DEVCORE
SECURITY
CONSULTING

你的資安策略夠明確嗎？
透過框架優先緩解真實威脅

翁浩正 (Allen Own)

鍾澤華 (Aaron Chung)

戴夫寇爾股份有限公司

contact@devco.re

2020.09.12 HITCON

講者簡介

翁浩正 (Allen Own)

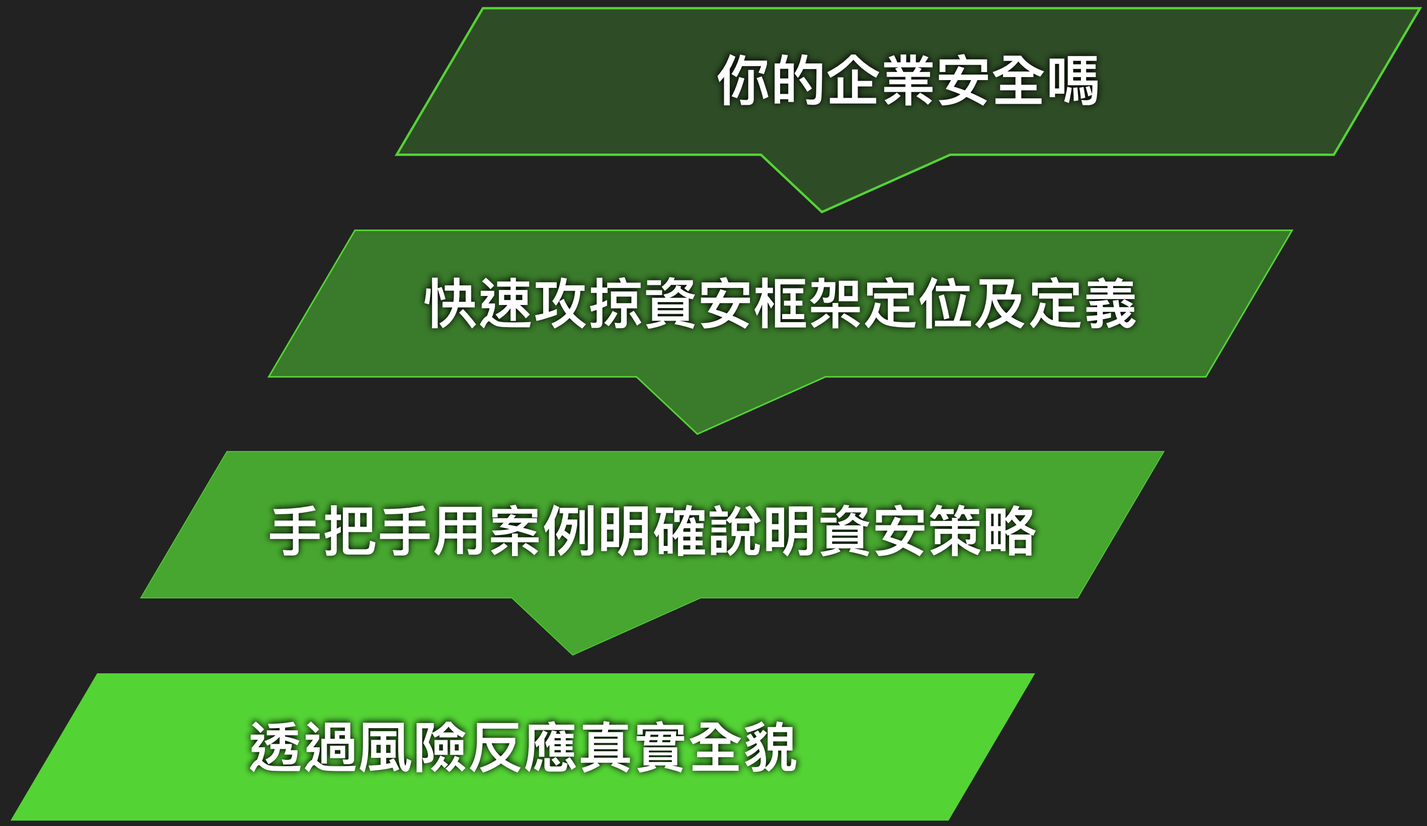
DEVCORE 執行長

鍾澤華 (Aaron Chung)

DEVCORE 事業發展經理

Agenda

你的資安策略夠明確嗎？
透過框架優先緩解真實威脅



你面對的是駭客
我們也是

- ✓ 紅隊演練
- ✓ 滲透測試
- ✓ 教育訓練
- ✓ 顧問服務

紅隊演練
Red Team Assessment
紅隊演練是真實的攻擊演練，這張戰場圖說明團隊的編制、任務目標、以及每個階段的成果。

68%
超過六成以上的專案可以控制 AD 伺服器、vCenter 等，進而控制企業核心系統

CORE ZONE

83%
破解超過 7.6 萬個員工之密碼，顯示八成以上企業密碼強度仍高度不足

100%
截至目前為止，戴夫寇爾平均 4 天內可以成功進入企業內部網路

DEMILITARIZED ZONE

64%
六成以上企業外洩可被利用之帳號密碼、原始碼、內部文件

INTERNET

打擊小隊
尋找同系列漏洞、設定 C2 中繼站、橫向及垂直移動及掃蕩內網關鍵基礎設施

研究小隊
針對特規系統或難以突破的節點研發 0-day 漏洞、開發漏洞利用程式

特攻小隊
負責找尋能順利入侵企業的第一個節點或嘗試取得資料

情搜小隊
針對已公開揭露或暗網之資訊進行偵查及收集，供特攻小組擬定作戰計畫

支援小隊
部署基礎設施、記錄戰況、維持系統存取連線及翻找機敏文件

DEVCORE SECURITY CONSULTING

資安策略

＝ 有順序性的待辦清單 (短、中、長期)

