



# 產業資安威脅議題攻略 產業資安佈署

奧義智慧科技 產品經理 林明緯 Jason



- 經歷

- 奧義智慧產品經理
- 曾任台灣威瑞特技術經理
- 曾任奧義智慧產品經理

- 擅長

- APT 攻擊研究
- 資安威脅及新趨勢研究
- 駭客入侵與資安事件調查及回應
- 資安防禦策略規劃

# 這個 talk 可以幫助您什麼？

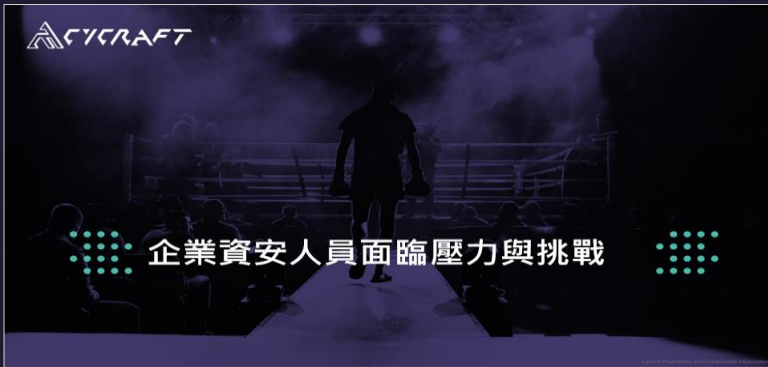
For 企業資安團隊

- ✓ 希望解決當下問題來找方案
- ✓ 想規劃合適的資安投資方向
- ✓ 正在擬定組織資安策略目標



# Agenda

## 企業資安人員 面臨壓力與挑戰



## 資安防護框架CDM Cyber Defense Matrix



## 善用AI協助企業 布局中場防線



The background of the slide is a dark, purple-tinted image of a boxing ring. A boxer is seen from behind, walking down a ramp towards the ring. The audience is visible in the foreground, and the ring ropes and structure are in the background.

# 企業資安人員面臨壓力與挑戰

# 資安從業人員迷思

目前流行的攻擊事件，我們單位均會發生？！？！



# 駭客集團針對特定產業(公司) 計畫竊密APT攻擊

- 攻擊時間：2018 ~ 2019 期間
- 攻擊對象：半導體產業
- 目標：竊取晶片相關文件、原始碼...等技術機密



至少 7 家  
半導體

至少達 1 年  
時間

合作夥伴  
上下游商

# 針對性擄資勒贖攻擊

## Big-Game Hunters Use APT Tactics

- Powertech (力成)
- MIRLE(盟立)
- Unimicron(欣興電子)
- Garmin(佳明)
- Golden Bridge(金橋)
- Compal Electronics (仁寶)
- Advantech Co., Ltd (研華)
- Foxconn Technology Group(鴻海)
- Quanta Computer Inc. (廣達)
- Acer Incorporated (宏碁)
- GIGABYTE Technology (技嘉)

## Hackers attacked 10 listed companies in Taiwan during pandemic

Notebook giant Compal Electronics and Advantech among targets: CTWANT

2108 Like 147 Share Tweet 分享

By Matthew Strong, Taiwan News, Staff Writer  
2020/12/09 14:07





威脅無處不在，每個都會發生在你身上？

DataLeakage PrintNightmare Mimikatz  
SQLInjection WebShell XSS  
Phishing APT Exploit  
CobaltStrike EternalBlue ZeroDay  
DDOS Cryptomining Virus  
SupplyChainAttack Ransomware  
JuicyPotato BEC Malware ZeroLogon  
MIRAI Worm PtH



# 資安從業人員迷思

眼前看到的問題著手解決？！？！

# 企業面臨資安事件的挑戰

## 未知與未來

- 駭客到底如何進入
- 未來是否仍會發生
- 如何評估潛在風險
- 資安事件如何應處

## 恐懼與壓力

- 暗網公布機密資料
- 受駭新聞持續發酵
- 供應鏈關係受創
- 事件處理時效壓力

## 評估與決策

- 哪些夥伴能幫助我
- 哪些工具能找到根因
- 我是否該支付贖金
- 法遵與應辦事項

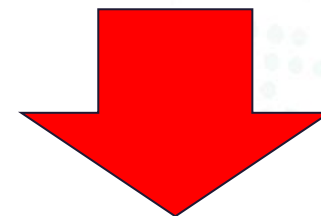


# 勒索軟體套路

## 亂槍打鳥的單台事件

- 攻擊成功後即快速加密勒索
- 效益低，回報低

目前多以此為主



## 人為大規模勒索

- 需規劃後始進行攻擊
- 攻擊成功後也不會立即勒索
- 勒索前先竊取單位內的機敏資料
- 攻陷派送系統後進行大規模勒索

# 駭客進行企業勒索四部曲 S.E.E.L

看見裂縫



使用APT手法入侵  
攻擊大部分人為操作  
鎖定單位AD主機  
鎖定重要資料  
HR、SAP、MES、Finance  
傳輸到雲端硬碟

AD部署加密程式  
AD設定定時炸彈  
實施檔案加密階段

暗網攻擊新聞發布  
寄給單位IT人員勒索訊息  
持續竊取資料

逐步洩漏資料  
公布洩漏進度比



# 資安從業人員迷思

產品買越多為什麼問題仍然還在？！？！



# 是否具備識破各廠商話術的包裝

- 駭客入侵後要達到真正的危害都需要提權，只要導入特權管理，讓駭客無權限可用則可以避免入侵造成的危害
- APT 攻擊以竊取單位內的機敏資料為主，那我導入 DLP 機制，駭客就算入侵，也沒辦法把機敏資料竊取走
- 陷入以上問題的，可能會造成單位內重複投資，買了不是防禦此問題最大效益的方案



# 資安防護框架CDM

## Cyber Defense Matrix



你無法管理你無法衡量的事物  
You can't manage what you don't measure.

