DEVCORE
SECURITY
CONSULTING

遇駭當下，如何處置?

翁浩正 (Allen Own)

戴夫寇爾股份有限公司

allenown@devco.re

2019.10.08 台灣資安通報應變年會

講者簡介

翁浩正 (Allen Own)

戴夫寇爾 DEVCORE 執行長

台灣駭客協會 HITCON 常務理事

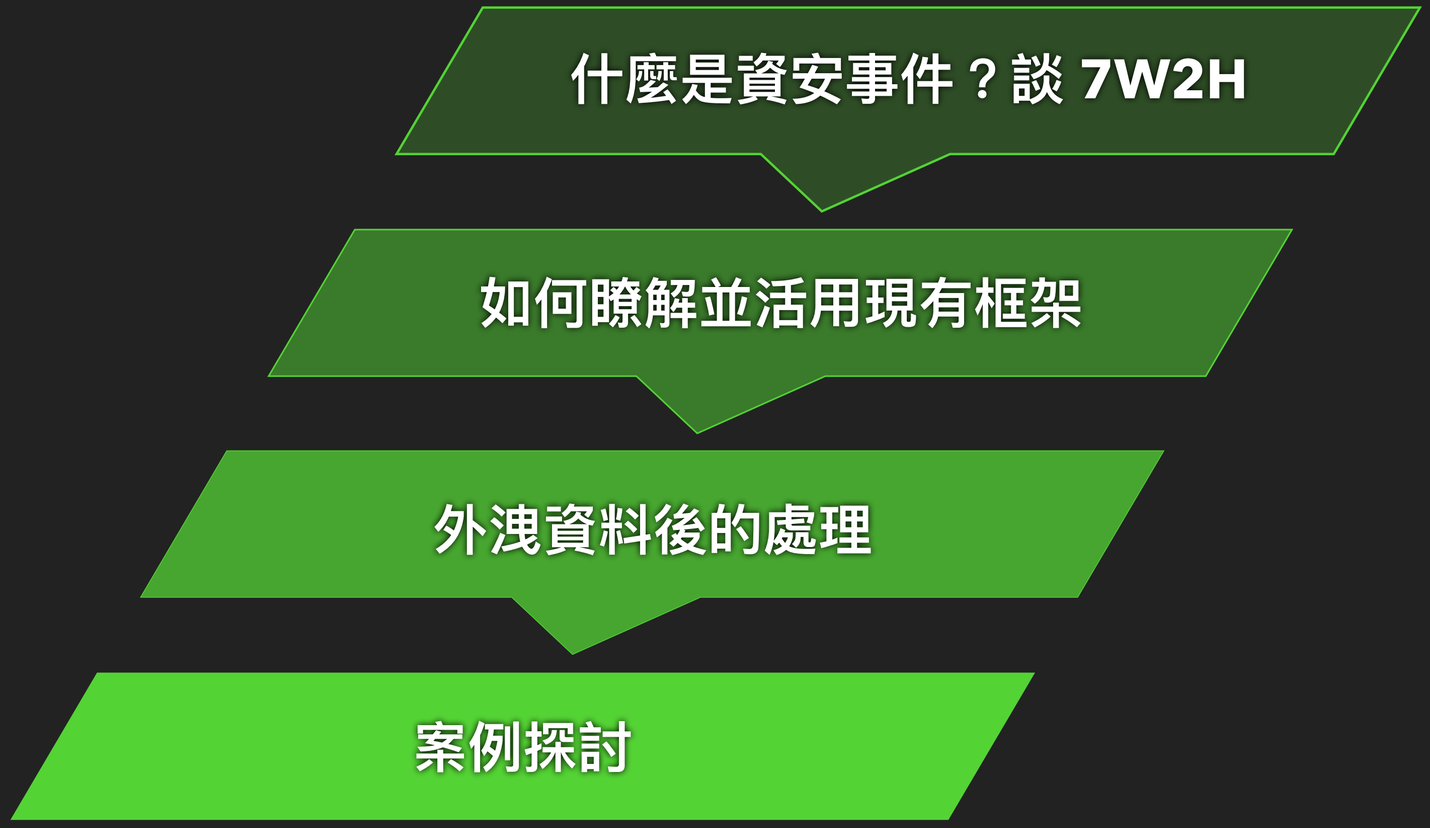
TiEA 協會理事及資安小組負責人

allenown@devco.re

專長：駭客攻擊手法分析、 紅隊演練

DEVCORE SECURITY CONSULTING

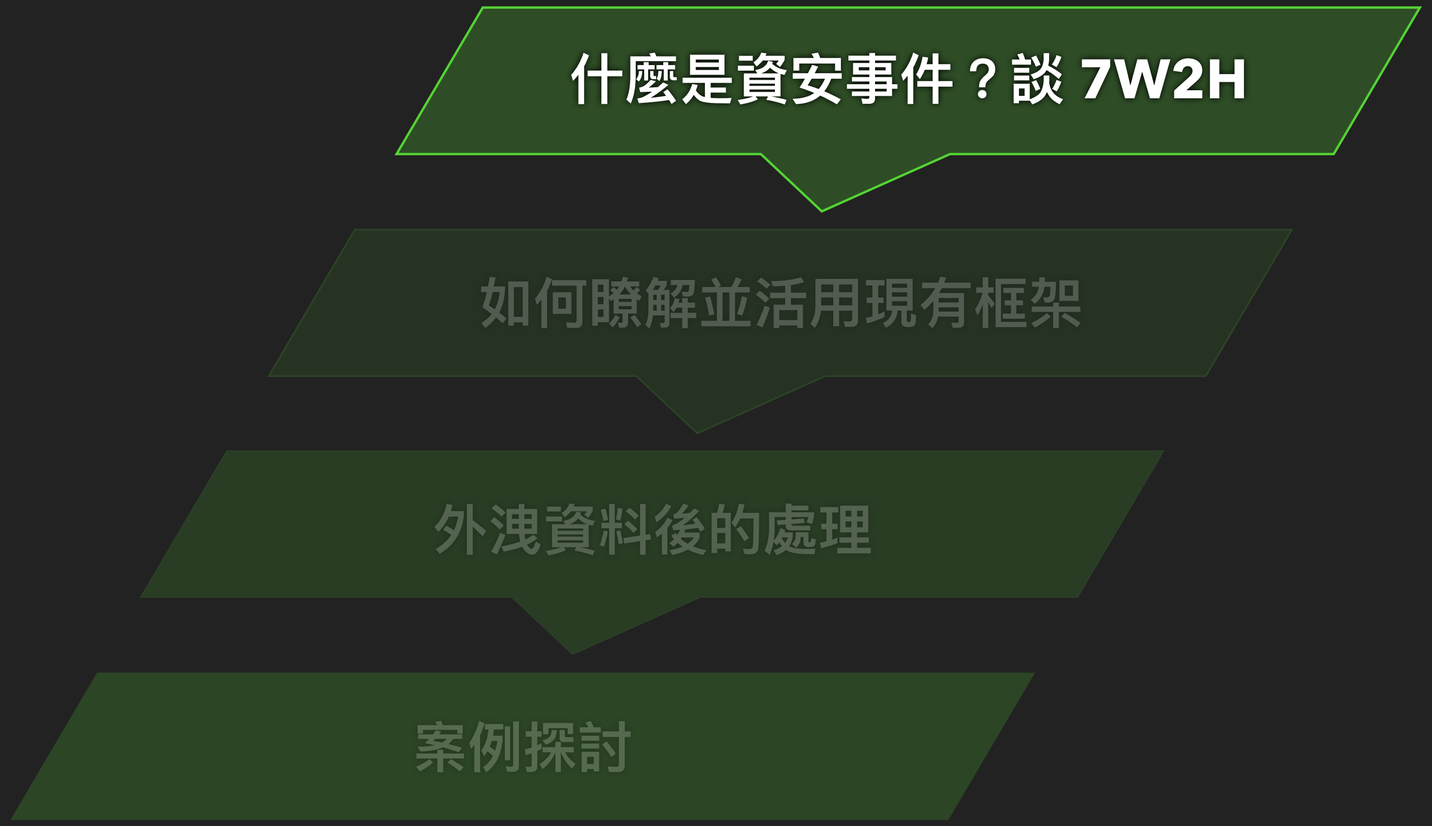
遇駭當下，如何處置?



DEVCORE SECURITY CONSULTING

遇駭當下，如何處置?

- ✓ 什麼是資安事件？
- ✓ 用資安事件的 7W2H 瞭解資安事件



遇駭當下，如何處置?

