

# 消失的界線：工業控制系統與企業網路的資安威脅與應對策略

中華資安國際股份有限公司

劉叡 經理

2024.05.16

# 一、關於中華資安國際

# 中華資安國際公司現況簡介

成立時間 106年12月 | 實收資本額3.28億元，中華電信持股77% | 員工 305人▲



中華電信集團的資  
安專業子公司



具備國家級資安專  
案建置能力與實績



服務超過200間以  
上企業和政府機關



提供事前檢測、事中監控應變、事後事件調查的資安服務

## ✓ 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

## ✓ 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

## ✓ 資安顧問

ISMS/PIMS制度導入輔導、資訊安全評估、PKI建置規劃

## ✓ 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(VMS)、資安資訊分享與分析系統(ISAC)、先進資安威脅防禦系統(SecuTex NP / SecuTex ED)

## ✓ 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

## ✓ 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

# 專業能力連續多年榮獲國內、外獎項肯定



獲獎紀錄



國際認證

ISO 27001 資訊安全管理驗證、ISO 27701 隱私資訊管理系統驗證  
ISO 20000 資訊技術服務管理驗證、ISO 17025 數位鑑識暨資安檢測中心驗證

2023

- 2023 HITCON Cyber Range 第一名
- Frost & Sullivan 2023 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

- 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) 獎」

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

2019

- 行政院資安服務廠商評鑑五項資安服務全數「A級」
- 工研院民生公共物聯網漏洞挖掘邀請賽：第三名
- TWCSA紅色警戒72小時(Red Alert 72)：亞軍

全國唯一連續四年資安服務評鑑「全項A級」廠商！

111 年共契資安服務廠商評鑑結果 資料來源：國家資通安全研究院

序號	得標廠商	SOC 服務	資安健診	弱點檢測	滲透測試	社交工程演練
1	三甲科技		B 級	A 級	A 級	
2	中芯數據		B 級	B 級	B 級	
3	中華資安	A 級	A 級	A 級	A 級	A 級
4	白帽犀牛		B 級	B 級	B 級	
5	光盾資訊		B 級	B 級	B 級	B 級
6	昕恩科技		B 級	B 級	B 級	B 級
7	馬拉數位	D 級				



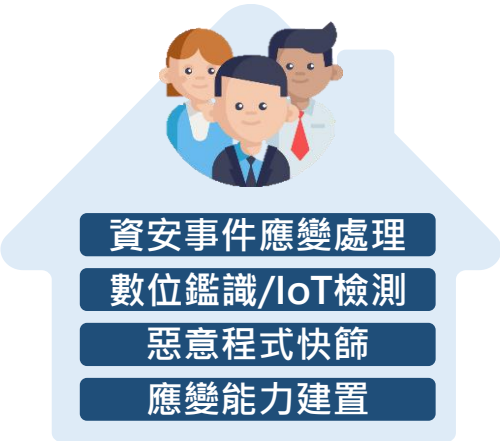
已累積取得97個以上CVE漏洞

問題產品	分類	CVE編號	風險等級
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
		CVE-2023-28704	8.8 HIGH
滲透工具	工具	CVE-2023-34758	8.1 HIGH
線上展示系統	網站	CVE-2023-37152	9.8 CRITICAL

# 數位鑑識暨資安檢測實驗室

► 2020/12/14 取得ISO17025認證，為TAF認可實驗室

- ISO/IEC 17025
- TAF
- 為全世界實驗室專家共同制定之國際標準，讓實驗室達到標準的通用性，並依循進行管理實驗室
  - 財團法人全國認證基金會，建立國內符合性評鑑機構之品質與技術能力之評鑑標準



► ISO17025認證

► 數位鑑識暨資安檢測中心

認證編號	機構名稱	實驗室名稱	實驗室地址	聯絡人姓名	聯絡人電話	認證狀態
3776	中華資安國際股份有限公司	數位鑑識暨資安檢測中心	台北市中正區杭州南路1段26號8樓	胡維軒	02-2343-1628 #8031	認可

檢視認可項目(View scope of accreditation)

認可項目 Scope of accreditation

基本資料

機構名稱：中華資安國際股份有限公司

機構地址：台北市中正區杭州南路1段26號8樓

實驗室名稱：數位鑑識暨資安檢測中心

實驗室地址：台北市中正區杭州南路1段26號8樓

認證編號：3776

認證依據：ISO/IEC 17025:2017

初次認證日期：2020/12/14

認證有效期間：2023/12/14 ~ 2026/12/14

認證範圍：實驗室測試

特定服務計畫：智慧連網服務系統資安

IEC62443 CBTL 認可  
檢測實驗室

TUVNORD

CERTIFICATE OF RECOGNITION

CHT Security Co., Ltd.  
Digital Forensics and Cyber Security Testing Center  
8F., No. 26, Sec. 1, Hangzhou S. Rd., Zhongzheng Dist., Taipei 10092, Taiwan (R.O.C.)

has been recognized to carry out the testing and/or activities under supervision of TÜV NORD. It has successfully demonstrated the capability within the applied scopes of

Cybersecurity Standards  
IEC 62443 series  
IoT-2001-1, IoT-2001-2

An assessment of the facility was conducted by TÜV NORD assessors according to the TÜV NORD requirements for "Test Facility Recognition Criteria" with reference to

ISO/IEC 17025

Certificate No.: TWTW2201R-01 Valid until: 2024-12-13

TÜV NORD  
Taiwan, 2023-12-14

20 21 資訊與通訊

網路攝影機

E 013 1級  
2級  
3級

1.IoT-2001-1  
i 通訊安全 除外  
2.IoT-2001-2  
i 通訊安全 除外  
報告簽署人：林峰

27 10 鑑識科學試驗

儲存媒體(硬碟、隨身碟、記憶卡)  
Z 078 資訊重現：刪除檔案還原、關鍵字搜尋  
TACL-305案件分析標準作業流程  
硬碟、隨身碟、記憶卡  
報告簽署人：馬洪雲、劉耕瑾、劉劍

特定服務計畫：智慧連網服務系統資安檢測實驗室認證服務計畫

20 21 資訊與通訊

網路攝影機

E 013 1級  
2級  
3級

1.IoT-2001-1影像監控系統資安測試規範：第一部\_一般要求 (「5.3.3 Wi-Fi 通訊安全」除外)  
2.IoT-2001-2影像監控系統資安測試規範：第二部\_網路攝影機 (「5.3.3 Wi-Fi 通訊安全」除外)  
影像監控系統-網路攝影機  
報告簽署人：林峰正