＝ 企業導入防禦措施後仍須持續處理的事項

資安策略

＝ 有順序性的待辦清單 (短、中、長期)

＝ 企業導入防禦措施後仍須持續降低風險的事項

企業應該知道的資安狀況

安不安全	企業執行面	目前資安有一些成效，持續在多個領域進行強化工作將提高業務績效 / 降低受害時的損害
面臨哪些風險	主要風險	最近新的供應商對我們的風險狀況影響很小。 其他重大風險均在可以控制的範圍內。
	外部環境	外部環境所可能造成的事件需要哪些戰術響應 勒贖軟體、資料外洩、服務中斷
需要哪些資源	資安策略	當前執行安全策略的目標很大。我們的流程成熟度不斷提高，超過了基準並持續接近目標值
	建議事項	記錄當前狀態並批准行動計劃

Reference: Board-Ready Slides for Cybersecurity and Technology Risk Sample Narrative, Gartner 2017

企業應該知道的資安狀況

現在 **安不安全**	企業執行面	目前資安有一些成效，持續在多個領域進行強化工作將提高業務績效 / 降低受害時的損害
現在及未來 **面臨哪些風險**	主要風險 (已經發現)	最近新的供應商對我們的風險狀況影響很小。 其他重大風險均在可以控制的範圍內。
	外部環境 (可能發生)	外部環境所可能造成的事件需要哪些戰術響應 勒贖軟體、資料外洩、服務中斷
現在及未來 **需要哪些資源**	資安策略	當前執行安全策略的目標很大。我們的流程成熟度不斷提高，超過了基準並持續接近目標值
	建議事項	記錄當前狀態並批准行動計劃

Reference: Board-Ready Slides for Cybersecurity and Technology Risk Sample Narrative, Gartner 2017

恢復原狀

1. 掌握現況
2. 緊急處理，將危害控制在最小範圍
3. 查明及分析發生原因
4. 將問題修復並還原
5. 研究對策，避免復發

資安事件調查結果
每週監控結果
每週設備 Top10 阻擋統計
每月事件單關單統計表
管理審查會議

防微杜漸

1. 定義**對企業營運可能造成衝擊的問題**
2. 識別造成問題的原因
3. 思考**預防**問題對策
4. 思考問題**發生時**的對策

勒贖軟體導致營運中斷
攻擊推陳出新
設備追到最新
訂定企業持續營運計畫

追求理想

1. 盤點並分析問題的優缺點
2. **設定企業理想目標**
3. 制定行動計畫來達成理想的對策

防微杜漸都做不完，不可能談理想，因為資源有限

DEVCORE SECURITY CONSULTING

無法掌握可能對企業造成的衝擊事件

盤點重要資產

自行定義資產威脅

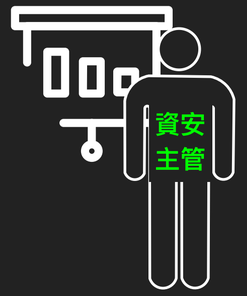
自行想像可能弱點

自行判斷發生機率
可能錯估情勢、可能不想面對

資產名稱	資產價值	威脅	弱點	衝擊等級	可能性	風險等級	控制措施降低可能性	企業承受的風險
SW - 核心系統	3	軟體失效	維護服務時間過長	3	1	9	1	9
SW - 核心系統	3	軟體失效	遭到 DDOS 攻擊	3	2	18	1	9
SW - 核心系統	3	未經授權存取	橫向移動	3	2	18	1	9
SW - 內部老舊系統	1	系統入侵	無法上 patch	2	2	4	2	4
DA - 重要電子紀錄	2	蓄意破壞	人員訓練不足	2	2	8	2	8
DA - 重要電子紀錄	2	蓄意破壞	建築物管制不足	2	2	8	2	8

恢復原狀

1. 掌握現況
2. 緊急處理，將危害控制在最小範圍
3. 查明及分析發生原因
4. 將問題修復並還原
5. 研究對策，避免復發



防微杜漸

1. 定義**對企業營運可能造成衝擊的問題**
2. 識別造成問題的**原因**
3. 思考**預防**問題對策
4. 思考問題**發生時**的對策

未雨綢繆

1. 盤點並分析問題的優缺點
2. **設定企業理想目標**
3. 制定行動計畫來達成理想的對策

資安事件調查結果
每週監控結果
每週設備 Top10 阻擋統計
每月事件單關單統計表
管理審查會議

勒贖軟體導致營運中斷
攻擊推陳出新
設備追到最新
訂定企業持續營運計畫

資安資源的對企業的幫助
預算投入的有效性評估
資安資源持續安排的優先序

DEVCORE SECURITY CONSULTING

資安策略的基礎是資安框架
而資安框架要有效果，要靠真實威脅調整

什麼是資安框架與標準？

EXECUTIVE

Risk Frameworks (SANS)

- NIST 800-39、NIST 800-30
- ISO 27005、CIS RAM

PROCESS

Program Frameworks (SANS)