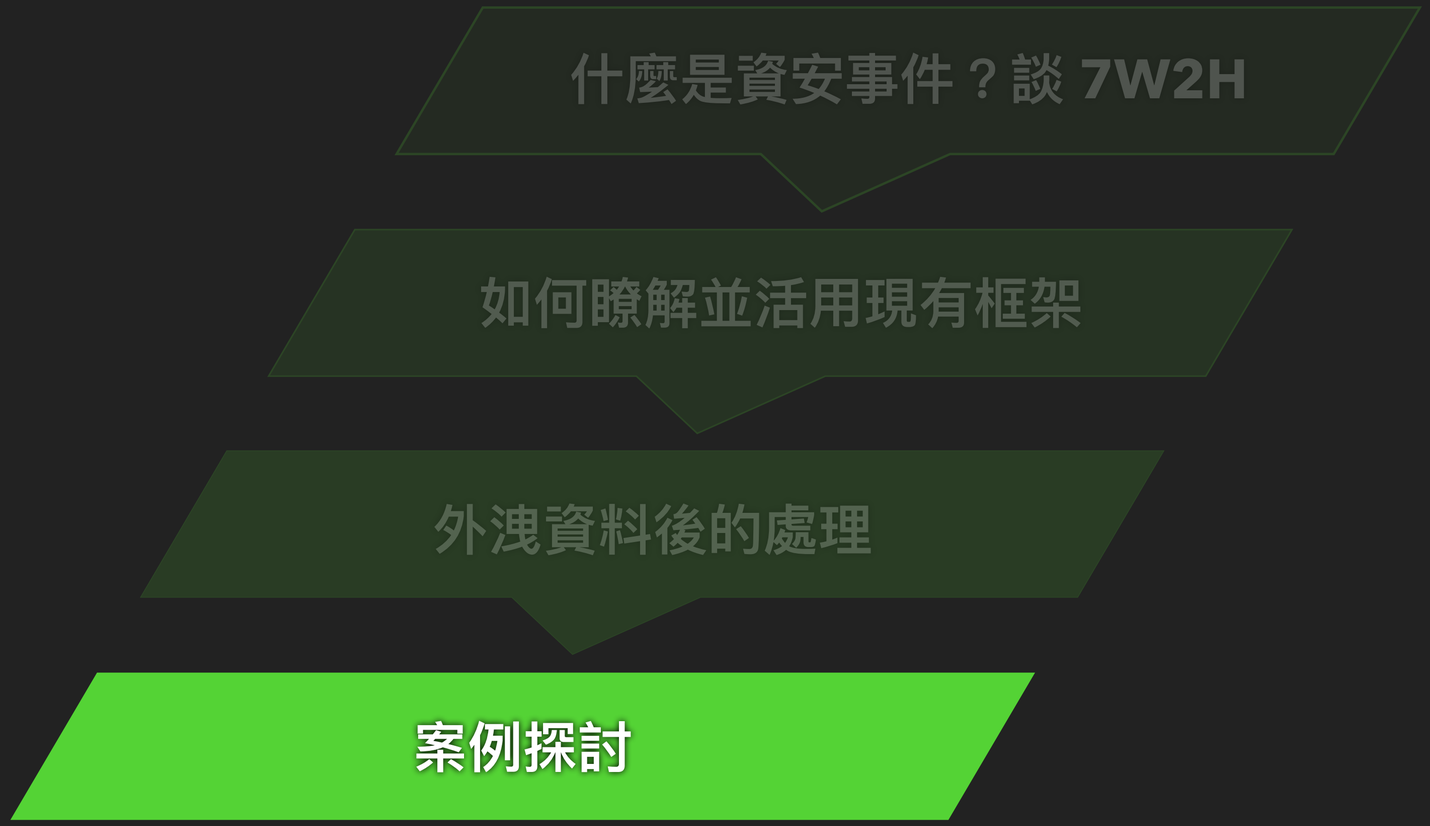
- ✓ NIST Cybersecurity Framework
- ✓ CREST Cyber Security Incident Response Guide
- ✓ MITRE ATT&CK Framework

遇駭當下，如何處置?

- ✓ 資料外洩之後的處理方針
- ✓ 如何有效的通知受害者

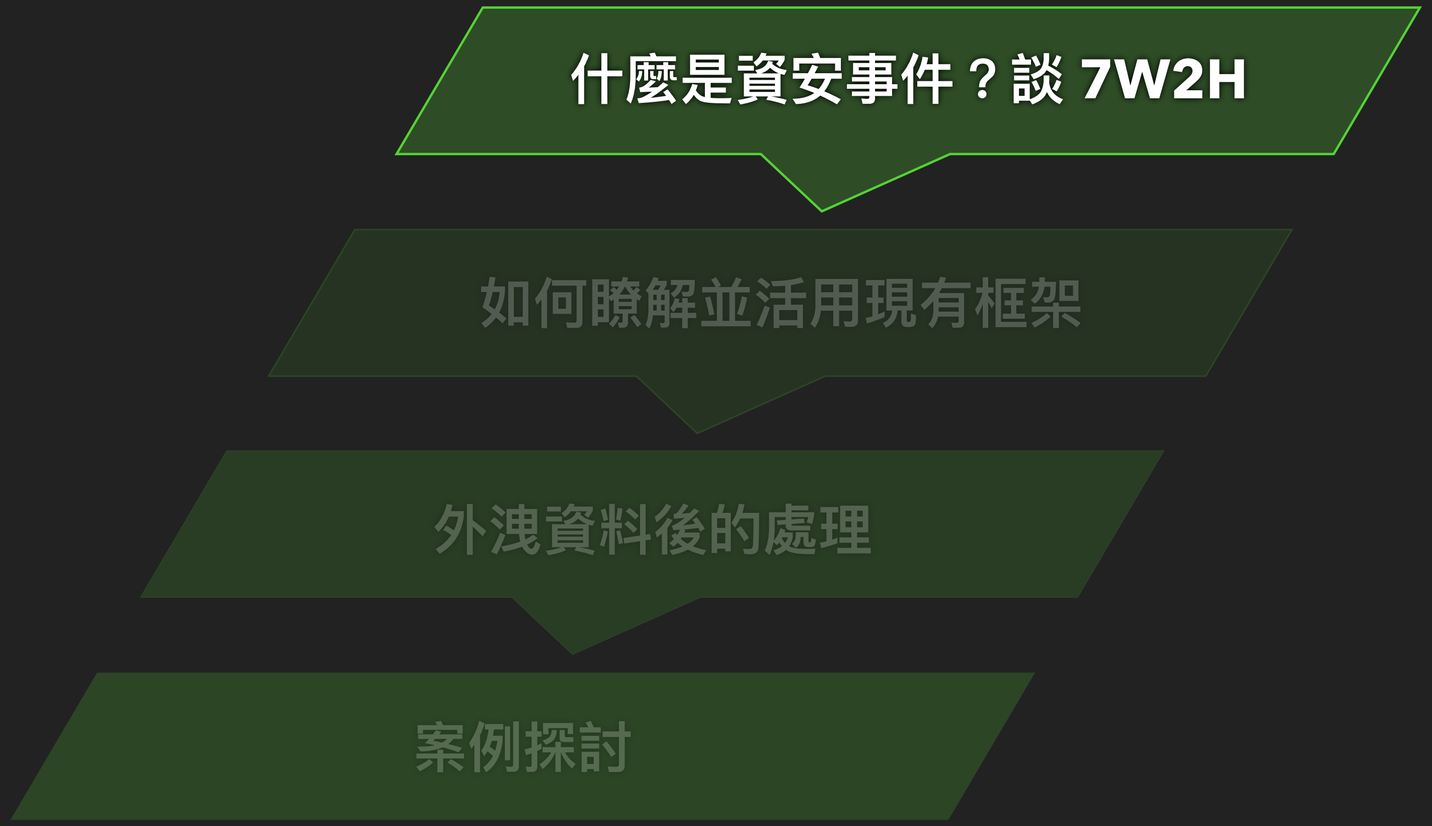
遇駭當下，如何處置?

- ✓ 案例探討



遇駭當下，如何處置?

- ✓ 什麼是資安事件？
- ✓ 用 7W2H 瞭解資安事件



什麼是資安事件？

若資安事件發生，建議流程：

- 制定、檢視、修正事件應變計畫
- 組織內部及外部規範對應處置（ISMS等）
- 立刻通知客戶、相關單位、主管機關
  - 說明目前情況、損失、影響、企業處置、客戶後續該做什麼處理
- 了解相關法規，通知律師並協調法律策略
- 媒體公關處理
- 尋找外部事件應變團隊
- 風險管控（如資安險）
- 警調報案

WHO
WHY
WHAT
WHOM
WHERE

WHICH
WHEN
HOW
HOW MUCH

資安事件的 7W2H

- WHO：攻擊者是誰？
- WHY：為什麼要攻擊？
- WHAT：攻擊者要的是什麼？
- WHOM：為什麼是我被攻擊？
- WHERE：從哪裡開始攻擊？
- WHICH：攻擊目標是誰？
- WHEN：什麼時候發動攻擊？
- HOW：怎麼攻擊？
- HOW MUCH：攻/防需要多少資源？

讓你的主管知道你需要投入多少資源，
及組織的資安防護應該做到什麼等級

WHO: 攻擊者是誰？

- 黑色產業
- 惡意駭客組織，並與詐騙集團合作
- 同業競爭對手
- 個體戶
- 國家級攻擊單位

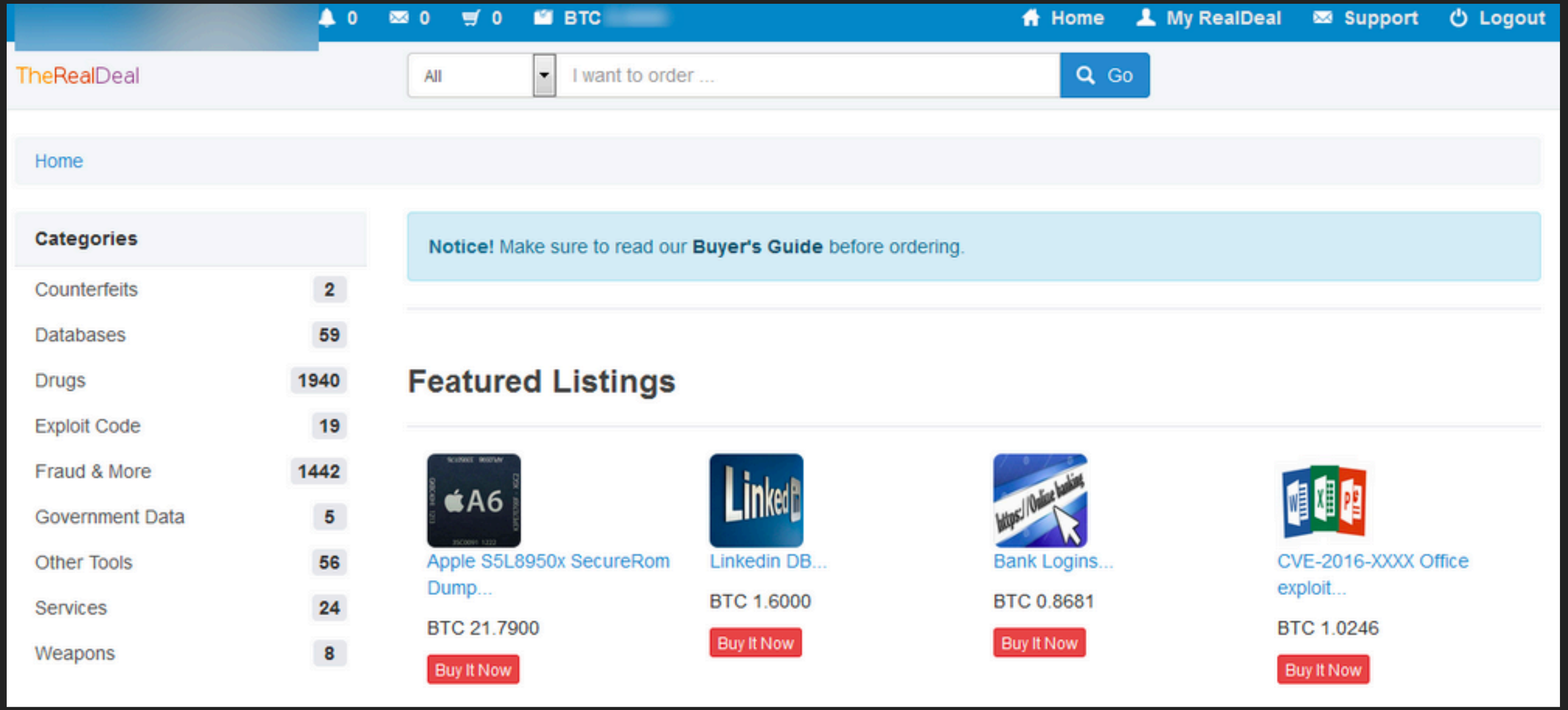
WHY: 為什麼要攻擊我？

- 為了錢財利益而攻擊
- 公務、私人恩怨
- 威脅
- 為了有趣、炫耀

WHAT: 攻擊者要的是什麼？

- 可以販賣的資料
  - 個資
  - 金融資料
  - 帳號密碼
  - 企業內部機敏資料
- 可以利用的資源
  - 作為跳板
  - 作為「肉機」
  - 作為殭屍網路

