資安事件調查與分析實務

蔡一郎、高偉碩

SHIELDXTREME

Defense | 授課時數：6小時 | 初階

課程目的

本課程將著重在資安事件調查與實務分析，介紹資安事件應變基準及常見的事件調查工具。課程包含上機實作，透過課程教學與實務演練，學員將學習如何進行資料採集與分析、封包分析進行資安事件調查與分析。學員將能夠掌握從事件識別到應對和恢復的完整流程，提升實務操作能力和事件調查的專業知識。

- 課程涵括(**此為課程大綱簡要**)
  - 資安事件調查與案例介紹
  - 資安事件調查工具介紹
  - 實務演練-封包、惡意程式分析
  - 綜合演練

日期	時數	學習目的		課程實作 一人一機搭配課程內容(X-Lab)	NICE framework
Day 1	6	上午	•資安事件調查與案例介紹 •實務演練-封包、惡意程式分析	•WK1: IR101	Securely Provision (SP) Protect and Defend (PR) Operate and Maintain (OM)
		下午	•資安事件調查工具介紹 •綜合演練	•WK2 : INC2403	

資安事件調查與案例介紹

最近的資安事件

工商時報 數位編輯 2023.06.30

台積電否認遭駭客入侵，而是其供應商擎昊科技被駭。圖／本報資料照片

據外媒報導，惡名昭彰的LockBit勒索軟體組織，屢屢駭入各大科技公司勒索巨資，這回鎖定全球晶圓代工大廠台積電，傳出勒索7000萬美元（約台幣21.7億元），並要求8月6日前付款；對此，台積電澄清沒這回事，完全沒受到任何影響。據了解，是台積電供應商擎昊科技被駭。

自由時報報導，據了解台積電資訊科技服務供應商擎昊科技於2023年6月29日上午，發現公司內部特定測試環境中，遭受外部團體的網路攻擊，並擷取相關資訊。擎昊科技表示，已通知客戶台積電，除了對此次資安事件受影響的客戶致歉，也將進行排查、強化資安防護。

台積電回應指出，這次供應商遭駭事件，台積電未受到任何影響。

Kinmax 擎昊科技

關於擎昊 | 最新消息 | 產品與服務 | 成功案例 | 企業據點

1. 本公司於2023年6月29日上午，發現公司內部特定測試環境中，遭受外部團體之網路攻擊，並擷取相關資訊。當日我們即與客戶完成通報並致歉，同時即邀請第三方資安團隊與客戶共同做損害控管。

2. 遭受攻擊之環境為工程測試區，此為替客戶準備之系統安裝環境，遭擷取之內容為安裝設定檔等參數資訊，但因使用到特定客戶之公司名稱，故引起網攻團體之注意，並試圖經此途徑取得客戶之機敏資料。

3. 因上述資訊並無關客戶之實際應用，僅為出貨時之基本設定，目前沒有造成客戶之損害，客戶也並未因此遭駭。

4. 公司已關閉受感染區段，第三方資安團隊目前也評定其餘網段環境為正常未受損，同時持續協助我們釐清風險足跡，檢討改善強化資安措施。

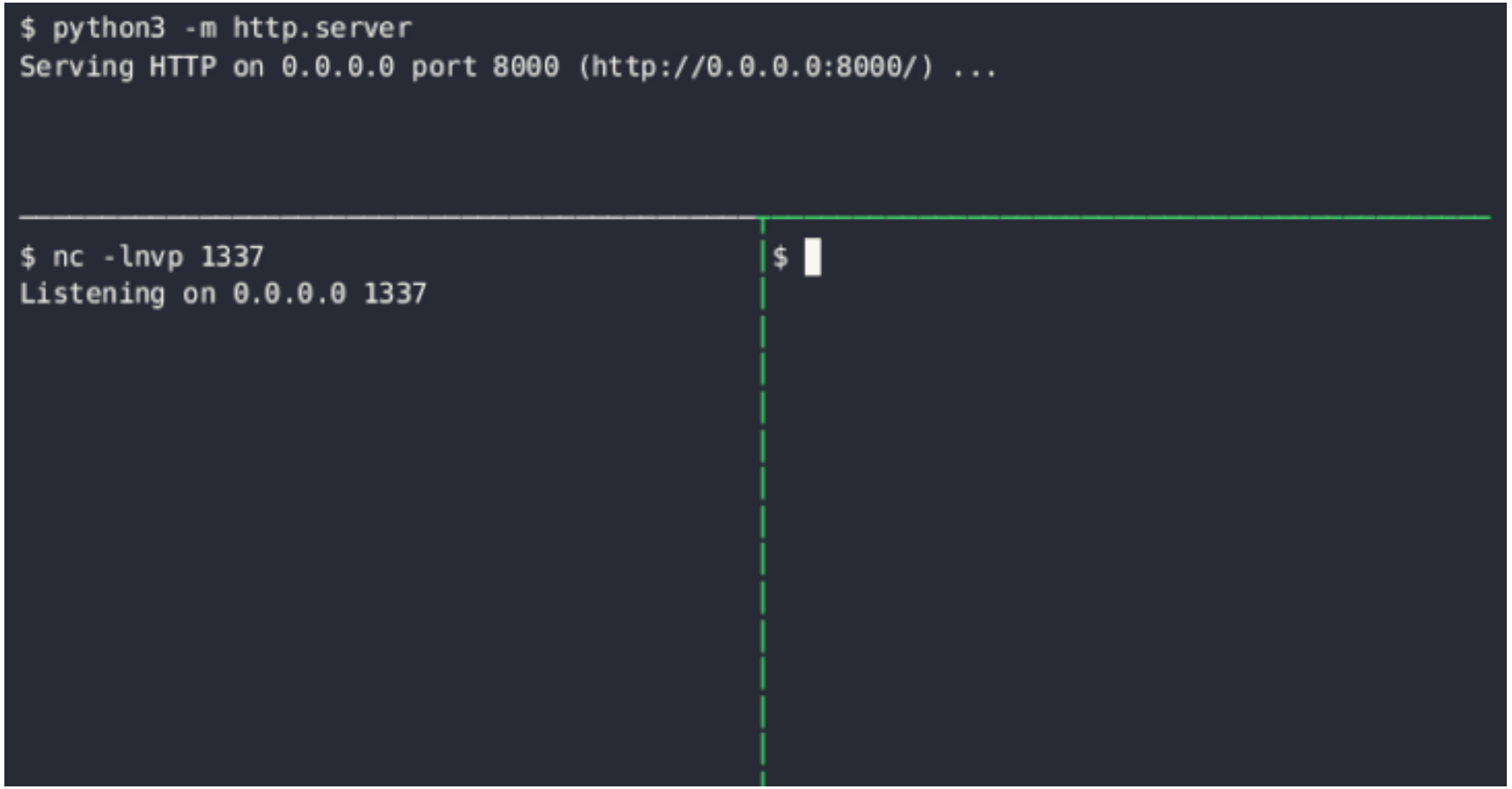
5. 公司營運狀況一切正常，並無造成公司實質損失，目前也同時完成調查局的立案，已進入刑事調查階段。

6. 原因檢討與改善：
本次事件肇因於 a. 測試區環境防火牆版本未即時更新
b. 測試區密碼強度不足
c. 區內之客戶名稱未作適當的遮蔽

https://www.kx.com.tw/KX_News_Letter_20230704-1

最近的資安事件

Alert: 330,000 FortiGate Firewalls Still Unpatched to CVE-2023-27997 RCE Flaw

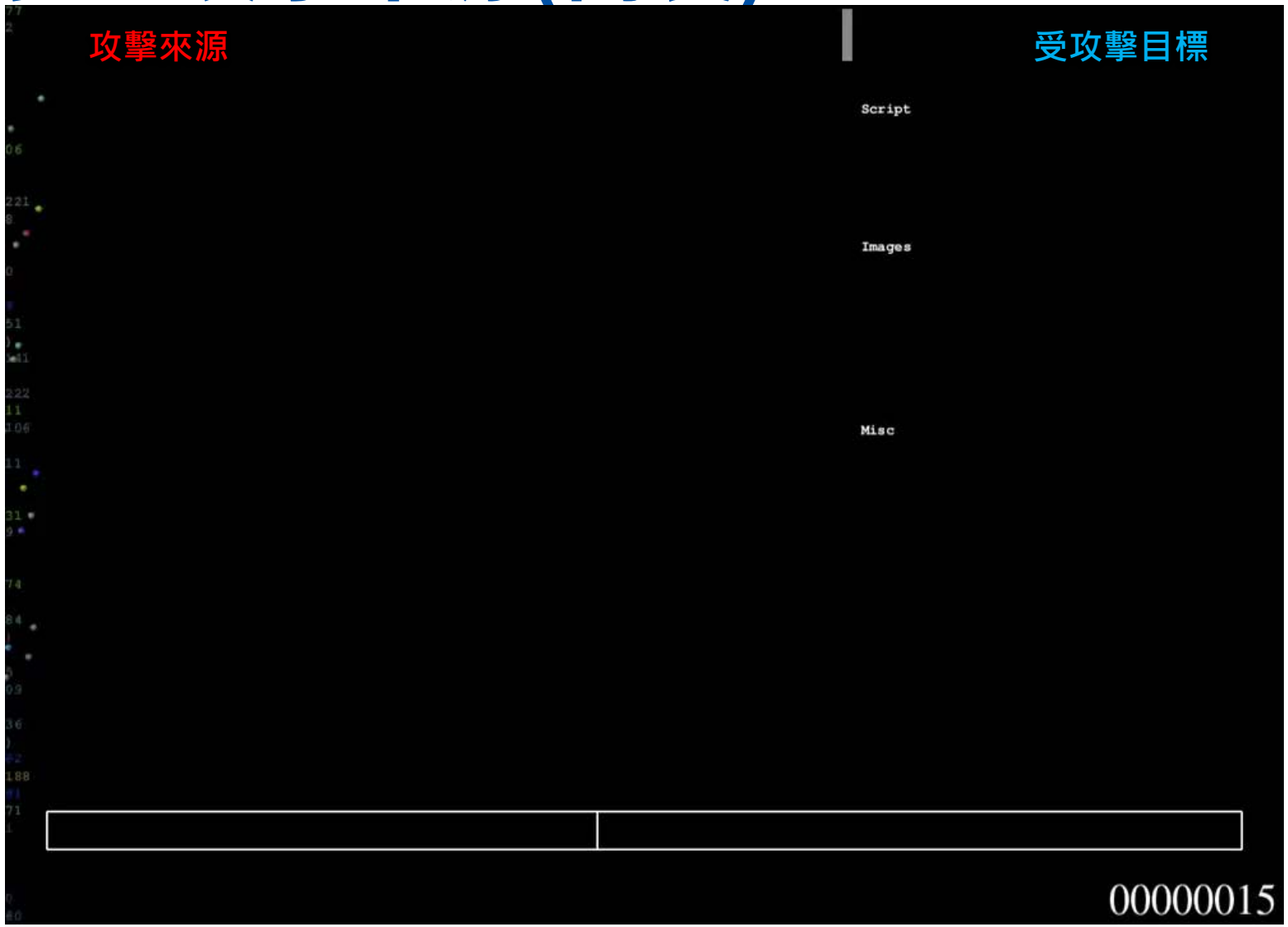


No less than 330,000 FortiGate firewalls are still unpatched and vulnerable to CVE-2023-27997, a critical security flaw affecting Fortinet devices that has come under active exploitation in the wild.

Cybersecurity firm Bishop Fox, in a report published last week, said that out of nearly 490,000 Fortinet SSL-VPN interfaces exposed on the internet, about 69 percent remain unpatched.

CVE-2023-27997 (CVSS score: 9.8), also called XORtigate, is a critical vulnerability impacting Fortinet FortiOS and FortiProxy SSL-VPN appliances that could allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.

多重攻擊來源(偽裝)



- 假冒IP位址，偽裝攻擊來源
- 無法單純的利用網路層的處理方式

SQL-Inject混合攻擊

- 駭客針對目標進行攻擊劇本的設計
- 利用固定的網路行為，隱藏其背後的目的

造成資安事件的原因

- **內部造成之事件**
  - 員工私自將組織的外接式儲存設備攜帶回家使用，因不慎遺失而導致組織的機密資料外洩
  - 員工因更新網路設備的設定檔時，不慎開放了外部的 IP可以接觸到組織內部的電腦，進而發生了駭客直接在外部透過遠端桌面遙控內部的電腦
- **外部造成之事件**
  - 組織發生了惡意程式碼感染，並造成大規模的資訊設備當機
  - 組織重要的對外服務遭受分散式阻斷服務攻擊，造成無法提供對外服務
  - 組織的網站伺服器因已知的漏洞位進行修補，導致首頁發生了網頁置換之情況

優先移除與復原

- 事件調查關鍵報告
- 依事件的影響衝擊決定處理流程
- 以「業務恢復」與「營運持續」為主要目標
- 依難易度配置投入資源
- 決定優先順序與關聯性
- 應變團隊須清楚知道處理流程與步驟

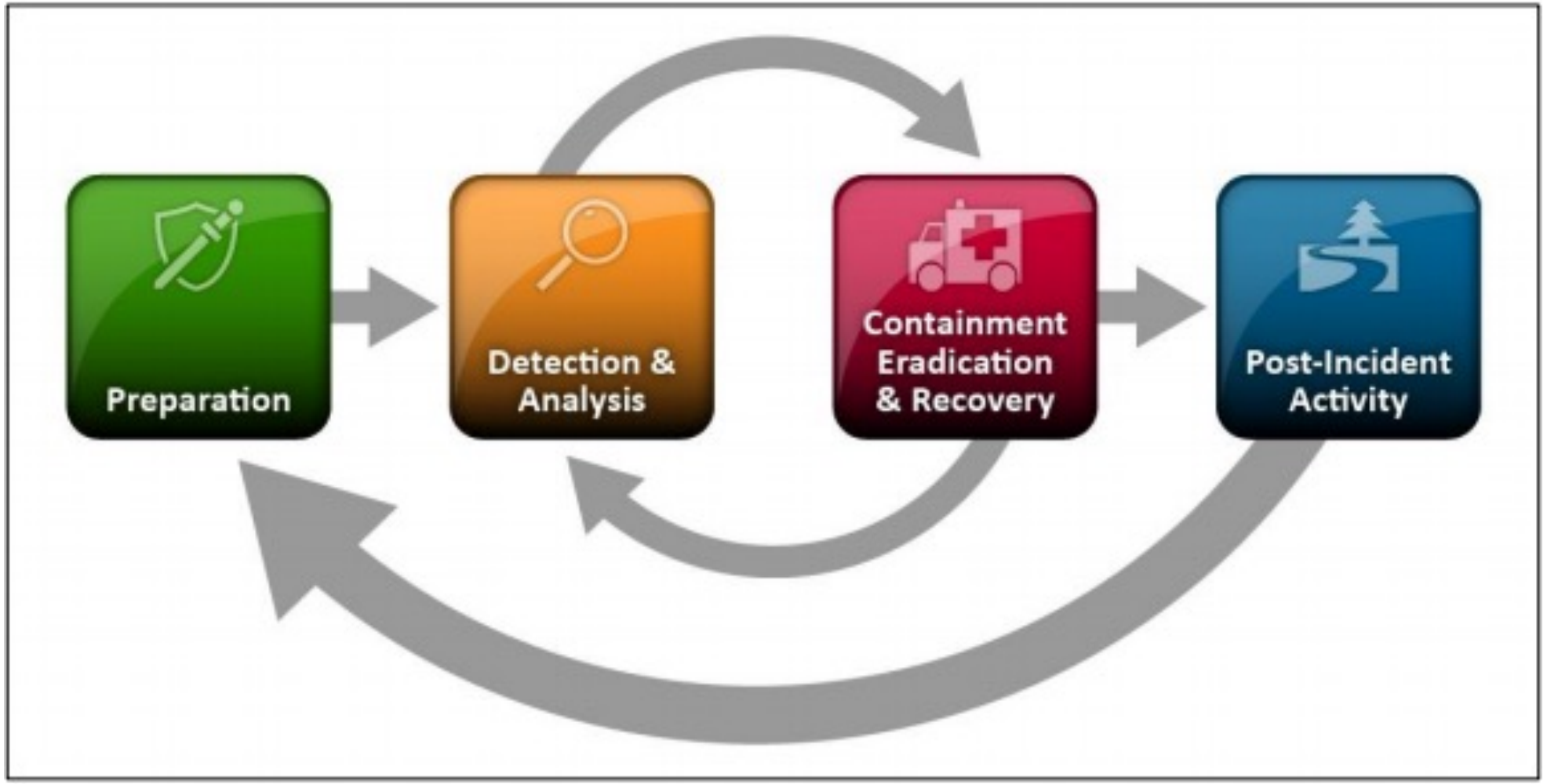
從每個事件中學習教訓

- **事件應變之後的分享**
  -建立事件處理生態系統
  -嘗試找出根本原因
  -「紅隊測試」與「藍隊防禦」思維
- **避免類似事件再度發生**
  -資源投入
  -改善已知問題
- **建立應變流程與基礎**
  -標準化與客製化
  - 5H2W (What、Who、When、Where、Why、How與How much)

SHIELDXTREME

(換圖示)

NIST Incident response



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

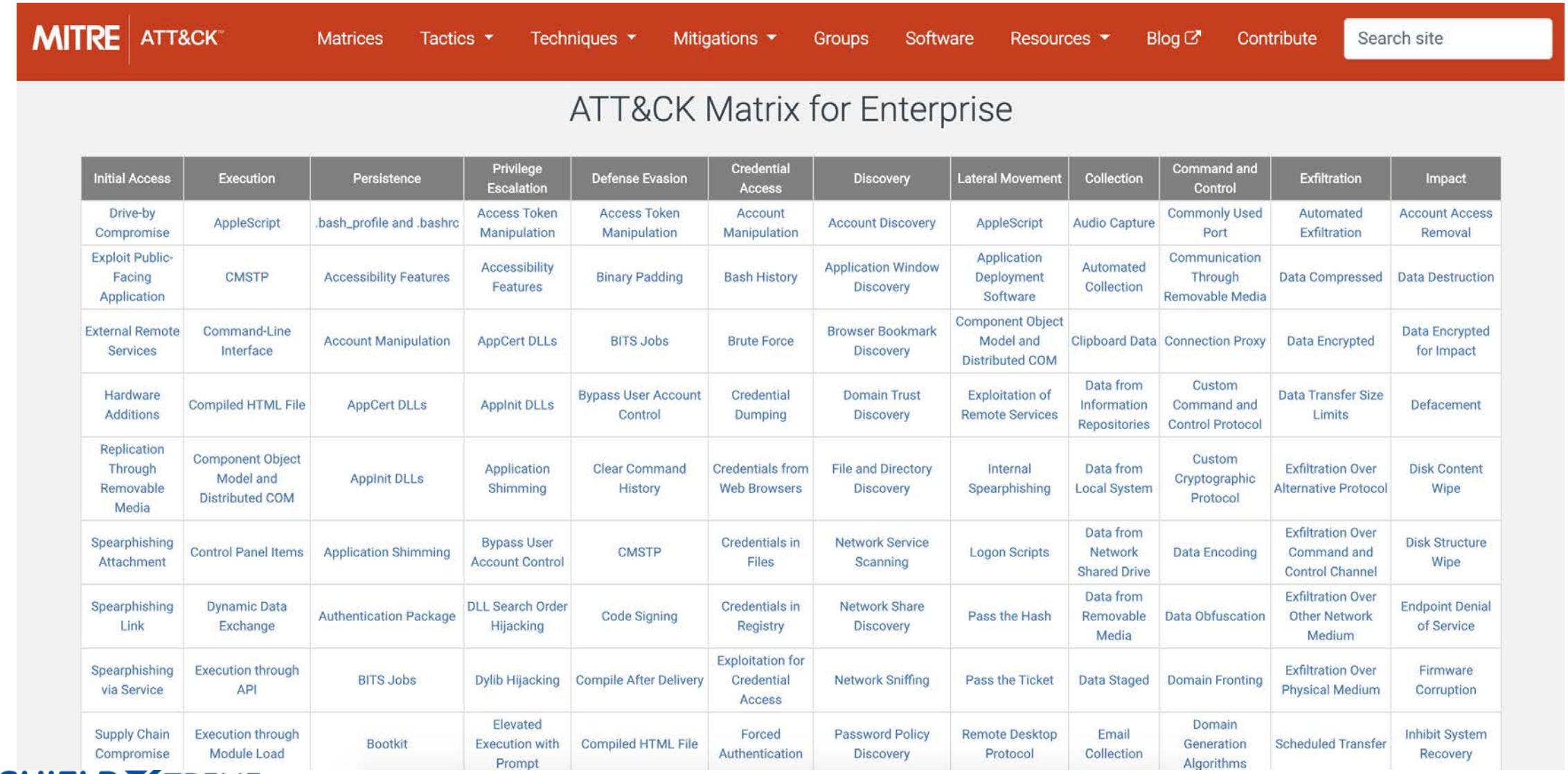
MITRE ATT&CK

- MITRE是美國非營利組織，除了協助進行多項資安相關研究，同時，也是維運CVE漏洞資料庫背後的組織，而ATT&CK框架的研究計畫，是該組織在2015年5月發起。

