DEVCORE
SECURITY
CONSULTING

你看得到我嗎？
以紅隊角度驗證企業偵測機制

翁浩正 (Allen Own)

戴夫寇爾股份有限公司

allenown@devco.re

2019.10.25 iThome CYBERSEC101

擴大資安視野 精進資安防禦

DEVCORE SECURITY CONSULTING

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

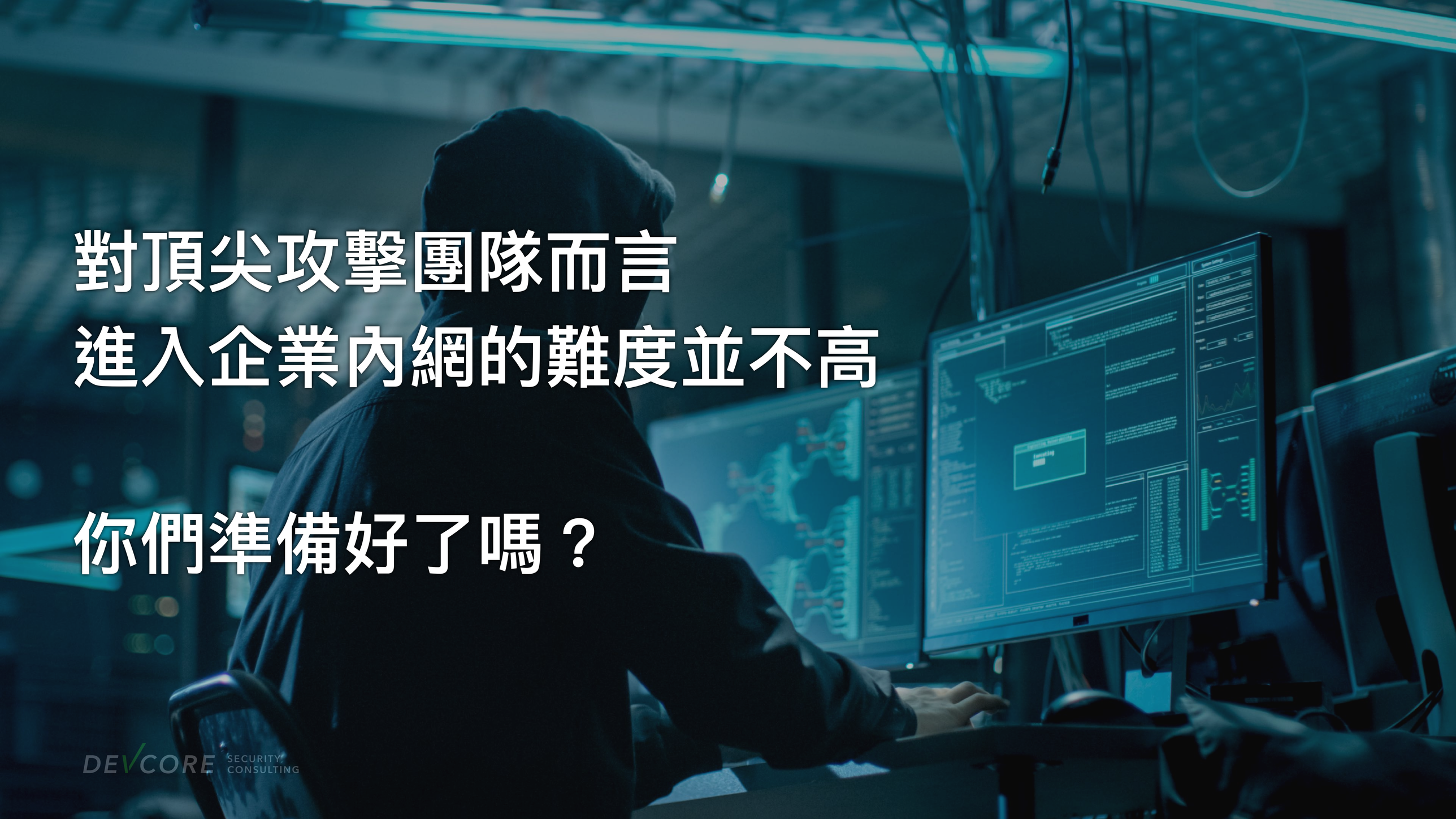
DEVCORE SECURITY CONSULTING

作為紅隊演練的領導廠商，我們自 2017 年至今

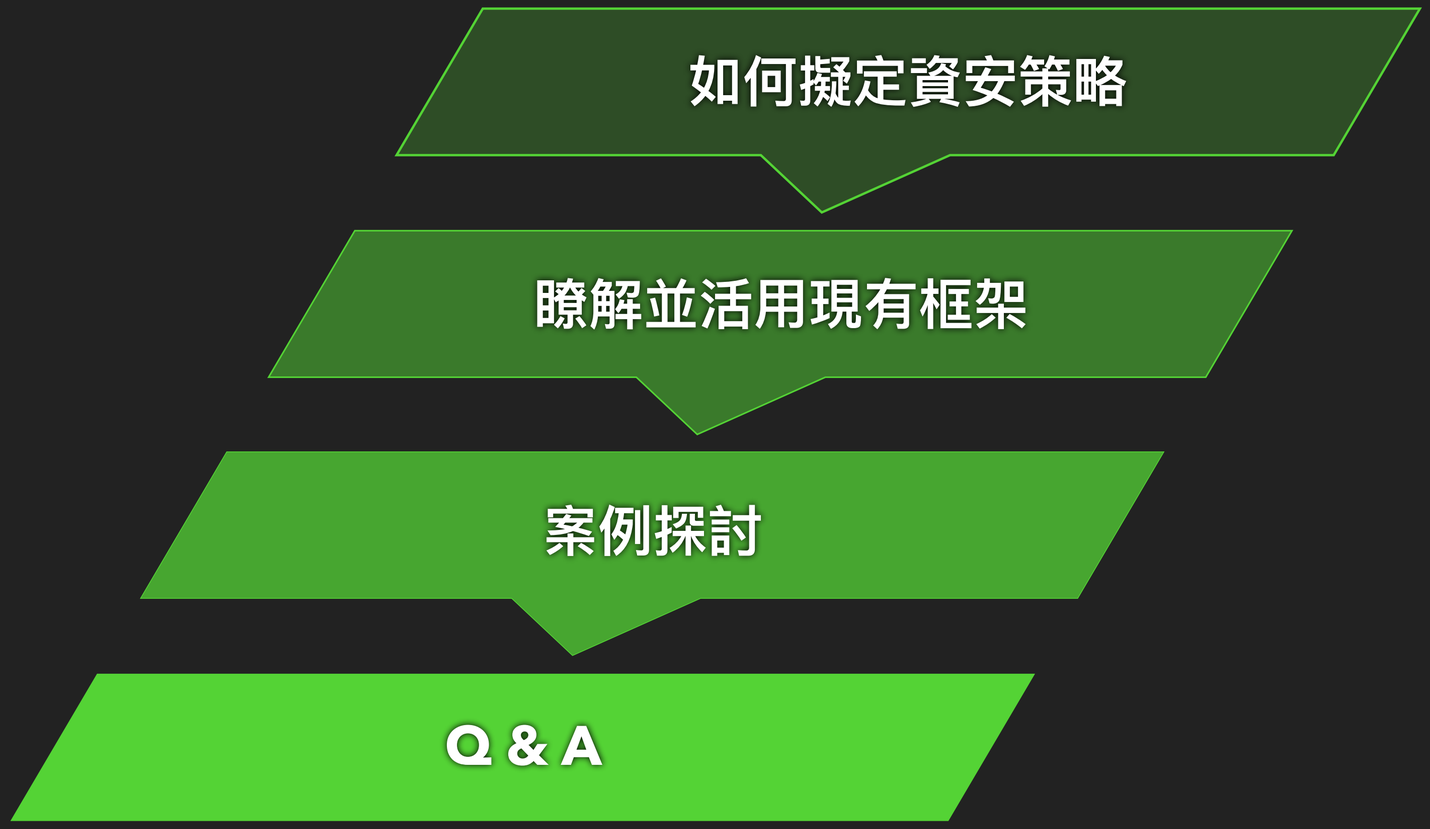
進入台灣企業內網成功率： 100%

超過六成演練案拿到 AD

（部分企業未使用 AD 管理）

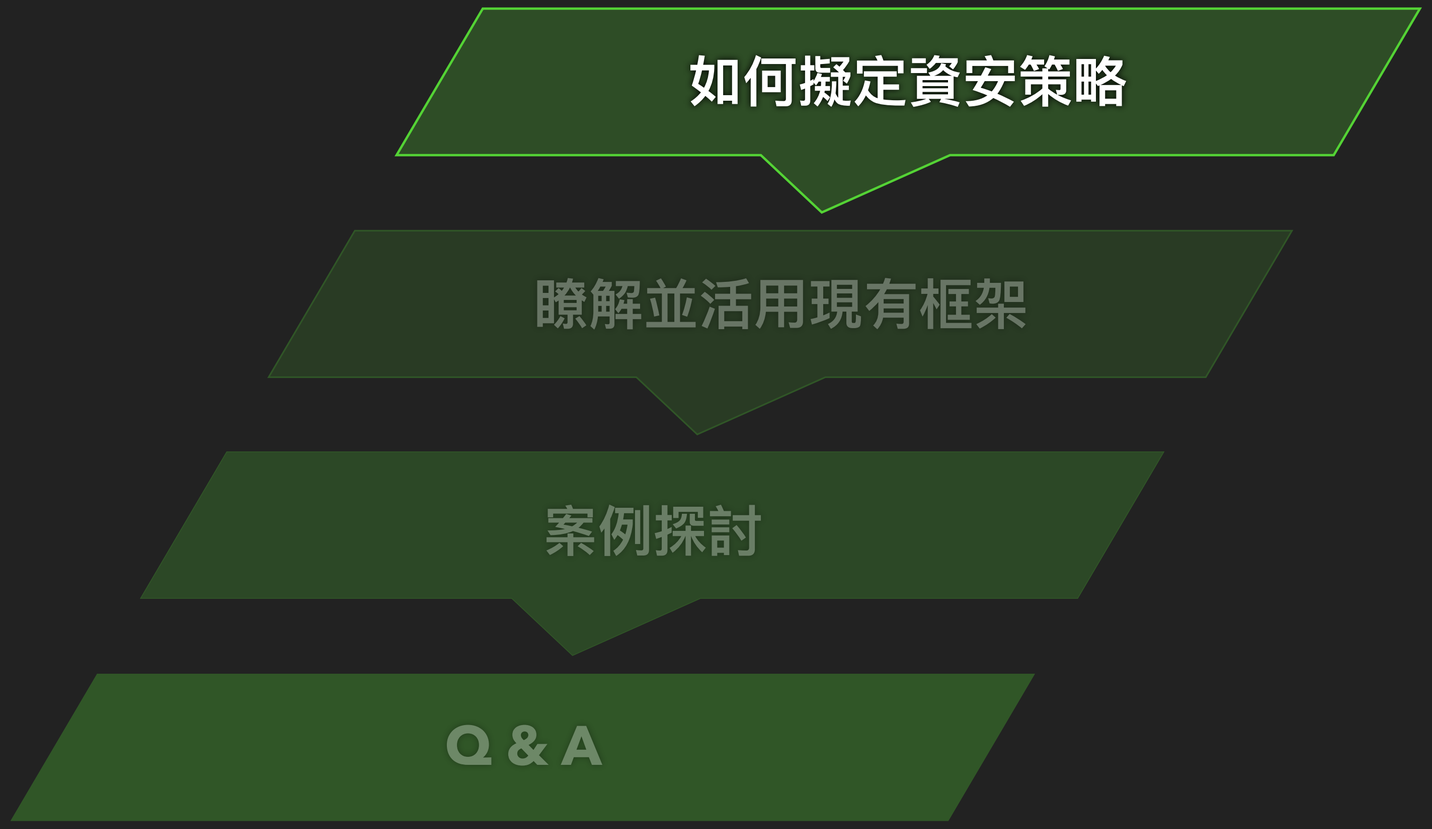

對頂尖攻擊團隊而言
進入企業內網的難度並不高
你們準備好了嗎？
DEVCORE
SECURITY
CONSULTING

你看得到我嗎？以紅隊角度驗證企業偵測機制



你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ 資安的目標到底是什麼
- ✓ 安全策略的層次
- ✓ 意識、策略、控制
- ✓ 常見增強資安的方案