已認證項目

1. 20 21 資訊與通訊，網路攝影機

2. 27 10 鑑識科學試驗，刪除檔案還原、關鍵字搜尋

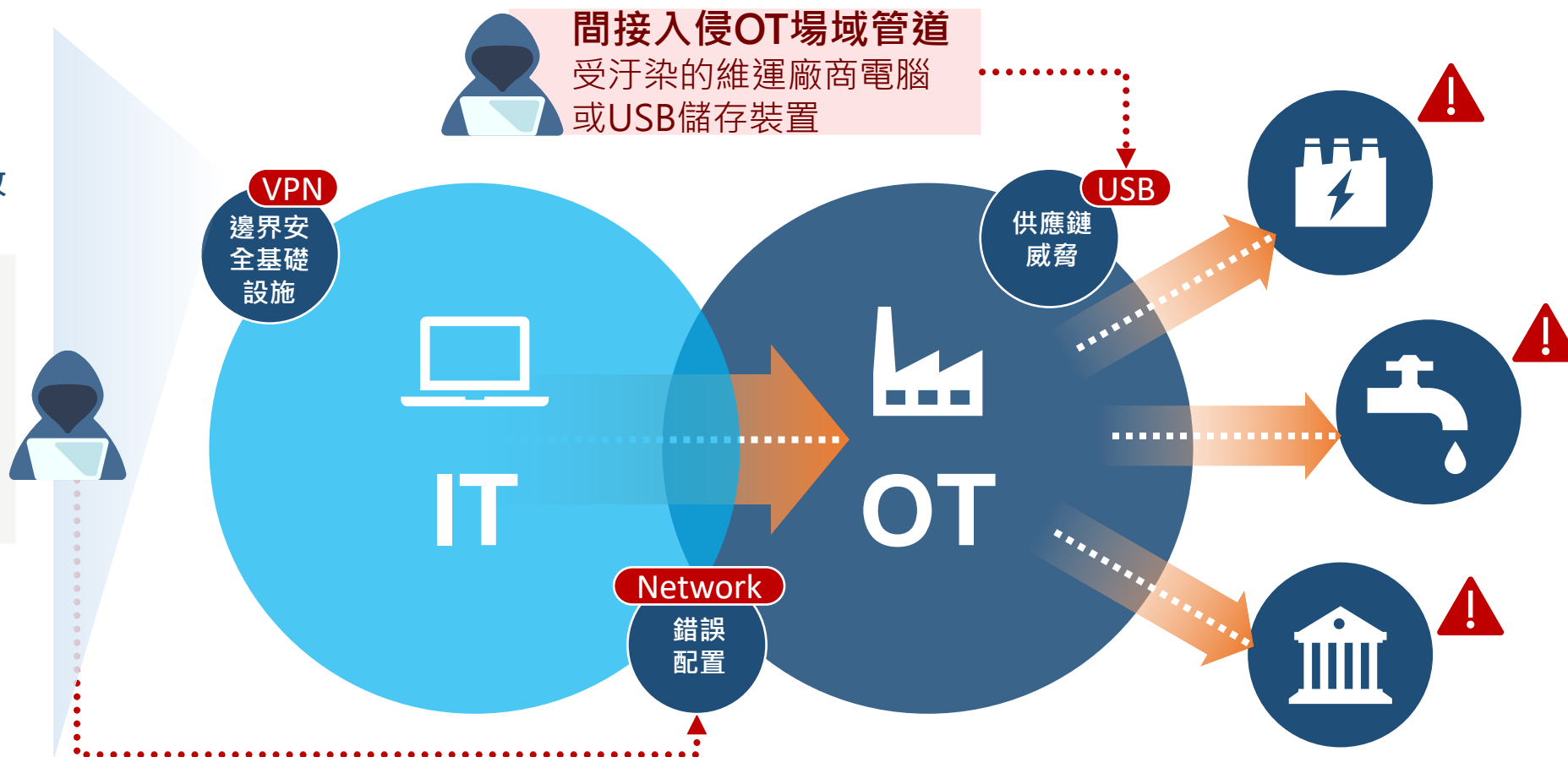
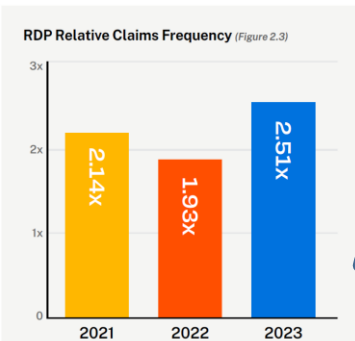


## 二、前言

# 消失的界線：工業控制系統與企業網路的資安威脅

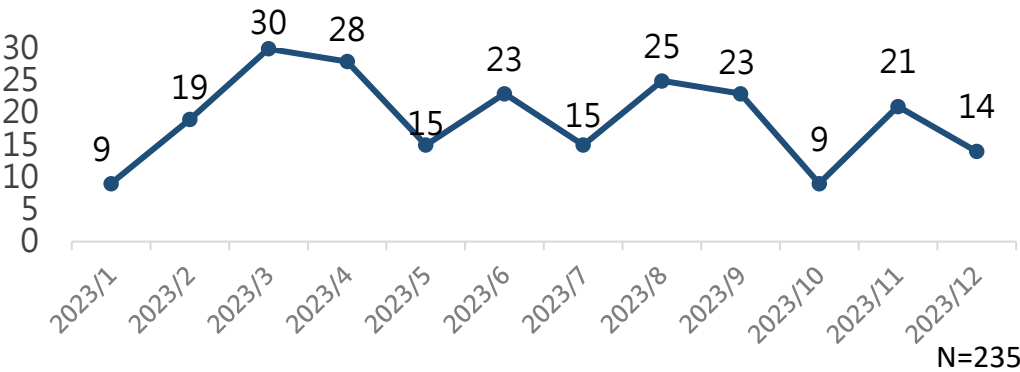
國際資安報告顯示，隨著IT與OT加速整合，網路安全邊界日益模糊，**同時影響IT與OT之勒索軟體攻擊從2021年的27%躍升至2023年的37%**。使用**特定邊界安全設備**的企業，遭遇資安事件的風險更是高達其他企業的**2-5倍**。企業亟需增強邊界防護韌性，全面提升威脅偵測和回應能力。

