中華資安國際
CHT Security

近期常見入侵案例分享及防駭方法

報告單位：中華資安國際股份有限公司

中華資安國際
CHT Security

Outline

01 近期常見的資安威脅

02 近期常見入侵案例分享及防駭方法

03 資安事件應變實務

講師介紹

- 姓名：馬洪雯 (Cindy)
- 工作經驗：
  - 財團法人資訊工業策進會 資安科技研究所
  - 中華資安國際股份有限公司 技術工程師
    - 數位鑑識暨資安檢測中心 技術主管
- 專長：
  - 數位鑑識
  - 事件回應
  - 網路分析

近期常見的資安威脅

- ✓ 資安威脅趨勢觀察
- ✓ 全球資安威脅趨勢觀察
- ✓ 中華資安之資安威脅趨勢觀察

資安威脅趨勢觀察

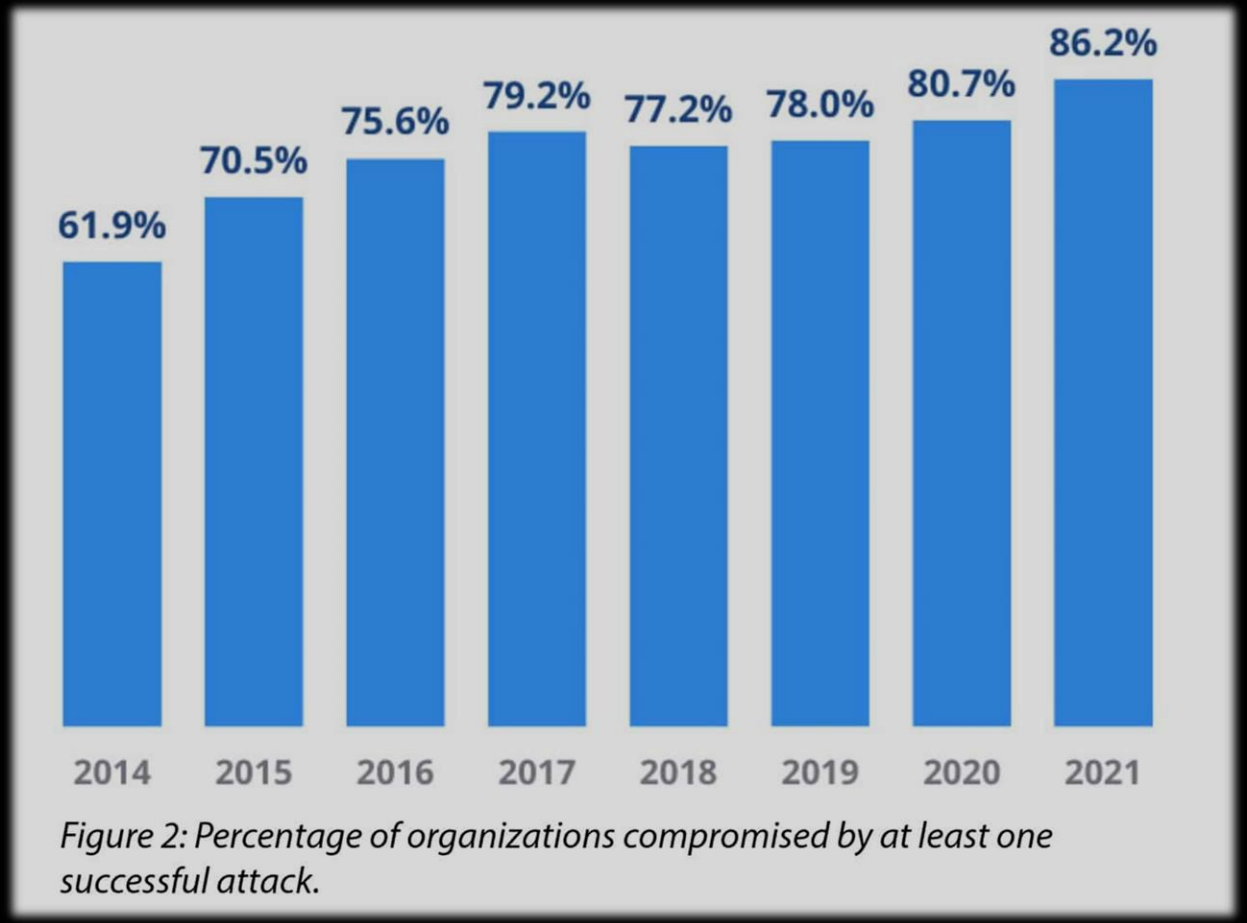


Figure 2: Percentage of organizations compromised by at least one successful attack.

馬里蘭大學於2007 年的一項研究發現，以前駭客以每 39 秒一次攻擊的速度攻擊主機和網路。互聯網犯罪投訴中心（The Internet Crime Complaint Center ‘s ）2020 年的報告發現，當年有 465,177 起事件，每 1.12 秒成功攻擊一次。值得注意的是，這不包括企圖攻擊或未回報的攻擊。

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com


CNN Money
HACKER?

中華資安國際
CHT Security

全球資安威脅趨勢觀察

惡意軟體統計

中華資安國際 CHT Security

惡意軟體是指任何旨在對數據、設備或人員造成傷害的軟體。惡意軟體的類型包括計算機病毒、特洛伊木馬、間諜軟體、勒索軟體、廣告軟體、蠕蟲、無檔案攻擊或混合攻擊等。隨著機器學習和有針對性的魚叉式網絡釣魚電子郵件的出現，最近的惡意軟體攻擊變得更加複雜。

- ✓ 92% 的惡意軟體是通過電子郵件發送的
- ✓ 每天會產生 230,000 個新的惡意軟體樣本——預計這個數字只會繼續增長
- ✓ 每週在給定時間有超過 1800 萬個網站感染了惡意軟體
- ✓ 34% 受到惡意軟體攻擊的企業需要一周或更長時間才能回覆服務
- ✓ 行動設備惡意軟體呈上升趨勢，2018 年行動設備惡意軟體的新變種數量增加了 54%
- ✓ 98% 的行動設備惡意軟體針對 Android 設備

Total Malware Infection Growth Rate (In Millions)

勒索軟體統計

勒索軟體是一種惡意軟體形式。勒索軟體攻擊通常通過社交工程進入受害者電腦，一旦用戶成為攻擊的受害者，他們的數據就會被加密，然後攻擊者要求受害者支付贖金，並承諾在付款後才會恢復。

- ✓ 2018 年，全球勒索軟體攻擊增加了 350%
- ✓ 據估計，到 2021 年，勒索軟體攻擊每年將造成 6 萬億美元的損失
- ✓ 勒索軟體每年給企業造成的損失超過 750 億美元
- ✓ 聯邦快遞在 2017 年第一季度因 NotPetya 勒索軟體攻擊損失了約 3 億美元
- ✓ 佐治亞州亞特蘭大在 2018 年 3 月遭受 SamSam 勒索軟體攻擊後，已花費超過 500 萬美元重建其主機網路
- ✓ 由於勒索軟體引起的停機，企業平均每小時損失約 8,500 美元

https://purplesec.us/resources/cyber-security-statistics/

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

勒索攻擊 (Ransomware Attack)

中華資安國際 CHT Security

“勒索軟體攻擊的感染率在 2020 年大幅增加，這主要是由於線上學習和遠端工作的日益增加

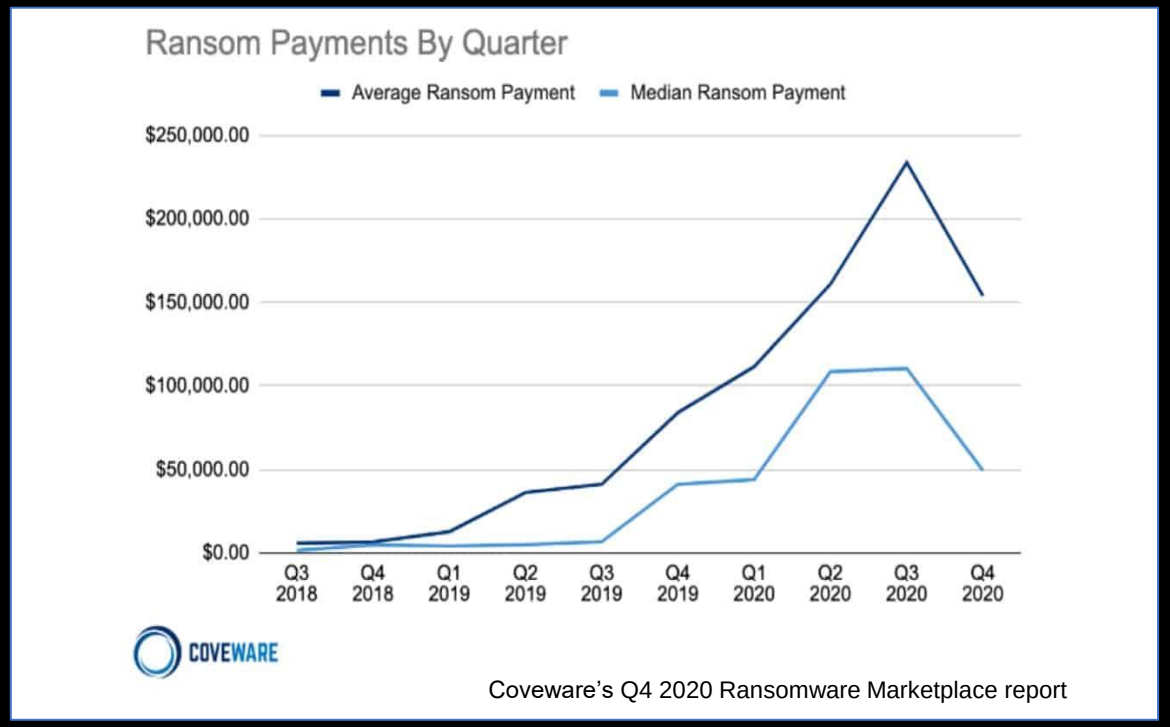
✓2020年，美國遭勒索軟體攻擊的成本估計為9.15億美元（ Emsisoft ）