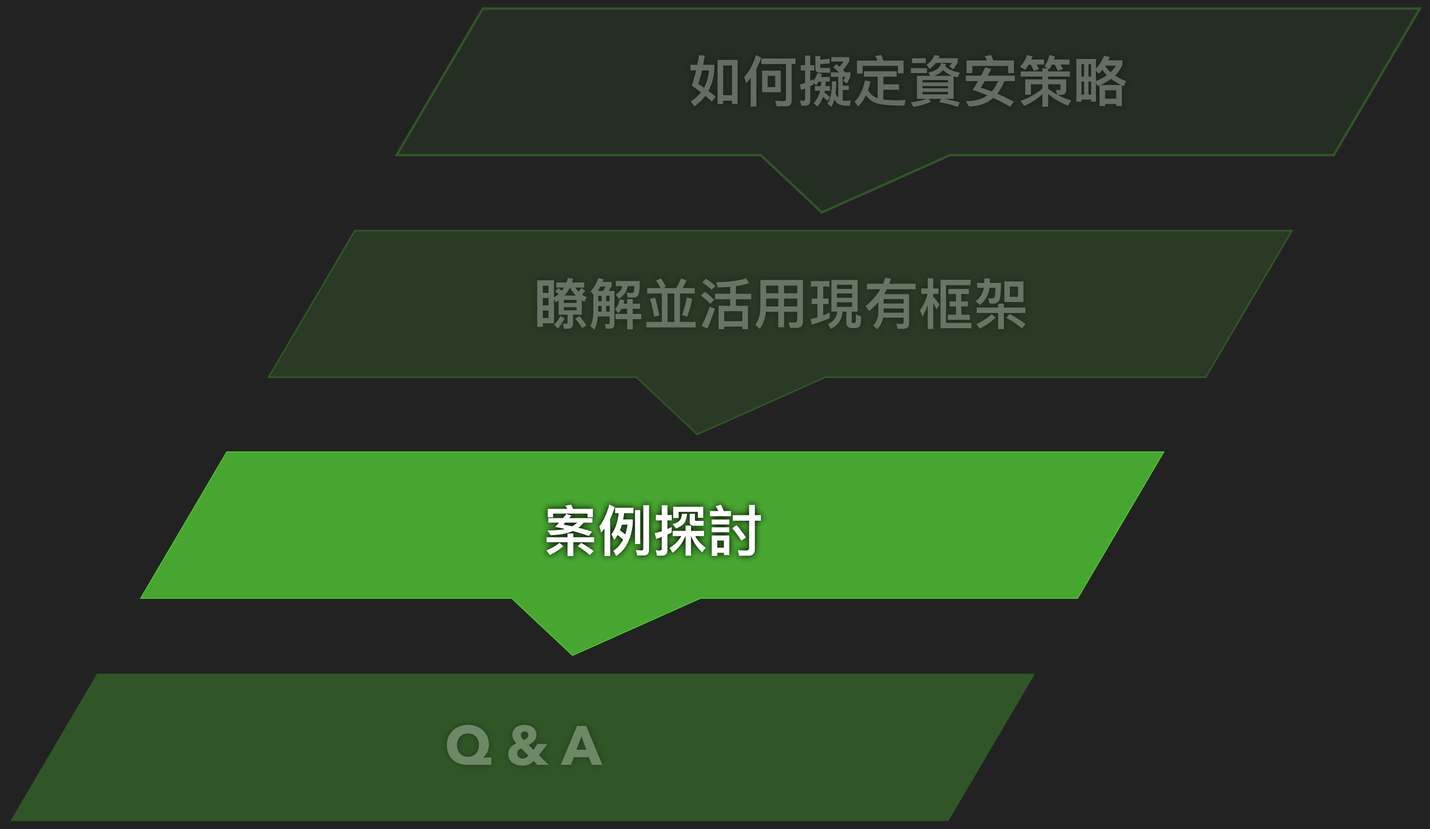


你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ NIST Cybersecurity Framework
- ✓ DETECT 介紹及子項目探討
- ✓ MITRE ATT&CK Framework
- ✓ CREST Cyber Security Incident Response Guide

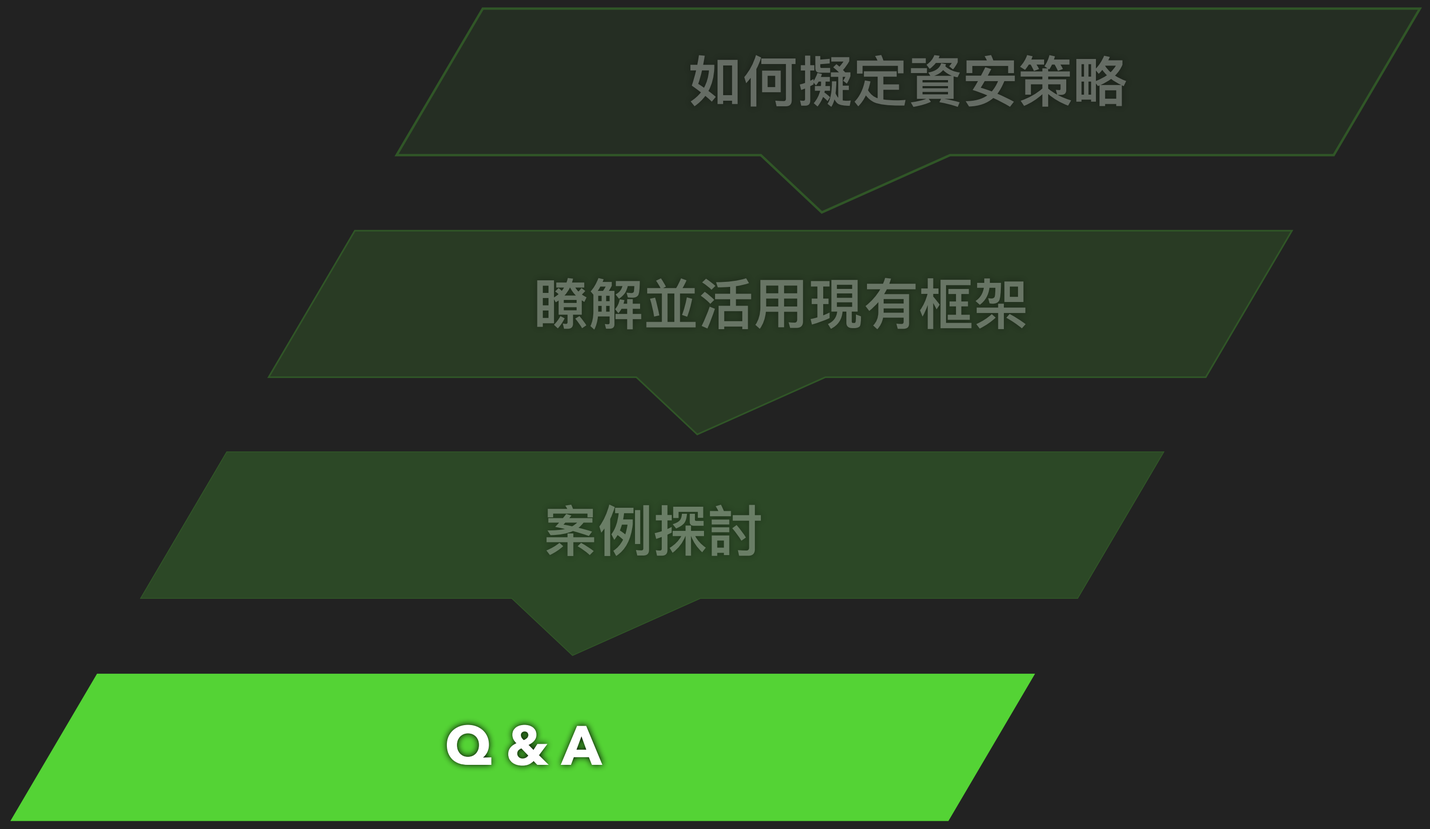
你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ 透過案例瞭解偵測機制
- ✓ 探討真實資安事件
- ✓ 探討紅隊演練案例



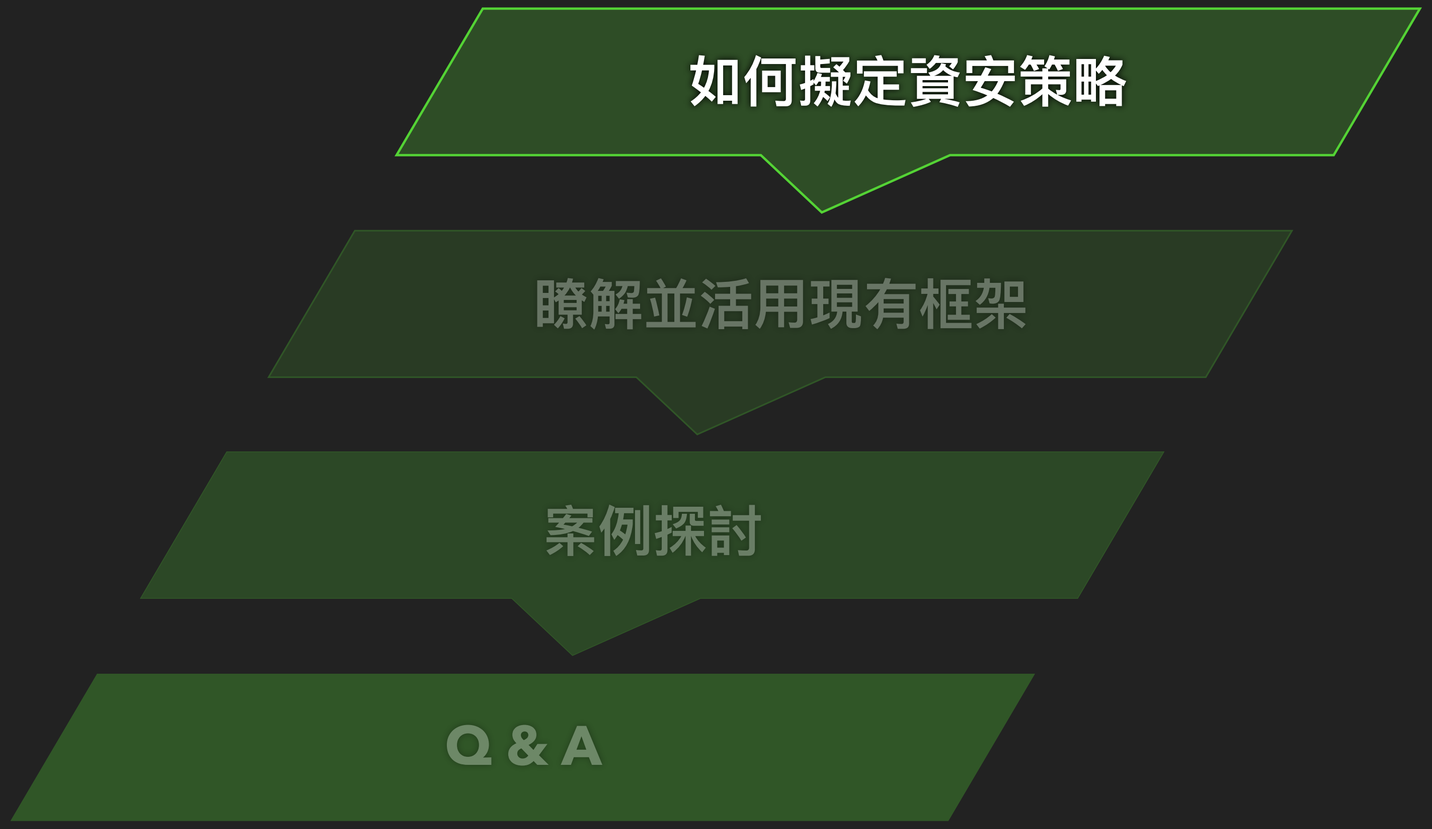
DEVCORE SECURITY CONSULTING

你看得到我嗎？以紅隊角度驗證企業偵測機制



你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ 資安的目標到底是什麼
- ✓ 安全策略的層次
- ✓ 意識、策略、控制
- ✓ 常見增強資安的方案