- NIST Cybersecurity Framework
- ISO 27001

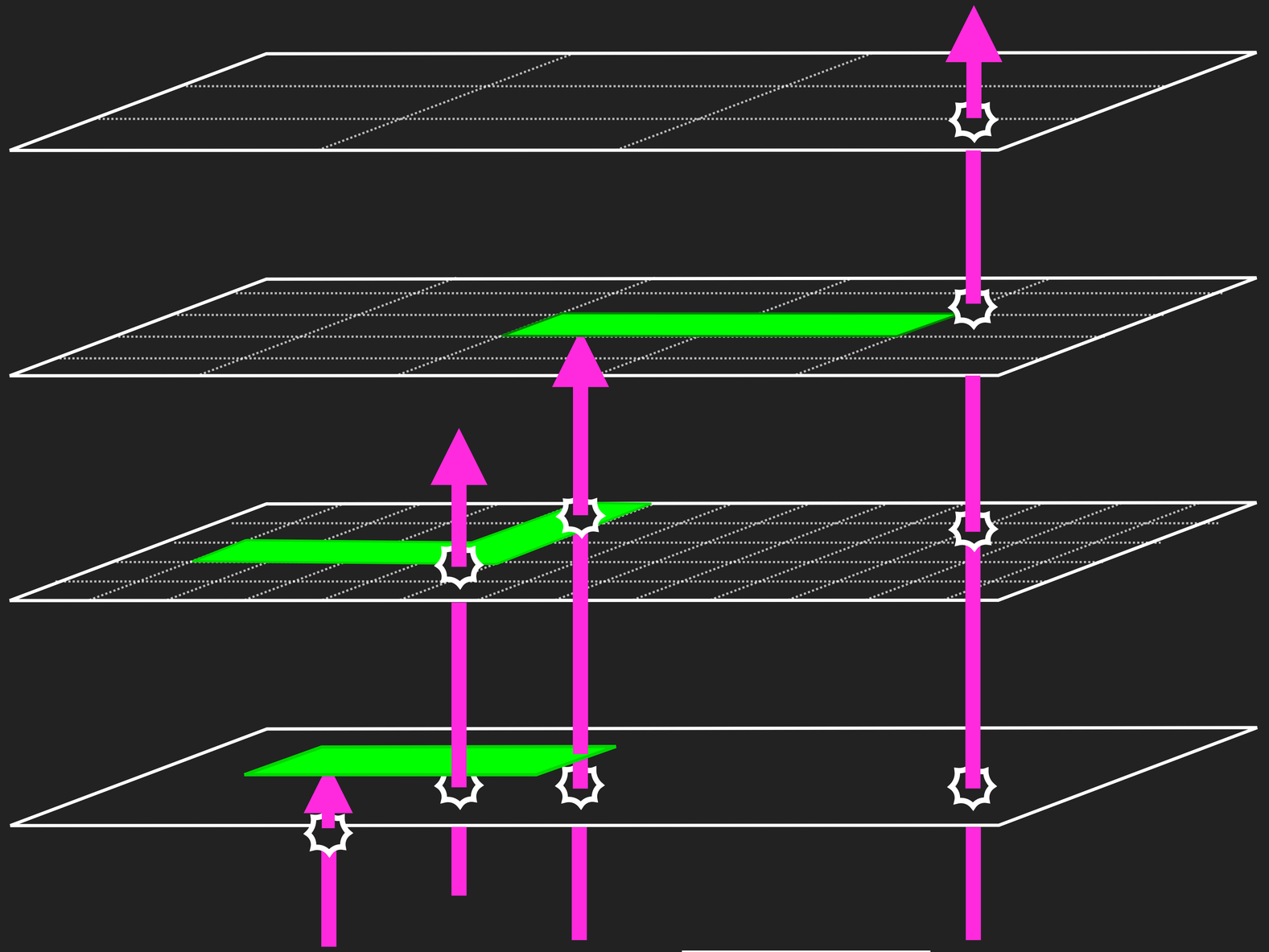
PROCEDURE

Controls Frameworks (SANS)

- NIST 800-53
- CIS Critical Security Controls

TECHNOLOGY VIEW

Defense Appliance / Service



EXECUTIVE

Risk Frameworks (SANS)

- NIST 800-39、NIST 800-30
- ISO 27005、CIS RAM

PROCESS

Program Frameworks (SANS)

- NIST Cybersecurity Framework
- ISO 27001

PROCEDURE

Controls Frameworks (SANS)