✓2020 年初對紐奧良市政府的勒索軟體攻擊使該市損失了 700 萬美元(SC 雜誌)

✓2020 年 2 月，勒索軟體攻擊使總部位於丹麥的 ISS 集團損失了超過 5000 萬美元。（ 環球通訊社 ）

✓ 2020 年Q4因勒索軟體攻擊造成的平均停機時間為 21 天，而 2020 年Q3為 19 天。（ Coveware 的 2020 年Q4勒索軟體市場報告 ）

✓ 勒索軟體攻擊的代價可能非常高。例如，航運公司Maersk因勒索軟體NotPetya的攻擊使損失了超過 2 億美元



Coveware’s Q4 2020 Ransomware Marketplace report

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

挖礦劫持(Cryptojacking)

中華資安國際
CHT Security

挖礦劫持是未經授權使用他人的電腦來挖掘加密貨幣。駭客通過讓受害者點擊在主機上加載加密挖掘代碼的電子郵件中的惡意連結，或通過在受害者的瀏覽器中加載後執行的 JavaScript 代碼感染網站來實現此目的。

✓在ENISA 2020 年威脅態勢報告：挖礦劫持中，ENISA 指出，2019 年有 6410 萬次挖礦劫持攻擊。其中39.3% 的目標是日本。

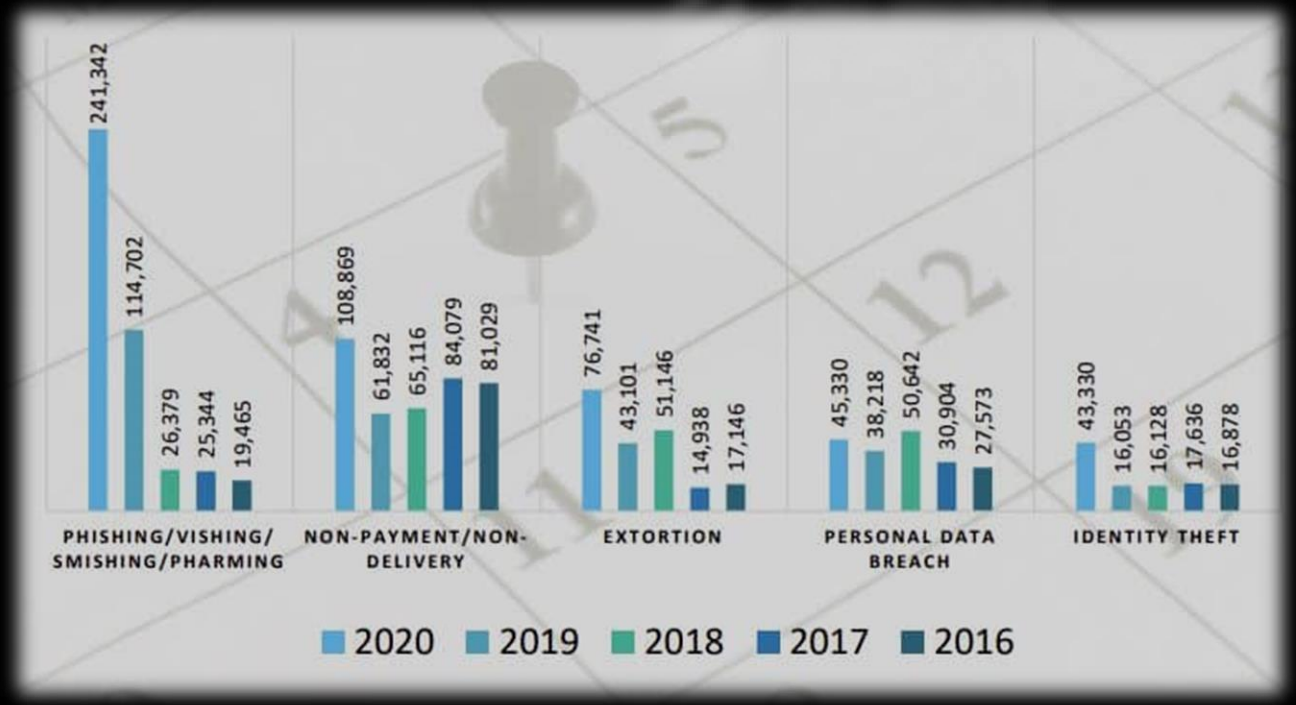
✓據估計，25% 的企業是加密劫持的受害者

> *An ongoing shift has been observed, however, from Coinhive to XMRig, another Monero cryptocurrency miner. An opensource code that is readily available, iterations of XMRig malware accounted for nearly 30 million of the 32.3 million total cryptojacking hits SonicWall observed in 2020.*

2020 SonicWall 網絡威脅報告

釣魚攻擊(Phishing attacks)

中華資安國際
CHT Security



- ✓ 在2020 年Internet Crime Complaint Center (IC3)的報告中，Phishing 為首要犯罪類型，其數量是2019 年的兩倍多(IC3 Internet Crime Report 2020)
- ✓ 2020 年的Q4，APWG 偵測到超過 636,000 個特殊的網絡釣魚網站，並發現超過 395,000 個特殊的網絡釣魚電子郵件主題(APWG’s Phishing Activity Trends Report for Q4 2020)
- ✓ 超過 60% 的網絡釣魚攻擊包含鍵盤側錄(keyloggers)
- ✓ 小型企業以更容易收到惡意電子郵件(Symantec’s Internet Security Threat Report 2019)
- ✓ 眾多行業中，又以金融機構為網絡釣魚攻擊最常見的目標，比上一季度增長了 3%(APWG’s Phishing Activity Trends Report for Q4 2020)

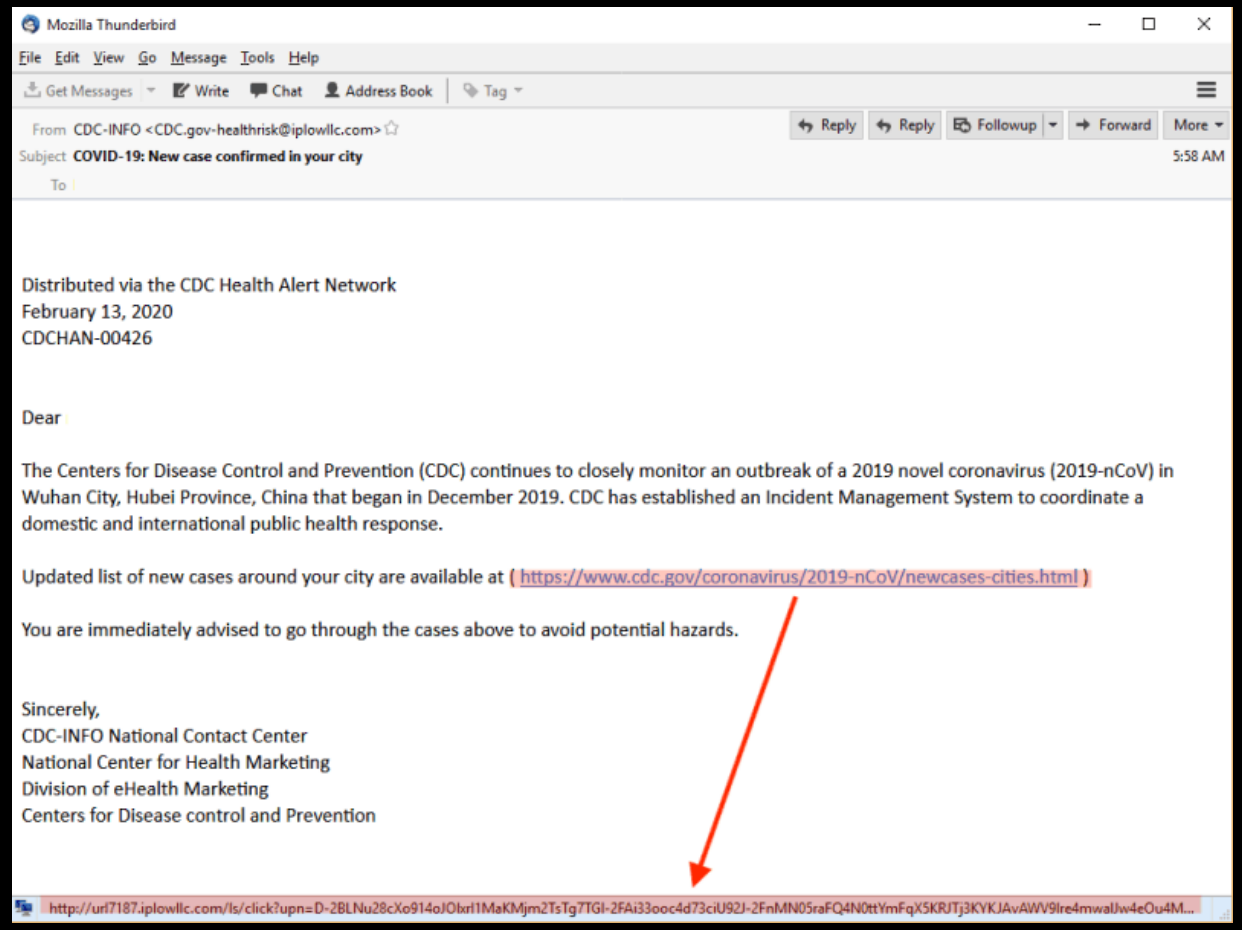
聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