在討論資安的時候，我們真正的目標是什麼？

在討論資安的時候，我們真正的目標是什麼？

期望我們能夠「安全」！

怎麼評估自己安不安全？
別被商業話術牽著走！

EPS 多少？阻擋多少攻擊？花多少錢？
還是多久能回應一個資安事件？

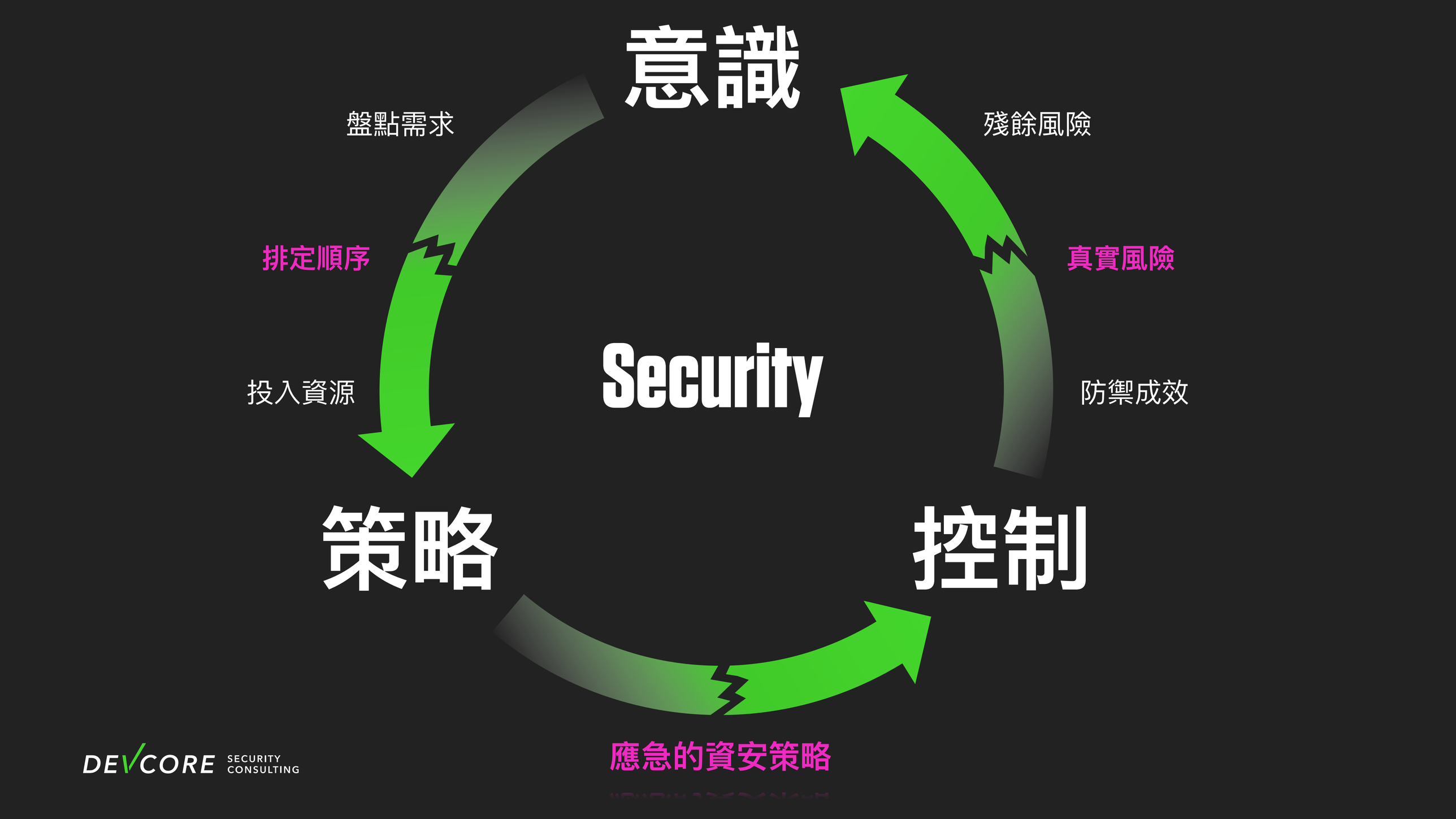
安全層次 (Security Level)

	測試方式	優點	缺點
真實的安全	資安事件 紅隊演練	最大化發現可能的問題 (設備組態、人員疏失、管理制度)	發現問題涵蓋範圍可能過廣， 缺乏提出一步到位的解決方案
潛在攻擊者的威脅	紅隊演練	針對特定攻擊類型 優先選擇對應措施，節省資源	不易辨識出攻擊者族群及手法
過去事件驗證過的安全	資安事件	真實性高 可能驗證設備、系統、管理及維運狀況	不容易掌握全貌 不容易重現攻擊
設備及系統安全	BAS、PT、VA	成本相對較低 可以驗證設備或服務投資效益	單點安全無法反映組織全貌 不易呈現漏洞組合利用
組織管理及維運安全	ISO、Framework	標準化、容易實作 提供基礎安全指引	不易反映真實威脅

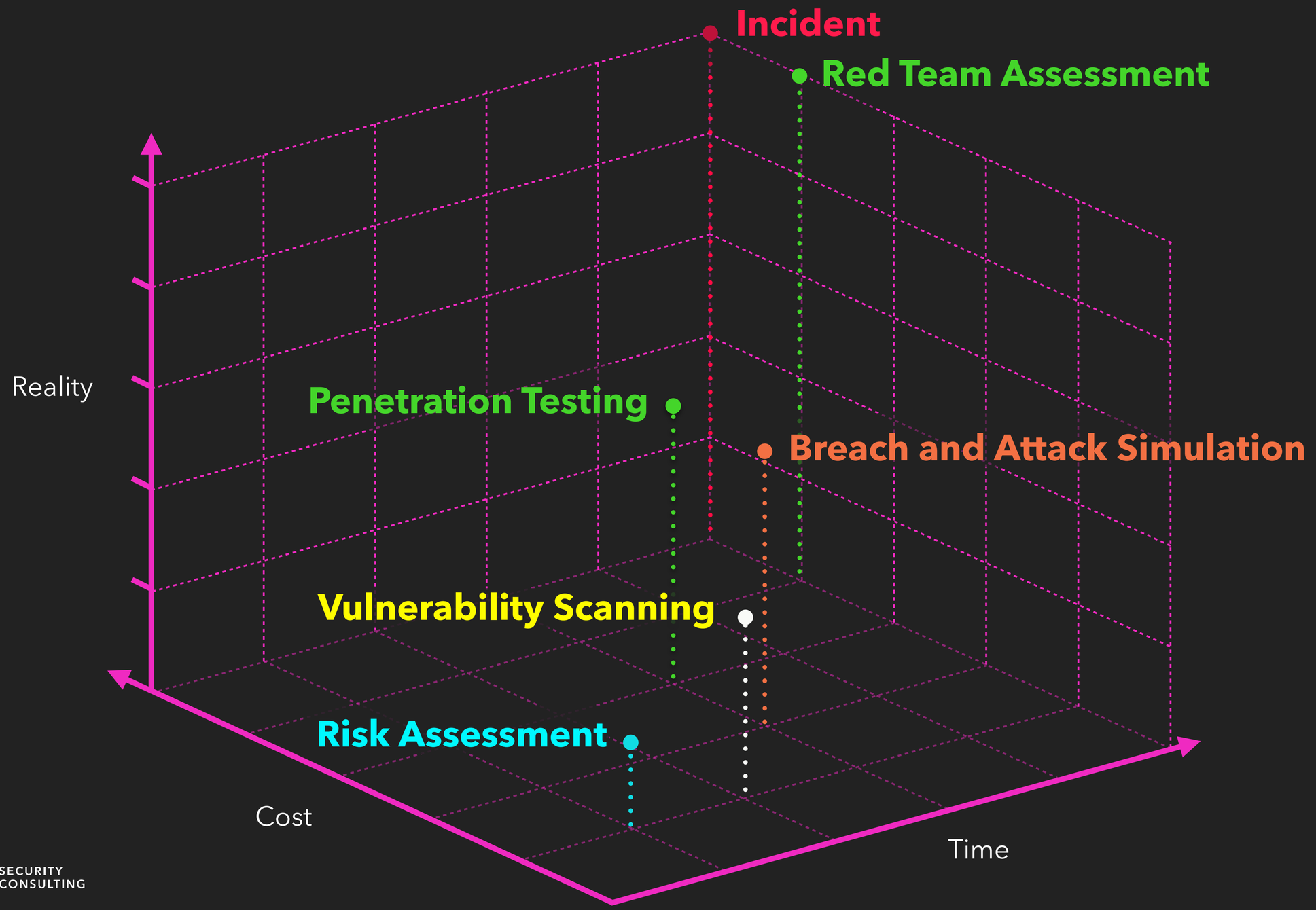
安全層次 (Security Level)

	測試方式	優點	缺點
真實的安全	資安事件 紅隊演練	最大化發現可能的問題 (設備組態、人員疏失、管理制度)	發現問題涵蓋範圍可能過廣， 缺乏提出一步到位的解決方案
潛在攻擊者的威脅	紅隊演練	針對特定攻擊類型 優先選擇對應措施，節省資源	不易辨識出攻擊者族群及手法
過去事件驗證過的安全	資安事件	真實性高 可能驗證設備、系統、管理及維運狀況	不容易掌握全貌 不容易重現攻擊
設備及系統安全	BAS、PT、VA	成本相對較低 可以驗證設備或服務投資效益	單點安全無法反映組織全貌 不易呈現漏洞組合利用
組織管理及維運安全	ISO、Framework	標準化、容易實作 提供基礎安全指引	不易反映真實威脅

