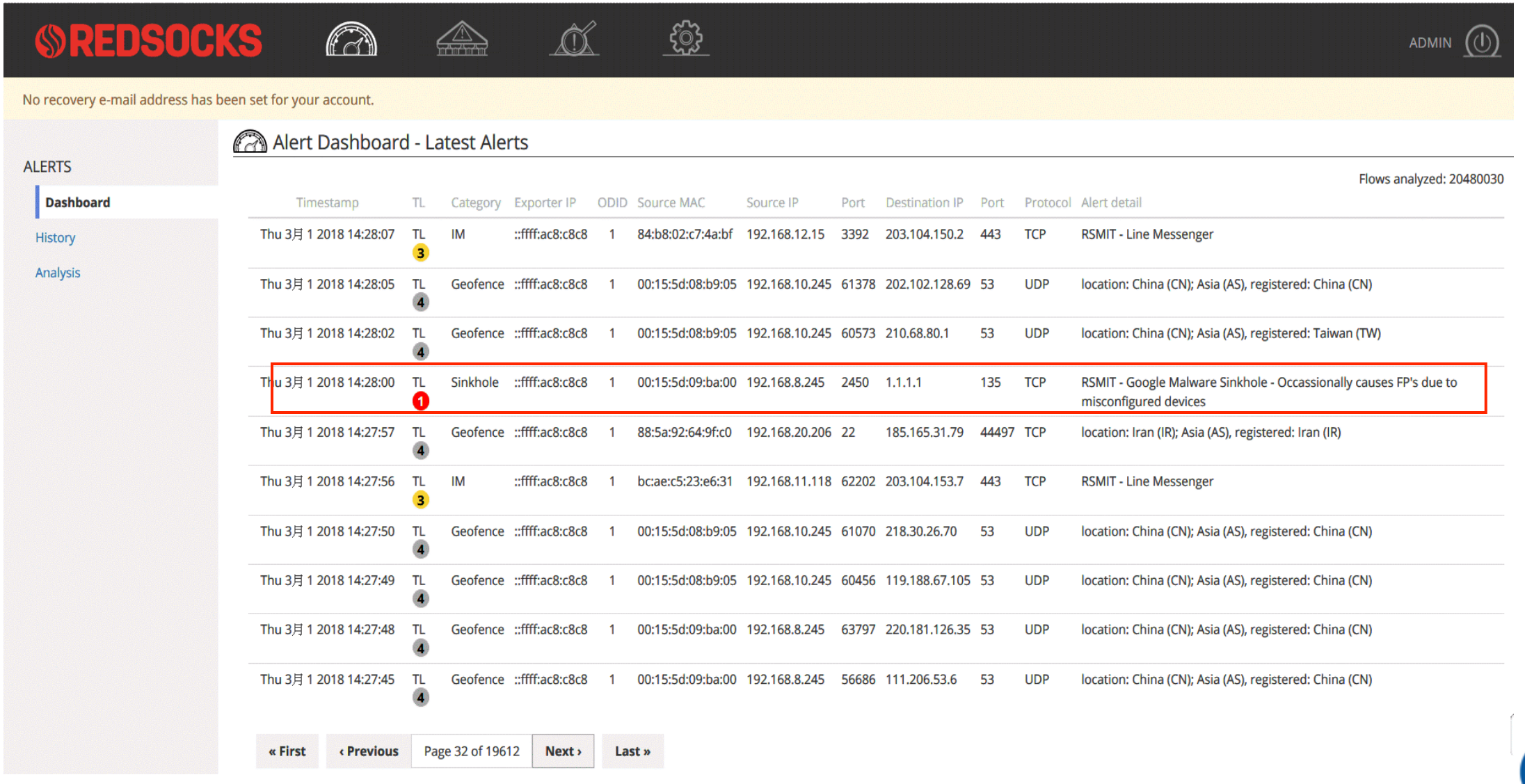
B 看到的來源只會是上一站來源位址



B

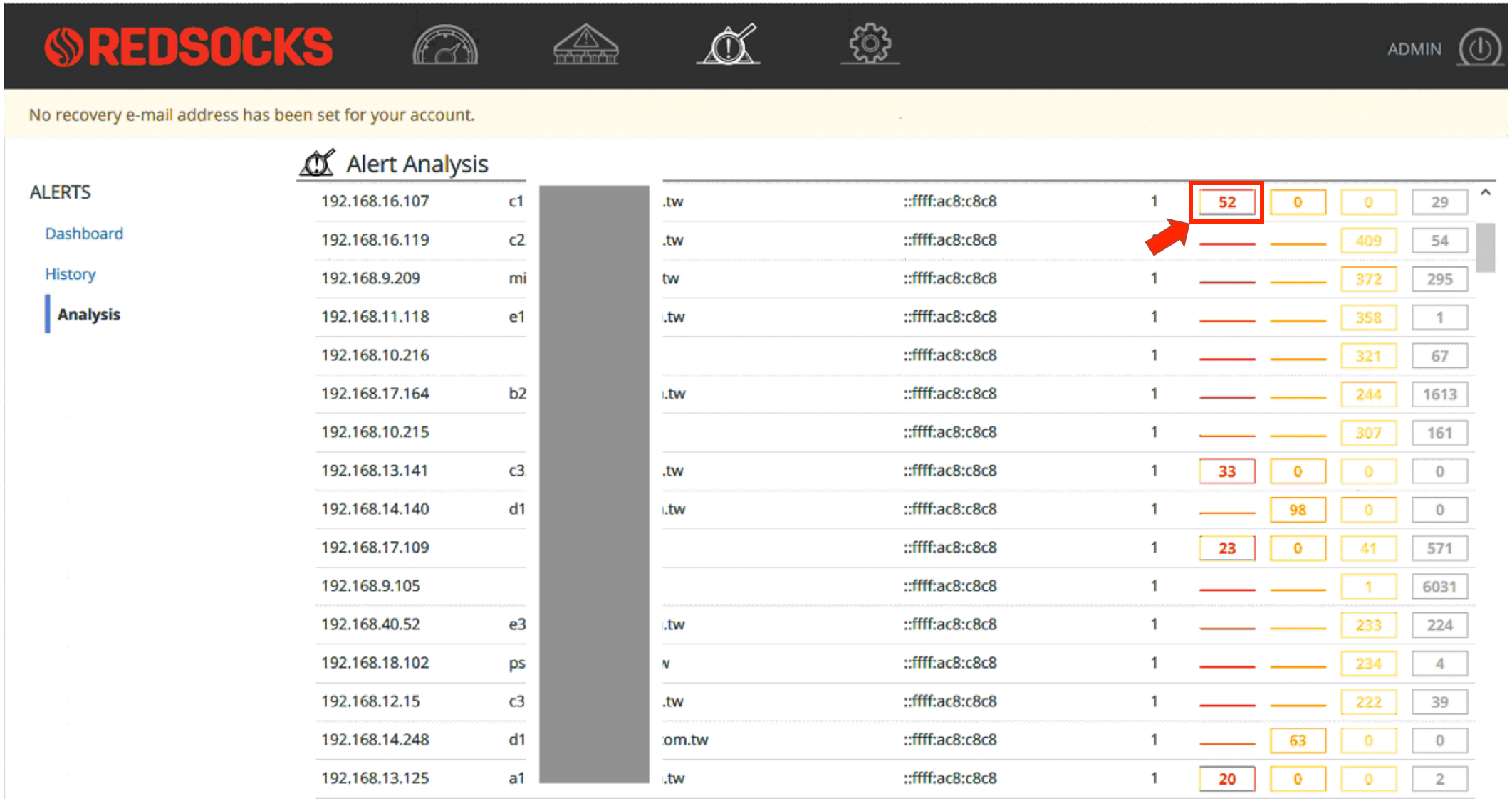
Cyberview 力悦資訊

RedSocks 儀表板



Cyberview 力悅資訊

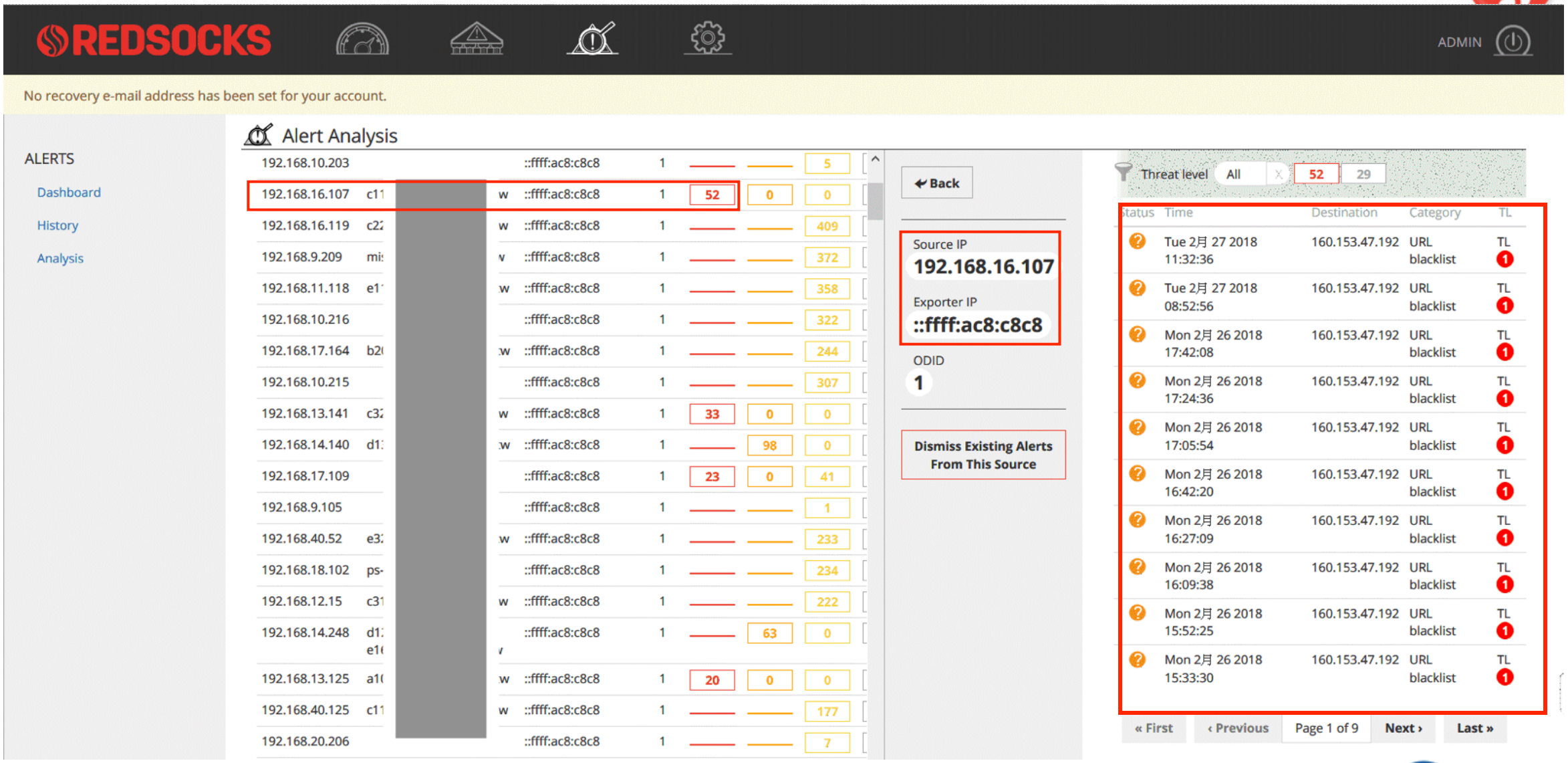
RedSocks 威脅分析 ① -直覺式高風險排序



192.168.16.107	c1	.tw	::ffff:ac8:c8c8	1	52	0	0	29
192.168.16.119	c2	.tw	::ffff:ac8:c8c8				409	54
192.168.9.209	mi	tw	::ffff:ac8:c8c8	1			372	295
192.168.11.118	e1	.tw	::ffff:ac8:c8c8	1			358	1
192.168.10.216			::ffff:ac8:c8c8	1			321	67
192.168.17.164	b2	.tw	::ffff:ac8:c8c8	1			244	1613
192.168.10.215			::ffff:ac8:c8c8	1			307	161
192.168.13.141	c3	.tw	::ffff:ac8:c8c8	1	33	0	0	0
192.168.14.140	d1	.tw	::ffff:ac8:c8c8	1		98	0	0
192.168.17.109			::ffff:ac8:c8c8	1	23	0	41	571
192.168.9.105			::ffff:ac8:c8c8	1			1	6031
192.168.40.52	e3	.tw	::ffff:ac8:c8c8	1			233	224
192.168.18.102	ps	v	::ffff:ac8:c8c8	1			234	4
192.168.12.15	c3	.tw	::ffff:ac8:c8c8	1			222	39
192.168.14.248	d1	om.tw	::ffff:ac8:c8c8	1		63	0	0
192.168.13.125	a1	.tw	::ffff:ac8:c8c8	1	20	0	0	2