黑色產業地下市集


0
0
0
BTC
Home
My RealDeal
Support
Logout
TheRealDeal
All
I want to order ...
Go
Home
Categories
Counterfeits 2
Databases 59
Drugs 1940
Exploit Code 19
Fraud & More 1442
Government Data 5
Other Tools 56
Services 24
Weapons 8
Notice! Make sure to read our Buyer's Guide before ordering.
Featured Listings
A6
Apple S5L8950x SecureRom Dump...
BTC 21.7900
Buy It Now
Linked
Linkedin DB...
BTC 1.6000
Buy It Now
Bank Logins...
BTC 0.8681
Buy It Now
CVE-2016-XXXX Office exploit...
BTC 1.0246
Buy It Now

WHOM: 為什麼是我？

- 軟柿子
  - 如：含有明顯漏洞的網站，比較好下手
- 核彈試爆場
  - 如：最近出現的新漏洞、新攻擊手法
- 看起來有錢人
  - 如：擁有大量金錢、如交易平台、比特幣

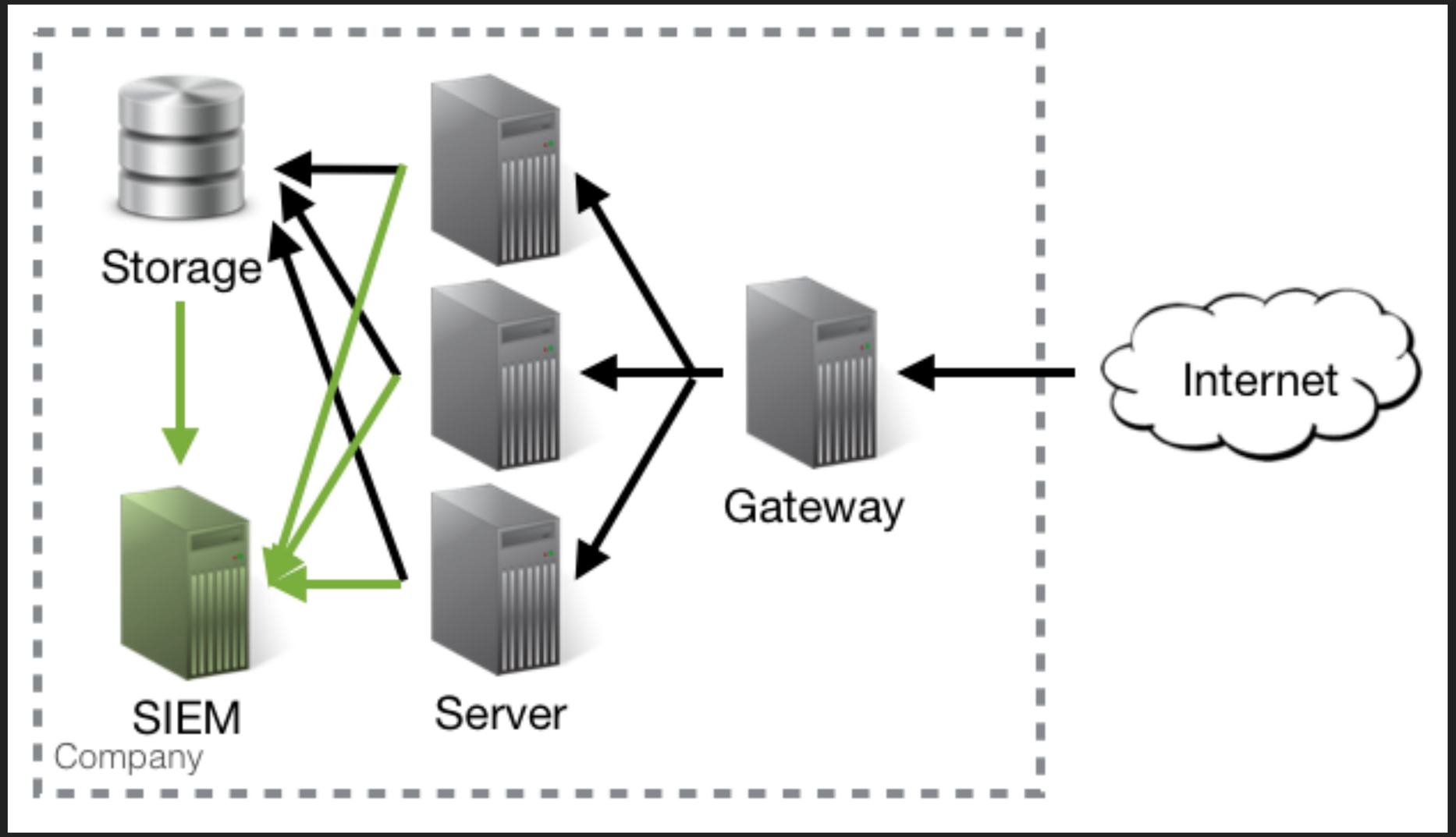
如何讓攻擊者不選我

- 需較多時間：資安防禦健全，紓緩攻擊的壓力
- 需較多資源：需要更多主機、花費進行破解
- 需較多風險：會暴露行蹤、有被抓的風險

如何讓攻擊者不選我

- 需較多時間：資安防禦健全，紓緩攻擊的壓力
  - 如防火牆、WAF、IDS、伺服器安全阻擋設定
- 需較多資源：需要更多主機、花費進行破解
  - 如強加密法、強演算法、或者資安防禦健全
- 需較多風險：會暴露行蹤、有被抓的風險
  - 如系統記錄遠端備份機制、監控機制

配置 SIEM 伺服器

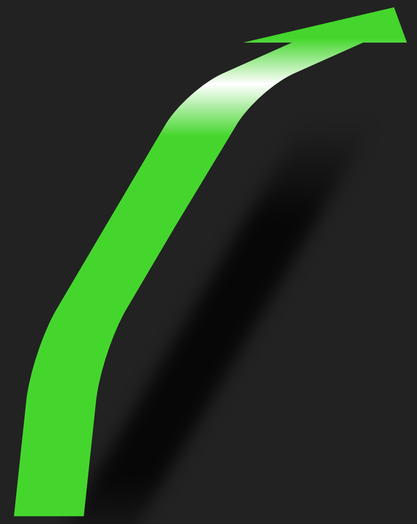


WHERE: 從哪裡開始攻擊？

- 正面迎擊
- 側面襲擊
- 背後突擊

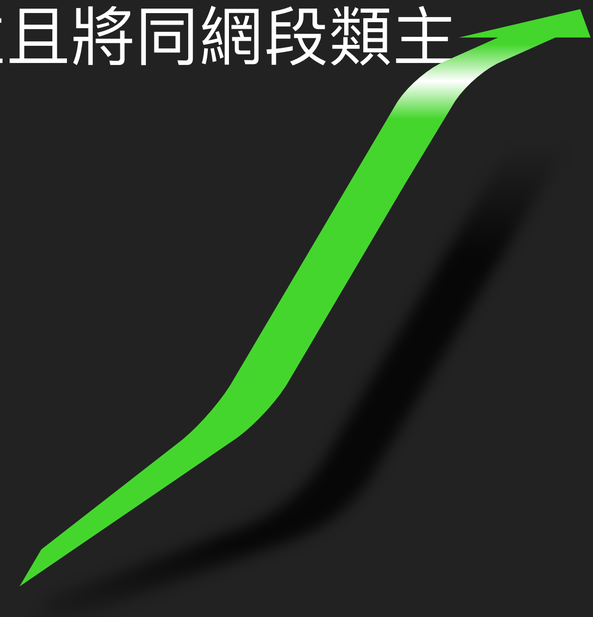
正面迎擊

- 直接正面迎戰網站服務，無畏防禦機制！
- 當網站有漏洞、未修補安全問題，或是網站吸引入侵者，攻擊者將會正面迎擊網站！
- 若網站防禦完備，較不需要擔心來自正面的攻擊，只要記得定期實施資安檢測、及確保系統的安全漏洞都及時修補完畢。



側面襲擊

- 透過入侵企業小型站台，或同主機其他站台，來攻回目標，又稱「旁注」。
- 如果正面無法被入侵，攻擊者會尋找同 IP、或相近網段的其他主機進行攻擊，若攻擊成功有機會可以滲透回目標網站。
- 企業必須將伺服器的網站單純化，避免不必要的站台共存，並且將同網段類主機信賴關係盤點清楚。



背後突擊

- 透過社交工程等方式，滲透企業內部，從背後發動攻擊。目前 APT 攻擊多採取此類方式，難以防禦。
- 攻擊者會製作一惡意文件，寄送給企業關鍵人物，誘使他開啟。若該人員沒有充足資安思維，或是使用的軟體含有安全漏洞，將可能直接遭到入侵。
- 藉由控制員工電腦可直接滲透企業內部竊取資料。