- NIST 800-53
- CIS Critical Security Controls

TECHNOLOGY VIEW

Defense Appliance / Service

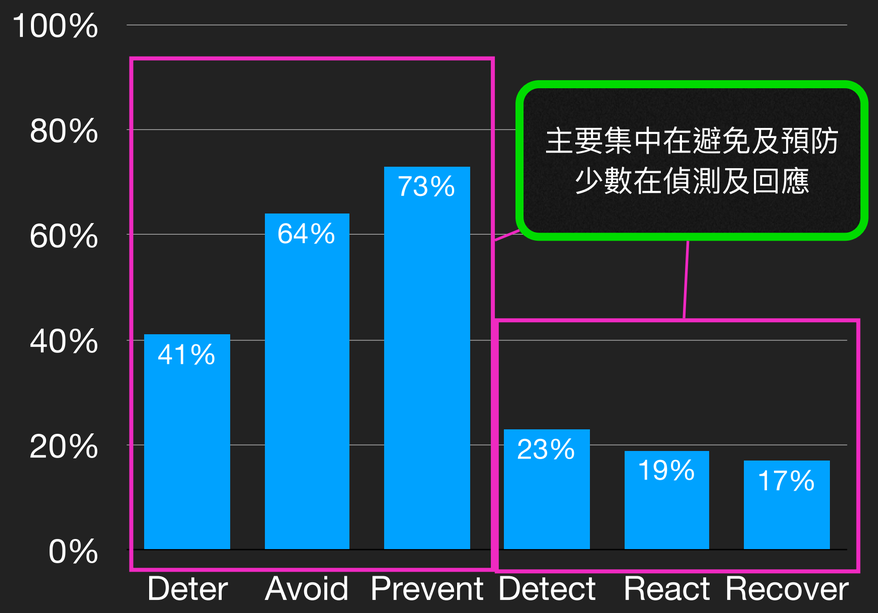
DEVCORE SECURITY CONSULTING

ATTACKER'S VIEW **MITRE ATT&CK**

框架與標準的定位

ISO 27001:2013

- 建立資訊安全管理系統的標準，幫助組織管理和保護資訊資產，確保達到客戶或利害關係人其安全的期待；可以驗證。
- 降低業務風險、提昇商業信賴度、有助於業務營運



NIST Cybersecurity Framework v1.1

- 網路安全框架：提供關鍵基礎設施或一般企業幫助組織管理和保護資訊資產，確保其安全無慮；可以驗證。
- 提供結構化的方式，讓組織資安成熟度持續強化。

Identify	Protect	Detect	Respond	Recover
資產管理 營運環境 治理 風險評估 風險管理策略	存取控制 意識與教育訓練 資料安全 資訊保護與程序 維護 防護技術	異常事件 持續安全監控 檢測流程	回應計畫 溝通 分析 緩解 改善	復原計畫 改善 溝通

CIS CSC v7.1

- 資訊安全控制指引：針對網路攻擊所應採取的控制項目提出優先執行順序，並依照組織規模(IG1-IG3) 提供執行建議。
- 分為基礎型、基本型及組織型，共 20 個控制群組、178 個子控制項。

基本型 (網路衛生)

1. 硬體資產盤點
2. 軟體資產盤點
3. 持續弱點管理
4. 特權帳號管控
5. 安全組態管理
6. 維護、監督及分析日誌

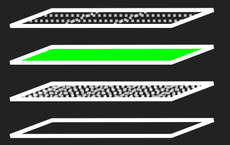
基礎型

7. 電子郵件與瀏覽器存取保護
8. 防範惡意軟體
9. 網路通訊埠限制與控制
10. 資料復原
11. 網路設備安全組態
12. 邊界防禦
13. 資料保護
14. 存取控制
15. 無線網路存取
16. 帳號監督與控管

組織型

17. 安全意識與訓練計畫
18. 應用程式軟體安全
19. 突發事件的反應與管理
20. 滲透測試與紅隊演練

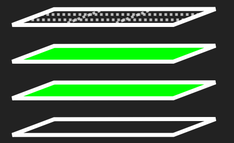
框架與標準的比較



ISO 27001:2013	NIST CSF v1.1
• 基於風險管理，僅在發現到網路安全風險時才要求實施安全措施 • 皆為技術中立	• 如何在組織中實施資訊安全或網路安全的方法，都能獲得不錯的成效 • 皆強調法律遵守
國際標準，可以驗證	由美國 NIST 制定，美國聯邦政府必須導入
文件化要求， 提供 P-D-C-A 良好的持續改善機制	• 功能以結構化方式分為**識別、防禦、偵測、回應與復原**的方式針對網路安全進行強化 • 彈性應用，具備**成熟度模式**便於衡量現況
重點在於**保護所有類型的訊息**，而不只是保護 IT 系統中存儲或處理的訊息。	支援其他架構 **ISO 27001**, COBIT, NIST **SP 800-53**, ISA 62443, and **CIS CSC** **提供成熟度模式** (Framework Implementation Tiers)

