Cyber X 資安防禦平台

Efficient professional after-sales service

High-quality and rapid Security solution

後資安防駭時期
Cyber X can Help!

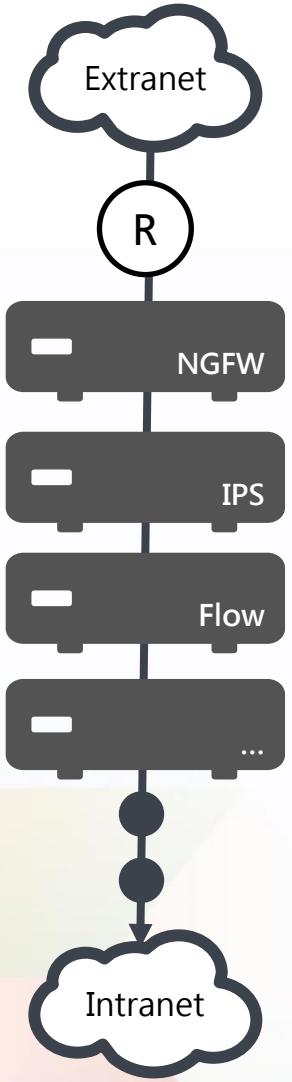
天禦慧智 Cyber X

Agenda

- Cyber X 產品差異
- Cyber X 功能介紹
- Ways To Help !
- Cyber X 方案
- Cyber X 整合中
- Cyber X 未來願景

Cyber X 產品差異

由傳統方式進化為提供集中的資安狀態呈現



- 分散的產品介面✗
- 不同的安全敏感度✗
- 分散各處的攔截與告警✗
- 分散各處的事件✗
- 同一事件各自告警✗
- 人工確認威脅✗

Cyber X 資安防禦服務平台

內部告警
情資

外部威脅
情資

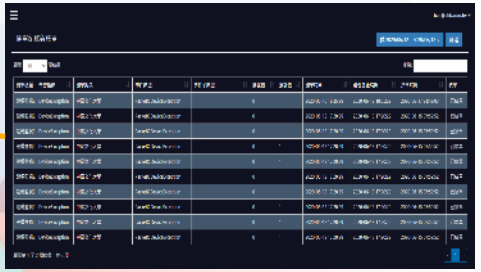
- 已知C2 URL
- 已知惡意IP
- 已知MD5

整合

分析去重複

攔截

告警



開單

SIEM、SOC、MSS？

什麼是SIEM(安全信息和事件管理)

- SIEM是軟體和服務的組合，是SIM（安全信息管理）和SEM（安全事件管理）的融合體。
- SIEM側重於日誌的集中式管理和審計，為來自企業和組織中所有IT資源（包括網絡、系統和應用）產生的安全信息（包括日誌、告警等）進行統一的實時監控、歷史分析。

什麼是SOC(安全運營中心)

- SOC是以資產為核心，以安全事件管理為關鍵流程，採用安全域劃分的思想，建立一套即時的資產風險模型，協助管理者進行事件及風險分析、預警管理、危機處理的集中安全管理系統。
- SOC是一個複雜的系統，它既有產品，又有服務，還有運維，SOC是技術、流程和人的結合。

什麼是MSS(可管理安全服務)

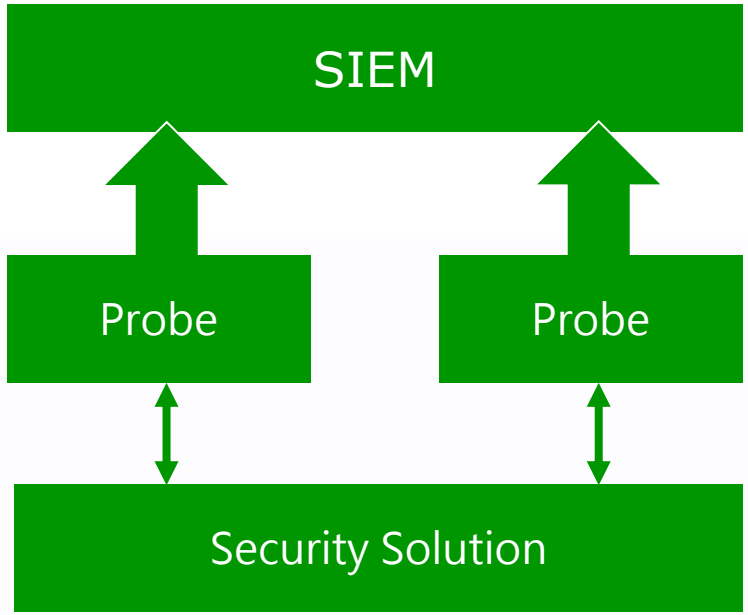
- MSS是由專業的MSSP（可管理安全服務提供商）提供的安全運維外包服務。
- MSS可為客戶帶來的效益
    1. 降低成本：人員配置、技能要求、場地需求。
    2. 全天候監控：7×24的監控服務。
    3. 風險監控：有效監控安全風險，第一時間提供解決方案。
    4. 發現和解決問題：及時發現和解決可能存在的安全問題。
    5. 趨勢分析：專業的安全趨勢分析，月、季、年安全分析報告。
    6. 日誌存儲和查詢：日誌有效存儲和備份、快速查詢定位。

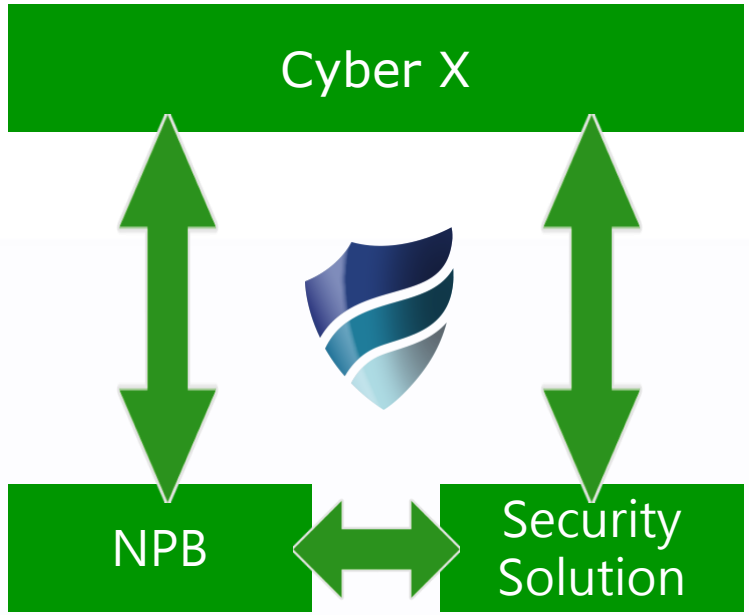
SIEM、SOC+MSS的區別

對於兩者之間的主要區別，SIEM只做到了傳統的安全日誌數量統計，SOC+MSS則是對安全日誌重定義並生成新的安全事件，實現對安全日誌的整併、過濾與威脅分級，將安全警報量化。