防火牆只要擋外部連線嗎？

DEVCORE SECURITY CONSULTING

Ref: https://www.facebook.com/thehackernews/posts/1307041839309688

WHICH: 攻擊目標是什麼？

- 攻擊必定帶隨利益，不僅錢財或者名聲
- 以攻擊者評估最容易被攻擊的目標
- 老舊主機、曾發生資安事件的主機、漏洞尚未修補完畢

WHICH

WHEN: 什麼時候會發動攻擊

- 無時無刻
- 有重大新漏洞發表的時候
- 企業被揭露資安漏洞時

WHEN

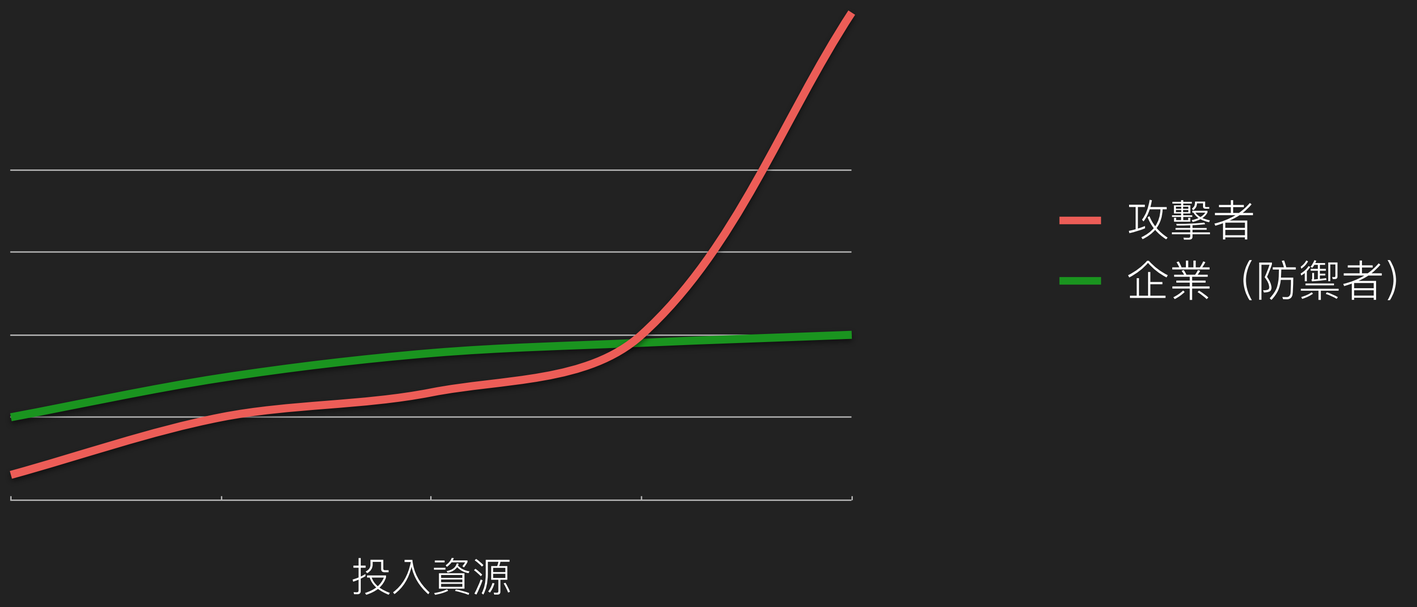
HOW: 怎麼攻擊的？

- 針對不同的攻擊階段、目的採取不同的攻擊方式，例如蒐集情報，或者是針對弱點進行客製化攻擊。
- 掃描服務：Port Scanning
- 攻擊特定漏洞：Vulnerability Exploit
- 人工客製化攻擊：尋找 0-day、邏輯問題等
- 阻斷服務攻擊：DoS、DDoS

HOW

HOW MUCH: 雙方的資源競爭

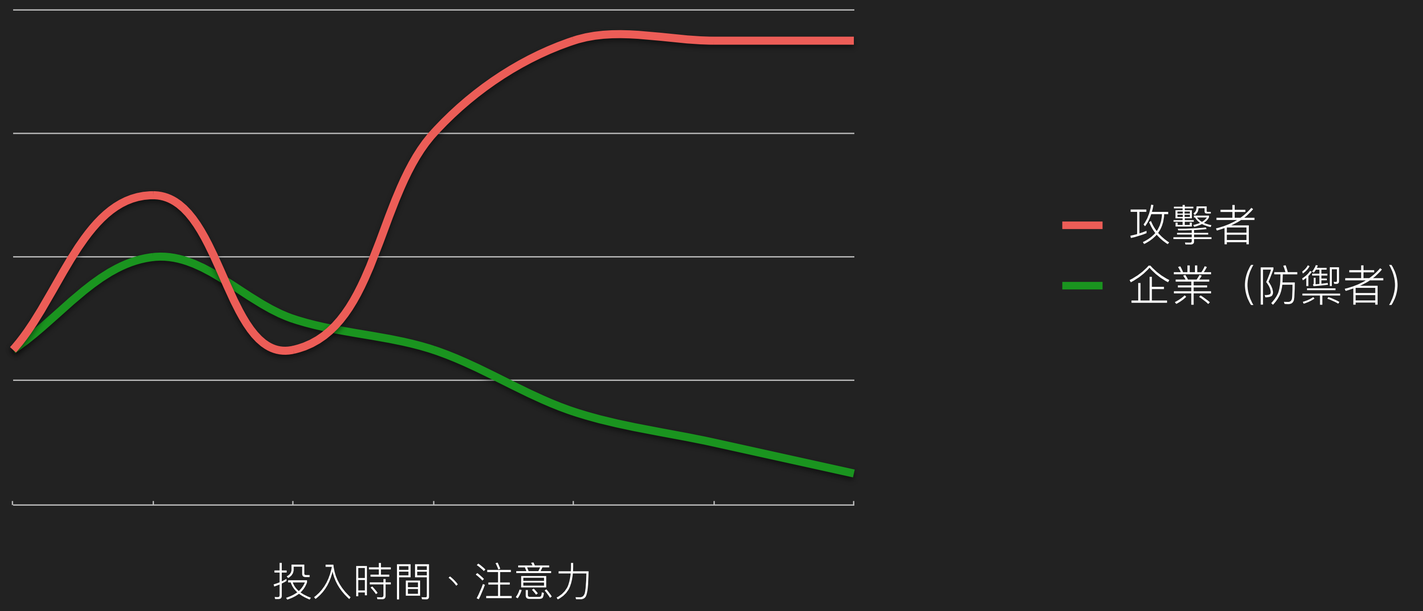
- 敵暗我明，攻擊者只要利用一點資源，狙擊企業的脆弱點，就能夠得到預期的資料。但當防禦等級達到一定程度，攻擊者就必須要花費極高成本達成攻擊。



HOW MUCH

HOW MUCH: 雙方投入注意力

- 但若攻擊者想達成的目的，讓他願意投入足夠的時間進行滲透（APT 攻擊），時間可能長達數個月至數年，則企業難以防禦，因無法維持長久精力注意。



HOW MUCH

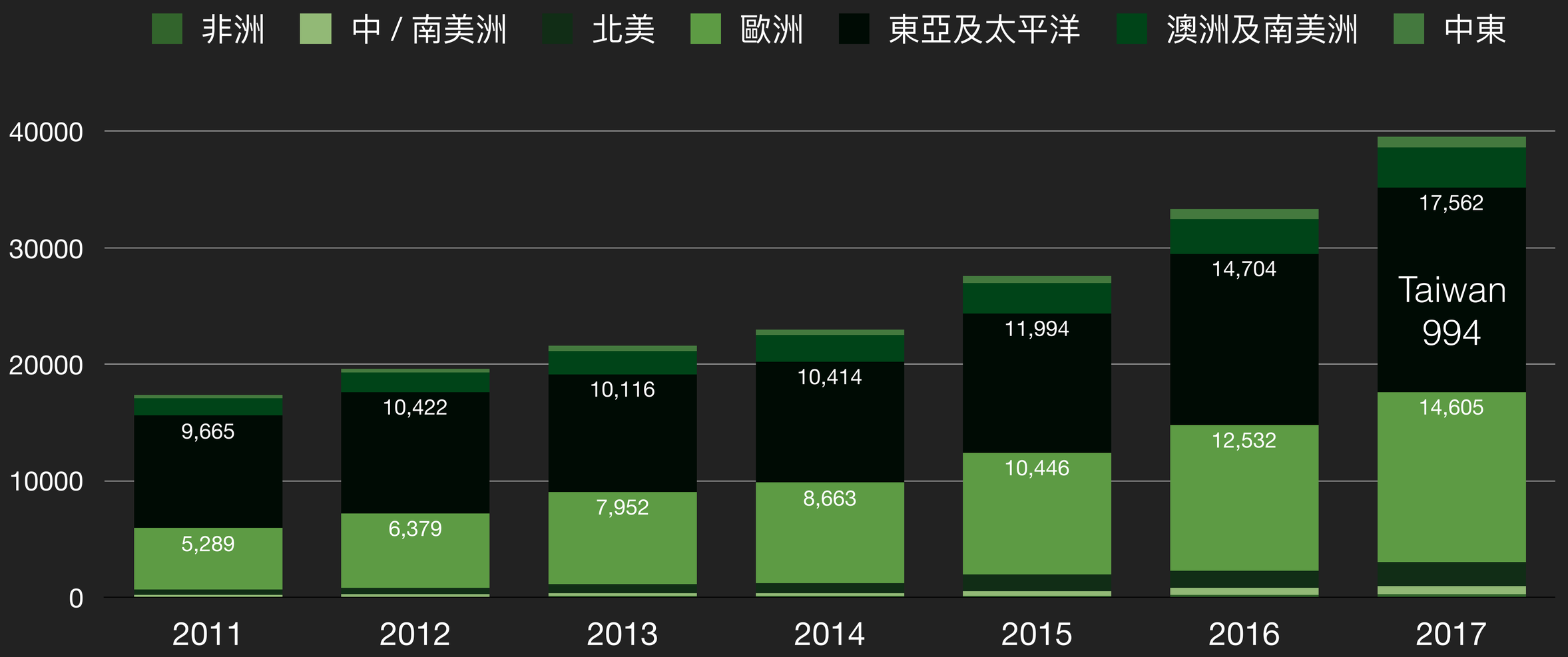
遇駭當下，如何處置?

