中華資安國際
CHT Security

AI 世代下的資安威脅應對策略

中華資安國際股份有限公司
王信富 副總經理
2025.04.15

中華資安國際
CHT Security

01 中華資安國際簡介

中華資安國際簡介

登記時間 106年12月 | 實收資本額3.632億元| 員工 340人▲

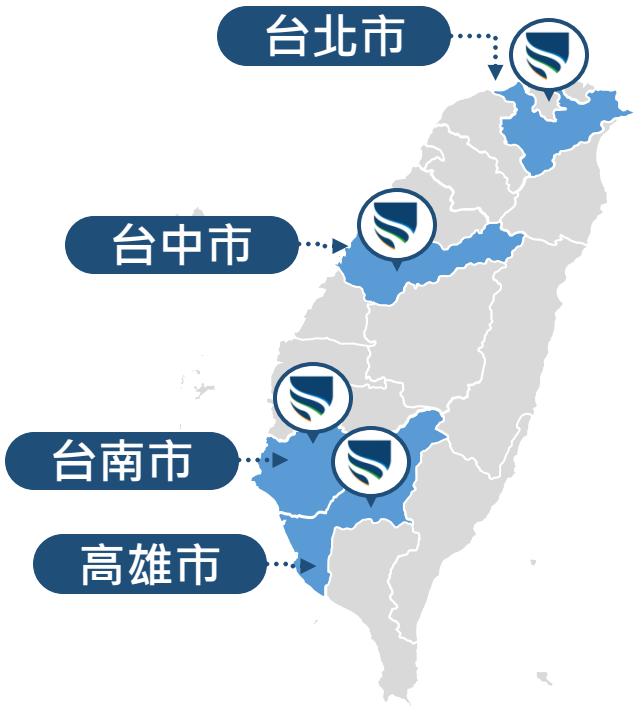
中華資安國際 CHT Security

中華電信集團旗下的資安專業公司

具備國家級資安專案建置能力與實績

2003年始經營資安業務，北、中、南區均有專業服務據點

提供事前檢測防護、事中監控應變、事後調查鑑識的資安服務



上網資安服務

對寬頻網路及行動網路的消費家庭、行動上網及企業客戶提供上網資安防護服務

資安專業服務

對客戶提供資安專業服務，包含資安檢測、SOC資安監控、MDR、資安事件應變與鑑識、ISMS顧問輔導等

商品銷售

引進國內外資安廠商軟硬體設備，助力客戶進行資安防禦與偵測應變管理，以及研發自有產品

專業能力連續多年榮獲國內、外獎項肯定

獲獎紀錄

2024
- 2018-2024年行政院資安服務廠商評鑑五項資安服務全數「A級」
- 2021-2024 Frost & Sullivan 台灣年度最佳資安服務公司大獎
- 2022-2024連續三年獲CIO Taiwan Elite Vendor「傑出品牌」
- Cyber Security Review 亞太區最佳滲透測試服務商
- 2024年正式成為全球規模最大的資安事件應變組織FIRST成員，與國際接軌經驗交流。

2023
- 2023 HITCON Cyber Range 第一名
- 2023 Frost & Sullivan 台灣年度最佳資安服務公司大獎
- SecuTex NP/ED 先進資安威脅防禦系統獲 2023 「CompuTex Best Choice 獎」
- CIO Taiwan 「資安產品與服務」傑出品牌獎

2022
- 行政院資安服務廠商評鑑五項資安服務全數「A級」
- 獲英國標準學會頒「 BSI 資訊韌性精銳獎」
- 獲選CIO Taiwan 2022 Elite Vendor「傑出品牌」
- SOC監控服務榮獲「CompuTex Best Choice Award資安服務獎」

2021
- 110年行政院資安服務廠商評鑑唯一五項資安服務全數「A級」之資安公司
- 台灣首家且於2022及2021皆榮獲 Frost & Sullivan「台灣年度安全託管服務商 (MSSP)

2020
- 行政院資安服務廠商評鑑五項資安服務全數「A級」
- 榮獲中華徵信所Top 5000服務業中排名第208名，「其他資訊服務業」排名第一名
- 榮獲BSI「 資訊服務品質深耕獎」
- 獲頒Top 10 Enterprise Security Startups in APAC 2020

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		108~113 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	AAAAAA	AAAAAA	AAAAAA	AAAAAA	AAAAAA
安O資訊	達標	達標	AA--AA	AA--AA	AA--AB	AA--AA	AA--AA
數O資安	達標	未達標	BABAAA	BBBBAA	A--BBA	B--BBA	A--BBA
果O數位	達標	達標	--BBCB	-----B	------B	------B	------
華O資訊	未曾參與共契評鑑						
知O系統	未曾參與共契評鑑						

-為該年度未參加廠商評鑑

資料來源：國家資通安全研究院

最大的共契資安服務商、實績涵蓋中南各場域

建立完整且嚴密的資安管理制度並取得5項國際認證

國際認證名稱	獲得認證時間	認證有效期
ISO 27001 資訊安全管理驗證	2018/06/25	2027/06/24
ISO 27701 隱私資訊管理系統驗證	2021/11/02	2027/06/24
ISO 20000 資訊技術服務管理驗證	2018/06/05	2027/06/24
ISO 17025 數位鑑識暨資安檢測中心驗證	2023/12/14	2026/12/13
IEC 62443 CBTL實驗室認證	2023/12/14	2026/12/13

專業能力連續多年榮獲國內、外獎項肯定

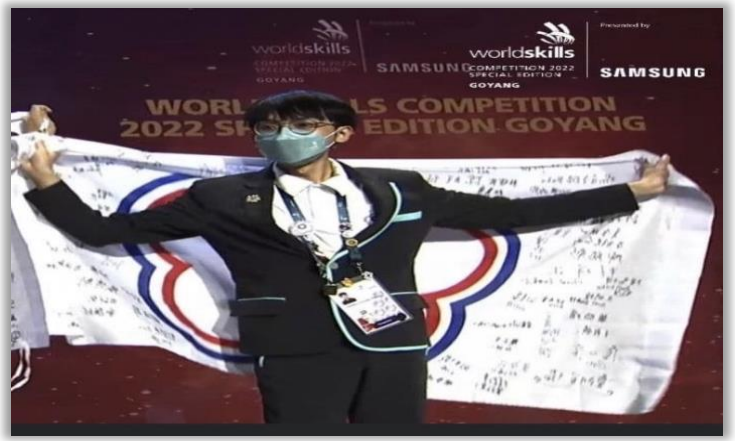
- 具備豐富經驗的紅(攻)、藍(防)隊專業團隊，可將此實務經驗整合至資安防護、監控應變等，協助提升企業資安防護成效

藍隊實力所向披靡

- 臺灣企業級難度最高的藍隊資安競賽 HITCON Cyber Range第一名

國際比賽屢獲佳績

- 代表國家出國比賽，取得「網路安全組：銀牌」WorldSkillsCompetition2022



國內最佳資安服務商

- 取得 2022「Computex Best Choice Award 資安獎得獎廠商」榮獲總統接見

獨家挖掘多個CVE漏洞

獨家挖掘多個CVE漏洞，已累積取得110+個CVE漏洞

原廠特別致謝

Citrix thanks Chiu TsungShu and Sheng-Fu Chang of CHT Security for working with us to protect Citrix customers.

Dell CVE-2024-49600: Dell Technologies would like to thank TsungShu Chiu (CHT Security) for reporting this issue.

年度	問題產品	分類	CVE編號	風險等級
2024年	電源管理軟體	軟體	CVE-2024-49600	HIGH
	遠端管理系統	軟體	CVE-2024-0740	CRITICAL
	身分認證系統	網站	CVE-2024-10653	HIGH
			CVE-2024-10651	MEDIUM
			CVE-2024-10652	MEDIUM
	內容管理系統	網站	CVE-2024-5514	CRITICAL
	數位學習系統	網站	CVE-2024-9980	8.8 HIGH
			CVE-2024-9981	8.8 HIGH
	財產管理系統	網站	CVE-2024-9972	CRITICAL
	郵件管理系統	網站	CVE-2024-4298	HIGH
			CVE-2024-4299	HIGH
	版本控管系統	網站	CVE-2024-1147	CRITICAL
			CVE-2024-1148	CRITICAL
	企業協同系統	網站	CVE-2024-26260	CRITICAL
			CVE-2024-26261	CRITICAL
	身份驗證App	APP	CVE-2024-4303	HIGH
	無線分享器	物聯網	CVE-2024-0570	9.1 CRITICAL
			CVE-2024-0569	9.1 CRITICAL