例如，A公司受到駭客的DDoS攻擊，15分鐘內收到了20W條相關的安全日誌。SIEM提供給客戶的警報為20W條，而SOC提供給客戶的警報為1條，顯然在安全風險管理的角度上來看，SIEM的計數方式是不科學的。

Cyber X 與其他產品的差異



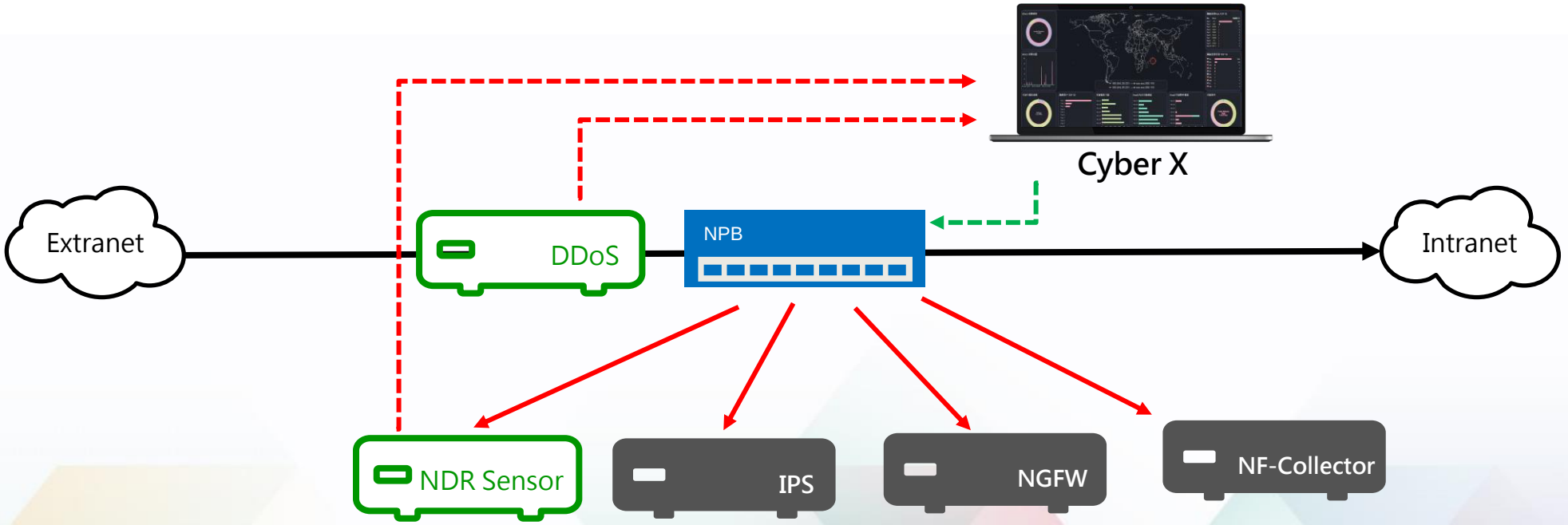


- 耗費資源
- 依賴人員分析
- 手動威脅 / 事件回報
- 額外建置成本

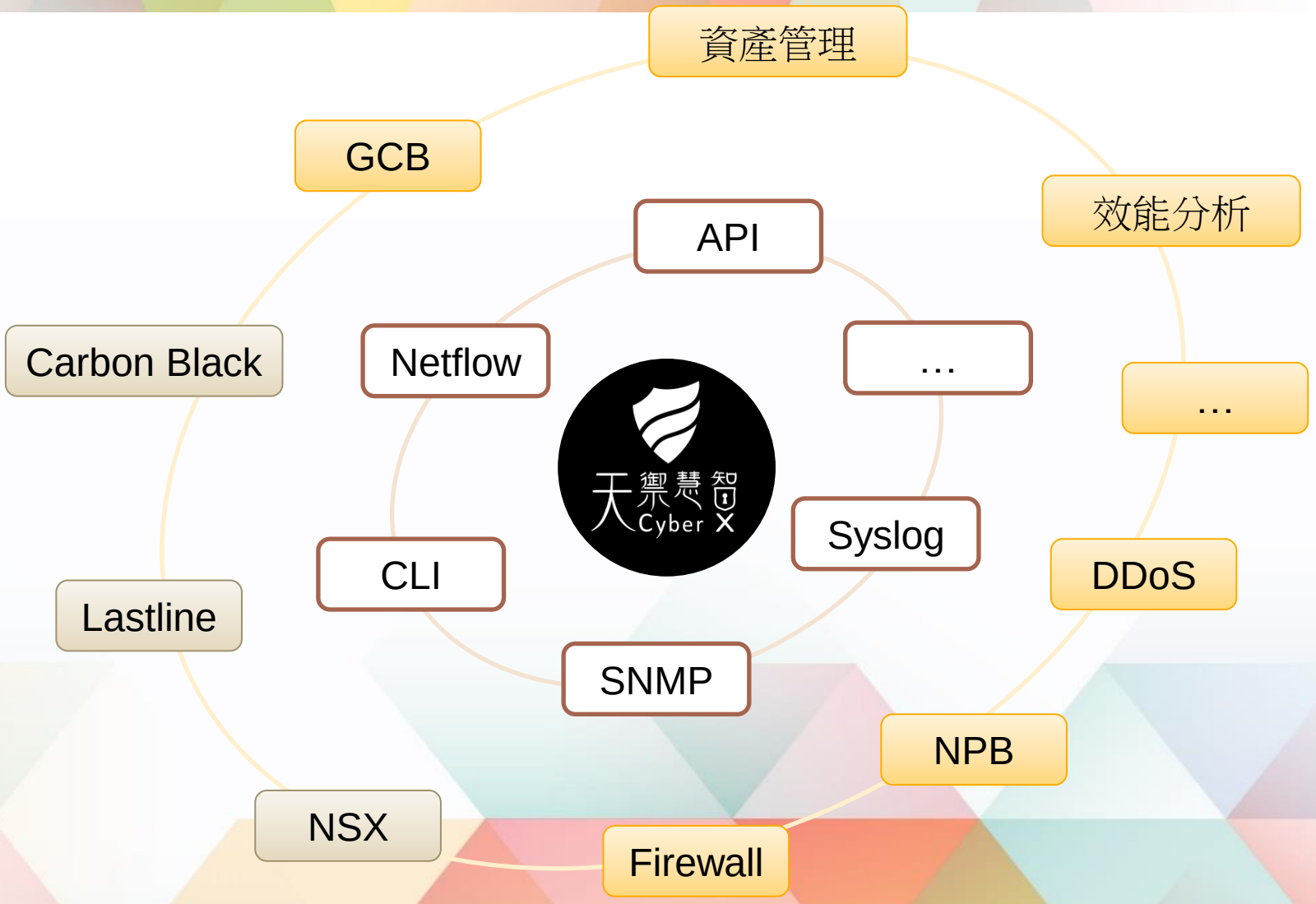
- 智慧型系統
- 自動化關聯
- 更快的決策訂立
- 加速發現威脅情資
- 自動化事件回報
- 簡單整合式管理