- ATT&CK資安框架由MITRE提出，不僅是讓威脅入侵的描述具有更**一致的標準**，成為有助於理解攻擊者具備能力的知識庫，並能為攻防演練或分析攻擊帶來幫助。

- 以**剖析攻擊面**為出發的資安框架

MITRE ATT&CK



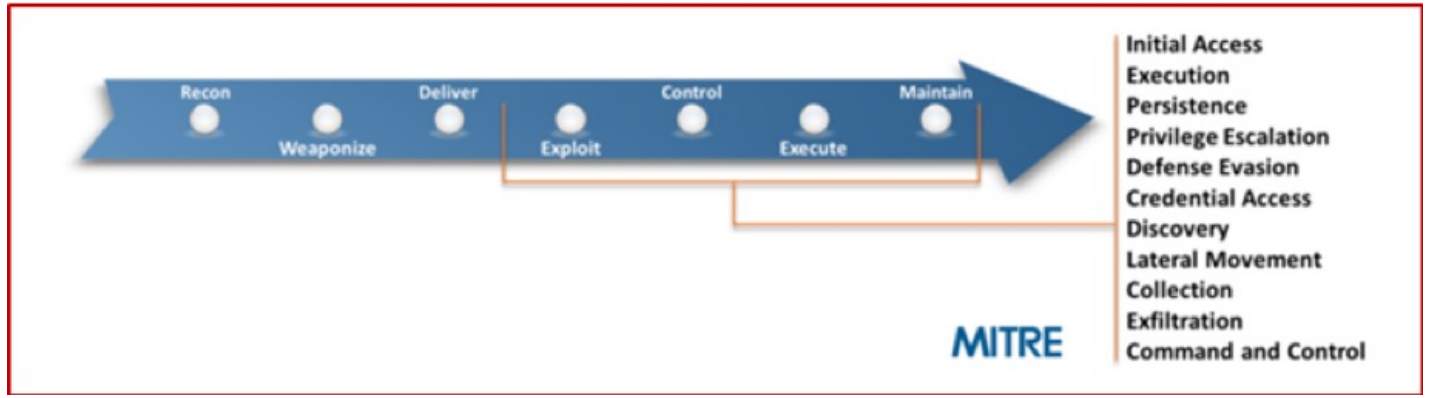
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery

https://attack.mitre.org/

MITRE ATT&CK

- 各資安業者定義的Cyber Kill Chain不盡相同，從入侵初始到結束的過程當中，有些業者畫分為5個階段，有些業者則是7個或9個等，因此，各家業者對同一事件報告的描述會有出入。
- MITRE提出的ATT&CK框架，是將入侵期間可能發生的情況，做出更細的劃分，以：入侵初期、執行、持續潛伏、權限提升、防禦跳脫、憑證存取、探勘發現、橫向移動、收集、滲透、命令與控制、衝擊，共12項戰術策略(Tactics)，細分為330項技術(Techniques)。



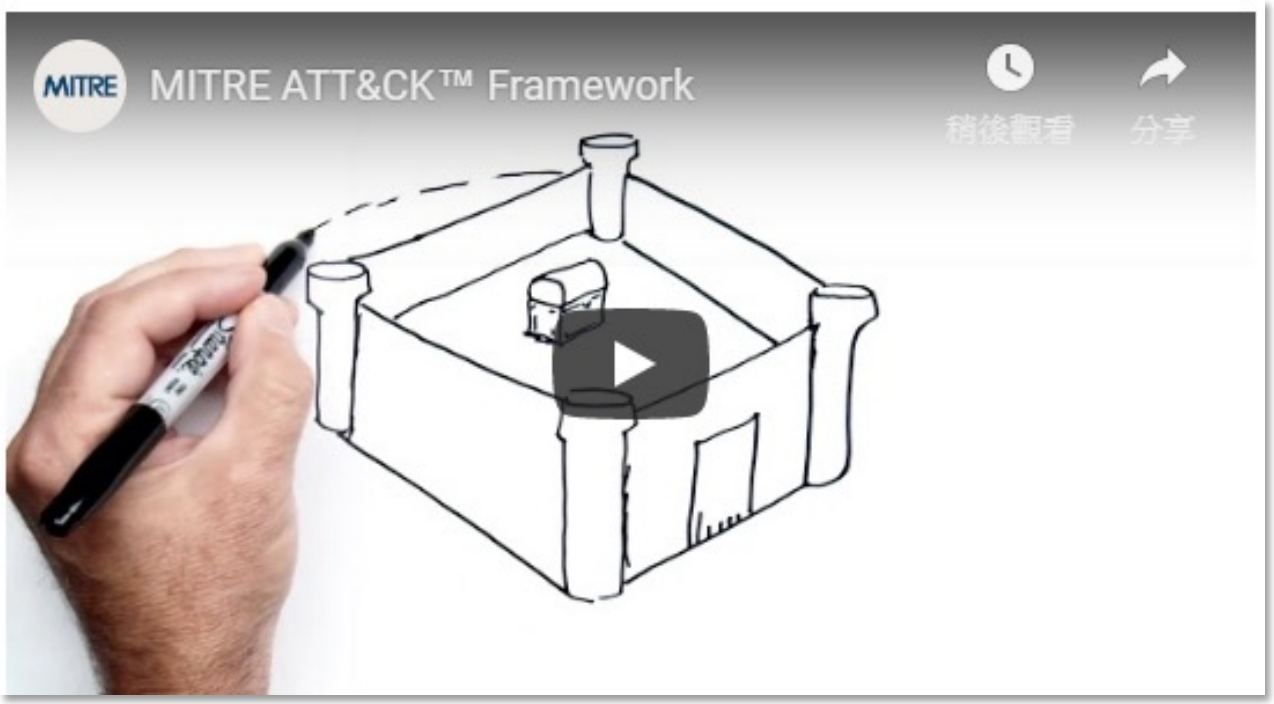
https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful

目的：讓入侵手法描述能有通用語言，幫助入侵事件的討論解釋等溝通

MITRE ATT&CK

- 提供了統一且結構化的方式，去描述攻擊者手法與行為，僅使用一張框架呈現，就能看出攻擊者所使用的策略與手法，並能透過更一致的過程來確認威脅的階段。換而言之，就是透過標準化、架構化的資訊，可以更快速檢視網路安全事件的全貌。

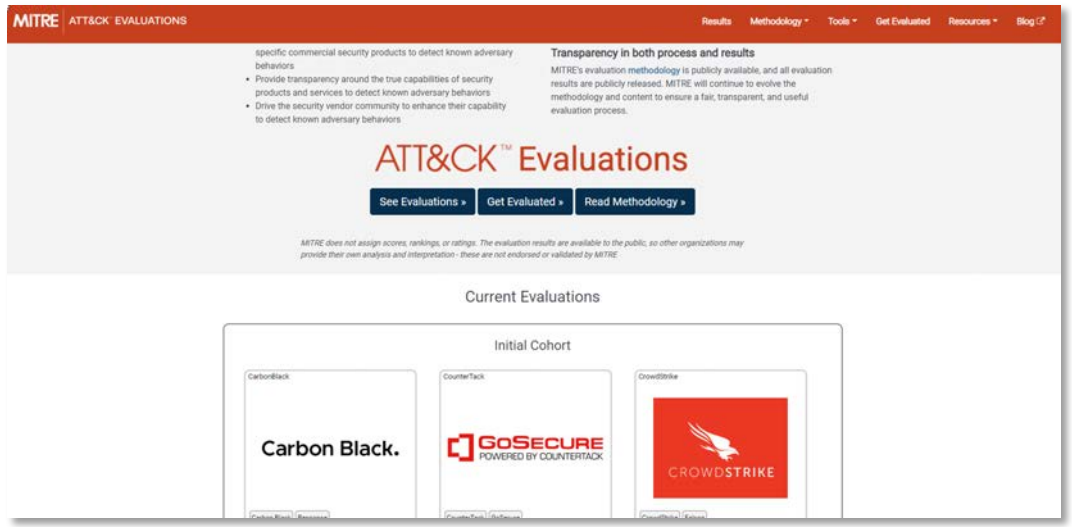
- 可用於：
  - 偵測與分析
  - 威脅情報
  - 弱點模擬驗證與紅隊訓練
  - 評估與安全工程系統
  - APT模擬 (Adversary Emulation)



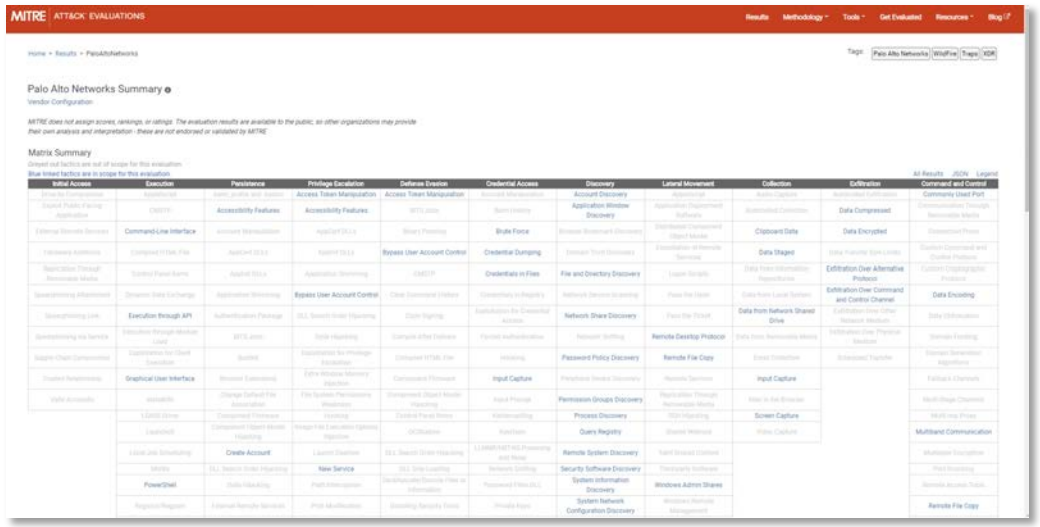
https://attack.mitre.org/resources/getting-started/

MITRE ATT&CK

- 許多企業要求資安業者融入ATT&CK，資安業者也在產品中使用ATT&CK，以便於在客戶溝通時能用通用的語言。
- 2018年11月，MITRE公布了一項ATT&CK評估（ATT&CK Evaluations）的計畫結果，共有7家業者參與，包括Carbon Black、CounterTack、Crowdstrike、Endgame、微軟、RSA與SentinelOne。



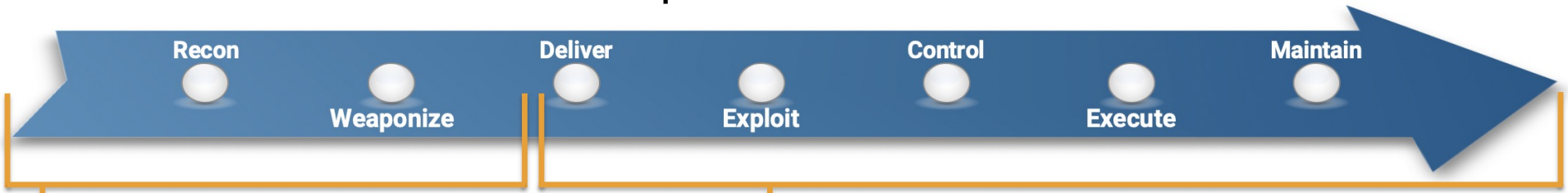
https://attackevals.mitre.org/



https://attackevals.mitre.org/APT3/results/paloaltonetworks/

MITRE ATT&CK

- PRE-ATT&CK和ATT&CK Enterprise結合起來形成了kill Chain完整戰術列表



PRE-ATT&CK

- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

參考連結： https://attack.mitre.org/resources/pre-introduction/

MITRE ATT&CK-Models

- ATT&CK模型可以分為四大部分，分別是PRE-ATT&CK、Enterprise與Mobile、ICS。

-PRE-ATT&CK定義了駭客攻擊前置作業，目前畫分為15個戰略階段

-Enterprise是指具體的攻擊入侵過程(Linux, macOS, Windows)

-Mobile則是針對行動平臺所發展(Android, iOS)

-ICS針對工控設備所研究的

MITRE ATT&CK小知識

"根據MITRE的說明，ATT&CK是基於現實世界觀測的對手戰術與技術知識庫。其中A為Adversarial，代表對抗性的攻擊者，兩個T是Tactics與Technical，分別代表對手採用的戰略與技術手法，而C與K則是Common knowledge，說明了這將是一個通用的知識庫。"

參考連結：https://www.ithome.com.tw/news/131274

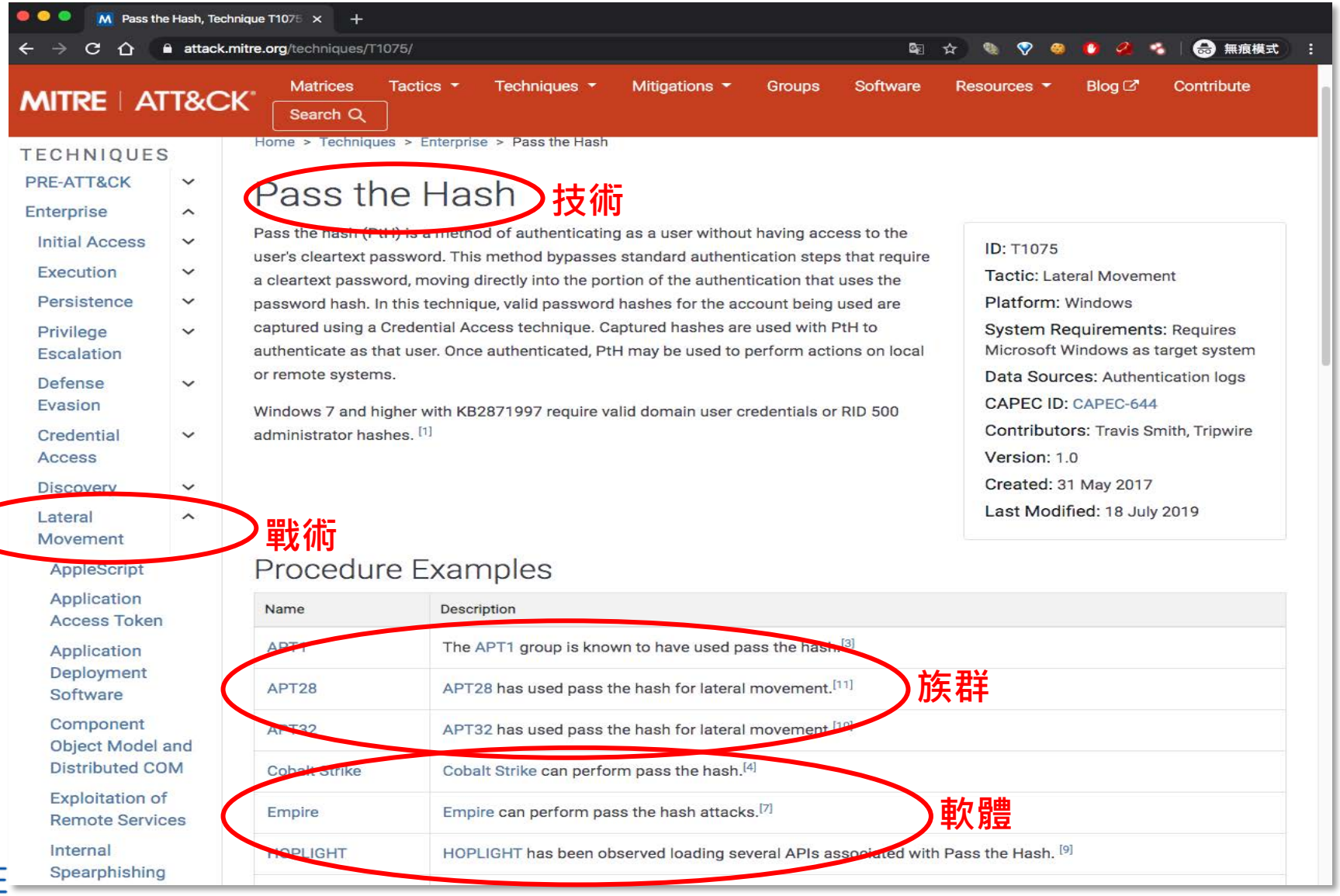
MITRE ATT&CK- Enterprise戰術策略(Tactics)

- 入侵初期(Initial Access)：攻擊者進入(網路的)企業的第一步
- 執行(Exection)：執行攻擊程式
- 持續潛伏(Persistence)：維持足跡
- 權限提升(Privilege Escalation)：取得系統上更高的權限
- 防禦跳脫(Defense Evasion)：避免被企業發現
- 憑證存取(Credential Access)：取得帳號密碼

MITRE ATT&CK- Enterprise戰術策略(Tactics)

- 探勘發現(Discovery)：瞭解企業系統環境
- 橫向移動(Lateral Movement)：逐步移動到目的地
- 收集(Collection)：收集機敏的檔案或資料
- 滲透(Exfiltration)：偷出資料
- 命令與控制(Command And Control)：持續與控制系統聯繫
- 衝擊(Impact)：對企業造成的損失

ATT&CK 網頁資訊



SHIELDXTREME

MITRE ATT&CK- 練習

- **User enumeration**

  -cat /etc/passwd

  -cat */????wd
- **Group enumerate**

  -cat /etc/group
- **System Enumeration**

  -uname -a
- **User Privilege enumeration**

  -sudo -l

MITRE ATT&CK- 練習(答案)

- **User enumeration(T1087** Account Discovery)

  -cat /etc/passwd

  -cat */????wd
- **Group enumerate(T1087)**

  -cat /etc/group
- **System Enumeration(T1082** System Information Discovery)

  -uname -a
- **User Privilege enumeration(T1033** System Owner/User Discovery)

  -sudo -l

觀念建立


RIK FERGUSON
TREND MICRO
一個根據案例改編而成的故事

如果你要調查駭客入侵的主因，請回答以下資訊

- 你需要調查哪些人？
- 你需要詢問哪些事情？
- 你需要的分析的時間範圍為？
- 你需要調查哪些事發地點？
- 你需要調查哪些設備？

事件處理流程

識別事件

- 網路釣魚
- 惡意程式
- 資料外洩
- 勒索軟體攻擊
- 漏洞攻擊
- 其他...

SHIELDXTREME

SANS Incident Response 6 steps

https://www.sans.org/media/score/504-incident-response-cycle.pdf

證據蒐集

揮發性及非揮發性資料搜集

證據搜集

- 合法性
- 完整性
- 連續性
- 即時性

可能留有事件的軌跡設備有哪些？

可能設備有以下地方

- SIEM
- Honeypot
- IDS/IPS
- NDR
- NGFW
- PC
- …

Windows / Linux 的日誌放在哪裡?

Where Is the Log ?