- ✓ NIST Cybersecurity Framework
- ✓ CREST Cyber Security Incident Response Guide
- ✓ MITRE ATT&CK Framework

資安框架 (Framework)

協助企業擬定資安整體規劃藍圖、實施風險控管

ISO 27001 認證數量統計

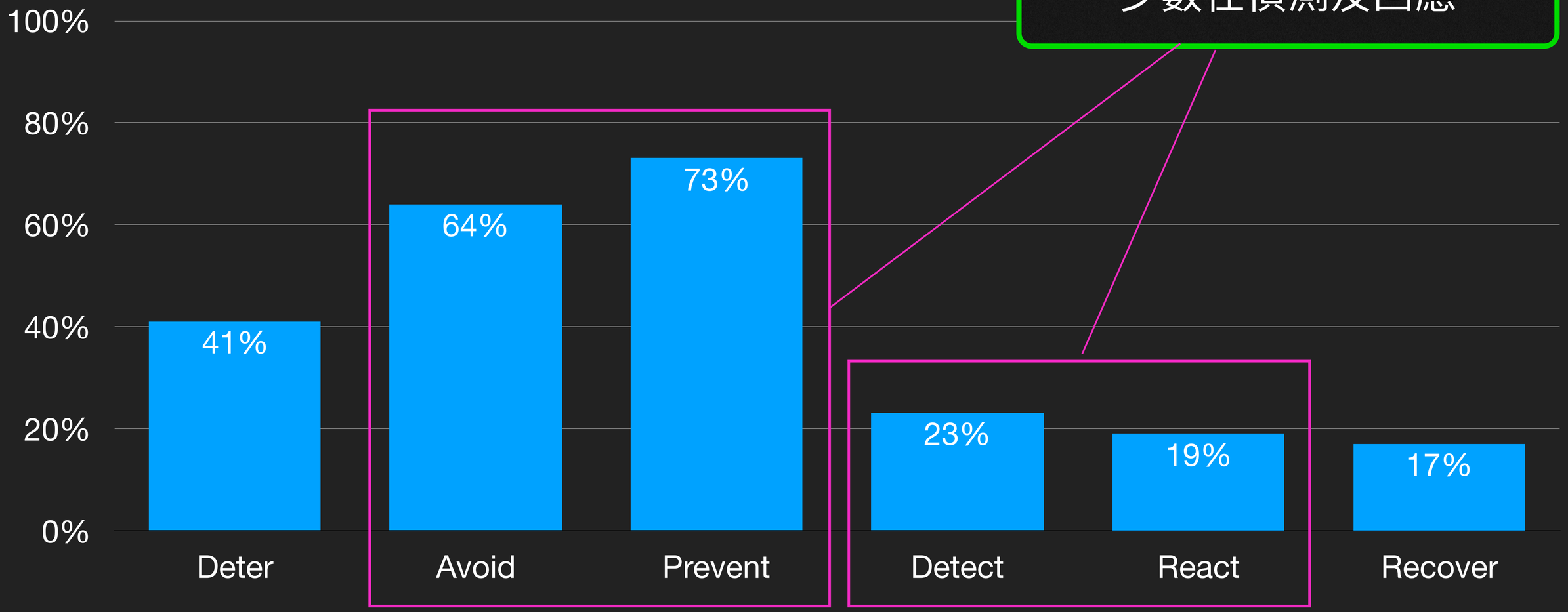


DEVCORE SECURITY CONSULTING

Source: http://www.iso27001security.com

框架特性

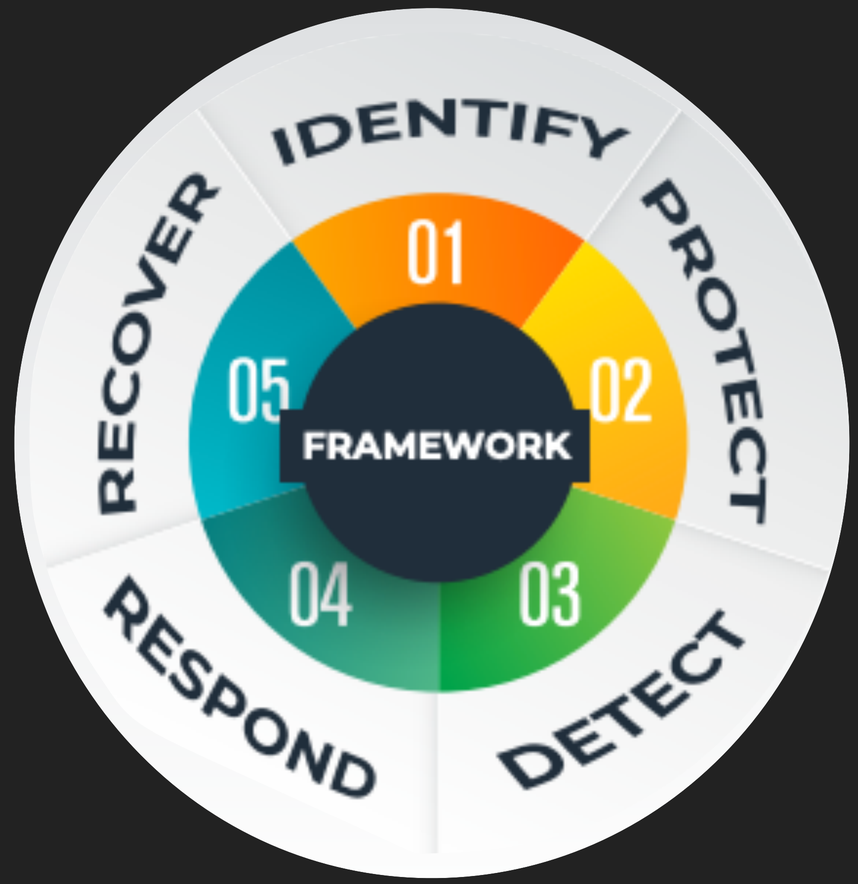
主要集中在避免及預防
少數在偵測及回應



http://www.iso27001security.com

NIST Cybersecurity Framework

- https://www.nist.gov/cyberframework
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx
- 2014年2月正式發布
  - Identify 識別
  - Protect 保護
  - Detect 偵測
  - Respond 回應
  - Recover 復原



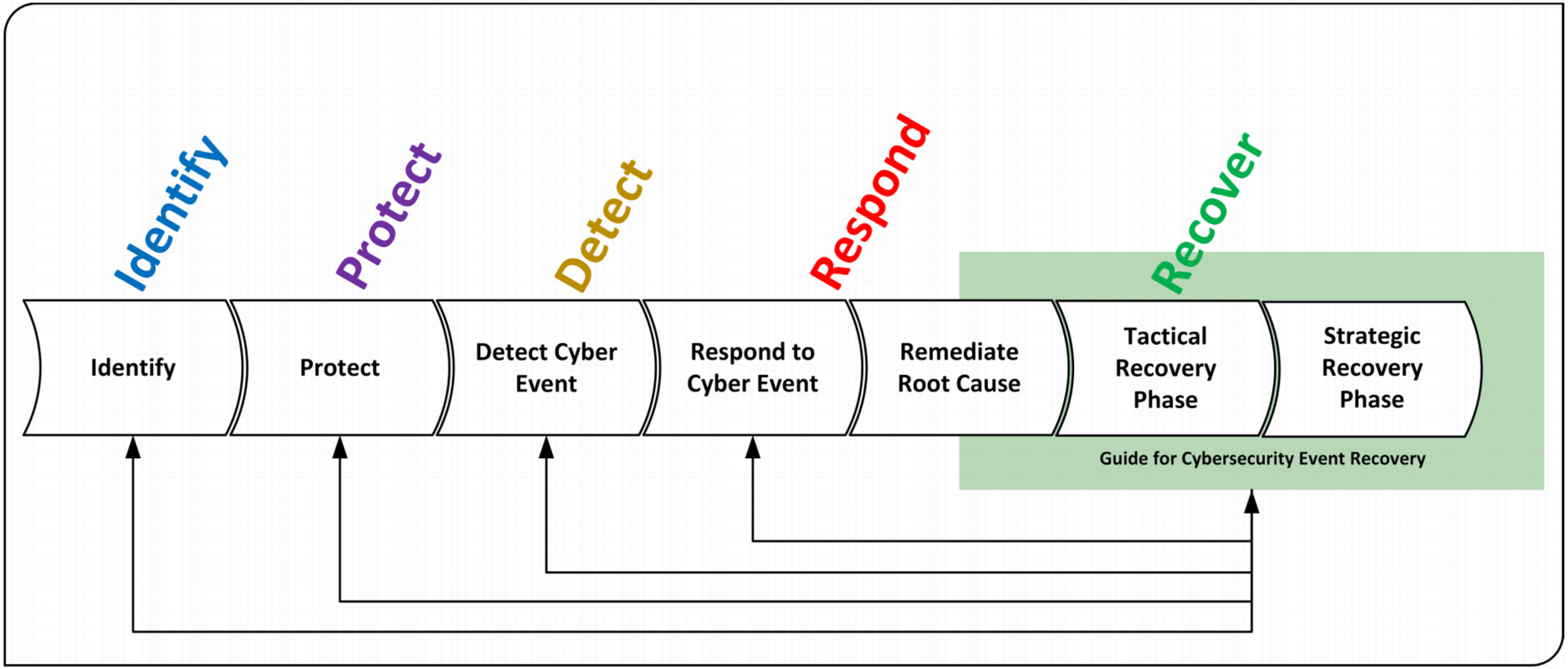


Figure 3-1: NIST SP 800-184 Guide for Cybersecurity Event Recovery Relationship with the NIST CSF

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

Function	Category
IDENTIFY (ID)	資產管理 Asset Management (ID.AM)
	營運環境 Business Environment (ID.BE)
	治理 Governance (ID.GV)
	風險評估 Risk Assessment (ID.RA)
	風險管理策略 Risk Management Strategy (ID.RM)
	供應練風險管理 Supply Chain Risk Management (ID.SC)
PROTECT (PR)	身分認證管理、授權及存取控制 Identity Management, Authentication and Access Control (PR.AC)
	意識及教育訓練 Awareness and Training (PR.AT)
	資料安全 Data Security (PR.DS)
	資訊保護流程及過程 Information Protection Processes and Procedures (PR.IP)
	維護 Maintenance (PR.MA)
	防護技術 Protective Technology (PR.PT)
DETECT (DE)	異常偵測及事件管理 Anomalies and Events (DE.AE)
	安全持續性監控 Security Continuous Monitoring (DE.CM)
	偵測流程 Detection Processes (DE.DP)
RESPOND (RS)	應變計畫 Response Planning (RS.RP)
	溝通 Communications (RS.CO)
	事件分析 Analysis (RS.AN)
	事件緩解 Mitigation (RS.MI)
	改善 Improvements (RS.IM)
RECOVER (RC)	復原計畫 Recovery Planning (RC.RP)
	改善 Improvements (RC.IM)
	溝通 Communications (RC.CO)

