中華資安國際
CHT Security

回顧近期資安威脅趨勢與重大案例，應用資安監控應變平台融合SOC+MDR+SOAR的最佳實踐

報告人：邱永興
SOC服務部 協理

報告內容

中華資安國際
CHT Security

一 資安事件處理統計結果與分析

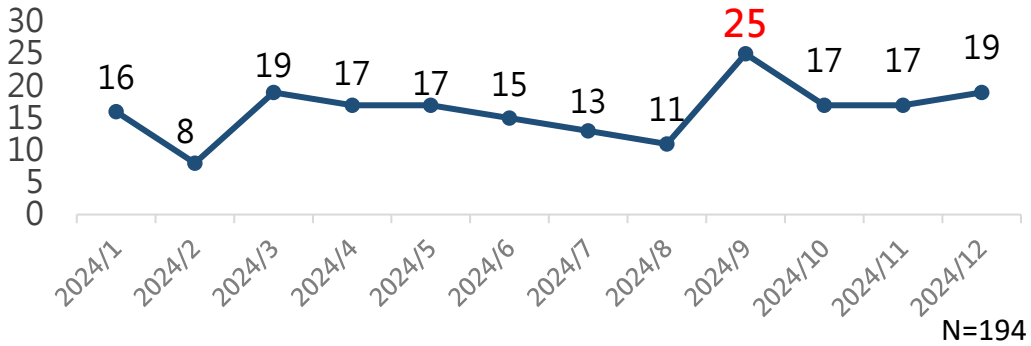
二 重大資安威脅案例說明

三 資安威脅應對與防禦策略

四 結語

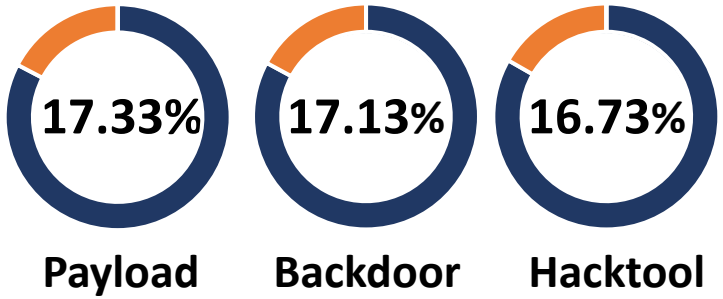
從2024年資安事件處理統計結果看問題(1/2)

資安事件調查數量



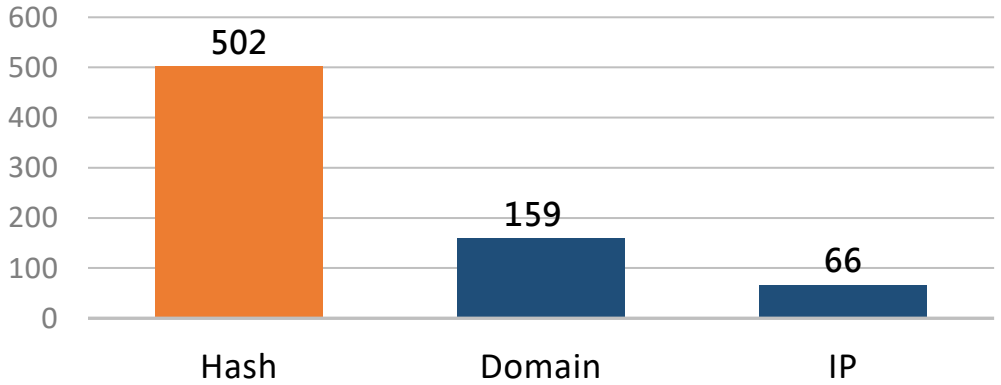
N=194

惡意程式類型

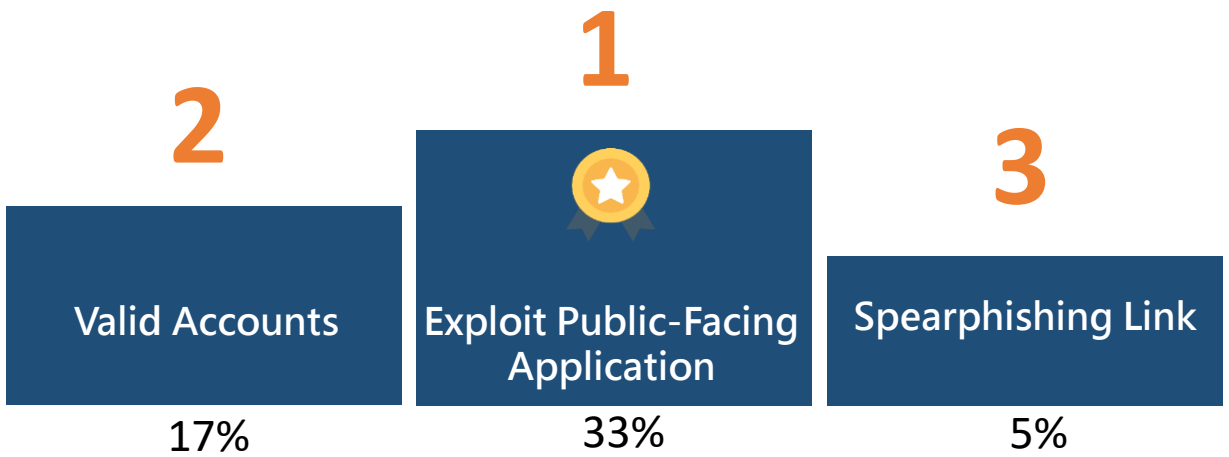


Loader 15.54%
Webshell 10.76%
Downloader 3.78%
Dropper 2.79%
Script 2.59%
Adware 1.79%
Ransomware 1.2%
Miner 1.2%
Else 0.8%
MalDoc 0.4%
Stealer 0.2%