- Windows
  - \Windows\System32\winevt\Logs\
- Windows IIS
  - \inetpub\logs\LogFiles
- Linux
  - /var/log/
  - /var/log/auth.log or /var/log/secure
  - /var/log/cron.log or /var/log/cron
  - /var/log/apache2/access.log

網路行為封包側錄

封包側錄

- 避免於受害主機上直接側錄（避免污染證物）
- 透過網路設備進行側錄
- 有必要使用遠端側錄
- 封包檔案切割（以時間/檔案大小)
- 如果已經鎖定目標請直接下相關語法減少雜訊
- 配合封包回放並且搭配IDS， 判斷網路行為
- 配合主機運作之Process && Netstat 進行分析

封包側錄

主要用途為取得封包，並且為了即時分析或是後續分析所需，故在封包側錄的過程當中需要了解用途，並且根據用途選定適當的解決方案。

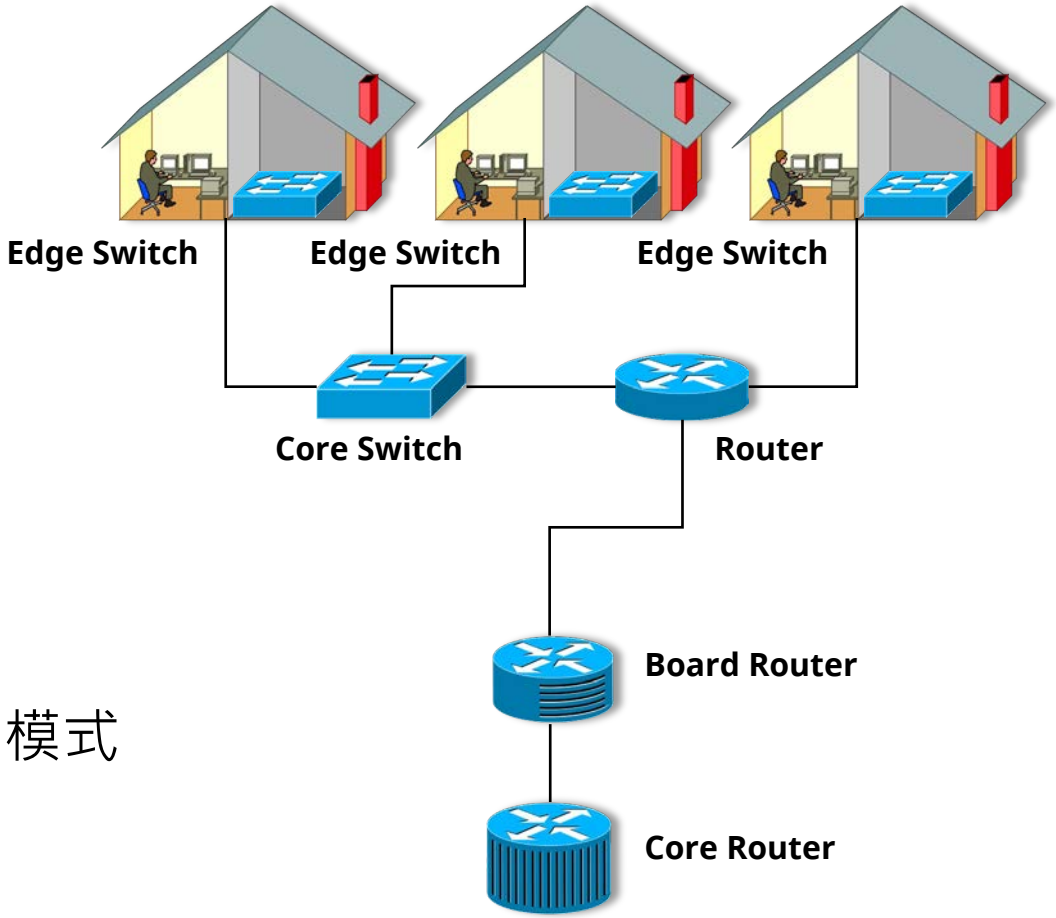
- **封包側錄同時需注意**
  - 硬體效能 (包含網路介面卡)
  - 流量大小
  - 儲存空間

封包擷取及分析

- 網路封包擷取的需求
  -瞭解電腦網路目前進行的動作
  -監聽側錄另一台電腦網路連線
  -瞭解網路程式如何運行
  -學習網路通訊協定

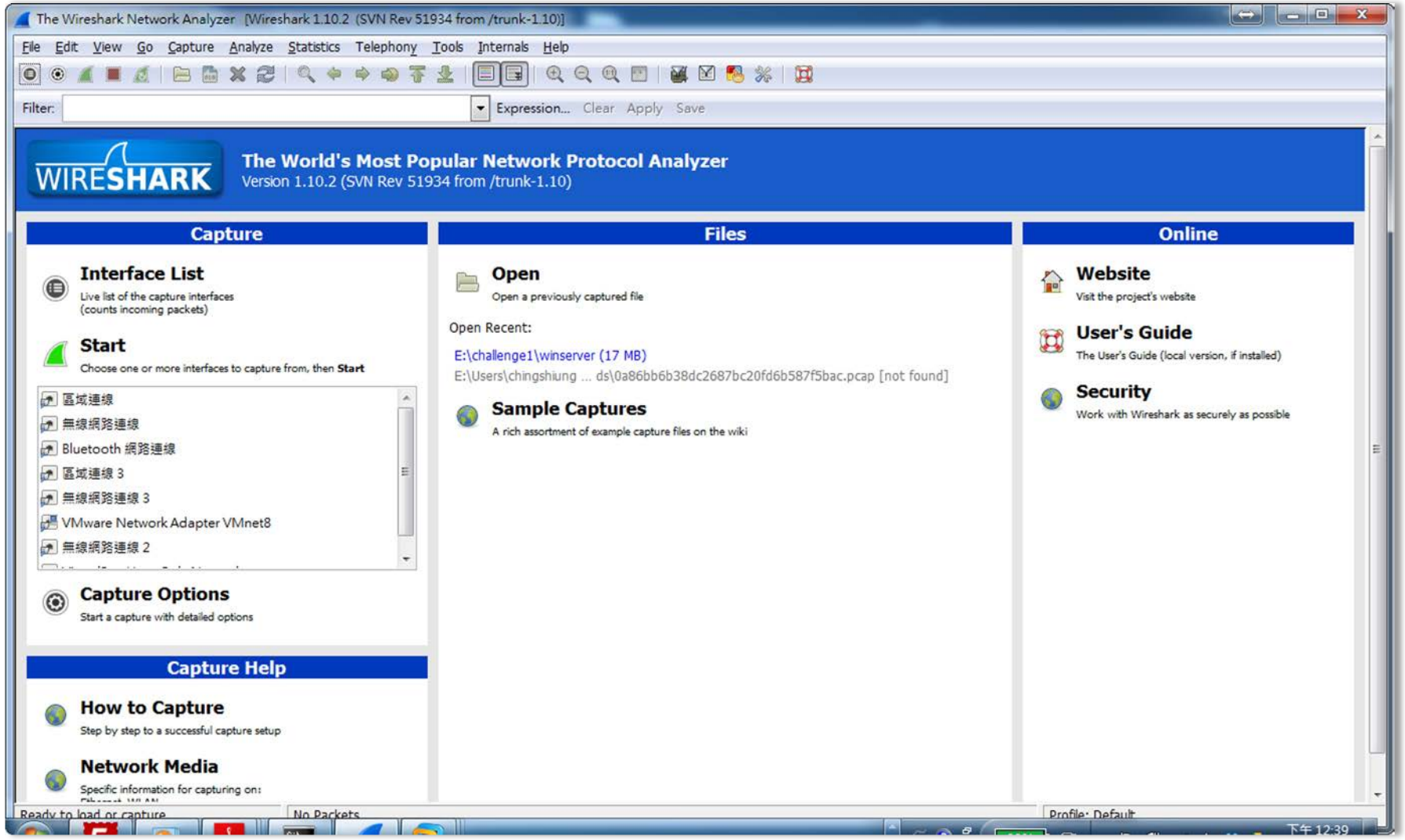
封包截取的關鍵

- **截取位置**
  - Host / Server
  - Edge Switch
  - Core Switch
  - Router
  - Board Router
  - Core Router



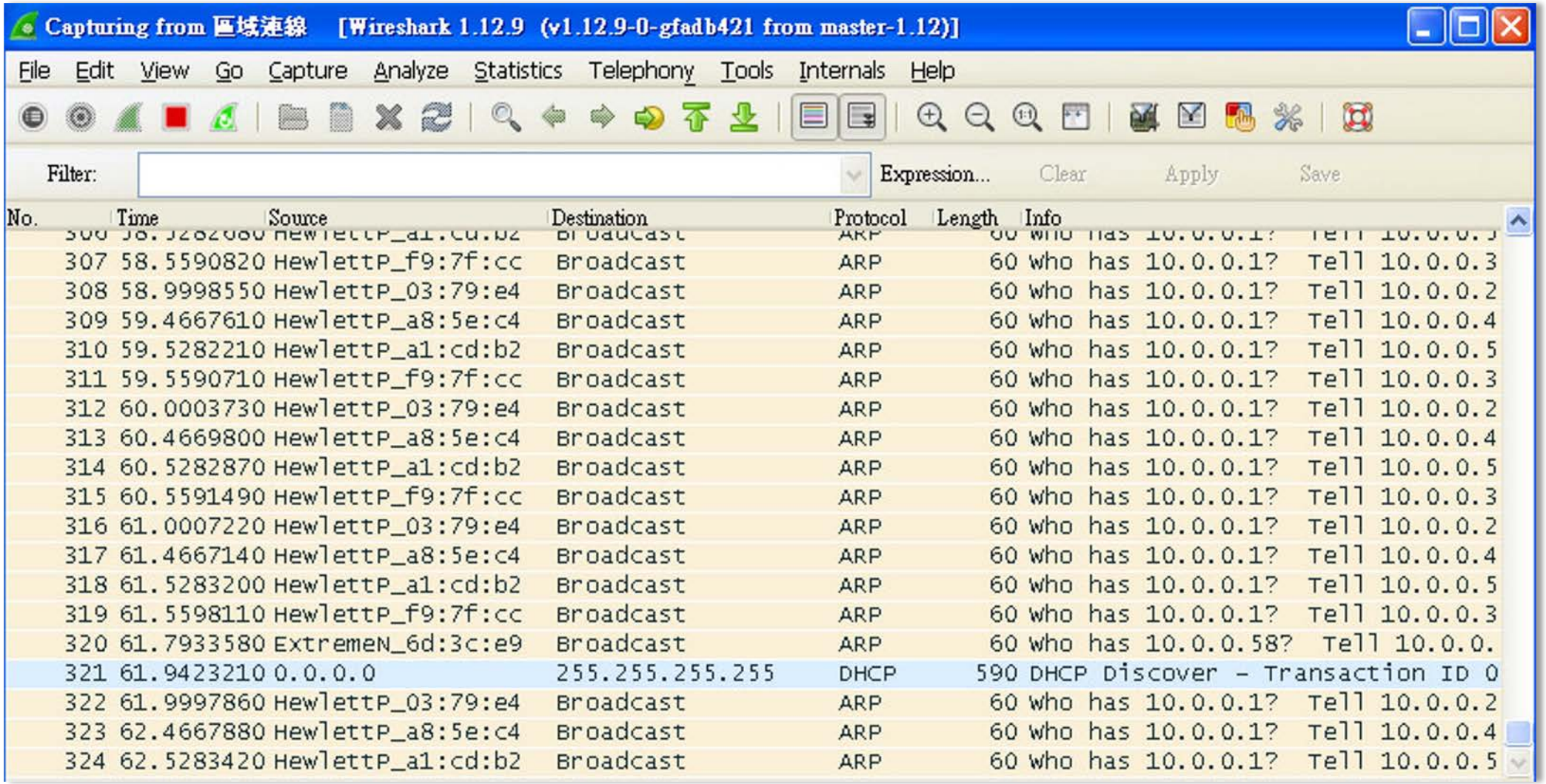
- **過濾條件**
  - 限制 or 忽略
  - 網路架構
- **差異**
  - IDS / IPS / IDP → 已知模式
  - 封包分析 → 未知模式

Wireshark



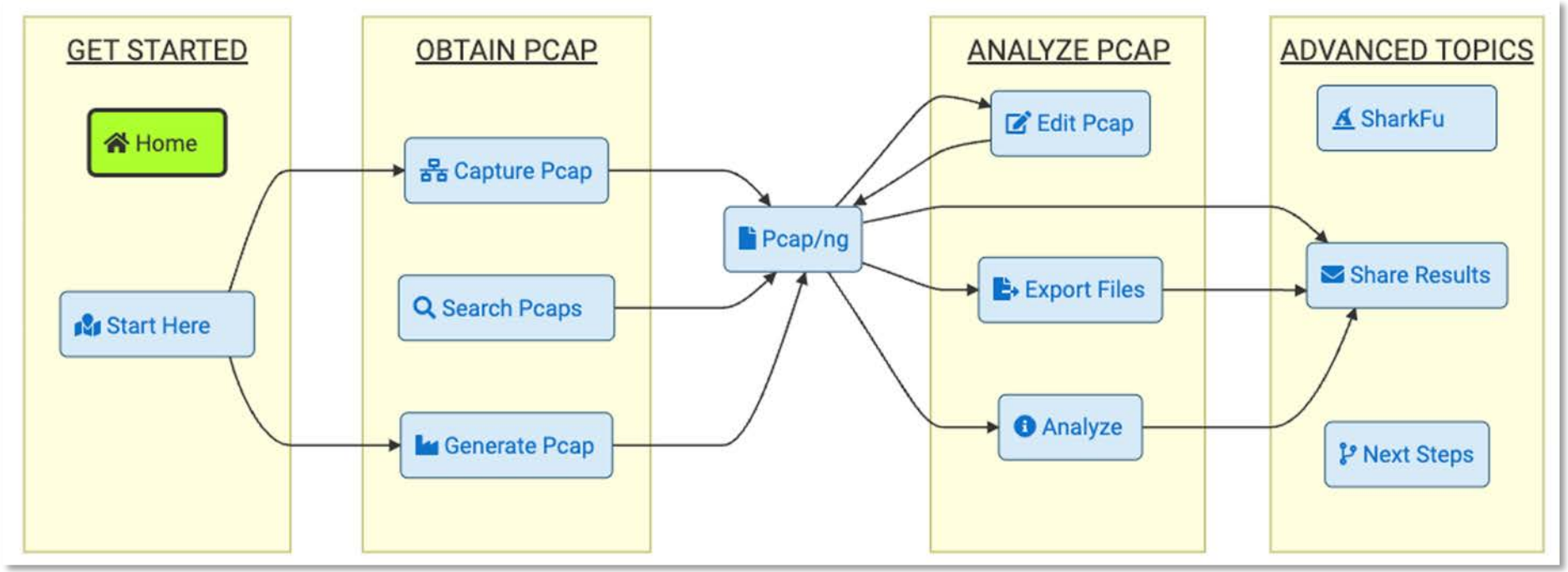
Web | https://www.wireshark.org/

Wireshark


Capturing from 區域連線 [Wireshark 1.12.9 (v1.12.9-0-gfadb421 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
307 58.5590820 HewlettP_f9:7f:cc Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.3
308 58.9998550 HewlettP_03:79:e4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
309 59.4667610 HewlettP_a8:5e:c4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.4
310 59.5282210 HewlettP_a1:cd:b2 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.5
311 59.5590710 HewlettP_f9:7f:cc Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.3
312 60.0003730 HewlettP_03:79:e4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
313 60.4669800 HewlettP_a8:5e:c4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.4
314 60.5282870 HewlettP_a1:cd:b2 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.5
315 60.5591490 HewlettP_f9:7f:cc Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.3
316 61.0007220 HewlettP_03:79:e4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
317 61.4667140 HewlettP_a8:5e:c4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.4
318 61.5283200 HewlettP_a1:cd:b2 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.5
319 61.5598110 HewlettP_f9:7f:cc Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.3
320 61.7933580 ExtremeN_6d:3c:e9 Broadcast ARP 60 Who has 10.0.0.58? Tell 10.0.0.
321 61.9423210 0.0.0.0 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0
322 61.9997860 HewlettP_03:79:e4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
323 62.4667880 HewlettP_a8:5e:c4 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.4
324 62.5283420 HewlettP_a1:cd:b2 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.5

Tshark

- 是一套 command - line 的封包捕捉軟體，你可以透過這一套進行封包的攔截及分析，Tshark 原生的檔案格式為 pcapng ，故格式上可以與 Wireshark 及其他封包分析軟體所使用。



Tshark

- 確認有哪些介面可以捕捉封包
  - tshark – D

```
└─# tshark -D
Running as user "root" and group "root". This could be da
1. eth0
2. any
3. lo (Loopback)
4. bluetooth-monitor
5. nflog
6. nfqueue
7. dbus-system
8. dbus-session
9. ciscodump (Cisco remote capture)
10. dpauxmon (DisplayPort AUX channel monitor capture)
11. randpkt (Random packet generator)
12. sdjournal (systemd Journal Export)
13. sshdump (SSH remote capture)
14. udpdump (UDP Listener remote capture)
```

- 捕捉10 秒內的 eth0 流量
  - tshark -i eth0 -a duration:10

```
└─# tshark -i eth0 -a duration:10
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
 ** (tshark:13030) 11:20:42.220096 [Main MESSAGE] -- Capture started.
 ** (tshark:13030) 11:20:42.220144 [Main MESSAGE] -- File: "/tmp/wireshar
    1 0.000000000 10.211.55.15 → 10.211.55.2  SSH 286 Server: Encrypted p
    2 0.000193212  10.211.55.2 → 10.211.55.15 TCP 66 60912 → 22 [ACK] Seq
85401954 TSecr=2834282737
    3 0.516881768 10.211.55.15 → 10.211.55.2  SSH 334 Server: Encrypted p
    4 0.517156231  10.211.55.2 → 10.211.55.15 TCP 66 60912 → 22 [ACK] Seq
85402471 TSecr=2834283254
    5 1.059178584 10.211.55.15 → 10.211.55.2  SSH 334 Server: Encrypted p
    6 1.059520881  10.211.55.2 → 10.211.55.15 TCP 66 60912 → 22 [ACK] Seq
85403014 TSecr=2834283796
    7 1.602229848 10.211.55.15 → 10.211.55.2  SSH 334 Server: Encrypted p
    8 1.603265325  10.211.55.2 → 10.211.55.15 TCP 66 60912 → 22 [ACK] Seq
```

- 捕捉 eth0 流量並且輸出檔案
  - tshark -i eth0 -w /root/output_file.pcap

```
└─# tshark -i eth0 -w /root/output_file.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
 ** (tshark:16242) 11:33:33.968174 [Main MESSAGE] -- Capture started.
 ** (tshark:16242) 11:33:33.968219 [Main MESSAGE] -- File: "/root/output_file.pcap"
46
```

Tshark Capture CheatSheet

- tshark -i 2
- tshark -i 2 -a duration:10
- tshark -i 2 -w output_file.pcap
- tshark -i wlan0 -Y http.request -T fields -e http.host -e http.user_agent
- tshark -i wlan0 -f "src port 53" -n -T fields -e dns.qry.name -e dns.resp.addr
- tshark -i wlan0 -f "src port 53" -n -T fields -e frame.time -e ip.src -e ip.dst -e dns.qry.name -e dns.resp.addr
- tshark -i wlan0 -Y 'http.request.method == POST and tcp contains "password"' | grep password

TCPDump

- TCPDump 可以透過指令來側錄網路封包

```
tcpdump version 4.99.1
libpcap version 1.10.1 (with TPACKET_V3)
OpenSSL 3.0.4 21 Jun 2022
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ] [--count]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ --immediate-mode ] [ -j tstamptype ]
                [ -M secret ] [ --number ] [ --print ] [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ --version ]
                [ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
                [ --time-stamp-precision precision ] [ --micro ] [ --nano ]
                [ -z postrotate-command ] [ -Z user ] [ expression ]
```

TCPDump

- **針對 eth0 進行側錄**

  -tcpdump -i eth0
- **針對 Port 22**

  -tcpdump -i eth1 port 22
- **儲存封包**

  -tcpdump -i eth1 -w /tmp/packet.pcap

TCPDump Capture CheatSheet

- tcpdump -i any
- tcpdump -i eth0
- tcpdump -i eth0 -c 10
- tcpdump –D
- tcpdump -i eth0 -w tcpdump.txt
- tcpdump -i eth0 -c 10 -w tcpdump.pcap tcp
- tcpdump -i eth0 port 80

TCPDump Capture CheatSheet

- tcpdump host 192.168.1.100
- tcpdump net 10.1.1.0/16
- tcpdump src 10.1.1.100
- tcpdump dst 10.1.1.100
- tcpdump http

分析及識別異常行為

識別什麼是正常什麼是異常 ，找出入侵軌跡

從檔案角度

-惡意程式
-時間
-建立者
-隱藏/刪除
-惡意程式屬性
-連線

從封包角度

-IP
-Domain
-Url
-行為

從日誌角度

- 時間
- 來源/目的
- 行爲分析
- 關聯分析

從情資角度

-IP
-Domain
-Url
-行為

分析檔案

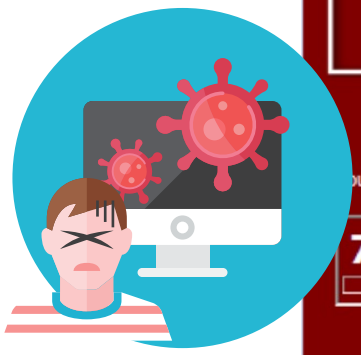
- 計算Hash Value
- 資源回收桶
- 檔案刪除
- 權限、使用者、時間