ISO 27001、NIST CSF 可以互補、相輔相成

CIS Controls 可以強化控制項目



EXECUTIVE

Risk Frameworks

- NIST 800-39、NIST 800-30
- ISO 27005
- CIS RAM

PROCESS

Program Frameworks

- NIST CSF
- ISO 27001

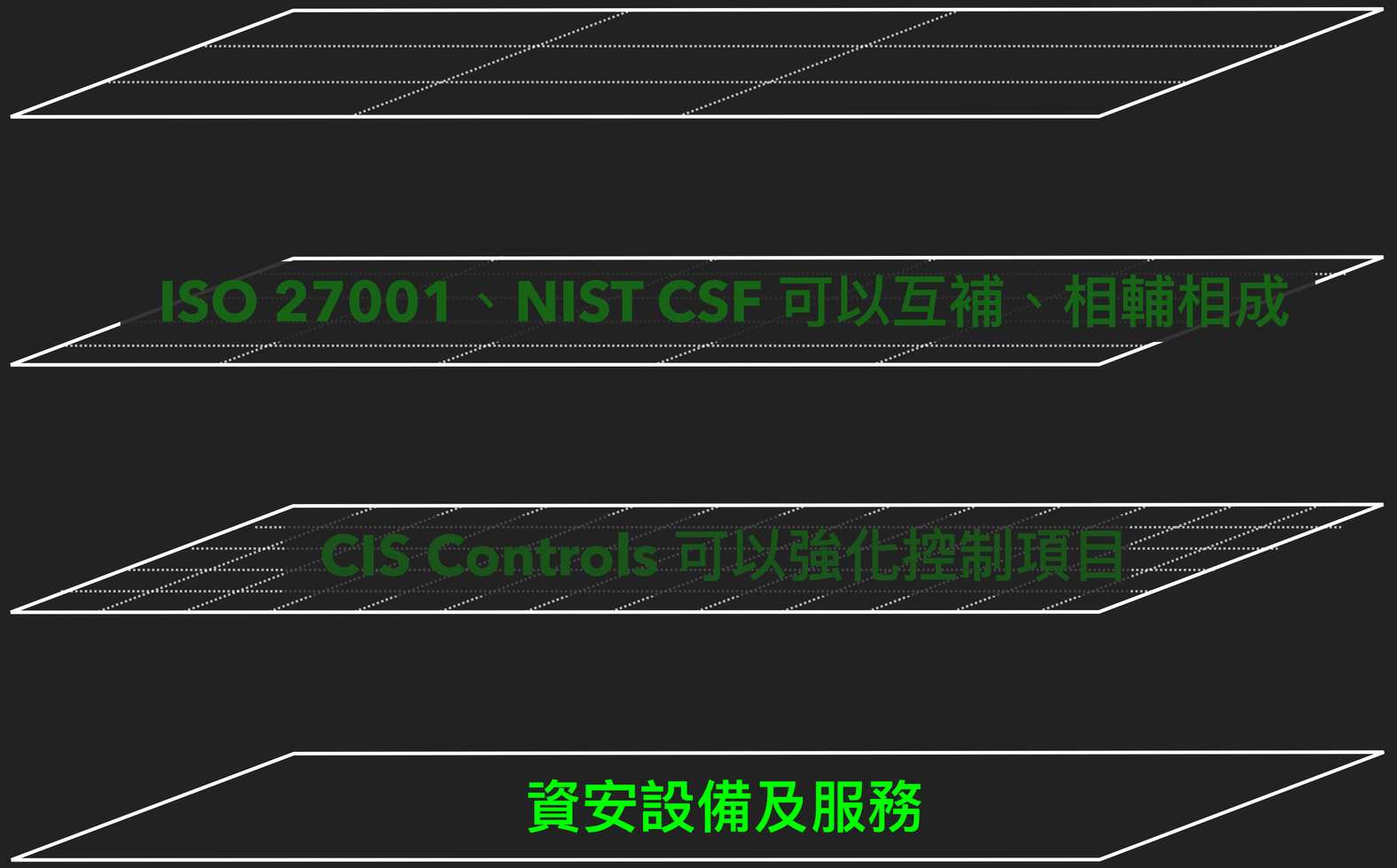
PROCEDURE

Controls Frameworks

- NIST 800-53
- CIS Controls

TECHNOLOGY VIEW

Defense Appliance / Service



EXECUTIVE

Risk Frameworks

- NIST 800-39、NIST 800-30
- ISO 27005
- CIS RAM

PROCESS

Program Frameworks

- NIST CSF
- ISO 27001

PROCEDURE

Controls Frameworks

- NIST 800-53
- CIS Controls

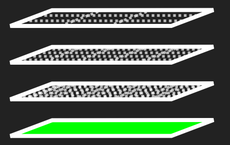
TECHNOLOGY VIEW

Defense Appliance / Service

資安頂級終極無敵解決方案

買了廠商說的 100% 資安防禦無敵解決方案