DEVCORE SECURITY CONSULTING



DEVCORE SECURITY CONSULTING



DEVCORE SECURITY CONSULTING

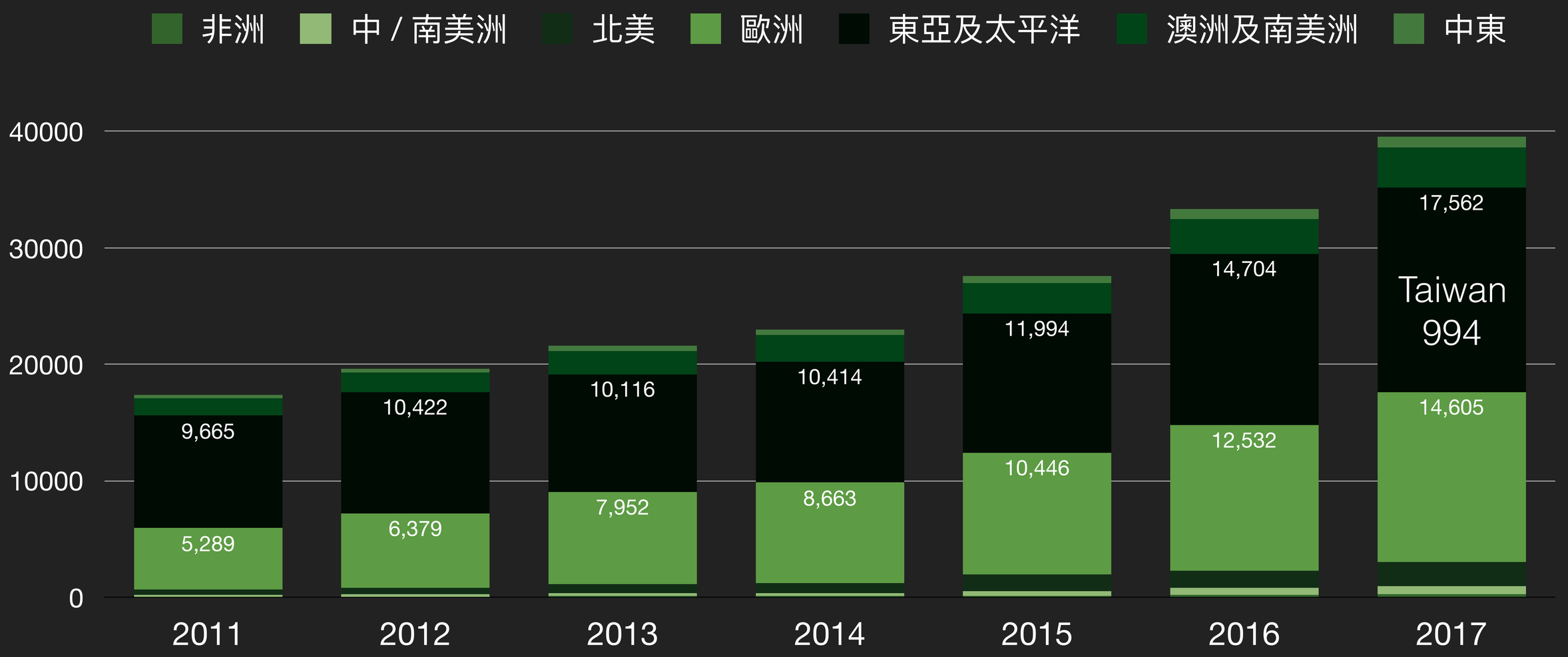
你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ NIST Cybersecurity Framework
- ✓ DETECT 介紹及子項目探討
- ✓ MITRE ATT&CK Framework
- ✓ CREST Cyber Security Incident Response Guide

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

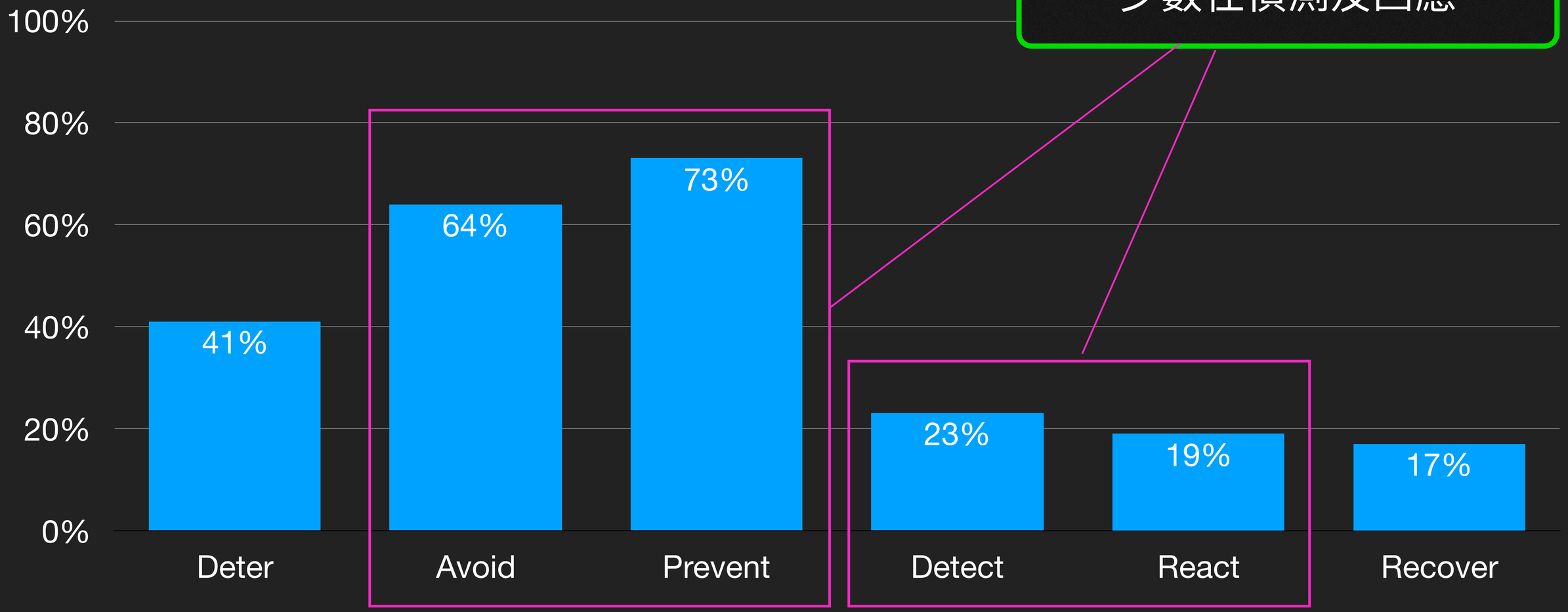


DEVCORE SECURITY CONSULTING

Source: http://www.iso27001security.com

框架特性

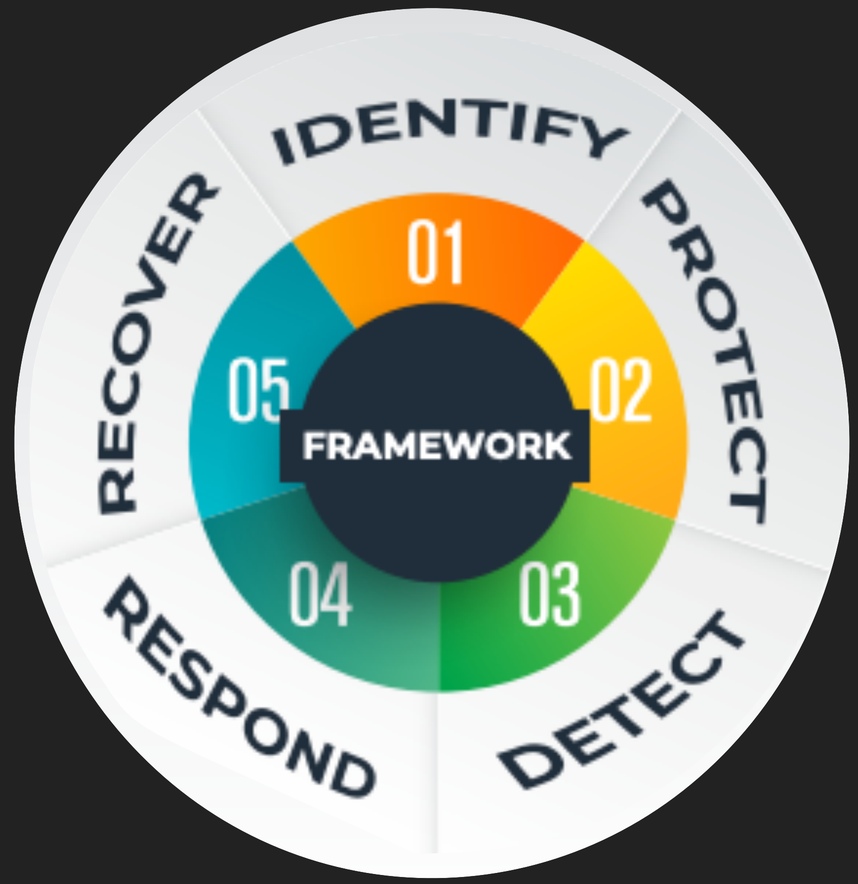
主要集中在避免及預防
少數在偵測及回應



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



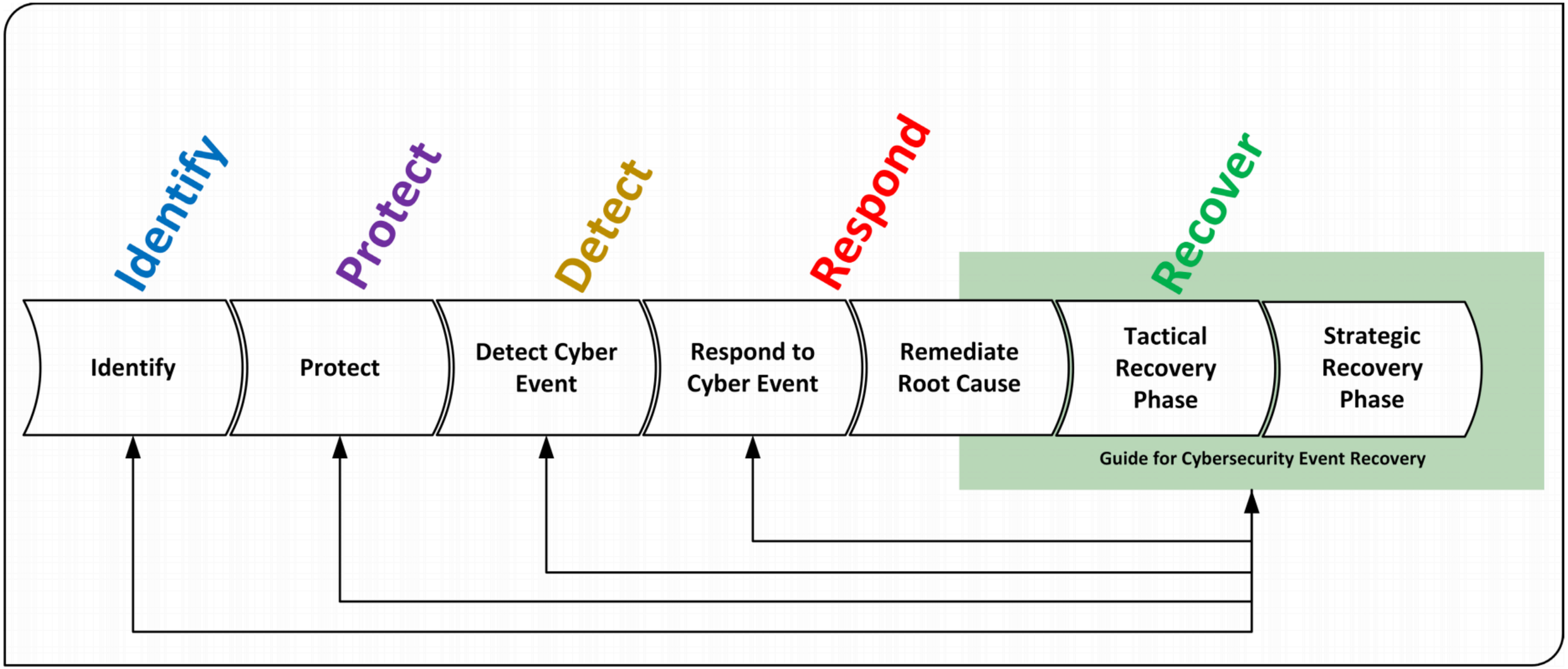


Figure 3-1: NIST SP 800-184 Guide for Cybersecurity Event Recovery Relationship with the NIST CSF

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)

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

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)

- DE 談的其實是驗證系統跟資產，在保護措施、流程、跟程序的有效性。
- 核心有兩個：
  - 第一：要驗證的是哪些系統跟資產 (屬於 IDENTITY)
    第二：前述的有效性
- 我們將用紅隊演練的案例來說明以上兩項核心