識別惡意程式-1

◆Ransomware

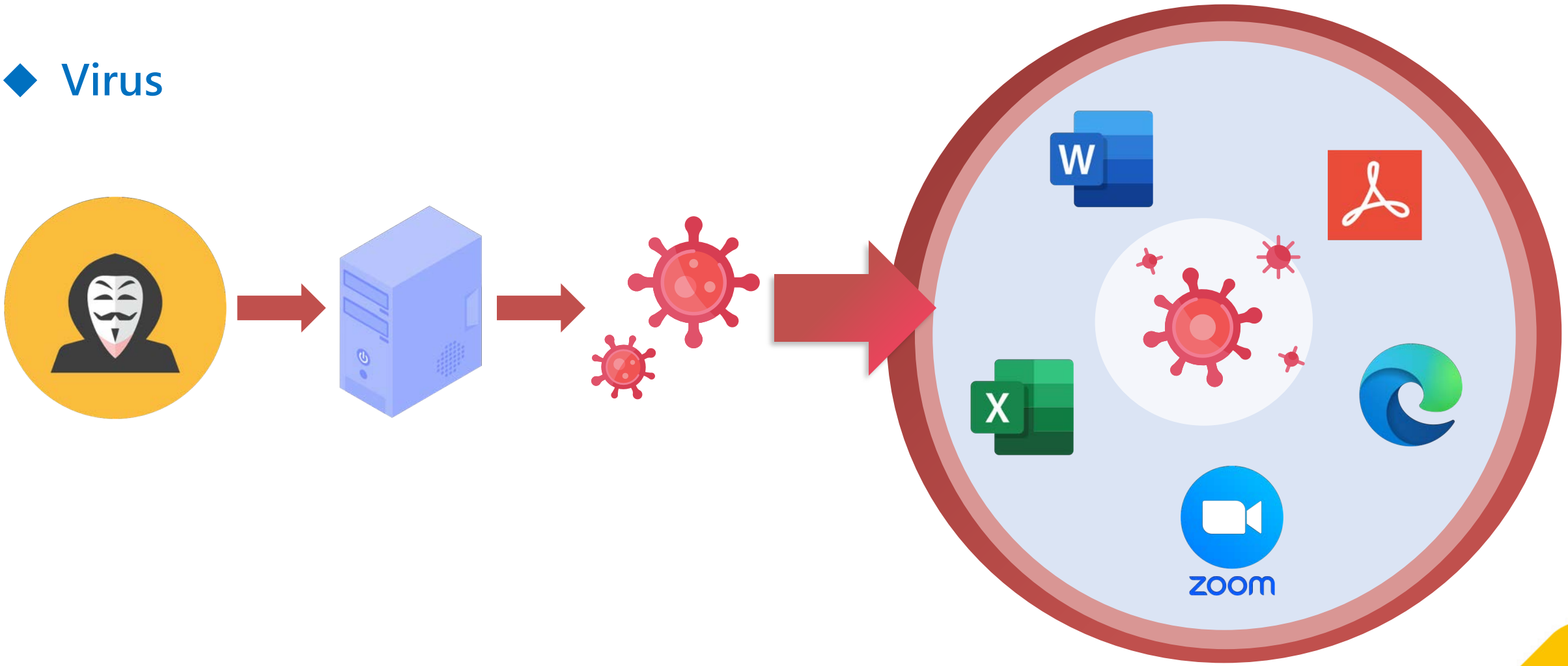
\ 散佈Ransomware /

郵件社交工程



識別惡意程式-2

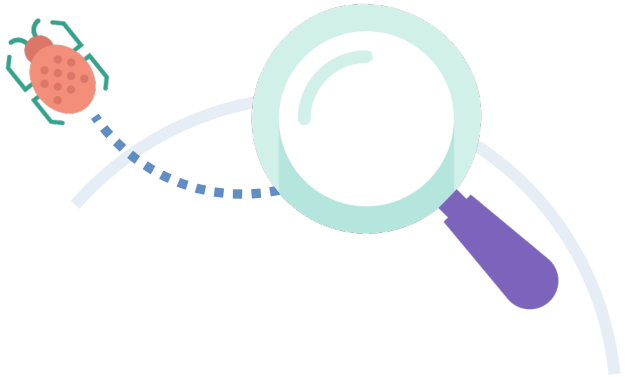
- Virus

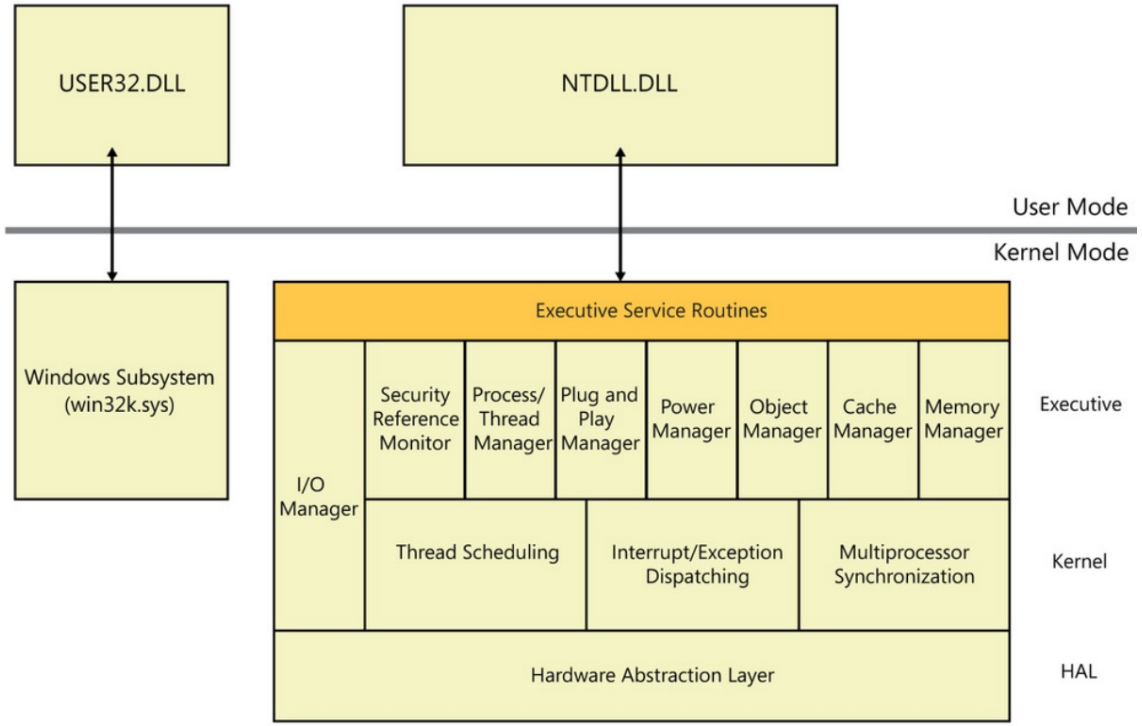


識別惡意程式-3

◆ Rootkit

- 可分為 User Mode和 Kernel Mode
- 具有高權限執行模式
- 隱藏足跡不易被發現



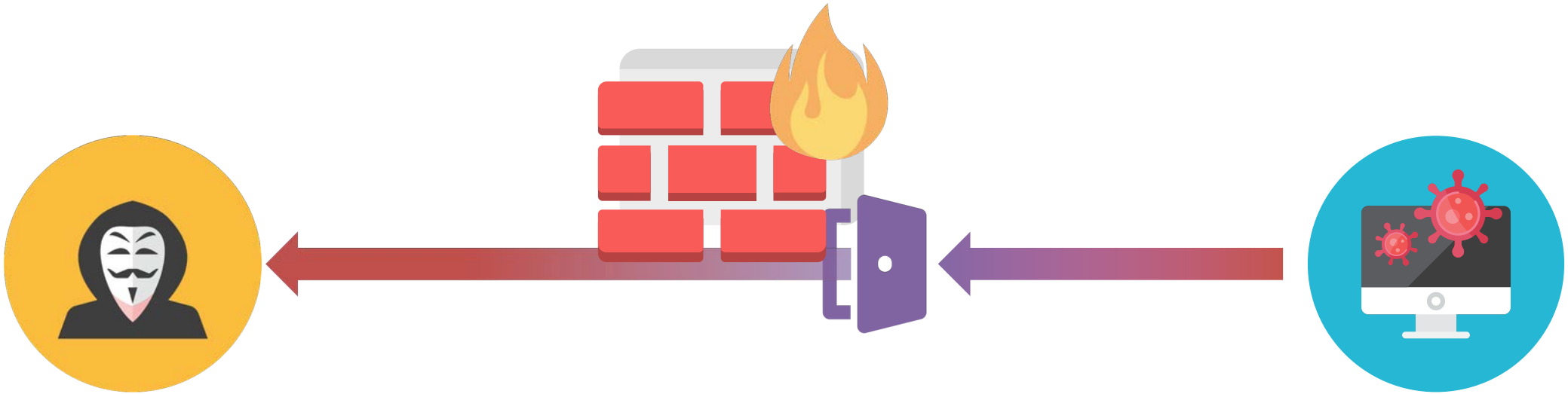


識別惡意程式-4

- Trojan
  - 偽裝正常程式
  - 不易被察覺(Downloader)
  - 具有C&C、Keylogger和竊取各種私有資訊

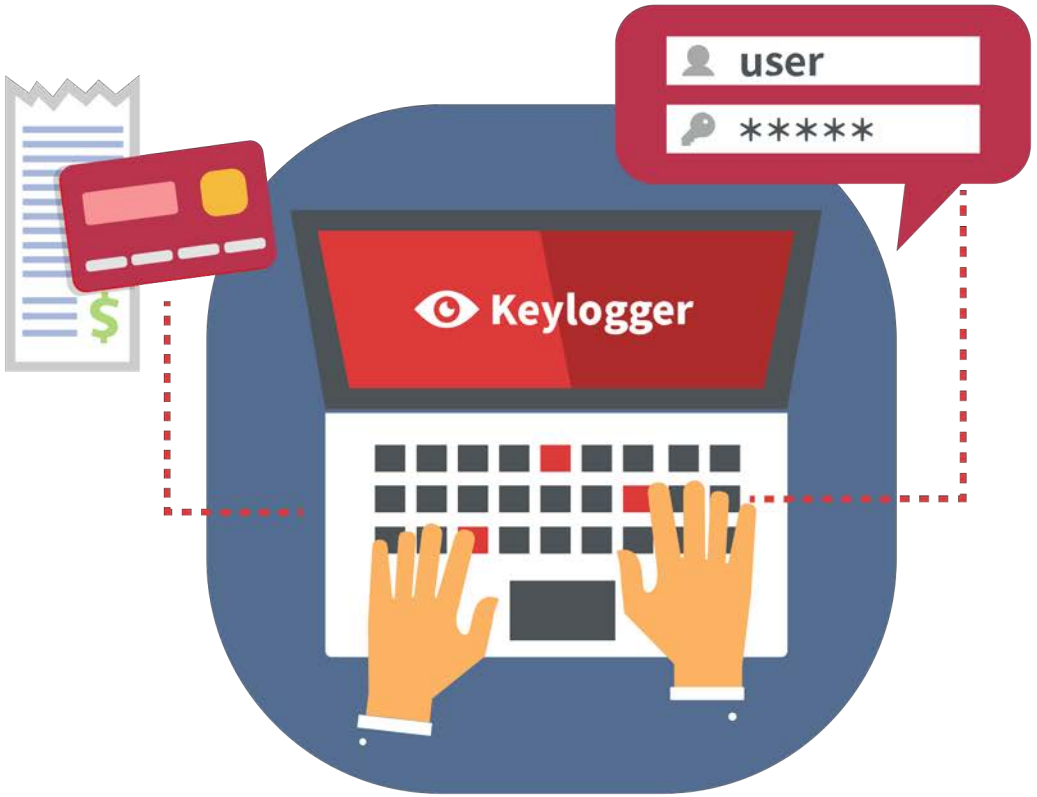
識別惡意程式-5

- Backdoor



識別惡意程式-6

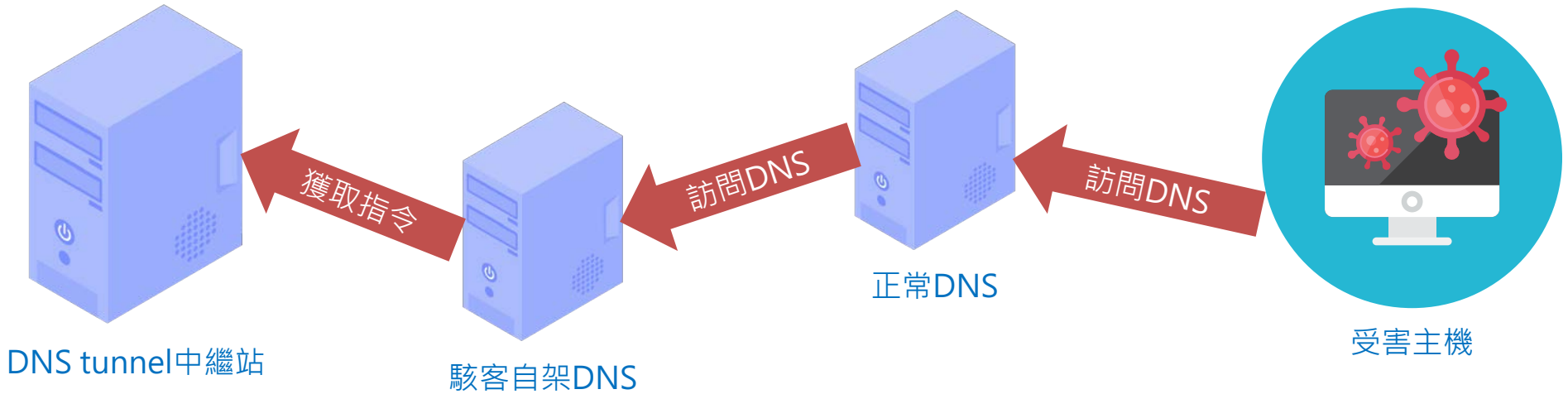
- Keylogger
  - 獲取受駭者的鍵盤輸入資訊
  - 竊取信用卡資訊
  - 竊取各種隱私
  - 螢幕側錄



識別惡意程式-7

- **DNS tunnel**
  - 透過DNS協定傳送資料
  - 不易阻擋
  - Sub-domain會特別長

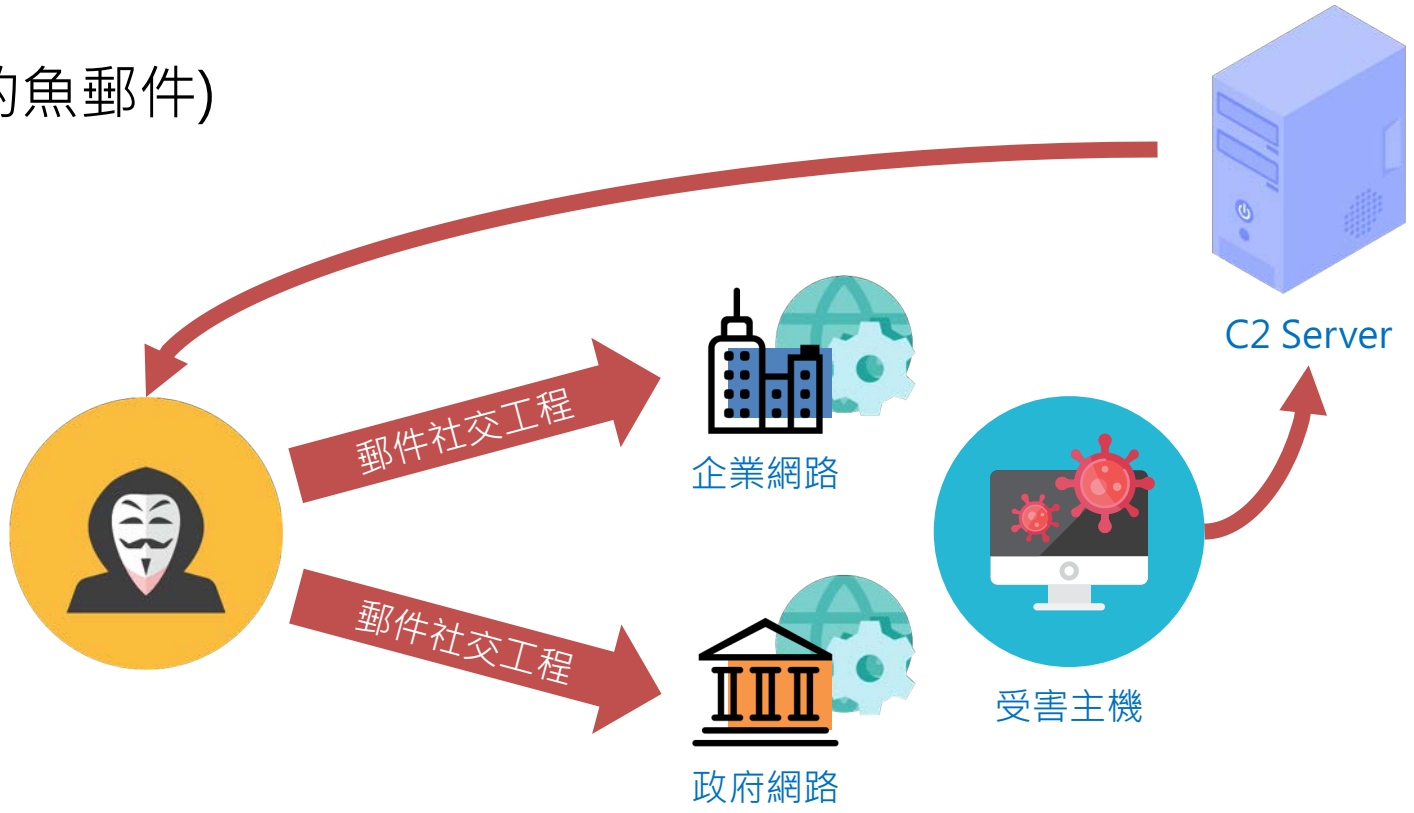
```
response 0x40f4 A api.9.hicloud.h1net.net A 255.255.255.255
response 0x54a5 A api.9.hicloud.h1net.net A 255.255.255.255
0x4b64 A www.994.hicloud.h1net.net
0x5948 A www.994.hicloud.h1net.net
response 0x5948 A www.994.hicloud.h1net.net A 8.8.8.8
response 0x4b64 A www.994.hicloud.h1net.net A 8.8.8.8
0x96a1 A post.57696e646f773204950204 36f6e6669677572617469 6f6e0d.hicloud.h1ne…
0xa897 A post.57696e646f773204950204 36f6e6669677572617469 6f6e0d.hicloud.h1ne…
response 0xa897 A post.57696e646f773204950204 36f6e6669677572617469 6f6e0d.hic…
response 0x96a1 A post.57696e646f773204950204 36f6e6669677572617469 6f6e0d.hic…
0xeeba A post.0a0d0a0d0a4574686572 6e6574206164617074657220457468.hicloud.h1ne…
0x13af A post.0a0d0a0d0a4574686572 6e6574206164617074657220457468.hicloud.h1ne…
response 0x13af A post.0a0d0a0d0a4574686572 6e6574206164617074657220457468.hic…
response 0xeeba A post.0a0d0a0d0a4574686572 6e6574206164617074657220457468.hic…
```



識別惡意程式-8

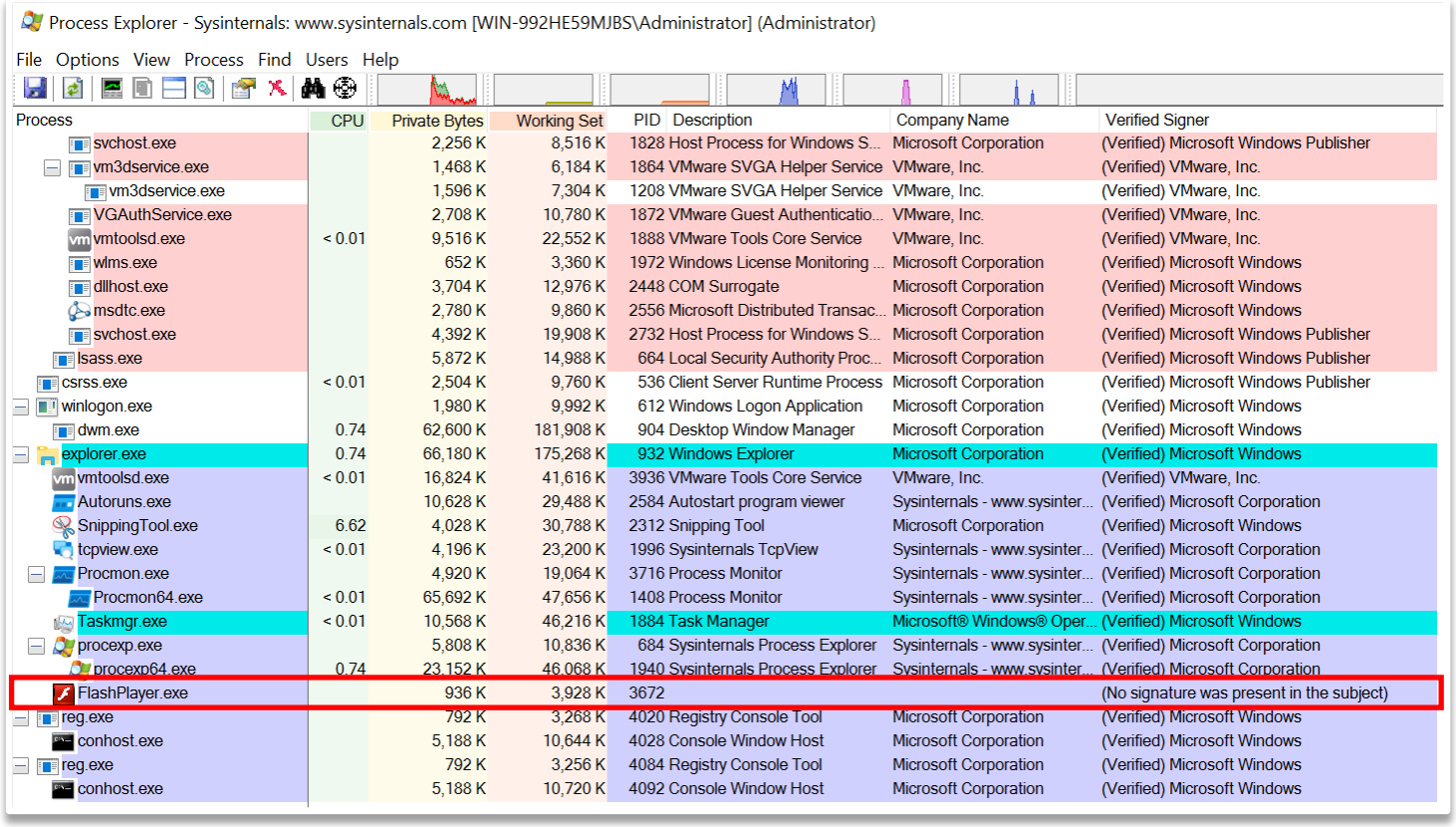
◆ Advanced persistent threat (APT) Attack