邊界設備成為駭客攻擊目標

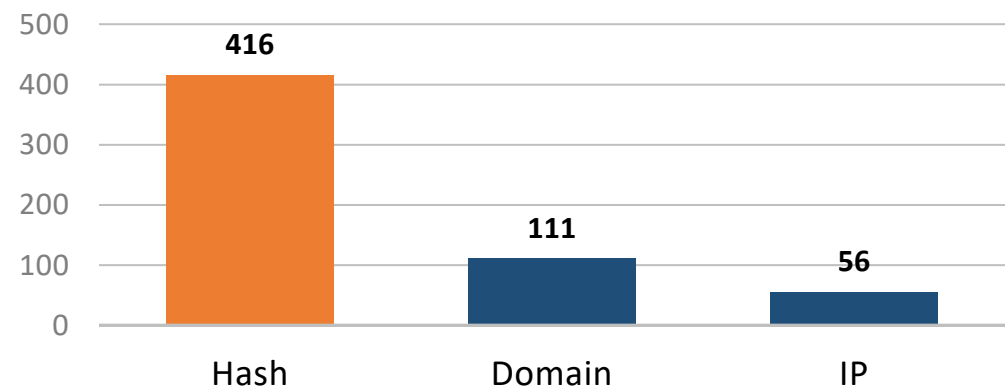


# 從2023年資安事件處理統計結果看問題(1/2)

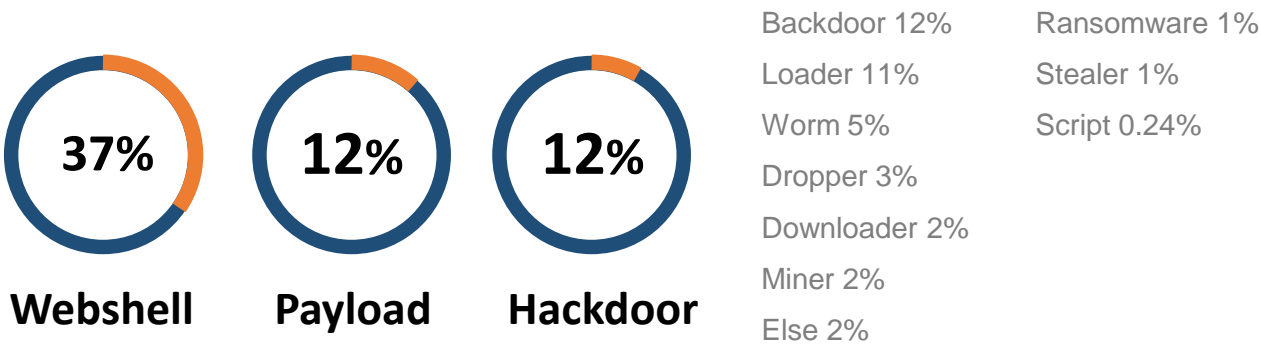
資安事件調查數量



新發現威脅情資



惡意程式類型



駭客入侵手法(Initial Access)

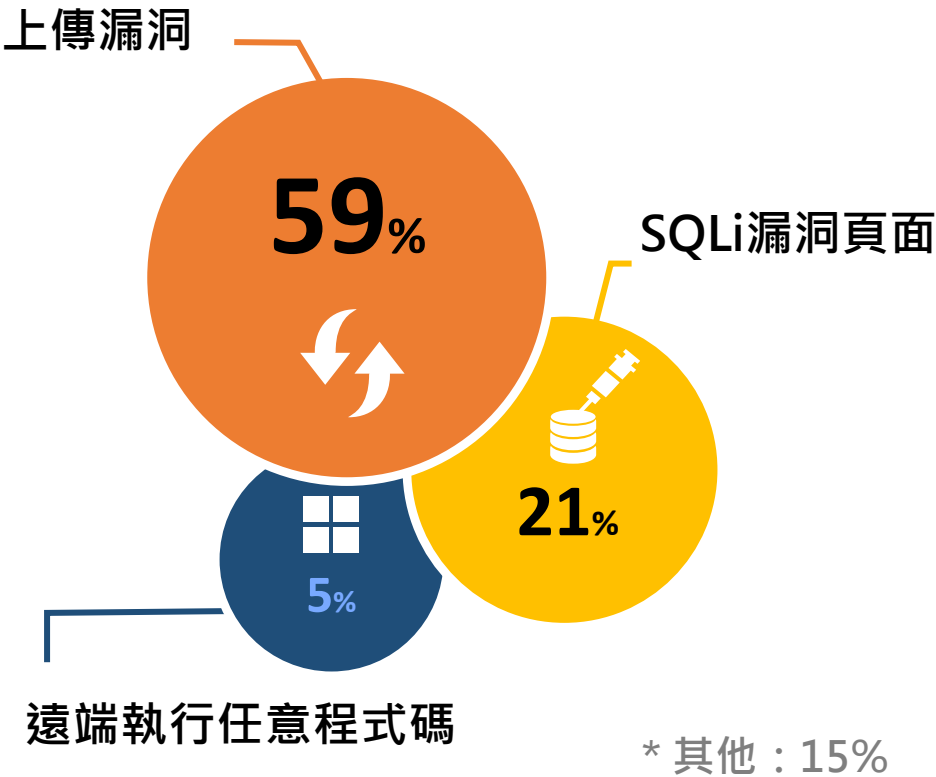




# 從2023年資安事件處理統計結果看問題(2/2)

## 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
<ul style="list-style-type: none"><li>• Continuous Threat Exposure Management</li><li>• Extending IAM's Cybersecurity Value</li><li>• Third-Party Cybersecurity Risk Management</li><li>• Privacy-Driven Application and Data Decoupling</li></ul>	<ul style="list-style-type: none"><li>• Generative AI</li><li>• Security Behavior and Culture Programs</li><li>• Cybersecurity Outcome-Driven Model's</li><li>• Cybersecurity Reskilling</li></ul>

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)