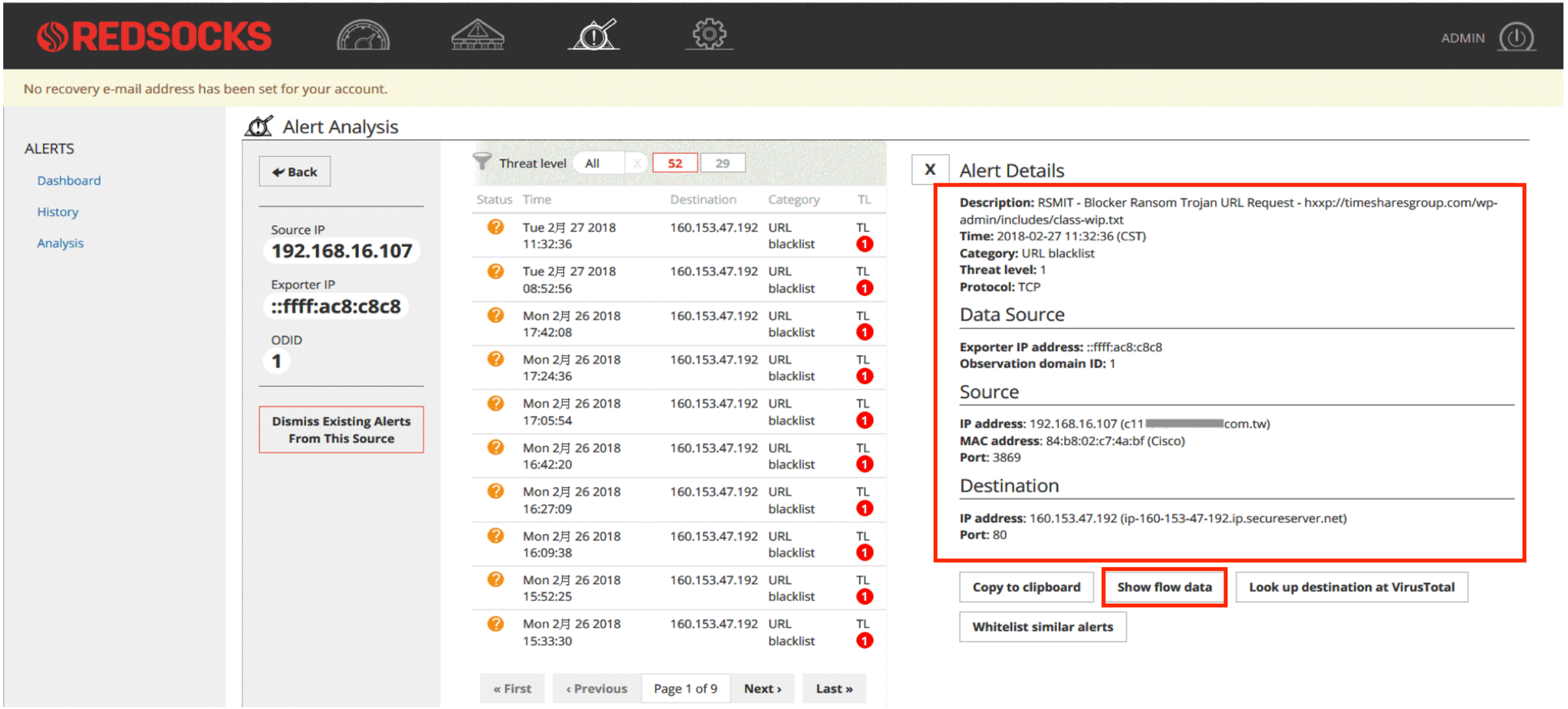
Cyberview 力悅資訊

RedSocks威脅分析 ② - C&C詳細通聯紀錄



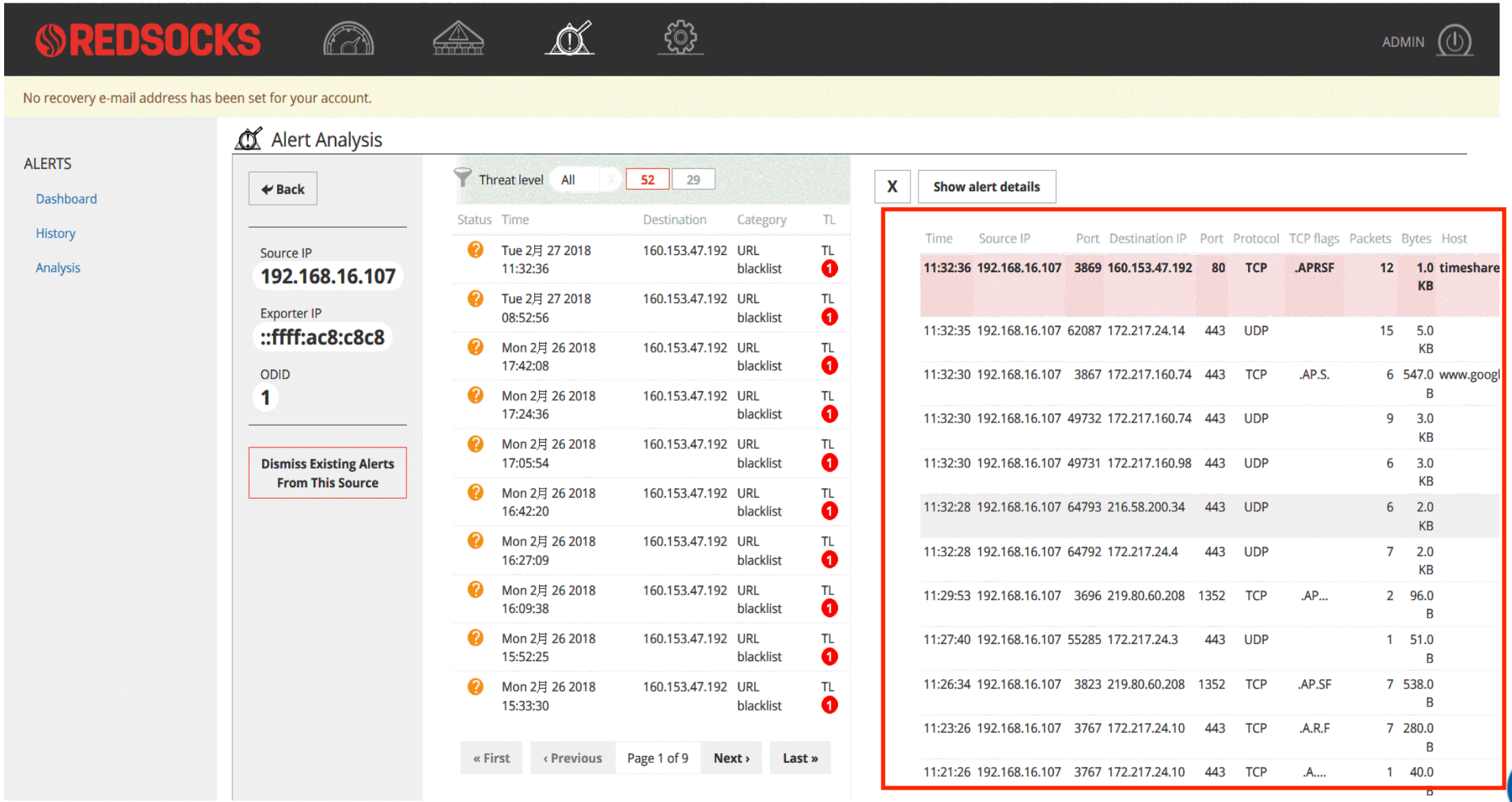
Cyberview 力悅資訊

RedSocks威脅分析 ③ - 威脅分析



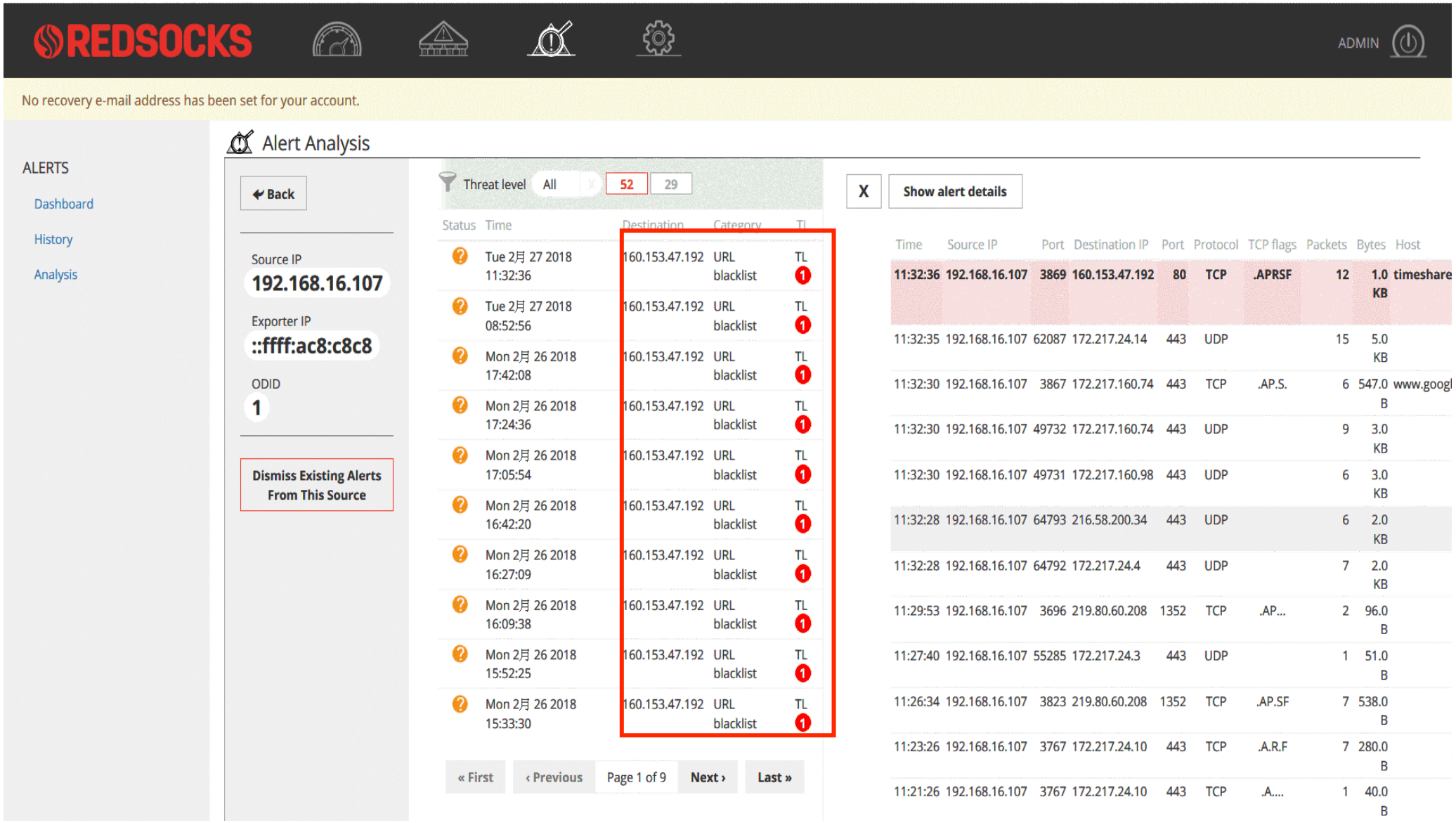
Cyberview 力悅資訊