“*由於 COVID-19 大流行，網絡犯罪增加了 600%*

由於 COVID-19 的爆發，網絡犯罪分子的複雜網絡釣魚電子郵件計劃呈上升趨勢。惡意行為者冒充疾病控制和預防中心 (CDC) 或世界衛生組織(WHO) 的代表。”

中華資安國際
CHT Security

✓這些電子郵件旨在欺騙和誘使收件人採取諸如單擊惡意鏈接或打開帶有病毒的附件之類的操作。



軟體/系統漏洞的威脅Vulnerabilities

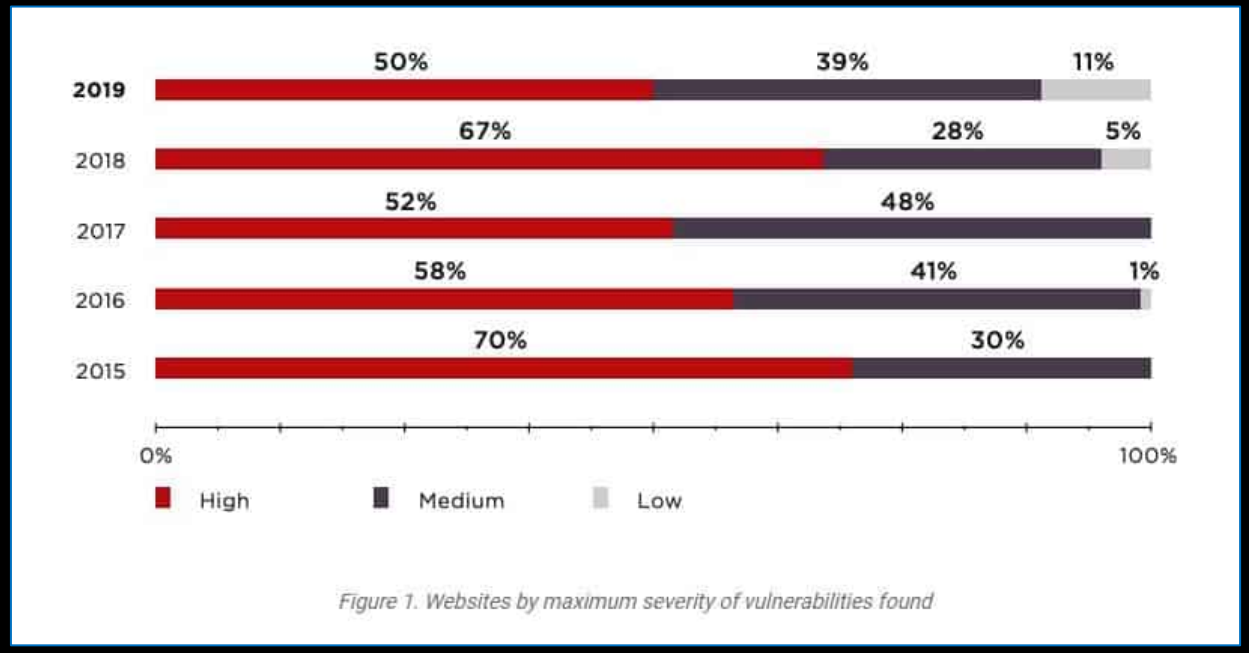
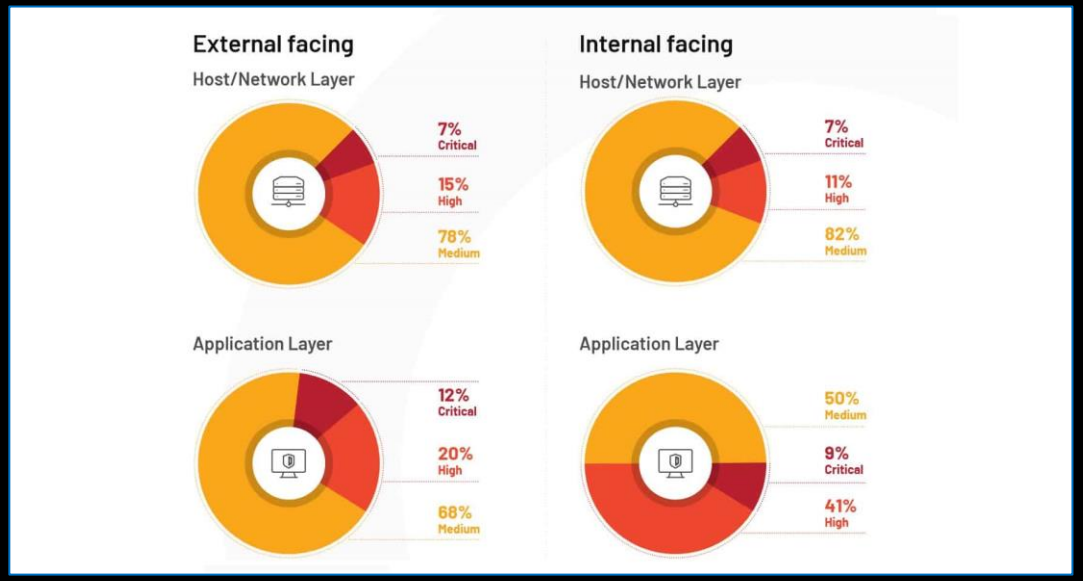


Figure 1. Websites by maximum severity of vulnerabilities found

Positive Technologies Web 應用程式漏洞和威脅：2019 年的統計數據

> *報告顯示**Web 應用程式**中的**安全漏洞仍然是一個巨大的問題**， 32% 的面向 Internet 的 Web 應用程式被認為是高風險或嚴重風險。*

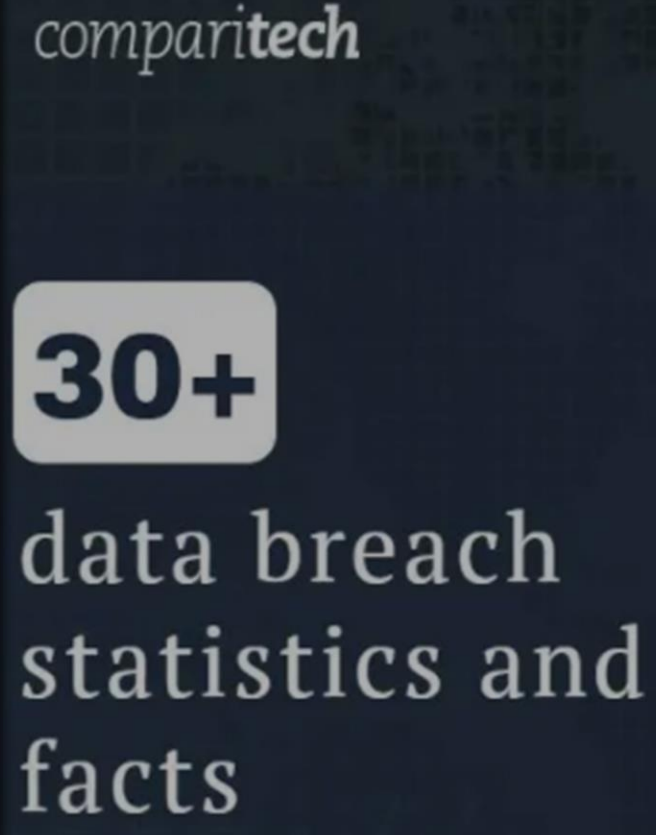


Edgescan 的 2021 年漏洞統計報告

- ✓2020 年 NVD 數據庫發布了18,362 個漏洞，略高於 2019 年的數量17,382(NVD Database)
- ✓有11.9%的漏洞被認為是critical級別的(CVE Details)