## 三、工業控制系統面臨的資安威脅

# Volt Typhoon 的攻擊手法

駭客組織 Volt Typhoon 對美國關鍵基礎設施發動了一系列攻擊

Volt Typhoon 利用多種手段入侵關鍵基礎設施網路



! 漏洞利用  
! 橫向移動  
! 竊取憑證

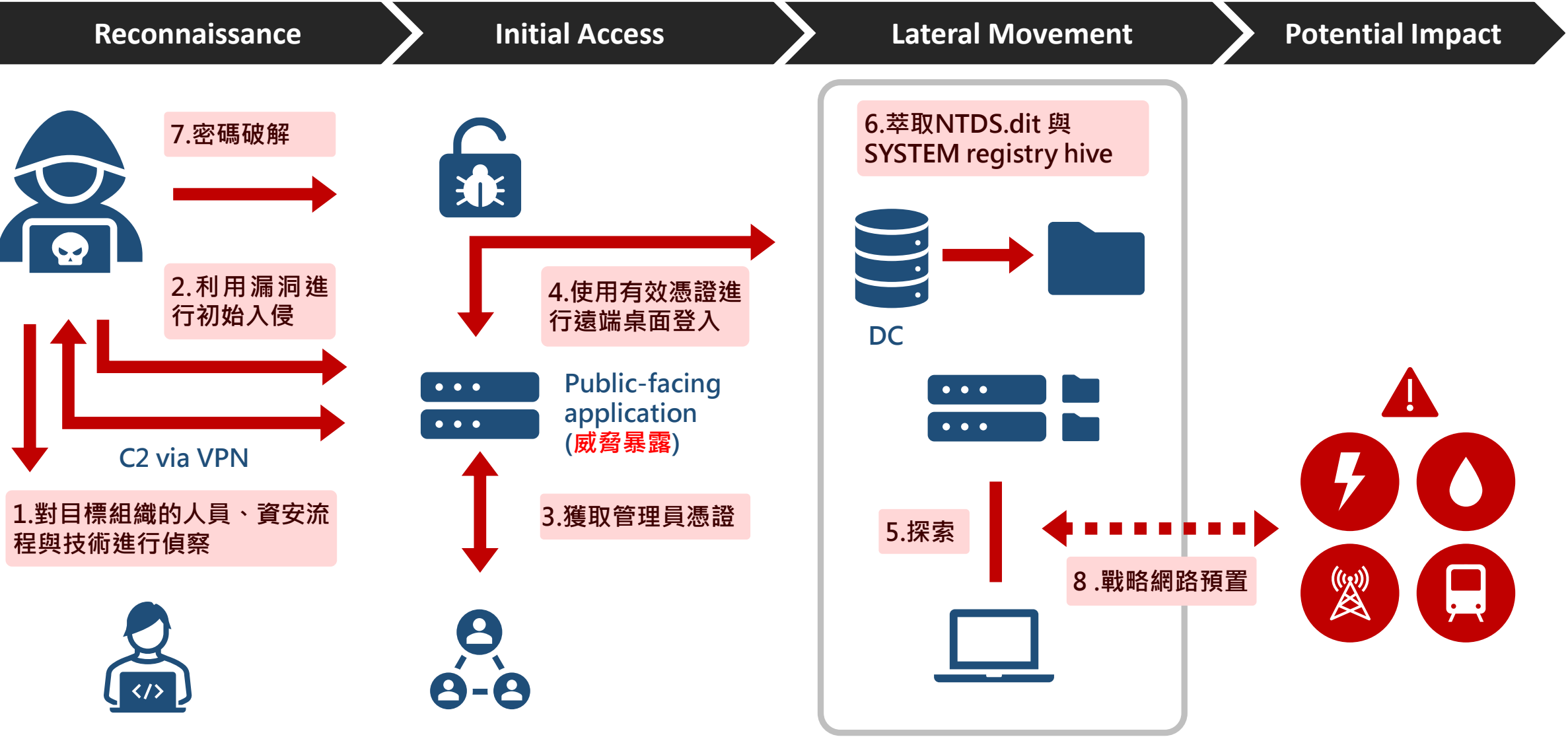


在關鍵基礎設施網路中建立長期持續性的存取，以便在發生衝突時實施破壞性攻擊



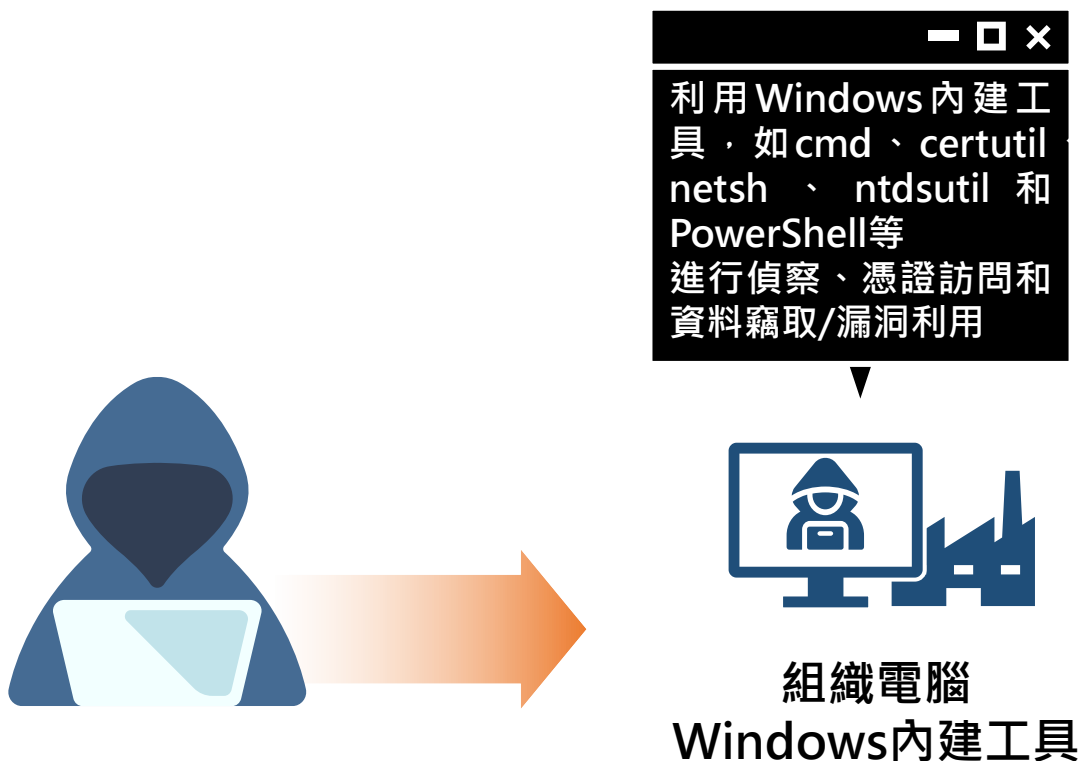
攻擊模式：  
廣泛的偵察、初始存取、權限提升、橫向移動到網域控制器 (DC) 竊取憑證、對操作技術 (OT) 系統的偵察與資料收集。