可以解決什麼問題？



弱點掃描

滲透測試

資安頂級終極無敵解決方案

紅隊演練

DDoS 防護設備

防火牆

應用程式防火牆

入侵防禦系統

端點偵測及回應

BAS

SIEM

SOAR

威脅情資

垃圾郵件防護

網頁內容過濾

資安健診

多因子認證

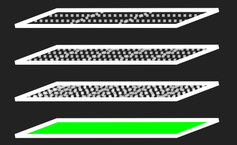
社交工程演練

ISO 27001 驗證

特權帳號管理

資安教育訓練

DEVCORE SECURITY CONSULTING



弱點掃描

滲透測試

資安頂級終極無敵解決方案

紅隊演練

BAS

DDoS 防護設備

SOAR

防火牆

入侵防禦系統

端點偵測及回應

SIEM

應用程式防火牆

威脅情資

垃圾郵件防護

網頁內容過濾

資安健診

多因子認證

社交工程演練

特權帳號管理

ISO 27001 驗證

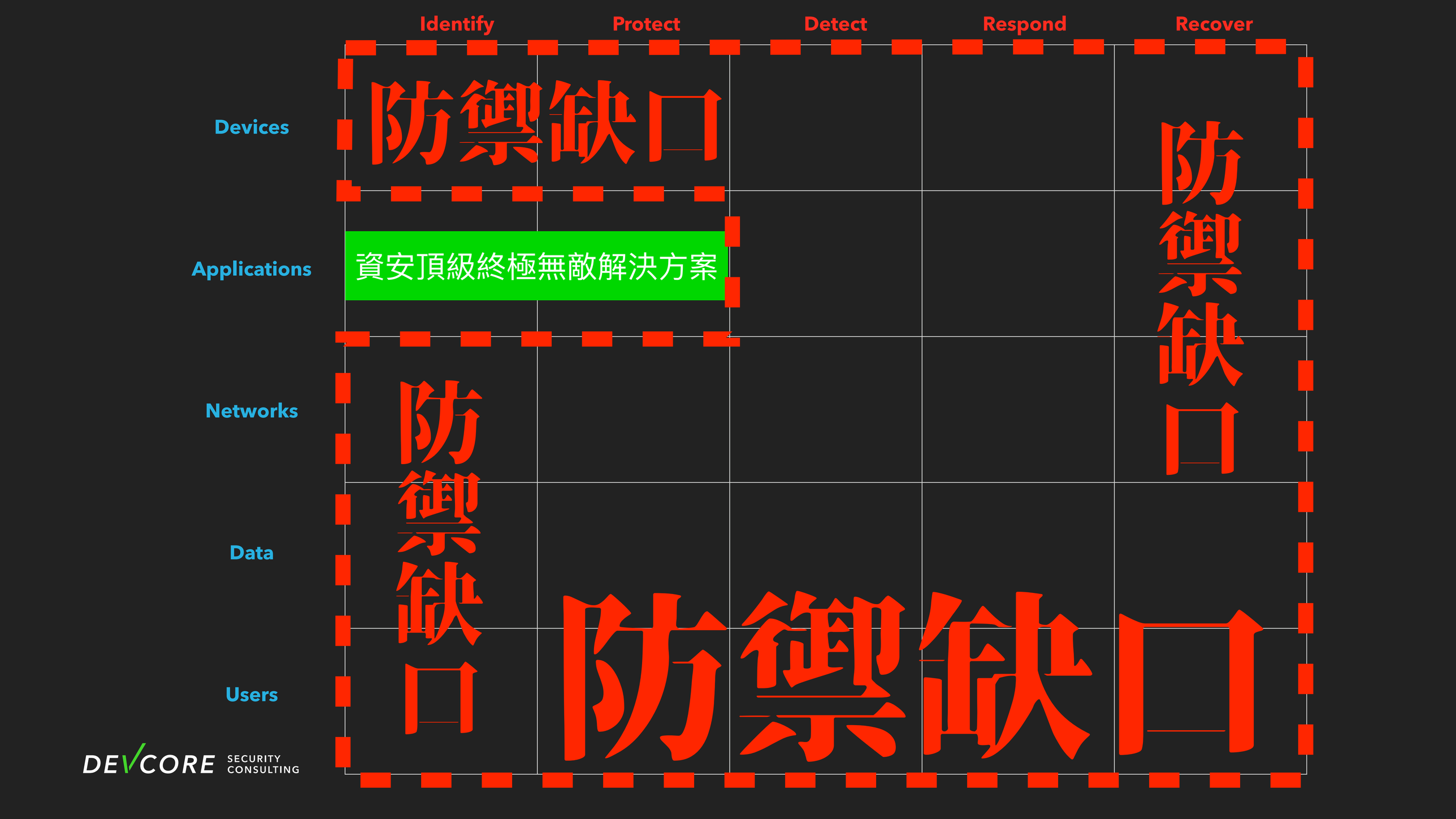
資安教育訓練

DEVCORE SECURITY CONSULTING

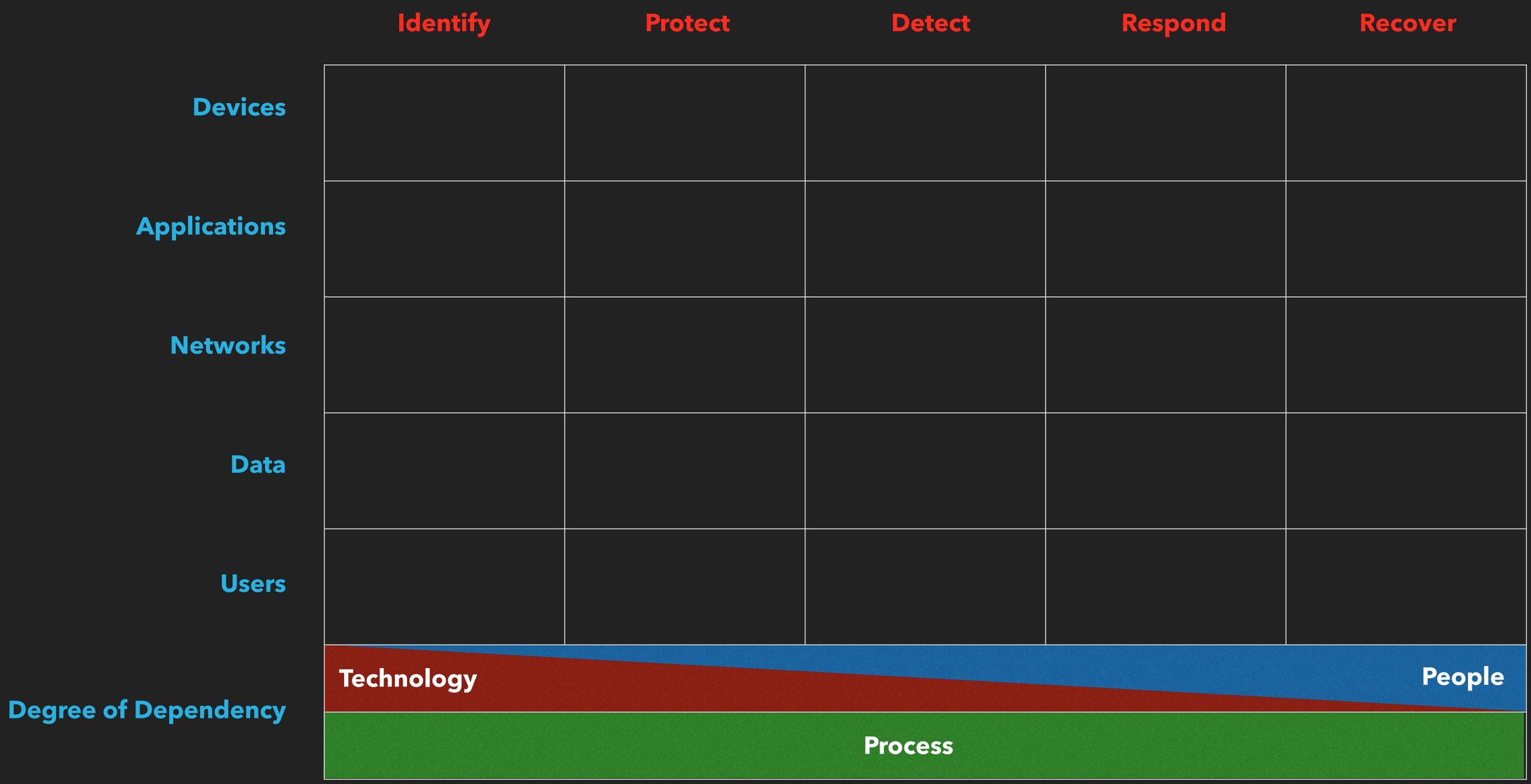
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications	資安頂級終極無敵解決方案				
Networks					
Data					
Users					

