資安法上路，別再單打獨鬥
CyberX 助您共同防禦

天禦慧智　　林士敏

2019

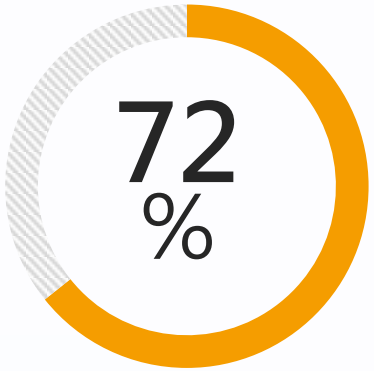
Agenda

- 資安攻防不對等，秒懂攻擊新趨勢
- 校園資安盤點，面對AI攻擊如何迎戰？
- CyberX 防禦應變通報平台，落實校園資安做好防護
- CyberX Live Demo
- Q&A

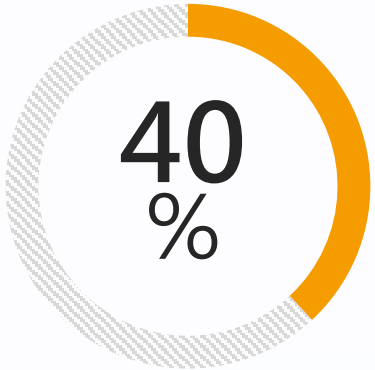
資安攻防不對等，秒懂攻擊新趨勢

CISO為何徹夜難眠？

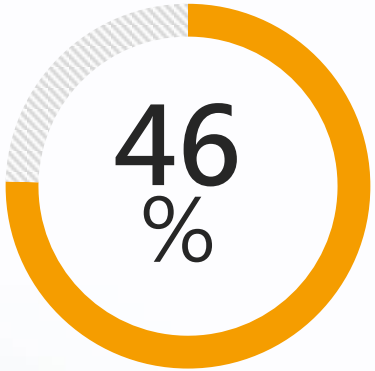
- 惡意駭客與未知威脅是使CISO徹夜難眠的第一主因，即使是精通處理網路安全風險的CISO也不願掉以輕心。



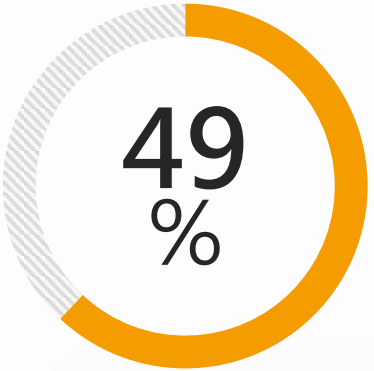
CISO 將大部分資源用於防禦惡意駭客與未知威脅



CISO 認為惡意駭客與未知威脅是組織中最重要的安全風險



CISO 認為惡意駭客與未知威脅是徹夜難眠的最大威脅之一



CISO 計畫未來投入更多資源來防禦惡意駭客與未知威脅

CISO為何徹夜難眠？

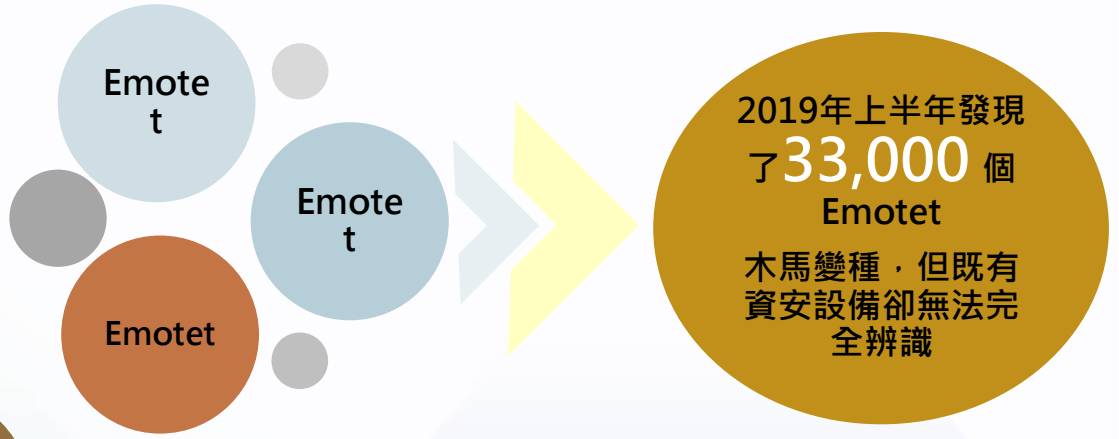
- 傳統資安檢測技術讓組織更易受到惡意駭客與未知威脅的攻擊。
- 近年來威脅的數量和復雜性大幅度的增加，隨著企業網路應用和威脅的發展，既有的資安防禦技術未能跟上步伐，無法阻止規避威脅更遑論 AI 恐已經淪為駭客利器。

01 **無法檢測內網橫向威脅** 80%
希望能更有效偵測網路內部駭客活動與橫向移動威脅

02 **SOC警報太多無法消化** 69%
IT資安管理人員表示“過多誤報”使得在SOC中心工作非常“痛苦”

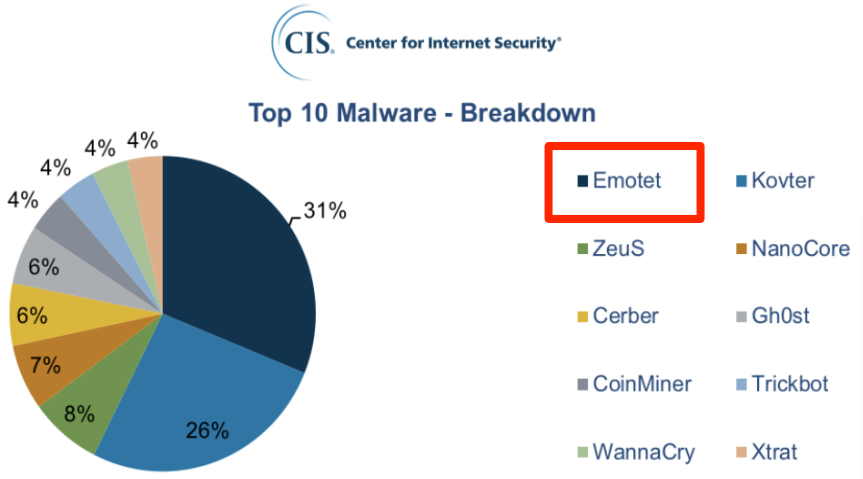
03 **層層堆疊設備卻無法自動化** 67%
資安管理人員表示“工作流程自動化”將“減輕SOC團隊的痛苦”

04 **無法擺脫人力大量投入的夢靨** 27%
資安管理人員表示，目前最耗時的任務是建立，微調與更新既有資安系統

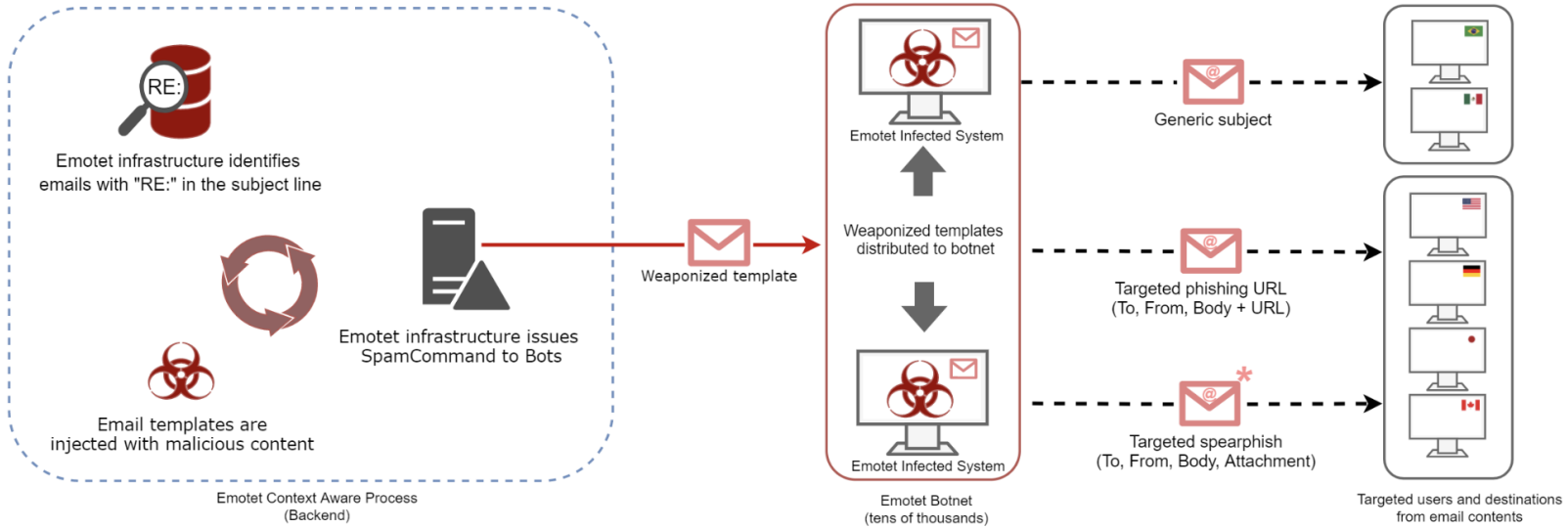


Emotet : AI-enabled Malware

- AI 人工智能驅動的網路攻擊已不是未來的假想概念，Emotet 是當今前十大的惡意程式之一，也是AI 原型攻擊的典型案例。
- 一旦 Emotet 被植入到受害裝置中，它可以作為惡意郵件活動的裝置源，並自動下載其他惡意軟體(如可使裝置所在的整個網路受到勒索軟體Ryuk感染的Trickbot)，同時感染網路內更多裝置，並可以輕鬆利用AI 來增強攻擊，透過 AI 分析電子郵件線程的上下文搭配學習和複製自然語言的能力，這意味著 AI 智能驅動的 Emotet 可以創建並插入完全客製與更可信的網路釣魚郵件。