年度	問題產品	分類	CVE編號	風險等級
2023年	郵件管理系統	網站	CVE-2023-48378	7.5 HIGH
			CVE-2023-48380	8 HIGH
	端點管理系統(MDM)	網站	CVE-2023-41344	7.5 HIGH
	數位學習系統	網站	CVE-2023-35850	7.2 HIGH
			CVE-2023-35851	7.5 HIGH
	電子郵件防禦系統	網站	CVE-2023-48384	9.8 CRITICAL
	網路攝影機	物聯網	CVE-2023-38027	9.8 CRITICAL
			CVE-2023-38025	9.8 CRITICAL
			CVE-2023-38024	9.8 CRITICAL
	紅隊滲透工具	開源工具	CVE-2023-34758	8.1 HIGH
	郵件歸檔稽核系統	網站	CVE-2023-24840	7.2 HIGH
			CVE-2023-24841	7.2 HIGH
	線上藝廊平台	網站	CVE-2023-37152	9.8 CRITICAL
	人員招募系統	網站	CVE-2023-39551	9.8 CRITICAL
	傳真平台	網站	CVE-2023-28701	9.8 CRITICAL
	網路攝影機	物聯網	CVE-2023-28704	8.8 HIGH
	人力資源發展平台	網站	CVE-2023-20852	9.8 CRITICAL
			CVE-2023-20853	9.8 CRITICAL
	負載平衡系統	網站	CVE-2023-24838	9.8 CRITICAL
			CVE-2023-24837	8.8 HIGH
	郵件過濾平台	網站	CVE-2023-24835	7.2 HIGH
	企業協同系統	網站	CVE-2023-25909	9.8 CRITICAL
2022年	國際開源專案	套件	CVE-2022-41418	7.2 HIGH
	數位簽章網頁元件	元件/金融	CVE-2022-46304	8.8 HIGH
			CVE-2022-46306	8.8 HIGH
	企業協同系統	網站	CVE-2022-38118	8.8 HIGH
	Apache開源專案	套件	CVE-2022-45378	9.8 CRITICAL
			CVE-2022-40705	7.5 HIGH
	電子表單系統	網站	CVE-2022-32456	9.8 CRITICAL
			CVE-2022-32458	7.5 HIGH
	信件行銷系統	網站	CVE-2022-32963	7.5 HIGH
			CVE-2022-32964	9.8 CRITICAL
			CVE-2022-32965	9.8 CRITICAL
			CVE-2022-35216	7.5 HIGH
	知識庫筆記軟體	軟體	CVE-2022-36450	9.8 CRITICAL
	信件行銷系統	網站	CVE-2022-35223	9.8 CRITICAL
	端點管理系統(MDM)	網站	CVE-2021-44519	8.8 HIGH
			CVE-2021-44520	8.8 HIGH
			CVE-2022-26151	7.2 HIGH

年度	問題產品	分類	CVE編號	風險等級
2021年	程式開發套件	套件	CVE-2021-36483	9.8 CRITICAL
	門禁差勤系統	網站	CVE-2021-35961	9.8 CRITICAL
			CVE-2021-35962	7.5 HIGH
	數位學習系統	網站	CVE-2021-35963	9.8 CRITICAL
			CVE-2021-35964	9.8 CRITICAL
			CVE-2021-35965	9.8 CRITICAL
	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年	數位監控設備(DVR)	物聯網	CVE-2020-10514	8.8 HIGH
	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
	教育訓練系統	網站	CVE-2020-10508	7.5 HIGH
	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	元件/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
	保全門禁系統	物聯網	CVE-2020-3934	9.8 CRITICAL
			CVE-2020-3935	7.5 HIGH
2019年	網路攝影機	物聯網	CVE-2019-11064	9.8 CRITICAL
			CVE-2019-13405	9.8 CRITICAL
			CVE-2019-13406	7.5 HIGH
	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年	SWIFT交易系統	網站/金融	CVE-2018-16386	7.5 HIGH

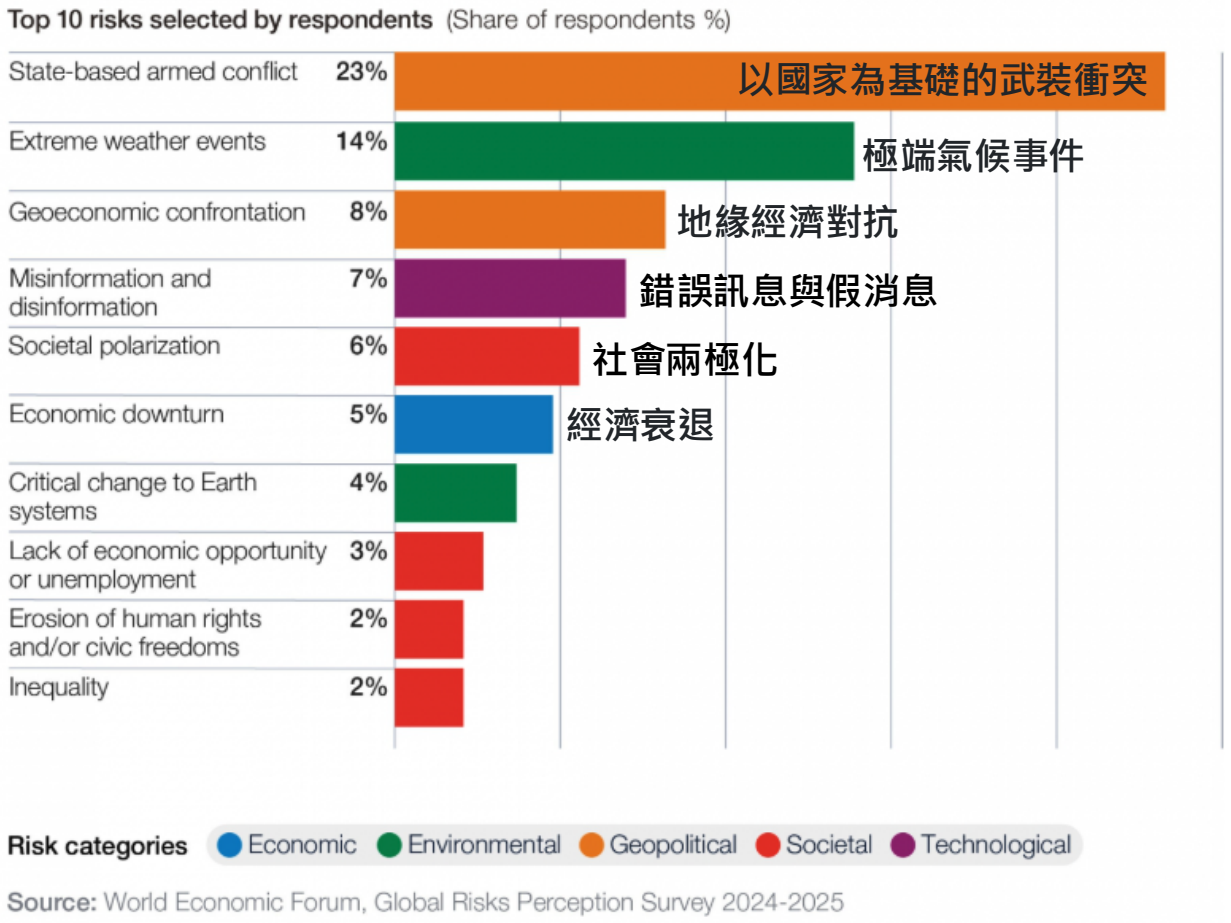
註: Common Vulnerabilities and Exposures, CVE

中華資安國際
CHT Security

02 全球資安威脅趨勢

WEF 2025 全球風險報告 - 假信息、網路間諜活動與戰爭風險甚鉅

- 根據WEF Global Risk Report 2025的調查，前十大風險項目如下：



- 根據WEF Global Risk Report 2025的調查，預測未來2年~10年依嚴重程度排序風險項目如下：

Reference : Global Risks Report 2025 | World Economic Forum
https://www.weforum.org/publications/global-risks-report-2025/

資訊戰與網路戰的融合

AI技術不僅降低了製造可信假訊息的成本和難度，使得針對品牌、信任和社會穩定的敘事攻擊更易發動，同時也增強了傳統網路攻擊的個人化程度和有效性。

敘事攻擊

AI生成虛假內容，損害品牌聲譽，影響併購交易

信任侵蝕

社會極化加劇，侵蝕公眾與機構間信任關係

網路入侵

利用混亂或不信任環境，實施竊取數據或破壞營運的攻擊

網路間諜活動的初始入侵往往依賴於社交工程或利用因假訊息而受損的信任關係

高階主管必須認識到，防禦網路威脅的範疇已擴展至包含對抗由AI驅動的複雜影響力作戰

Reference : The World Economic Forum: AI-Powered Narrative Attacks Remain Top Global Risk in 2025
https://blackbird.ai/blog/world-economic-forum-narrative-attack-top-global-risk/

塑造2025年資安格局的核心驅動力

2025年的網路安全環境正進入一個「前所未有的複雜」時代。多重因素疊加，使得風險管理極具挑戰性。72%的受訪組織表示過去一年中網路風險有所上升。

1 **地緣政治緊張加劇**

導致更不確定的環境，催生更多國家級資安攻擊和間諜活動

2 **新興技術快速採用**

特別是AI，在帶來機遇的同時也引入了新的漏洞

3 **供應鏈依賴性增加**

更複雜、更緊密交織的供應鏈導致風險環境更加不透明

4 **網路犯罪策略進化**

攻擊者利用新技術，手法日益精密 & 規模擴大

5 **監管要求激增**

全球範圍內不斷增加的法規雖旨在提升韌性，但也帶來合規負擔

5 **技能差距擴大**

持續存在的網路安全人才短缺問題，使得有效管理日益複雜的風險變得更加困難

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

2025年值得C-Level關注的關鍵AI驅動網路威脅

AI作為威脅放大器 、47%的組織將由GenAI驅動的敵對進展視為主要擔憂

AI驅動威脅	描述與機制	主要業務衝擊
超個人化釣魚/社交工程	GenAI利用抓取的資料創建極具說服力、針對性的電子郵件/簡訊/語音訊息	憑證竊取、金融詐騙、惡意軟體傳播
深度偽造	AI生成冒充高階主管或可信來源的虛假音訊/影片	金融詐騙（如電匯詐騙）、聲譽損害、繞過身份驗證
AI輔助惡意軟體/勒索軟體	AI協助創建惡意軟體變種、改進規避技術、增強勒索軟體誘餌	資料外洩、營運中斷、財務損失
自動化攻擊系統	AI工具自動化偵察、漏洞利用和橫向移動	更快的入侵速度、更廣泛的系統受損、攻擊量增加
敘事攻擊/假訊息	AI規模化創建/傳播針對品牌或信任的虛假資訊	聲譽損害、股價操縱、社會動盪關聯