CREST
Cyber Security Incident Response Guide

DEVCORE SECURITY CONSULTING

CREST Cyber Security Incident Response Guide

- CREST Cyber Security Incident Response Guide
- https://www.crest-approved.org/

- Prepare
- Response
- Follow Up

PHASE 1 — Prepare

- **Step 1.** Conduct a criticality assessment for your organisation
- **Step 2.** Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals
- **Step 3.** Consider the implications of people, process, technology and information
- **Step 4.** Create an appropriate control framework
- **Step 5.** Review your state of readiness in cyber security incident response

PHASE 2 — Respond

- **Step 1.** Identify cyber security incident
- **Step 2.** Define objectives and investigate situation
- **Step 3.** Take appropriate action
- **Step 4.** Recover systems, data and connectivity

PHASE 3 — Follow Up

- **Step 1.** Investigate incident more thoroughly
- **Step 2.** Report incident to relevant stakeholders
- **Step 3.** Carry out a post incident review
- **Step 4.** Communicate and build on lessons learned
- **Step 5.** Update key information, controls and processes
- **Step 6.** Perform trend analysis

DEVCORE SECURITY CONSULTING

Topic	Basic cyber security incident	Sophisticated cyber security attack
Type of attacker	• Small-time criminals • Individuals or groups just 'having fun' or ' responding to a challenge' • Localised, community or individual Hacktivists • Insiders	• Serious organised crime • State-sponsored attack • Extremist groups
Target of attack	• General public • Private sector • Non-strategic government departments	• Major corporate organisations • International organisations • Governments • Critical national infrastructure • National security / defence
Purpose of attack	• Financial gain • Limited disruption • Publicity • Vendettas or revenge	• Major financial reward • Widespread disruption • Discover national secrets • Steal intellectual property of national importance • Terrorism • Warfare
Capability of attacker	• Low skill • Limited resource • Publicly available attack tools • Not well organised • Local reach	• Highly skilled professionals • Extremely well resourced • Bespoke tools • Highly organised • International presence
Response requirements	• Restore services • Special monitoring and organisation • Some industry information sharing	• Tailored guidance for specialist industry and specific capabilities • Implications for government security services • CNI sector-specific industry response

Cyber Attacks Phrases

CREST Cyber Security Incident Response Guide

https://www.crest-approved.org/

① Reconnaissance

- Identify target
- Look for vulnerabilities

② Attack Target

- Exploit vulnerabilities
- Defeat remaining controls

③ Achieve Objective

- Disruption of systems
- Extraction
- Manipulation

Countermeasures

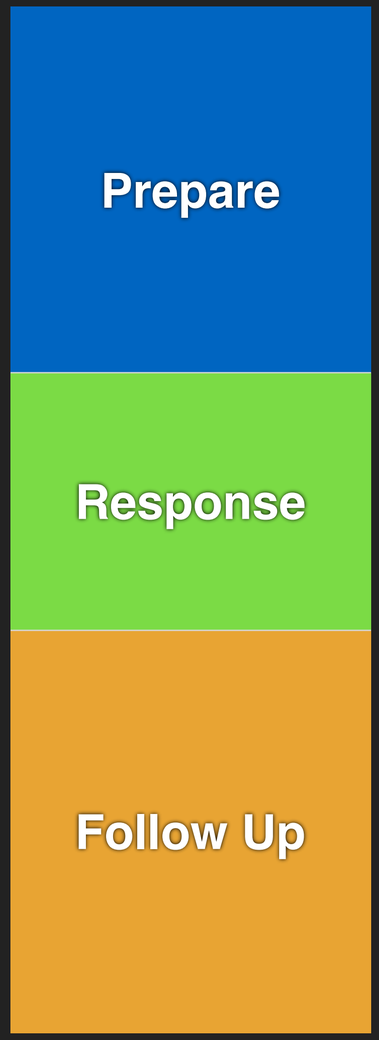
- Monitoring and Logging
- Situational awareness
- Collaboration

- Solid architectural system design
- Standard controls
- Penetration Testing

- Cyber security incident response
- Business continuity and disaster recovery plans
- Cyber security insurance

DEVCORE SECURITY CONSULTING

CREST Cyber Security Incident Response



Step 1. Conduct a criticality assessment for your organisation
Step 2. Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals
Step 3. Consider the implications of people, process, technology and information
Step 4. Create an appropriate control framework
Step 5. Review your state of readiness in cyber security incident response

Step 1. Identify cyber security incident
Step 2. Define objectives and investigate situation
Step 3. Take appropriate action
Step 4. Recover systems, data and connectivity

Step 1. Investigate incident more thoroughly
Step 2. Report incident to relevant stakeholders
Step 3. Carry out a post incident review
Step 4. Communicate and build on lessons learned
Step 5. Update key information, controls and processes
Step 6. Perform trend analysis

DEVCORE SECURITY CONSULTING

Prepare

Step 1. 實施組織內關鍵資產分析 Conduct a criticality assessment for your organisation

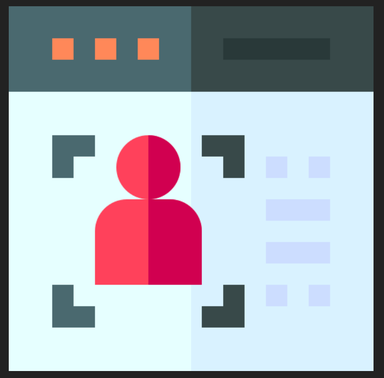
1. 定義關鍵資訊資產
2. 確定哪些安全威脅最可能影響這些關鍵資訊資產
3. 實施管理或技術控制措施，降低影響關鍵資訊資產資安事件發生的可能性和影響
4. 提升對資安事件應變能力的需求
5. 確認資安事件發生時業務衝擊等級

Prepare

Step 2. 實施資安風險威脅分析 Carry out a cyber security threat analysis

- **用真實的情境或者演練進行資安威脅分析，用以瞭解組織的威脅等級**
- **先盤點資產、後盤點內外部威脅**

- 瞭解公司業務性質，業務策略，業務流程和風險承受能力
- 盤點關鍵的人員、科技、供應商、合作伙伴
- 盤點可能被鎖定攻擊的資產，如基礎建設、金錢、智慧財產或人員
- 盤點可能與組織有關的弱點攻擊程式、惡意程式、或駭客組織



Prepare

Cyber Security Incident Scenarios

- Determining what the threat is to your organisation
- Assessing your risk profile (to key assets)
- Considering threat intelligence providers
- Evaluating situational awareness and applicability to your organisation
- **Simulating a real attack as closely as possible**
- Ensuring the right person is doing the right thing at the right time.

Prepare

Step 3. Consider the implications of people, process, technology and information

- 安排人員、程序、科技、資訊 (people, process, technology, information)
- 人員編組、執掌，事件相關的流程、工具、系統，資訊流的整理等等

Prepare

Step 4. Create an appropriate control framework

- 選定合適的控制框架及措施
- 傳統防禦措施雖然無法防禦攻擊，但可以減緩攻擊成功率及速度
- 良好的控制框架中會明確表示該進行哪些措施，可以成功防堵攻擊行為

Prepare

Step 5. Review your state of readiness in cyber security incident response

- 檢討組織在資安事件應變中的準備狀態
- 組織必須擁有資安事件應變能力，由完善的流程、技術人員、相關技術組成。擁有事件應變能力可以幫助組織徹底的調查事件，並成功消除潛藏在環境中的敵人
- 評估準備完成度：
  - People, process, technology, information
  - Preparedness, response and follow up activities.

Response

Step 1. Identify cyber security incident

- 最為挑戰的部分，因為資安事件通常難以精準偵測及處理

- 確定可疑的資安事件
- 分析與潛在資安事件相關的所有可用資訊
- 確定實際發生的事件情況（如 DDoS 攻擊）
- 確認確實受到攻擊或發生網絡資料外洩

Response

Step 2. Define objectives and investigate situation

- 定義事件處理的目標，攻擊事件的始末。可參考外部威脅情資。
- 瞭解資安事件：
  - 攻擊者是誰
  - 攻擊的範圍和程度
  - 攻擊事件發生的時間
  - 攻擊者取走了什麼資料
  - 為什麼他們要進行攻擊
- 進行初步事件回應及分析

Response

Step 3. Take appropriate action

- 初步調查後要採取的首要重點措施是控制資安事件造成的損害。
- 控制資安事件現況：
  - 阻擋並記錄未經授權的存取
  - 阻擋惡意程式來源，如信件跟網站
  - 關閉特定的連接埠及郵件主機
  - 若主機可能遭駭，更換系統管理員密碼
  - 防火牆過濾流量
  - 轉移網站首頁
  - 隔離系統
- 消除事件的發生原因
  - 辨識所有受影響的主機
  - 進行惡意程式分析
  - 應對若攻擊者是否有進一步動作
- 收集並保存證據

Response

Step 4. Recover systems, data and connectivity

- 最後一步是還原系統並恢復正常營運，並且確認漏洞都已經修補，以防相同攻擊再次發生。
- 需要擬定還原計畫，確保乾淨的重建目標伺服器。例如還原已經被感染的檔案、移除不必要的檔案、重設密碼、系統更新、確認系統完整性。

Follow Up

Step 1. Investigate incident more thoroughly

- 事件事後的調查需要比事件當下更為詳細，便於找出事件發生真正原因、改善控制措施、分享相關資料予合作伙伴，並且預防事件再次發生。
- 調查也可能需要引入外部資源，例如數位鑑識團隊、專家等等。

Follow Up

Step 2. Report incident to relevant stakeholders

- 當事件已經處理完畢，需要給予內部以及外部利害關係人正式報告。
- 完整描述事件的性質，事件相關記錄以及進行了哪些補救措施
- 真實評估事件對財務損失以及對業務的衝擊，如商譽受損
- 建議新增或強化相關控制措施，強化資安事件的預防、偵測、補救、復原

Follow Up

Step 3. Carry out a post incident review

- 針對資安事件進行事後回顧，探討事件中的重要資訊。如：
  - 同仁如何處理資安事件？有遵循何者程序？
  - 流程中有無阻礙事件處理的項目
  - 下次再次發生類似事件，同仁會採取什麼不同的措施？
  - 資訊分享該如何改進
  - 如何將事件結果回饋至風險評估方法？