- 攻擊政府或企業網路
- 經常使用社交工程(釣魚郵件)
- 竊取各種重要情資



Process Explorer

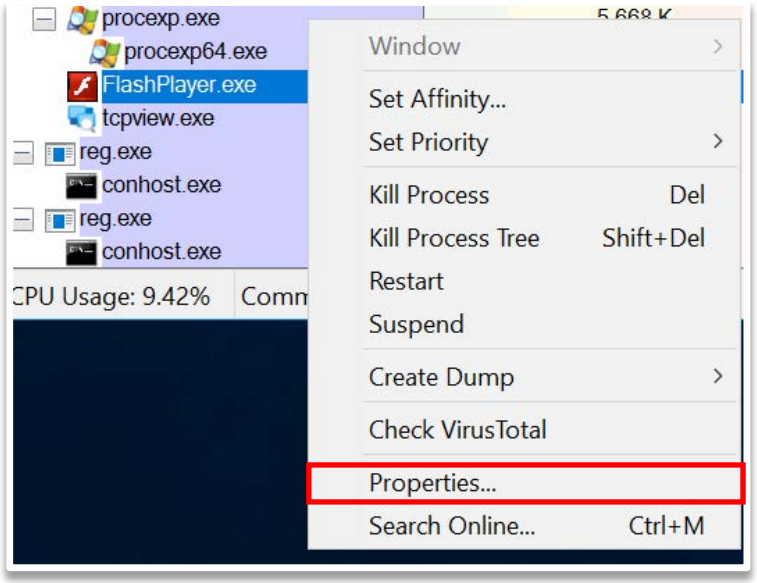
- 利用 Process Explorer找出可疑未簽章的程式
  - 發現 FlashPlayer.exe並未簽章，疑似冒充 Adobe的 FlashPlayer.exe程式。

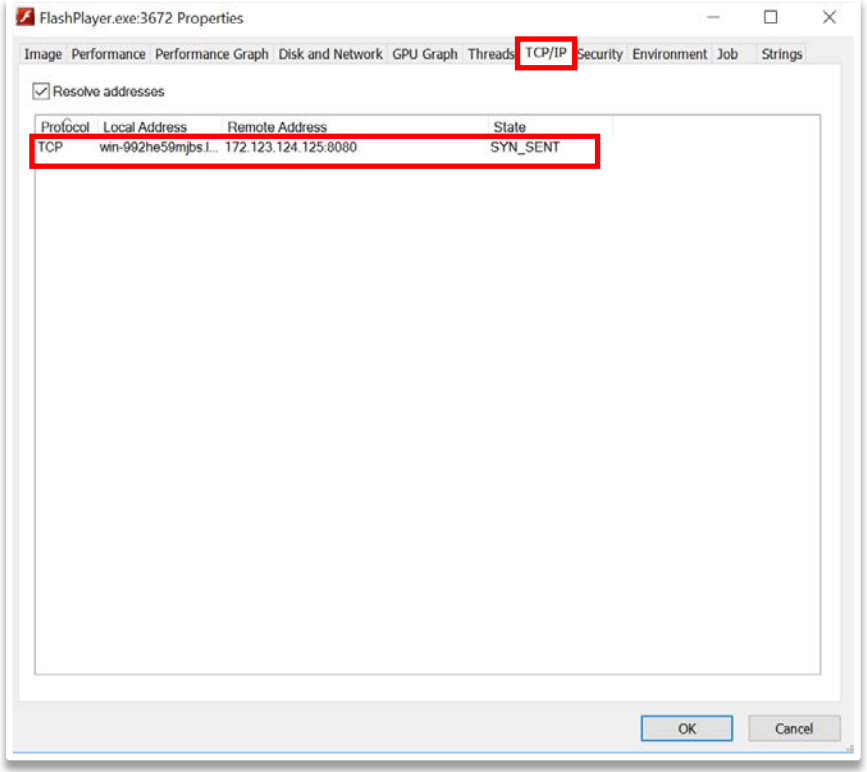


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
svchost.exe		2,256 K	8,516 K	1828	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
vm3dservice.exe		1,468 K	6,184 K	1864	VMware SVGA Helper Service	VMware, Inc.	(Verified) VMware, Inc.
vm3dservice.exe		1,596 K	7,304 K	1208	VMware SVGA Helper Service	VMware, Inc.	(Verified) VMware, Inc.
VGAuthService.exe		2,708 K	10,780 K	1872	VMware Guest Authenticatio...	VMware, Inc.	(Verified) VMware, Inc.
vmtoolsd.exe	< 0.01	9,516 K	22,552 K	1888	VMware Tools Core Service	VMware, Inc.	(Verified) VMware, Inc.
wlms.exe		652 K	3,360 K	1972	Windows License Monitoring ...	Microsoft Corporation	(Verified) Microsoft Windows
dllhost.exe		3,704 K	12,976 K	2448	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows
msdtc.exe		2,780 K	9,860 K	2556	Microsoft Distributed Transac...	Microsoft Corporation	(Verified) Microsoft Windows
svchost.exe		4,392 K	19,908 K	2732	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
lsass.exe		5,872 K	14,988 K	664	Local Security Authority Proc...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
csrss.exe	< 0.01	2,504 K	9,760 K	536	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows Publisher
winlogon.exe		1,980 K	9,992 K	612	Windows Logon Application	Microsoft Corporation	(Verified) Microsoft Windows
dwm.exe	0.74	62,600 K	181,908 K	904	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows
explorer.exe	0.74	66,180 K	175,268 K	932	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows
vmtoolsd.exe	< 0.01	16,824 K	41,616 K	3936	VMware Tools Core Service	VMware, Inc.	(Verified) VMware, Inc.
Autoruns.exe		10,628 K	29,488 K	2584	Autostart program viewer	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
SnippingTool.exe	6.62	4,028 K	30,788 K	2312	Snipping Tool	Microsoft Corporation	(Verified) Microsoft Windows
tcpview.exe	< 0.01	4,196 K	23,200 K	1996	Sysinternals TcpView	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
Procmon.exe		4,920 K	19,064 K	3716	Process Monitor	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
Procmon64.exe	< 0.01	65,692 K	47,656 K	1408	Process Monitor	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
Taskmgr.exe	< 0.01	10,568 K	46,216 K	1884	Task Manager	Microsoft® Windows® Oper...	(Verified) Microsoft Windows
procexp.exe		5,808 K	10,836 K	684	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
procexp64.exe	0.74	23,152 K	46,068 K	1940	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft Corporation
FlashPlayer.exe		936 K	3,928 K	3672			(No signature was present in the subject)
reg.exe		792 K	3,268 K	4020	Registry Console Tool	Microsoft Corporation	(Verified) Microsoft Windows
conhost.exe		5,188 K	10,644 K	4028	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows
reg.exe		792 K	3,256 K	4084	Registry Console Tool	Microsoft Corporation	(Verified) Microsoft Windows
conhost.exe		5,188 K	10,720 K	4092	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows

Process Explorer

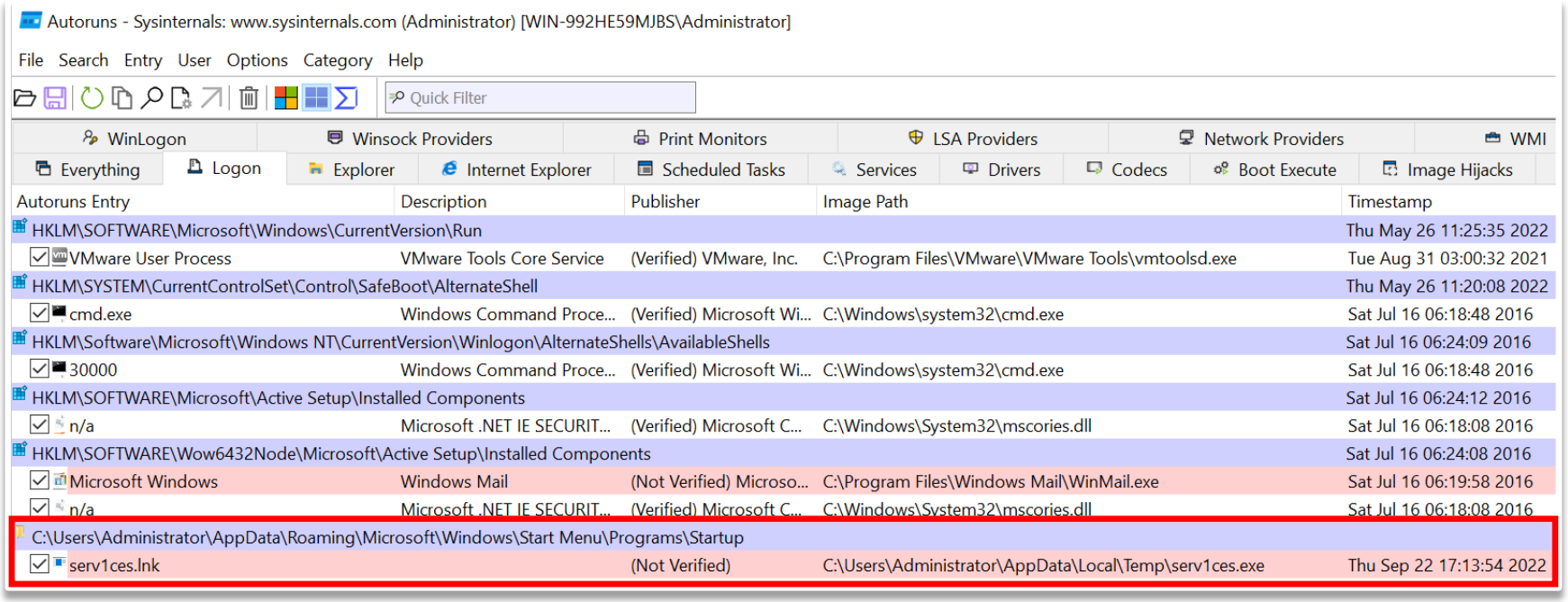
- 透過 Process Explorer分析連線資訊
  - 我們可以在 TCP/IP的欄位查看此程式是否有嘗試連到外網伺服器。
  - 發現程式會連到 172.123.124.125:8080。





Autoruns

- 利用Autoruns可以找出有哪些程式是自動開機執行，因為大多數惡意程式需要直接或間接被執行，所以觀察Autoruns是找出惡意程式的其中一個方法。
- serv1ces.lnk是可疑程式，可以進一步分析。



練習

- 請嘗試分析一下此電腦正在運行的惡意程式完整路徑。(答案有分大小寫)
- 請嘗試分析一下該惡意程式連線至的中繼站IP及Port，假設答案為8.8.8.8 Port 53，則回答8.8.8.8:53 。
- 請分析一下駭客使用什麼方法讓該惡意程式每次重開機都進行重新啟動，請回答MITRE ATT&CK ID編號，需回答Other sub-techniques。英文字請以大寫為主（答案格式：TXXXX.XXX)。

從檔案角度

-惡意程式
-時間
-建立者
-隱藏/刪除
-惡意程式屬性
-連線

從封包角度

-IP
-Domain
-Url
-行為

從日誌角度

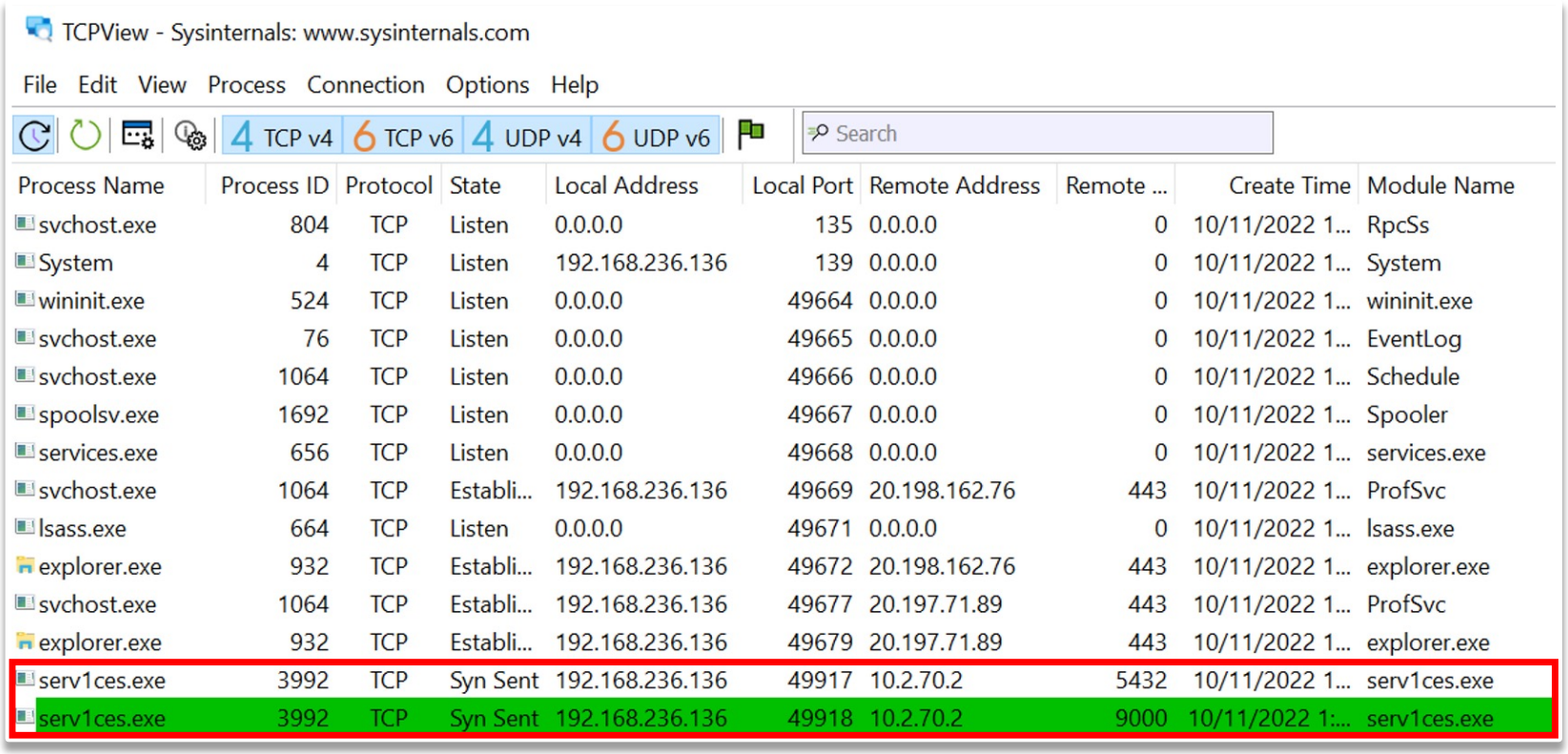
- 時間
- 來源/目的
- 行爲分析
- 關聯分析

從情資角度

-IP
-Domain
-Url
-行為

TCPView

- 利用TCPView找出可疑的連線程式
  - 遠端IP 10.2.70.2:5432
  - 遠端IP 10.2.70.2:9000



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote ...	Create Time	Module Name
svchost.exe	804	TCP	Listen	0.0.0.0	135	0.0.0.0	0	10/11/2022 1...	RpcSs
System	4	TCP	Listen	192.168.236.136	139	0.0.0.0	0	10/11/2022 1...	System
wininit.exe	524	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	10/11/2022 1...	wininit.exe
svchost.exe	76	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	10/11/2022 1...	EventLog
svchost.exe	1064	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	10/11/2022 1...	Schedule
spoolsv.exe	1692	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	10/11/2022 1...	Spooler
services.exe	656	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	10/11/2022 1...	services.exe
svchost.exe	1064	TCP	Establi...	192.168.236.136	49669	20.198.162.76	443	10/11/2022 1...	ProfSvc
lsass.exe	664	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	10/11/2022 1...	lsass.exe
explorer.exe	932	TCP	Establi...	192.168.236.136	49672	20.198.162.76	443	10/11/2022 1...	explorer.exe
svchost.exe	1064	TCP	Establi...	192.168.236.136	49677	20.197.71.89	443	10/11/2022 1...	ProfSvc
explorer.exe	932	TCP	Establi...	192.168.236.136	49679	20.197.71.89	443	10/11/2022 1...	explorer.exe
serv1ces.exe	3992	TCP	Syn Sent	192.168.236.136	49917	10.2.70.2	5432	10/11/2022 1...	serv1ces.exe
serv1ces.exe	3992	TCP	Syn Sent	192.168.236.136	49918	10.2.70.2	9000	10/11/2022 1:...	serv1ces.exe

Wireshark

- **分析**
  - Follow TCP Stream
  - 透過 TCP Stream 觀察到應用程式層 (Application Layer) 流量
  - 流量資料的瑞士刀！
- **統計**
  - Conversations
  - 分別將資料、時間、通訊埠 (protocol) 區分顯示
- **過濾**

Wireshark Cheat Sheet

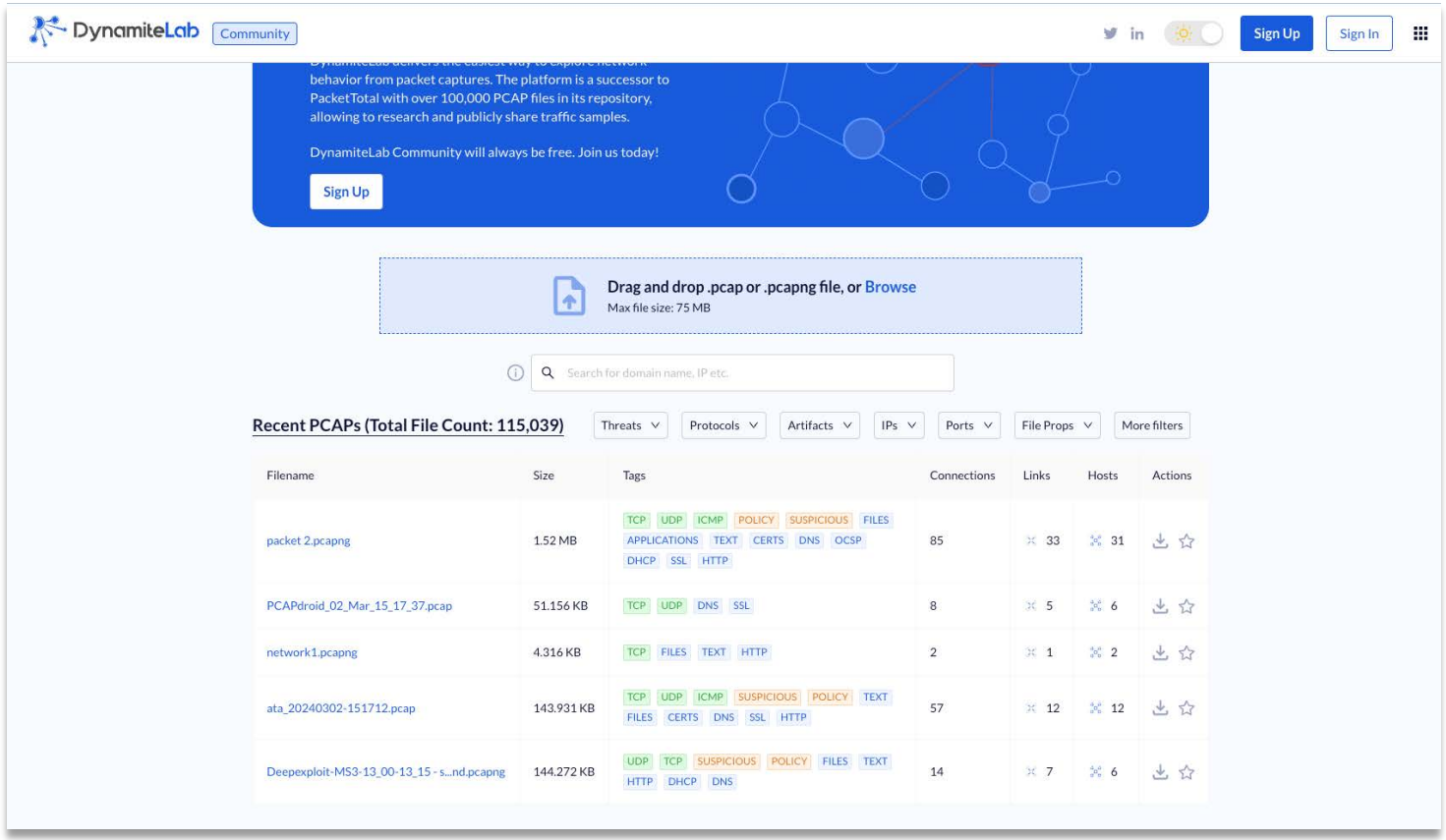
Logical Operators

OPERATOR	DESCRIPTION	EXAMPLE
and or &&	Logical AND	All the conditions should match
or or ||	Logical OR	Either all or one of the conditions should match
xor or ^^	Logical XOR	Exclusive alterations - only one of the two conditions should match not both
not or !	Not (Negation)	Not equal to
[n] [...]	Substring operator	Filter a specific word or text

https://www.stationx.net/wireshark-cheat-sheet/

PacketTotal

- 以線上服務方式提供網路封包分析
  - https://lab.dynamite.ai/



練習

- 請嘗試分析 惡意程式樣本(40545f66ad0d3b96d4ea0348a705d15c)中的 droiddddddOnline.pcap ，請問總共有幾個Hosts
- 請嘗試分析惡意程式樣本(40545f66ad0d3b96d4ea0348a705d15c)中的 droiddddddOnline.pcap ，請問駭客是透過什麼協定傳檔案html到遠端主機
- 請嘗試分析惡意程式樣本(40545f66ad0d3b96d4ea0348a705d15c)中的 droiddddddOnline.pcap droiddddddOnline.pcap ，請問傳送過程中有使用什麼帳號密碼？

從檔案角度

-惡意程式
-時間
-建立者
-隱藏/刪除
-惡意程式屬性
-連線

從封包角度

-IP
-Domain
-Url
-行為

從日誌角度

- 時間
- 來源/目的
- 行爲分析
- 關聯分析

從情資角度

-IP
-Domain
-Url
-行為

怎樣才算合格的 Log 紀錄?