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

企業AI應用：機遇與新風險並存

企業正加速採用AI以推動創新、提高效率並獲取競爭優勢

趨勢是從概念驗證階段邁向更廣泛的部署，旨在實現生產力提升和自動

66%

AI影響認知

組織預計AI將在2025年對資訊安全產生最顯著的影響

37%

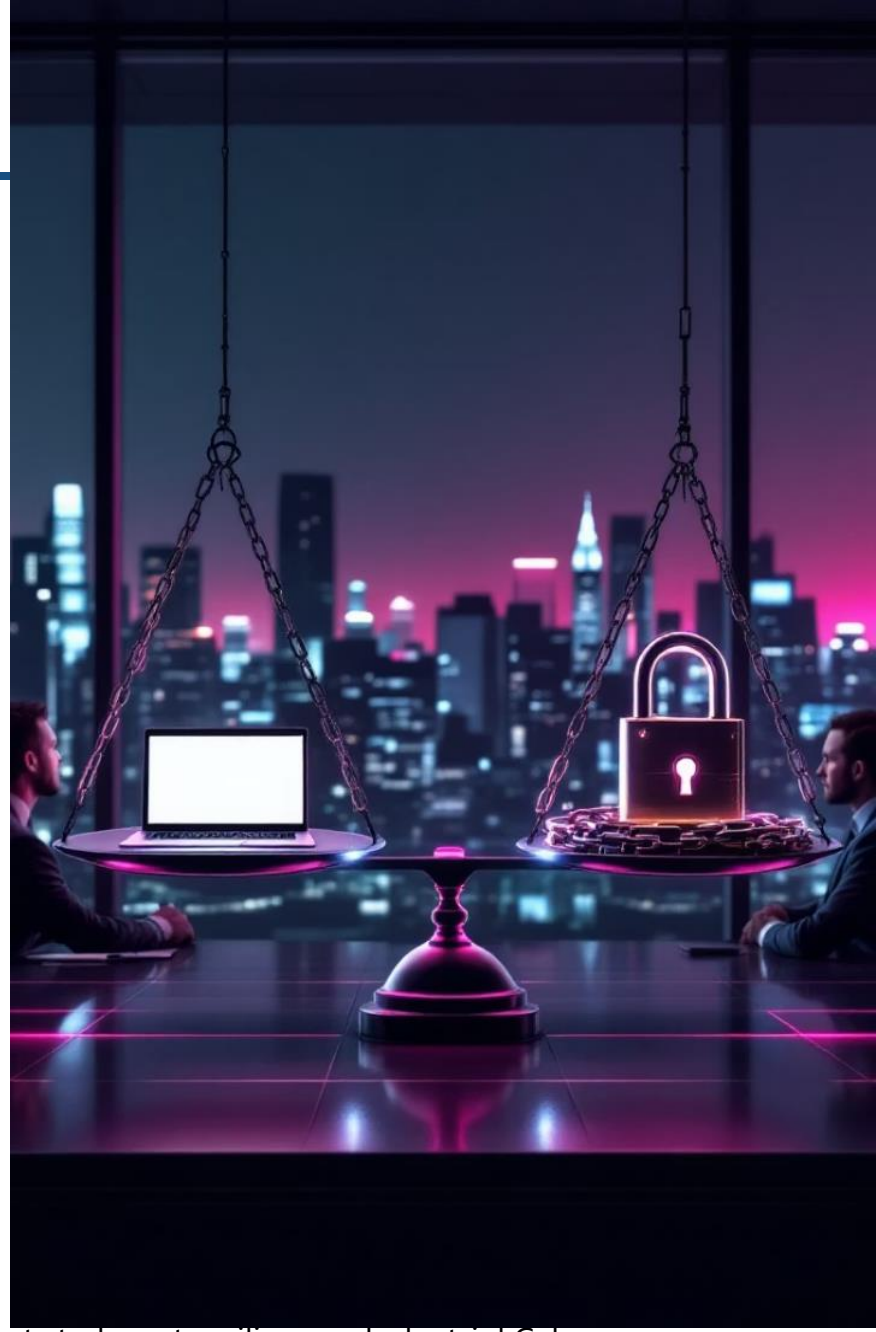
安全評估

組織建立了在部署前評估AI工具安全性的流程

20%

影子AI風險

員工未經授權使用AI工具的預估比例



在推動AI創新的同時，實施強健的風險管理，確保AI專案符合整體業務目標，並處於組織風險承受範圍之內

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

AI引發的關鍵資安風險

- 導入AI應用系統會產生新的脆弱點並擴大攻擊面
- AI安全與資料安全之間存在密不可分的關係、AI模型的效能和可靠性取決於訓練資料的品質和完整性

資料中毒

攻擊者操縱訓練資料以破壞AI模型，導致模型產生偏見或錯誤的輸出

模型竊取

竊取專有的AI模型，代表重大的智慧財產權損失

影子AI

員工未經批准使用AI工具，給資料安全和合規性帶來重大風險

提示注入

攻擊者精心設計惡意輸入，使大型語言模型產生意外行為，可能洩露敏感資料

AI工具自身漏洞

企業使用的AI驅動工具，在部署前必須經過嚴格得安全漏洞測試

攻擊面擴大

特別是連接到其他網路或資料源的系統，為攻擊者提供了新的入侵點

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

AI風險識別框架

資產盤點

識別所有AI系統及其訪問的資料類型、重要性與敏感度。

威脅建模

分析潛在攻擊媒介、攻擊者動機與可能的攻擊方式。

漏洞評估

檢測AI系統中的技術漏洞與流程缺陷。

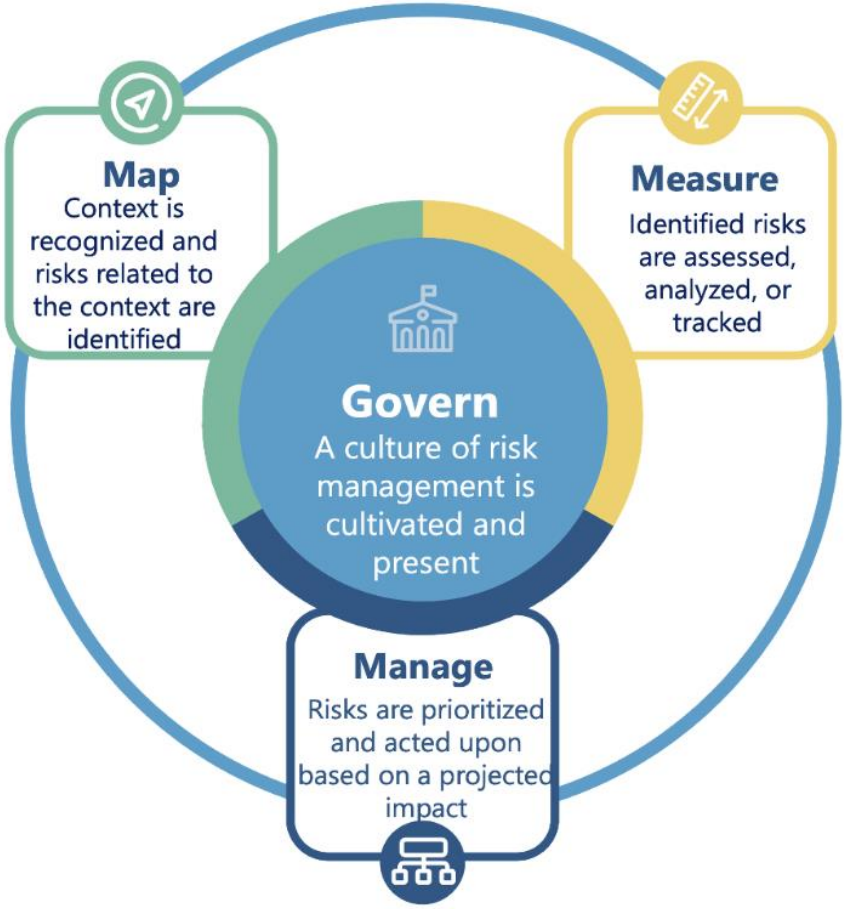
風險量化

評估每項風險的可能性與潛在影響，確定風險優先級。

持續調整

隨AI技術發展不斷完善風險識別方法

NIST AI RMF Core



美國NIST的AI RMF和歐盟的AI法案為組織提供了結構化方法來識別、評估和降低AI相關風險。

AI資安風險控管策略

安全設計原則

將資安考量納入AI開發全生命週期，實現安全設計。

- 開發初期即導入安全審核
- 資料最小化原則
- 預設加密策略

監控應變與稽核

建立全面監控機制，即時偵測異常活動。

- AI行為記錄與威脅偵測
- 持續監控、確保及時可視性
- 制定AI事件回應計劃

防禦縱深

構建多層次防禦架構，避免單點失效。

- 識別模型風險，實施安全控制與資料存取控制
- 模型隔離機制，或採用加密模型，限制資訊推斷
- 持續滲透測試

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

企業AI安全治理模型

高階領導層責任制

明確C-level主管在AI安全中的角色與責任

政策與標準

制定AI安全政策、標準與指導方針

專責團隊

建立AI安全專家團隊，負責實施與監督

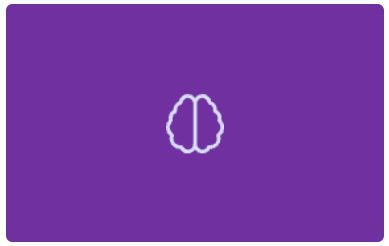
合規與認證

確保符合行業標準與監管要求

有效的AI安全治理模型應融入企業整體資安架構，確保協調一致的安全防護。

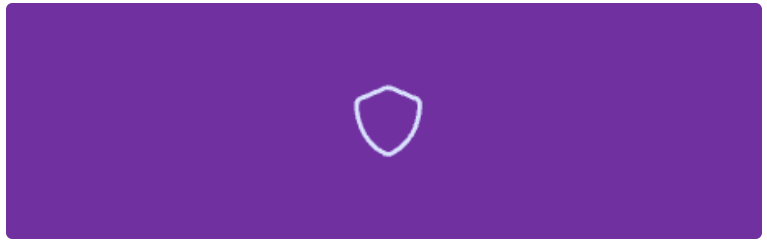
Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

AI世代下的資安思維



理解AI的雙重角色

AI既是攻擊工具，也是防禦關鍵



建立全面防禦體系

涵蓋風險識別、控制與資源配置

保持韌性與適應性

持續調整策略應對演變中的威脅

企業必須將資安融入AI應用的每一個階段，從設計到部署再到營運，建立起一道堅固的防線。

在AI這場持續進行的網路安全競賽中，唯有具備韌性和適應性的安全態勢，才能確保企業在未來持續發展和成功。

Reference: WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber
https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

帶來資安威脅的不只是AI ...