Top 10 industries affected by Emotet Trojan malware	
1	Consulting
2	Education
3	Manufacturing
4	Hospitality/Leisure
5	Government
6	Retail
7	Transportation and logistics
8	Chemicals
9	Healthcare
10	Technology



AI 攻擊應用場景

Vulnerability Discovery

AI可以夠過從目標系統上運行的服務中提取訊息來幫助進行漏洞分析和利用。

Exploitation

人工智能可以幫助攻擊者找到正確的方法來產生可入侵特定應用程序/系統/環境/基礎架構的漏洞，與人類相比機器運行速度快得多，並可快速改編漏洞利用代碼。

Data Theft

駭客獲利的主要來源，AI 非常適合快速搜索，駭客可以使用它來搜索和分類關鍵用戶數據（例如信用卡，SSN，用戶電子郵件和密碼等)。

Phishing

機器學習最常見的應用就是自然語言處理（NLP），駭客可以使用機器學習對系統進行培訓，產生仿真度極高的釣魚郵件來確保更智能的社交工程攻擊。

Smart Botnet

智能物聯網設備可透過培訓使其攻擊能量擴展，殭屍電腦將變得更聰明且不受殭屍網路牧者的干預，具備同時攻擊多個目標的能力，將大幅的阻礙受害者恢復到正常運營的能力。

Evasive Malware

機器學習與人工智能技術越來越成熟，已證明機器學習可以即時修改代碼來創建具備強大規避能力的惡意程式。