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

資料外洩 (Data breach)



1. 49% 的美國公司經歷過資料外洩
   - 451 Research 進行的2021 Thales Data Threat Report調查了 2,600 名高級管理者，他們分別代表不同行業。調查發現，近一半 (45%) 的美國公司過去曾遭受過資料外洩。
2. 2020 年首批數據洩露之一涉及 2.5 億條記錄
   - 微軟在 2020 年開局不利。在 1 月份報告中，它遭受了大量資料外洩，涉及可追溯到十多年超過 2.5 億條客服支援紀錄。
3. 2020 年至少有四次洩露涉及超過 10 億條記錄
   - 雖然微軟的漏洞是一個很大的漏洞，但它絕不是最大的。2020 年其他值得注意的資料外洩：CAM4 (108.8 億條記錄) 、 Advanced Info Service (AIS) (83 億條記錄) 和 Keepnet Labs (50 億條記錄) 。當然，還有12 月發現的SolarWinds 漏洞，大約 18,000 名 SolarWinds 客戶。

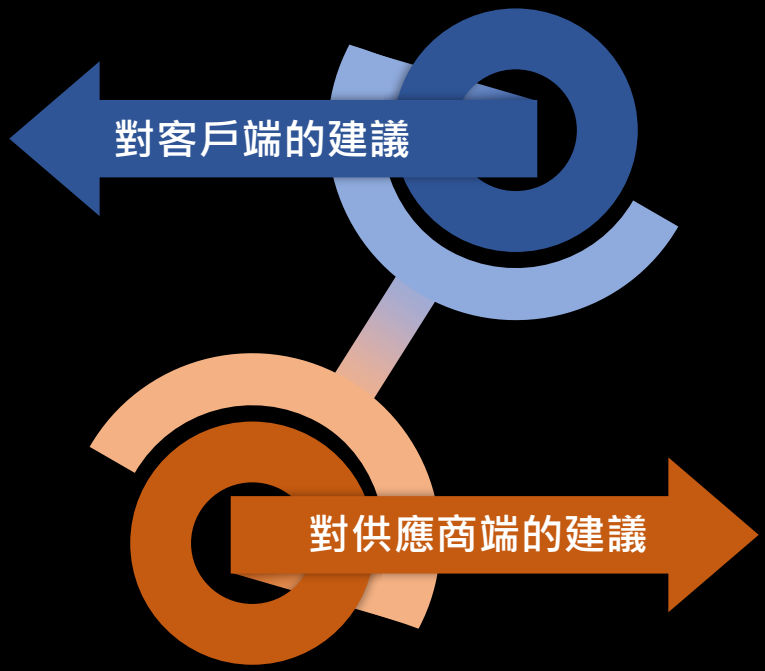
*“ **小型企業更有可能成為目標**，佔所有資料外洩的 50% 以上。比去年增加了近 100%，對比當時他們只有 28% 是受害者(Verizon 2021 Data Breach Investigations Report)*

https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

供應鏈攻擊(Supply Chain Attack)

中華資安國際
CHT Security

1. 識別與紀錄供應商和服務提供商
2. 定義不同類型的供應商及服務，如供應商與客戶間的依賴關係、關鍵軟體的依賴關係、單點故障等風險標準
3. 監控供應鏈的風險及威脅
4. 在產品或服務的整個生命周期內管理供應商，處理程序包含處理報廢產品或套件，對與供應商共享的資產或訊息進行分類，並定義存取和處理的相關程序
5. 該報告還建議了可能採取的行動，以確保產品和服務的開發符合安全流程。 例如，建議供應商落實漏洞和Patch管理



1. 確保用於設計、開發、製造及交付產品、套件和服務的基礎設施應遵循網絡安全守則
2. 遵循一般產品開發、維護及支援流程
3. 監控內部和外部來源的安全漏洞報告，包括使用過的第三方套件
4. 維護包含Patch相關訊息的資產清單

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

中華資安之資安威脅趨勢觀察

公司簡介

領先業界之專業能力！

2017年成立 | 實收資本額3.09億 | 員工 196人

中華資安國際 CHT Security

中華電信集團的**資安專業公司，**服務超過上百家

具備**國家級資安專案建置能力與實績**

2003年開始經營資安業務，**於北中南區有服務據點**

提供事前檢測、事中監控應變、事後事件調查的資安服務

1. **上網資安防護服務**：ISP雲端的入侵防護服務、DDoS防護服務、防駭守門員、APT防護、新世代防火牆、WAF等
2. **資安專業服務**：紅隊演練、滲透測試、IoT檢測、資安健診、金融安全評估、SOC監控、MDR、事故應變與鑑識調查、工控(ICS)資安
3. **資安顧問**：ISMS/PIMS制度導入輔導、資訊安全評估、PKI建置規劃
4. **資安管理平台規劃建置**：資安監控分析通報平台、弱掃管理平台、資安資訊分享與分析系統(ISAC)、網路威脅偵測與應變系統(SecuTex)
5. **身分識別產品與應用**：安全晶片與PKI應用、加密安全通訊解決方案
6. **企業資安整體解決方案**：資安、網路、雲端、軟硬體整體解決方案之規劃及建置

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

公司簡介

中華資安國際 CHT Security

A級資安團隊 (2020)

2017年成立 | 實收資本額3.09億 | 員工 196人

2020

--- 行政院資安共同供應契約評鑑

序號	受評廠商	SOC 監控服務	資安健診服務	弱點掃描服務	滲透測試服務	社交工程 郵件測試服務
3	中華資安	A 級	A 級	A 級	A 級	A 級

獲得最新行政院共契之評鑑「全項A級」廠商！

公司簡介

中華資安國際 CHT Security

2017年成立 | 實收資本額3.09億 | 員工 196人

安全評估/紅隊演練/資安檢測/SOC/事件處理(IR)經驗豐富！

工控場域資安服務實績

通過ISO 17025認證之數位鑑識與資安檢測實驗室

台灣電力公司 TAIWAN POWER COMPANY
台灣高鐵 TAIWAN HIGH SPEED RAIL
Accton Making Partnership Work
CSC Group
中鋼集團
台灣自來水公司 TAIWAN WATER CORPORATION
台灣中油股份有限公司 CPC Corporation, Taiwan

滲透測試與紅隊演練服務實績

國內唯一通過ISO 20000之紅隊演練服務商

中華民國總統府 Office of the President Republic of China (Taiwan)
臺灣證券交易所 TWSE
富邦金控
中華郵政
國泰世華銀行 Cathay United Bank
財金資訊股份有限公司 FINANCIAL INFORMATION SERVICE CO., LTD.
玉山銀行
臺灣集中保管結算所 TDCC Taiwan Depository & Clearing Corporation
tsmc 台灣積體電路製造股份有限公司 Taiwan Semiconductor Manufacturing Company, Ltd.

政府、金融、交通、科技、醫療業及跨國公司資安服務

中華民國總統府 Office of the President Republic of China (Taiwan)
EVA AIR 長榮航空
AOI APPLIED OPTOELECTRONICS, INC.
nuvoTon DIRECT
ST Electronics
TH INDUSTRIES
IGS鈊象電子 http://www.igs.com.tw
winbond 華邦電子
LITEON 光寶科技
交通部臺灣鐵路管理局 Taiwan Railways Administration.MOTC 安全、準確、服務、創新、團結、榮譽
Panasonic
世界先進 VIS
中興保全 SECOM
tsmc 台灣積體電路製造股份有限公司 Taiwan Semiconductor Manufacturing Company, Ltd.

聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

團隊經驗與實績 - 獨家挖掘多個CVE漏洞

中華資安國際 CHT Security

	問題產品	分類	CVE編號	風險等級
2021	電子簽核平台	網站	CVE-2021-28171	9.8 CRITICAL
			CVE-2021-28172	7.5 HIGH
			CVE-2021-28173	9.8 CRITICAL
	公文編輯系統	網站	CVE-2021-22859	9.8 CRITICAL
			CVE-2021-22860	9.8 CRITICAL
2020	數位監控設備(DVR)	物聯網	CVE-2020-10514	8.8 HIGH
			CVE-2020-10513	6.5 MEDIUM
	校務資訊系統	網站	CVE-2020-10505	9.8 CRITICAL
			CVE-2020-10507	9.8 CRITICAL
	電子郵件系統	網站	CVE-2020-10511	9.8 CRITICAL
			CVE-2020-10512	8.8 HIGH
	電子郵件系統	網站	CVE-2020-5540	6.1 MEDIUM
			CVE-2020-5541	6.1 MEDIUM
	教育訓練系統	網站	CVE-2020-10508	7.5 HIGH
			CVE-2020-10509	6.1 MEDIUM
			CVE-2020-10510	6.5 MEDIUM
	電子郵件系統	網站	CVE-2020-3922	9.8 CRITICAL
	數位監控設備(DVR)	物聯網	CVE-2020-3923	9.8 CRITICAL
			CVE-2020-3924	9.8 CRITICAL
	數位簽章網頁元件	應用程式/金融	CVE-2020-3925	8.8 HIGH
			CVE-2020-3926	7.5 HIGH
			CVE-2020-3927	7.5 HIGH
	證券選股系統	網站	CVE-2020-3937	7.5 HIGH
			CVE-2020-3938	7.5 HIGH
			CVE-2020-3939	6.1 MEDIUM
	保全門禁系統	物聯網	CVE-2020-3933	5.3 MEDIUM
			CVE-2020-3934	9.8 CRITICAL
			CVE-2020-3935	7.5 HIGH