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
	DE.AE-2: Detected events are analyzed to understand attack targets and methods
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors
	DE.AE-4: Impact of events is determined
	DE.AE-5: Incident alert thresholds are established
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
	DE.CM-4: Malicious code is detected
	DE.CM-5: Unauthorized mobile code is detected
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
	DE.CM-8: Vulnerability scans are performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
	DE.DP-2: Detection activities comply with all applicable requirements
	DE.DP-3: Detection processes are tested
	DE.DP-4: Event detection information is communicated
	DE.DP-5: Detection processes are continuously improved

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A **baseline** of network operations and expected data flows for users and systems is established and managed
	DE.AE-2: Detected events are **analyzed** to understand **attack targets and methods**
	DE.AE-3: Event data are **collected and correlated** from multiple sources and sensors
	DE.AE-4: Impact of events is determined
	DE.AE-5: Incident alert thresholds are established
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The **network** is **monitored** to detect **potential cybersecurity events**
	DE.CM-2: The **physical** environment is **monitored** to detect **potential cybersecurity events**
	DE.CM-3: Personnel activity is monitored to detect **potential cybersecurity events**
	DE.CM-4: Malicious code is detected
	DE.CM-5: Unauthorized mobile code is detected
	DE.CM-6: External service provider activity is monitored to detect **potential cybersecurity events**
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
	DE.CM-8: Vulnerability scans are performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1: Roles and responsibilities** for detection are well defined to ensure **accountability**
	DE.DP-2: Detection activities comply with all applicable requirements
	DE.DP-3: Detection processes are tested
	DE.DP-4: Event detection information is communicated
	DE.DP-5: Detection processes are **continuously improved**

Subcategory - 值得注意討論的項目

- DE.AE-2: Detected events are analyzed to understand attack targets and methods
- DE.AE-3: Event data are collected and correlated from multiple sources and sensors
- DE.AE-4: Impact of events is determined
- DE.CM-1: The network is monitored to detect potential cybersecurity events
- DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
- DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
- DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
- DE.DP-3: Detection processes are tested
- DE.DP-5: Detection processes are continuously improved

DE.AE-2: Detected events are analyzed to understand attack targets and methods

- 透過系統記錄或者系統分析已經偵測到的事件
- 重點：判讀攻擊目標以及手法
- 是較為困難的部分，通常事件的分析需要比較多經驗。建議先求記錄完整，當事件發生時可以透過記錄與委外團隊合作調查

DE.AE-3: Event data are collected and correlated from multiple sources and sensors

- 從各種不同設備及伺服器蒐集事件資料，並進行關連
- 需要評估 event 量的大小，是否能夠收容足夠長的時間
- **Event 絕不是多就好，要避免過度誤報，避免讓維運人員習慣性忽略 event**

DE.AE-4: Impact of events is determined

- 確認事件的實際影響及危害
- 事件影響判讀時切勿過度樂觀理想化，應以最大損失進行評估
- 透過事件後的分析回顧，重新調整資安策略、風險評估

DE.CM-1: The network is monitored to detect potential cybersecurity events

- 怎麼定義 potential cybersecurity events ?
- 有足夠的資料進行分析
- 透過平時正常的流量，分析出異常的流量
- 透過公司內部以及外部情資搜尋潛在威脅

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

- 哪些人的行為需要被特別注意，通常也是網軍/紅隊演練攻擊的目標。
- 如何監控這些人的行為
- 如何讓中高階長官也配合

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

- 通常也是外部情蒐後，可以打進內網的偵查動作。
- 供應鍊、雲端服務都是需要監控的對象

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

- 盤點究竟有哪些地方需要監控
- 怎麼監控、怎麼通知、誰來處理、有無可能自動化
- 案例：原本系統會監控異常的使用者登入行為，但服務的異常行為卻忘了監控。

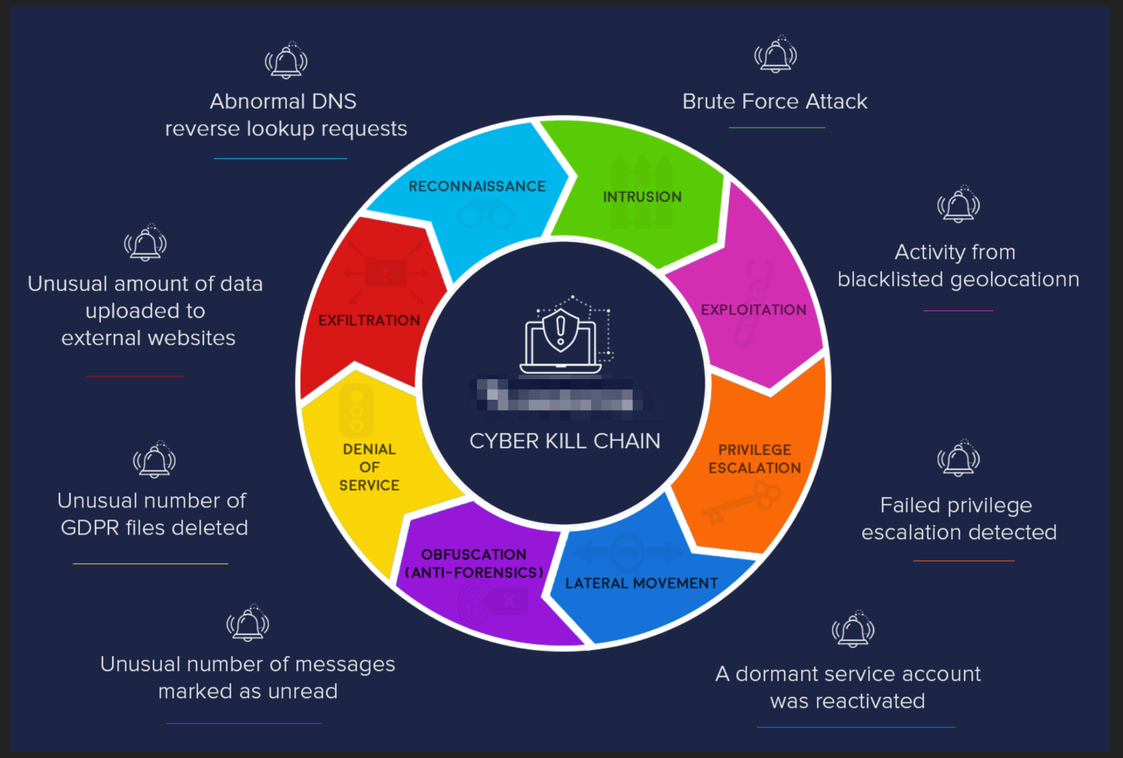
DE.DP-3: Detection processes are tested

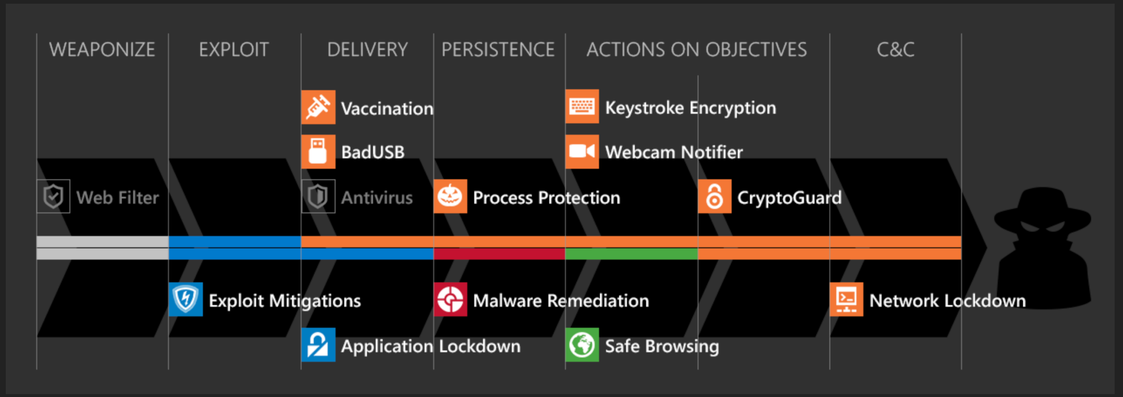
DE.DP-5: Detection processes are continuously improved

- SOC 等監控機制是否有經過測試？
- 範圍是否足夠、設備的誤判是否存在？
- 機制在正常實施之後，有無觸發過事件？可以怎麼改善

MITRE **ATT&CK** Enterprise Framework

- **A**dversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge
- 全球公開、免費的攻擊者戰術與技術的通用資料庫
- 基於觀察真實世界攻擊者行為
- 將入侵流程的描述標準化
- 可協助紅隊演練模擬敵方、威脅情資評估防禦成效等
- https://attack.mitre.org/





DEVCORE SECURITY CONSULTING

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

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

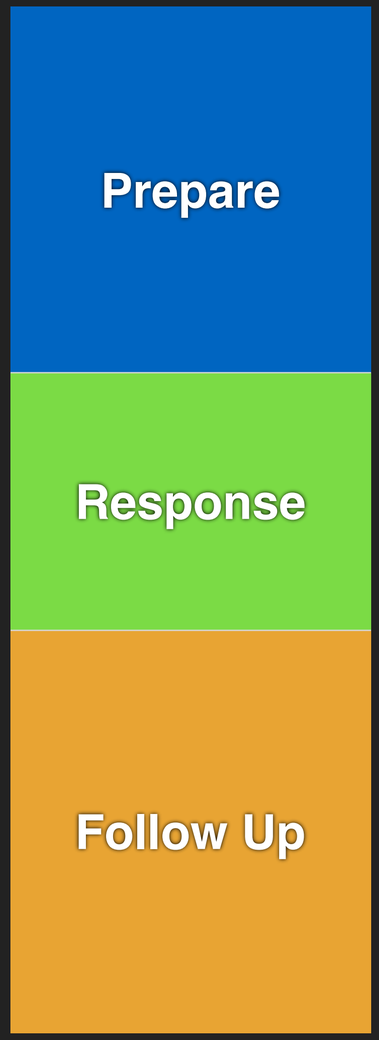
- **Step 1.** Identify cyber security incident
- **Step 2.** Define objectives and investigate situation
- **Step 3.** Take appropriate action
- **Step 4.** Recover systems, data and connectivity