Cyber X 功能介紹

Cyber X架構圖


Cyber X
Extranet
DDoS
NPB
Intranet
NDR Sensor
IPS
NGFW
NF-Collector

Cyber X 平台


資產管理
GCB
效能分析
API
Carbon Black
Netflow
…
…
天禦慧智 Cyber X
Syslog
CLI
DDoS
Lastline
SNMP
NPB
NSX
Firewall

Cyber X 帶來的便利性

- 包含軟體、硬體、維護，節省其他支出。
- 多來源IOC情資分享。
- 多樣設備整合，單一介面搜尋查看多種設備資訊。
- 整合介面中文化，並提供多國語系。
- 平台呈現重點資訊，沒有複雜難懂的資料。
- 可客製化的資安日/周/月/季報表。
- 可客製化的系統擴充、其他系統介接。

Cyber X 功能特色

- AI分析與沙箱模擬檢測。
- 自定義的告警，不受限設備告警條件。
- 自定義的攔截，不受限設備攔截條件。
- 集中定義的攔截清單。
- 自動化的情資統合、去重複。
- 可依設備/單位，分組定義多條件分流、攔截觸發規則。
- 可分別定義內對外、外對內規則清單。
- 可對IP、Domain、Port、Application...各類條件定義規則清單。

防禦關鍵策略：資安防護自動化服務

1

資安防禦應變通報整合平台

- 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。

資安防禦應變通報整合平台

防禦關鍵策略：資安防護自動化服務

1

資安防禦應變通報整合平台

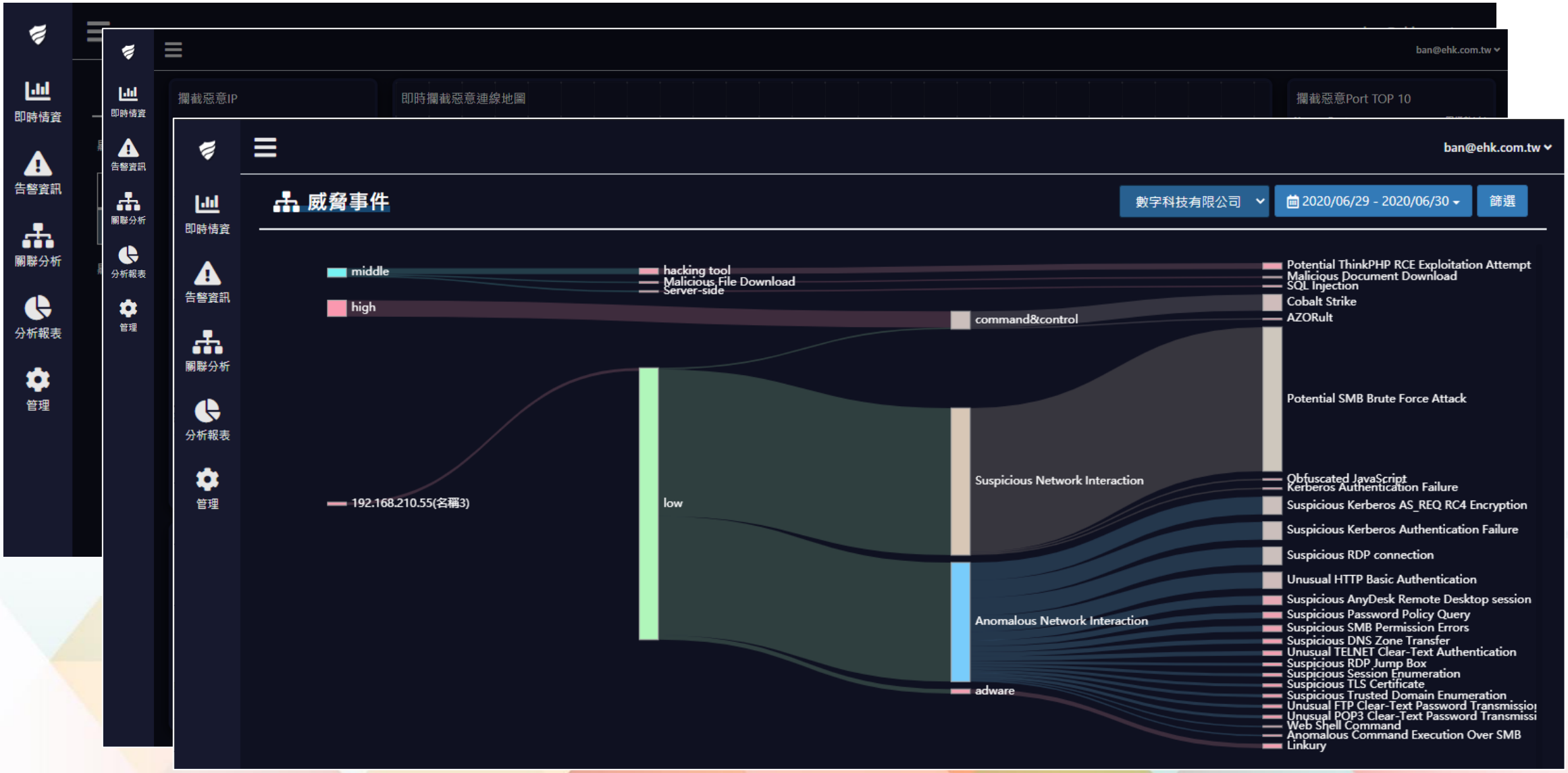
- 整合平台透過API整合資安防禦設備，利用共享威脅情資機制對新型態威脅攻擊提供及早預警與防禦機制。

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。

智能資安防禦檢測


即時情資
告警資訊
關聯分析
分析報表
管理
ban@ehk.com.tw
攔截惡意IP
即時攔截惡意連線地圖
攔截惡意Port TOP 10
威脅事件
數字科技有限公司
2020/06/29 - 2020/06/30
篩選
middle
high
192.168.210.55(名稱3)
hacking tool
Malicious File Download
Server-side
low
command&control
Suspicious Network Interaction
Anomalous Network Interaction
adware
Potential ThinkPHP RCE Exploitation Attempt
Malicious Document Download
SQL Injection
Cobalt Strike
AZORult
Potential SMB Brute Force Attack
Obfuscated JavaScript
Kerberos Authentication Failure
Suspicious Kerberos AS_REQ RC4 Encryption
Suspicious Kerberos Authentication Failure
Suspicious RDP connection
Unusual HTTP Basic Authentication
Suspicious AnyDesk Remote Desktop session
Suspicious Password Policy Query
Suspicious SMB Permission Errors
Suspicious DNS Zone Transfer
Unusual TELNET Clear-Text Authentication
Suspicious RDP Jump Box
Suspicious Session Enumeration
Suspicious TLS Certificate
Suspicious Trusted Domain Enumeration
Unusual FTP Clear-Text Password Transmissio
Unusual POP3 Clear-Text Password Transmissi
Web Shell Command
Anomalous Command Execution Over SMB
Linkury