DDoS

以Mirai殭屍網路攻擊為例，人工智能的發展證明可利用物聯網放大DDoS產生毀滅性攻擊。

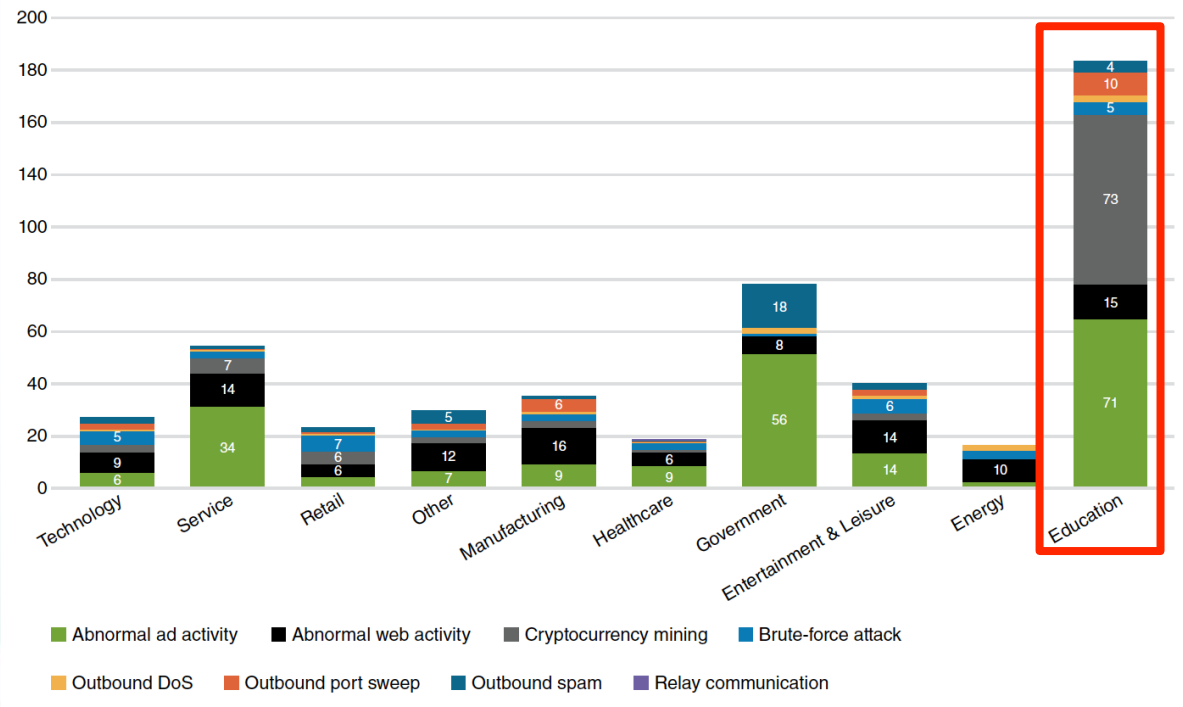
02

校園資安盤點，面對 AI 攻擊如何迎戰？

校園資安盤點

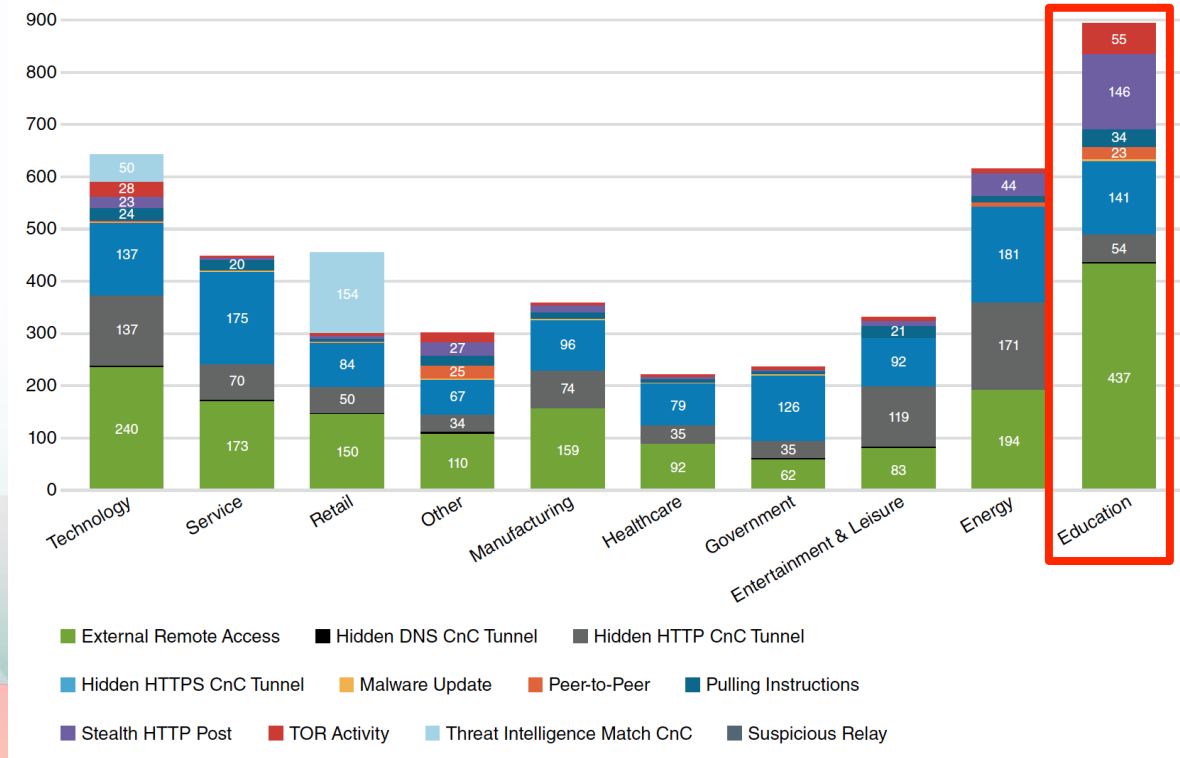
Botnets

分析報告顯示校園網路中加密貨幣挖掘趨勢持續升高，特別是在大學網路中，可能由於缺乏安全控管，讓大學成為殭屍網路牧民的鎖定目標，以及免費電力的獲得。



C&C 中繼站連線

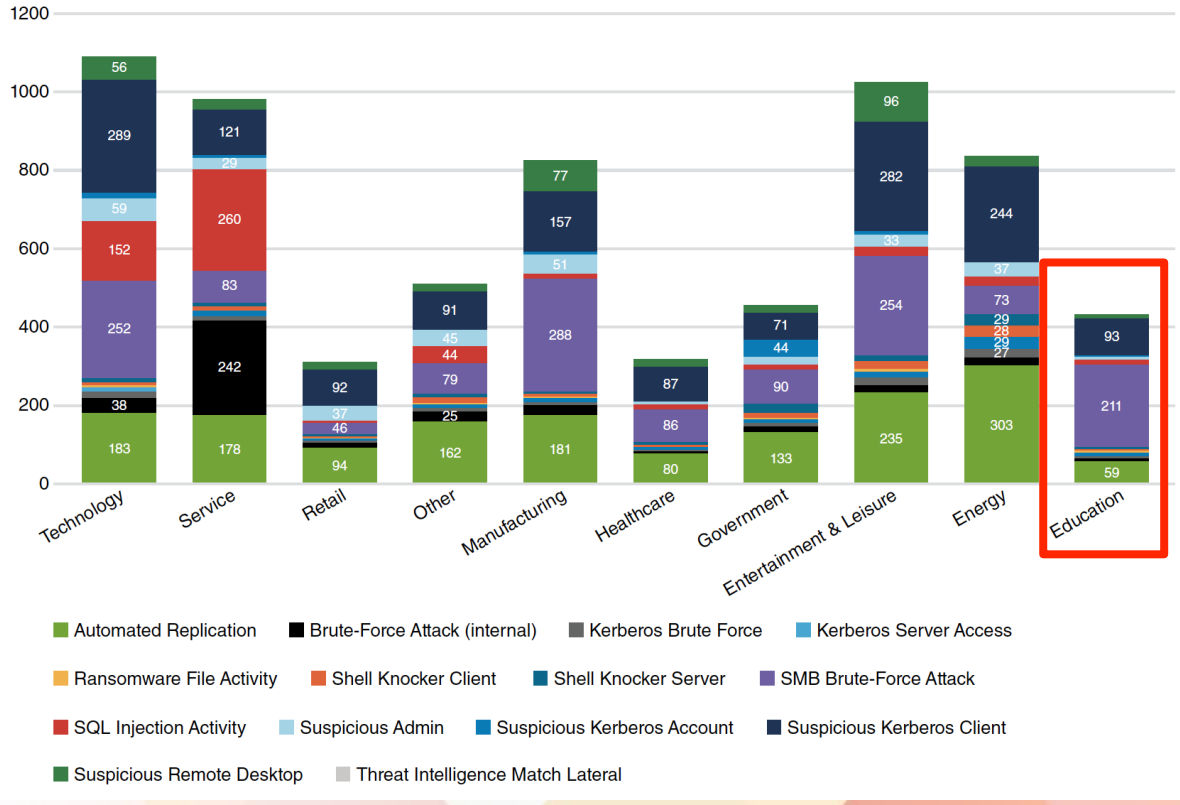
從分析報告顯示，校園網路存在大量的 C&C 連線行為，由於中繼站連線其意圖繞過安全檢查，所以代表了巨大的風險。



校園資安盤點

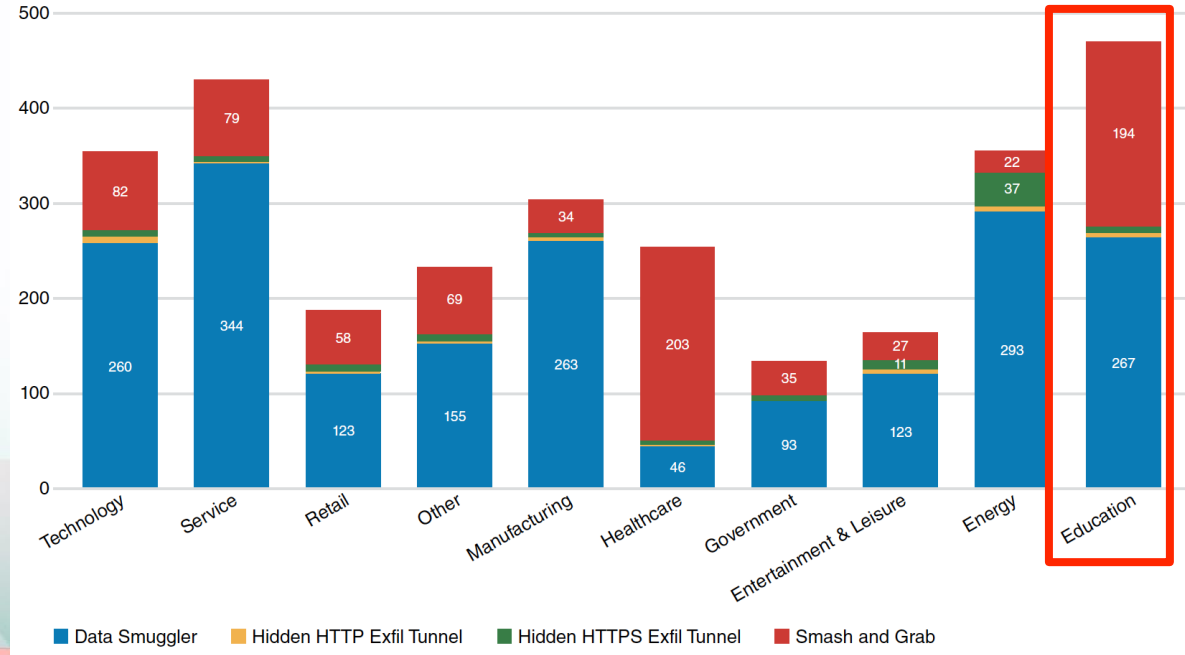
Lateral movement

橫向移動技術廣泛應用APT攻擊，攻擊者使用此技術訪問受感染系統中的其他主機，並訪問敏感資源與竊取更有價值的憑證，透過橫向移動攻擊最終可以拿到權限，進而控制校園內重要主機。

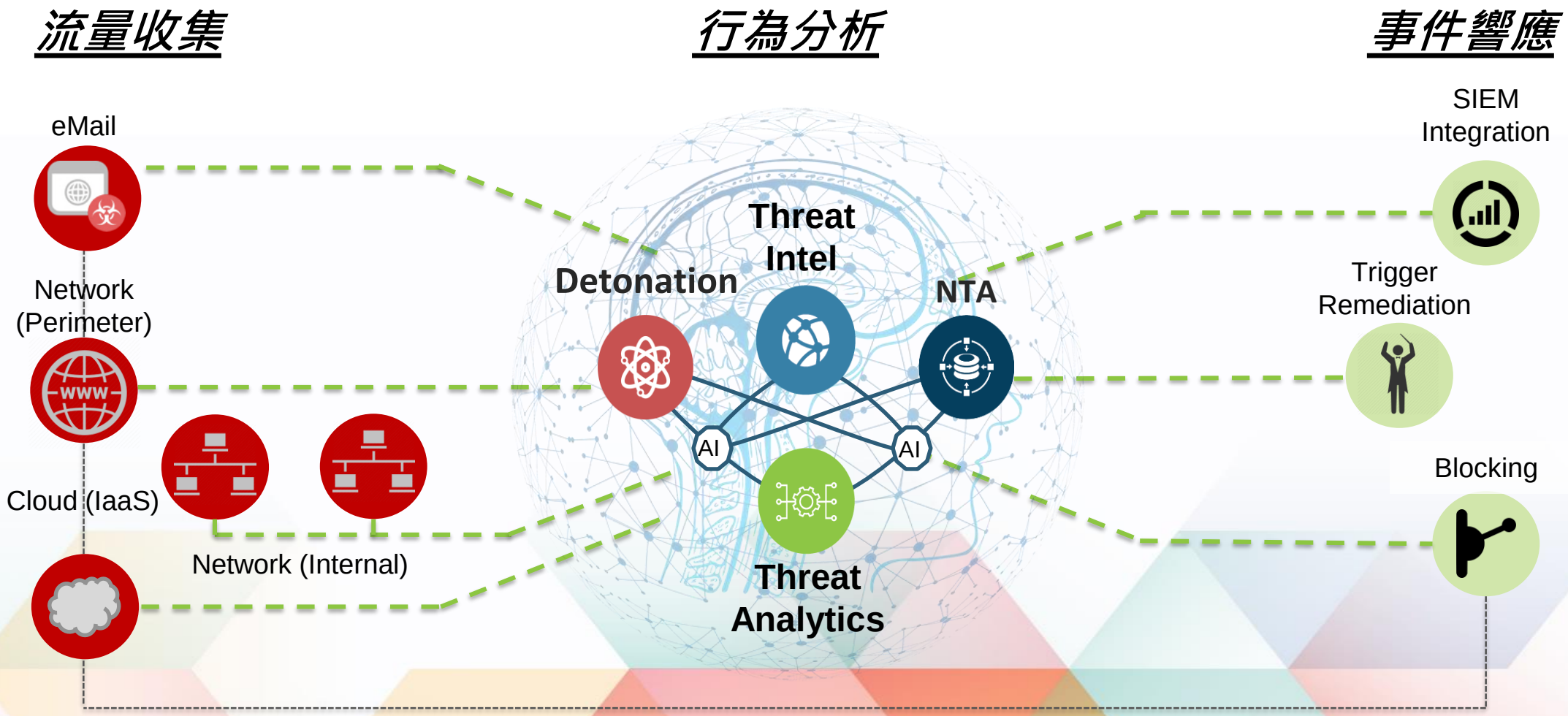


Exfiltration

從報告數據顯示，校園網路存在許多數據外洩行為與風險，當內部主機從一個或多個伺服器獲取大量數據並將大量數據發送到外部系統時，特別當此行為並不被允許時，應進行進一步檢查。