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

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

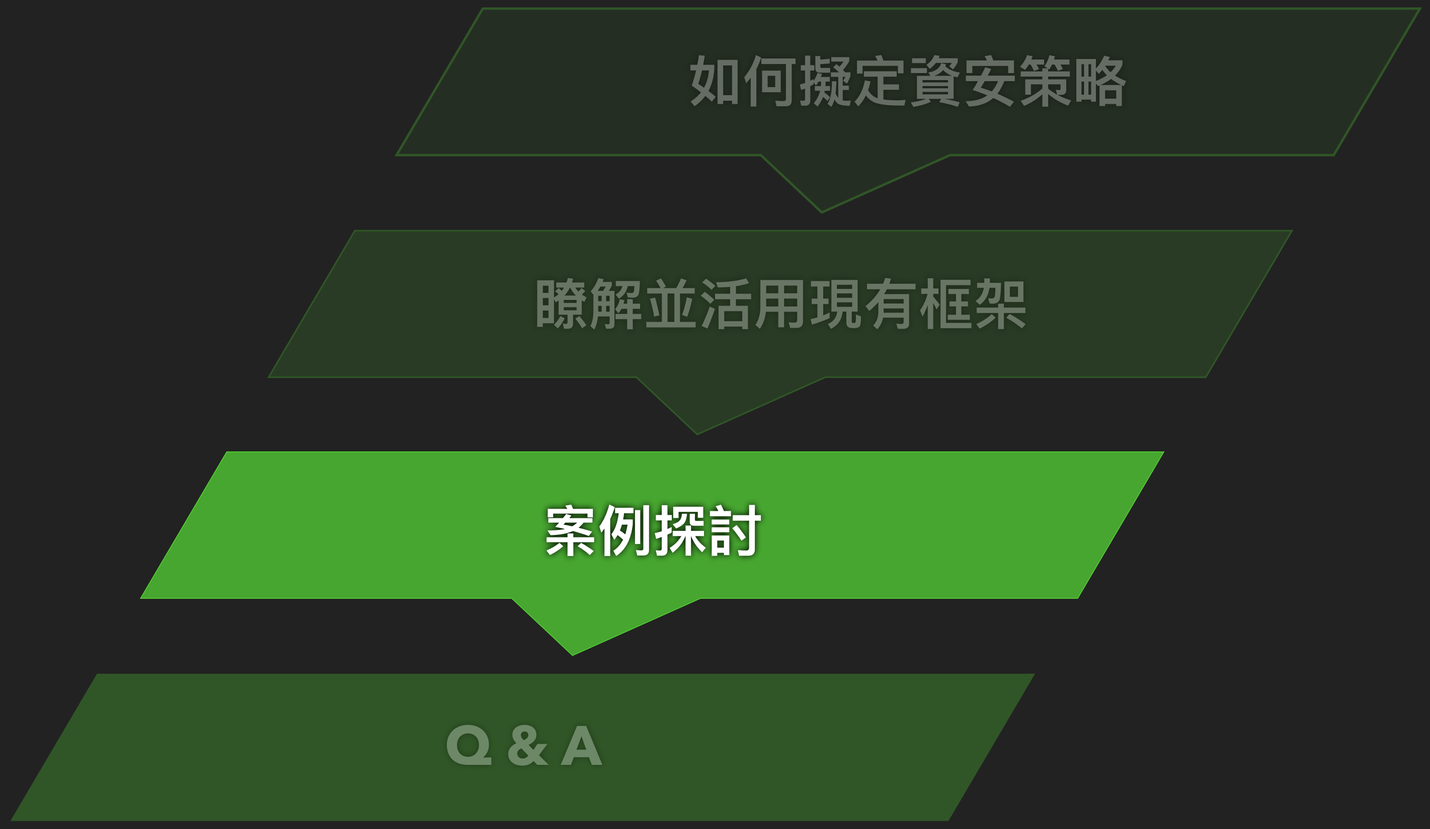
Step 1. Identify cyber security incident
Step 2. Define objectives and investigate situation
Step 3. Take appropriate action
Step 4. Recover systems, data and connectivity