- **5W原則**
- **發生什麼事 (What)**
  - 要有適當的細節資訊
- **發生於何時 (When)**
  - 持續了多久?
- **發生於何處 (Where)**
  - 主機名稱、應用程式名稱、port #
- **參與者有誰 (Who)**
  - 參與者來源 (Where)

常見的 Log 協定

- **syslog**
  - syslog, rsyslog, syslog-ng
- **SNMP**
  - Windows Event Log
- **關聯式資料庫**
  - MySQL, PostgresSQL, Oracle
- **NoSQL資料庫**
  - MongoDB

系統日誌儲存格式

- **純文字**
  - Unix syslog
  - XML
  - JSON
  - CSV / TSV
- **Binary格式**
  - Windows Event Log
  - Unix wtmp
  - Tcpdump (pcap)

日誌格式介紹 以Apache為例

日誌格式 — Apache Combined Access Log

- 資料範例

```
236.184.27.219 - - [10/Sep/2016:18:27:10] "GET /product.screen?productId=FL-NYC-44
&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" 200 3930 "http://www.yahoo.com"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 797
```

- 欄位說明

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

  - ✓ 236.184.27.219 (%h)
    - 發出請求的 client IP (remote host)
  - ✓ - (%l)
    - Remote logname，因為容易偽造，所以通常沒人用
  - ✓ - (%u)
    - 對網頁發起要求的 user，因為容易偽造，所以通常沒人用
  - ✓ [10/Sep/2016:18:27:10] (%t)
    - Web server 收到 request 的時間
  - ✓ "GET /product.screen?productId=FL-NYC-44&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" (\"%r\")
    - Client 端發出的要求字串

日誌格式 — Apache Combined Access Log

- 資料範例

```
236.184.27.219 - - [10/Sep/2016:18:27:10] "GET /product.screen?productId=FL-NYC-44
&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" 200 3930 "http://www.yahoo.com"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 797
```

- 欄位說明

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

✓ 200 (%>s)
  - Server 端回覆的狀態碼

✓ 3930
  - 回覆給 client 端的資料大小

✓ "http://www.yahoo.com" (\"%{Referer}i\")
  - 這次呼叫的前一個網頁

✓ "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" (\"%{User-agent}i\")
  - 使用者使用的瀏覽器資訊

✓ 797 (?)
  - 標準規範以外的其他資訊

主要的網頁程式

```
"GET /product.screen?productId=FL-NYC-44&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1"
```

- /product.screen
  - ✓ 網頁程式名稱
- productId
  - ✓ 參數名稱: 商品代碼
  - ✓ FL-NYC-44
- JSESSIONID
  - ✓ JSP (Java) 用來記錄對話 Session 的代碼
  - ✓ CA10MO3AZ7USANA5006

網頁程式名稱

```
"GET /product.screen?productId=FL-NYC-44&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1"
```

- /product.screen
  - ✓顯示商品資訊
- /category.screen
  - ✓顯示商品類別資訊
- /cart.do
  - ✓購物車操作指令
- /cart/success.do
  - ✓回覆確認購物車操作成功

Linux 常用分析指令介紹

指令 vi / vim

- vi:
  - ✓ 文字編輯器
  - ✓ vim: 程式開發編輯器
- 用 / 進行 [尋找]
  - ✓ 找下一個: n
  - ✓ 找前一個: N
- 載入超大檔案?
- 數位採證的證據力?

```
$ vim /var/log/auth.log

/COMMAND
```

指令 cat / more / less

- cat: 將檔案內容輸出到螢幕 (stdout)
- more:
  - ✓ 提供換下一頁功能 (空白鍵)
  - ✓ 用 / 進行 [尋找]
  - ✓ 結束後，按下 q 跳出
- less:
  - ✓ more 的加強版
  - ✓ 提供往回翻頁功能
  - ✓ 可用鍵盤方向鍵控制

```
$ cat /var/log/auth.log

$ more /var/log/auth.log
$ cat /var/log/auth.log | more

$ less /var/log/auth.log
$ cat /var/log/auth.log | less
```

指令 wc / nl

- wc: 計算檔案中下列數量
  - ✓ 換行
    wc -l / wc --lines
  - ✓英文單字
    wc -w / wc --words
  - ✓Byte 數
    wc -c / wc –bytes
- nl: line numbering filter
  - ✓ 在每一行前面加上行號

```
$ wc -l /etc/passwd

$ cat /etc/passwd | wc -l

$ nl /etc/passwd
$ cat /etc/passwd | nl
```

指令 head / tail

- 可處理超大檔案
- head:
  - ✓ 預設為檔案開頭的前 10行
  - ✓ 指定前3行: head -n 3 / head -3
- tail:
  - ✓ 預設為檔案尾端的最後10行
  - ✓ 指定最後3行: tail -n 3 / tail -3
  - ✓ 持續監視新增的資料: tail -f

```
$ head /etc/passwd

$ head -n 3 /etc/passwd
$ tail -n 3 /etc/passwd

$ tail -f /var/log/auth.log
$ sudo echo 'Hello world'
```

指令 sort / uniq

- sort:
  - ✓預設為字典排序 (文字排序)
  - ✓以數值方式排序
  - ✓反向排序
  - ✓去除重複

```
$ ls -al /var/log/ | awk '{print $5, $9}' | sort
$ ls -al /var/log/ | awk '{print $5, $9}' | sort -n
$ ls -al /var/log/ | awk '{print $5, $9}' | sort -r
$ ls -al /var/log/ | awk '{print $5}' | sort -u
```

- uniq:
  - ✓過濾重複出現的資料，還可以計算重複次數

```
$ ls -al /var/log/ | awk '{print $5}' | sort -n | uniq -c
```

日誌分析

- 日誌分析前請先了解目前發生的**現況**
- 理解日誌**所有欄位**的意思(包含成功、失敗、錯誤、警告)
- 建立**調查起始**及**結束時間**
- 必要時需要配合**其他日誌做關聯分析**(如DNS/FW/IPS等)
  - A 日誌、在B設備是否有看到同樣的狀態 ？
- 在做分析時請善用交集/ 聯集/ 差集/ 對稱差集
- 必要時搭配ELK、Graylog 、Splunk及Wazuh等日誌分析軟體

- set1 = {1, 2, 3}
- set2 = {3, 4, 5}

交集：{3}
聯集 ： {1, 2, 3, 4, 5}
差集 ： {1, 2}
對稱差集 ： {1, 2, 4, 5}

日誌行為態樣

- 異常行為
  - 狀態
    - 日誌當中出現**失敗、錯誤、警告**等。
  - 量化
    - 日誌中的一些紀錄出現**大量**紀錄（Ex:網路掃描、密碼破解)
    - 日誌中看到一些**沒看過**的紀錄
  - 時間
    - 人在**非正常**時間（例如下班過後還有連線紀錄
    - 人在**正常**時間 ，**行為異常**
  - 位置
    - IP位置
  - 人
    - 使用者 、帳號

練習

- 請嘗試分析C:\Users\Administrator\Desktop\Log1\webapplogs 日誌當中，駭客的攻擊來源IP 為何？
- 請嘗試分析 C:\Users\Administrator\Desktop\Log1\webapplogs日誌當中，駭客可能使用哪種掃描工具對網頁伺服器主機進行掃描，請回答工具名稱，如有多個請擇一回答即可。
- 請嘗試分析C:\Users\Administrator\Desktop\Log1\webapplogs日誌當中，請問分析看看哪一個頁面有遭疑似遭受到駭客使用SQL Injection 注入攻擊？請回答完整的檔案名稱，如test.php。

從檔案角度

-惡意程式
-時間
-建立者
-隱藏/刪除
-惡意程式屬性
-連線

從封包角度

-IP
-Domain
-Url
-行為

從日誌角度

- 時間
- 來源/目的
- 行爲分析
- 關聯分析

從情資角度

-IP
-Domain
-Url
-行為

談「情資」之前...

https://www.talosintelligence.com/

Thinking...

- 您清楚資安維運需要的情資嗎？
- 您明白情資如何使用嗎？
- 您瞭解情資是有生命週期的嗎？
- 您知道該如何使用情資嗎？
- 您知道在有限的應變時間內，如何有效的運用情資嗎？

資安情資分析

- **利用機器學習分析惡意程式**
  -惡意程式族群
  -IoT
- **社群媒體分析**
  -黑市
  -近期感興趣話題
- **CVE弱點**

情資類型與運用

戰術情資 Tactical intelligence

- IOCs
- Malicious IP, Domain URLs, File hashes

營運情資 Operational intelligence

- Terrorist Tactics, Techniques, and Procedures(TTPs)
- Attack Use Case

戰略情資 Strategic intelligence

- Global Events, Foreign Policies
- Potential events that will impact the cyber security wellness of an organization

SHIELDXTREME

IoC類型 -1

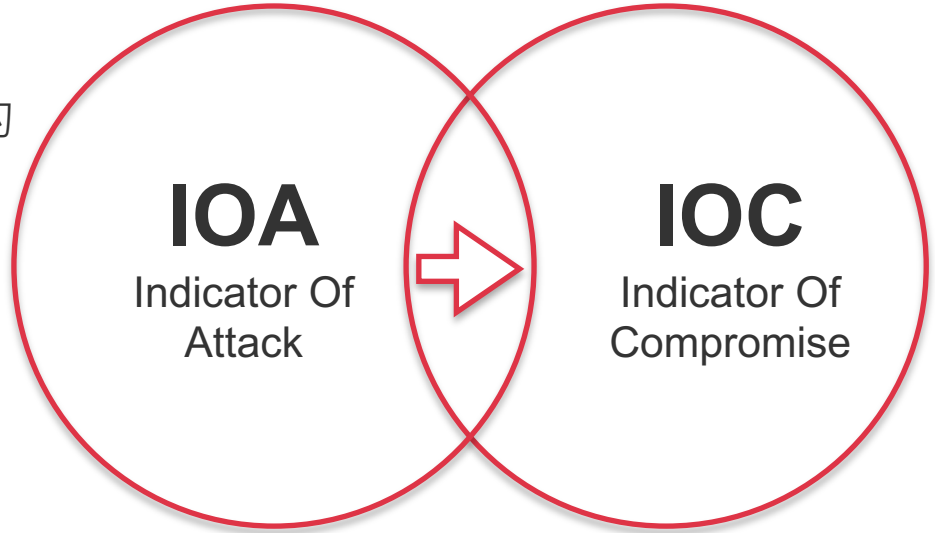
- **基於網路的 IoC:**
  - 惡意 IP 位址、網域或 URL
- **網路流量模式、異常連接埠活動**
  - 與已知惡意主機的連線或資料外流模式
- **基於主機的 IoC:**
  - 工作站或伺服器上的活動，如檔案名稱、雜湊值、登錄機碼
  - 可疑程序

IoC類型 -2

- **基於檔案的 IoC:**
  - 惡意程式碼或指令碼等惡意檔案
- **行為型 IoC:**
  - 可疑的使用者行為、登入模式
  - 網路流量模式和驗證嘗試
- **中繼資料 IoC:**
  - 與檔案或文件相關的中繼資料，如作者、建立日期或版本資訊

情資的分析與運用

- 結構化資料：資料可以被呈現在資料庫table的行、欄。
- 一行(row)代表一筆紀錄，統計的術語稱為觀測(observation)。
- 每個欄位(column)則稱為表徵(characteristics)或變數。
- 因此以統計的術語來說，table資料的每一行或說每一筆紀錄都代表著一次觀測，而一個觀測中每一個欄位都是該觀測的表徵。



資安大數據的資料分析

- 非結構化資料：形式自由且不遵循標準的格式規範，一團沒有組織的數據。
- 非結構化數據的示例包括圖像，音頻，視頻，電子郵件，電子表格和文字處理文檔，實質上是存儲為文件的東西。
- 非結構化數據往往比結構化數據更大，佔用更多存儲空間。