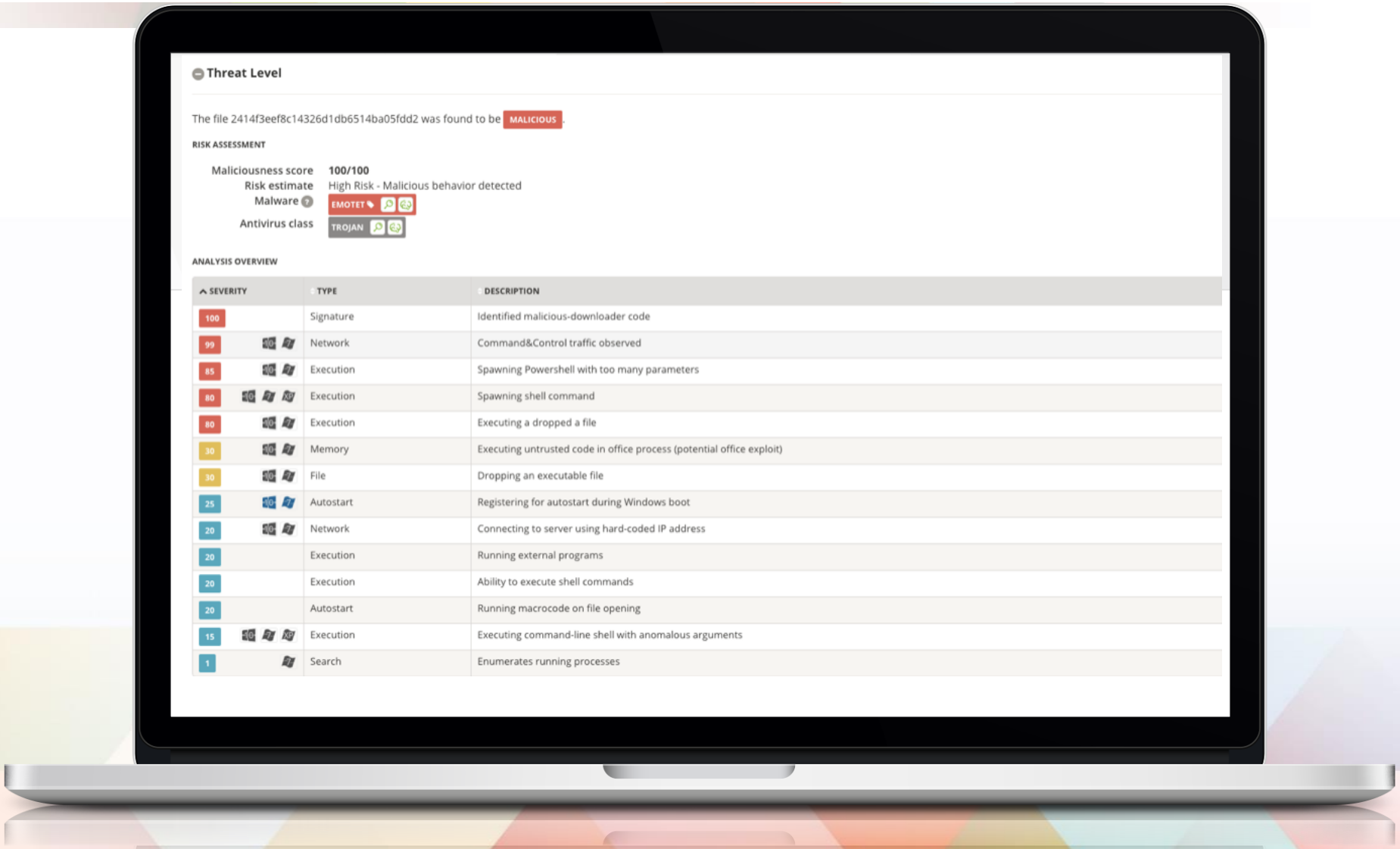


AI 迎戰 AI 實現智能化防禦部署

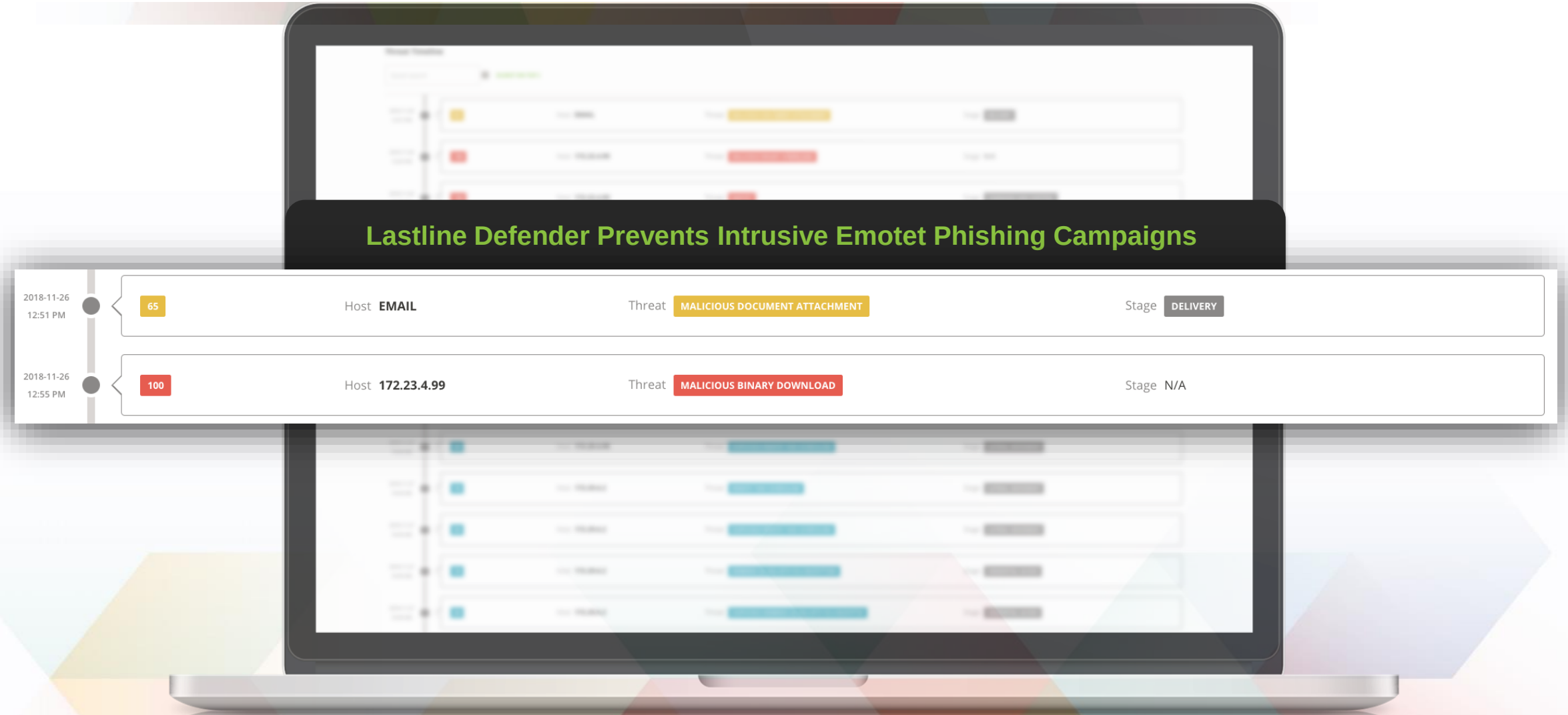


Emotet 威脅行為智能化分析 - 攻擊鍊關聯視圖

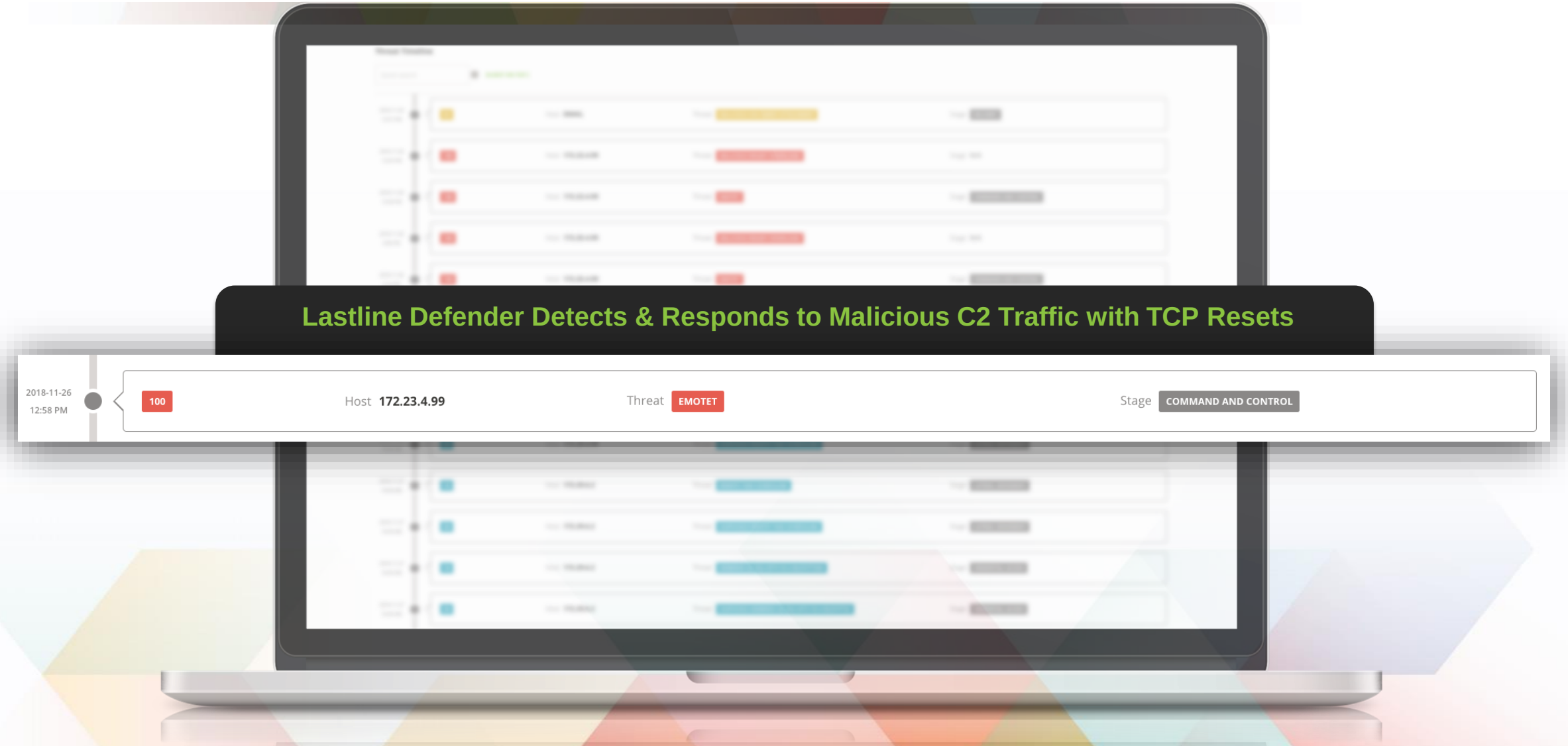
Emotet 威脅行為智能化分析 - 沙箱報告



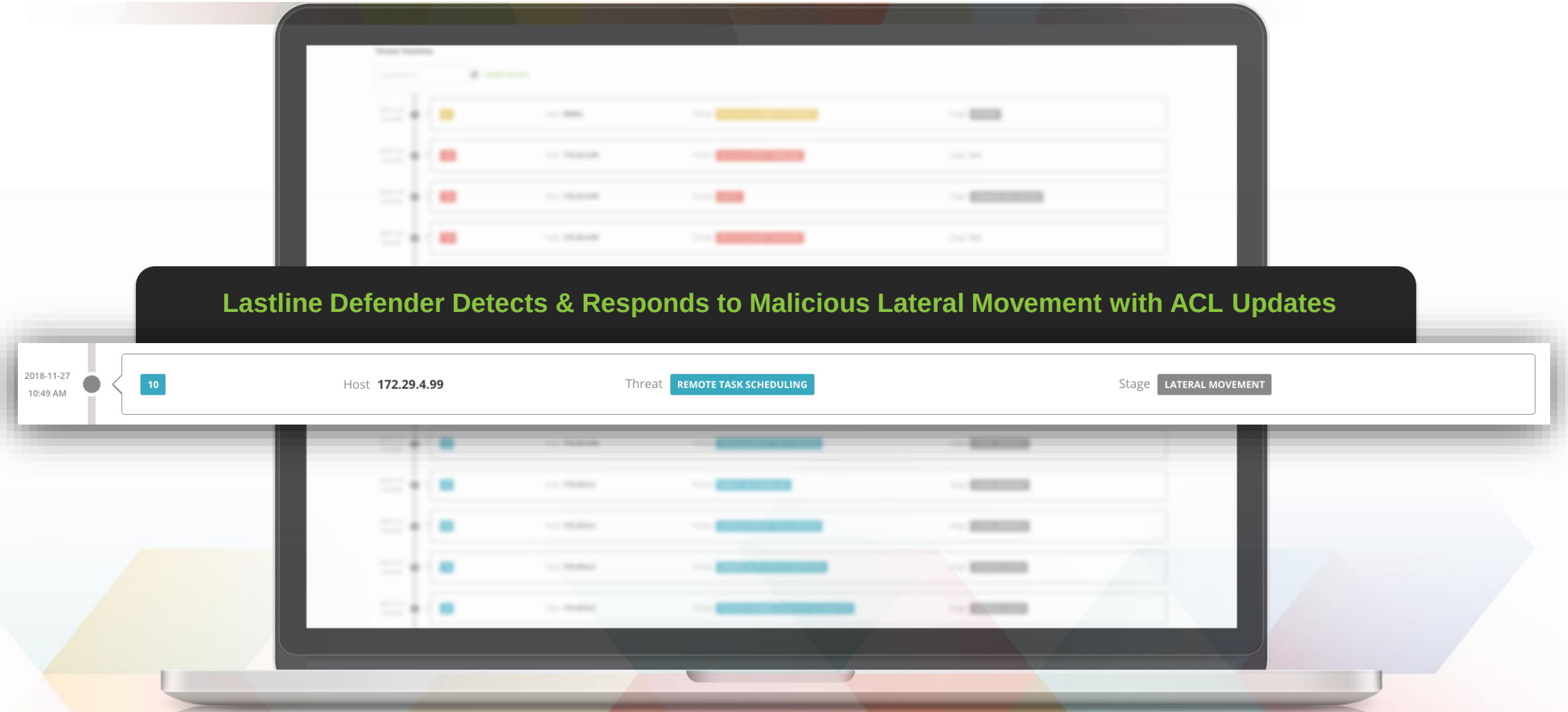
Emotet 威脅行為智能化分析 - 事件響應



Emotet 威脅行為智能化分析 - 連線阻擋



Emotet 威脅行為智能化分析 - 內網橫向移動行為檢測



03

CyberX 防禦應變通報平台，落實校園資安做好防護