RedSocks威脅分析 ④ - 完整通聯紀錄



Cyberview 力悅資訊

RedSocks威脅分析 ④ - 殭屍就在您我之間



Cyberview 力悅資訊

RedSocks威脅分析 ④ - 殭屍就在您我之間

1、資安功能 VS 資安產品

2、公司官網淪為惡意程式下載點、C&C、Botnet
(主動攻擊C&C是否可行？)

3、平均感染率2%(台灣>全球平均)

4、DC(兵家必爭之地)

Cyberview 力悅資訊

與眾不同的特點

市場最佳威脅情資

快速即時

非侵入式

大規模擴充

最大隱私權

歐盟資料保護規範

- 任何協定與埠號，包含加密
- 不影響網路、大規模分散式佈建
- 時光回溯
- 紀錄所有通聯
- 零誤判
- 上線立即產生效益

彈性的商業模式

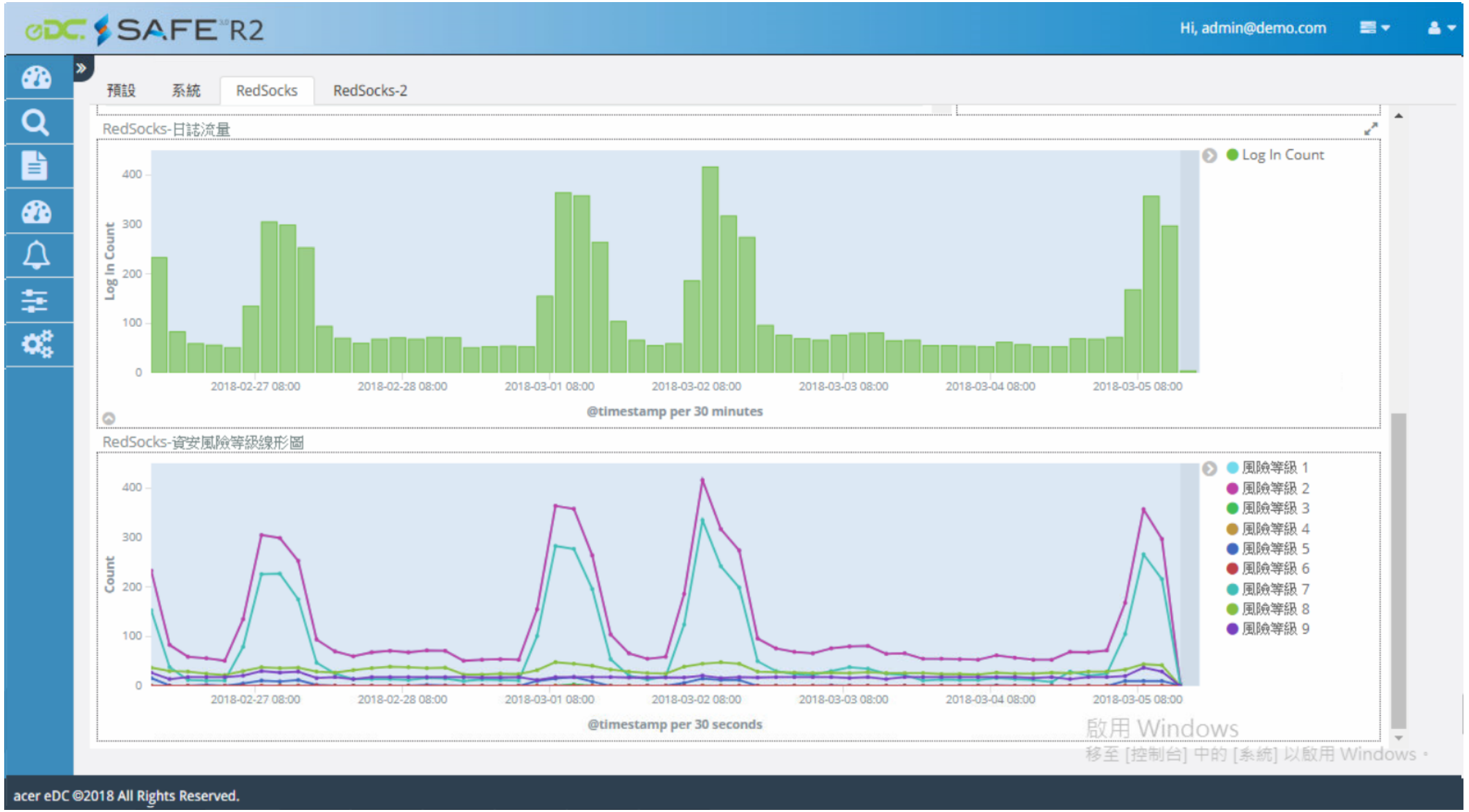
- **軟體建置長期分析**
  - 持續且深入的資訊安全預警系統
  - 保持即時的威脅情資更新
  - 可依照彈性安排優先處理順序