https://ithelp.ithome.com.tw/articles/10200157

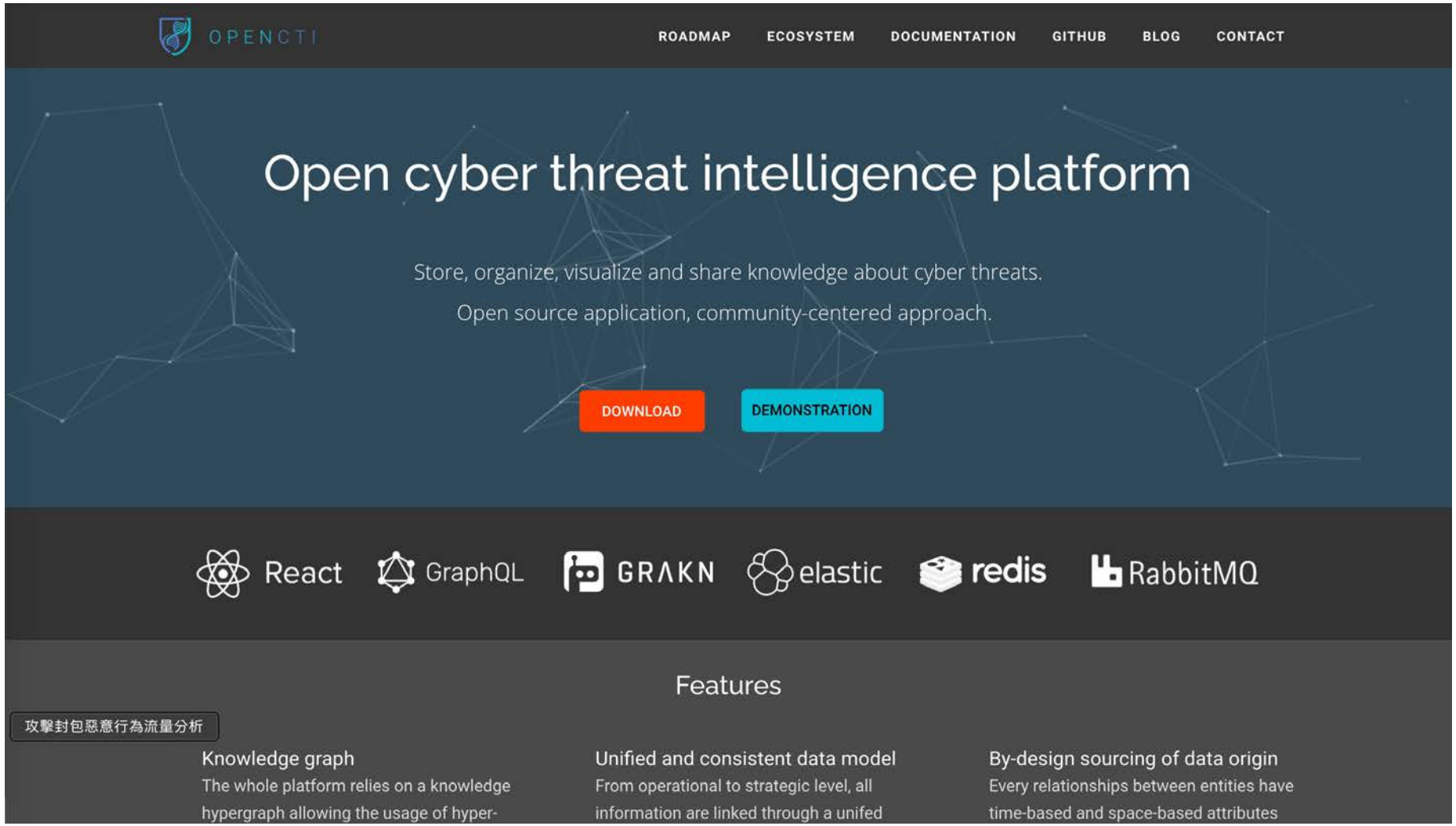
資安威脅情資適用時機

- 想要識別以下資訊
- IP
- Domain
- URL
- HashValue
- Email Address
- …

常見的資安情資平台

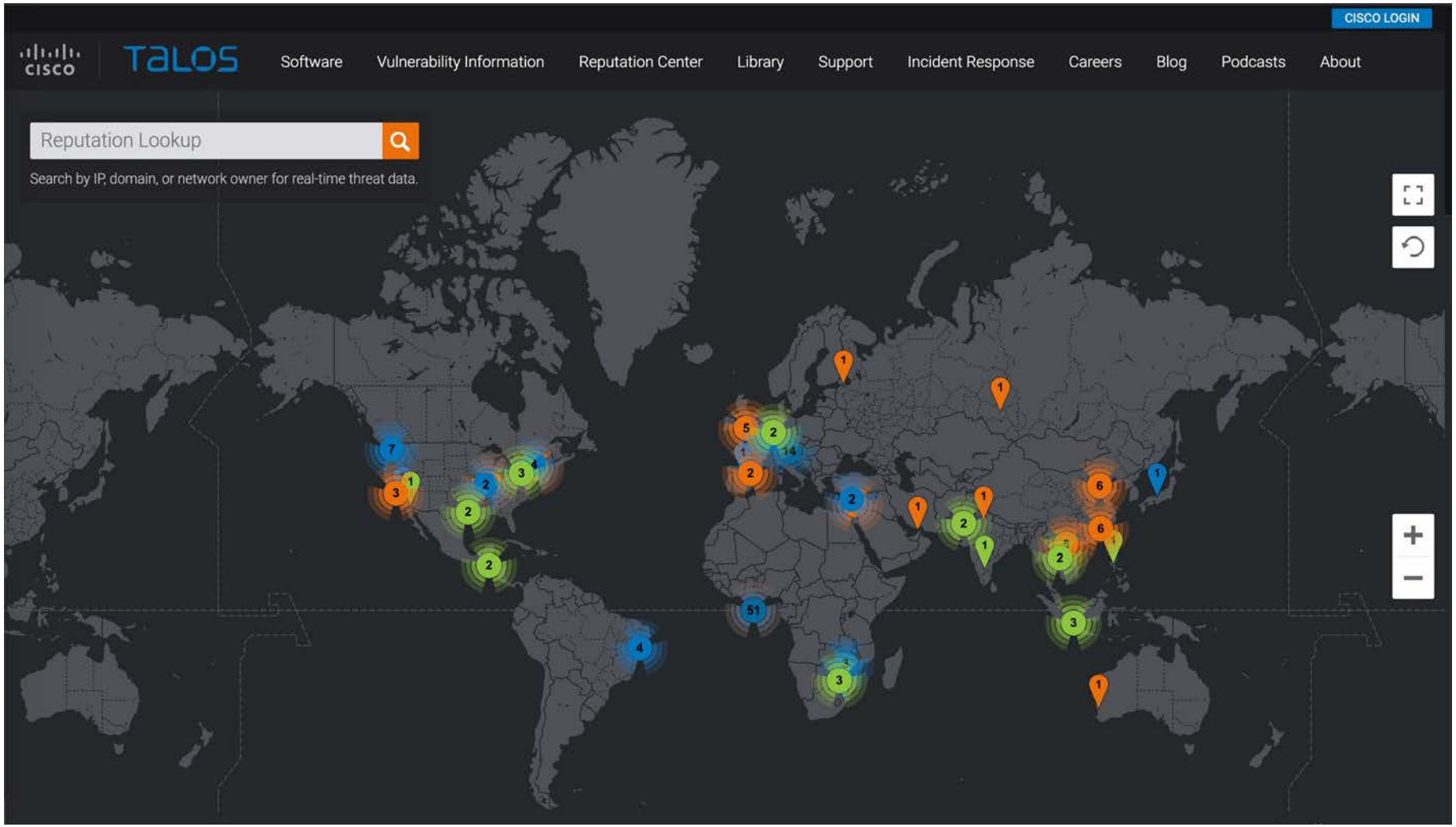
綜合型情資

OpenCTI



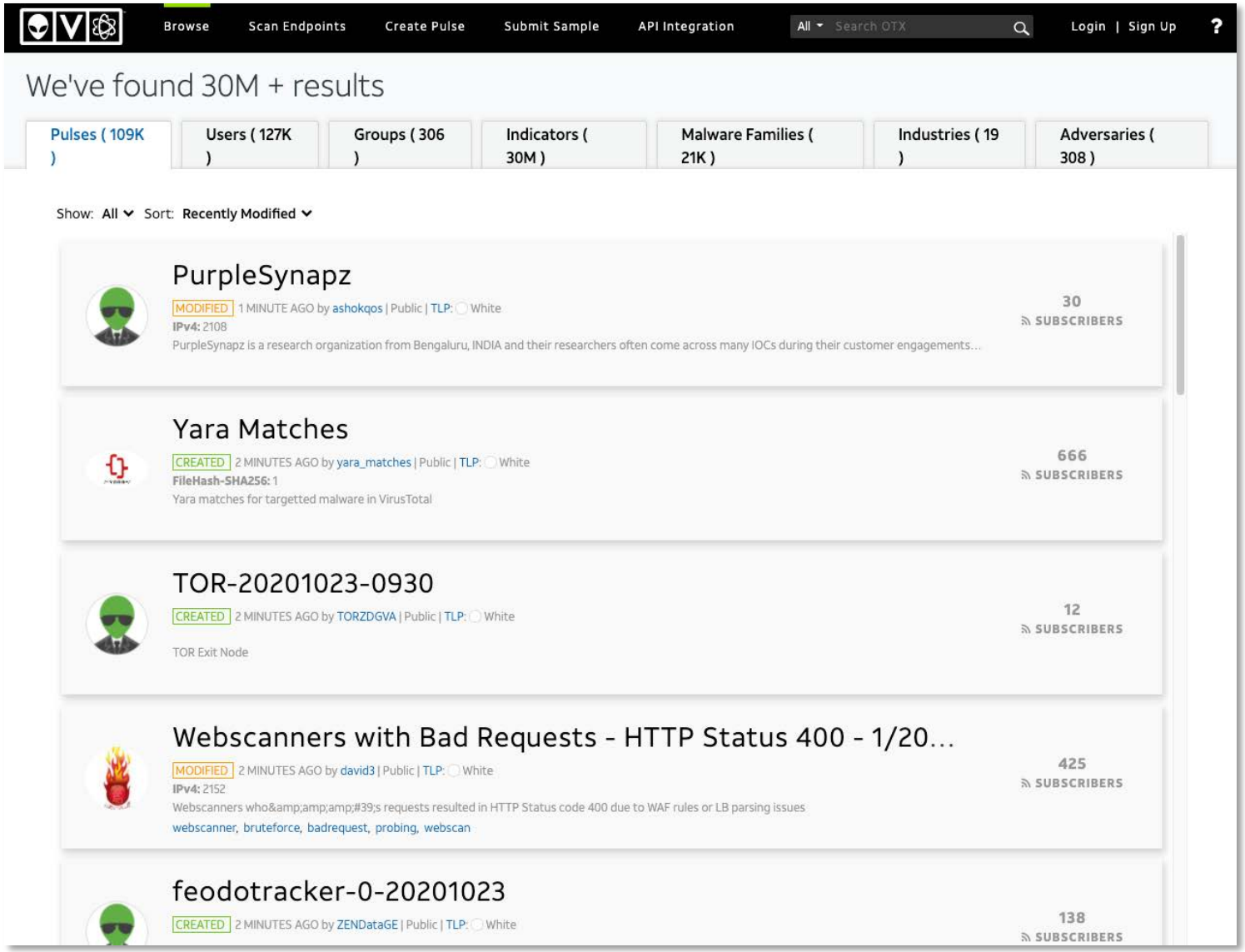
https://www.opencti.io/en/

Cisco Talos



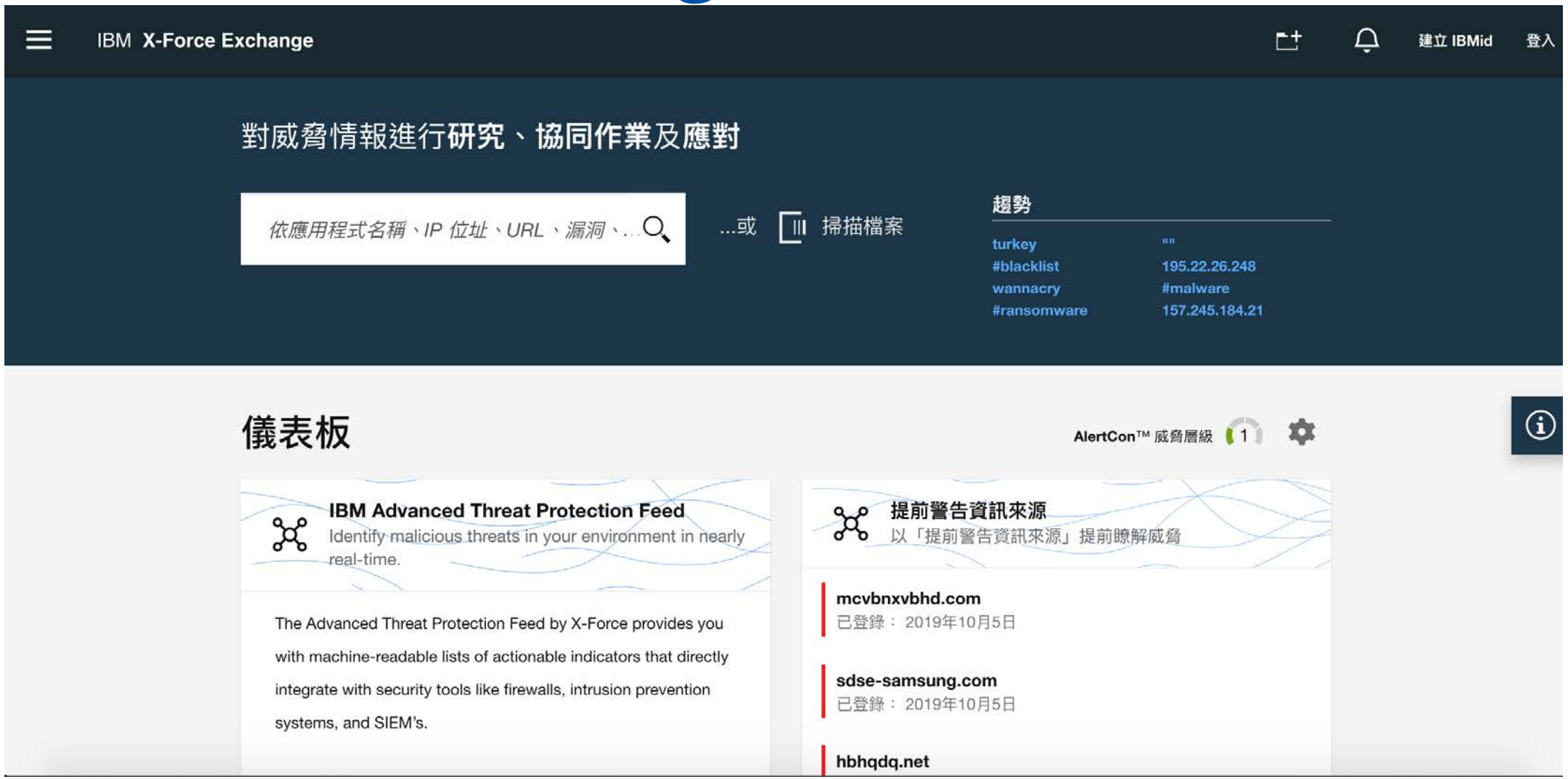
https://talosintelligence.com/

AlienVault



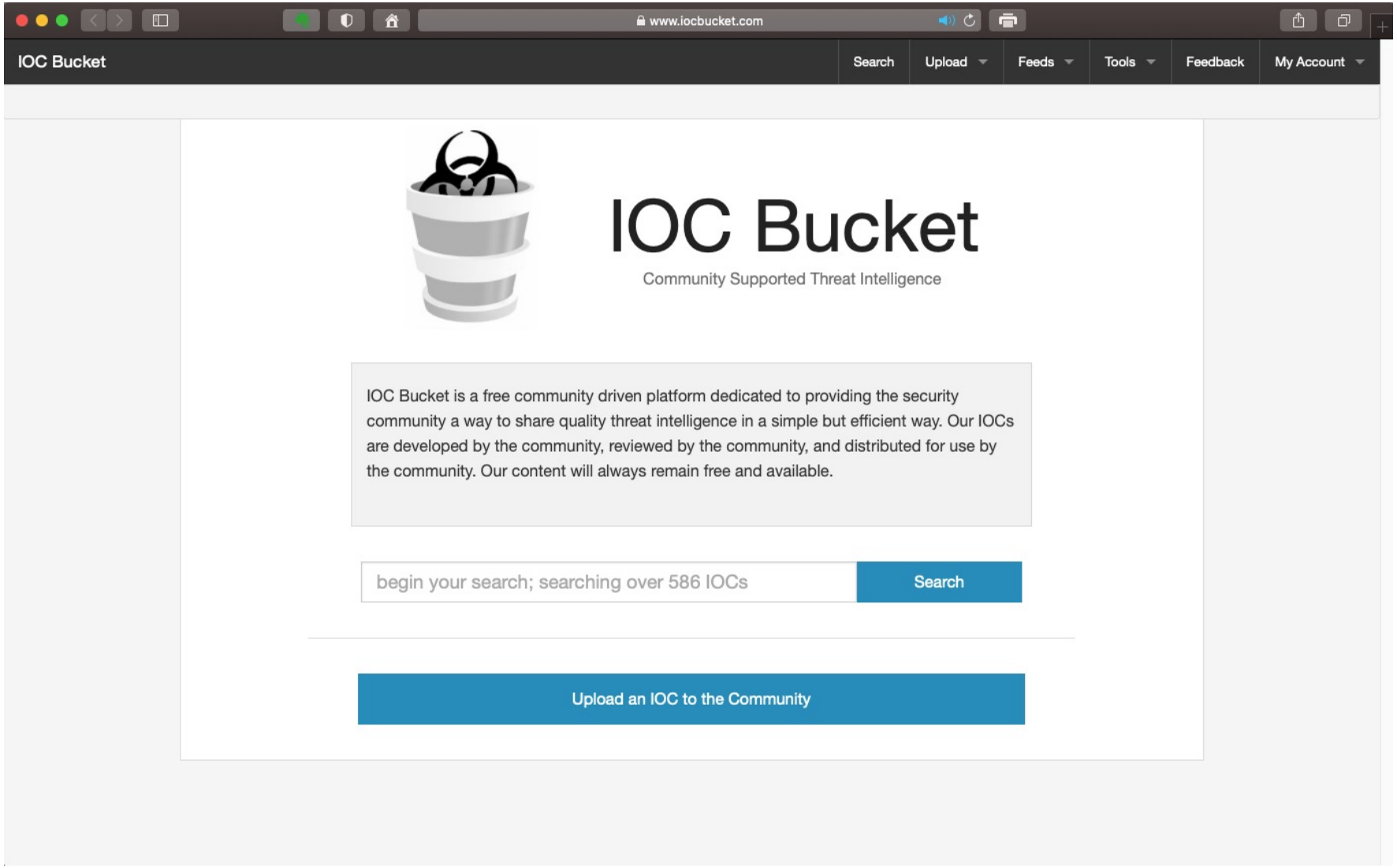
https://otx.alienvault.com/

IBM X-Force Exchange



https://exchange.xforce.ibmcloud.com/

IOC Bucket



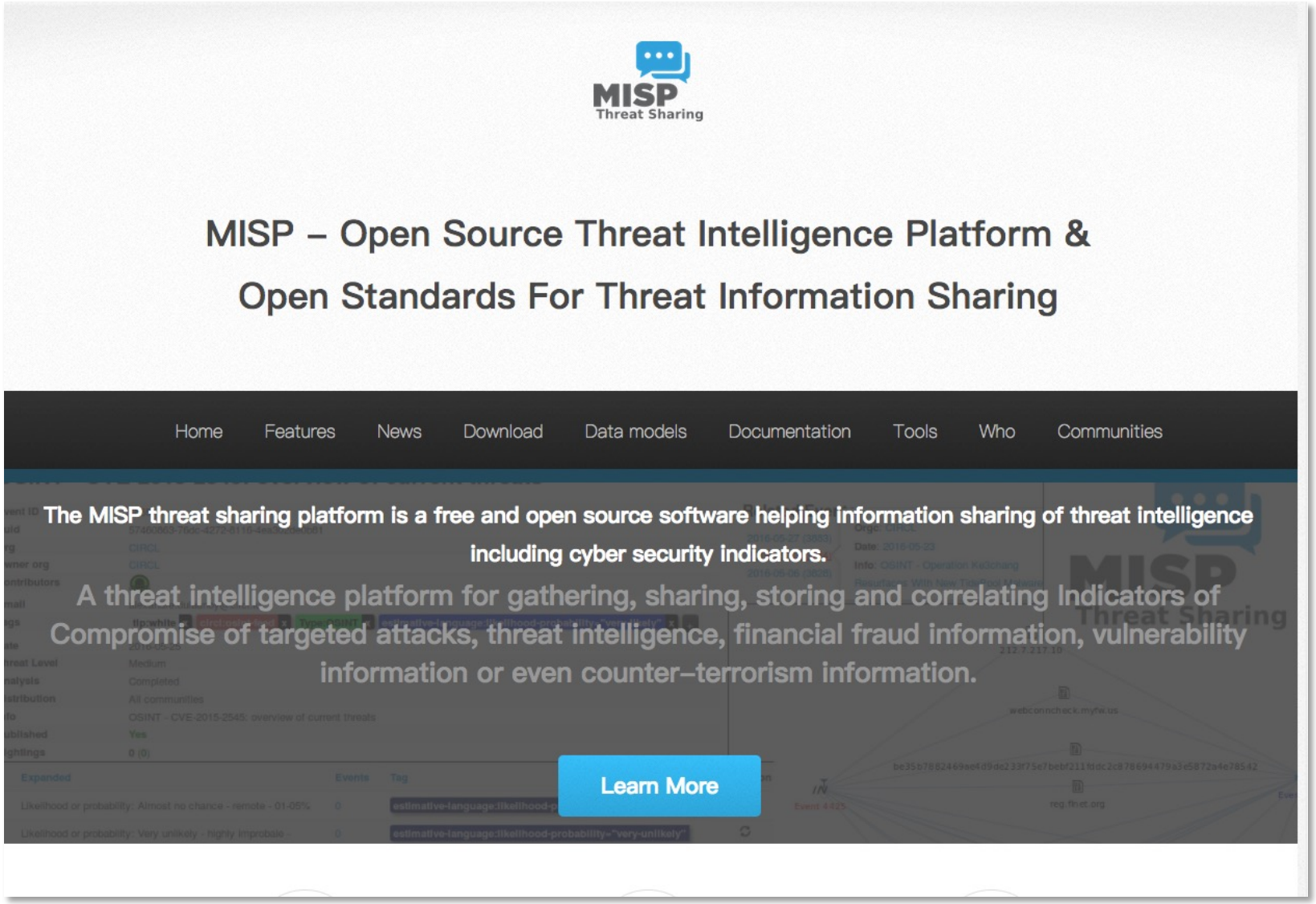
SHIELDXTREME

https://www.iocbucket.com

常見的資安情資平台

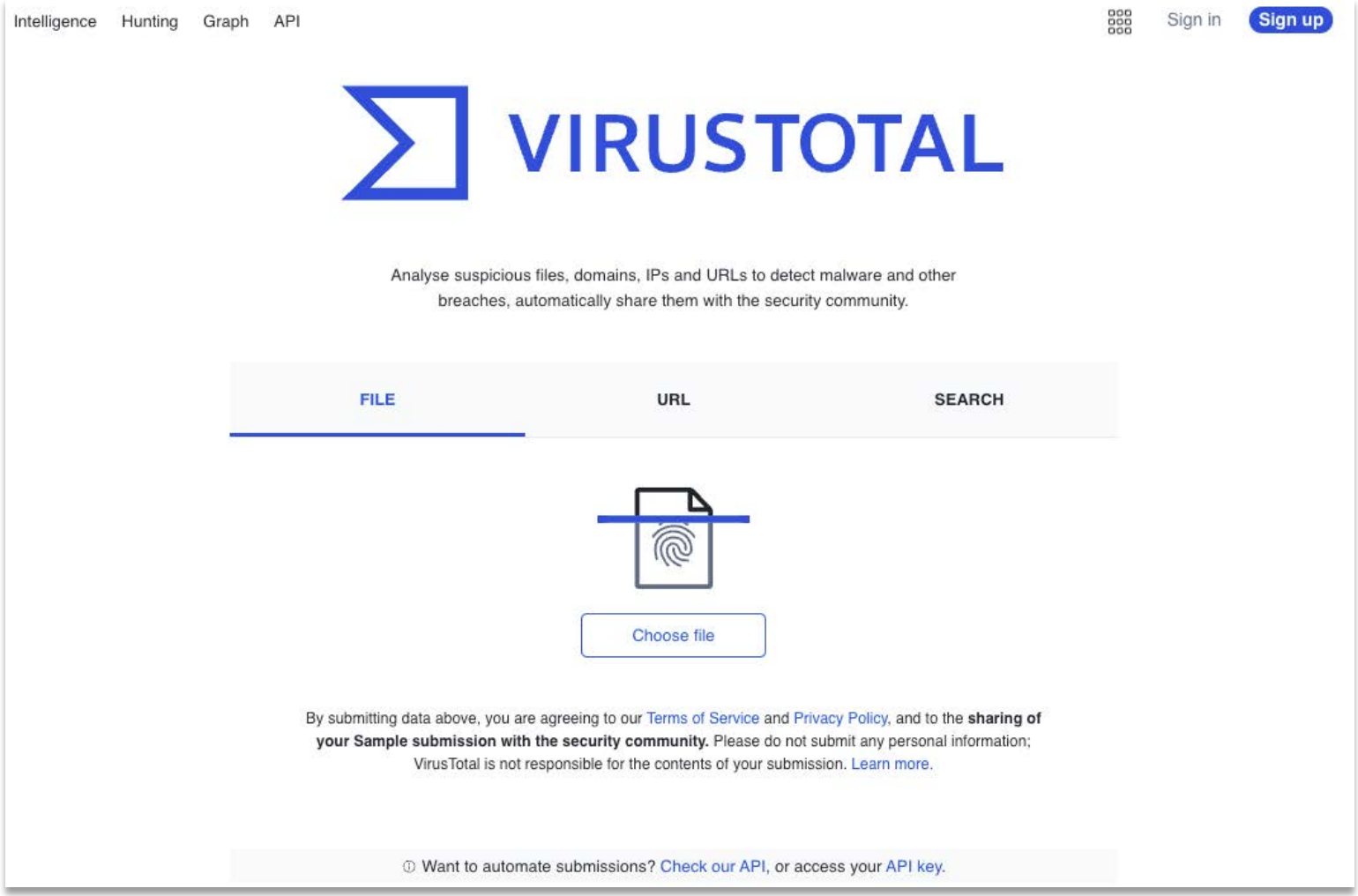
惡意程式類型

MISP公開情資系統



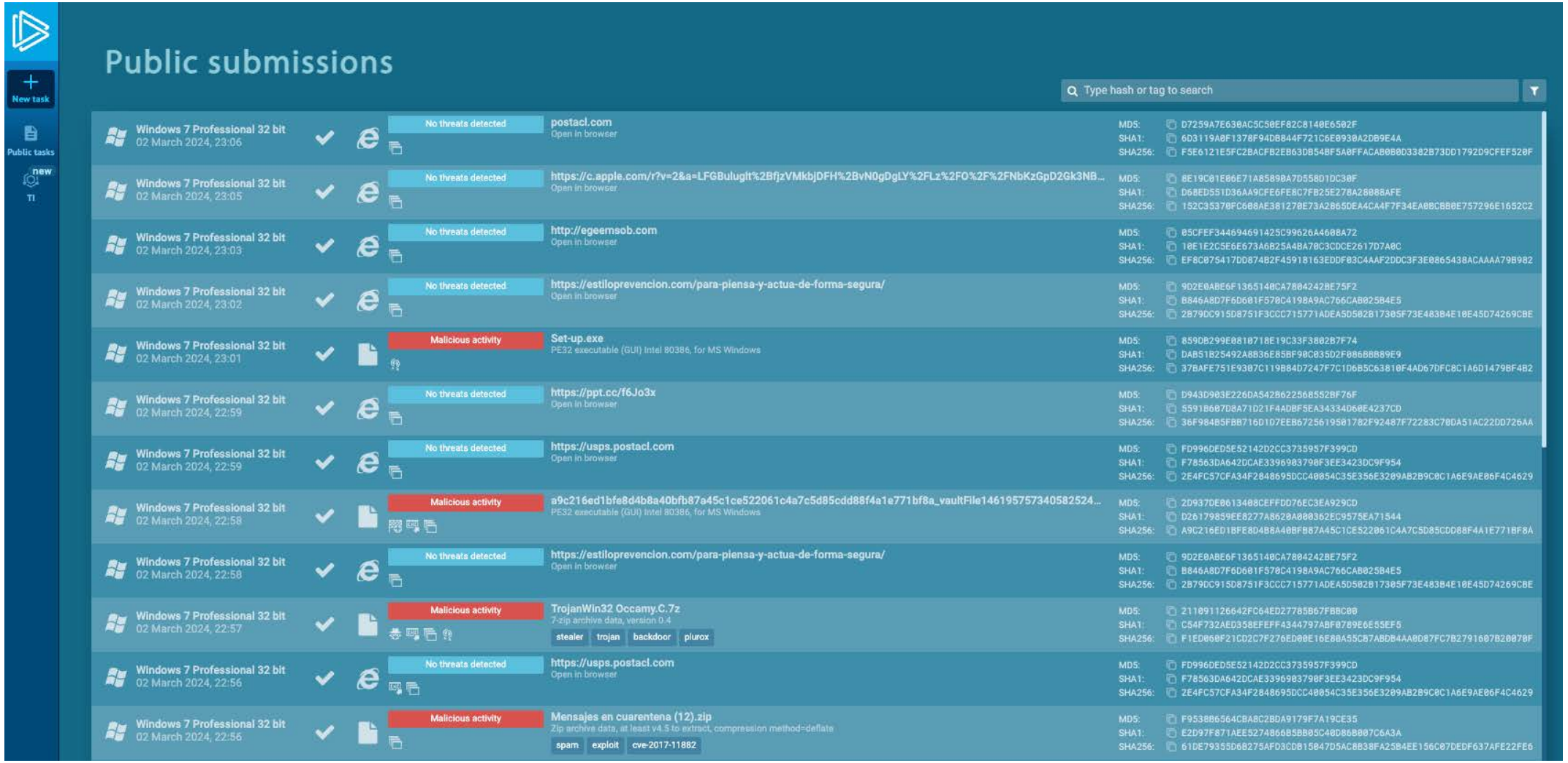
https://www.misp-project.org/

VirusTotal



https://www.virustotal.com/

AnyRun

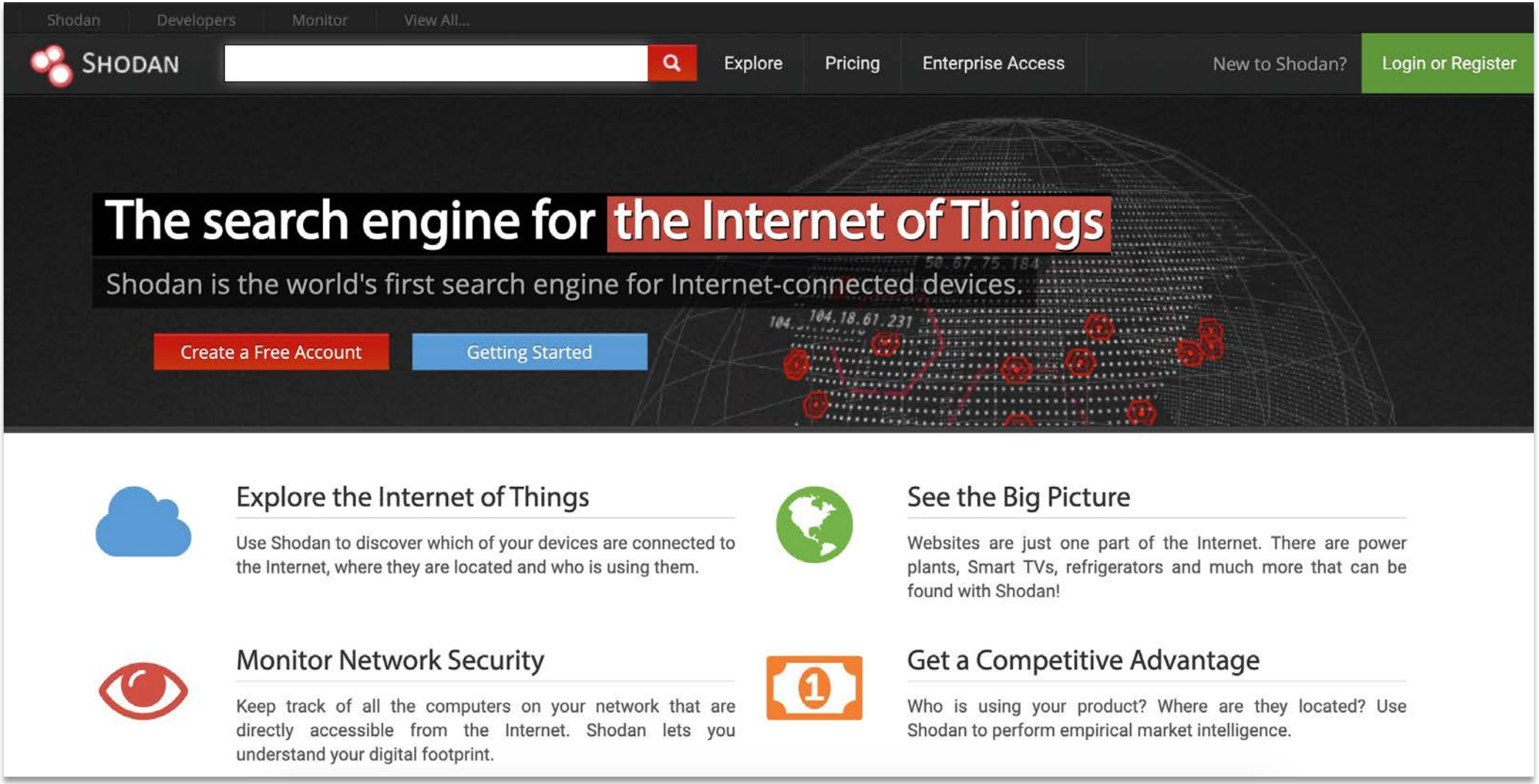


https://app.any.run/

常見的資安情資平台

網路服務類型

SHODAN



https://www.shodan.io/

練習

- 請嘗試分析(40545f66ad0d3b96d4ea0348a705d15c)中的droiddddddOnline.pcap 進行分析此封包檔案對應到的Signature ID ，請使用lab.dynamite.ai 封包分析平台 。
- 請問嘗試分析 (40545f66ad0d3b96d4ea0348a705d15c)中的droiddddddOnline.pcap 是否有可能適合對應IoC的 HTTP/HTTPS requests，如果有請把對應的URI 提供出來。
- 請嘗試分析一下此電腦正在運行的惡意程式，是否可以被 Proofpoint IDS Rules 偵測到，如果無請回答none ，如果可以請回答規則名稱或是規則的Unique rule identifier 。