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

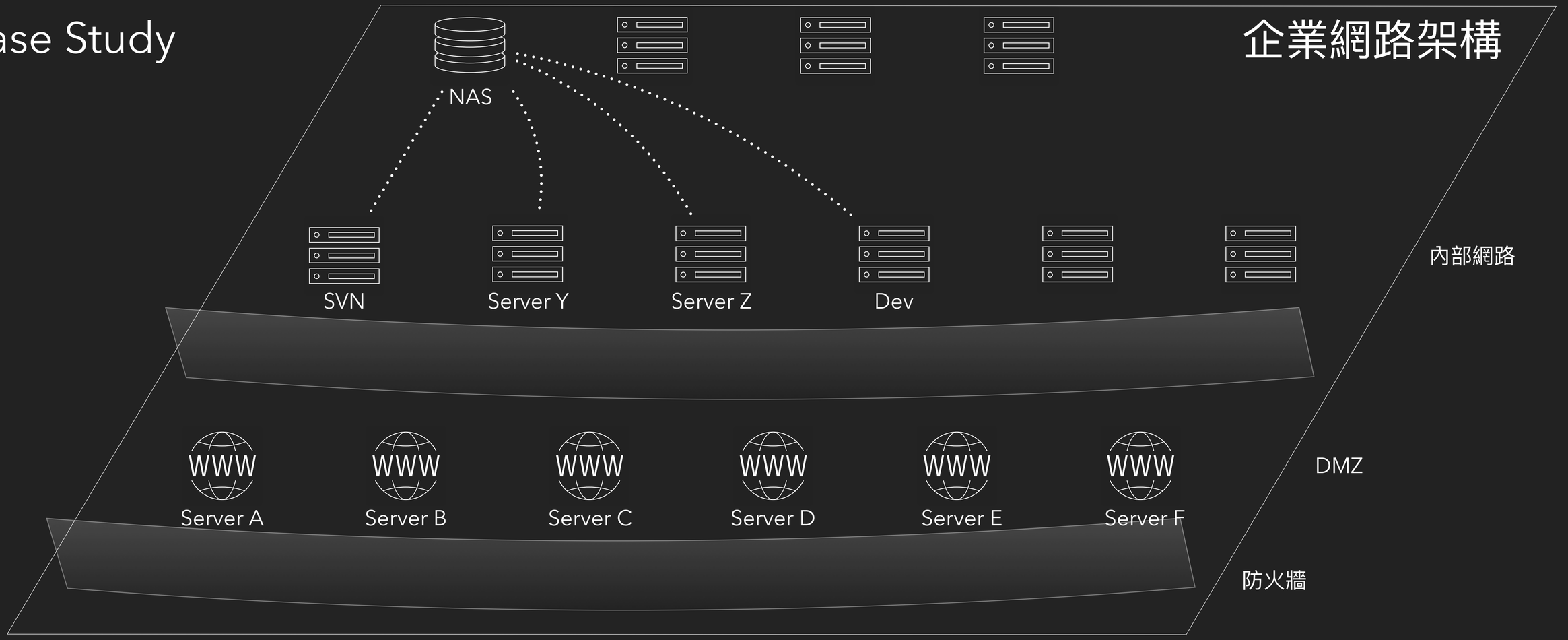
你看得到我嗎？以紅隊角度驗證企業偵測機制

- ✓ 透過案例瞭解偵測機制
- ✓ 探討真實資安事件
- ✓ 探討紅隊演練案例



DEVCORE SECURITY CONSULTING

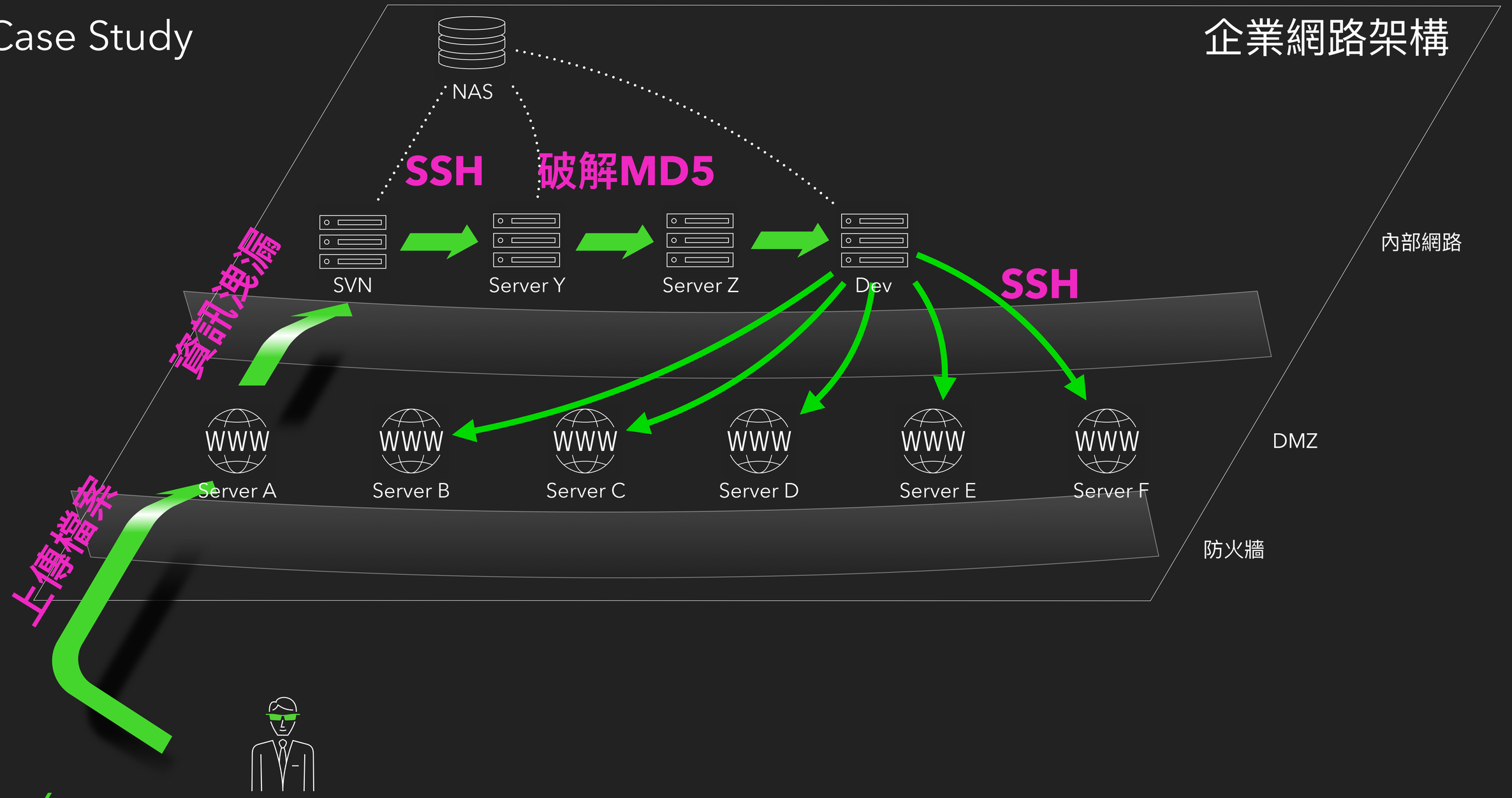
Case Study



DEVCORE SECURITY CONSULTING

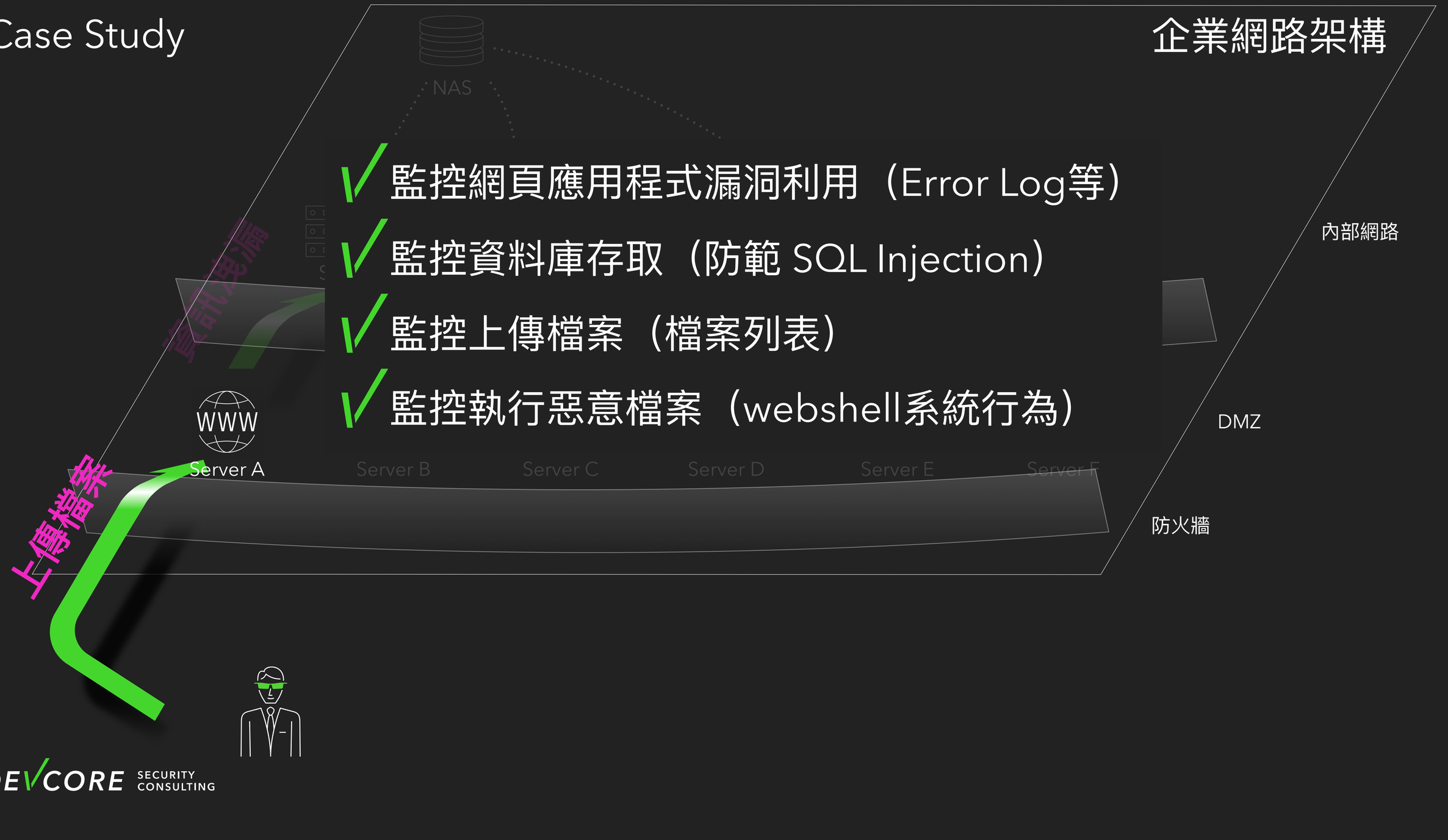
Case Study

企業網路架構



DEVCORE SECURITY CONSULTING

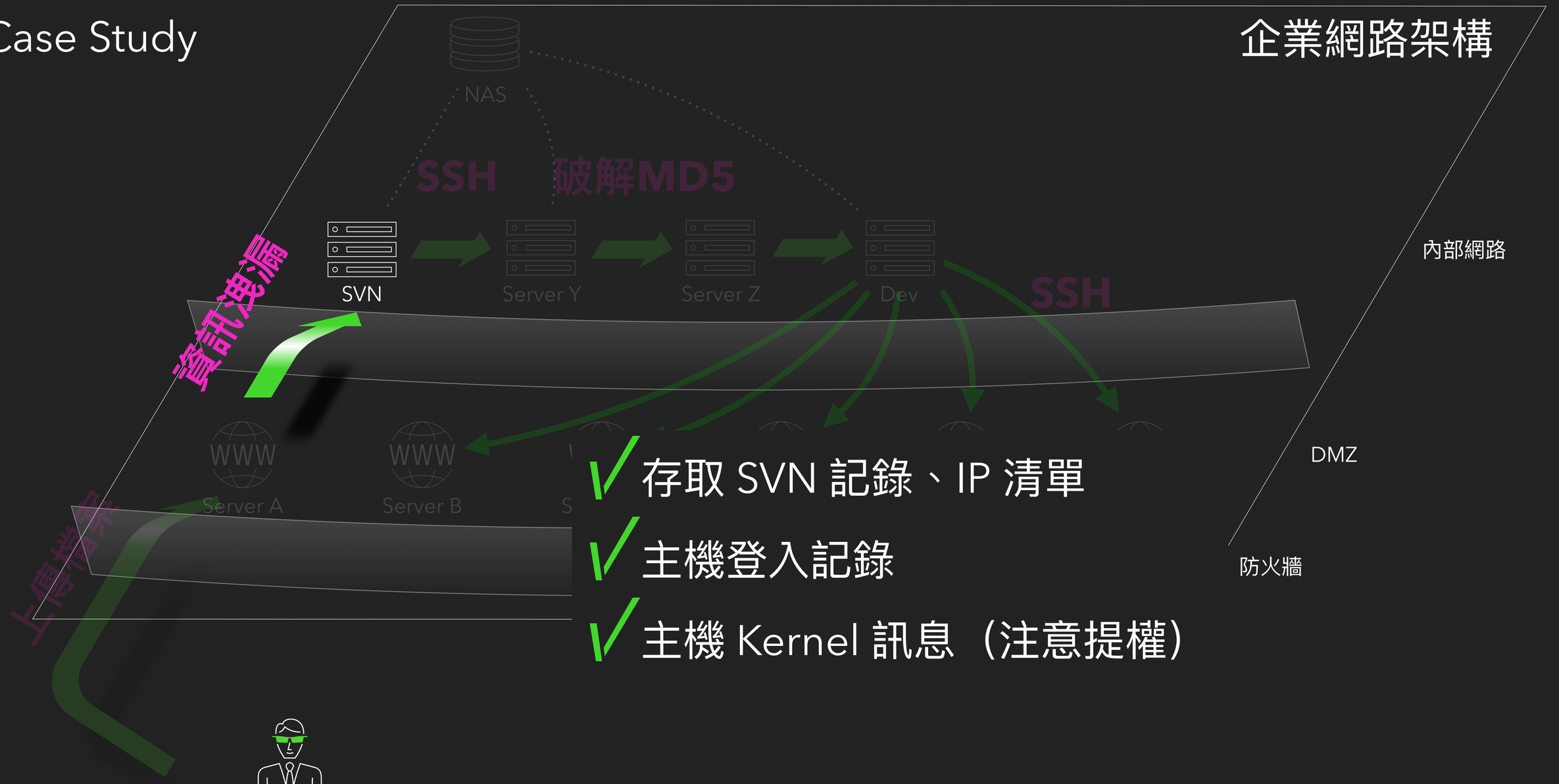
Case Study



DEVCORE SECURITY CONSULTING

Case Study

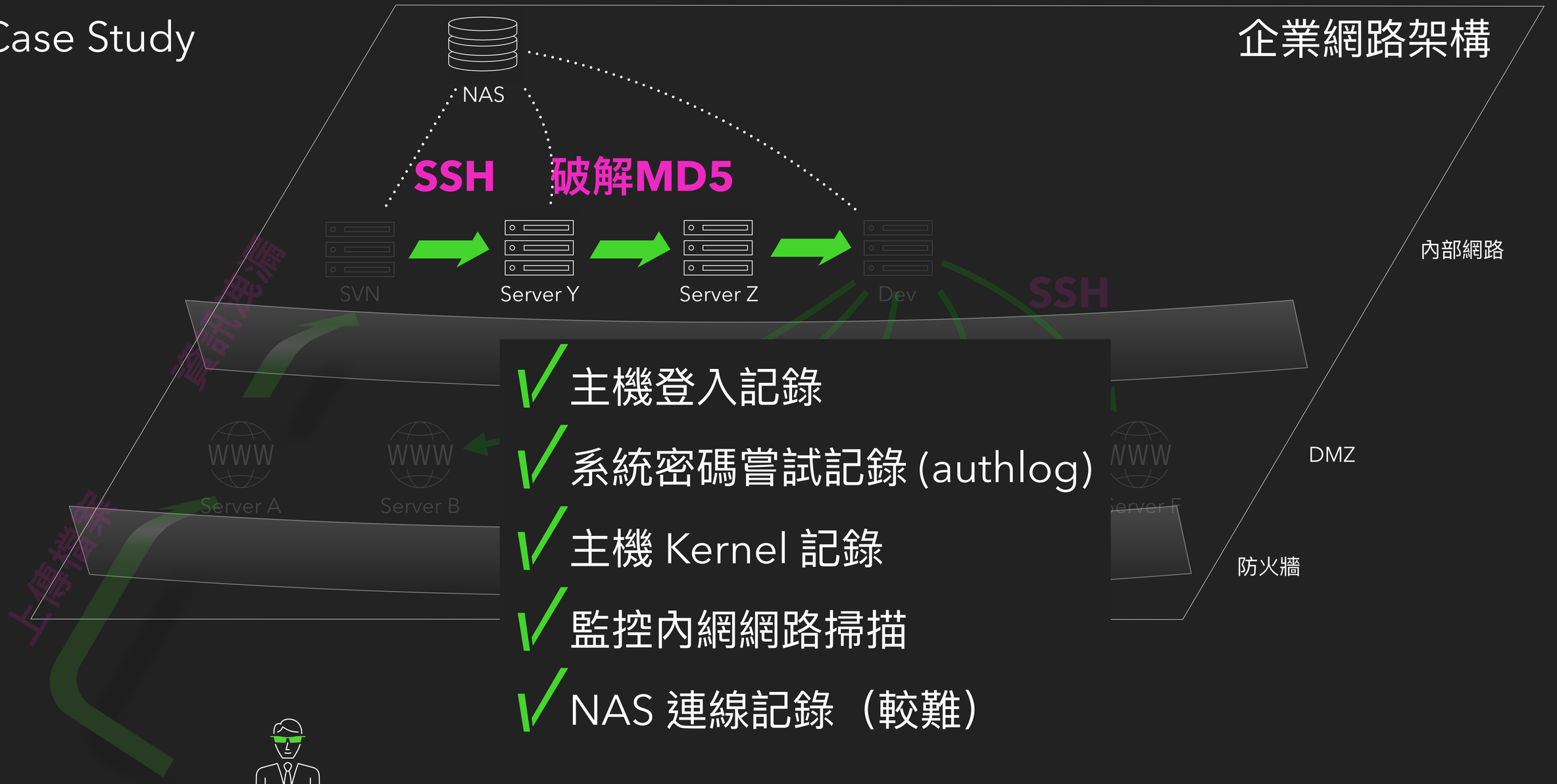
企業網路架構



- ✓ 存取 SVN 記錄、IP 清單
- ✓ 主機登入記錄
- ✓ 主機 Kernel 訊息（注意提權）

DEVCORE SECURITY CONSULTING

Case Study

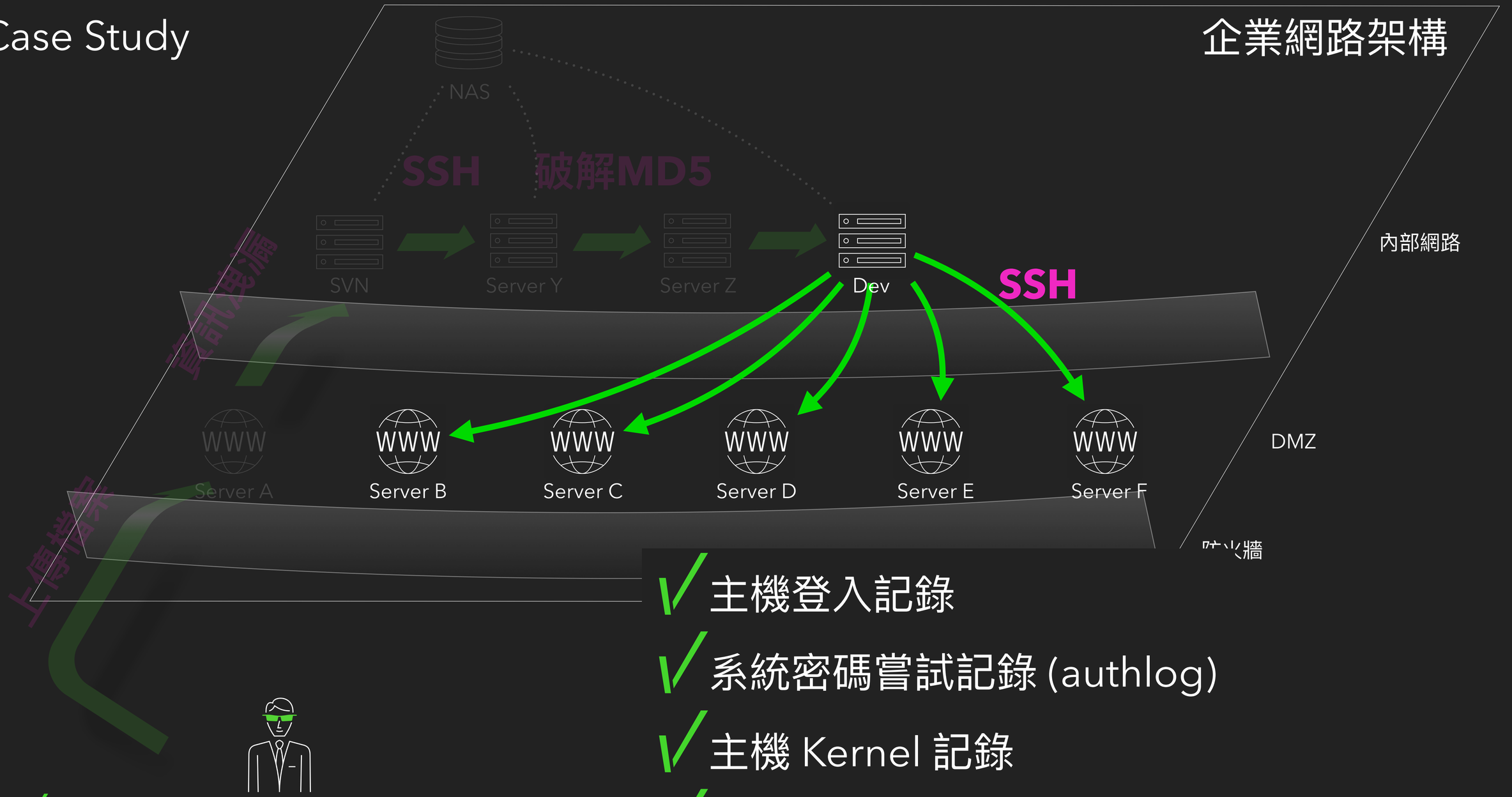


- ✓ 主機登入記錄
- ✓ 系統密碼嘗試記錄 (authlog)
- ✓ 主機 Kernel 記錄
- ✓ 監控內網網路掃描
- ✓ NAS 連線記錄（較難）

DEVCORE SECURITY CONSULTING

Case Study

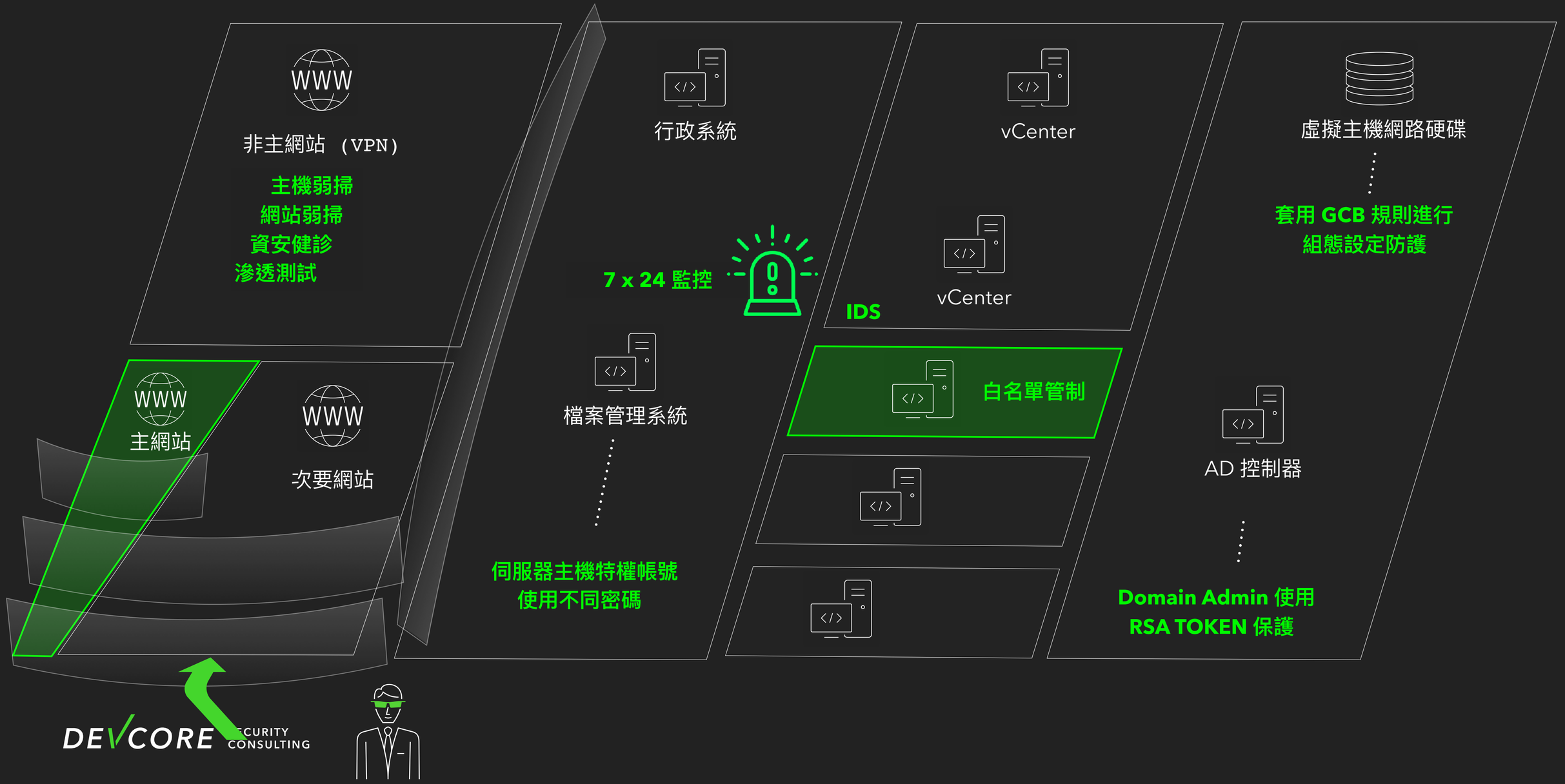
企業網路架構



- ✓ 主機登入記錄
- ✓ 系統密碼嘗試記錄 (authlog)
- ✓ 主機 Kernel 記錄
- ✓ 監控內網網路掃描

DEVCORE SECURITY CONSULTING

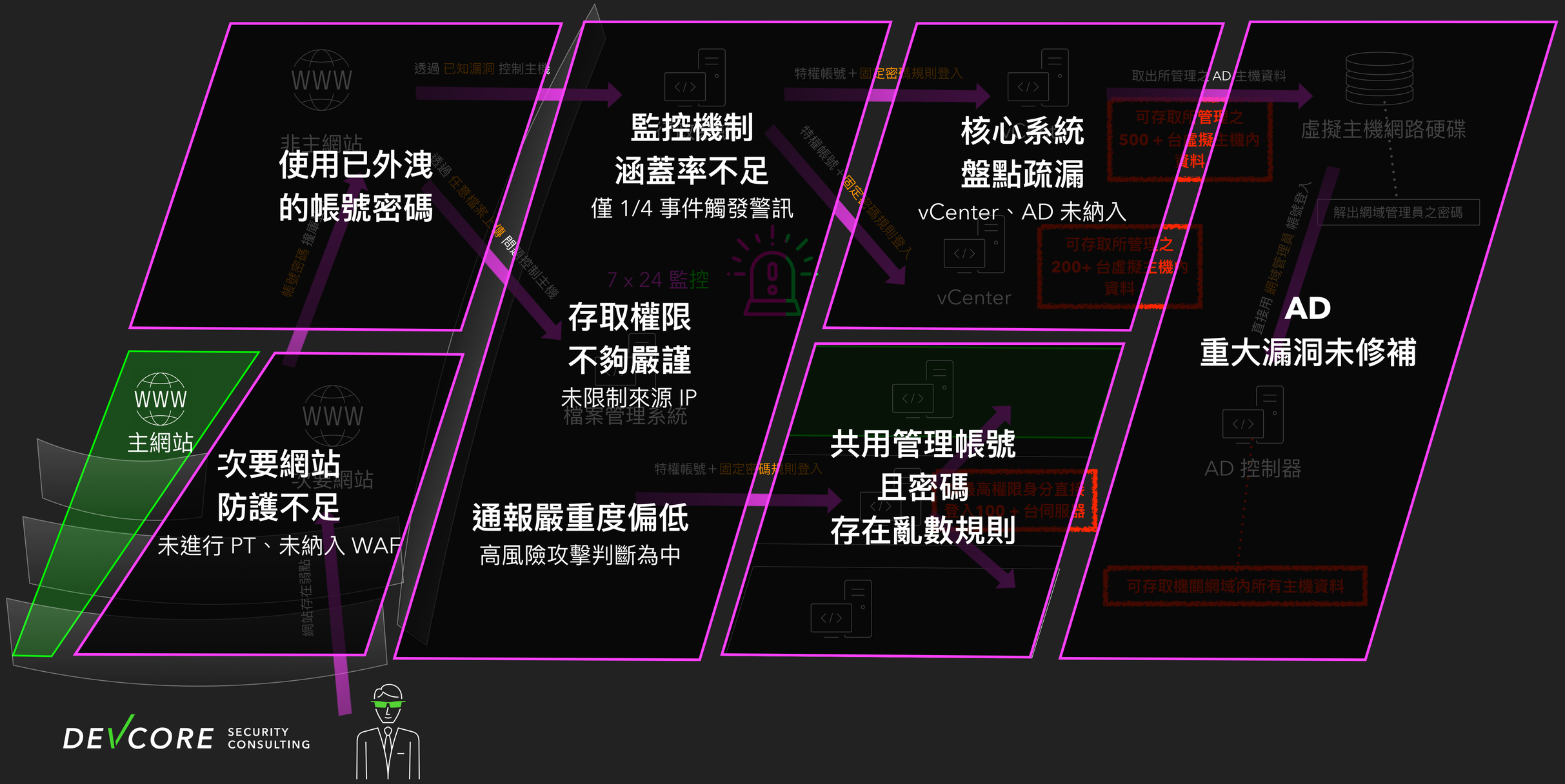