持續存在與持續演變的資安威脅

勒索軟體攻擊升級

攻擊策略已從單純加密演變為「雙重勒索」(竊取數據+加密)甚至多重勒索 ，增加了對受害者的壓力及攻擊的影響力
GenAI可能通過製作更有效的誘餌來提高勒索軟體的成功率 。醫療保健、製造業、金融 仍然是主要攻擊目標

內部威脅

由AI驅動的、針對員工的社交工程攻擊加劇了內部威脅 。憑證竊取仍然是一個嚴重問題。遠程工作的普及擴大了端點受損和數據外洩的攻擊面

雲端基礎設施漏洞

72%重大資料外洩與雲端配置錯誤有關。

供應鏈攻擊增加

供應鏈的複雜性、缺乏可見性以及對第三方供應商的依賴，創造了重大的脆弱點 。
攻擊者常通過攻擊供應商來滲透到更大的目標組織

Gartner 對企業資安威脅的分類

Top Threats

定義:組織高度意識到威脅，並且由於潛在的變化而年復一年地保持相關性

- Malware-Ransomware
- Evolving Phishing Tactics
- Employee Account Takeover

High-momentum threats

定義:威脅正在高度成長，但對此的認識尚未達到與Top Threats 相同的程度

- Customer Account Takeover
- Cloud Risks
- API Abuse
- Targeted Attacks on Cyber-Physical Systems (CPS)

Uncertain threats

定義:新的和潛在的威脅，屬於低信號威脅，可能是危險的，也可能是過度炒作的、分散注意力的

- Attackers Using AI
- Attacks on AI
- Nontechnology Threats
- Employee activism

中華資安國際
CHT Security

03 台灣資安威脅趨勢

臺灣常見的資安威脅

01

DDoS攻擊

02

APT攻擊

03

勒索軟體

04

利用網通Edge與物聯網裝置入侵

05

供應鏈攻擊

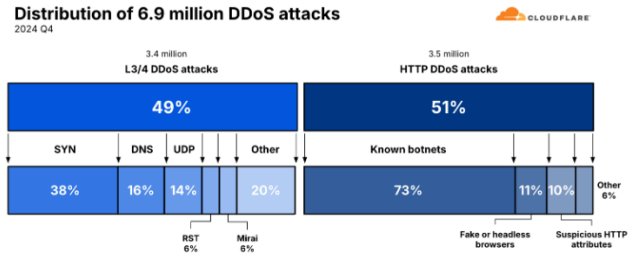
06

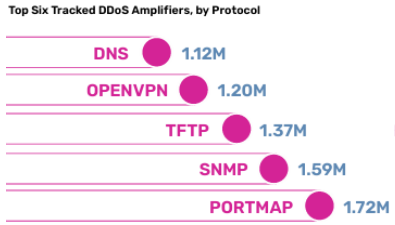
假訊息與詐騙

2024年國內DDoS最大攻擊流量為224Gbps

全球 DDoS攻擊趨勢(2024)：

- 2024 DDoS攻擊頻率持續上升，攻擊次數較去年成長53%，最大攻擊流量達5.6Tbps (by Mirai botnet)
- L3/L4 DDoS攻擊佔54%，其中主要類型為DNS Flood攻擊(27%)，其次為 SYN Flood攻擊(24%)
- HTTP DDoS攻擊佔另外的46%，其中主要類型為已知Botnets攻擊(65%)，其次為Headless browser (16%)
- 放大反射攻擊使用的協定前三名為SSDP、DNS和OpenVPN
- 五月有16%的用戶遭DDoS攻擊者威脅或勒索，其次為六月與十二月的14%，且在第四季有逐月增加的趨勢
- 目標地區前三名為中國、香港和新加玻，台灣在Q4躍升為第三名
- 目標產業前三名為資訊科技、電信和網際網路





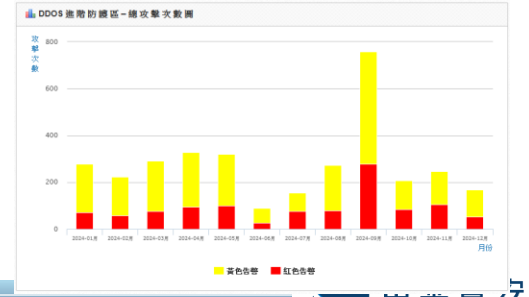
來源: CLOUDFLARE DoS threat report for 2024 Q1 - Q4
來源: 2024 DDoS Weapons Report – A10 Networks

CHT Security SOC 觀察(2024)：

- 2024年國內平均每天發生約35次攻擊
- 2024年最大攻擊量(8月)達224Gbps (UDP Flood) ，攻擊以HTTP Flood (37%)為大宗
- HTTP Flood較去年成長42%，駭客組織利用Botnet針對特定網站發動攻擊，透過大量請求造成網站無法對外提供服務，建議導入CDN、WAF或DDoS防護服務
- DNS Flood較去年成長44%，IoT 設備易於入侵且不易發現，成DDoS攻擊來源主力，建議DNS伺服器須建立DDoS防護機制，或申租DNS代管服務
- 遭攻擊對象偏重證券業(19.8%)、貨幣中介業 (17.8%) ，其次為機械器具批發業、資訊服務業、主機及網站代管服務業等
- 最長攻擊時間為1442分鐘(DNS Flood、12月)、持續時間小於10分鐘的攻擊佔了73%

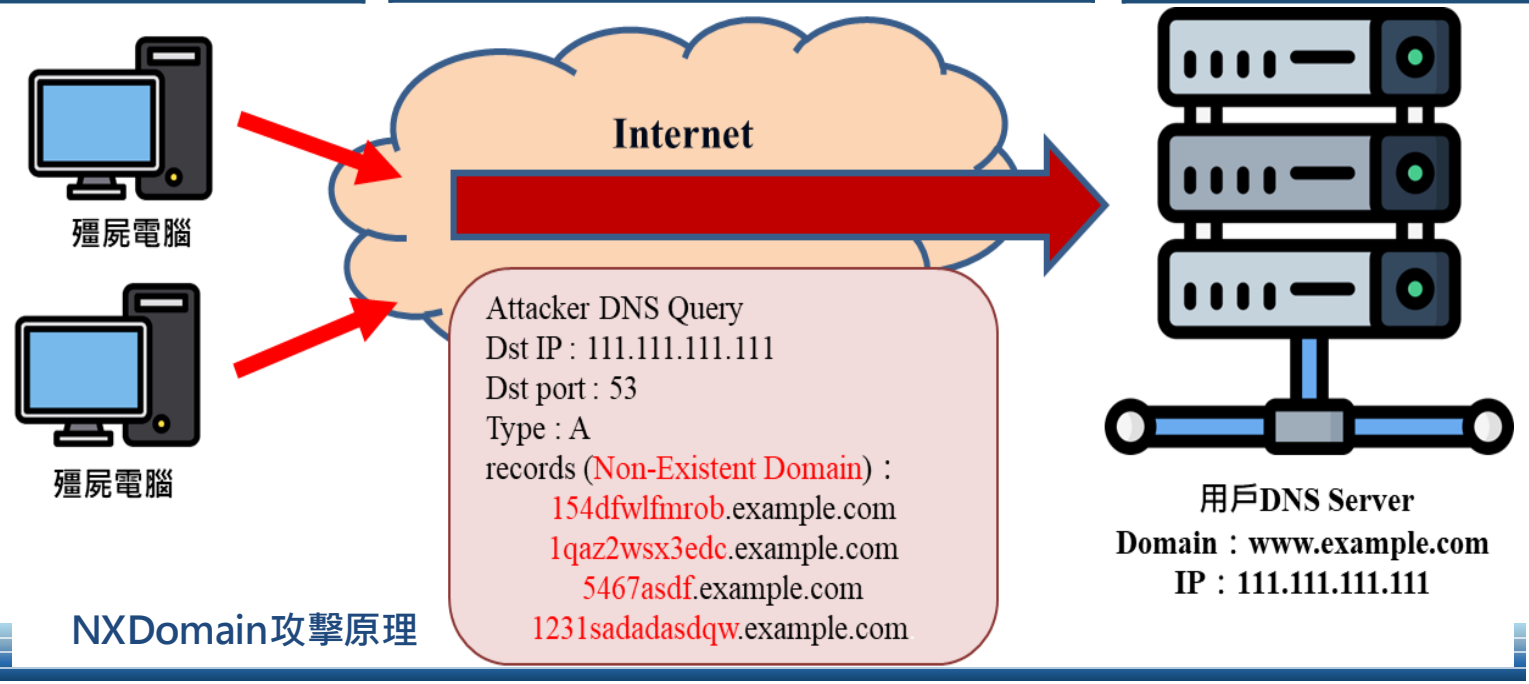
遭受DDoS攻擊客戶類型 (2024)

HiNet DDoS攻擊次數 (2024)



2024年DDoS攻擊案例分享(1)