新發現威脅情資



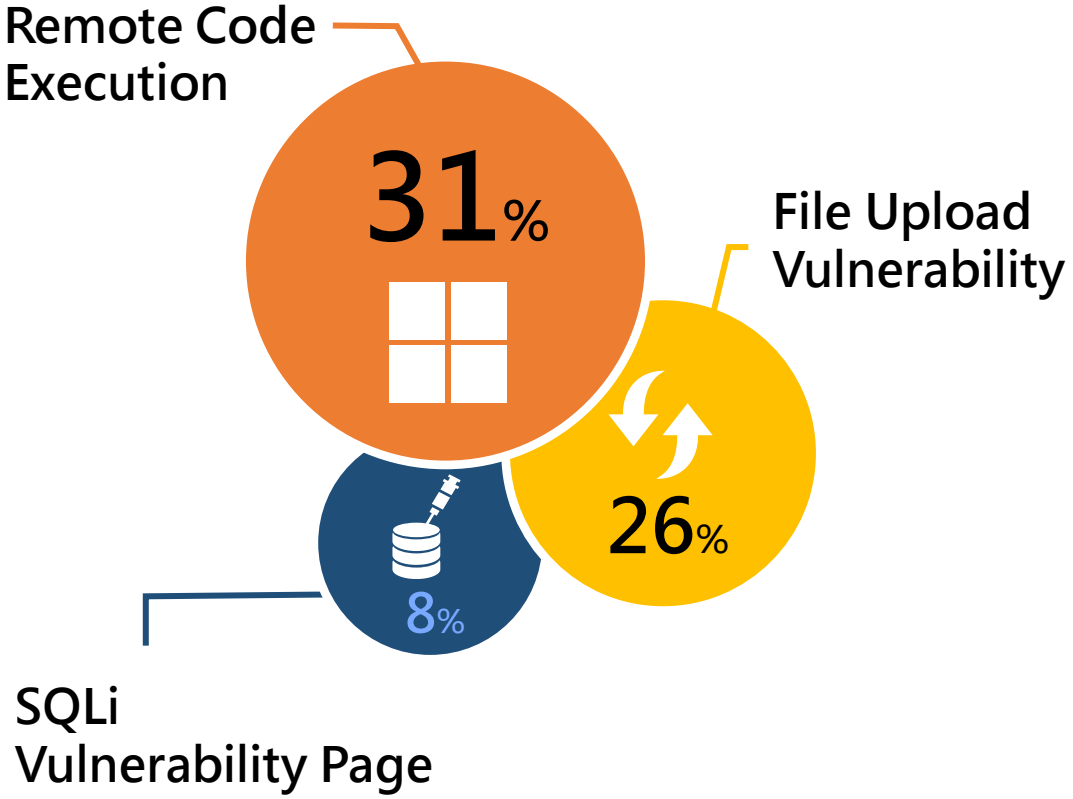
駭客入侵手法 (Initial Access)



從2024年資安事件處理統計結果看問題(2/2)

Exploit Public-Facing Application

公開漏洞類型 Top 3



Our findings are the same as Gartner's

Top Cybersecurity Trends for 2024

Optimizing for Resilience	Optimizing for Performance
• Continuous Threat Exposure Management • Extending IAM's Cybersecurity Value • Third-Party Cybersecurity Risk Management • Privacy-Driven Application and Data Decoupling	• Generative AI • Security Behavior and Culture Programs • Cybersecurity Outcome-Driven Model's • Cybersecurity Reskilling

Source: Gartner
802944_C

Gartner

持續威脅暴露管理（Continuous Threat Exposure Management）
擴展IAM的網路安全價值（Extending IAM's Cybersecurity Value）
第三方網路安全風險管理（Third-Party Cybersecurity Risk Management）
隱私驅動應用和數據解耦(Privacy-Driven Application and Data Decoupling)

【中華資安國際】資安事件調查發現資安風險趨勢

Our findings are the same as Gartner's

Top Cybersecurity Trends in 2024

產業	入侵管道	事件簡述
金融產業	Exploit Public-Facing Application 利用公開漏洞 TOP1	EDR偵測到惡意行為，調查後研判攻擊者利用頁面將惡意檔案上傳並利用，未發生後續橫向滲透狀況。
	Spearphishing Link 透過連結進行魚叉式網路釣魚 TOP1 TOP2	攻擊者假冒公司名義進行詐騙使用者下載惡意程式，透過連結進行魚叉式網路釣魚。
醫療產業	Valid Accounts 利用合法帳號 TOP1 TOP2 TOP3	防毒軟體偵測到惡意程式，攻擊者可能取得合法帳號並登入網通設備進行內網存取，並執行後續惡意行為。
	Exploit Public-Facing Application 利用公開漏洞 TOP1	攻擊者透過CVE-2024-4577漏洞，植入網頁木馬並將網頁資訊打包，緊急發現並快速處理後，未發生後續橫向滲透狀況。
關鍵基礎設施	Valid Accounts 利用合法帳號 TOP1 TOP2 TOP3	Domain Admins群組的高權限帳號遭登入，攻擊者最早可能透過入侵A主機，並進一步橫向到其他主機進行惡意行為。 但由於A主機相關日誌並無保留當時的紀錄，故無法進一步確認入侵根因。
	Exploit Public-Facing Application 利用公開漏洞 TOP1 TOP2 TOP3	駭客利用近期重大安全漏洞CVE-2024-4577對網頁程式植入網頁木馬，並對內部主機進行橫向滲透。
高科技製造	Valid Accounts 利用合法帳號 TOP1 TOP2 TOP3	客戶發現主機存在異常活動，進一步安裝EDR後，偵測到惡意行為。調查後研判攻擊者利用合法帳號，透過Unified Access Gateway及VMware Horizon成功登入受駭主機，並進一步橫向滲透到其他主機。