# Volt Typhoon 關鍵基礎設施攻擊案例分享



# 利用LoTL技術逃避偵測

Volt Typhoon廣泛使用“生活於土地之上”(LoTL)技術來迴避偵測和維持持久性存取



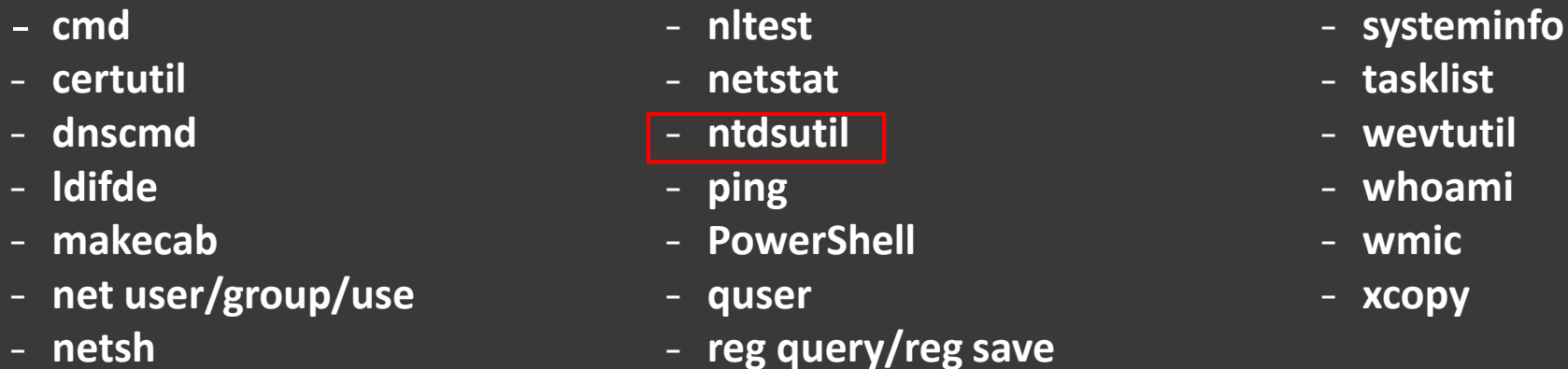
## LoTL(Living Off-the-Land)

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

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



## 企業防護措施

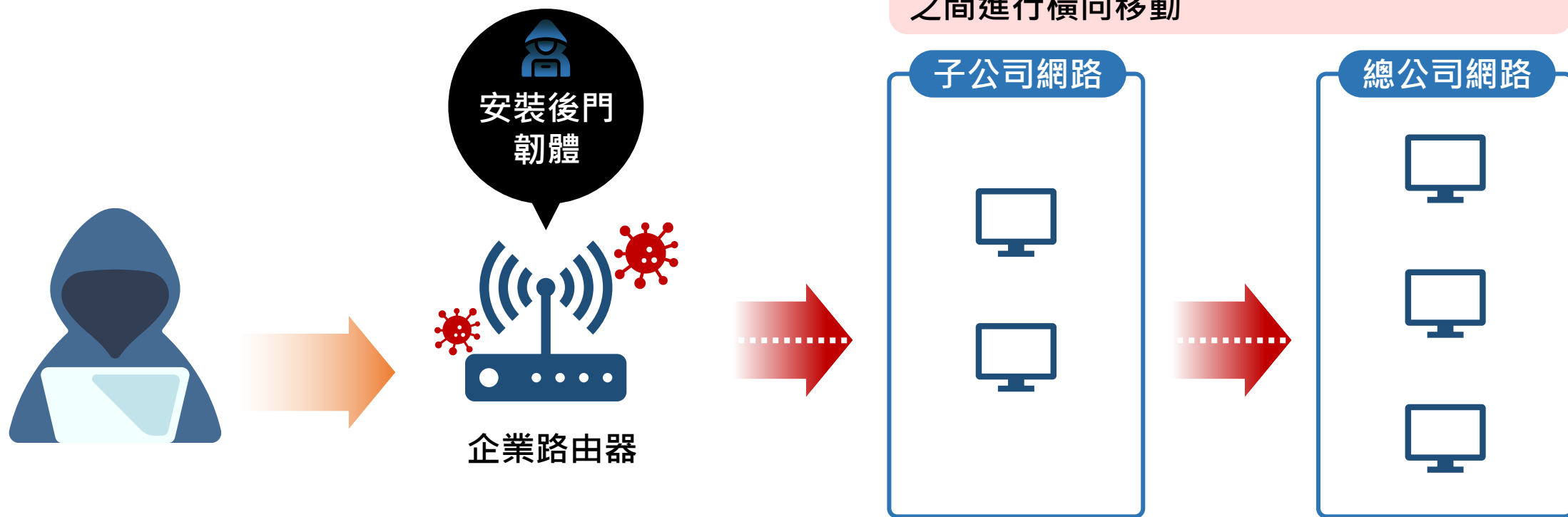
1. 啟用PowerShell/WMI活動記錄
2. 監控LoTL命令模式
3. 尋找異常用戶行為
4. 集中存儲日誌
5. 採取緩解措施