- **短期資訊安全顧問服務**
  - 為期四週的網路行為收集分析
  - 專業的資訊安全顧問深度剖析
  - 實証為資訊安全政策提供正確方向

Cyberview 力悅資訊

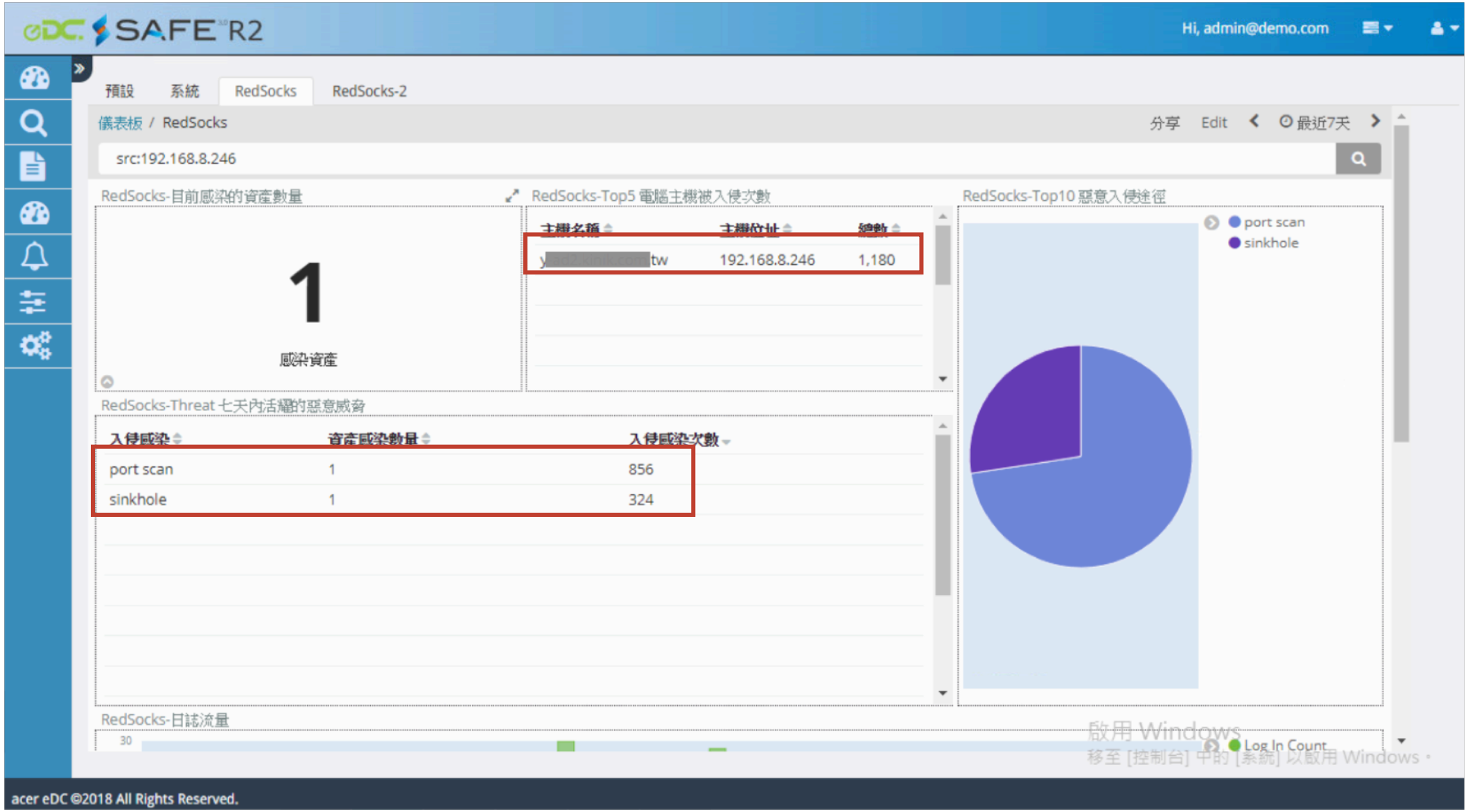
One more thing…