報告內容

中華資安國際
CHT Security

一 資安事件處理統計結果與分析

二 重大資安威脅案例說明

三 資安威脅應對與防禦策略

四 結語

看不見的資安風險，BlackTech入侵網通設備案例分享(1/2)

駭客入侵某關鍵基礎設施並**潛伏多年**，雖陸續曾有其他團隊執行過事件調查，但**因缺乏網路可視性**，無法有效根除入侵管道

本團隊協助部署**SecuTex NP Box**，逐步破解駭客能夠**隱匿多年**的攻擊手法，協助管理者收回場域控制權

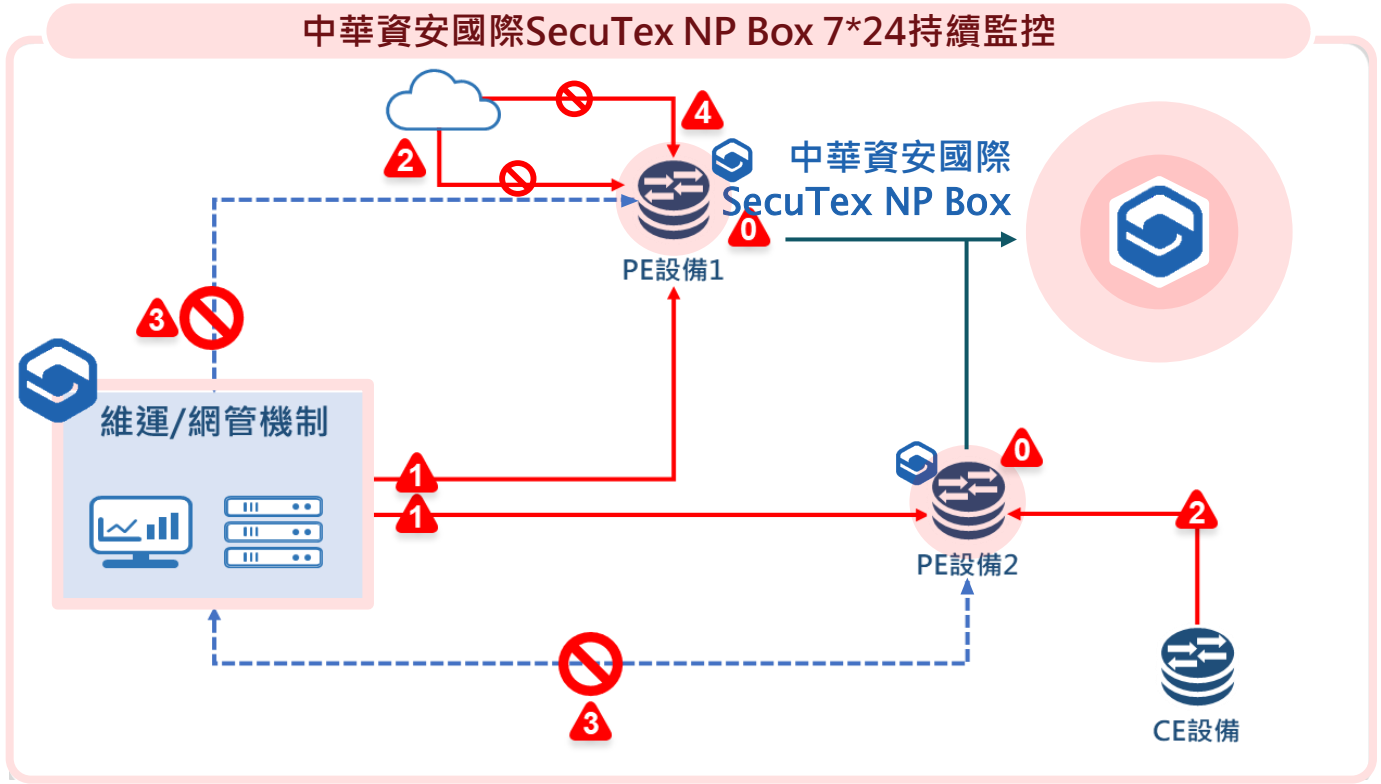
0 攻擊者能夠**置換Router功能模組**與**進入底層Linux**

1 有**帳號**遭利用軌跡

2 攻擊來源包含**Internet介面**與**客戶CE 介面**

3 攻擊者能夠**繞過或關閉AAA** & **SYSLOG** 認證機制

4 攻擊者會**異動組態設定**，目的為SSH進Router & 透過VPN連入特定場域



看不見的資安風險，BlackTech入侵網通設備案例分享(2/2)

攻擊策略及技術分析

Initial Access	Privilege Escalation	Defense Evasion	Lateral Movement	Persistence	Command and Control
TA0001 Initial Access 攻擊者透過利用路由器來存取受害者網路	TA0004 Privilege Escalation 攻擊者在受害者的網路上獲得了更高的特權	T1562.003 Impair Defenses: Impair Command History Logging 攻擊者停用受感染路由器上的日誌紀錄，以避免遭即時監控與事後稽核發現	T1201.004 Remote Services: SSH 攻擊者使用 SSH 在受害者網路中橫向移動	TA0003 Persistence 攻擊者建立惡意控制網路以持續存取受害者的網路	TA0011 Command and Control 攻擊者控制受害者的網路基礎設施
T1199 Trusted Relationship 攻擊者利用路由器的可信任域關係來存取其他受害者網路		T1601.001 Modify System Image: Patch System Image 攻擊者修改路由器韌體以迴避偵測		T1205 Traffic Signaling 攻擊者傳送特製封包以啟用或停用受感染路由器上的後門功能	T1071.002 Application Layer Protocol: File Transfer Protocols 攻擊者使用 FTP 透過受害者的網路傳送資料或傳送用於破壞路由器的腳本
				T1542.004 Pre-OS Boot: ROMMONkit 攻擊者修改路由器韌體以維持持久性	T1090 Proxy 攻擊者使用受感染的路由器來代理流量