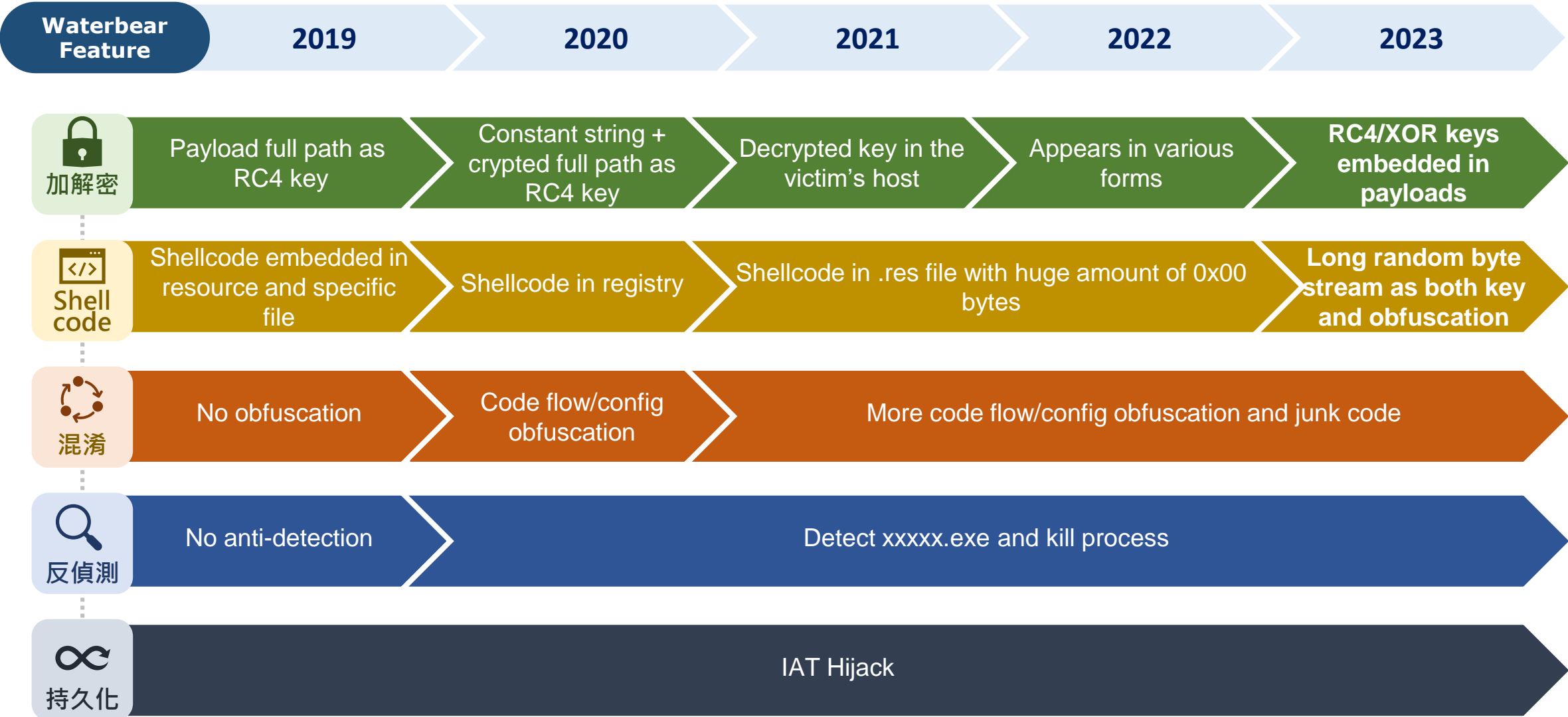
## 四、企業網路面臨的資安威脅

# BlackTech 隱藏在路由器韌體中

駭客組織 BlackTech 能夠修改路由器韌體，受害者環境中部署惡意控制網路，並利用受感染路由器之間的信任關係在網路之間進行橫向移動



# Waterbear 特徵技術分析



## 五、應對策略

# 2024年資安強化作為

優化企業網路安全強韌性，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/EASM

### 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

⚠ 新興技術發展使攻擊者更膽大妄為

⚠ 雲服務使用率提升

⚠ 身份識別架構失效

⚠ 網通設備資安威脅

⚠ 暴險介面持續增加

### 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

### 將顛覆轉化為資安機會

生成式人工智慧  
(Generative AI)

✓ AI TRiSM

# 建立持續性的資安防護與評估機制

事前：

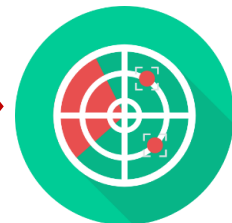
制度、防護、檢測評估



- 資安管理制度
- 資產盤點與風險識別
- 資安防護與存取管控
- 資安健診與檢測演練
- 資安教育訓練
- 安全開發流程

事中：

偵測、監控、事件應變



- SOC/MDR/XDR
- 日誌(Log)保留與監控
- 網路流量異常分析
- 主機異常行為分析
- 情資獵捕
- 偵測與回應

事後：

鑑識、復原、強化



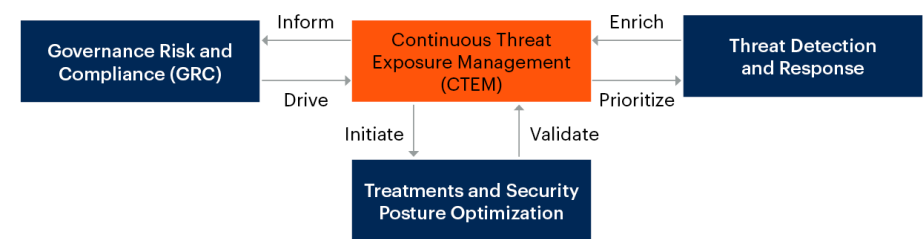
- IR Policy/Playbook
- 損害控制/影響評估
- 鑑識調查/入侵管道
- 災後復原/強化重建

1. 管理制度：關鍵資產盤點、組織人員+流程+工具 (ISO 27001 管理制度、NIST IPDRR資安框架)
2. 資安技術：防護架構、偵測監控、緊急應變的技術框架及基準線
3. 人員訓練：資安認知+資安技能

企業可採用 EASM/BAS 資安評級服務，或是選擇 Red Teaming 檢視防護的有效性

可以參考Gartner CARTA 持續性的適應風險和信任評估 ( Continuous Adaptive Risk and Trust Assessment )，提高資安防護適應能力

## Continuous Threat Exposure Management



2024年Gartner十大科技戰略趨勢



# 導入VMS，即時監控與持續監管曝險漏洞

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

Zero-Day防不勝防，影響範圍持續擴大

挑戰

因應

弱點即時掃描與通報，並將修補作業程序納入監管



## ■ 事件追蹤管理系統效益

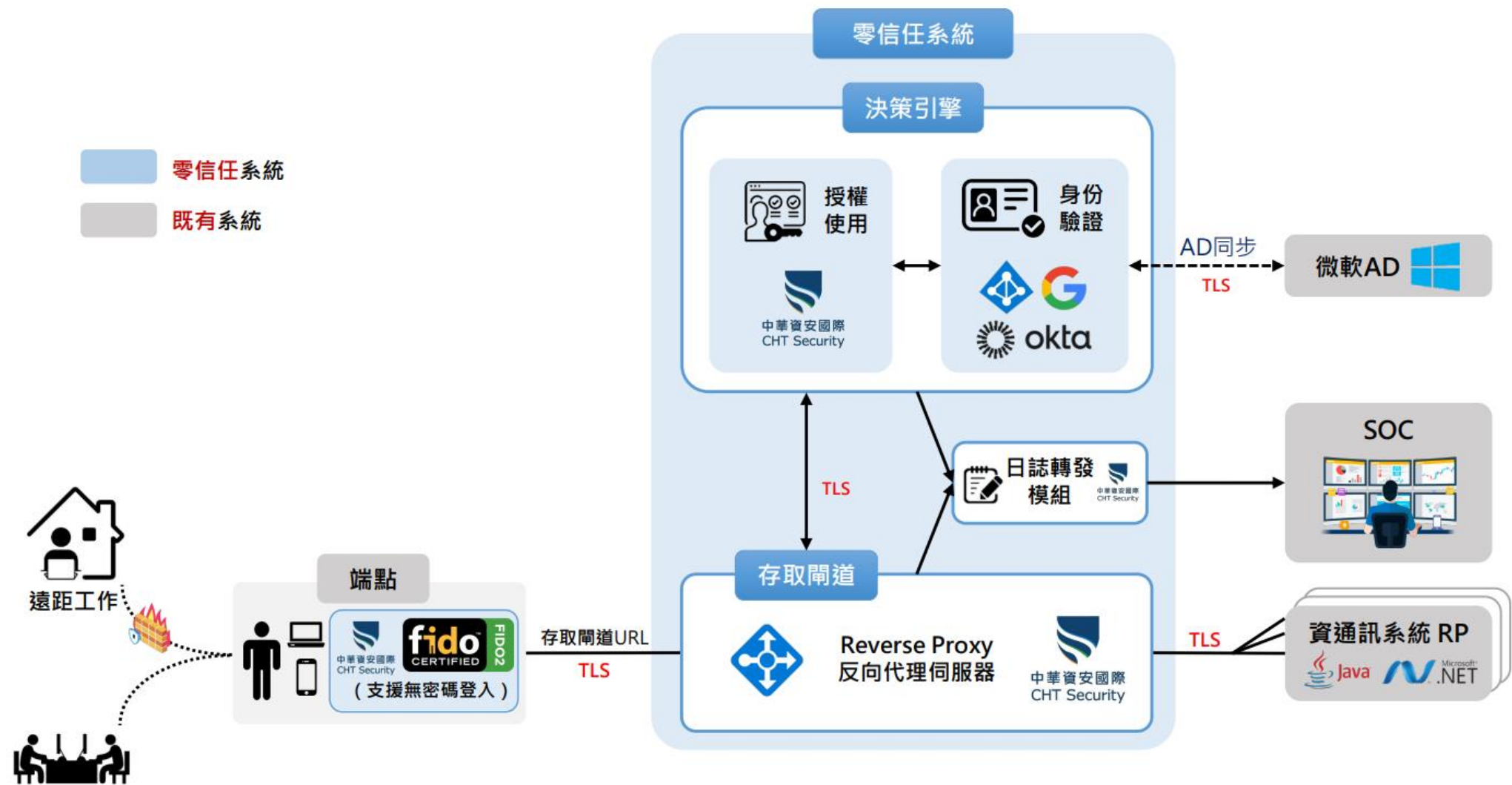
- 客製化符合企業事件通報組織及處理機制
- 完整紀錄事件處理內容及各類型報表，大幅降低日後稽核時間
- 管理人員可透過圖形化介面即時掌控事件處理狀態
- 帳號可與企業LDAP整合，提高安全性與方便性