與宏碁雲架構合作強化預警系統



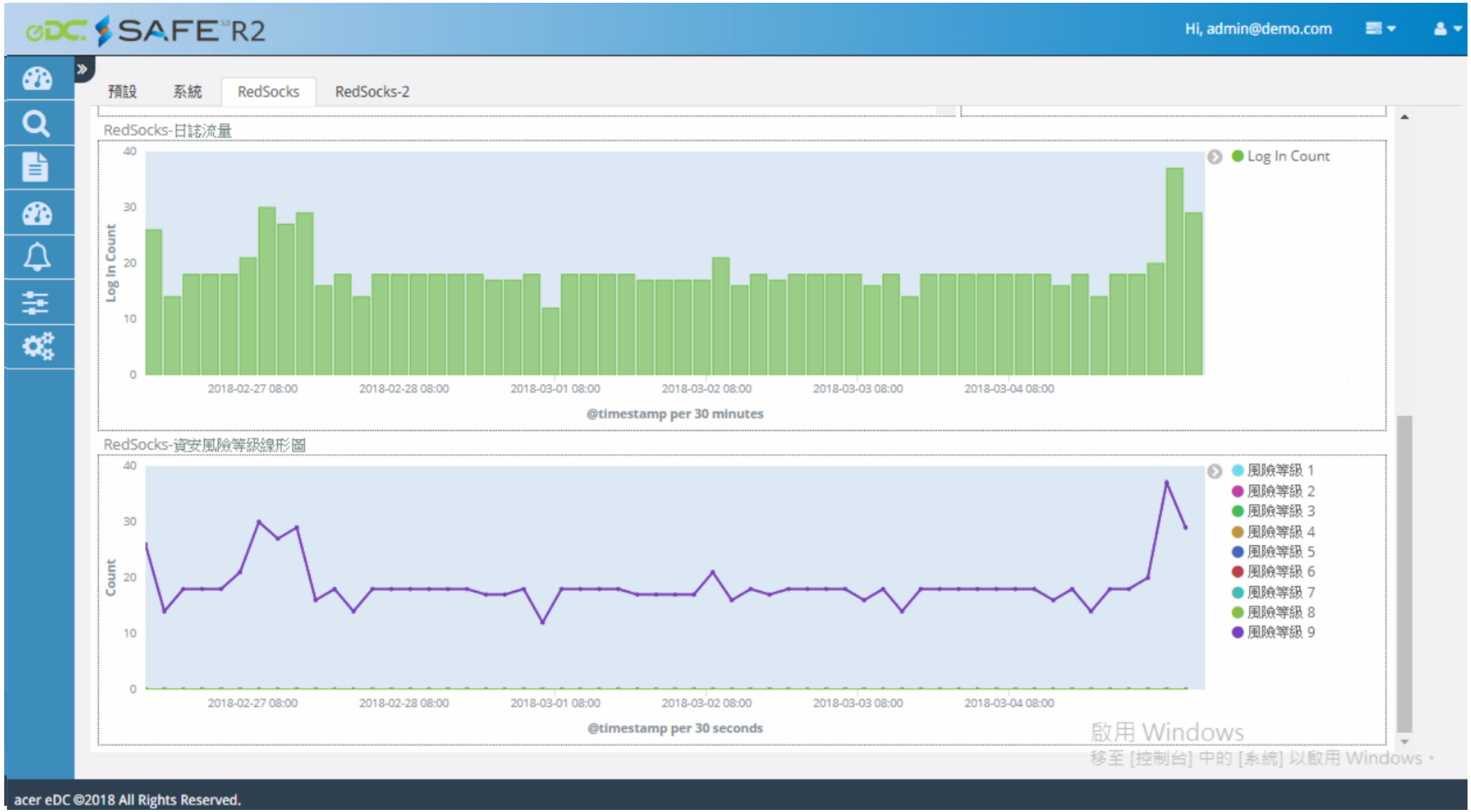
Cyberview 力悅資訊

與宏碁雲架構合作強化預警系統 – 端點感染情況



Cyberview 力悅資訊

與宏碁雲架構合作強化預警系統－高風險威脅感染情況



Cyberview 力悅資訊