本團隊分析結果與美/日之國家級單位發佈報告相同

供應鏈資安威脅，Waterbear攻擊案例分享

某機關伺服器因連線**Waterbear中繼站**產生告警，經本團隊調查發現攻擊者為**中國網軍BlackTech**，透過**委外系統開發商供應鏈**入侵

本團隊仔細搜尋與分析不易被抹除的紀錄，如Registry異動時間、網路設備紀錄檔等，**還原入侵所使用的帳號與登入行為軌跡**

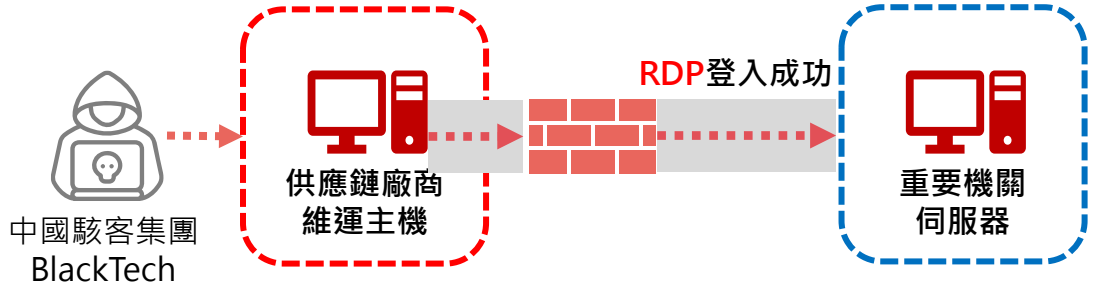
惡意連線紀錄

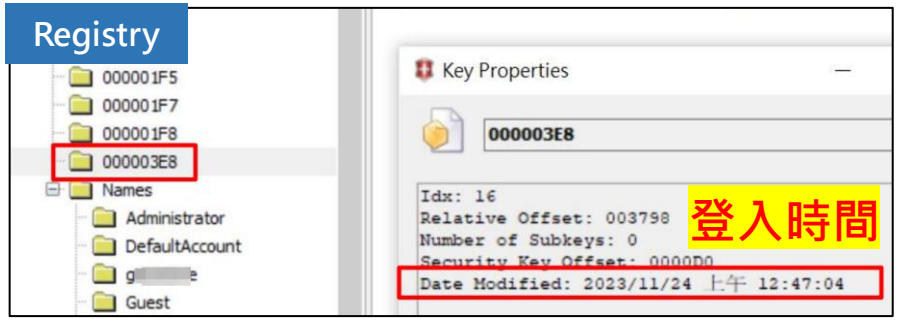
起始時間	結束時間	來源IP	目的IP Waterbear中繼站
2023/11/24 09:05	2023/11/24 09:06	11[redacted].235	36.[redacted].85

防火牆連線紀錄

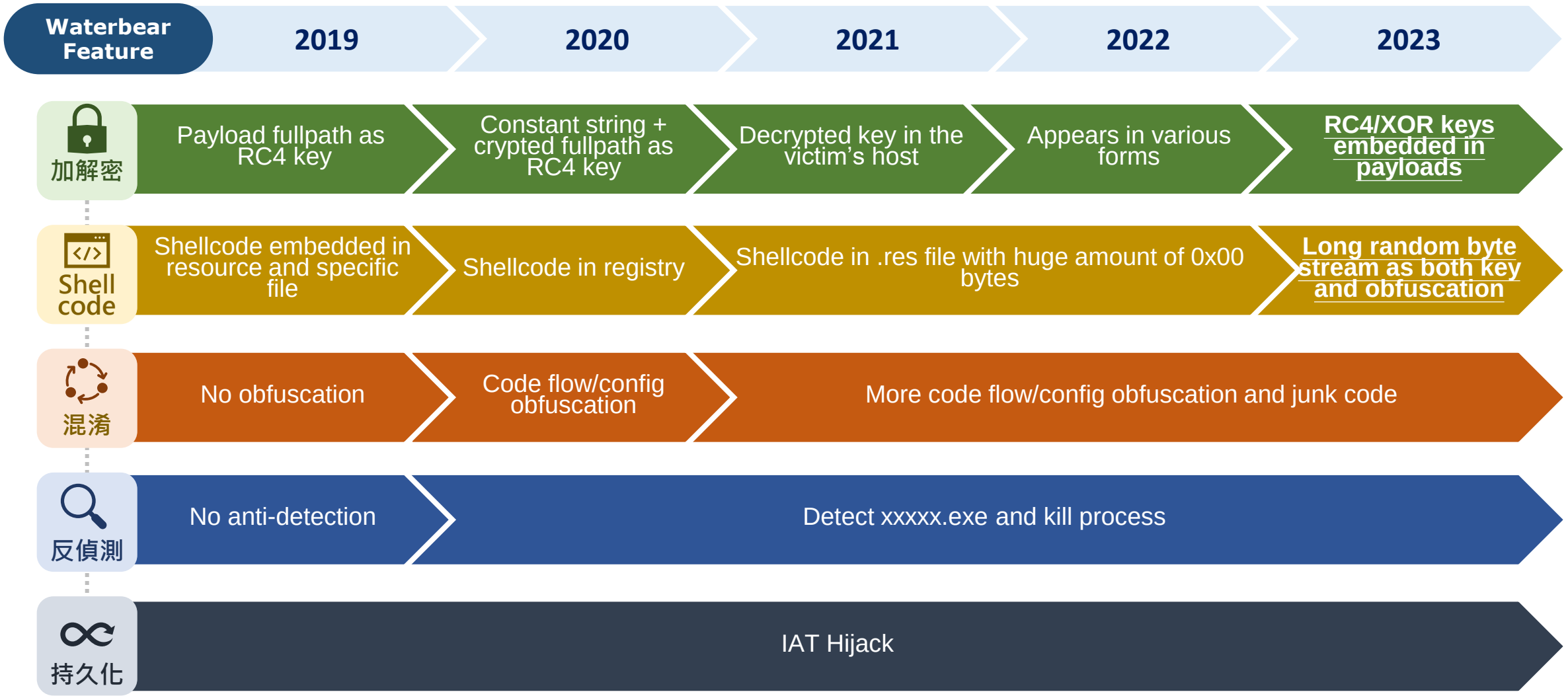
14[redacted].253	192.168.128.10	3,389	Nov 24, 2023 @ 08:36:41.000
14[redacted].253	192.168.128.10	3,389	Nov 24, 2023 @ 08:37:54.000
14[redacted].253	192.168.128.10	3,389	Nov 24, 2023 @ 08:49:30.000
14[redacted].253	192.168.128.10	3,389	Nov 24, 2023 @ 09:05:03.000