提升整體通報效率高達5倍以上

縮短事件及弱點追蹤時間50%以上

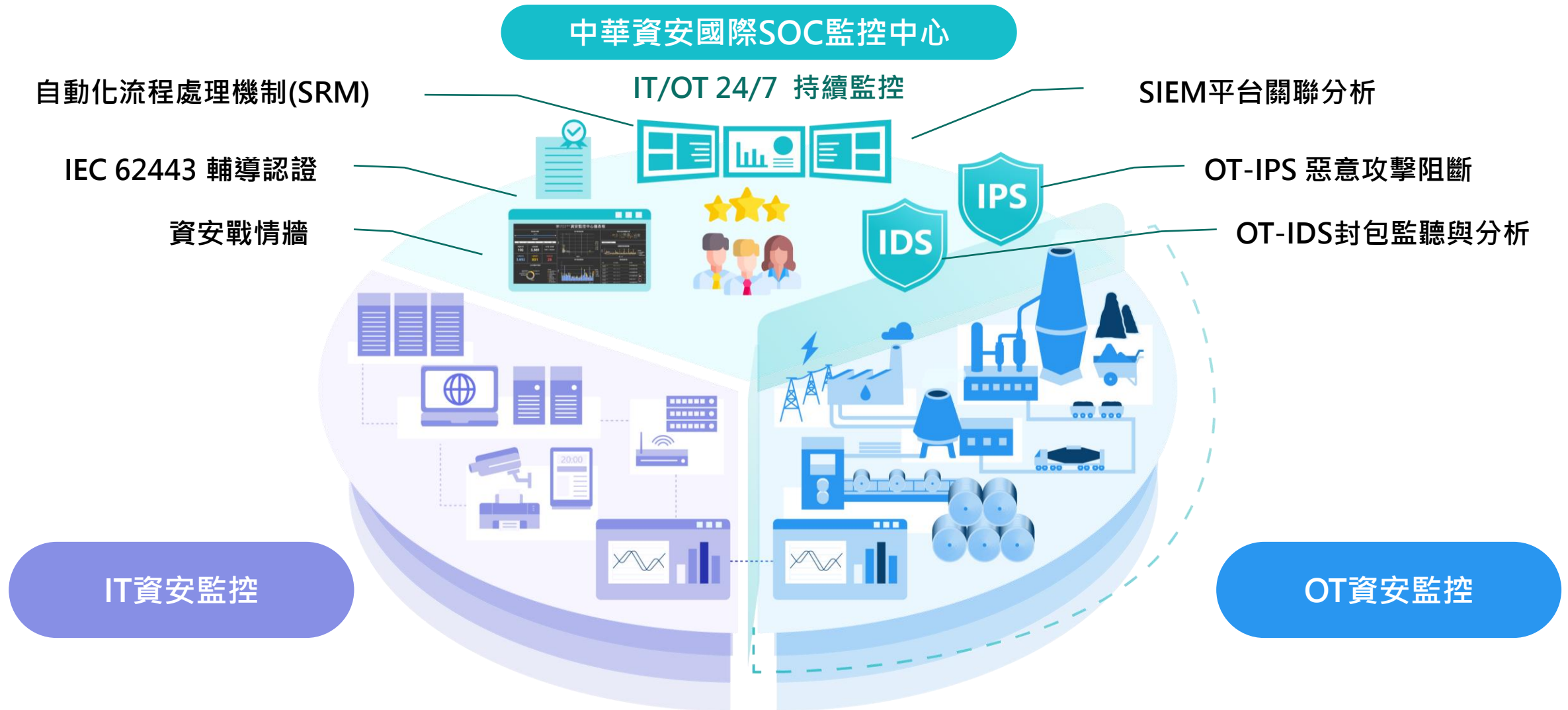
# 導入零信任架構解決方案

擴展IAM的網路安全價值  
( Extending IAM's Cybersecurity Value )



# 24\*7 IT x OT SOC監控應變服務

偵測和強化最佳實踐  
(Detection Best Practices)