管理學之父彼得·杜拉克 ( Peter Drucker )



# 先來收斂資安戰場...

## 駭客的攻擊手法

SQL Injection, Phishing Email, AD  
Exploit, Lateral movement, APT  
Malware, Ransomware

## 資安產品與服務

AntiVirus, DLP, IDS, Firewall,  
EDR/MDR, SOC, Forensics, Risk  
Assessment

## 資訊流與管理框架

公司的IT管理架構，資訊稽核、人員組織與權責、ISO 270XX, ISMS

# 資安奧義鐵三角

攻擊

Attack/Threat

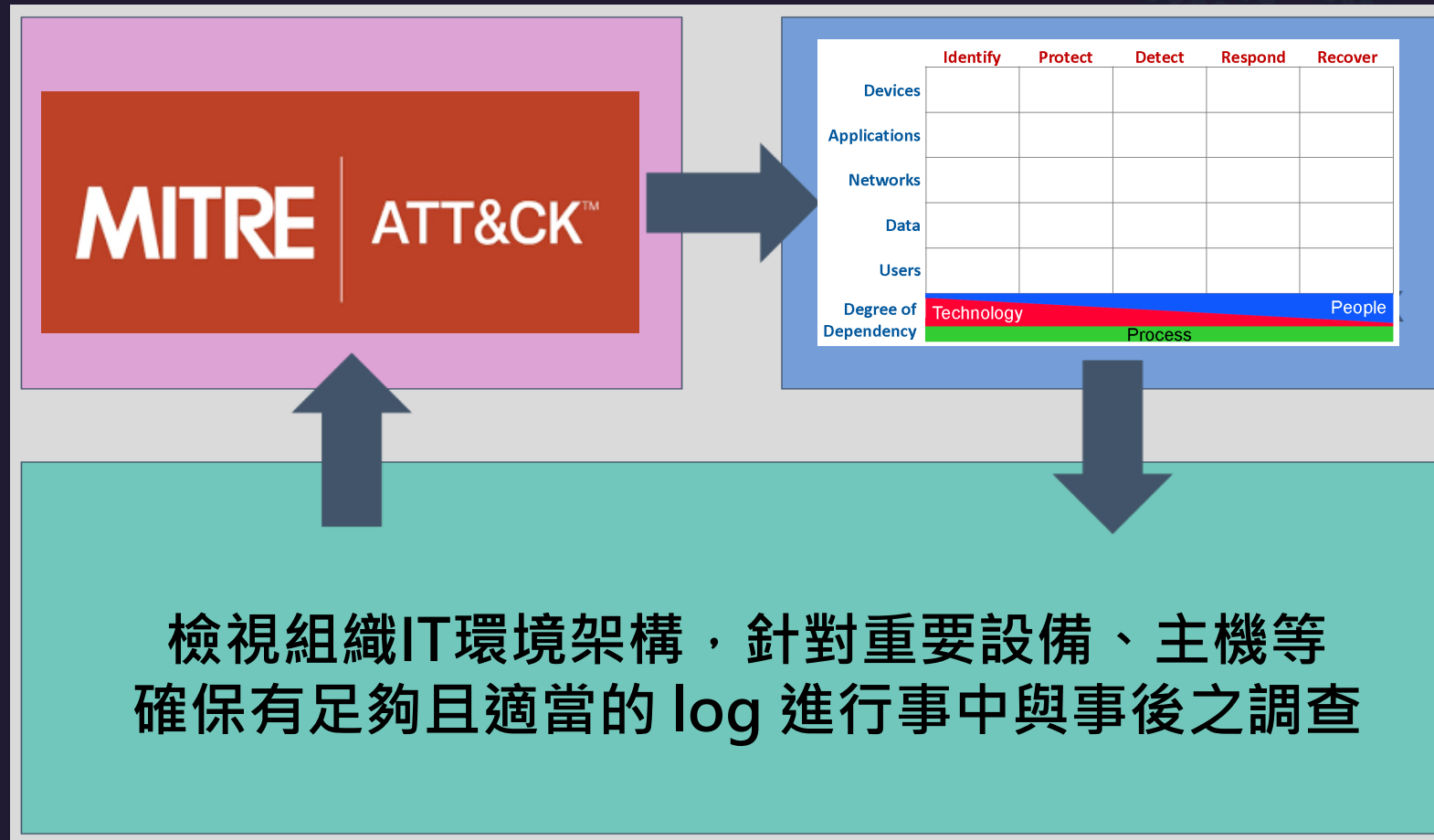
防禦

Defense/Response

框架

IT Framework

# 運用資安奧義鐵三角，你可以這樣做





# 補充：MITRE ATT&CK 駭客入侵手法框架

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (B2)	Acquire Infrastructure (B5)	Drive-by Compromise (B2)	Command and Scripting Interpreter (B1)	Account Manipulation (B4)	Abuse Elevation Control Mechanism (B4)	Abuse Elevation Control Mechanism (B4)	Brute Force (B4)	Account Discovery (B4)	Exploitation of Remote Services (B2)	Archive Collected Data (B2)	Application Layer Protocol (B4)	Automated Exfiltration (B1)	Account Access Removal (B2)
Gather Victim Host Information (B4)	Compromise Accounts (B2)	Exploit Public-Facing Application (B2)	Container Administration Command (B2)	BITS Jobs (B1)	Access Token Manipulation (B1)	Access Token Manipulation (B1)	Credentials from Password Stores (B1)	Application Window Discovery (B4)	Internal Spearphishing (B2)	Audio Capture (B2)	Communication Through Remote Media (B2)	Data Transfer Size Limits (B2)	Data Destruction (B2)
Gather Victim Identity Information (B2)	Compromise Infrastructure (B5)	External Remote Services (B2)	Deploy Container (B2)	Boot or Logon Autostart Execution (B1)	Boot or Logon Autostart Execution (B1)	Build Image on Host (B2)	Exploitation for Credential Access (B2)	Browser Bookmark Discovery (B4)	Lateral Tool Transfer (B2)	Automated Collection (B2)	Data Encoding (B2)	Exfiltration Over Alternative Protocol (B2)	Data Encrypted for Impact (B2)
Gather Victim Network Information (B5)	Develop Capabilities (B4)	Hardware Additions (B2)	Exploitation for Client Execution (B2)	Boot or Logon Initialization Scripts (B1)	Boot or Logon Initialization Scripts (B1)	Desktop/Decode Files or Information (B2)	Forge Web Credentials (B2)	Cloud Infrastructure Discovery (B4)	Remote Service Session Hijacking (B2)	Clipboard Data (B2)	Data Obfuscation (B2)	Exfiltration Over C2 Channel (B2)	Data Manipulation (B2)
Gather Victim Org Information (B4)	Establish Accounts (B2)	Phishing (B2)	Inter-Process Communication (B2)	Browser Extensions (B2)	Create or Modify System Process (B4)	Deploy Container (B2)	Input Capture (B4)	Cloud Service Discovery (B4)	Remote Services (B5)	Data from Cloud Storage Object (B2)	Dynamic Resolution (B2)	Exfiltration Over Other Network Medium (B1)	Disk Wipe (B2)
Phishing for Information (B2)	Obtain Capabilities (B5)	Replication Through Remote Media (B2)	Native API (B2)	Create Account (B2)	Domain Policy Modification (B2)	Direct Volume Access (B2)	Man-in-the-Middle (B2)	Container and Resource Discovery (B4)	Replication Through Remote Media (B2)	Data from Configuration Repository (B2)	Encrypted Channel (B2)	Exfiltration Over Physical Medium (B1)	Endpoint Denial of Service (B2)
Search Closed Sources (B2)	Stage Capabilities (B1)	Supply Chain Compromise (B2)	Scheduled Task/Job (B7)	Create or Modify System Process (B4)	Escape to Host (B2)	Execution Guardrails (B1)	Modify Authentication Process (B4)	File and Directory Discovery (B4)	Software Deployment Tools (B2)	Data from Information Repositories (B2)	Fallback Channels (B2)	Exfiltration Over Web Service (B2)	Firmware Corruption (B2)