案例說明	應變方式	建議措施
• 6-7月發生多起**DNS Flood攻擊**，範圍涵蓋政府機關、金融業、資訊科技業、製造業、運輸業影響用戶DNS服務與對外系統運作 • DNS Flood類型皆為**NXDomain攻擊**，屬**資源消耗型**，攻擊量最大約100Mbps，透過**高RPS**(Requests Per Second)的DNS查詢(**查詢Non-Existent Domain**)癱瘓用戶DNS服務	• 協助用戶導入**DDoS防護服務**緩解攻擊 • 協助用戶**監控DNS服務與對外系統**運作情形 • 必要時於防護設備加入**用戶網域白名單**阻擋不存在的網域查詢	• DNS伺服器導入**DDoS防護機制** • 申租**DNS代管服務** • 定期執行**DDoS攻防演練**



NXDomain攻擊原理

2024年DDoS攻擊案例分享(2)

案例說明

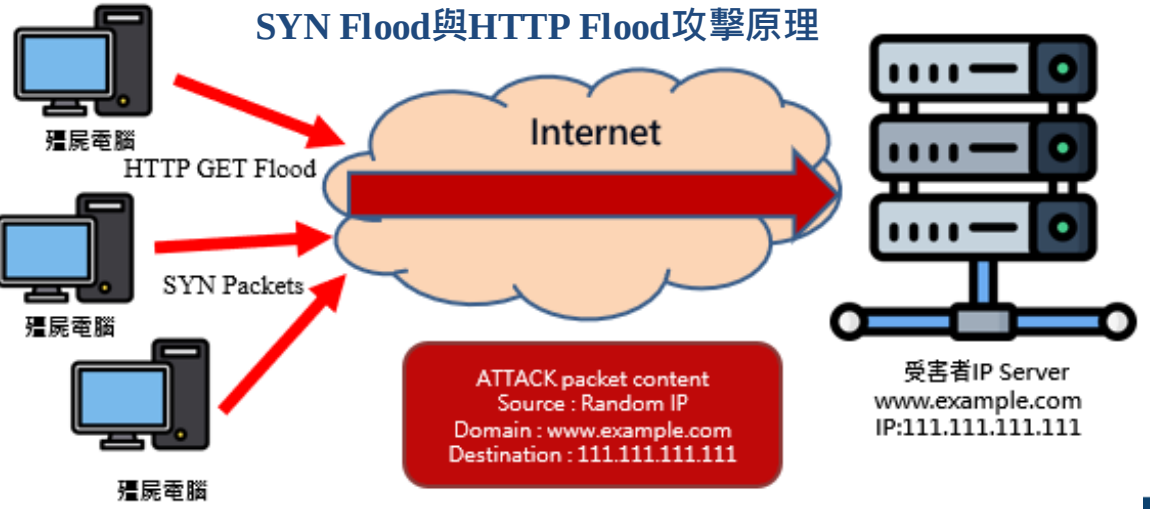
- 於 9/10-9/13 期 間 ， **親 俄 駭 客 組 織 NoName057 與 RipperSec**陸續對台灣政府與非政府單位發動DDoS攻擊，影響用戶對外網站運作
- 期間觀察到駭客主要使用**SYN Flood**與**HTTP Flood**也輔以ACK Flood、PUSH-ACK Flood進行攻擊，攻擊量大約介於10Mbps - 25Mbps
- SYN Flood原理為**發送大量SYN封包**給網站，利用三項交握讓網站處於**半開模式(Half Open)**，導致網站資源耗盡無法提供服務
- HTTP Flood原理為**發送大量請求封包**給網站，若網站沒有資源同時處理這些封包，就會無法提供服務

應變方式

- 協助用戶導入**DDoS防護服務**緩解攻擊
- Botnets來自於俄國與烏克蘭，於防護設備開啟**國別阻擋功能**攔阻相關國別的IP
- 協助用戶**監控對外網站**運作情形

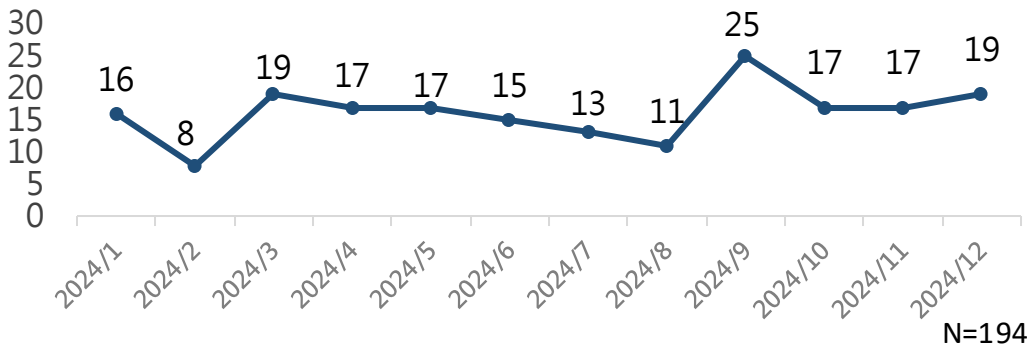
建議措施

- 導入**CDN服務**，請求由CDN端回覆，減少原站負擔
- 導入**WAF服務**或**DDoS防護服務**緩解攻擊
- 以**雲地聯防**的概念，透過**雲端**防護機制做第一層流量清洗，再透過**地端**防護設備做第二層的進階防禦
- 定期執行**DDoS攻防演練**

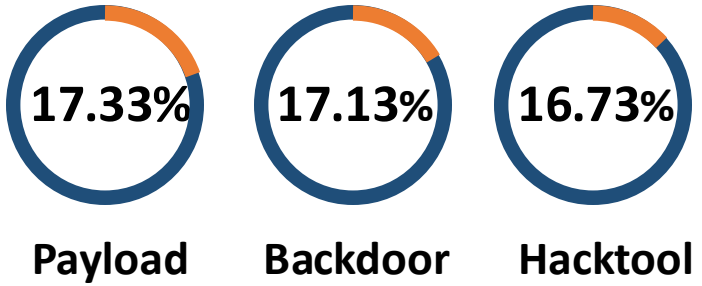


從2024年資安事件處理統計結果看問題(1/2)

資安事件調查數量

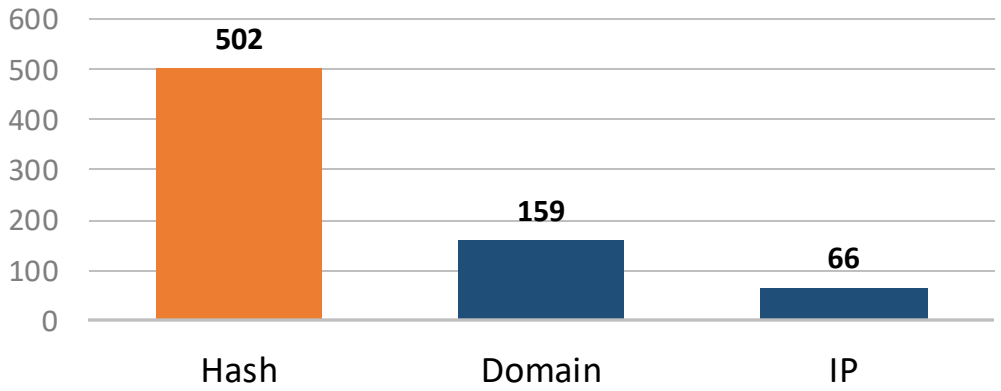


惡意程式類型



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%
Trojan 0%
Worm 0%
Keygen 0%

新發現威脅情資

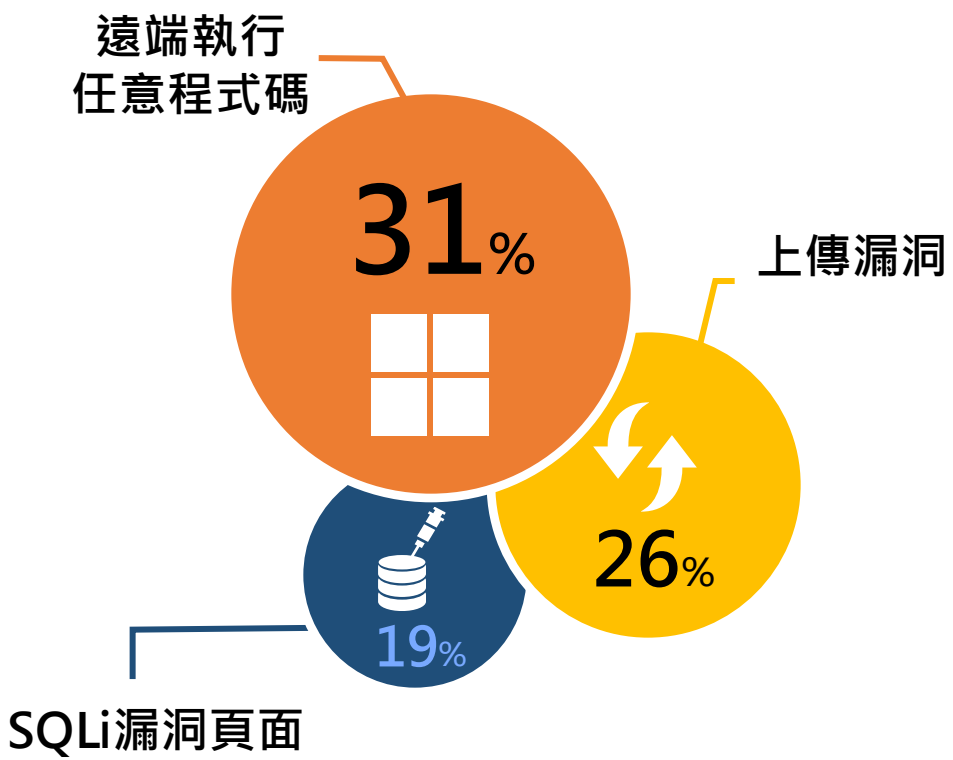


駭客入侵手法(Initial Access)