關鍵日誌軌跡未保留，無法還原  
事件現場，調查資安事件根因

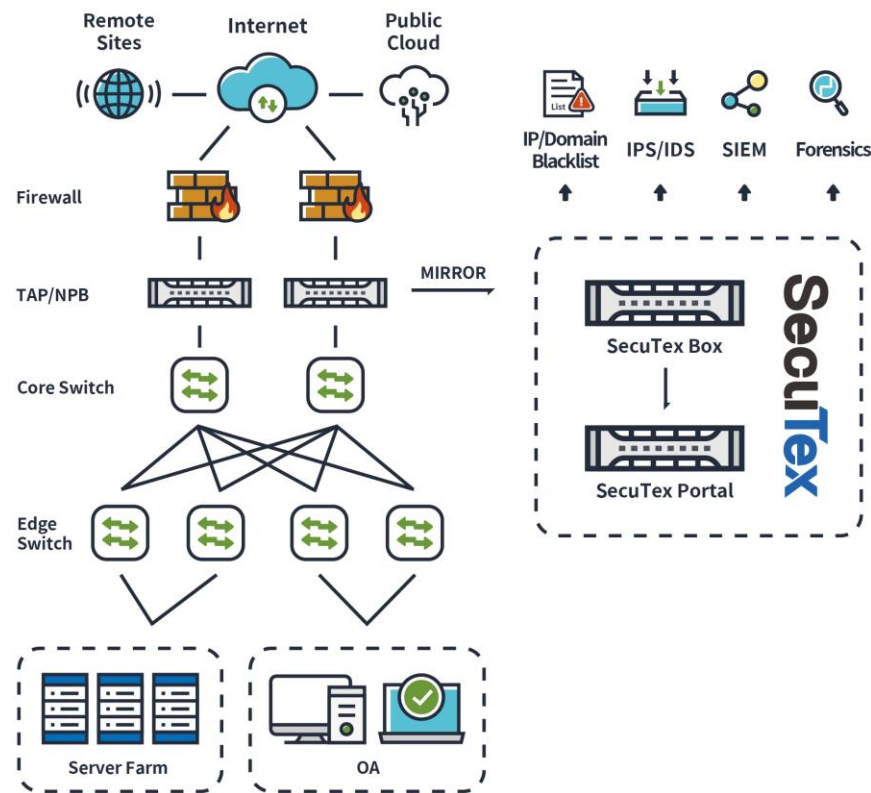
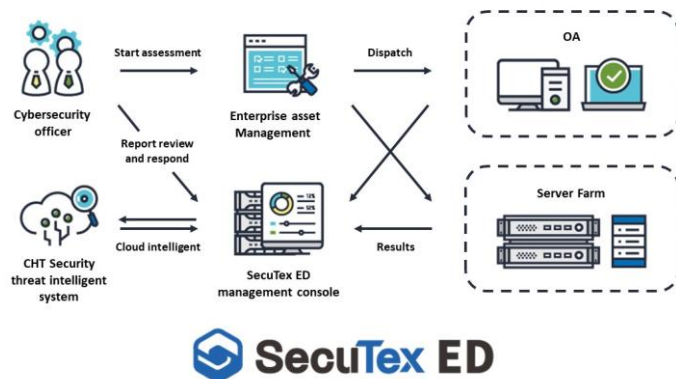
挑戰

因應

24/7全時側錄網路流量，需要時  
可快速回溯調查，分析入侵管道

## ■ 現有網路資安威脅防護設備的缺點：

- 只在偵測到危機時才開始保留證據
- 保留的證據不足，沒有Raw Data
- 不同系統的證據需要時間同步、彙整
- 端點跡證難以保留，甚至遭駭客刪除，缺少網路軌跡資料



為了有效應對LoTL技術和其他APT惡意網路活動，企業應實施全面的偵測和強化最佳實踐



通過將這些最佳實踐整合到其網路安全策略中，企業可以顯著提高檢測和緩解LoTL攻擊的能力



強化面

企業應採用資安防護強化指引、實施應用程式白清單、增強網路隔離與微分割，以及實施強認證控制



實施面

實施詳細的日誌記錄、建立正常行為基線、使用自動化來檢查日誌、減少誤告警，以及實體行為分析（UEBA）

# 第三方網路安全風險管理的重要性

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



## 第三方網路安全風險管理方法



有效的第三方網路風險管理可最大限度地降低因遭到入侵而造成的損害



在採購/供應商合同流程中整合安全設計原則，包括確保合規性和修補機制，同時指導軟體開發團隊在整個現有實踐中貫徹安全軟體開發框架（SSDF）



企業應識別並限制使用任何違反最小權限原則的產品



企業應識別未明確列舉所需訪問權限的產品



# 緊急應變計畫作為核心要素

- 基企業現有資安事件應變(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，**客製化符合場域需求之IR Playbook及執行IR應變演練**

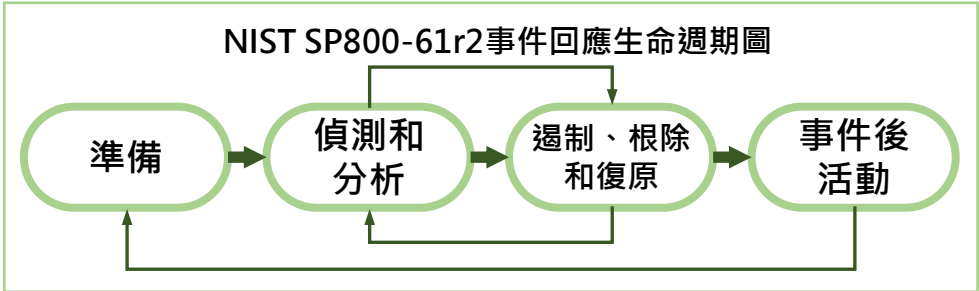
+ 優化制度

現行IR制度

差異化分析報告



NIST SP800-61r2標準



客製化



團隊服務實績橫跨金融業與製造業

1. 勒索加密事件	
事件描述	2023年10月10日，某金融機構客戶發生勒索加密事件，勒索軟體為「LockBit 3.0」，攻擊者透過釣魚郵件進入系統，加密了客戶的財務數據和客戶資料。
事件影響	客戶財務數據和客戶資料被加密，業務運作中斷，客戶面臨重大財務損失和信譽風險。
事件處理	1. 立即斷網，防止勒索軟體擴散。 2. 通知客戶，並啟動應急響應機制。 3. 聯繫專業安全團隊進行分析。 4. 嘗試解密數據，並恢復系統。 5. 加強客戶系統安全，防止再次發生。
事件總結	此次事件暴露出客戶系統存在安全漏洞，需要加強安全防護，並定期進行安全演練。

2. 勒索加密事件	
角色	描述
戰略室	進行演練成效評估
技術人員	提供資安事件調查技術協助
記錄人員	完整記錄演練過程中所發生的任何決策、執行及執行結果
溝通人員	說明演練情況，確保演練從演練目的進行
事件發現人員	1. 模擬中斷資安團隊緊急應變模式 2. 通報真實事件發生
事件通報窗口	接受事件發現人員通報
第一線處理人員	通報緊急處理組
緊急處理組	1. 召喚指揮緊急處理組作業 2. 要求外部單位(如:IDS廠商)協助



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

## 六、結語

# 資訊安全風險 – 彼の威脅、己的漏洞

## 威脅說明(Threat)

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

## 漏洞說明(Vulnerability)

雲端服務、SaaS 應用和第三方供應鏈的興起，企業網路環境變得空前複雜。這就好比一座古老的城池，城牆上的缺口和薄弱點也越來越多，守衛們疲於奔命，總有漏網之魚的風險

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

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，企業焦點應放在涵蓋面更廣的「持續威脅曝露管理」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

# 攜手應對，重視安全



## 全面應對策略保護企業IT/OT網路安全

✓ 持續威脅暴露管理

✓ 偵測和強化最佳實踐

✓ 擴展IAM安全價值

✓ 加強供應鏈風險管理

✓ 制定完善的事件應對計劃