Search Open Technical Databases (B2)		Trusted Relationship (B2)	Shared Modules (B2)	Event Triggered Execution (B1)	Exploitation for Defense Evasion (B2)	File and Directory Permissions Modification (B2)	Network Sniffing (B4)	File and Directory Discovery (B4)	Taint Shared Content (B2)	Data from Local System (B2)	Ingress Tool Transfer (B2)	Inhibit System Recovery (B2)	Network Denial of Service (B2)
Search Open Websites/Domains (B2)		Valid Accounts (B4)	Software Deployment Tools (B2)	External Remote Services (B2)	Hijack Execution Flow (B1)	Hide Artifacts (B2)	OS Credential Dumping (B2)	Network Service Scanning (B4)	Use Alternate Authentication Material (B4)	Data from Network Shared Drive (B2)	Multi-Stage Channels (B2)	Scheduled Transfer (B2)	Resource Hijacking (B2)
Search Victim-Owned Websites (B2)			System Services (B2)	Hijack Execution Flow (B1)	Implant Internal Image (B2)	Hijack Execution Flow (B1)	Steal Application Access Token (B4)	Network Sniffing (B4)		Data from Remote Media (B2)	Non-Application Layer Protocol (B2)	Transfer Data to Cloud Account (B2)	Service Stop (B2)
			User Execution (B2)	Implant Internal Image (B2)	Modify Authentication Process (B4)	Indicator Removal on Host (B5)	Steal or Forge Kerberos Tickets (B4)	Network Sniffing (B4)		Data Staged (B2)	Non-Standard Port (B2)		System Shutdown/Reboot (B2)
			Windows Management Instrumentation (B2)	Modify Authentication Process (B4)	Office Application Startup (B5)	Indirect Command Execution (B2)	Steal Web Session Cookie (B2)	Peripheral Device Discovery (B4)		Email Collection (B2)	Protocol Tunneling (B2)		
				Pre-OS Boot (B1)	Scheduled Task/Job (B7)	Masquerading (B4)	Two-Factor Authentication Interception (B2)	Permission Groups Discovery (B2)		Input Capture (B4)	Proxy (B4)		
				Scheduled Task/Job (B7)	Server Software Component (B2)	Modify Authentication Process (B4)	Unsecured Credentials (B2)	Process Discovery (B4)		Man in the Browser (B2)	Remote Access Software (B2)		
				Traffic Signaling (B1)	Traffic Signaling (B1)	Modify Cloud Compute Infrastructure (B4)		Query Registry (B4)		Man-in-the-Middle (B2)	Traffic Signaling (B1)		
				Valid Accounts (B4)	Valid Accounts (B4)	Modify Registry (B2)		Software Discovery (B1)		Screen Capture (B2)	Web Service (B2)		
						Modify System Image (B2)		System Information Discovery (B4)		Video Capture (B2)			
						Network Boundary Bridging (B1)		System Location Discovery (B4)					
						Obfuscated Files or Information (B3)		System Network Configuration Discovery (B1)					
						Pre-OS Boot (B1)		System Network Connections Discovery (B4)					
						Process Injection (B1)		System Owner/User Discovery (B4)					
						Rogue Domain Controller (B2)		System Service Discovery (B4)					
						Rootkit (B2)		System Time Discovery (B4)					
						Signed Binary Proxy Execution (B1)		Virtualization/Sandbox Evasion (B2)					
						Signed Script Proxy Execution (B1)		Weaken Encryption (B2)					
						Subvert Trust Controls (B5)		XSL Script Processing (B2)					
						Template Injection (B2)							
						Traffic Signaling (B1)							
						Trusted Developer Utilities Proxy Execution (B1)							
						Unused/Unsupported Cloud Regions (B2)							
						Use Alternate Authentication Material (B4)							
						Valid Accounts (B4)							
						Virtualization/Sandbox Evasion (B2)							
						Weaken Encryption (B2)							

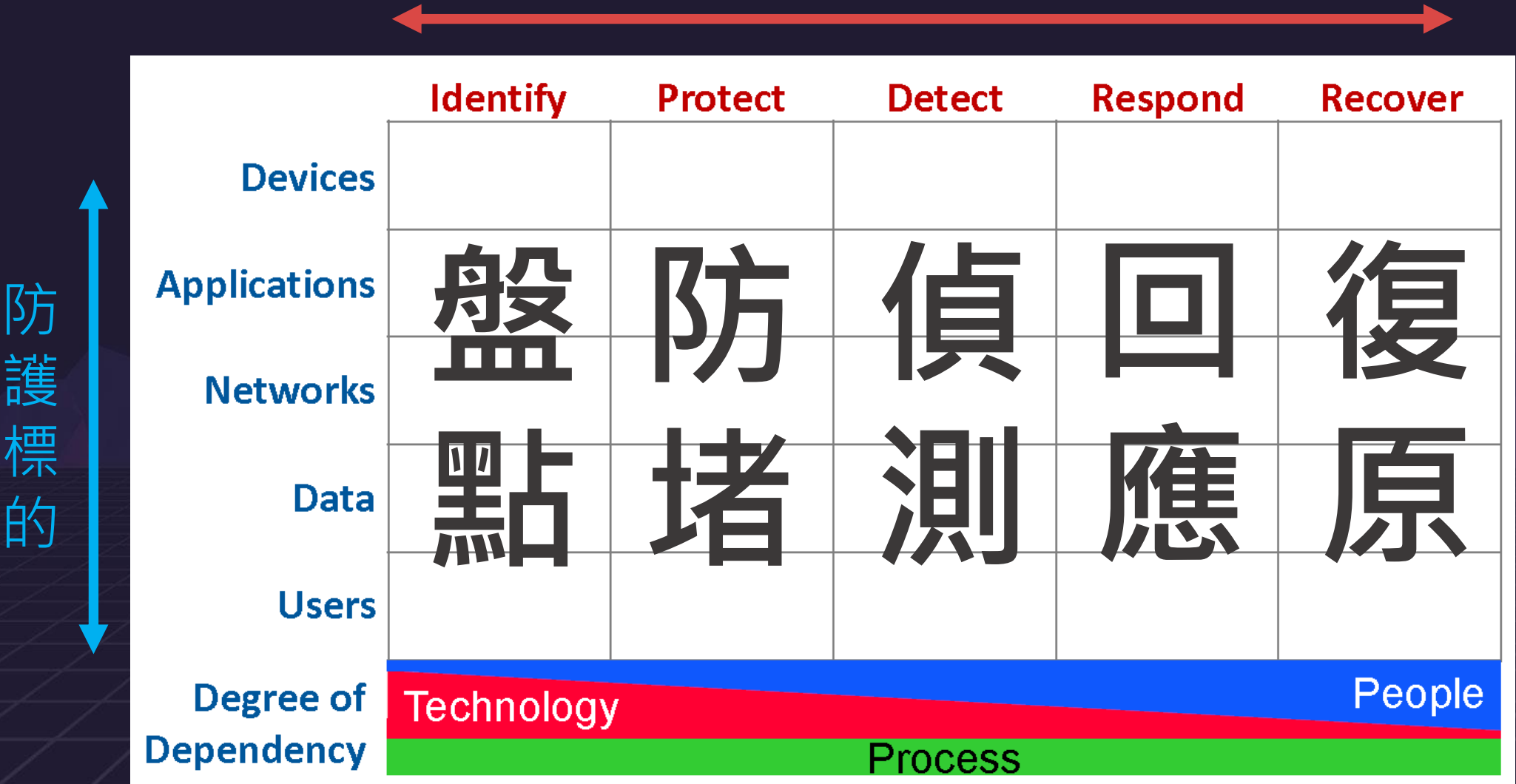
最新版 v9 (共 552 招)