駭客入侵軌跡示意圖

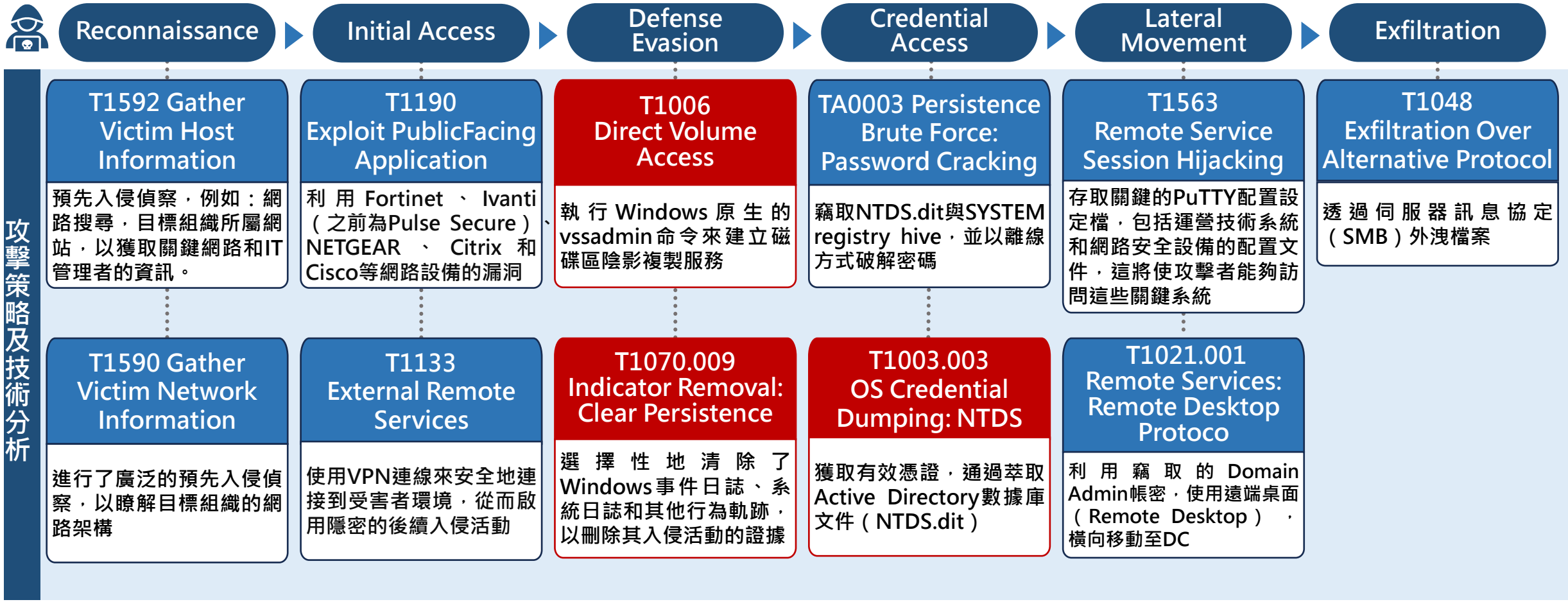




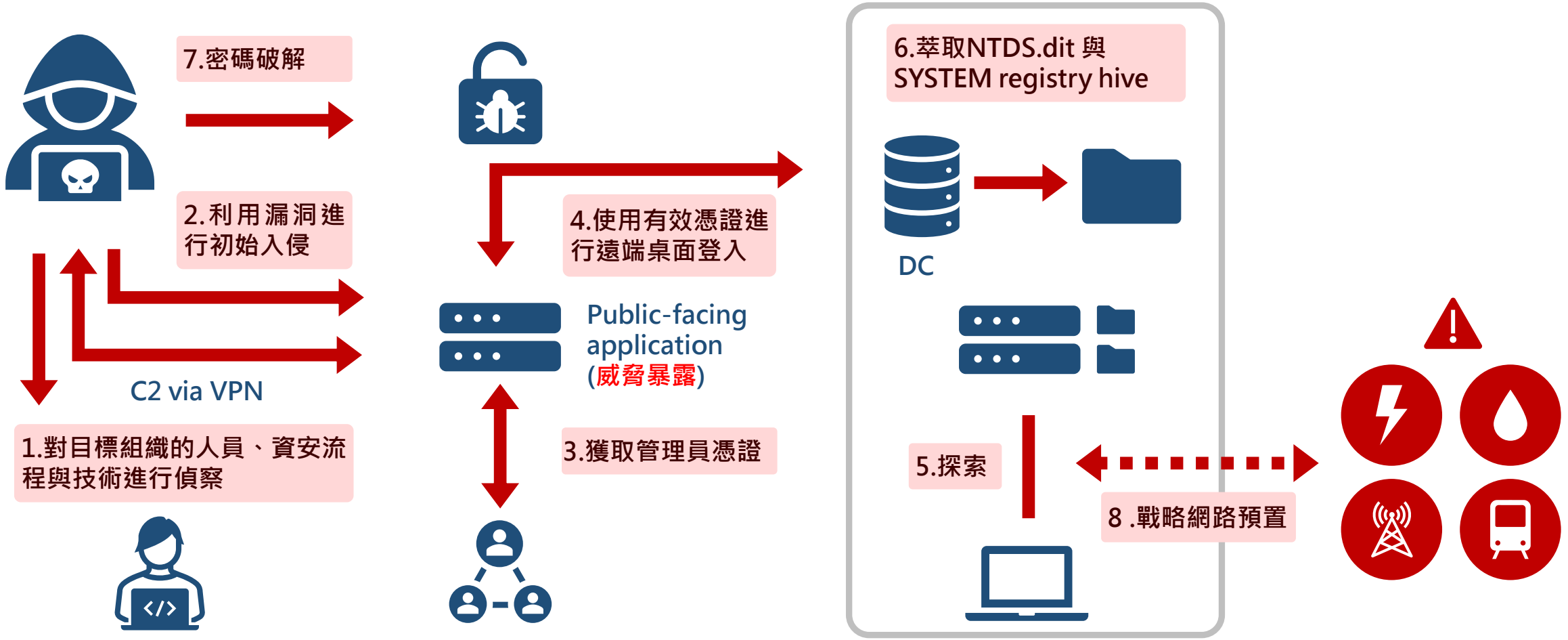
Waterbear 特徵技術分析



Volt Typhoon 關鍵基礎設施攻擊案例分享(1/2)



Volt Typhoon 關鍵基礎設施攻擊案例分享(2/2)



Volt Typhoon-LOTL(Living Off-the-Land)寄生攻擊

Volt Typhoon 至少使用以下 LOTL 工具和指令執行系統資訊、網路服務、群組和使用者探索等攻擊活動：

- cmd
- certutil
- dnscmd
- ldifde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