	問題產品	分類	CVE編號	風險等級
2019	電子郵件系統	網站	CVE-2019-15071	6.1 MEDIUM
			CVE-2019-15072	6.1 MEDIUM
			CVE-2019-15073	6.1 MEDIUM
	網路攝影機(IPCAM)	物聯網	CVE-2019-11064	9.8 CRITICAL
			CVE-2019-13405	9.8 CRITICAL
			CVE-2019-13406	7.5 HIGH
			CVE-2019-13407	6.1 MEDIUM
			CVE-2019-1348	3.3 LOW
	公文編輯系統	網站	CVE-2019-11232	9.8 CRITICAL
			CVE-2019-11233	7.5 HIGH
	數位學習系統	網站	CVE-2019-11062	9.8 CRITICAL
2018	SWIFT交易系統	網站/金融	CVE-2018-16386	7.5 HIGH

已累積取得40個CVE漏洞

- 利用PoC程式可遠端入侵數位學習系統
- 未登入狀態存取下洩漏公文系統密碼

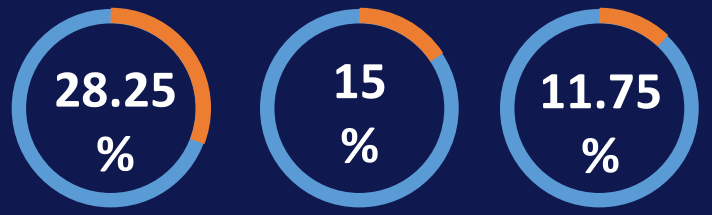
聯絡資訊 電話：(02) 2343-1628 Email：service@chtsecurity.com

團隊經驗與實績 - 近一年資安事件處理統計

中華資安國際 CHT Security

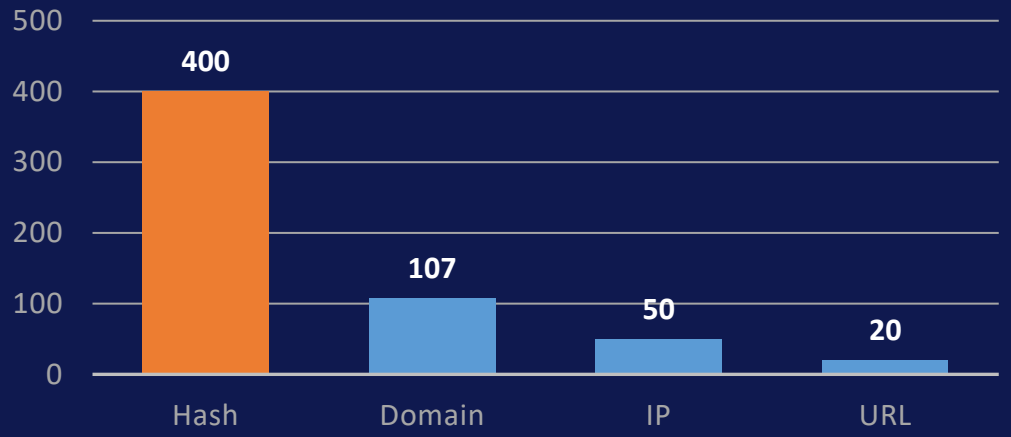
資安事件調查數量

惡意程式類型



- Payload 10.25%
- Trojan 7.75%
- Else 7%
- Downloader 5.75%
- Dropper 3%
- Miner 2.75%
- Stealer 2.25%
- Script 1.75%
- Keygen 1.5%
- Backdoor 1%
- Ransomware 1%
- Worm 0.5%
- MalDoc 0.5%

新發現威脅情資



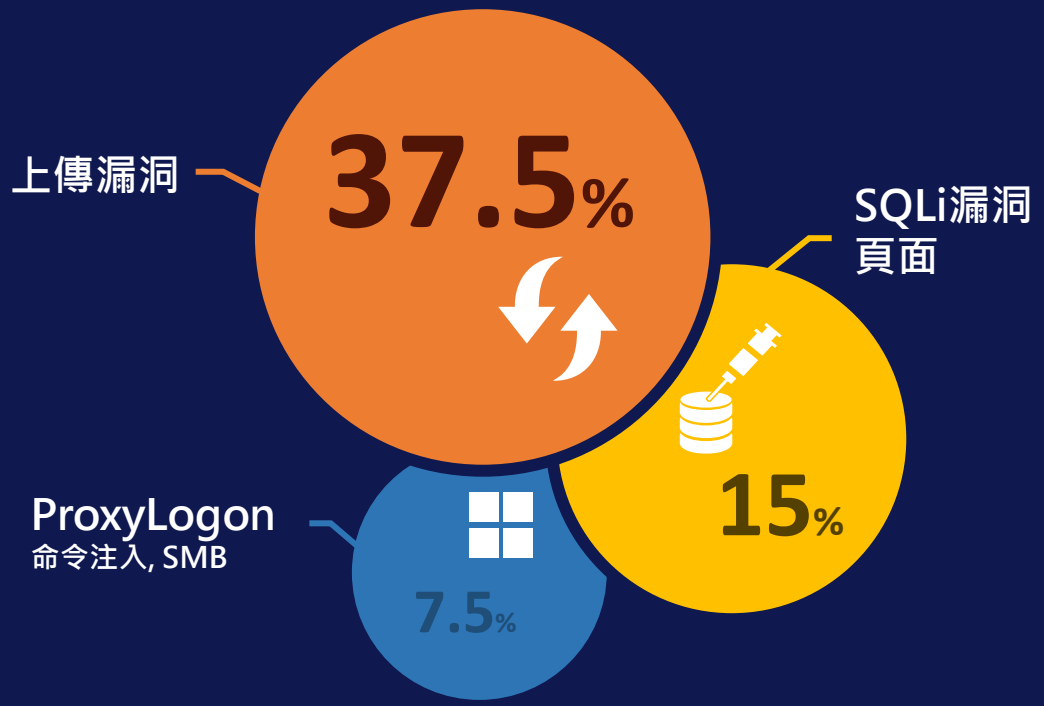
駭客入侵手法

1. Valid Accounts
2. Exploit Public-Facing Application
3. Drive-by Compromise& Trusted Relationship

團隊經驗與實績 - 近一年資安事件處理統計

中華資安國際 CHT Security

Exploit Public-Facing Application



駭客橫向移動方式

79.1%

利用遠端服務
(Exploitation of Remote services)

SMB和RDP等常見服務以及可能在內部網路中使用的應用程式中存在的漏洞

4%

使用認證資料
(Use Alternate Authentication Material)

攻擊者可能會使用替代身份驗證資訊，例如密碼雜湊值、Kerberos票證和應用程序訪問令牌，以便在環境中橫向移動並繞過正常的系統訪問控制

近期常見入侵案例分享及防駭方法

- ✓ 勒索病毒攻擊 (Targeted Ransomware Attack)
- ✓ 挖礦劫持 (Cryptojacking)
- ✓ 軟體/系統漏洞的威脅(Vulnerabilities)
- ✓ 資料外洩 (Data breach)