# 資安防護框架 CDM 是什麼？

- 美國銀行首席安全科學家 Sounil Yu 所提出並納入 OWASP (2016)
- CDM (Cyber Defense Matrix) 由一個 5x5 的矩陣所構成。
- 橫軸是 NIST CSF (Cybersecurity Framework) 的五大類別；縱軸則是資產盤點常見的分類
- 組織可此矩陣來盤點所建構之資安防禦設備，更精準的確認需要保護的資產是否在 NIST CSF (Cybersecurity Framework) 的每個類別都有對應的措施。

# Cyber Defense Matrix 資安防護框架

防護階段



資料來源:<https://owasp.org/www-project-cyber-defense-matrix>

# 工具自動化 與 人工介入 程度

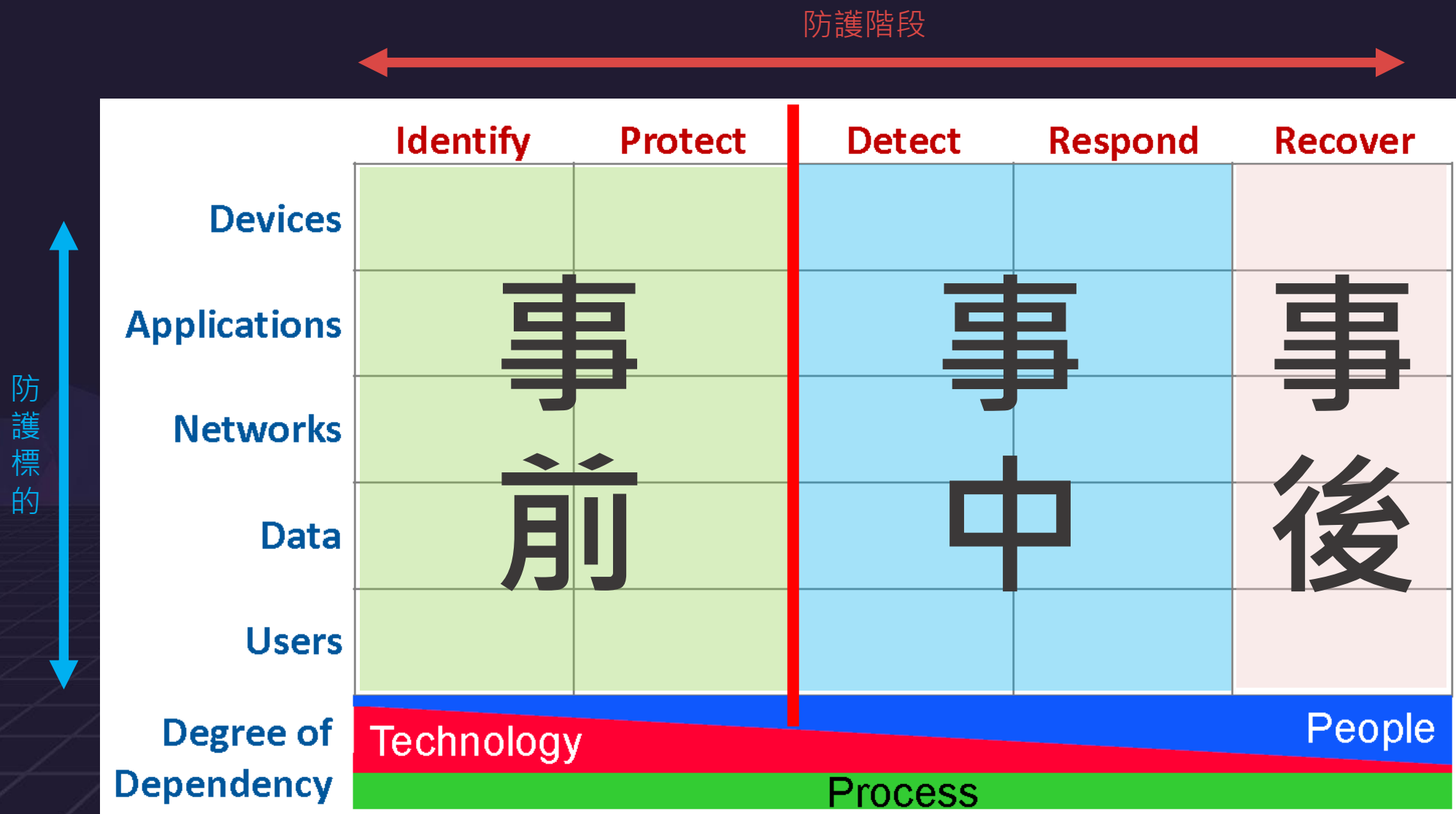
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	Technology			People	
	Process				

- 不同資料來源(data source)在每個階段程序中有不同自動化程度
- 於資安事件生命週期越早期處理，越需要高科技自動化
- 反之，越往後段目前需要的人工介入相對較高
- 未來產品及服務也是會持續往自動化去發展