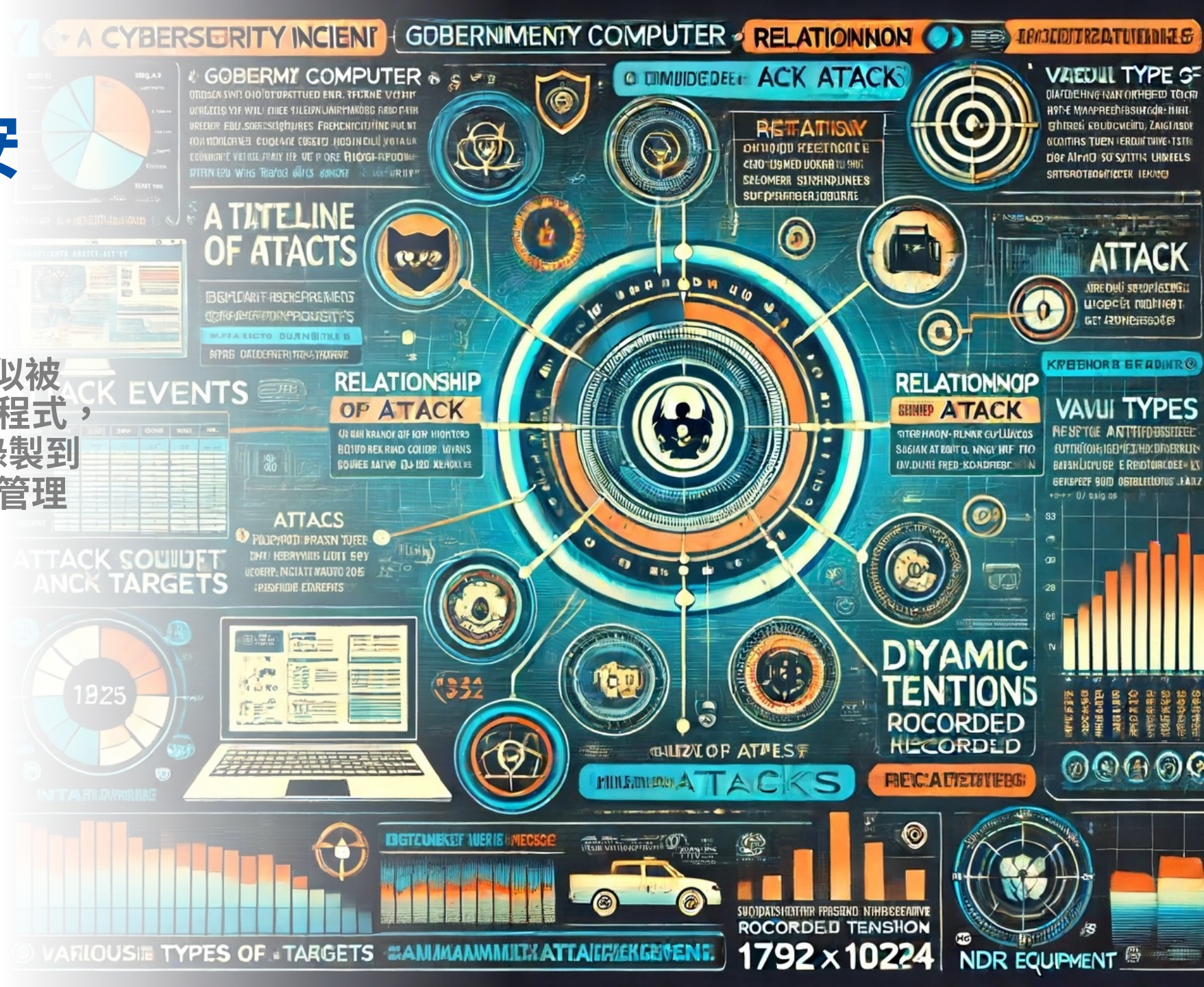
綜合練習

INC2403

XYZ政府資安事件調查

- XYZ政府單位的電腦疑似被駭客攻擊並植入了惡意程式，此攻擊有被NDR 設備錄製到一些行為，請協助系統管理員分析此資安事件。

- 預計題目總數
  - 15

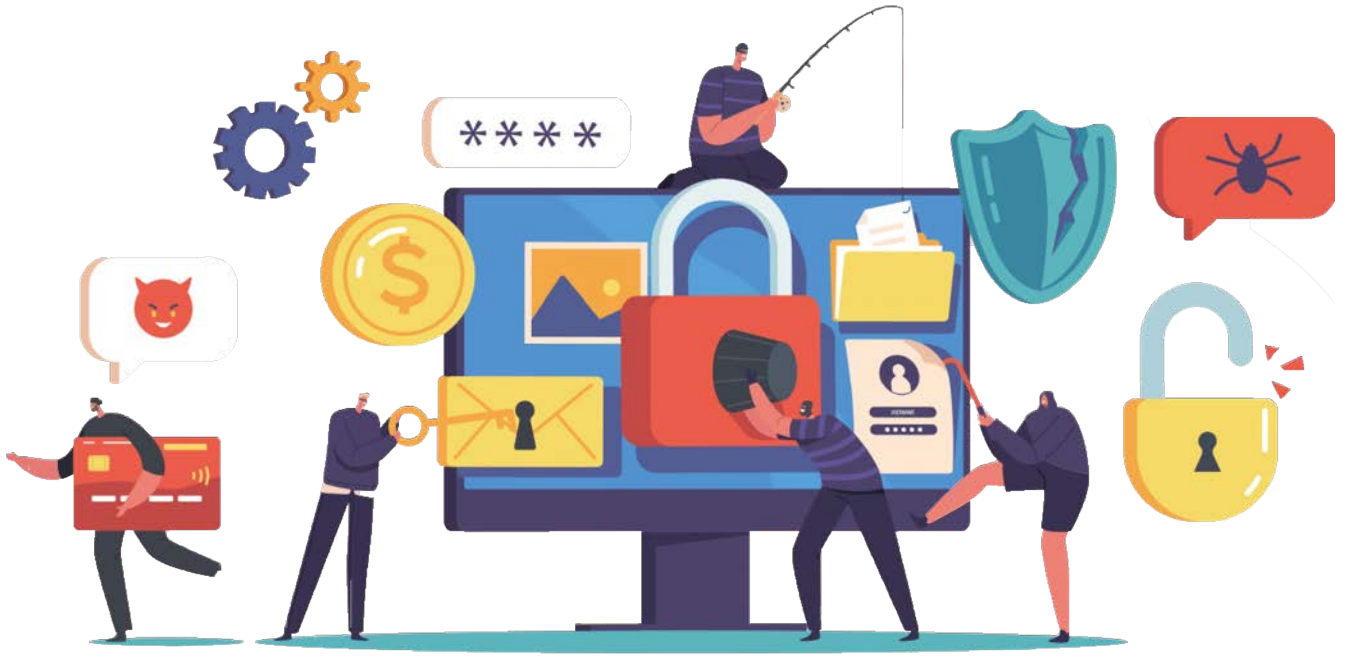


如何緩解

降低損失

攻擊事件緩解

- 惡意程式感染
- 資料外洩
- DDoS
- 社交工程攻擊



緩解 – 惡意程式(包含勒索軟體)

- 即刻緩解:
  - 斷開受影響系統的網路連接，防止惡意軟體傳播。
  - 運行端點保護軟體識別和隔離惡意程式。
- 經過分析後的緩解:
  - 識別惡意軟體的入侵路徑和感染方式。
  - 更新或修補被利用的軟體和系統漏洞。
  - 找到核心問題後的復原。

緩解-資料外洩

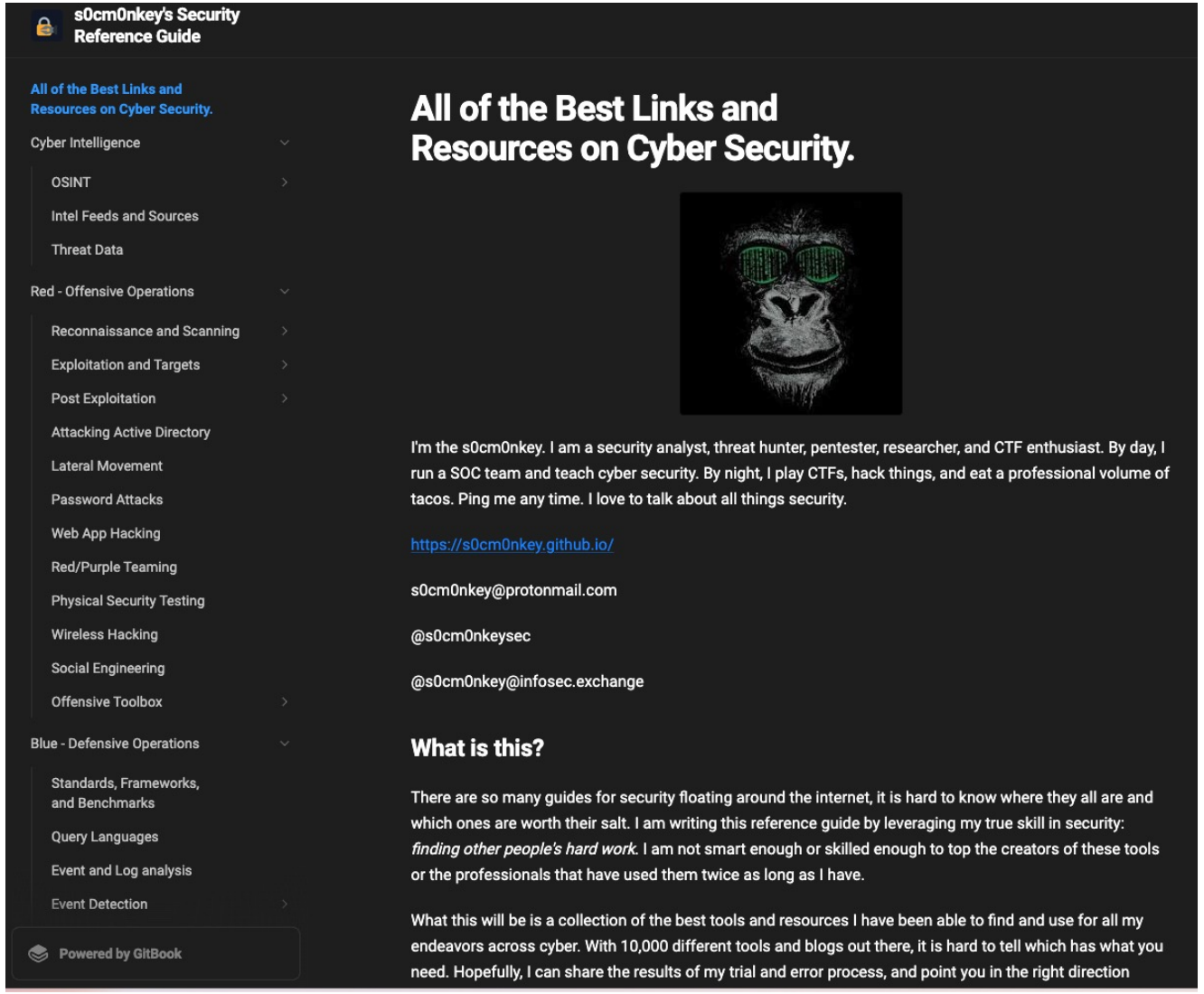
- 即刻緩解:
  - 網頁資料外洩
    - 確認入侵方式
    - 有限制的存取網頁、資料庫
  - 惡意程式
    - 分析網路行為，並且封鎖連線
    - 啟用端點保護啟用分析
- 經過分析後的緩解:
  - 網頁資料外洩
    - 修補網頁程式漏洞
    - 加入特定WAF規則
  - 惡意程式
    - 尋找其他主機上是否有相同的hashvalue

緩解-DDoS

- 即刻緩解:
  - 釐清攻擊手法
  - 進行攻擊來源限制
  - 伺服器主機參數調整
  - 搭配CDN 或是流量清洗
- 經過分析後的緩解:
  - 識別攻擊的源頭和類型，實施針對性的過濾規則
  - 加強邊界防禦和流量監控

緩解-社交工程

- 即刻緩解:
  - 分析可疑的信件、網頁連結、IP
  - 根據有問題的IP、Domain以及URL進行封鎖
- 經過分析後的緩解:
  - 分析攻擊手法來源和使用的技術，更新防護策略
  - 搭配端點保護軟體進行識別，防止淺在的惡意程式。



補充資料

https://s0cm0nkey.gitbook.io/s0cm0nkeys-security-reference-guide/

結 語

重點摘要

- 面臨未知型態的資安威脅與日俱增，現有資安防禦機制是否有效
- 這一場永無止盡的競賽，每一次都希望能夠防禦成功
- 數位時代須改變思維，以駭客的角度看待企業資安防禦
- 雲端服務成為企業的平台之之一，透過技術與管理層面的實施，以確保企業的營運安全
- 巨量成長的資安數據，須滿足時效性與精準度
- 資安事件調查在於掌握證據力


A
Q

Hackers are anywhere, any time! Are you READY ?

Welcome to Shieldx.io

SHIELDXTREME