防駭方法_因應措施

IR應變與強化步驟

辨識惡意程式及徹底移除相關檔案

- 刪除惡意程式及其搭配工具
- 一併清查受影響範圍的系統

清除

增強資安體質及提升威脅抵抗力

- 修補已知的系統漏洞及脆弱點
- 調整網路架構及防火牆規則
- 部署資安防禦設備

強化

重建

確認系統安全及重新上線

- 確認部署的系統無異常檔案
- 進行系統上線前檢測

監控

檢視改善成效及管控潛在威脅

- 驗證修補措施的效用
- 及早偵測攻擊徵兆
- 評估潛在影響範圍

對應的**事前**解決方案

IT資安健診

- 網路架構檢視
- 網路惡意活動檢視
- 使用者電腦檢視
- 伺服器主機檢視
- 安全設定檢視

資安設備部署

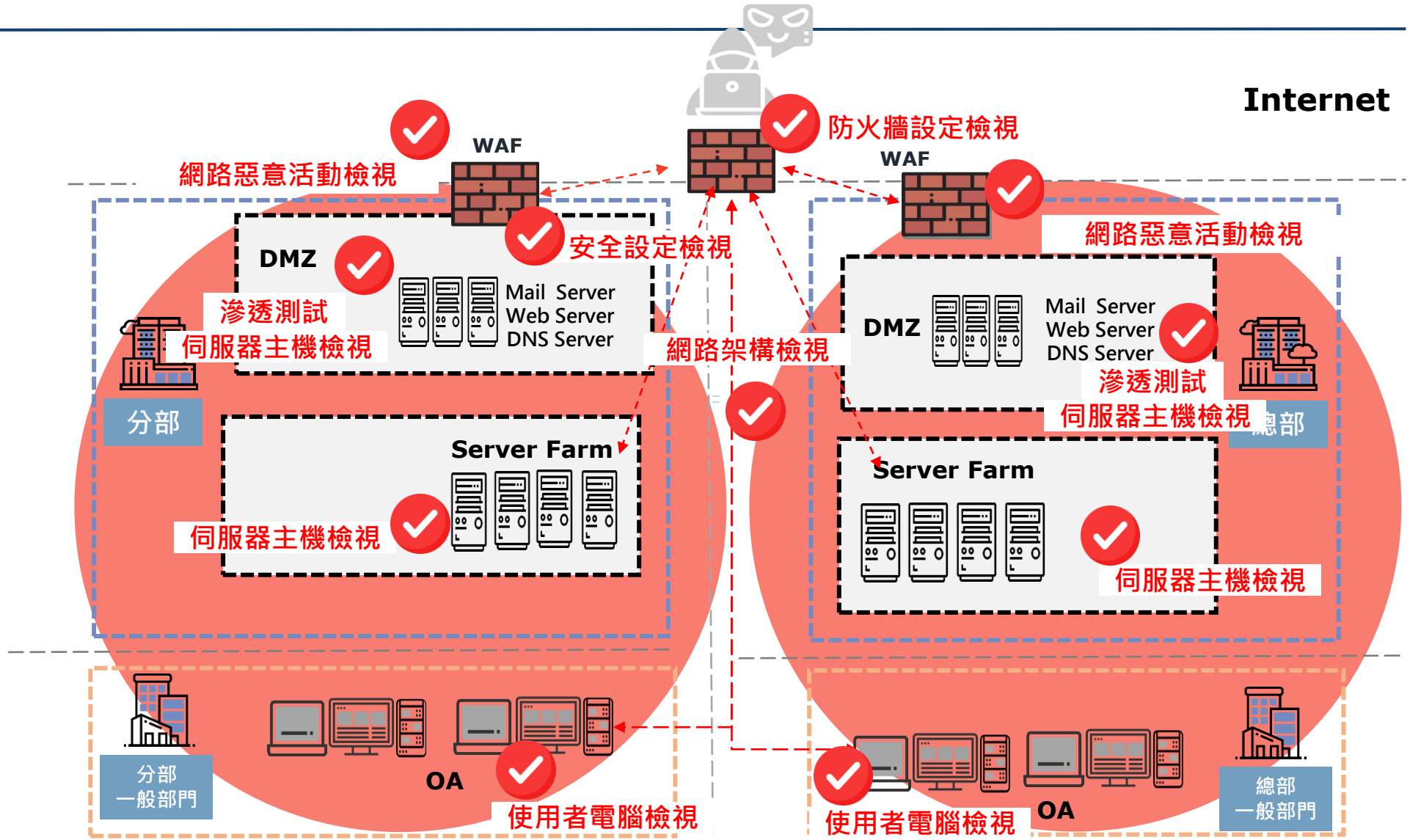
- WAF
- IPS

滲透測試

- 邏輯漏洞
- 輸入驗證
- Web Service

源碼檢測

- OWASP Top 10
- OWASP Mobile Top 10
- SANS Top 25



對應的**事中與事後**解決方案

IT SOC
- 7*24 IT SOC

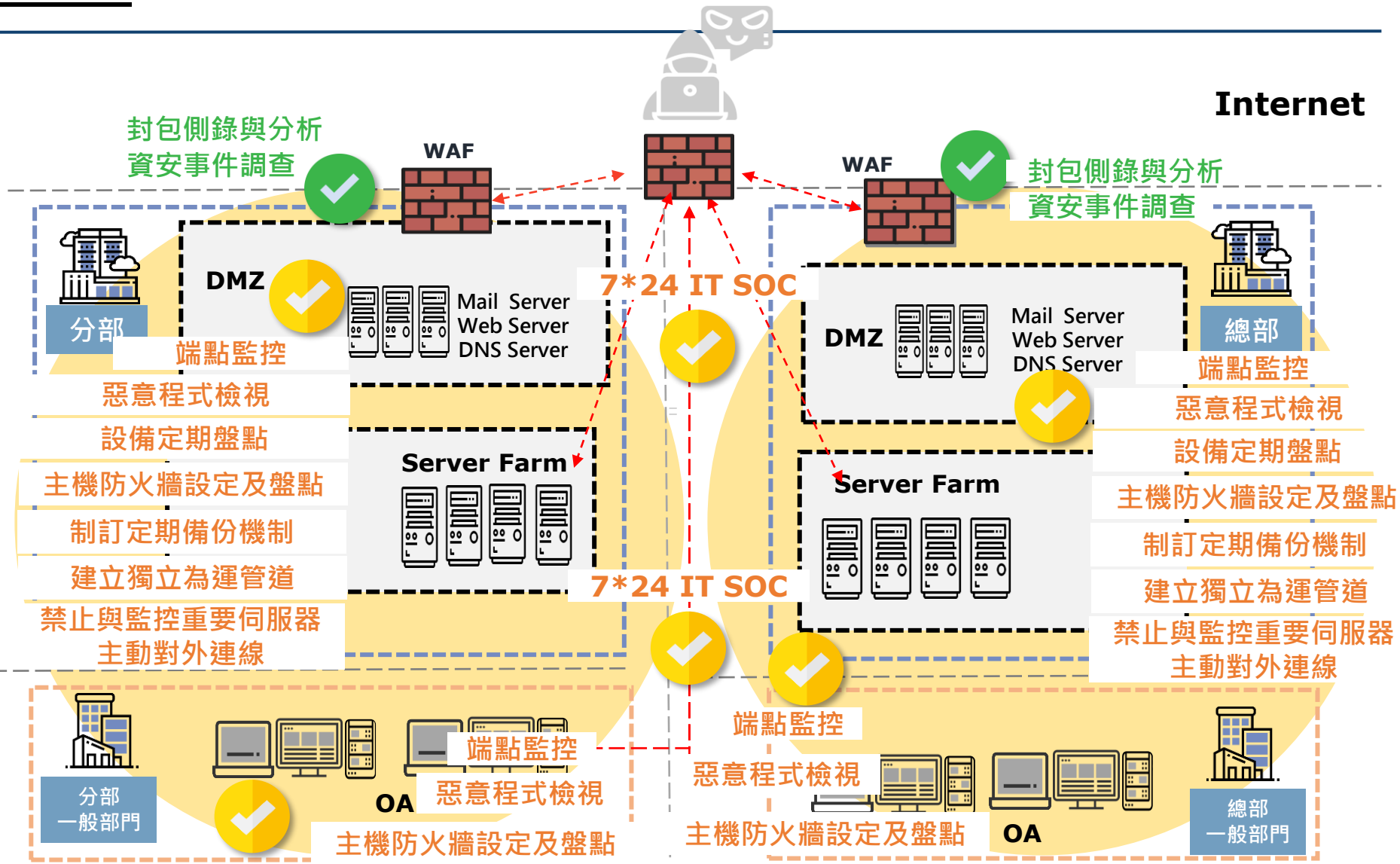
MDR
- 端點監控

切片快篩
- 惡意程式檢視

切片快篩
- 設備定期盤點
- 主機防火牆設定及盤點
- 制訂定期備份機制
- 建立獨立為運管道
- 禁止與監控重要伺服器主動對外連線

IR
- 資安事件鑑識調查

全時側錄
- 全時封包側錄與異常分析



勒索病毒感染應變建議

如何建置縱深防禦措施

網路隔離

1. 落實DMZ區與內部Server Farm區的完全隔離
2. 以白名單設定主機與網路防火牆規則，設定點對點規則至IP與Port，且避免遠端管理通訊埠暴露在Internet上
3. 將全區VPN主機版本更新至最新，並限縮使用者的登入來源IP，且導入雙因子認證