# 一般常講的事前事中事後如何分？



# 我們應該把觀念微調

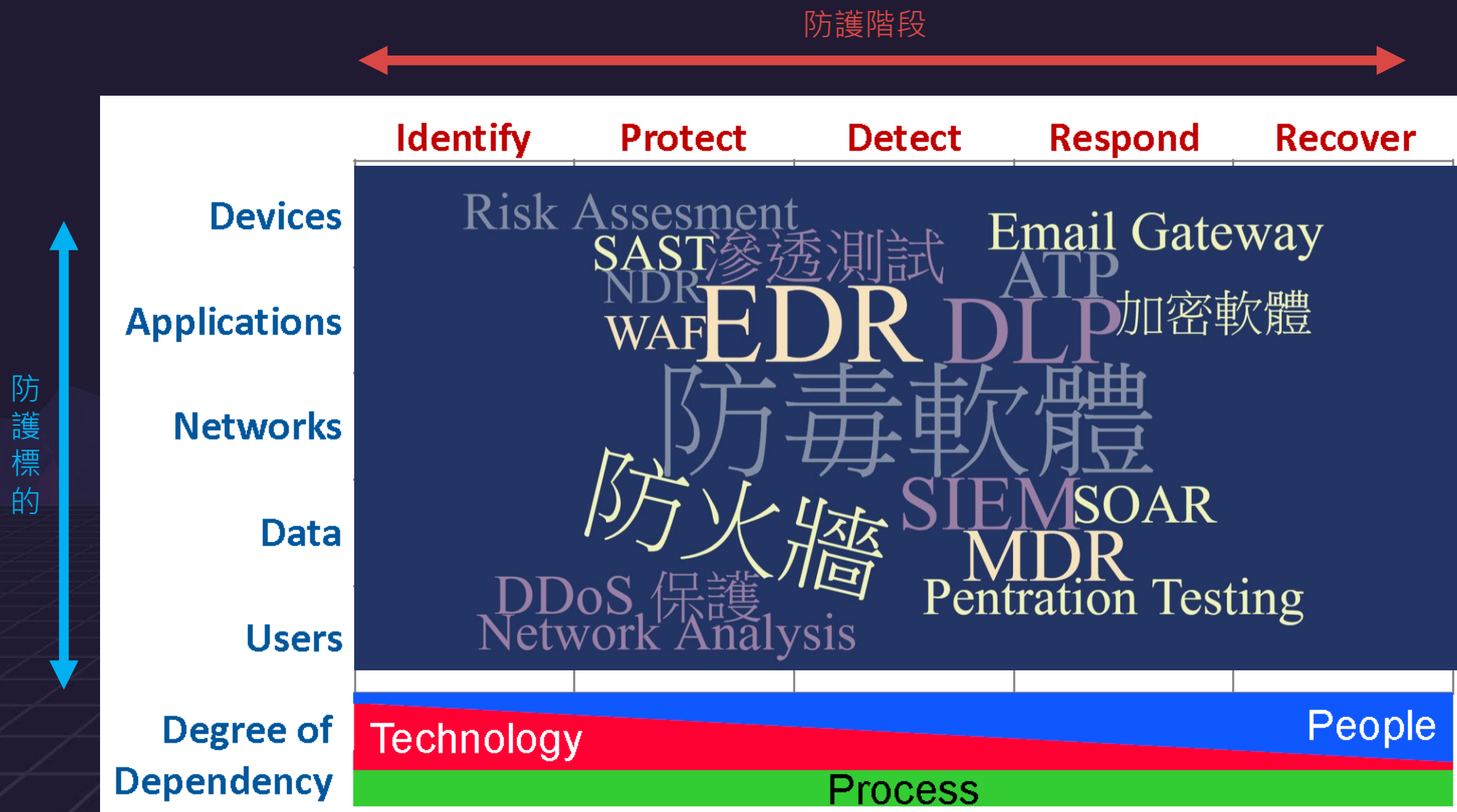
基礎資安防護概念

近期資安策略：組織資安韌性

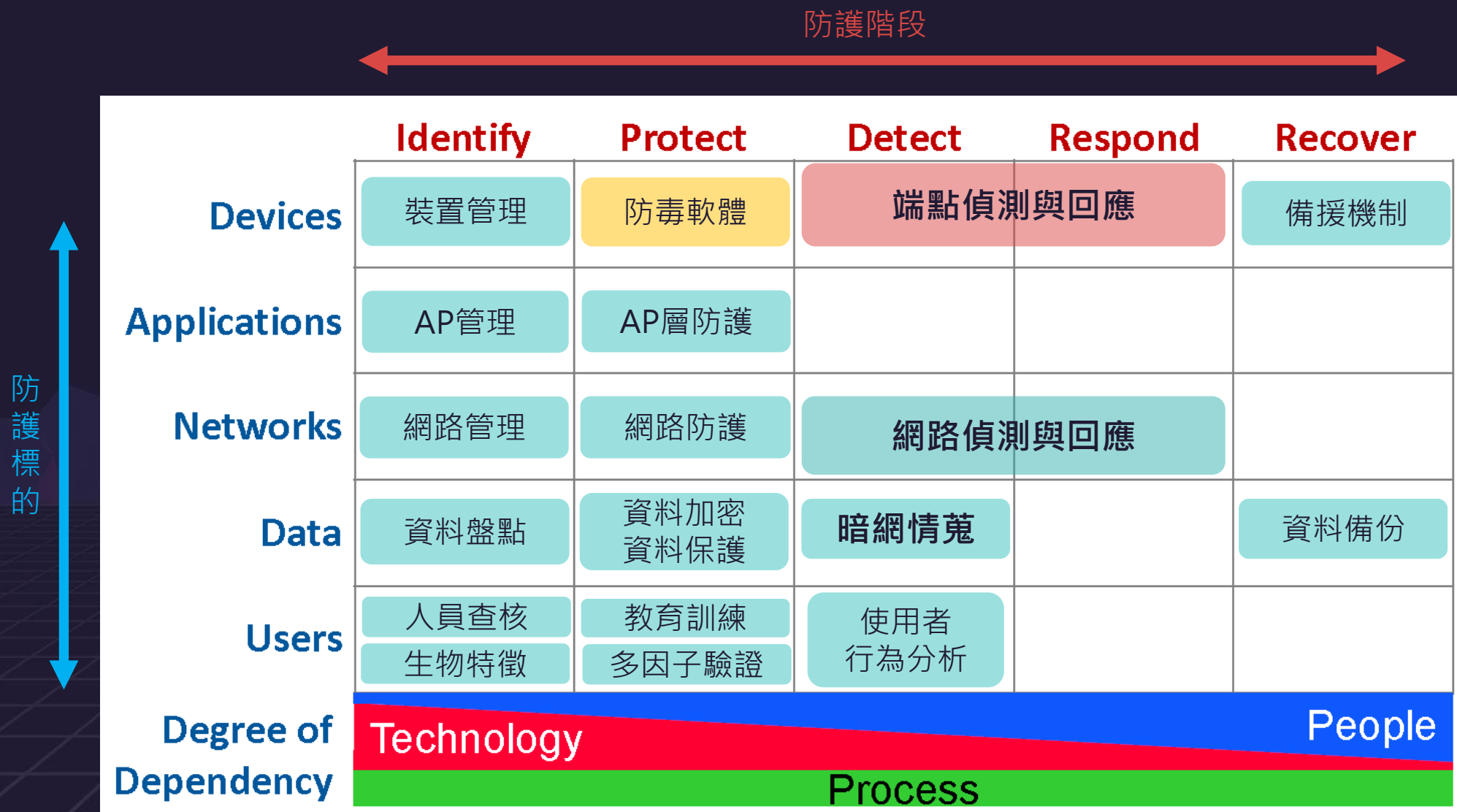
防護標的

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications	<div>防禦不是 0 或 1</div> <div>而是 0%~100% 的過程</div> <div>企業應思考 資安韌性</div>				
Networks					
Data					
Users					
Degree of Dependency	Technology			People	
	Process				