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

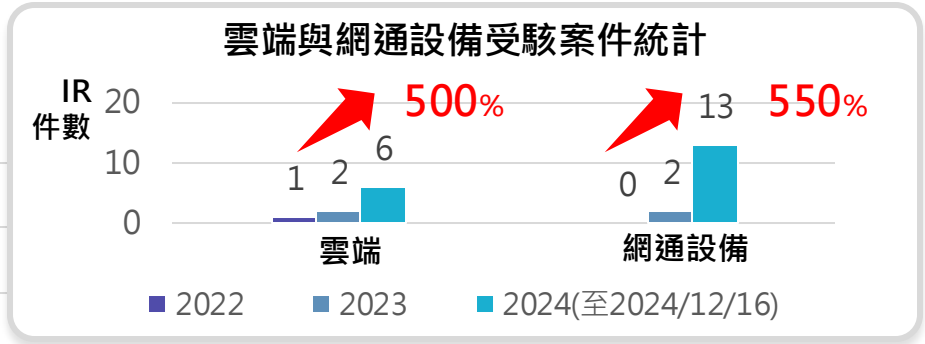
Gartner

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)

資安事件緊急應變服務 - 資安事件趨勢分析

■ 客戶受駭事件依產業別與年份統計(來源：CHTS IR MISP資料庫)

從2018統計至2024，關鍵基礎設施、製造業、運輸業與醫療業的IR案例數量有顯著增加，雲端環境及網通設備受駭案件呈現逐年上升趨勢



	中央	地方	基礎建設	教育業	服務業	科技業	製造業	資訊業	運輸業	醫療業	金融業	電子業
2018	0	2	0	2	0	0	0	0	0	0	0	0
2019	3	8	0	0	0	0	0	2	0	2	2	1
2020	35	37	2	2	2	0	3	15	0	16	7	3
2021	43	59	5	5	6	0	6	6	0	17	14	3
2022	48	60	6	1	3	4	13	13	1	16	8	7
2023	40	61	5	3	7	2	17	9	1	21	10	2
2024(至2024/12/16)	37	37	3	1	7	0	7	6	7	13	2	4

IR 件數

從2024年資安事件處理統計結果看問題(2/2)

Our findings are the same as Gartner's

Top Cybersecurity Trends in 2024

Optimizing for Resilience

TOP1 - Continuous Threat Exposure Management
TOP2 - Extending IAM's Cybersecurity Value
TOP3 - Third-Party Cybersecurity Risk Management

根據這些調查結果，我們可以總結出幾個關鍵的資安風險趨勢：

1. 合法帳號濫用：是多個產業的主要入侵管道，突顯了身份和存取管理的重要性。

2. 公開漏洞利用：面向公眾的應用程式和服務仍然是主要的攻擊目標。

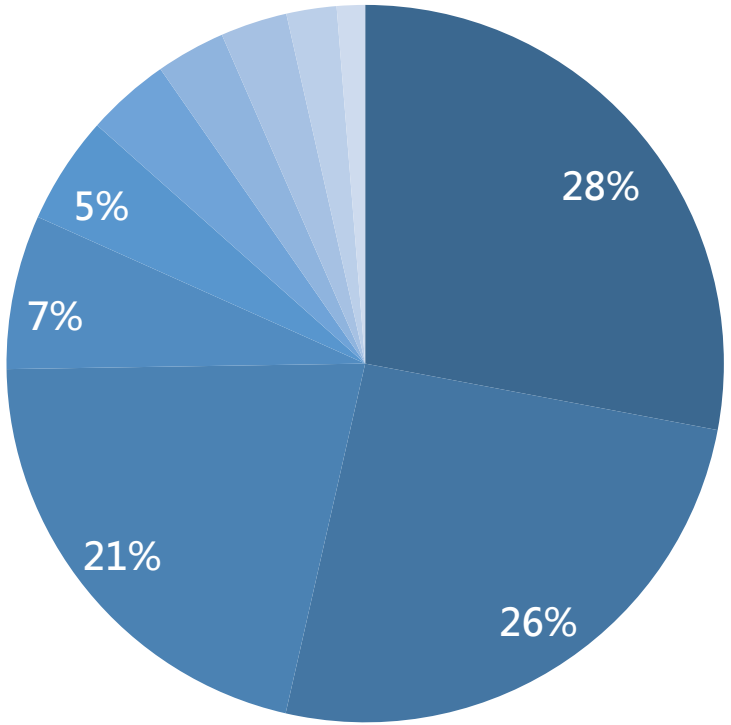
3. 供應鏈風險：子公司或合作夥伴可能成為攻擊的入口。

4. 關鍵基礎設施的特殊風險：網路設備和遠端存取成為重要的攻擊目標。

【中華資安國際】紅隊演練及滲透測試發現資安風險趨勢

2024 全年資安檢測統計，針對 280 個以上組織，挖掘超過 7,000 個風險漏洞，其中約 2,000 個高風險漏洞

中華資安國際2024年10大高風險漏洞風險統計



- 高 跨站腳本攻擊(XSS)
- 高 SQL injection
- 高 權限跨越
- 高 弱密碼
- 高 任意檔案上傳
- 高 敏感資訊洩漏
- 高 下載弱點
- 高 身分驗證方式瑕疵
- 高 標頭注入(Header Injection)
- 高 功能惡用

資料來源：CHT Security PT Team 2024年統計

常見前三大發現事項及風險

跨站腳本攻擊 (XSS)

注入惡意HTML或JavaScript語法至頁面，輕則造成企業聲譽受損，重則可利用於竊取身份憑證，或是發動詐騙、釣魚等攻擊。

資料庫注入攻擊（SQL Injection）

在資料庫存取字串中，注入特殊變造語法，改變命令邏輯，從而擷取任意資料，甚至執行系統指令或讀寫檔案。

權限跨越

未適當檢查登入權限，導致使用者間可查詢或修改彼此資訊，或甚至跨越至高階主管或管理者權限。

IR
件數

【中華資安國際】紅隊演練及滲透測試常見漏洞及攻擊手法

Top 1 常見漏洞及攻擊手法 | MITRE ATT&CK

偵查階段

① 開發商曝漏系統源碼(Github、更新包)

初始接觸

② 外部OO系統存在高風險漏洞

繞過防禦

③ WAF、防毒軟體可繞過 (未安裝EDR/MDR)

取得帳密

④ HashDump系統登入密碼雜湊(可爆破明文)

內部探索

⑤ 利用Bloodhound 蒐集 AD網域資訊

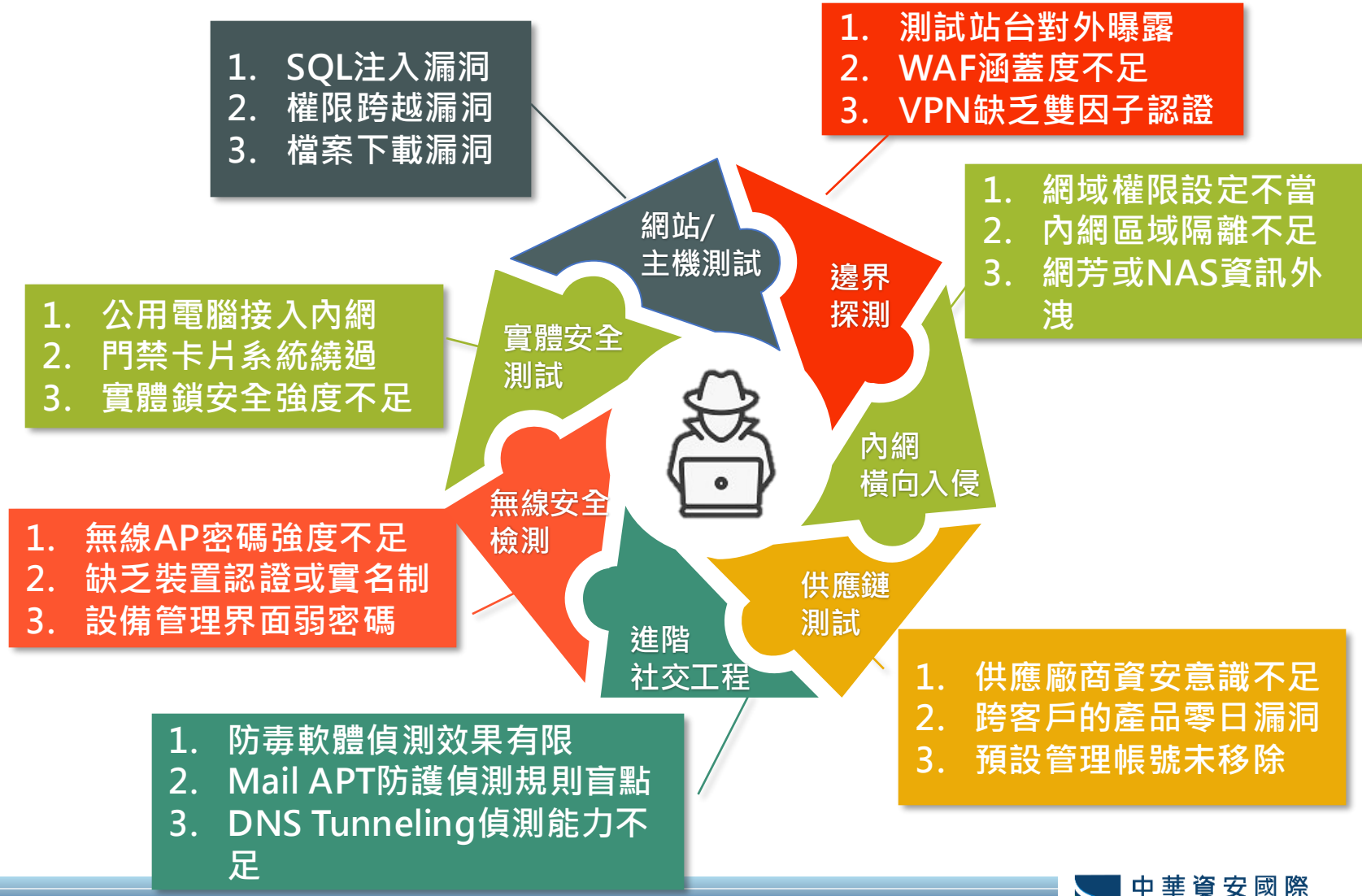
橫向移動

⑥ 濫用不當設定之網域帳密修改DC屬性，提權成為AD網域管理者(RBCD攻擊)