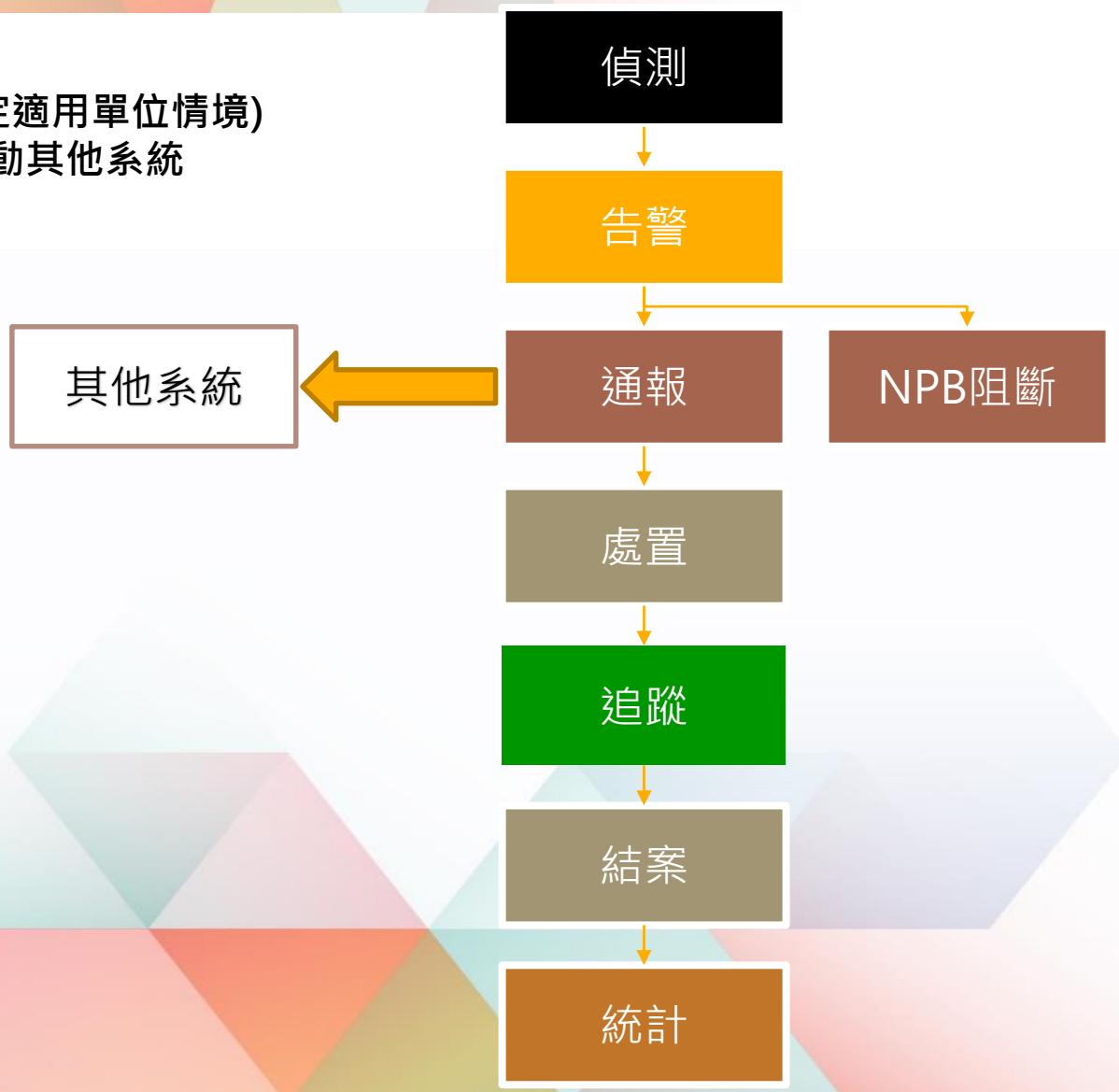
防禦關鍵策略：資安防護自動化服務

資安防禦應變通報整合平台

1. **整合平台透過API整合資安防禦設備，利用共享威脅情資機制對新型態威脅攻擊提供及早預警與防禦機制。**
2. **智能資安防禦檢測**
   導入 MITRE ATT&CK 資安框架，提供內外網網路流量智能檢測分析與惡意程式掃描檢測機制。
3. **威脅情資整合分享**
   平台蒐集IOC情資與告警資訊、過濾彙整、交換，並藉由後續加入之單位子版，將個子版間情資進行彙整、交換，達到區域威脅情資聯防分享。
4. **惡意攻擊阻斷**
   針對異常行為與惡意主機IP、惡意網域名稱或者殭屍網路(C&C)之連線執行即時比對與攔阻。
5. **事件通報應變**
   簡化資安「事件分類」應變與處理通報機制，建立自動化通報事件處理流程。