防禦關鍵策略：資安防護自動化服務

1

資安防禦應變通報整合平台

- 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，藉由後續加入之子版，將各子版間情資進行彙整交換，達到威脅情資聯防分享。

威脅情資整合分享

阻擋清單

顯示 10 項結果　　搜尋:

情資來源	攔截描述	攔截起始時間	攔截結束時間
Custom Lastline Event	Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=6,confidence>=30	2020-04-03 05:59:29	2020-04-17 05:59:29
Custom Lastline Event	Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=6,confidence>=30	2020-03-17 17:00:59	2020-03-31 17:00:59

顯示第 1 至 2 項結果，共 2 項　　‹ 1 ›

攔截清單

顯示 10 項結果　　搜尋:

發生時間	來源IP	來源PORT	來源國家	目的IP	目的PORT	目的國家	來源方向
2020-04-07 10:20:14	51.68.32.21	35341	FR	140.137.17.233	23	TW	外 → 內
2020-04-07 10:20:13	51.68.32.21	10467	FR	140.137.43.63	23	TW	外 → 內
2020-04-07 10:20:13	51.68.32.21	35341	FR	140.137.126.181	23	TW	外 → 內
2020-04-07 10:20:12	51.68.32.21	42316	FR	140.137.51.43	23	TW	外 → 內
2020-04-07 10:20:12	51.68.32.21	35341	FR	140.137.16.146	23	TW	外 → 內
2020-04-07 10:20:12	51.68.32.21	26409	FR	140.137.36.235	23	TW	外 → 內
2020-04-07 10:20:11	51.68.32.21	45148	FR	140.137.111.44	23	TW	外 → 內
2020-04-07 10:20:11	51.68.32.21	33412	FR	140.137.61.128	23	TW	外 → 內
2020-04-07 10:20:11	51.68.32.21	55291	FR	140.137.106.251	23	TW	外 → 內
2020-04-07 10:20:11	51.68.32.21	45148	FR	140.137.8.240	23	TW	外 → 內

顯示第 1 至 10 項結果，共 50 項　　‹ 1 2 3 4 5 ›

防禦關鍵策略：資安防護自動化服務

1. **資安防禦應變通報整合平台**
   - 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，藉由後續加入之子版，將各子版間情資進行彙整交換，達到威脅情資聯防分享。
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。

惡意攻擊阻斷


編輯
ban@ehk.com.tw
攔截惡意IP
2020/04/01 - 2020/04/07
篩選
匯出CSV
顯示 10 項結果
搜尋:
發生時間 | 外部IP | 發生次數 | 來源方向 | 攔截描述 | 情資來源
2020-04-07 10:25:00 | 58.227.54.120 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,confidence>=30 | Custom Lastline Event
2020-04-07 10:25:00 | 59.127.69.82 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=13,confidence>=3 | Custom Lastline Event
2020-04-07 10:25:00 | 59.127.89.148 | 2 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,confidence>=30 | Custom Lastline Event
2020-04-07 10:25:00 | 220.135.246.63 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=10,confidence>=3 | Custom Lastline Event
2020-04-07 10:25:00 | 24.170.52.108 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=10,confidence>=3 | Custom Lastline Event
2020-04-07 10:25:00 | 41.204.5.97 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=17,confidence>=3 | Custom Lastline Event
2020-04-07 10:25:00 | 189.1.163.207 | 1 | 外 → 內 | Black IP List | Cyber X IOC
2020-04-07 10:25:00 | 94.201.112.59 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=6,confidence>=30 | Custom Lastline Event
2020-04-07 10:25:00 | 188.230.121.115 | 1 | 外 → 內 | Mirai Login Attempt 阻斷,threat_class=Suspicious Network Interaction,threat=Mirai Login Attempt,impact>=6,confidence>=30 | Custom Lastline Event
2020-04-07 10:25:00 | 188.230.121.115 | 1 | 外 → 內 | threat_class=Suspicious Network Interaction,threat=Mirai Variant,confidence>=90 | Lastline Event
顯示第 1,441 至 1,450 項結果，共 1,664 項
‹ 1 ... 144 145 146 ... 167 ›

防禦關鍵策略：資安防護自動化服務

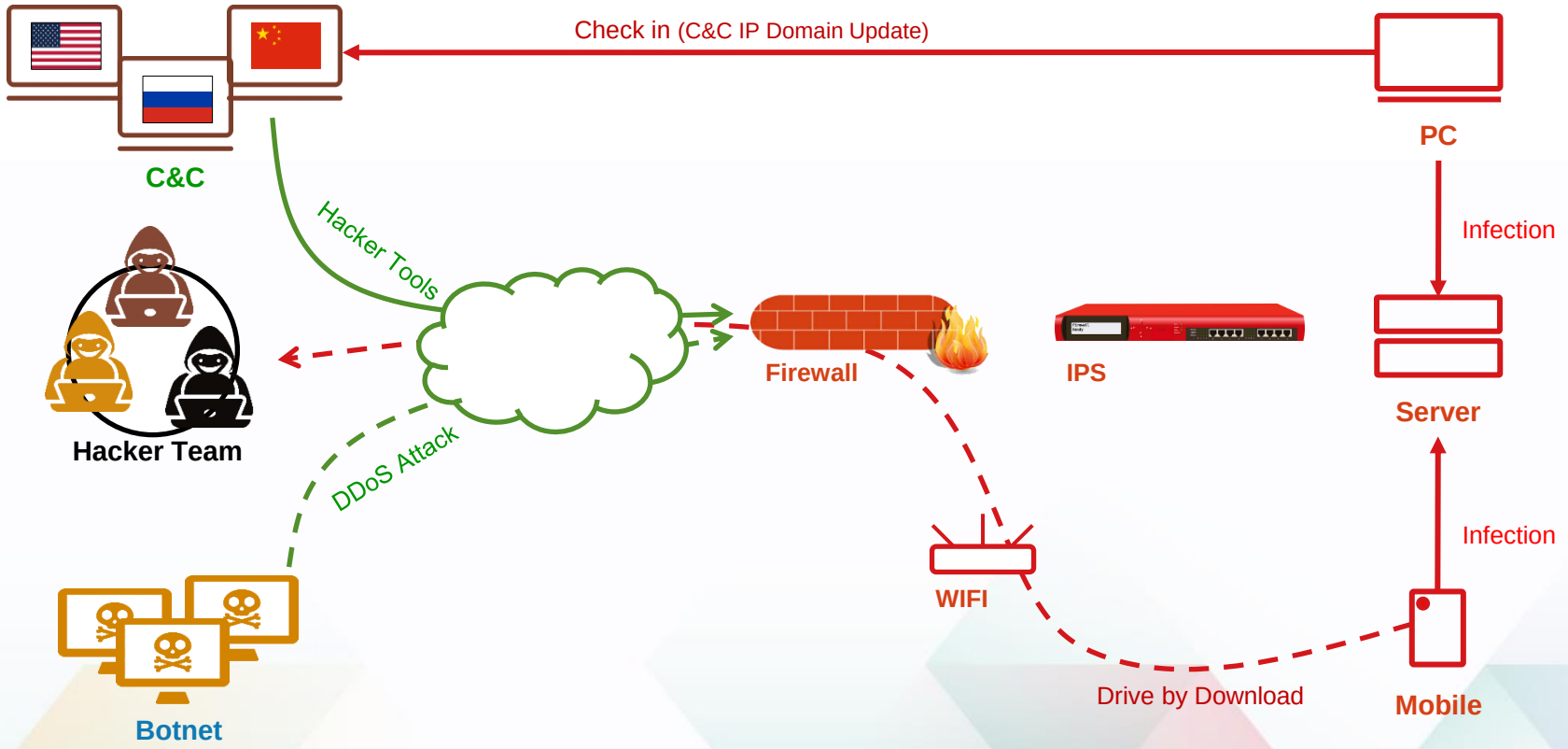
1. **資安防禦應變通報整合平台**
   - 整合平台透過API整合資安防禦設備，利用共享威脅情資機制對新型態威脅攻擊提供及早預警與防禦機制。
2. **智能資安防禦檢測**
   - 導入 MITRE ATT&CK 資安框架，提供內外網網路流量智能檢測分析與惡意程式掃描檢測機制。
3. **威脅情資整合分享**
   - 平台蒐集IOC情資與告警資訊、過濾彙整，藉由後續加入之子版，將各子版間情資進行彙整交換，達到威脅情資聯防分享。
4. **惡意攻擊阻斷**
   - 針對異常行為與惡意主機IP、惡意網域名稱或者殭屍網路(C&C)之連線執行即時比對與攔阻。
5. **事件通報應變**
   - 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。