資安強化

1. 部署端點與伺服器防毒防駭偵測與MDR防禦機制
2. 部署閘道異常流量與惡意郵件偵測與防禦機制
3. 導入7x24 SOC 資安監控中心

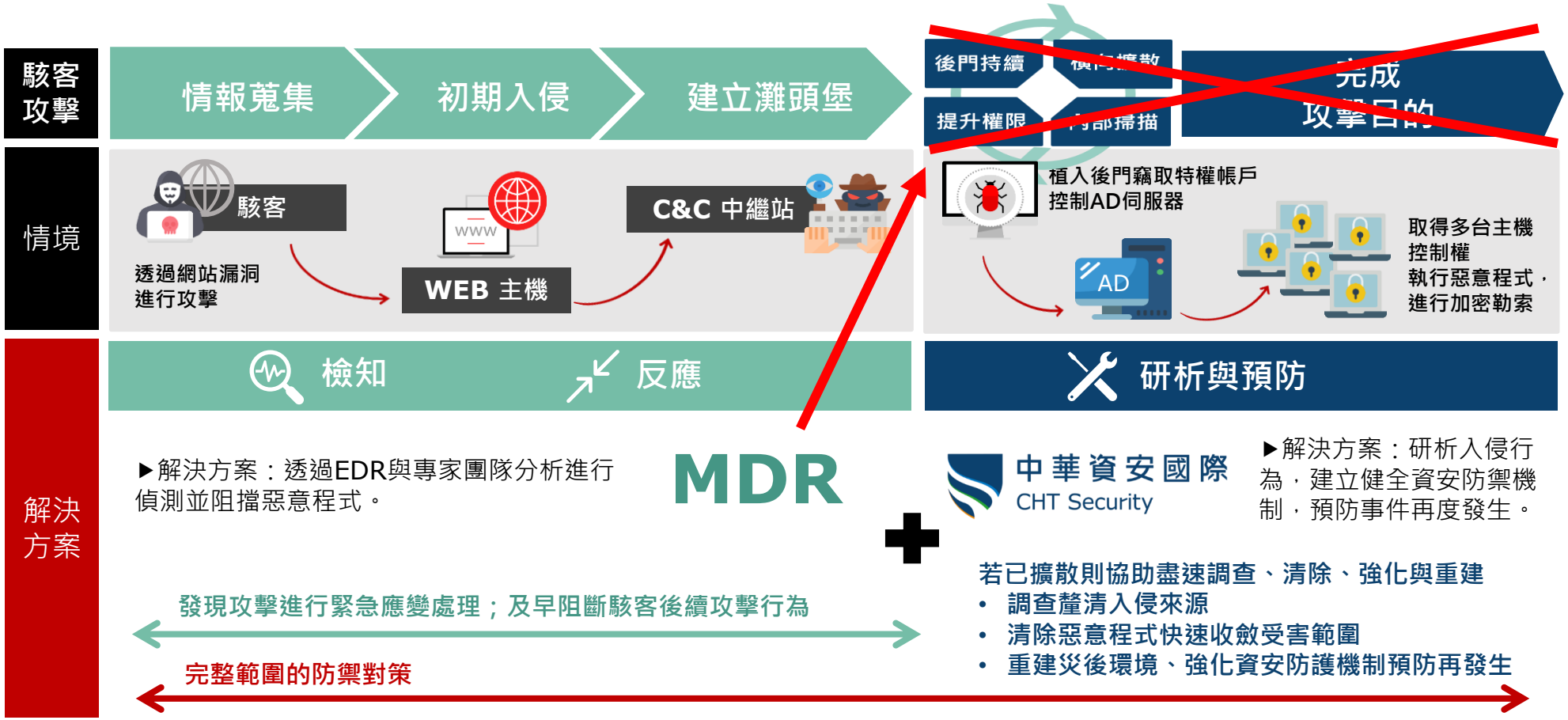
事前預防

1. 定期執行VA/PT/Code Review/Red Team/資安健診
2. 建立漏洞追蹤與管理機制，當對外服務介面(如：網站與VPN)出現漏洞時須即時加以修補，以抵擋攻擊
3. 落實異地備份備援機制，並定期演練

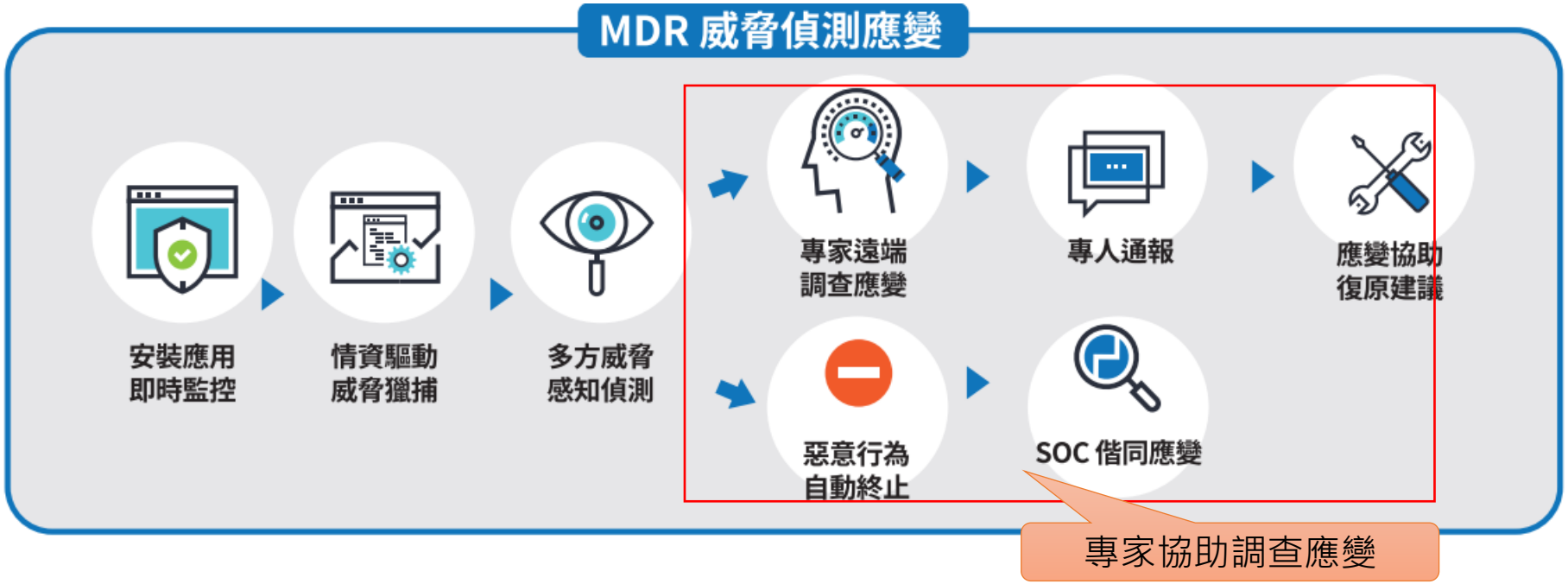
防駭方法_MDR

MDR(7*24端點威脅偵測與回應)

提升場域端點可視性，在初始入侵階段就切斷攻擊鏈



MDR (7*24端點威脅偵測與回應)