LOTL(Living Off-the-Land)：攻擊者使用受駭電腦中的合法工具/指令執行攻擊，這種手法被稱作「Living Off-the-Land（LoTL）」，目的是藉由這些合法工具來掩護非法行動，將惡意活動與合法的網路行為融為一體，這使得即使是擁有成熟安全態勢感知能力的組織也很難區分。

報告內容

中華資安國際
CHT Security

一 資安事件處理統計結果與分析

二 重大資安威脅案例說明

三 資安威脅應對與防禦策略

四 結語

資安威脅應對與防禦策略

建立資安管理制度、管控曝險、導入零信任、整合監控應變、驗證有效性

即時有效的威脅暴露管理系統

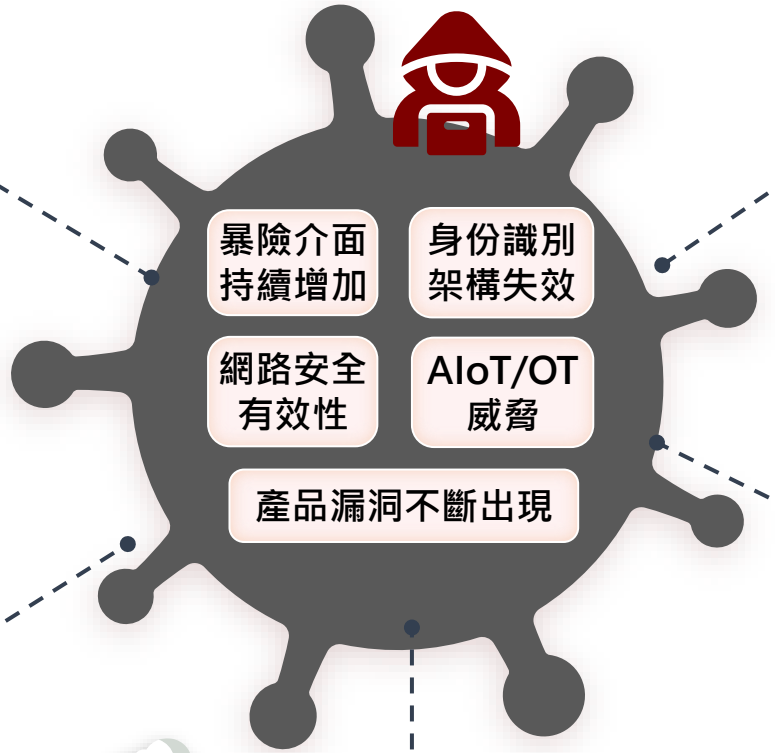
威脅暴露管理
(Threat Exposure Management)

✓ 建立VANS/VMS

整合資安監控應變平台

資安平台融合
(Cybersecurity Platform Consolidation / Operating)