事件通報應變


新增
編輯
事件主旨 *
設備健康狀態監視
告警範圍 *
全部
告警種類 *
DeviceException
裝置 *
Lastline
開單處理天數 *
3
告警開單管理者Email *
測試
告警開單處理人Email *
測試
啟用告警
啟用開單
儲存
取消
告警設定
即時情資
告警資訊
關聯分析
分析報表
管理
ban@ehk.com.tw
事件主旨
Test
測試2
設備監視1
設備監視2
啟用告警
啟用開單
編輯
刪除

Ways To Help !

APT 攻擊手法



受攻擊面越來越多

- 端點 → 閘道
- 實體 → 虛擬
- 跨平台系統

威脅更複雜

- 混合式攻擊
- 攻擊比防禦更有組織及協調性

混合式攻擊 (Hybrid Attack)

自由時報 Liberty Times Net

即時 政治 社會 生活 國際 地方 人物 蒐奇 影音 財經 娛樂 汽車
時尚 體育 3C 評論 玩咖 食譜 健康 地產 專區 TAIPEI TIMES

IG、Facebook等社群大當機！ 傳遭針對性大規模DDoS攻擊

〔即時新聞／綜合報導〕3日晚間10時左右，陸續有網友發現Instagram（IG）、Facebook的圖片傳送出現異常。不少網友在社群回報，雖然可以傳送圖片，不過對方卻收不到訊息。目前網友回報到大規

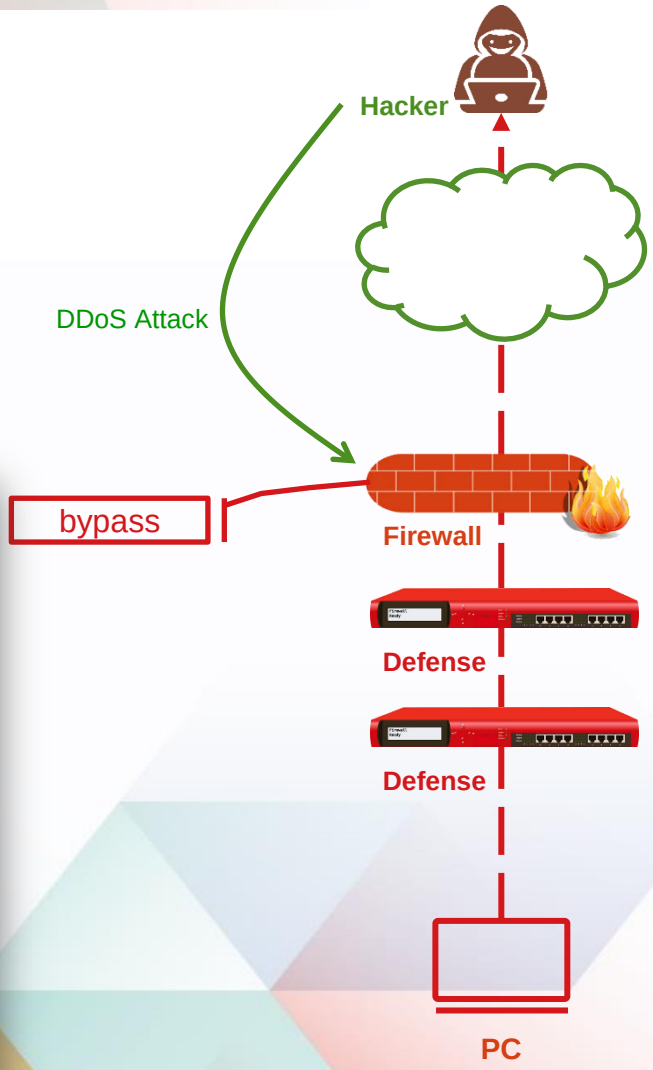
根據彭
WhatsA
「down

iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 社

企業最害怕的APT攻擊，韓國是最明顯的例子，臺灣也有很多實際案例，就是看起來像是遭DDoS攻擊，但進一步協助事件處理時會發現，駭客真實目的就是APT。

因此，他提醒，當企業遭到DDoS攻擊同時，也得留意其他資安警告，如入侵防禦設備告警、APT偵測到有異常事件發生等。他建議，企業此時最好有一個可針對各種警告做蒐集分析的SOC（資安維運中心），且將這些異常進行事件的關聯性分析後，比較可找到駭客攻擊和企業受害的脈絡。

金融業DDoS防護工作時，觀察到一特殊DDoS現象，有時駭客只攻擊1小時後便收手，但此「短暫」DDoS攻擊後，網路閘道端設備如IPS，因無法承受大量DDoS攻擊，會自動切換成關閉防護功能的Bypass模式，來確保經過設備的網路還可暢通，而駭客能藉機繞過IPS，送入惡意木馬等。



進階規避式技術 (AET, Advanced Evasion Technique)

Call Home:

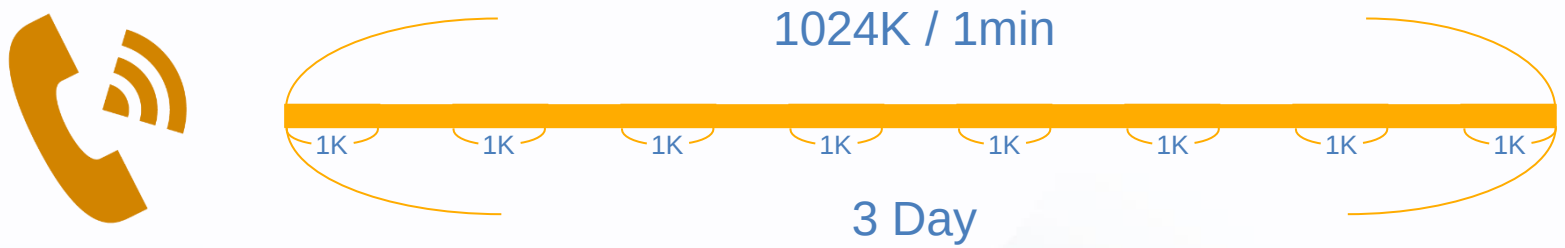
https://www.microsoft.com/abc.exe

https://www.dropbox.com/abc.exe

https://bbm2016.net/public/infected.exe

https://skydrive.com/aabbcc

https://xxxxxx.google.com/aabbcc



進階規避式技術-無檔案攻擊手法

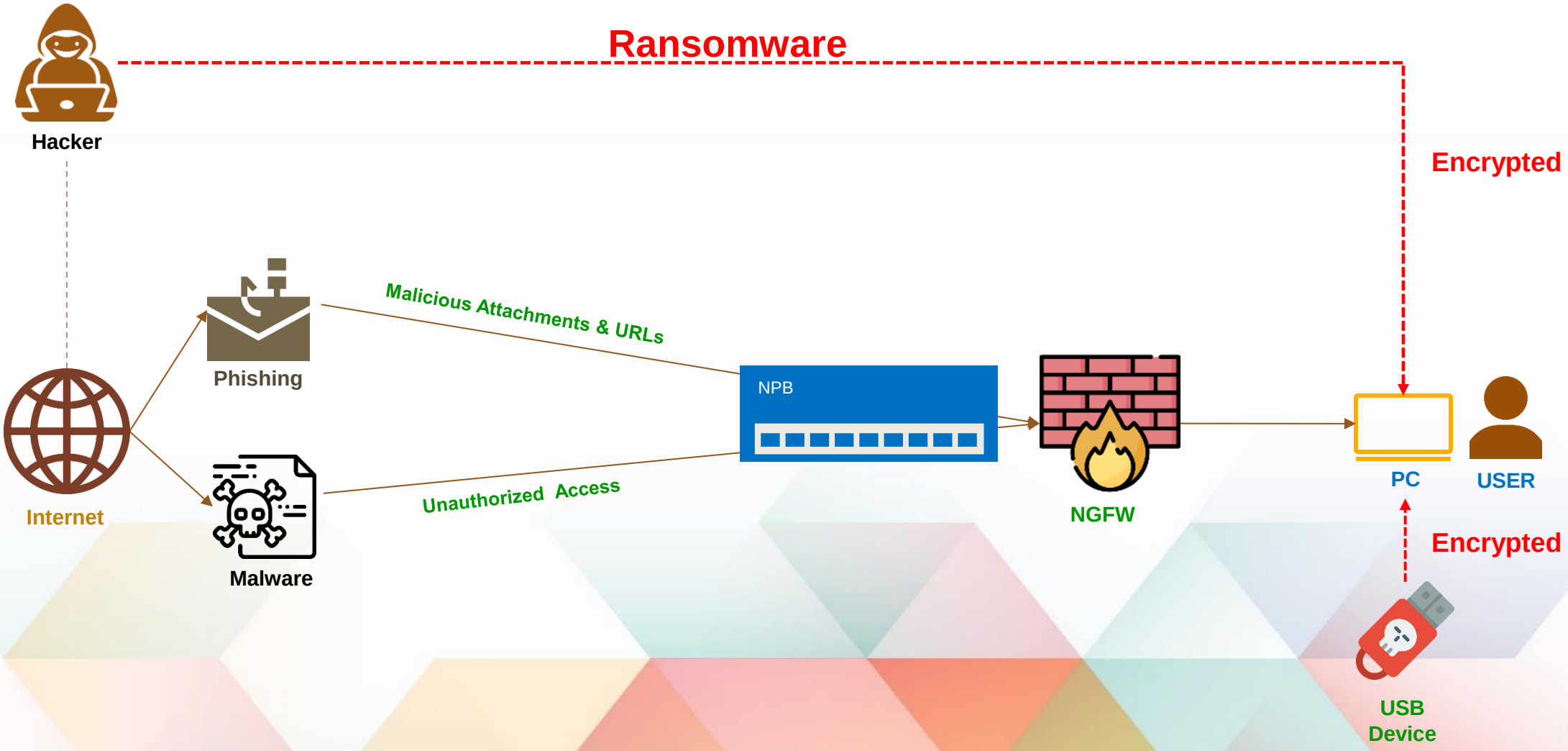
無檔案式威脅基礎觀念

無檔案式威脅基礎觀念

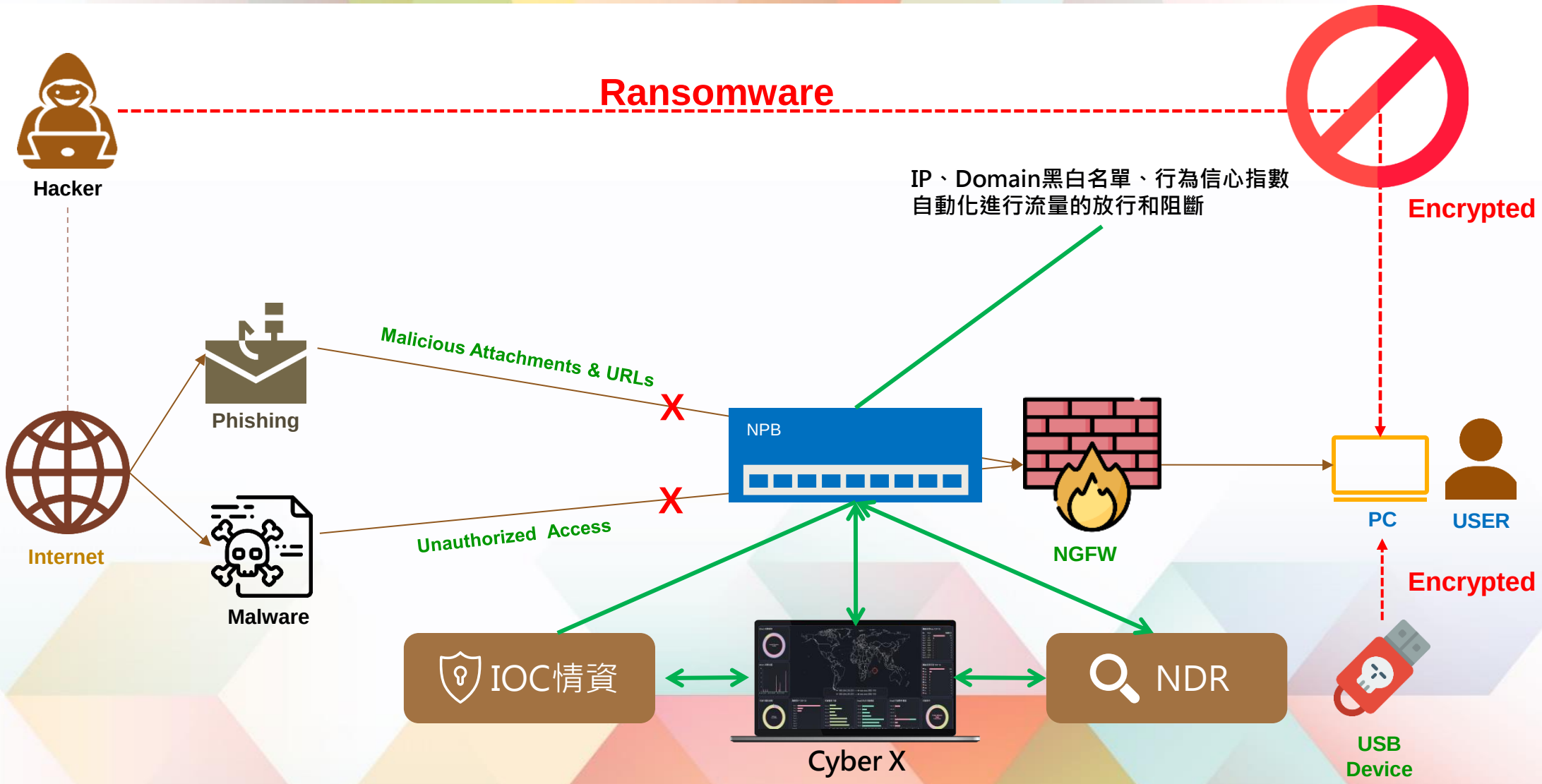
- 沒有可辨識的程式碼或特徵碼以及特定的行為可供傳統資安軟體偵測。
- 屬於記憶體式威脅，存在於電腦記憶體內。
- 利用系統上的執行程序來輔助攻擊。
- 可能搭配其他類型的惡意程式。
- 無法被白名單機制攔截，因為它利用的是系統上允許執行的應用程式。

svchost.exe (1264)	zappa-ca13902bd.localdomain	1900			UDP	
svchost.exe (1264)	localhost	1900			UDP	
svchost.exe (2860)	zappa-ca13902bd.localdomain	1312	v164337.vps.mcdir.ru	80	TCP	FIN Wait 2
svchost.exe (2860)	zappa-ca13902bd.localdomain	1317	v164337.vps.mcdir.ru	80	TCP	FIN Wait 2
svchost.exe (2860)	zappa-ca13902bd.localdomain	1319	v164337.vps.mcdir.ru	80	TCP	FIN Wait 2
svchost.exe (2860)	zappa-ca13902bd.localdomain	1324	v164337.vps.mcdir.ru	80	TCP	Established
svchost.exe (972)	zappa-ca13902bd	135		22643	TCP	Listen
System (4)	zappa-ca13902bd	445		29	TCP	Listen
System (4)	zappa-ca13902bd.localdomain	139		41207	TCP	Listen
System (4)	zappa-ca13902bd.localdomain	137			UDP	
System (4)	zappa-ca13902bd.localdomain	138			UDP	
System (4)	zappa-ca13902bd	445			UDP	
Waiting Connections	zappa-ca13902bd.localdomain	1311	v164337.vps.mcdir.ru	80	TCP	Time Wait
Waiting Connections	zappa-ca13902bd.localdomain	1316	v164337.vps.mcdir.ru	80	TCP	Time Wait
Waiting Connections	zappa-ca13902bd.localdomain	1318	v164337.vps.mcdir.ru	80	TCP	Time Wait
Waiting Connections	zappa-ca13902bd.localdomain	1323	v164337.vps.mcdir.ru	80	TCP	Time Wait