連線中繼站

⑦ 透過 DNS 協定連線中繼站

Top 3 各類別發現風險事項



中華資安國際
CHT Security

04 AI 世代的資安威脅應對策略

優化網路安全強韌性，重塑資安防禦模式，推動業務導向新策略

AI/Edge devices 興新威脅與對策

即時有效威脅暴露管理

持續威脅暴露管理
(Continuous Threat Exposure Management)

✓ 建立VANS/VMS/xASM

緊急應變計畫作為核心要素

第三方網路安全風險管理
(Third-Party Cybersecurity Risk Management)

✓ IR PLAYBOOK

導入ZTA 零信任架構

擴展身份存取管理（IAM）的網路安全價值
(Extending IAM’s Cybersecurity Value)

✓ MFA/FIDO ZTNA、CypherCom

關注雲端供應鏈安全

雲端安全態勢管理
（Cloud Security Posture Management）

✓ 雲端資安健診/Cloud SOC

資安監控應變平台融合 - SOC+MDR+SOAR

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

資安監控應變平台融合，提供資安洞察與協作應變

資安平台融合
Cybersecurity Platform Consolidation / Operating

自主研發SRM資安風險管理平台融合各監控應變系統，統整掌握企業風險與資安洞察

資安戰情牆

威脅情資中心

IoC

資安事件處理

CTI

CTI

SRM 資安風險管理平台

預警情資 | 資安洞察/戰情牆 | 事件通報管理 | 情資交換 | SOAR

Event

IT/OT SOC + MDR 監控應變服務　多維度關聯分析

AI/ML
情資回溯

elastic

SIEM即時
關聯分析

MDR
技術諮詢
深層分析

XDR
檢傷分類
客製回應

Log

Log

日誌收集器

雲端平台、網路閘道、管理系統、端點主機

雲 XDR/SaaS/...

閘 FW/NDR/Proxy

管 PAM/IDS/...

端 EPP/EDR/...

CROWDSTRIKE

次世代防毒引擎

遠端隔離與調查

主動威脅獵捕

CTI

Playbook

阻擋可疑IP/
阻擋惡意情資

隔離受駭
端點

刪除
惡意程式

SRM為中華資安所開發之資安風險管理平台

資安眼HorusEyes - 資安曝險評級服務

持續威脅暴露管理
Continuous Threat Exposure Management

利用AI技術對企業網站與網路資產進行曝險分析評分，並提供專家報告與修補建議

AI數位邊界探索

- 只需提供Domain/IP，**自動挖掘網路數位資產**
- **AI 自動找尋與企業相關的資產，範圍更大、正確性更高**

非侵入式持續曝險評估

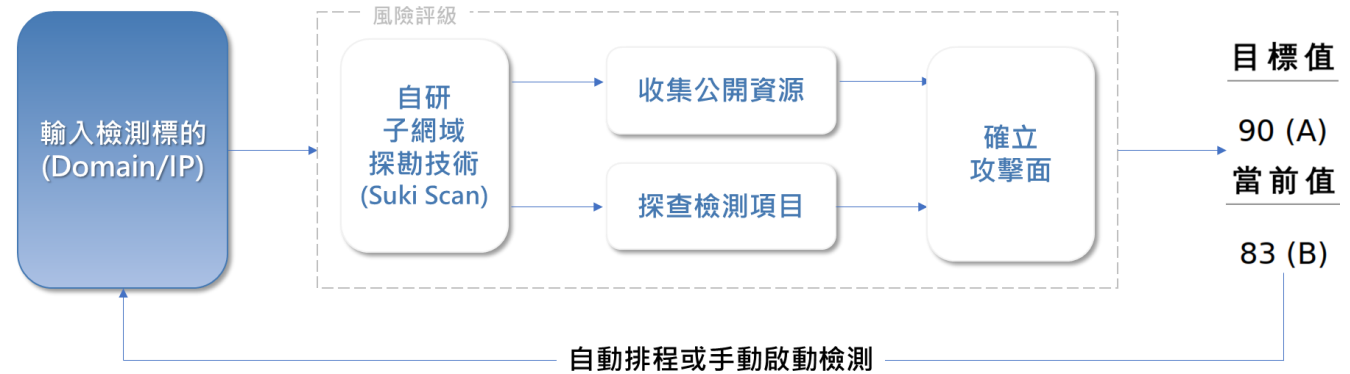
- 評估數據由公開資產信譽和非入侵式的偵測方法

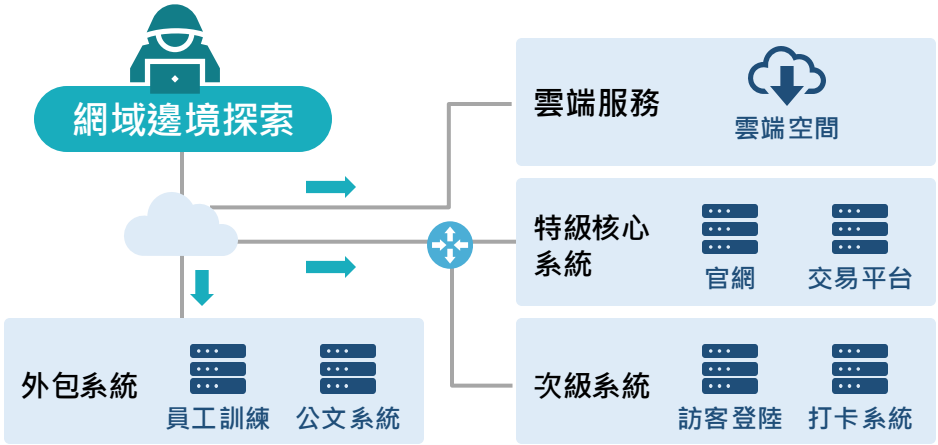
資料外洩、被社交工程評估

- 提供評估是否有相關外洩資料或可能被社交工程可能風險的評估

AI曝險報告、AI線上專家

- **針對曝險弱點找到最即時風險和修復建議**
- 以自然語言回覆弱點修補建議





資安事件應變處理能力建立 – IR Playbook

基於企業現有IR制度架構，參考NIST SP800-61r2 定義的事件回應生命週期，準備、偵測和分析、遏制、根除和復原與事件後活動，客製化符合領域需求之IR Playbook及執行IR應變演練