✓ SOC+MDR, IT+OT, NP+ED



OT/IIoT 檢測與監控興新威脅與對策

導入 ZTA 零信任架構

身分結構免疫
(Identity Fabric Immunity)

✓ MFA/FIDO ZTNA、CypherCom

資安防禦機制有效性驗證

網路安全驗證
(Cybersecurity Validation)

✓ EASM、BAS、紅隊演練

SOC x MDR x SOAR 全面監控，即時回應

SOC

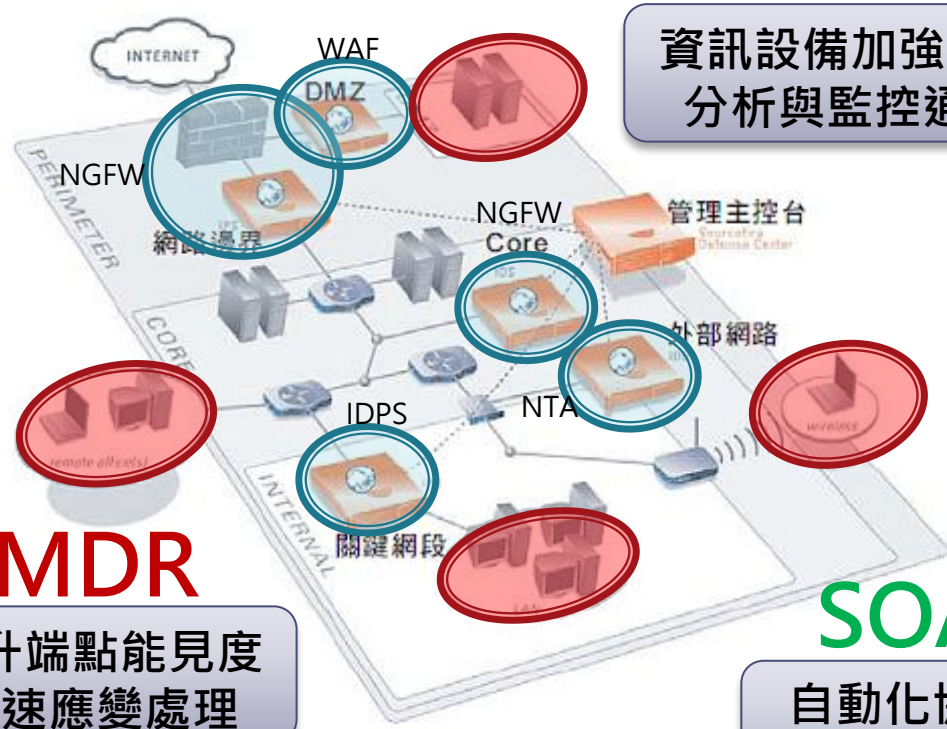
- 監控IT、資安設備（FW、IPS）
- 閘道防護全面監控
- 外部風險監控
- 多性質日誌整合
- 協助事件調查、確認受害範圍

MDR

- 監控 PC、Server
- 單位守備、精準打擊
- 針對APT攻擊手法的偵測規則
- 識別惡意指令 > 橫向移動指令
- 無檔案攻擊 > 一句話木馬

SOAR

- 自動回應劇本 (Playbook)
- 溝通協調防護機制、串聯協防
- 自動化進行風險回應
- 提升風險處理時效



SOC

資訊設備加強關聯
分析與監控通報

MDR

提升端點能見度
快速應變處理

SOAR

自動化協作回應
縮短事件應變時間

融合 SOC+MDR+SOAR 的資安風險管理平台 (SRM)

Security Risk Management (SRM)

資安戰情牆

威脅情資中心

資安事件處理

CTI

CTI

IoC

SRM 資安風險管理平台

預警情資 | 資安戰情牆 | 事件通報管理 | 情資交換 | SOAR

Event

SOC監控服務　多維度關聯分析

elastic AI/ML 情資回溯

ArcSight An HP Company SIEM即時關聯分析

Microsoft Sentinel / Google SecOps 雲地整合

Log

日誌收集器

雲端平台、網路閘道、管理系統、端點主機

雲 AWS/Azure/GCP

閘 FW/IPS/WAF

管 AD/DNS

端 EPP/EDR

Playbook

Playbook

通報事件自動阻擋

PA-NGFW
FortiGate
CheckPoint

MDR
端點/網路
威脅偵測回應

CROWDSTRIKE

SentinelOne

Microsoft Defender

SRM 內建戰情牆


統計週期
通報事件統計
事件處理狀態統計
中華資安國際股份有限公司
1
(未結案) 高風險
14
(未結案) 中風險
20
(未結案) 低風險
42
未結案
3
結案
42
未接單事件
9
逾期未結案事件
↑上區塊
↓下區塊
統計週期
每日的數量統計
事件概況
事件觸發趨勢
2025-01-29
2025-01-30
2025-01-31
2025-02-01
2025-02-02
2025-02-03
2025-02-04
2025-02-05
資安院十大類
通報類別
依照登錄的單位
處理單位統計
初始單位
Infra營運管理科
Top 5 事件分析
單一事件對應多個ATT&CK
通報事件
ATT&CK
外部攻擊來源 IP
內部風險主機
排序順位：風險等級->事件量
最近5筆事件
即時新進案件
CHT_Sec-SN-20250206-1610-000001 外部主機對內進行違編維運工具連線
CHT_Sec-SN-20250206-1427-000001 單一主機偵測病毒(已刪除)
CHT_Sec-SN-20250206-1335-000001 內部主機對內進行違編維運工具連線
CHT_Sec-SN-20250206-1203-000002 外部主機對內進行違編維運工具連線
CHT_Sec-SN-20250206-0337-000001 非上班時間特權帳號登入成功