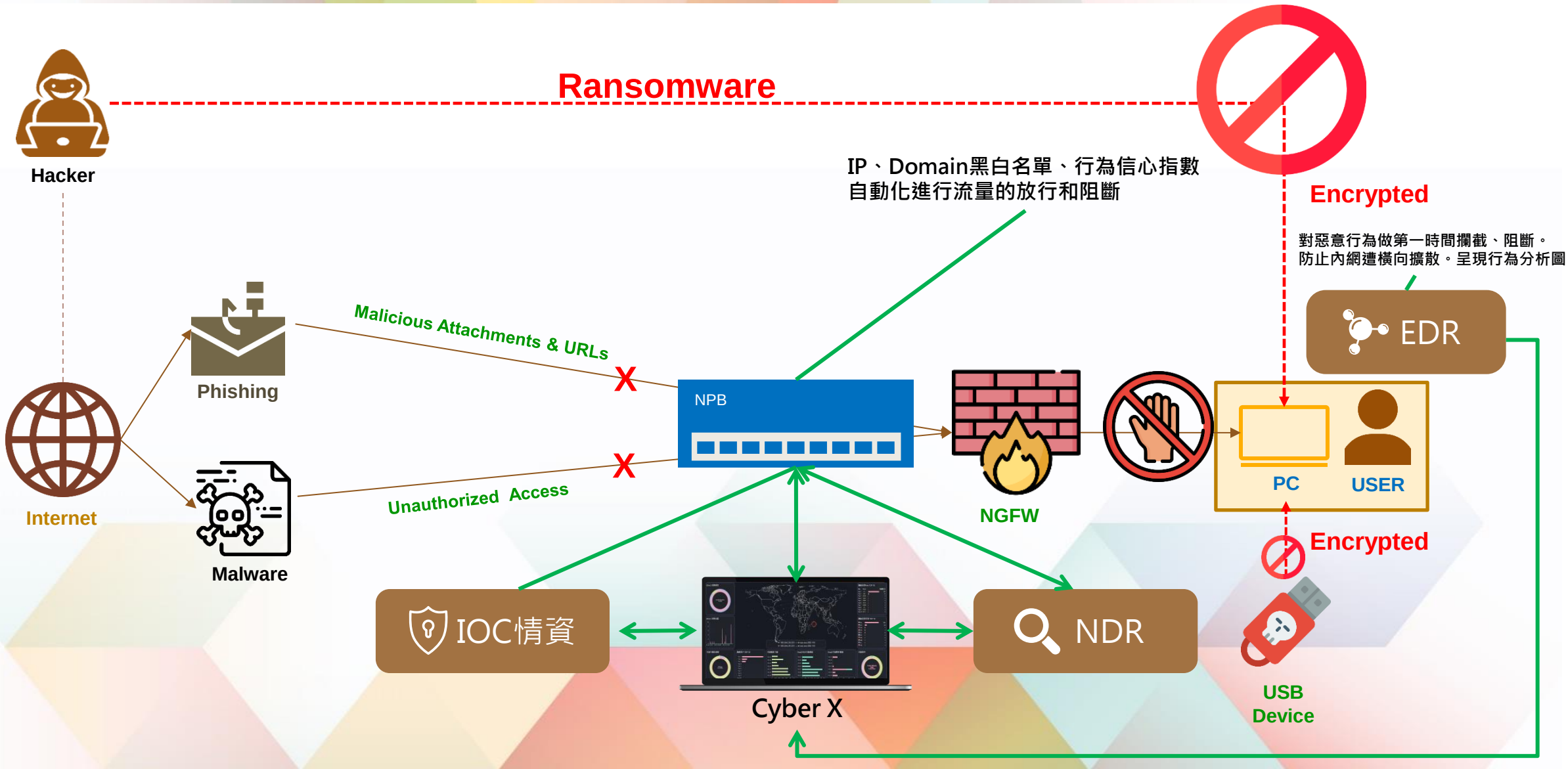
以勒索病毒入侵方式為例



勒索病毒防護方案-Cyber X 閘道端防護



勒索病毒防護方案-Cyber X 閘道端防護+端點防護



04

Cyber X 方案

Cyber X 共契項目

1080204 資安_網路安全

- 293項次
- 294項次
- 295項次
- 296項次
- 297項次
- 298項次
- 299項次
- 300項次
- 301項次
- 302項次
- 303項次
- 304項次
- 305項次

1090201 資安_網路安全

- 280項次
- 281項次
- 282項次
- 283項次
- 284項次
- 285項次
- 286項次
- 287項次
- 288項次
- 289項次
- 290項次
- 291項次
- 292項次

1090201 資安_安全管理與弱點評估

- 124項次
- 125項次

Cyber X 資安防禦服務平台

方案	項次	價格(NTD)	備註
PacketX SDN分流與防禦系統 資安_網路安全	Standard(305)	$446,701	Cyber X + NPB
	Advanced (303)	$1,340,102	
	Enterprise(304)	$1,908,629	
Cyber X資安防禦平臺 資安_網路安全	Standard(302)	$1,137,056	Cyber X + NPB + NDR(雲端版)
	Advanced (300)	$2,030,457	
	Enterprise(301)	$2,598,985	

Cyber X 整合中

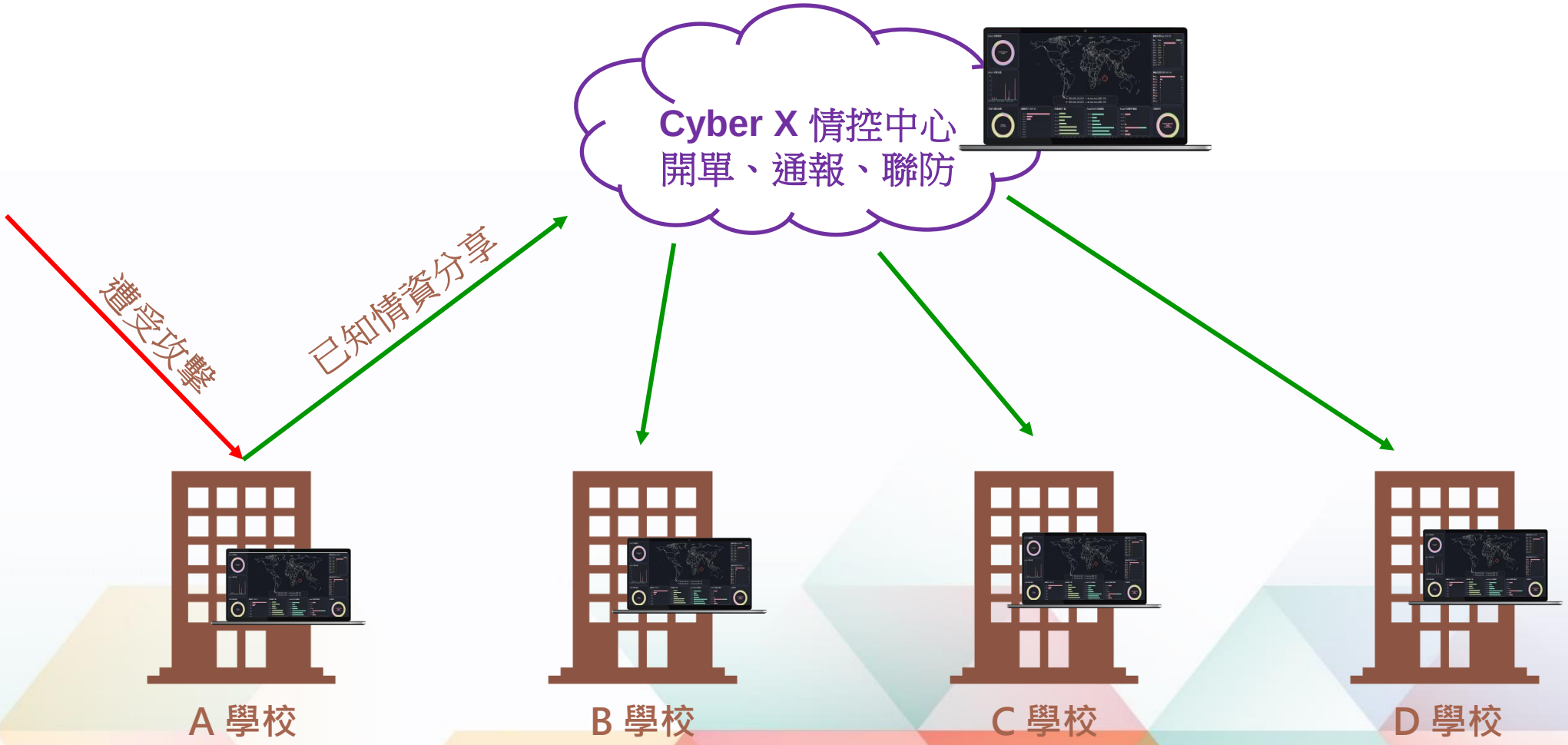
Cyber X 整合 VMware

- Carbon Black
  - 由端點補足閘道上缺少的防護
  - 目前線上設備數量 / 已植Agent設備數量
  - 設備的健康狀態(高風險的Top10)
  - 呈現相關告警的事件
  - 由告警的事件進行端點電腦的阻斷、事件放行
  - 由告警的MD5進行黑白名單放行
- NSX
  - 由分散式防火牆補足東西向防護
  - 東西向流量使用Lastline進行分析檢測
  - 呈現相關告警事件
  - 由告警事件自動觸發Policy進行權限限縮

06

Cyber X 未來願景

Cyber X 未來願景



Q&A