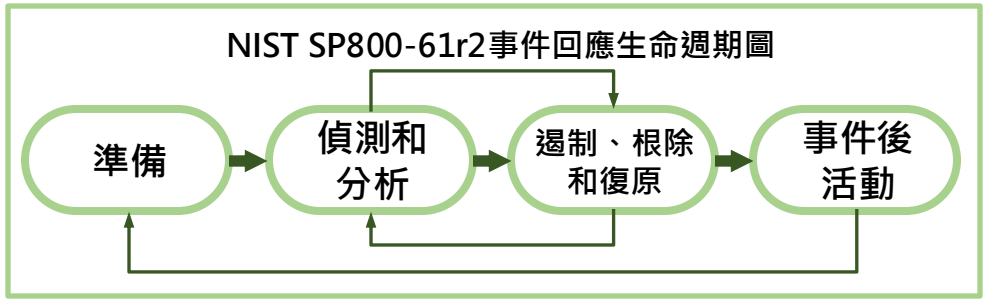
優化制度

現行IR制度

差異化分析報告

差異分析

NIST SP800-61r2標準



客製化

團隊服務實績橫跨金融業與製造業

優化既有IR程序

演練情境與腳本

IR PLAYBOOK

資安事件應變演練計畫書

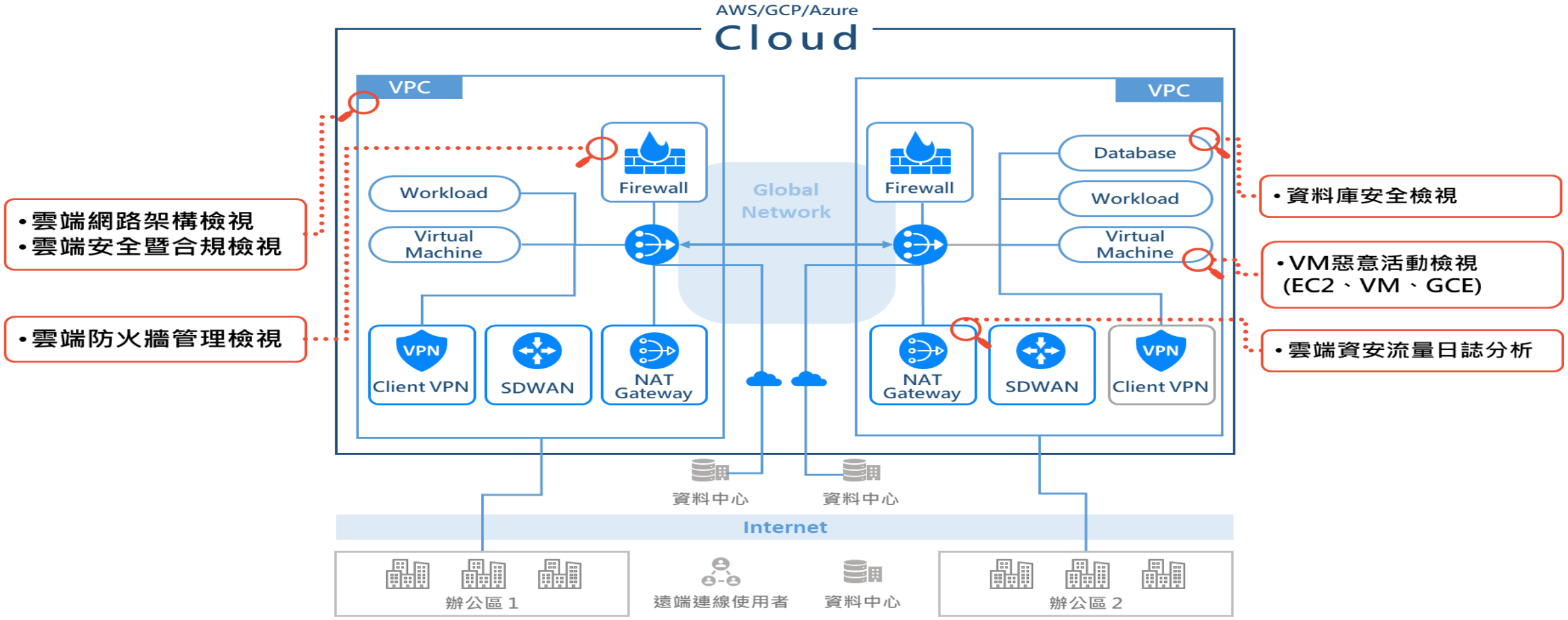
資安事件應變演練執行方式

桌上推演

使用模擬環境攻防

雲端資安健診

支援三大公雲(AWS、Azure、GCP)與三大公雲之雲地混合環境，協助企業檢視其雲端環境的安全性和合規性



CypherCom 端對端加密通訊系統

透過高強度**硬體式端對端加密通訊機制**，確保通訊內容不被監聽、竊聽，機敏資訊不外洩

端對端硬體加密

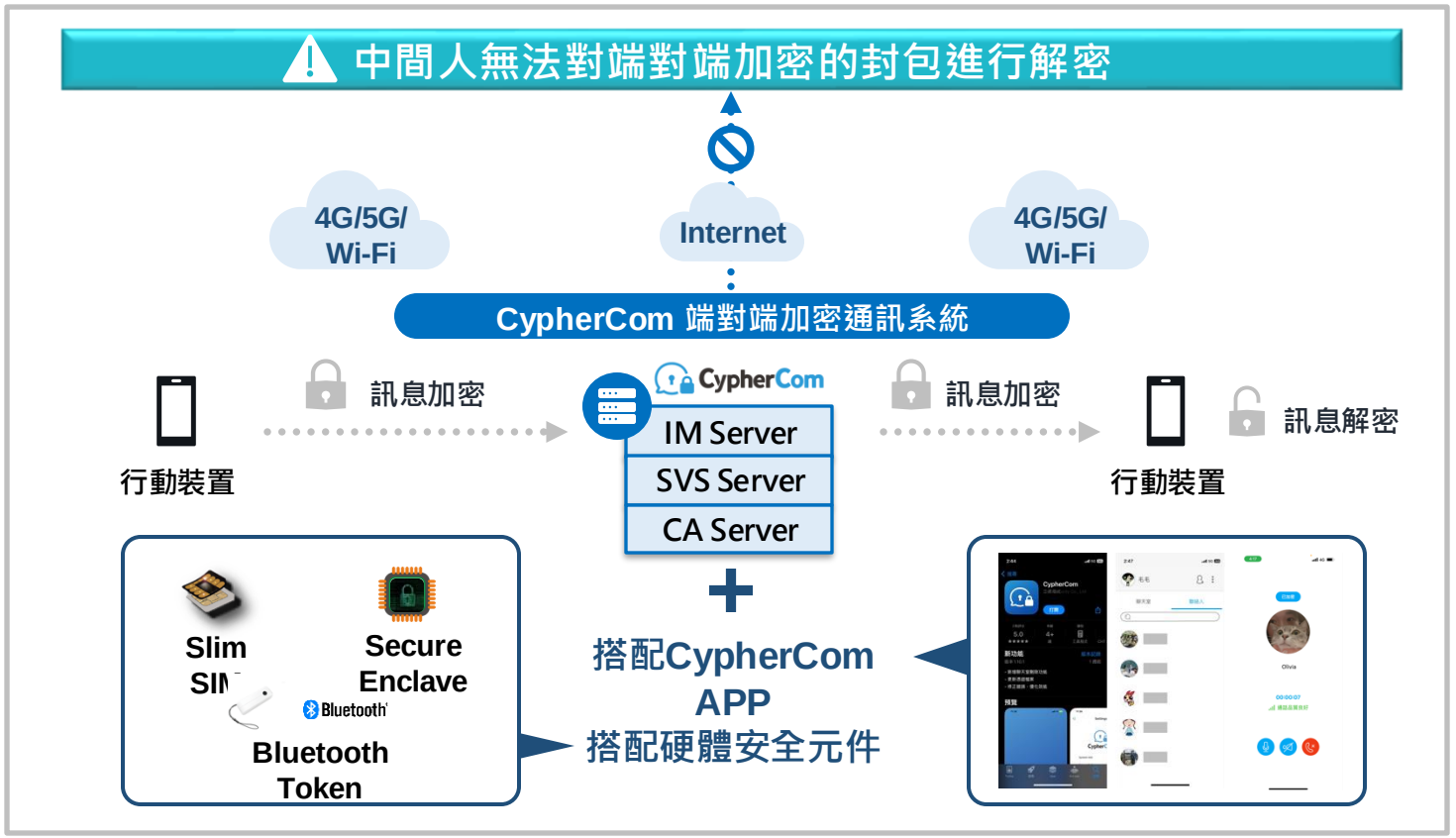
- 硬體安全晶片通過**FIPS 140-2 Level 3 密碼模組**安全驗證
- 多種加密技術，如：雙棘輪演算法、非對稱式金鑰交換、對稱式加密等
- **E2EE加密**，整合語音VoIP、視訊通話、即時通訊IM，確保內容不被竊聽

自主管理通訊系統

- 支援Android與iOS平台
- 支援On Premise建置，自管金鑰生命週期

通訊安全韌性

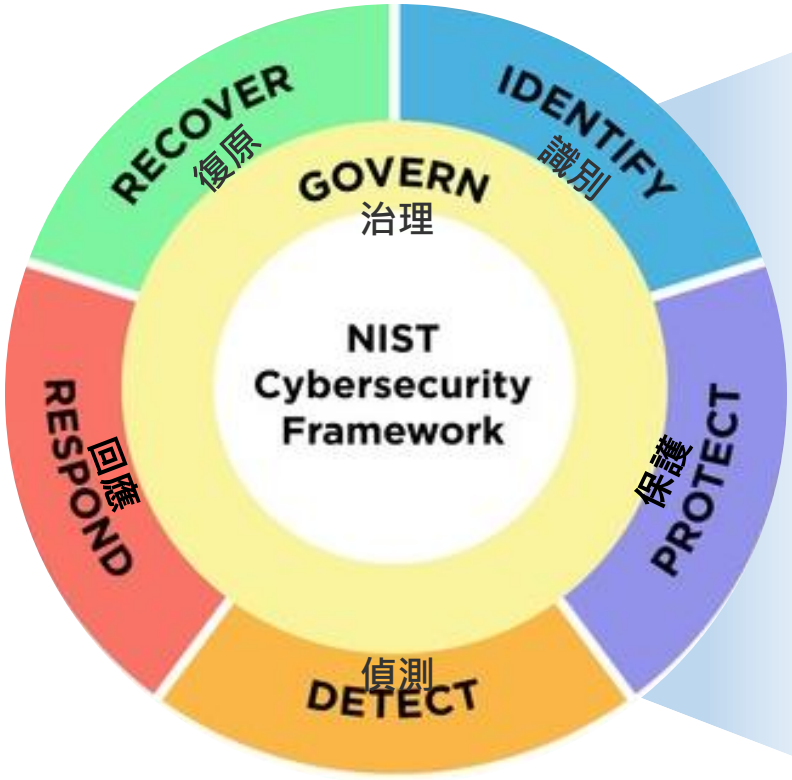
- 可用3G/4G/5G 或 Wi-Fi連線
- **支援低頻寬衛星網路**



CHT Security can help you

協助組織建立及實施 NIST CSF 2.0框架

提供符合美國NIST網路安全框架2.0的事前檢測、事中監控應變、事後鑑識復原，以及資安治理的一站式資安服務，協助政府及企業強化資安韌性



事前

- 資安健診
- OT資安健診
- 雲端資安健診服務
- 原始碼檢測
- 弱點掃描
- 滲透測試
- 紅隊演練
- APP檢測服務
- IoT 檢測服務
- 社交工程演練
- 資安曝險評級服務
- BAS藍隊演練服務
- 電腦系統資訊安全評估
- IR Playbook 演練

事中

- 資通安全威脅偵測管理(SOC)服務
- MDR威脅偵測應變服務
- 網頁存活與異動監測服務
- 惡意程式快篩服務
- 資安自動化應變(SOAR)
- 資安情資分享與自動聯防

事後

- 資安事件緊急應變服務
- 數位鑑識服務
- 災後復原/強化重建
- 資料備份與系統備援
- 業務持續計畫（BCP）


中華資安國際
CHT Security
中華電信 Chunghwa Telecom 關係企業
謝謝您 敬請指教!
一站式滿足企業資安需求
www.chtsecurity.com
02-2343-1628 SERVICE@CHTSECURITY.COM