# 將各種資安產品/服務進行分類分組

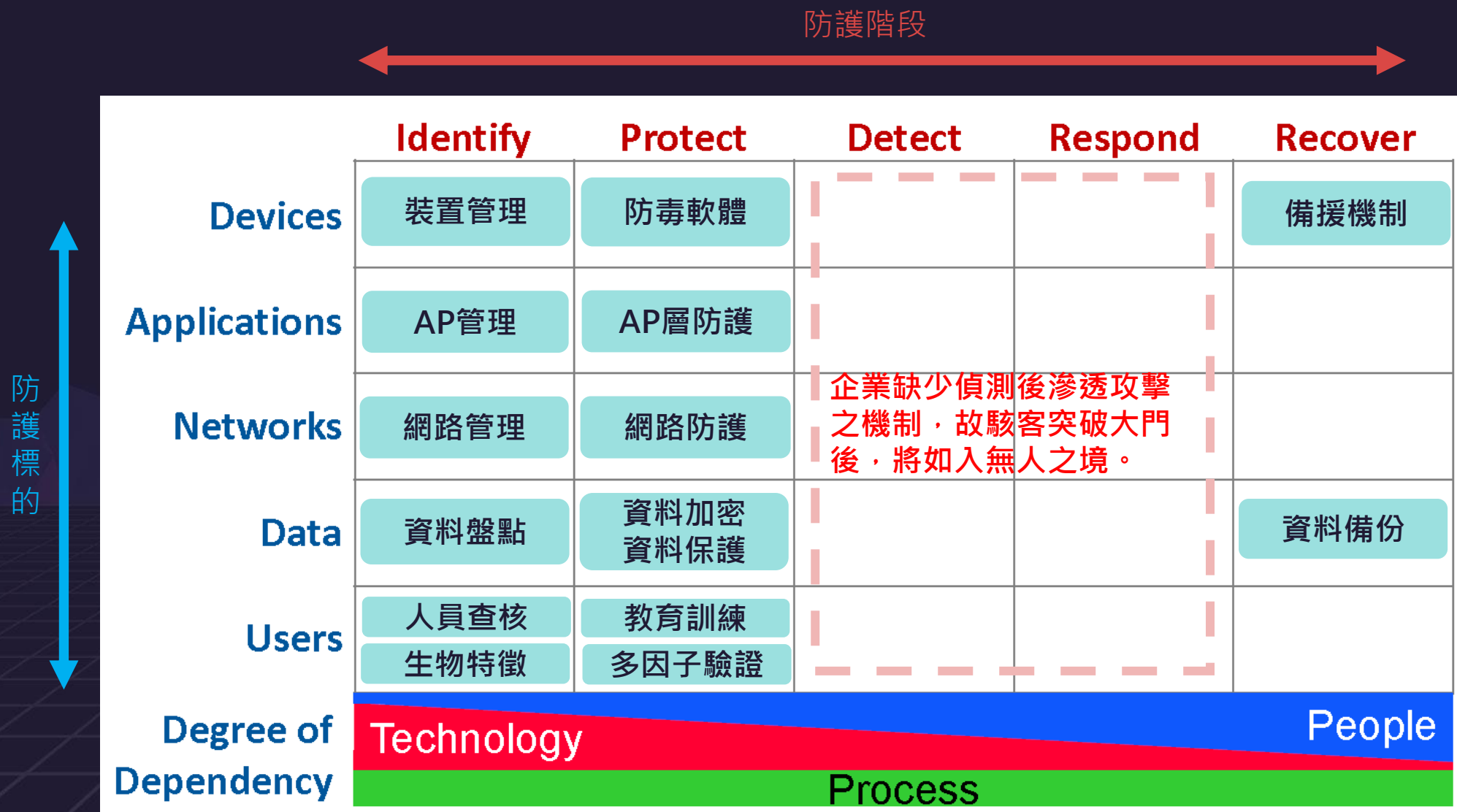


# 盤點企業資安防禦部署方式

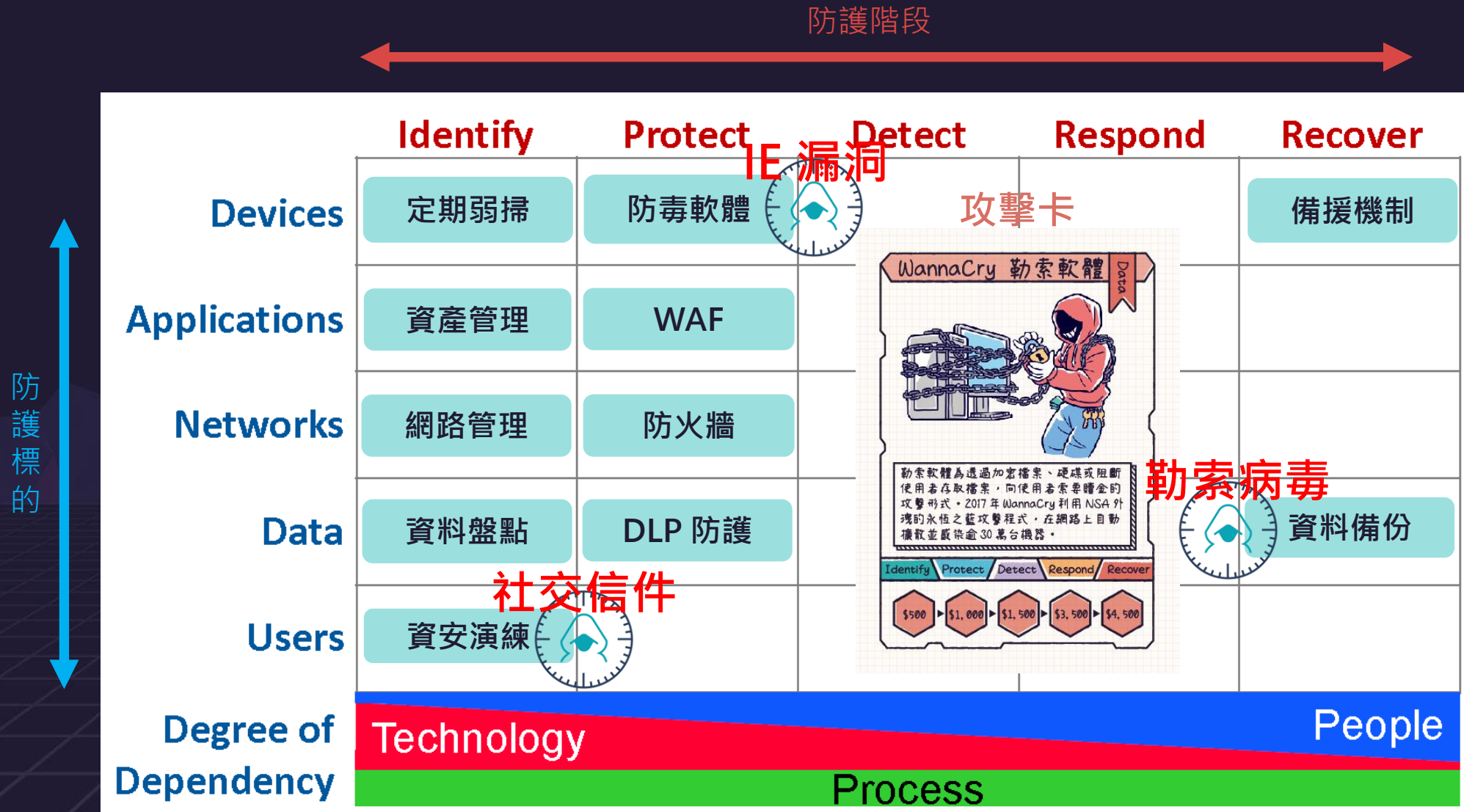




# Case : (資安盤點)發現最脆弱環節落在事中階段



# Case : (事件分析) 社交工程郵件+ IE 漏洞+勒索



# 如何具體運用CDM

1. 確認問題的面向，選擇適合解決方案  
理解CDM各防護目標與階段意含，明確所面臨之問題，進而尋找合適解決方案
2. 盤點防護能量，檢視成本配置情況  
盤點組織目前已具備之防護面向及成本投入，釐清是否有重複投資
3. 透過事件根因分析，調整資安配置  
從事件中經驗學習去找到組織防禦中的弱區，進行資安部署調整或是優化事件應變程序
4. 評估風險衝擊，發展未來資安策略  
評估組織內部資安風險程度以及帶來的衝擊程度，規劃後續資安佈局

# 投資成本與CDM

Use Case 6: Understand how to balance your portfolio without breaking the bank #RSAC

	Identify	Protect	Detect	Respond	Recover	Total
Devices		\$50	\$100		\$50	\$200
Applications	\$50	\$100		\$50	\$100	\$300
Networks	\$100		\$100	\$50		\$250
Data		\$50	\$50		\$50	\$150
Users	\$50			\$50		\$100
Total	\$200	\$200	\$250	\$150	\$200	\$1000

**ILLUSTRATIVE**

@sounil

18

RSAConference2016



A soldier in a futuristic, dark-colored combat suit is shown in a dynamic, mid-air pose, possibly jumping or falling. The suit has various straps and equipment. The background is a dark, deep blue with a subtle geometric pattern of white lines and dots, suggesting a digital or networked environment.

# 善用AI協助企業 佈局中場防線





# 奧義智慧科技



奧義智慧持續厚積台灣能量，以 AI 驅動的資安自動化服務在國內諸多領域保持第一的市占率，獲得政府機關、金融、高科技等財星500大企業之肯定，2019年獲邀美國 MITRE ATT&CK® 攻擊框架評測計畫，2020年官方公開評測結果，奧義智慧以最高偵測告警能力，技冠群雄獲全球21家國際大廠之最。

奧義智慧已在日本、新加坡成立據點，策略合作夥伴遍及東協泰國、馬來西亞、印尼、越南及菲律賓等10國，持續積極將台灣能量推向世界舞台。我們以人工智慧提供高度自動化的 MDR、SOC、威脅情資、資安健診、數位鑑識，資安事件處理 IR 等資安服務。