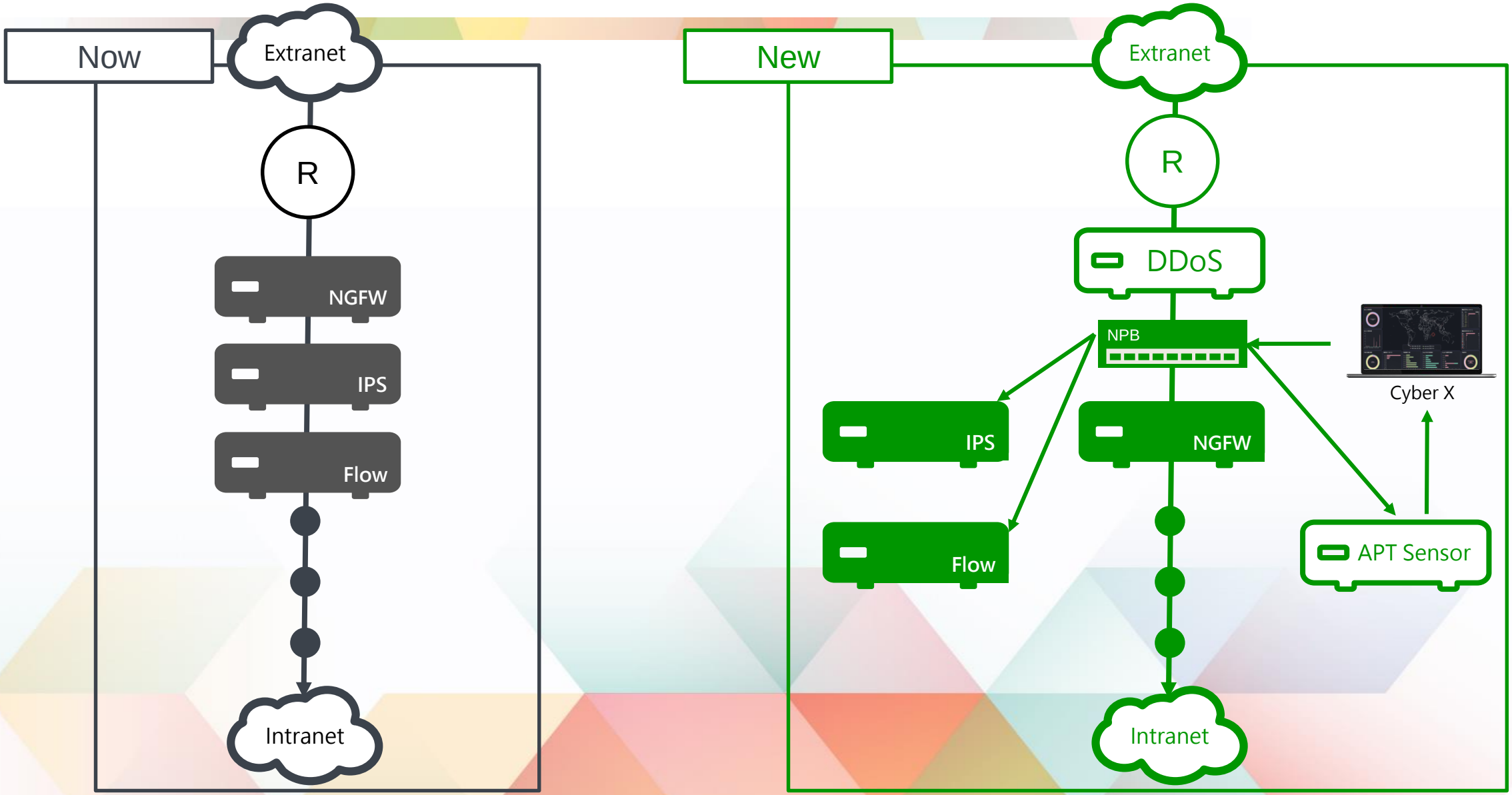
Cyber X 通報流程

- 偵測：智慧型偵測
- 告警：自訂觸發條件(各項設備告警條件不同，不一定適用單位情境)
- 通報：自訂通報機制(分層，分條件自動通報)，可連動其他系統
- 阻斷：自訂條件設定NPB自動阻斷
- 處置：派工進行內部風險確認、排除
- 追蹤：持續追蹤是否仍有風險
- 結案：該通報事項處理完成結案
- 統計：產出相關自訂告警事件報表



CyberX Live Demo

Cyber X系統架構


Now
Extranet
R
NGFW
IPS
Flow
Intranet
New
Extranet
R
DDoS
NPB
IPS
NGFW
Flow
Cyber X
APT Sensor
Intranet

即時情資


攔截惡意IP
71.6.146.130 → xxx.xxx.111.3
80.82.77.139 → xxx.xxx.42.56
185.142.236.35 → xxx.xxx.147.198
71.6.199.23 → xxx.xxx.3.124
185.142.236.34 → xxx.xxx.8.149
71.6.199.23 → xxx.xxx.119.13
71.6.146.130 → xxx.xxx.46.45
80.82.77.139 → xxx.xxx.6.85
66.240.236.119 → xxx.xxx.127.222
80.82.77.139 → xxx.xxx.44.6
172.104.242.173 → xxx.xxx.50.199
71.6.158.166 → xxx.xxx.101.169
185.142.236.34 → xxx.xxx.20.17
66.240.236.119 → xxx.xxx.128.46
71.6.199.23 → xxx.xxx.122.189
80.82.77.139 → xxx.xxx.23.159
93.174.95.106 → xxx.xxx.119.60
80.82.77.139 → xxx.xxx.107.196
66.240.236.119 → xxx.xxx.51.7
66.240.236.119 → xxx.xxx.48.42
66.240.205.34 → xxx.xxx.62.121
80.82.77.139 → xxx.xxx.137.7
71.6.199.23 → xxx.xxx.105.182
xxx.xxx.32.2 → 117.50.0.119
即時攔截惡意連線地圖
LIVE CYBER
DIGITAL
ATTACK MAP
天 禦 慧 智
攔截惡意Port TOP 10
No. Port 阻擋數(次)
Top 1 29011 4601
Top 2 23320 1866
Top 3 44183 1714
Top 4 0 1514
Top 5 24858 1403
Top 6 43664 1110
Top 7 80 724
Top 8 18438 597
Top 9 20368 371
Top 10 20012 312
攔截惡意來源 TOP 10
US 16413
NL 11121
TW 2413
CN 171
BR 89
RU 32
ES 5
FR 4
IN 3
IT 2
可疑中繼站連線
Total Attacks
high
2 (100%)
風險客戶 TOP 10
Top 1
Top 2
Top 3
Top 4
Top 5
Top 6
Top 7
Top 8
Top 9
Top 10
可疑檔案下載
10-18
10-17
10-16
10-15
10-14
10-13
10-12
0 500 1K 1.5K 2K 2.5K 3K
Email 內含可疑連結
10-18
10-17
10-16
10-15
10-14
10-13
10-12
0 300 600 900 1.2K 1.5K 1.8
Email 可疑附件檔案
10-18
10-17
10-16
10-15
10-14
10-13
10-12
0 0.5 1 1.5 2
可疑事件
Malicious Binary Download
2190 (98.56%)