報告內容

中華資安國際
CHT Security

一 資安事件處理統計結果與分析

二 重大資安威脅案例說明

三 資安威脅應對與防禦策略

四 結語

結語：資訊安全風險 – 彼的威脅、己的漏洞

威脅說明(Threat)	漏洞說明(Vulnerability)
個人或團體(駭客、網軍、競業、惡意員工、頑童...)因金錢、政治理念、商業機密、犯罪心態等目的，蓄意或不小心的作為，導致企業的損害或危險	由於對雲端、SaaS與第三方供應商關係的投資企業現在面對的攻擊面不斷擴大，這意味著傳統漏洞管理方式無法全面涵蓋

Risk = Threat x Vulnerability x Impact

資安風險 = 內外威脅 x 自身漏洞弱點 x 影響衝擊

預期損失 Annual Loss Expectancy vs. 資安預算投入 Cybersecurity Budget

威脅不可控，CISO 焦點應放在涵蓋面更廣的「威脅曝露管理」流程上。同時，需要預先建立有效的「威脅應變」程序，以應對發現的問題

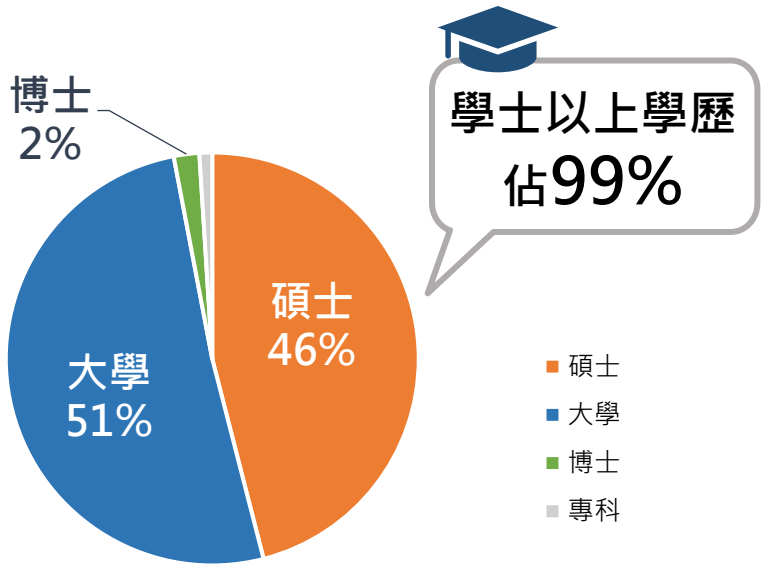
中華資安是值得信賴、財務穩健的專業資安公司

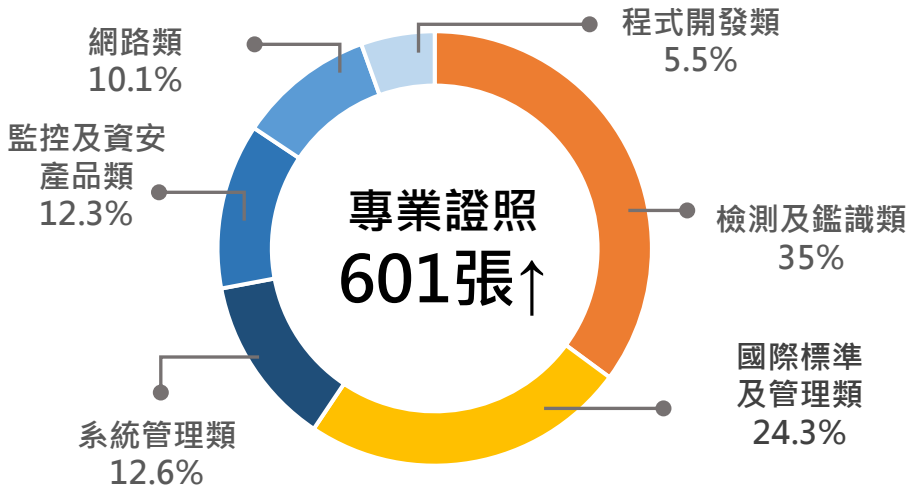
- **中華電信集團的資安專業公司**，前身是中華電信對外的資安服務團隊
- 自2003年開始經營資安業務，具**北、中、南區均有在地資安技術人力**
- 具備**國家級資安專案建置能力與實績**，每年服務超過上百家客戶
- 提供**事前防護檢測、事中監控應變、事後鑑識復原**的一站式資安服務

民國106年	3.635億元	352人▲
成立公司	實收資本額	員工總數

資料時間：113.11

- **建立完整且嚴密的資安管理制度並取得5項國際驗證**
  - ISO 27001 資訊安全管理
  - ISO 27701 隱私資訊管理系統
  - ISO 20000 資訊技術服務管理
  - ISO 17025 數位鑑識暨資安檢測中心
  - IEC 62443 CBTL實驗室認證





- **全國唯一連續六年資安服務評鑑「全項A級」廠商！**

資訊來源

廠商名稱 \ 項目	情資品質		108～112年共契廠商評鑑				
	額外回饋情資	威脅樣態涵蓋率	SOC服務	資安健診	弱點檢測	滲透測試	社交工程演練
中華資安國際	達標	達標	AAAAA	AAAAA	AAAAA	AAAAA	AAAAA
安○資訊	達標	達標	AA--A	AA--A	AA--A	AA--A	AA--A
凌○電腦	未達標	未達標	BBCBB	BBBBB	BB--B	BB--B	BBBBB
數○資安	達標	未達標	BABAA	BBBBA	A--BB	B--BB	A--BB

- 為該年未參加廠商評鑑