Follow Up

Step 4. Communicate and build on lessons learned

- 在後續追蹤資安事件中，重點是文件化記錄、溝通和記取教訓
- 與所有利益關係人的溝通應清晰、簡潔，並專注於解決問題和控制改進。須明確指出仍然存在的理想差距，並提出減少差距的措施。
- 需要建立計劃，說明組織如何利用事件中的教訓來面對未來的攻擊，讓組織變得更有韌性。計劃應包括技術和非技術性的項目，這將有助於減少攻擊者的成功率，並更快且有效地處理攻擊者的行為。分析資安事件時，應評估是技術能力差距或是人員流程導致攻擊成功。
- 每個計畫項目都應分配給指定同仁，並安排優先權及完成日期，監督所有工作項目的狀態。

Follow Up

Step 5. Update key information, controls and processes

- 資安事件後，重要的是更新事件應變方法、控制措施及相關文件
- 通常較為困難的是：資安事件管理方法論、流程、管理措施、技術控制措施、業務連續性計劃、災難控制計畫、內部 IT 稽核流程

Follow Up

Step 6. Perform trend analysis

- 組織必須保留所有安全/資安事件的記錄及其他相關訊息，並定期查看相關的資安事件數據
  - 評估資安事件的模式和趨勢
  - 確定影響資安事件的常見因素
  - 確認控制措施的有效性
  - 了解發生資安事件相關的成本和衝擊

MITRE ATT&CK Framework

- https://attack.mitre.org/

Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and	The adversary is trying to communicate with compromised systems
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta	Path Interception		DCShadow	Private Keys		Third-party Software		Port Knocking		
	PowerShell	Port Monitors		Deobfuscate/Decode Files or Information	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	Service Registry Permissions Weakness			Two-Factor Authentication Interception		Windows Remote Management		Remote File Copy		
	Regsvr32	Setuid and Setgid		Disabling Security Tools		System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Startup Items		DLL Side-Loading		System Owner/User Discovery			Standard Cryptographic Protocol		
	Scripting	Web Shell		Execution Guardrails		System Service Discovery			Standard Non-Application Layer Protocol		
	Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Exploitation for Defense Evasion		System Time Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Account Manipulation		File Deletion		Virtualization/Sandbox Evasion			Web Service		
		Authentication Package	SID-History Injection	File Permissions Modification							
	Signed Script Proxy Execution	BITS Jobs	Sudo								
		Bootkit	Sudo Caching								
	Source	Browser Extensions		File System Logical Offsets							
	Space after Filename	Change Default File Association		Gatekeeper Bypass							
	Third-party Software			Group Policy Modification							
	Trusted Developer Utilities	Component Firmware		Hidden Files and Directories							
	User Execution	Component Object Model Hijacking		Hidden Users							
	Windows Management Instrumentation			Hidden Window							
		Create Account		HISTCONTROL							
	Windows Remote Management	External Remote Services		Indicator Blocking							
		Hidden Files and Directories		Indicator Removal from Tools							
	XSL Script Processing	Hypervisor		Indicator Removal on Host							
		Kernel Modules and Extensions		Indirect Command Execution							
		Launch Agent		Install Root Certificate							
		LC_LOAD_DYLIB Addition		InstallUtil							
		Login Item		Launchctl							
		Logon Scripts		LC_MAIN Hijacking							
		Modify Existing Service		Masquerading							
		Netsh Helper DLL		Modify Registry							
		Office Application Startup		Mshta							
		Port Knocking		Network Share Connection Removal							
		Rc.common		NTFS File Attributes							
		Redundant Access		Obfuscated Files or Information							
		Registry Run Keys / Startup Folder		Port Knocking							
		Re-opened Applications		Process Doppelgänging							
		Screensaver		Process Hollowing							
		Security Support Provider		Redundant Access							
		Shortcut Modification		Regsvcs/Regasm							
		SIP and Trust Provider Hijacking		Regsvr32							
		System Firmware		Rootkit							
		Systemd Service		Rundll32							
		Time Providers		Scripting							
		Windows Management Instrumentation Event Subscription		Signed Binary Proxy Execution							
		Winlogon Helper DLL		Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE

遇駭當下，如何處置?

- ✓ 資料外洩之後的處理方針
- ✓ 如何有效的通知受害者

Data Breach Response: A Guide for Business

- 保護你的營運 (Secure Your Operations)
- 修補漏洞 (Fix Vulnerabilities)
- 通知相關單位及個人 (Notify Appropriate Parties)

https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

保護你的組織營運 Secure Your Operations

- 召集專家組成團隊（鑑識、資安、法務、人資、公關等）
  - 定義數位鑑識小組 （瞭解事件影響範圍及證據）並與法律顧問諮詢
- 保護實體區域安全
  - 若事件與實體相關，如門禁系統，必須更換門禁等密碼
- 避免更多資料損失
  - 將影響主機下線並禁止關機，等鑑識團隊處理。更換帳號密碼憑證等。
- 移除網路上不適合出現的資訊
  - 自己網站：移除資料，並移除搜尋引擎快取
  - 外部網站：搜尋外洩資料在哪些網站出現，通知站方移除資料
- 與發現外洩資訊的人面談
- 避免影響或摧毀證據

修復資安漏洞 Fix Vulnerabilities

- 外部服務廠商或供應鍊
  - 確認廠商存取多少個資、更換存取權限、確認廠商已處理事件並修補漏洞
- 確認網路隔離
  - 將受影響主機隔離，避免危害擴張
- 與數位鑑識專家合作
  - 確認受害範圍（主機、資料）、備份還原、確認並調查系統記錄、處理問題
- 制訂溝通計畫
  - 對員工、客戶、投資人、合作伙伴制訂溝通計畫，避免資訊落差或公開資料

通知相關單位及個人 Notify Appropriate Parties

- 確認國家法律及規範需求 Determine Your Legal Requirements
- 通知執法機關 Notify Law Enforcement
  - 評估委請執法機關介入處理調查
- 外洩資料是否與電子醫療資料有關 Did the Breach Involve Electronic Health Information?
  - 聯邦貿易委員會的「醫療資訊外洩通報規則」
- 通知受影響的企業 Notify Affected Businesses
  - 通知合作廠商資訊外洩（外洩或被外洩），情況嚴重時通知主管機關
- 通知個人 Notify Individuals

通知個人使用者 Notify Individuals

- 通知受影響之使用者法律相關、外洩資料類型、內容、濫用可能性、潛在損失
- 諮詢執法機關聯絡窗口
- 指派組織內公關公告資訊或聯繫使用者
- 評估提供受影響使用者免費監控或支援
- **清楚描述目前資安事件的情況**
- 根據外洩資訊類型，告知受影響使用者可以採取什麼行動，並提供相關的聯絡資訊
- 如何從外洩事件或身份盜用中復原
- 在執法機關同意之下，考慮提供執法機關調查進度資訊
- 鼓勵資訊被濫用的使用者向 FTC 投訴 (IdentityTheft.gov)
- 通知未來針對事件會如何跟他們聯繫

通知個人使用者 Notify Individuals: 清楚描述目前資安事件的情況

- 資安事件怎麼發生的
- 被取得了什麼資料
- 攻擊者已經如何使用這些外洩資料
- 組織已經做了哪些處理措施
- 組織將提供給受影響使用者哪些額外防禦措施
- 如何聯繫組織內的聯絡窗口

範例通知信

[Name of Institution/Logo] ____ ____ Date: [insert date] NOTICE OF DATA BREACH Dear [Insert Name]: We are contacting you about a data breach that has occurred at [insert Company Name].	What Happened?	…..
	What Information Was Involved?	…..
	What We Are Doing	…..
	What You Can Do	…..
	Other Important Information	…..
	For More Information	…..