國際企業安全事件  
應變認證



2020 MITRE ATT&CK  
權威評測最高信噪比



2021網路安全卓越獎  
逾 10 項金獎肯定



日本Interop  
最佳資安產品獎



ISO/IEC  
27001

# 企業建構自動化安全防禦三面向：端點、閘道、情資

## 組建三大防禦面向之階段目標

### • 第一階段〔Health Check & RiskINT〕

定期資安健診了解企業風險  
端點風險 與 情資曝險

### • 第二階段〔MDR Service〕

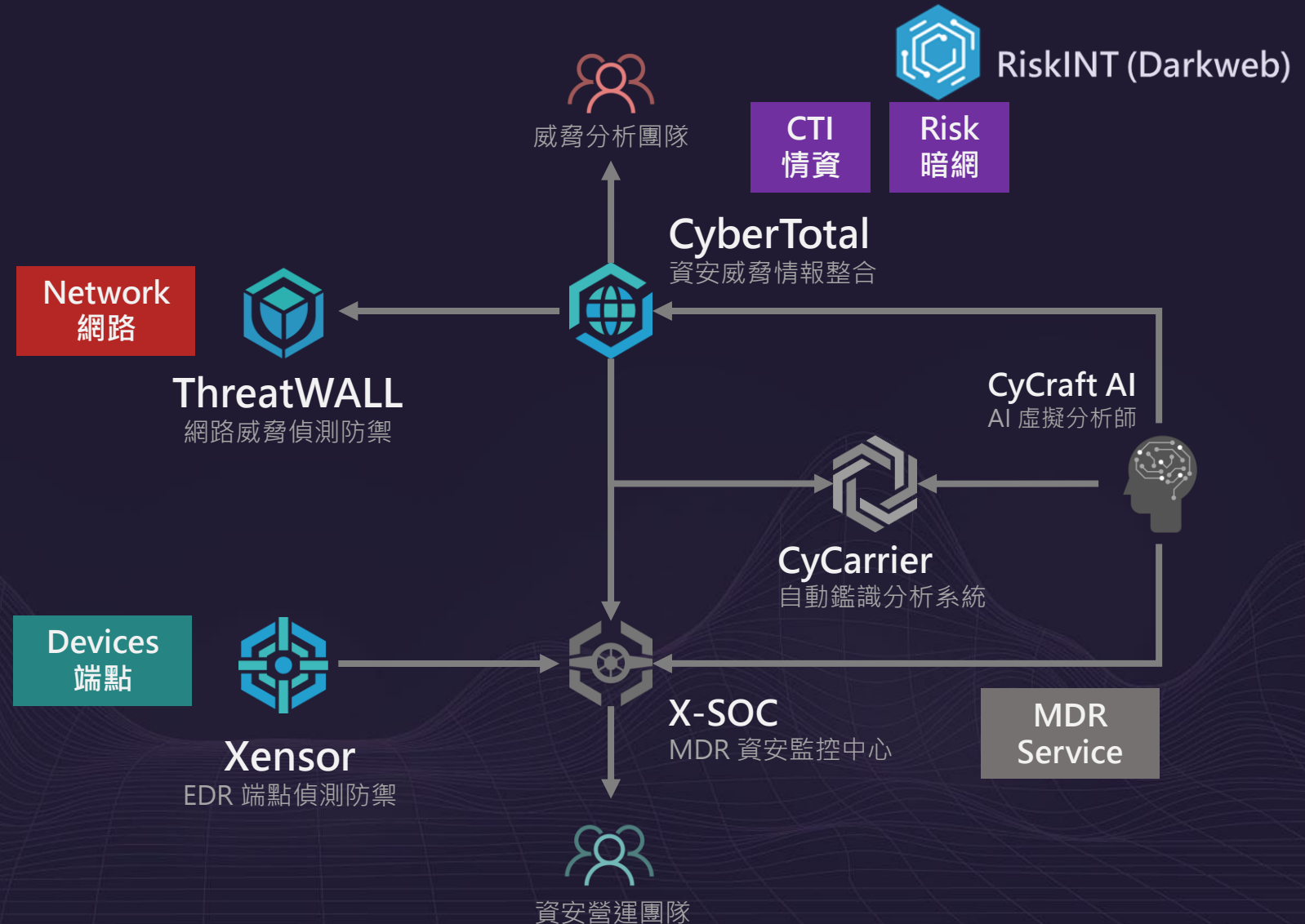
企業場域端點偵測與防禦  
威脅即時通報與及時診治

### • 第三道防線〔Threat Wall〕

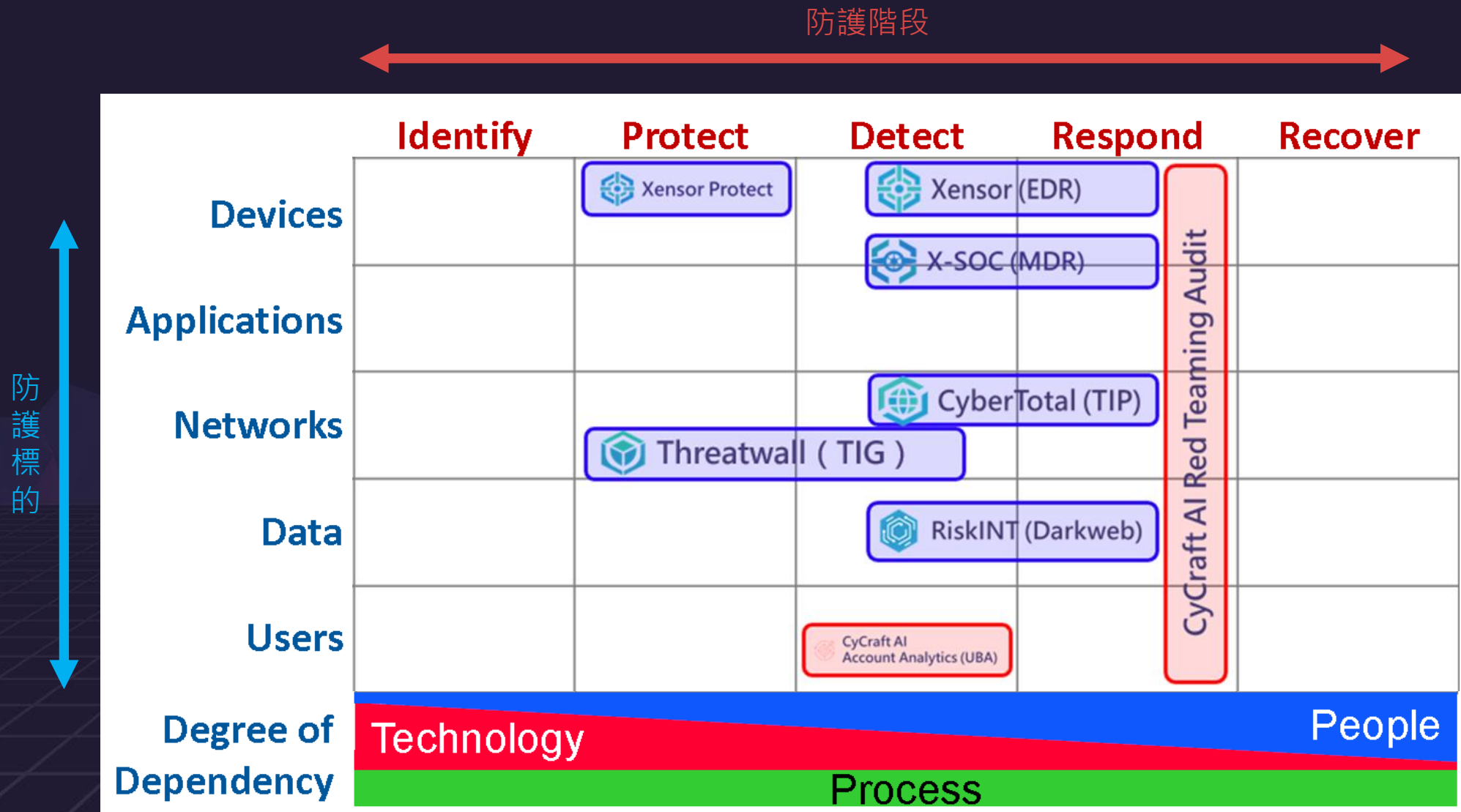
閘道檢測攔阻惡意連線

### • 第四道防線〔CyberTotal〕

即時掌握全球資安威脅超前部署



# Mapping CyCraft to CDM







# 持續改善建議

## 下一周你需要做：

- 檢視組織的整體運作及商業流程
- 可與我們聯繫，討論相關建議方案與配置規劃

## 接下來三個月內你該做：

- 利用 CDM 框架進行組織內部配置檢視
- 思考並建構屬於自己組織的防禦架構

## 六個月內你該做：

- IT 或資安部門小範圍兵棋推演，事件前/中/後應變處置流程
- 以衝擊程度較大的資安威脅類型優先規劃

奧義智慧 守護企業資安場域  
成為資安團隊強力靠山

Thank You



奧義官網



奧義粉專



奧義 Medium