重要資產及防護機制


WWW
非主網站 (VPN)
主機弱掃
網站弱掃
資安健診
滲透測試
WWW
主網站
WWW
次要網站
行政系統
檔案管理系統
伺服器主機特權帳號
使用不同密碼
7 x 24 監控
vCenter
IDS
vCenter
白名單管制
虛擬主機網路硬碟
套用 GCB 規則進行
組態設定防護
AD 控制器
Domain Admin 使用
RSA TOKEN 保護
DEVCORE SECURITY CONSULTING

演練實例

DEVCORE SECURITY CONSULTING

演練發現摘要



DEVCORE SECURITY CONSULTING

演練發現摘要


A.9.4.3
通行碼管理系統
不同系統使用相同帳號密碼
A.13.1.3 網路區隔
VPN 網段存取內部系統
4.2 關注方之需要與期望
僅監控到 1/4 攻擊流量
4.3 決定 ISMS 範圍
可考慮擴大
驗證範圍
A.9.4.1 系統存取限制
重要系統未限制來源 IP
A.14.1.1 資訊安全
要求事項分析及規格
次要網站防護不足
A.9.4.1 系統存取限制
未限制來源 IP
A.16.1.4
資安事件評估及決策
通報嚴重度偏低
A.9.4.3
通行碼管理系統
共用管理帳號
且密碼存在亂數規則
A.12.6.1
技術脆弱性管理
重大漏洞因故無法修補

Bonus: 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

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

Bonus 懶人包: 若發生資安事件，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

Takeaways

- ✓ 參考各種 Framework 建立完整策略及控制措施
- ✓ 安排年度計畫逐步達成完整策略
- ✓ 利用紅隊演練盤點企業策略及控制缺口，並持續改善

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