全方位的統計資訊

數字科技有限公司

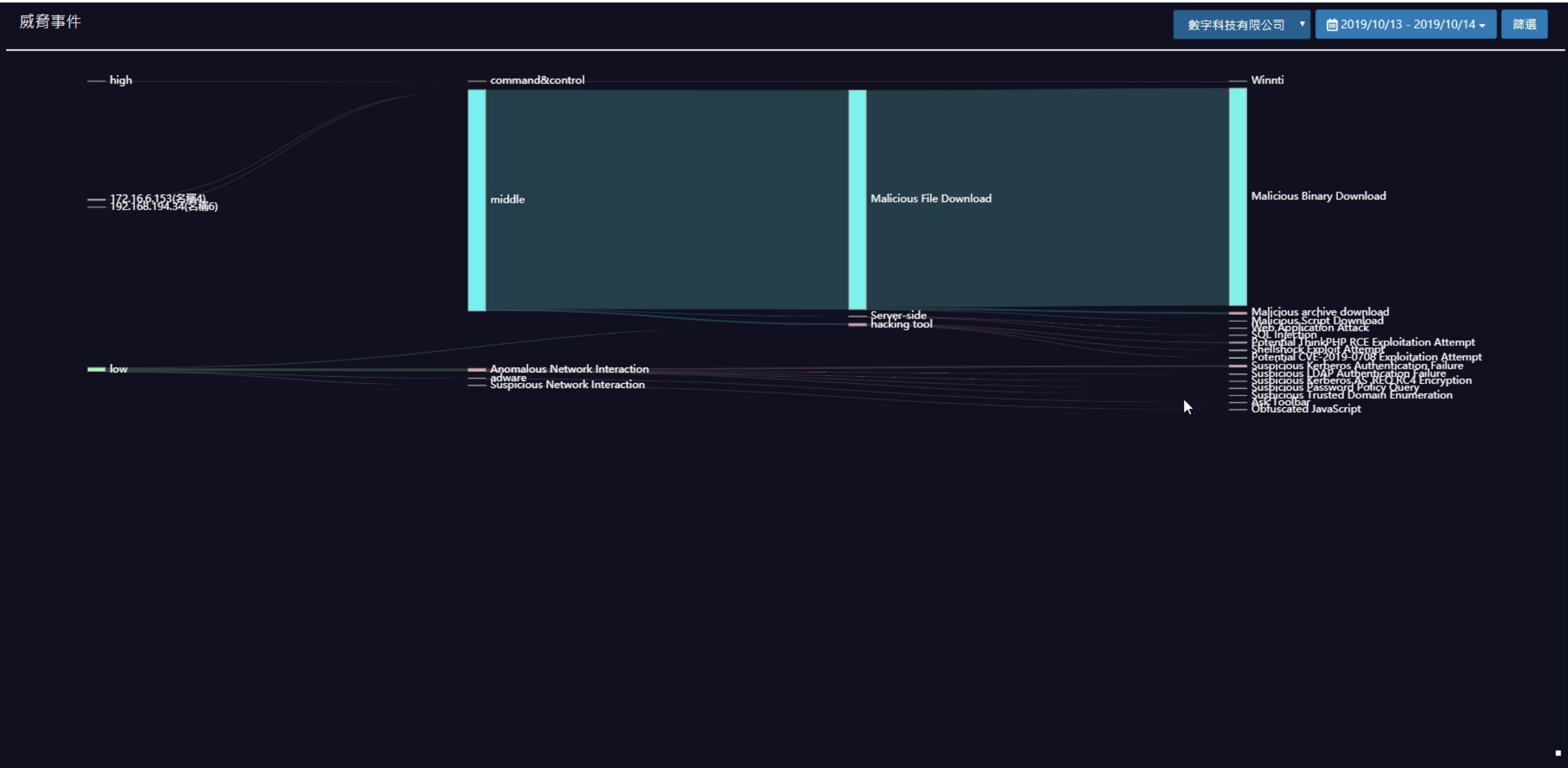
日期區間 | 篩選 | 搜尋: | 顯示 10 項結果

事件時間	寄件人	收件人	主旨	附件	URL	病毒名稱	病毒類型	影響等級
2019-10-03 10:49:21	王麦成	IR@POWERCHIP.COM	URGENT ORDER PC1907005J	2	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-03 10:49:21	王麦成	MSHSU@POWERCHIP.COM	URGENT ORDER PC1907005J	2	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 17:34:12	SALES56@SPSERVICES.CO.UK	CHINGHO@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 17:39:13	SALES56@SPSERVICES.CO.UK	GLADYSH@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 17:39:13	SALES56@SPSERVICES.CO.UK	GRACEYEH@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 17:40:13	SALES56@SPSERVICES.CO.UK	HR@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 17:55:16	SALES56@SPSERVICES.CO.UK	MSHSU@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 18:00:17	SALES56@SPSERVICES.CO.UK	SAKAMOTO@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 18:03:18	SALES56@SPSERVICES.CO.UK	SINDY@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100
2019-10-07 18:07:19	SALES56@SPSERVICES.CO.UK	WWL@POWERCHIP.COM	RE:DUE OUTSTANDING INVOICES	1	0	MALICIOUS ARCHIVE ATTACHMENT	MALICIOUS MAIL ATTACHMENT	100

顯示第 1 至 10 項結果，共 40 項

‹ 1 2 3 4 ›

全視角威脅關聯圖


威脅事件
數字科技有限公司
2019/10/13 - 2019/10/14
篩選
high
172.16.6.153(名稱4)
192.168.194.34(名稱6)
low
command&control
middle
Anomalous Network Interaction
adware
Suspicious Network Interaction
Malicious File Download
Server-side
hacking tool
Winnti
Malicious Binary Download
Malicious archive download
Malicious Script Download
Web Application Attack
SQL Injection
Potential ThinkPHP RCE Exploitation Attempt
Shellshock Exploit Attempt
Potential CVE-2019-0708 Exploitation Attempt
Suspicious Kerberos Authentication Failure
Suspicious LDAP Authentication Failure
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Password Policy Query
Suspicious Trusted Domain Enumeration
Ask Toolbar
Obfuscated JavaScript

全視角郵件關聯圖


郵件事件
數字科技有限公司
寄件者
2019/10/13 - 2019/10/14
篩選
Hi@edm.17life.com.tw
Inform_alarm@powerchip.com
info@gomaji.com
Mail Attachment

威脅事件紀錄

威脅事件

數字科技有限公司 | 2019/10/08 - 2019/10/14 | 篩選 | 匯出CSV

顯示 10 項結果　　搜尋:

事件時間	事件主機	目的IP	目的主機	威脅名稱	威脅類型	影響等級
2019-10-13 04:27:07	167.99.187.122	172.16.6.153:443	172.16.6.153	Winnti	command&control	90
2019-10-12 22:34:05	167.99.187.122	172.16.6.153:443	172.16.6.153	Winnti	command&control	90
2019-10-12 20:40:41	167.99.187.122	172.16.6.153:443	172.16.6.153	Winnti	command&control	90
2019-10-12 16:28:15	167.99.187.122	172.16.6.153:443	172.16.6.153	Winnti	command&control	90
2019-10-13 05:42:54	172.30.200.62	148.70.0.128:80	148.70.0.128	SQL Injecti...	Server-side	64
2019-10-12 19:53:32	172.16.6.156	118.126.101.81:80	118.126.101.81	SQL Injecti...	Server-side	64
2019-10-13 15:48:14	172.16.6.153	190.42.176.189:80	190.42.176.189	Potential T...	hacking tool	45
2019-10-13 11:02:44	172.16.6.153	185.128.41.50:80	185.128.41.50	Potential T...	hacking tool	45
2019-10-13 05:38:20	172.30.200.62	148.70.0.128:80	148.70.0.128	Potential T...	hacking tool	45
2019-10-13 23:41:23	e00d02m00979.twn.psc	172.16.6.48:445	172.16.6.48	Malicious ...	Malicious File Download	43

顯示第 1 至 10 項結果，共 1,000 項

‹ 1 2 3 4 5 ... 100 ›

主機威脅事件統計

主機威脅事件

數字科技有限公司 | 2019/10/08 - 2019/10/14 | 篩選 | 匯出CSV

顯示 10 項結果　　搜尋:

事件主機	事件次數	起始時間	結束時間	威脅名稱	威脅類型	影響等級
172.16.5.160	1	2019-10-11 14:41:20	2019-10-14 12:29:03	Obfuscate...	Suspicious Network Interaction	12
e00d02x04193.twn.psc	1	2019-10-11 14:41:19	2019-10-11 14:41:19	Obfuscate...	Suspicious Network Interaction	12
172.30.200.62	2	2019-10-13 05:38:20	2019-10-13 05:42:54	SQL Injecti...	Server-side	64
172.16.6.156	2	2019-10-11 21:30:03	2019-10-12 19:53:32	SQL Injecti...	Server-side	64
172.16.5.160	2	2019-10-09 10:49:27	2019-10-09 10:49:57	Phishing	phishing	25
e00d02x05126.twn.psc	1	2019-10-09 10:49:27	2019-10-09 10:49:27	Phishing	phishing	25
p1dc02.twn.psc	1	2019-10-09 03:21:18	2019-10-09 03:21:22	Phishing: ...	phishing	20
e00d02m00955.twn.psc	2	2019-10-13 23:25:38	2019-10-14 08:02:59	Malicious ...	Malicious File Download	43
172.26.129.11	2	2019-10-13 22:08:03	2019-10-13 22:08:39	Malicious ...	Malicious File Download	43
e00n02m00241.twn.psc	3	2019-10-13 21:55:30	2019-10-13 21:55:47	Malicious ...	Malicious File Download	43

顯示第 1 至 10 項結果，共 1,000 項

‹ 1 2 3 4 5 ... 100 ›

自訂義告警

告警設定

新增

顯示 10 項結果

搜尋:

事件主旨	告警範圍	告警種類	累計時間(min)	事件類型	風險等級	觸發值	啟用告警	編輯	刪除
APT發現高風險超過10次	All	APT	120	All	high	10	false		
DDoS累計阻斷封包次數超過200次	數字科技有限公司	DDoS Type (Packets Dropped)	5	All		200	false		
DDoS累計阻斷封包超過2%	All	DDoS Flow (Packets)	10	Inbound		2	false		
DDoS累計阻斷流量超過10MB	All	DDoS Type (MB Dropped)	20	All		10	true		
DDoS累計阻斷流量超過2%	All	DDoS Flow (Bytes)	10	Inbound		2	false		
Test-1	數字科技有限公司	APT	15	command%26control	medium	2	false		
Test2	數字科技有限公司	DDoS Type (MB Dropped)	10	ATLAS Threat Categories		2	true		
阻斷惡意連線超過100次	All	Block	10	Inbound		100	false		

顯示第 1 至 8 項結果，共 8 項

‹ 1 ›

自訂義阻斷

阻斷設定

新增

顯示 10 項結果

搜尋:

事件主旨	阻斷類型	設定值	啟用阻斷	編輯	刪除
IP阻擋1	IP阻斷	192.168.0.2	true		
IP阻擋2	IP阻斷	192.168.0.1	true		
阻斷IP3	IP阻斷	192.168.0.3	false		
阻斷事件2	事件阻斷	Crypto Jacking (All)	true		
阻斷事件3	事件阻斷	Security Software (SonicWall)	true		
阻斷事件4	事件阻斷	unknown (unknown - HTTP)	false		

顯示第 1 至 6 項結果，共 6 項

‹ 1 ›

多樣來源整合-防火牆設備安全

設備安全指數	設備複雜度	導致嚴重控制失敗的規則	請選擇設備
3.01	54.7%	18	請選擇...