情資驅動 威脅獵捕

Intelligence-Driven Detection

監控端點活動軌跡
整合國內外情資進行威脅搜捕

即時監控 全時守護

7*24 Monitoring and Triage

全時監控，即時鎖定威脅範圍
專人即時通報及處理

即刻救援 有效阻斷

Response and Mitigation

遠端隔離主機、刪除惡意程式防止橫向滲透
IR團隊專業調查分析及應變

資安專家 定期體檢

Human Expertise for Consulting

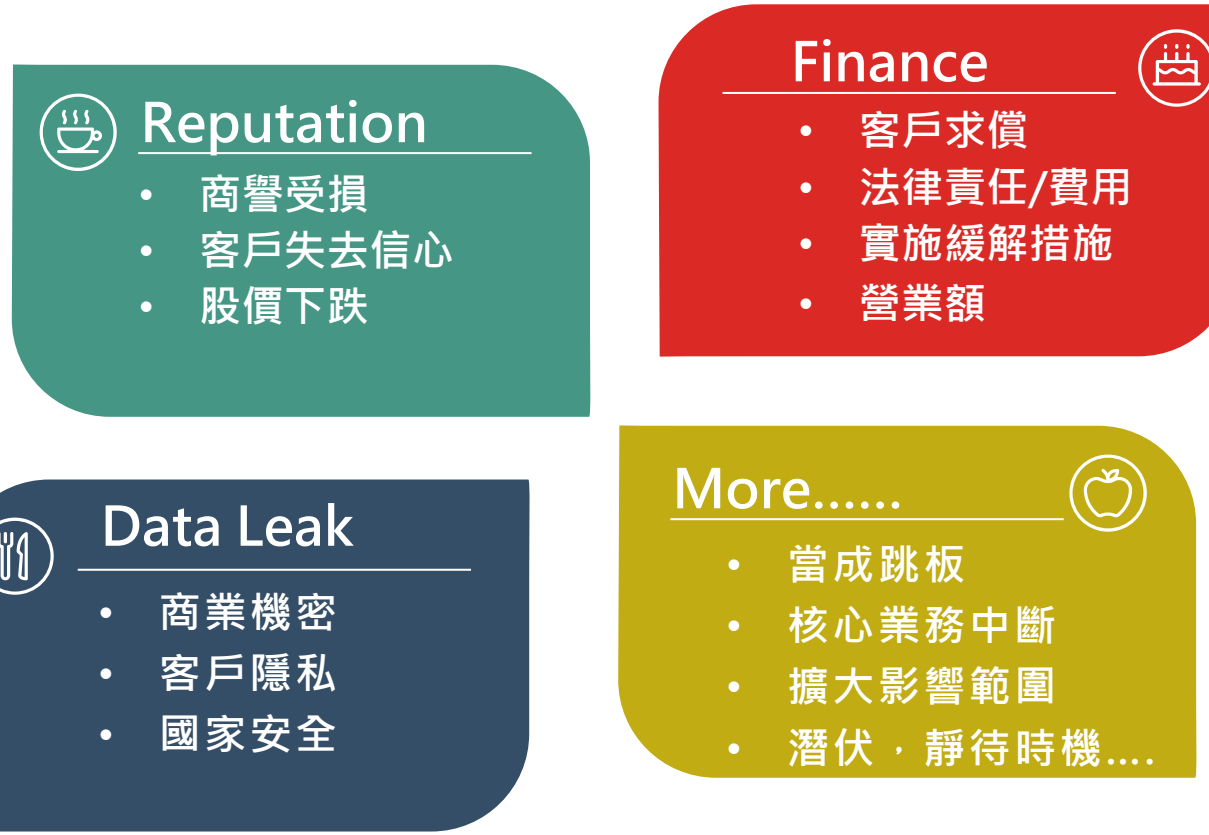
每月服務分析報告
專業IR團隊資安建議

資安事件應變實務

- ✓ 資安事件帶來的影響
- ✓ 實際資安事件處理流程

資安事件帶來的影響

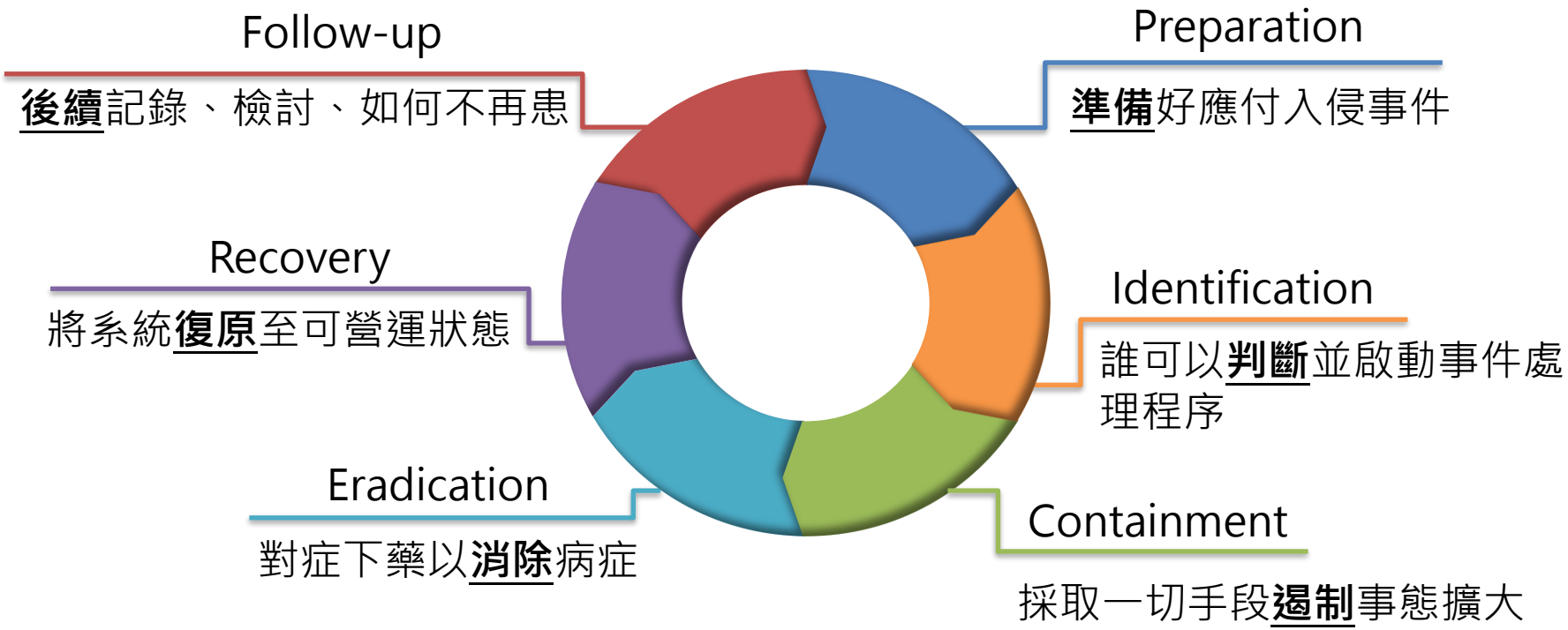
資安事件帶來的影響


Reputation
• 商譽受損
• 客戶失去信心
• 股價下跌
Finance
• 客戶求償
• 法律責任/費用
• 實施緩解措施
• 營業額
Data Leak
• 商業機密
• 客戶隱私
• 國家安全
More.....
• 當成跳板
• 核心業務中斷
• 擴大影響範圍
• 潛伏，靜待時機....

實際資安事件處理流程

資安事件處理建議步驟

SANS：Computer Security Incident Handling: Step-by-Step



實際資安事件處理流程

接獲需求/通報

通報來源：客戶本身、SOC監控中心
事件評估：人、事、時、地、何(Why)

事件處理

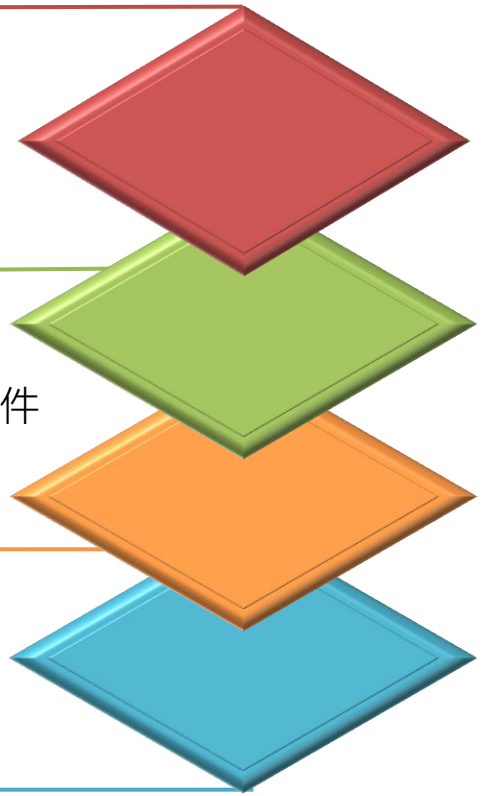
Incident Response (IR)
效果：快速止血、找出受害原因及時間軸，釐清事件真相

防禦策略修訂

根據事件處理結果，針對防禦弱點加強

回復至可持續營運狀態

面對災害發生，如何讓企業回復至正常(不受影響)狀態，以繼續營運



實際資安事件處理流程-接獲需求/通報

接獲需求/通報

通報來源：客戶本身、SOC監控中心

事件評估：人、事、時、地、何

告警規則遭觸發

事件通報單

SOC 7*24 監控中心

可疑的現象發生

收到黑函

客戶反應

客戶

鑑識工程師

實際資安事件處理流程-事件處理

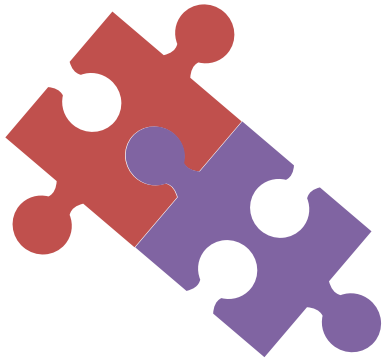
事件處理

- **Incident Response (IR) Team**：資安事件解決小組
- 效果：快速止血、找出受害原因及時間軸，釐清事件真相

CERT (Computer Emergency Response Team):
電腦緊急應變小組

主要業務之一就是負責協處國內的資安事件及發布資安警訊

台灣電腦網路危機處理暨協調中心
TWCERT/CC



CSIRT(computer security incident response team):
電腦資安事件應變小組

特別指跟電腦資安事件應變小組，組織本身的主要業務是資安事件處理

台灣電腦安全事件應變中心
TWCSIRT

實際資安事件處理流程-事件處理

日誌檔分析

Security.evtx
Application.evtx
System.evtx
Registry
etc.

記憶體分析

網路連線狀態
程式執行狀態
記憶體內存資料

(資安)設備
日誌檔分析

FireWall
Server
Database
Email
etc.

惡意程式分析

程式行為
是否有Hard Code
程式之間是否有關聯性

中華資安國際
CHT Security

實作課程

實作課程

- Lab_hackedcomputer
  - 主機遭駭，請利用主機上採好的採證檔找出惡意程式之路徑
    - 請善用Sysinternals Suite的工具與date_ip內的採證檔進行調查
  - 請驗證發現的可疑程式為惡意程式

中華資安國際
CHT Security

如有問題，請聯絡以下聯絡窗口資訊

- 電話：(02) 2343-1628
- Email：service@chtsecurity.com

Thank you!

中華資安國際Can Help!