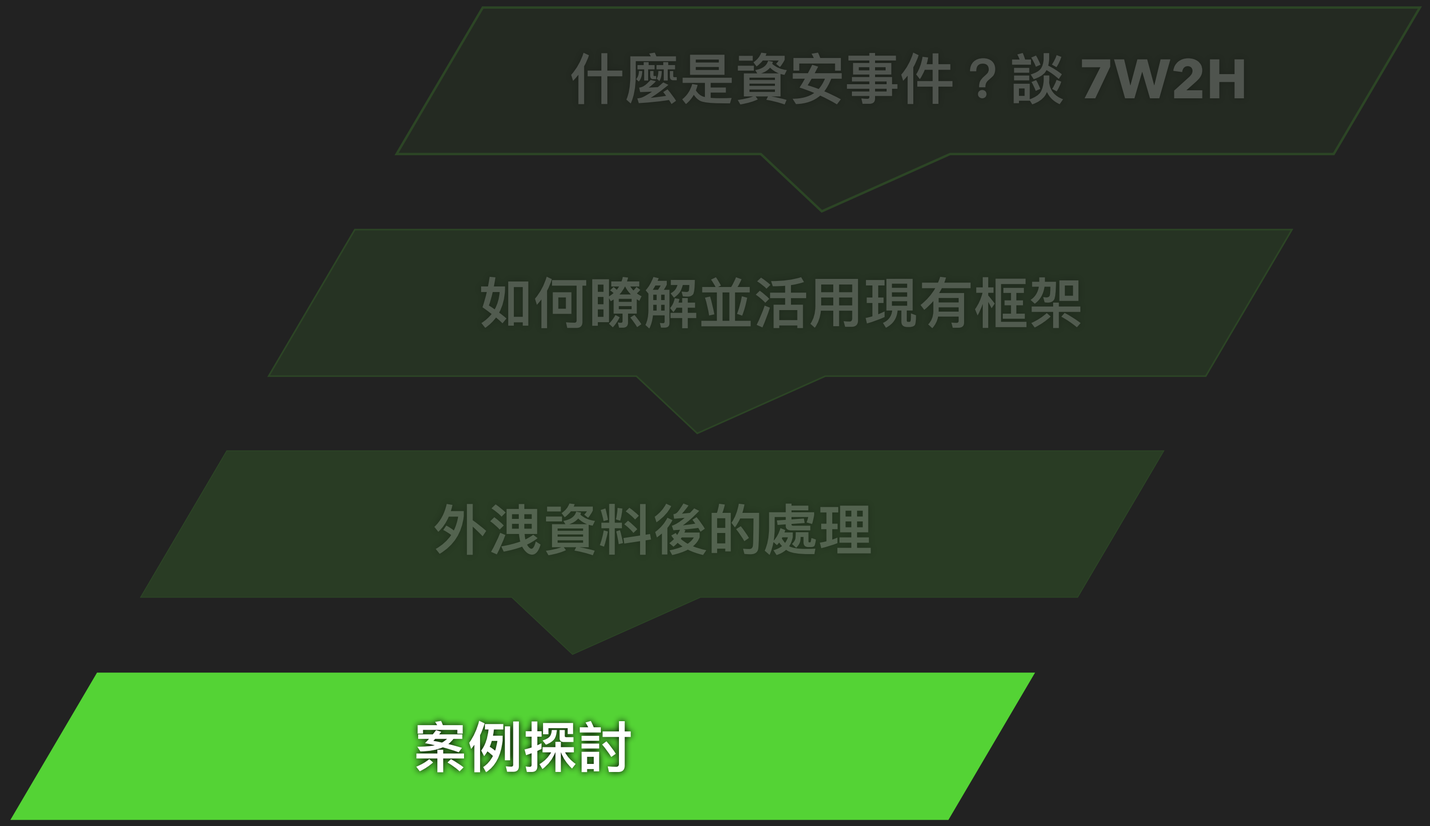
DEVCORE SECURITY CONSULTING

Reference

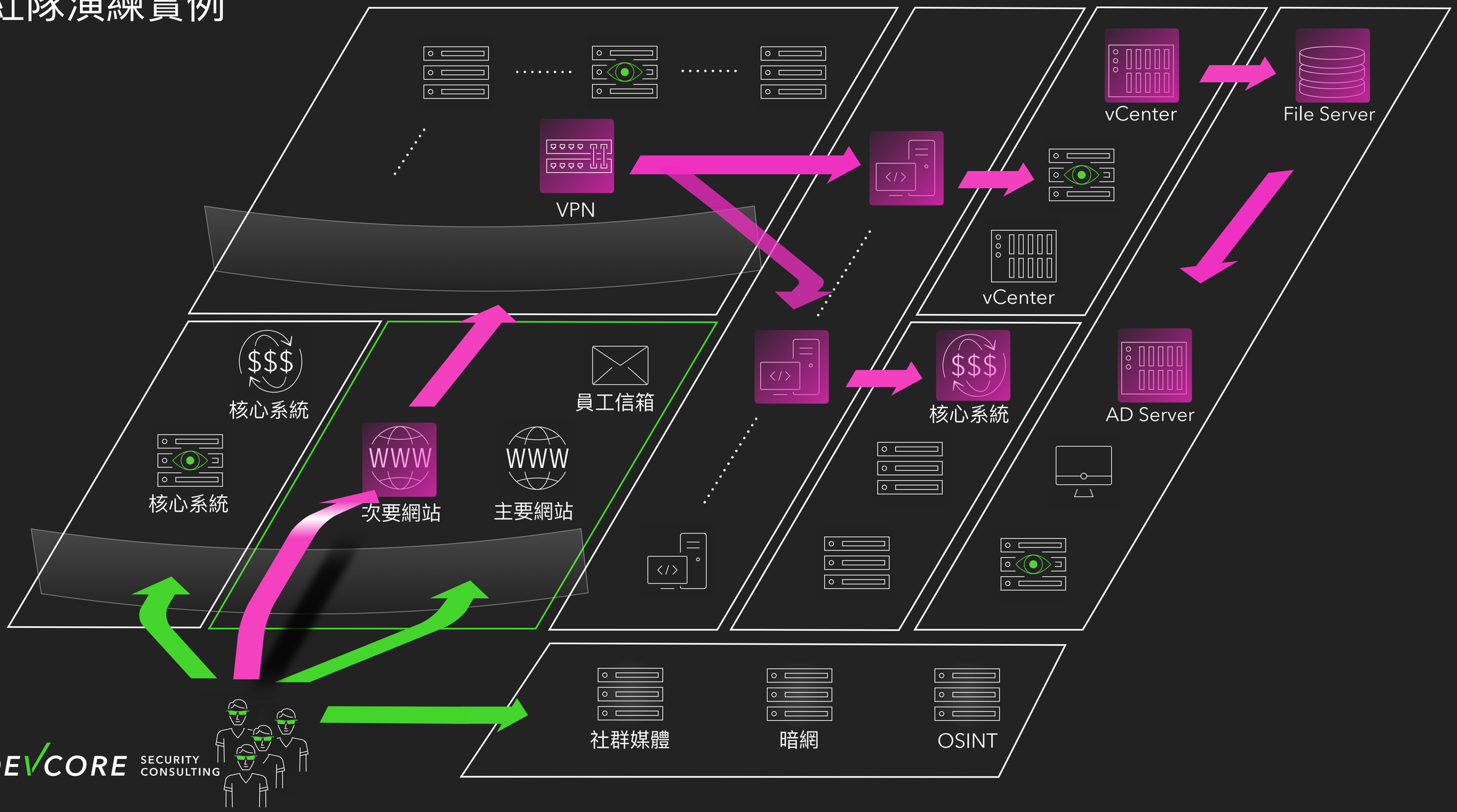
- Computer Security Incident Handling Guide (NIST SP 800-61)
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Guide for Cybersecurity Event Recovery (NIST SP 800-184)
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- Data Breach Response: A Guide for Business
  https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

遇駭當下，如何處置?

- ✓ 案例探討

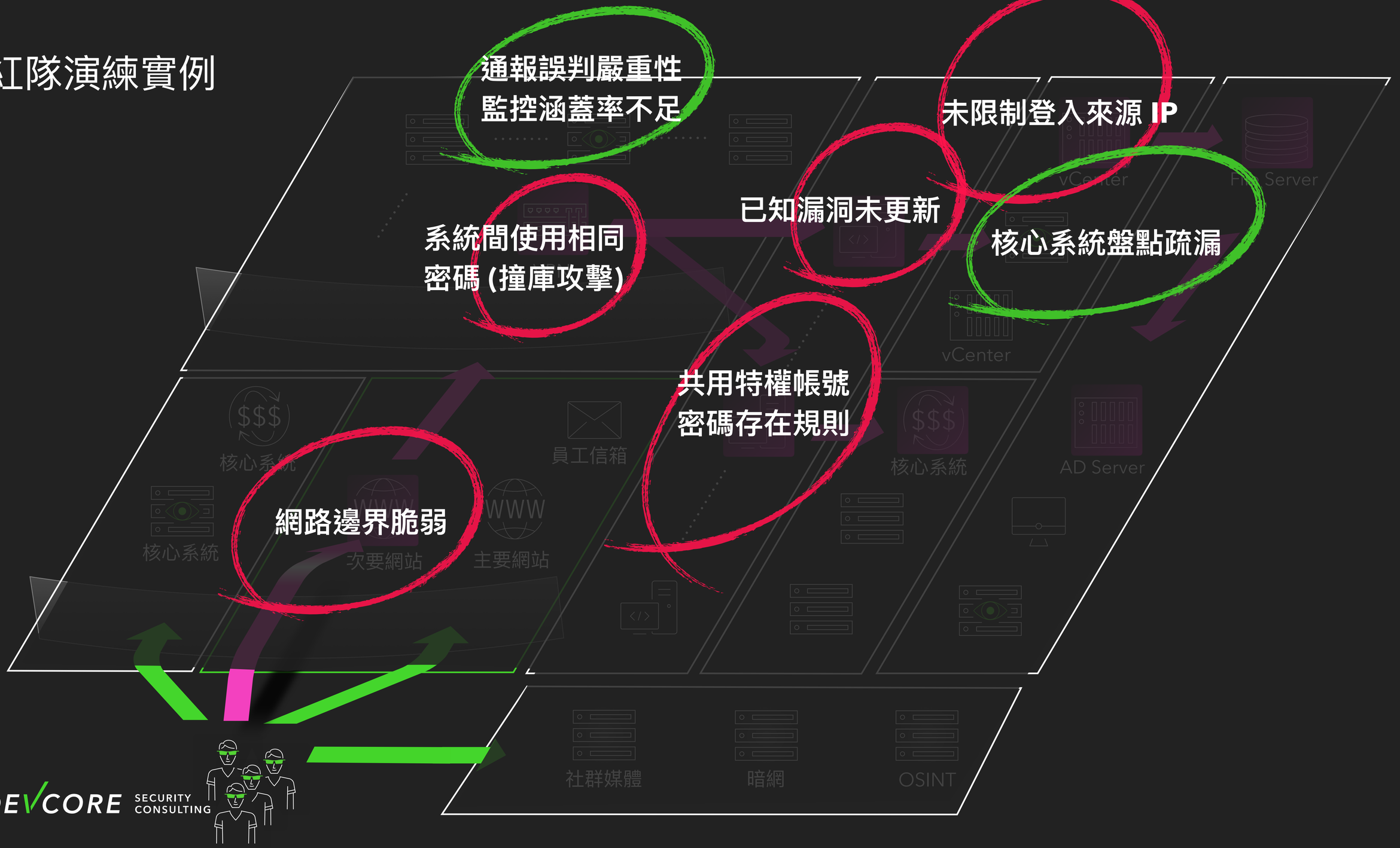


紅隊演練實例



DEVCORE SECURITY CONSULTING

紅隊演練實例



DEVCORE SECURITY CONSULTING

演練發現 vs. ISO 27001

不同系統使用相同帳號密碼
A.9.4.3 通行碼管理系統

VPN 網段存取內部系統
A.13.1.3 網路區隔

核心系統盤點疏漏
4.3 決定 ISMS 範圍

未限制來源 IP
A.9.4.1
系統存取限制

僅 1/4 具備監控資料
4.2 關注方之需要與期望

次要網站防護不足
A.14.1.1 資訊安全
要求事項分析及規格

通報嚴重度偏低
A.16.1.4
資安事件評估及決策

管理帳號使用存在
密碼規則
A.9.4.3
通行碼管理系統

AD 重大漏洞未修補
A.12.6.1
技術脆弱性管理

DEVCORE SECURITY CONSULTING

若資安事件發生，建議流程：

- 制定、檢視、修正事件應變計畫
- 組織內部及外部規範對應處置（ISMS等）
- 立刻通知客戶、相關單位、主管機關
  - 說明目前情況、損失、影響、企業處置、客戶後續該做什麼處理
- 了解相關法規，通知律師並協調法律策略
- 媒體公關處理
- 尋找外部事件應變團隊
- 風險管控（如資安險）
- 警調報案

DEVCORE
SECURITY
CONSULTING

感謝聆聽，請多指教！

Q&A

戴夫寇爾股份有限公司
contact@devco.re