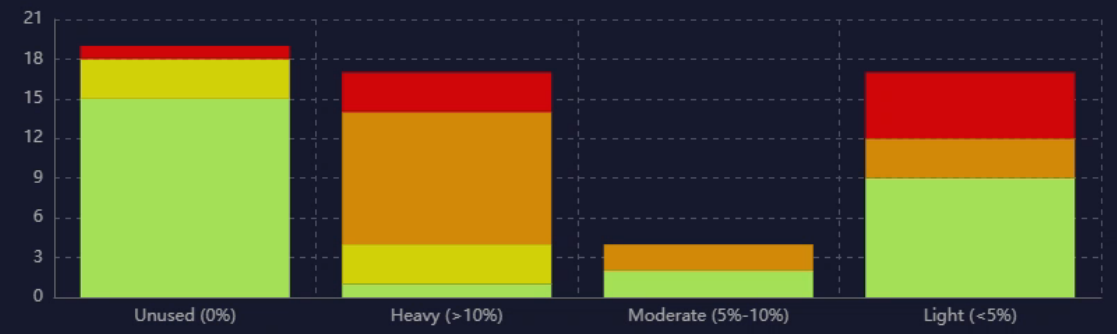
最嚴重的控制失敗 Top10

Severity	Control Code	Control Name	Failed Rules
3	AU-00006	Rules without Owner or Busi...	37
3	AU-00007	Rules without Comments	33
5	AU-00018	Expired rules	31
7	SC-00031	TCP High Ports with Action o...	27
6	RA-00002	Unused Rules - 90 Days (Rul...	24
4	RA-00001	Unused Rules - 30 Days (Rul...	24
7	RA-00003	Unused Rules - 180 Days	20

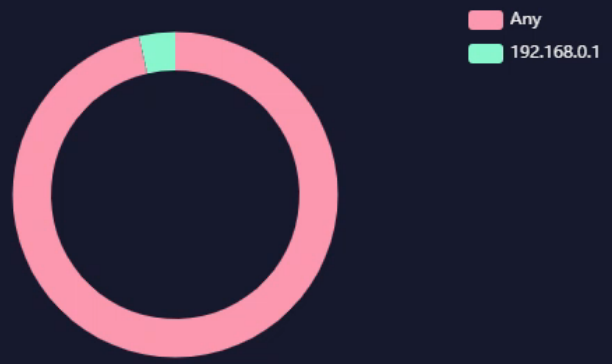
TCP High Ports with Action of Accept

規則使用程度&累積嚴重性

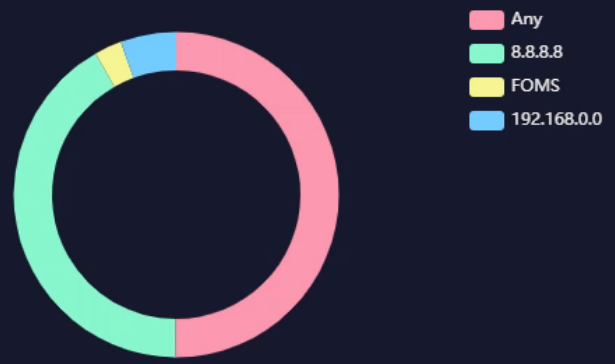
健康度： Critical



連接來源紀錄



連接目標紀錄



多樣來源整合-教室資源使用

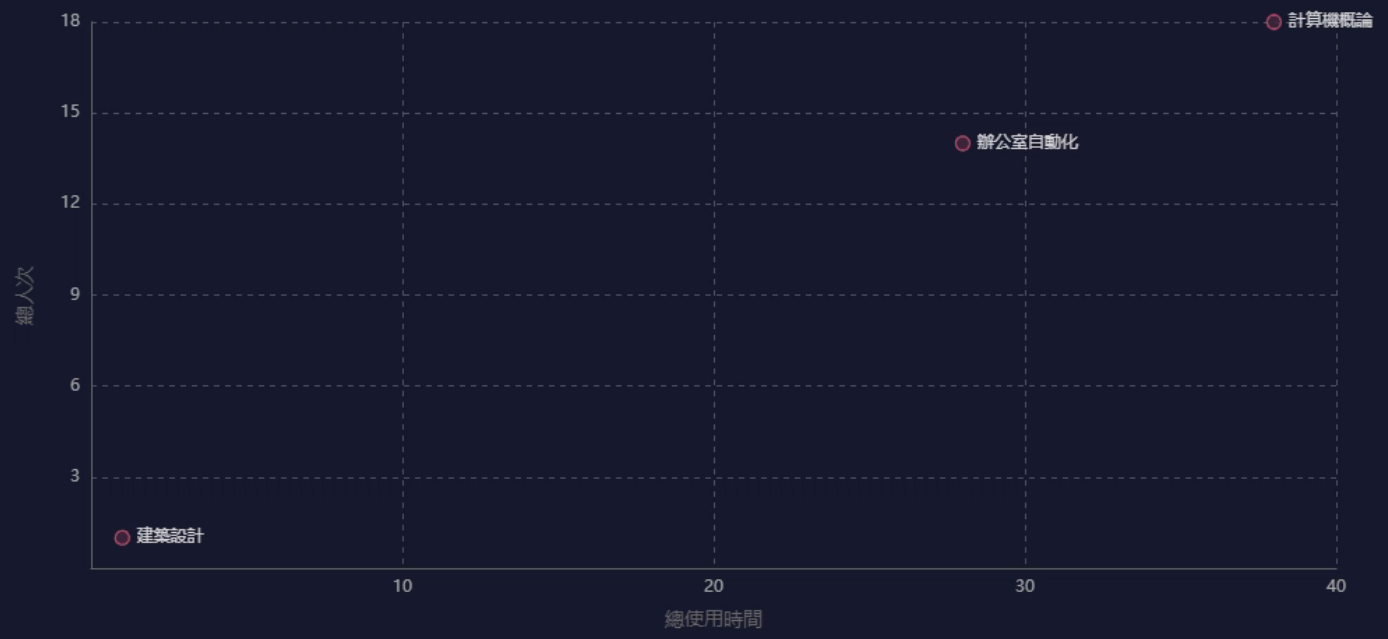
統計各科目使用Lab教室/服務的次數與時間

統計各單位使用Lab教室/服務的次數與時間

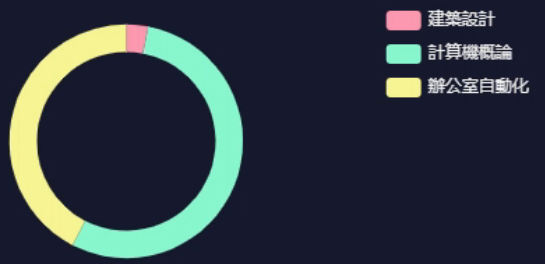
統計各Lab教室/服務使用的次數與時間

各科目使用分析

目前顯示 108 上 學期



各科目總使用人次分析



各科目總使用時間分析

Cyber X給學校的好處-法規面

資安法-大項	資安法-次項	A級辦理次數	B級辦理次數	C級辦理次數	天御平台整合服務方案說明(修改)
安全性檢測	網站安全弱點檢測	每年2次	每年1次	每2年1次	可搭配提供核心系統弱點檢測與報告分析
資通安全健診	網路架構檢視	每年1次	每2年1次	每2年1次	
	網路惡意活動檢視	每年1次	每2年1次	每2年1次	7x24網路流量與行為分析
	使用者電腦惡意活動檢視	每年1次	每2年1次	每2年1次	7x24網路流量與行為分析
	伺服器惡意活動檢視	每年1次	每2年1次	每2年1次	7x24網路流量與行為分析
	目錄伺服器設定	每年1次	每2年1次	每2年1次	
	防火牆設定檢視	每年1次	每2年1次	每2年1次	
資通安全監控管理機制					提供7x24x365自動化安全監控管理機制，如有異常攻擊將會警示，有專責人員處理
資通安全防護	防毒軟體	V	V	V	可搭配提供端點偵測及回應整合服務
	網路防火牆	V	V	V	可提供簡易管制
	郵件過濾	V	V	V	提供APT+Email防護機制
	入侵偵測與防禦機制	V	V		提供偵測與防禦機制
	進階持續性威脅防禦措施	V			提供APT攻擊防禦機制
黑名單情資同步					如TACERT有自動化機制與提供黑名單配合辦理整合
資安事件自動通報					如SOC有自動化機制與提供黑名單，配合辦理整合

Cyber X給學校的好處-管理面與執行面

- 管理面
  - 校際資安情資分享
  - 整合不同資安產品做聯防
  - 季報呈現校內每季的資安事件的現況並提供資安顧問建議
  - 不用投資人力在資安產品的學習上,人力可作更有效率的應用,做更有價值的工作
- 執行面
  - Cyber X 平臺整合不同資安系統，提高監控可視性。
  - 節省對不同資安產品的學習人力
  - Cyber X SOC 服務能 7x24 小時不間斷的對校內網路環境進行監控，並能針對惡意之 IP 進行阻斷。
  - 本案服務內容提供 5x8資安人力顧問，協助校方進行資安事件調查服務。
  - Cyber X服務除系統示警外,還有人力通知,顧問分析並回報建議處置方式,協助調整,讓校內資安防護化被動為主動
  - Cyber X彈性自訂各資安產品的資安事件示警,能符合學校資安防護所需
  - 每季提供資安報告，讓使用單位了解校內發生資安狀況。並針對各種新式的資安事件做防護


Q & A