DEVCORE SECURITY CONSULTING


Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
資安頂級終極無敵解決方案
防禦缺口
DEVCORE SECURITY CONSULTING


Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
防禦缺口
防禦缺口
資安頂級終極無敵解決方案
防禦缺口
防禦缺口
防禦缺口
DEVCORE SECURITY CONSULTING

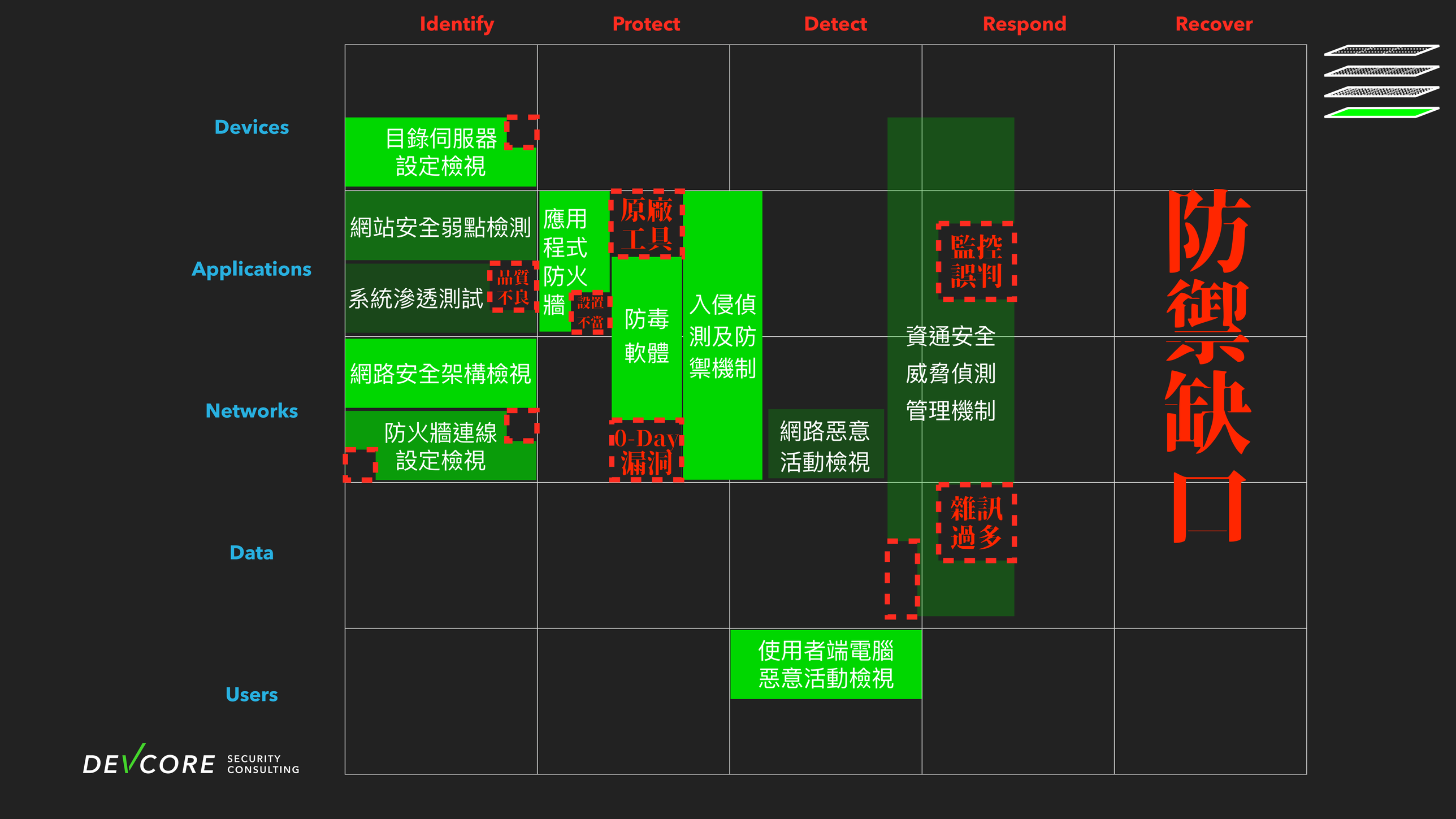
OWASP Cyber Defense Matrix

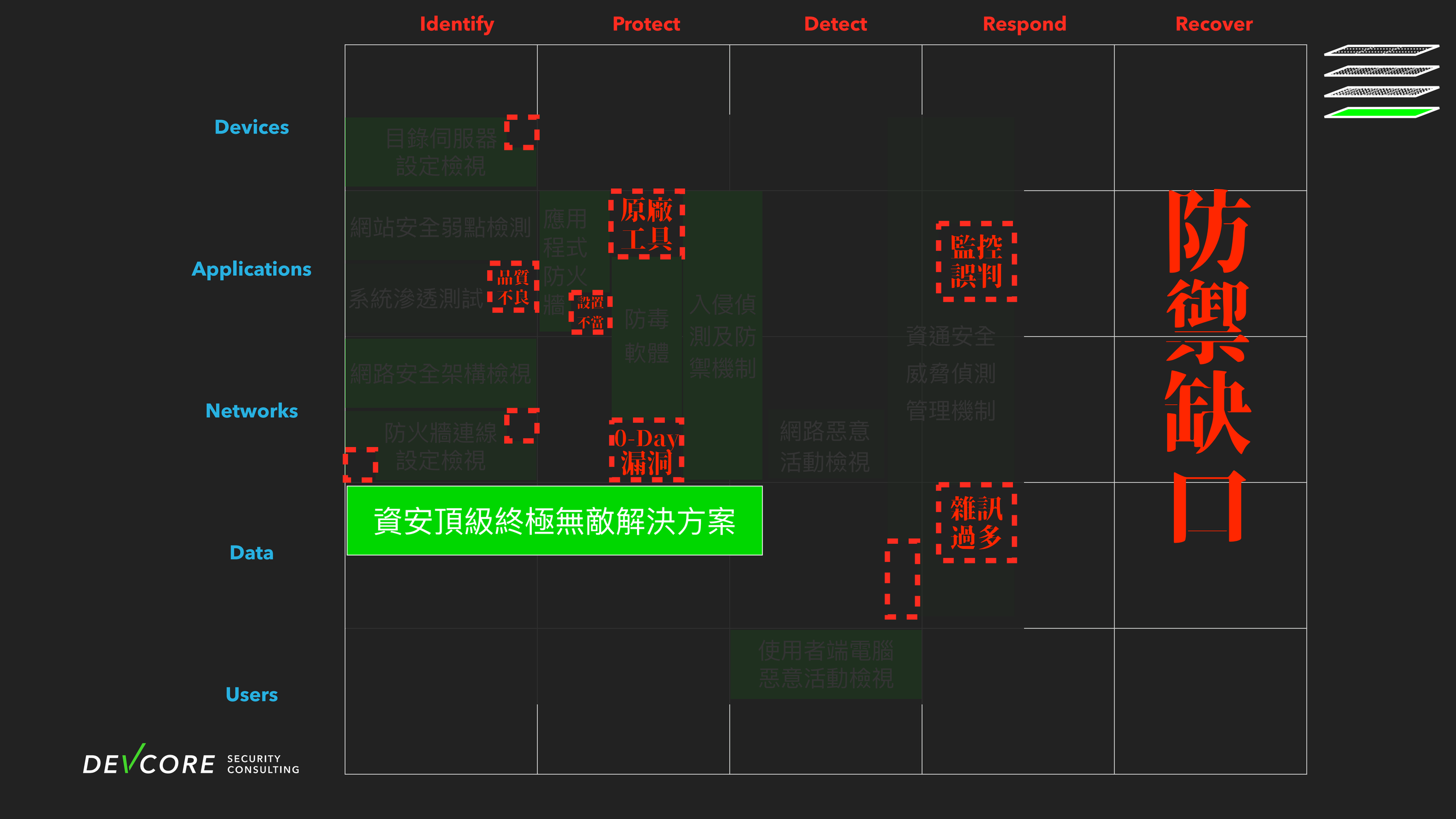


https://owasp.org/www-project-cyber-defense-matrix/

DEVCORE SECURITY CONSULTING


Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
目錄伺服器
設定檢視
網站安全弱點檢測
系統滲透測試
網路安全架構檢視
防火牆連線
設定檢視
應用
程式
防火
牆
防毒
軟體
入侵偵
測及防
禦機制
網路惡意
活動檢視
資通安全
威脅偵測
管理機制
專職人員教育訓練
使用者端電腦
惡意活動檢視
DEVCORE SECURITY CONSULTING


Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
目錄伺服器
設定檢視
網站安全弱點檢測
系統滲透測試
品質不良
網路安全架構檢視
防火牆連線
設定檢視
應用程式防火牆
設置不當
原廠工具
防毒軟體
0-Day漏洞
入侵偵測及防禦機制
網路惡意活動檢視
監控誤判
資通安全威脅偵測管理機制
雜訊過多
使用者端電腦惡意活動檢視
防禦缺口
DEVCORE SECURITY CONSULTING

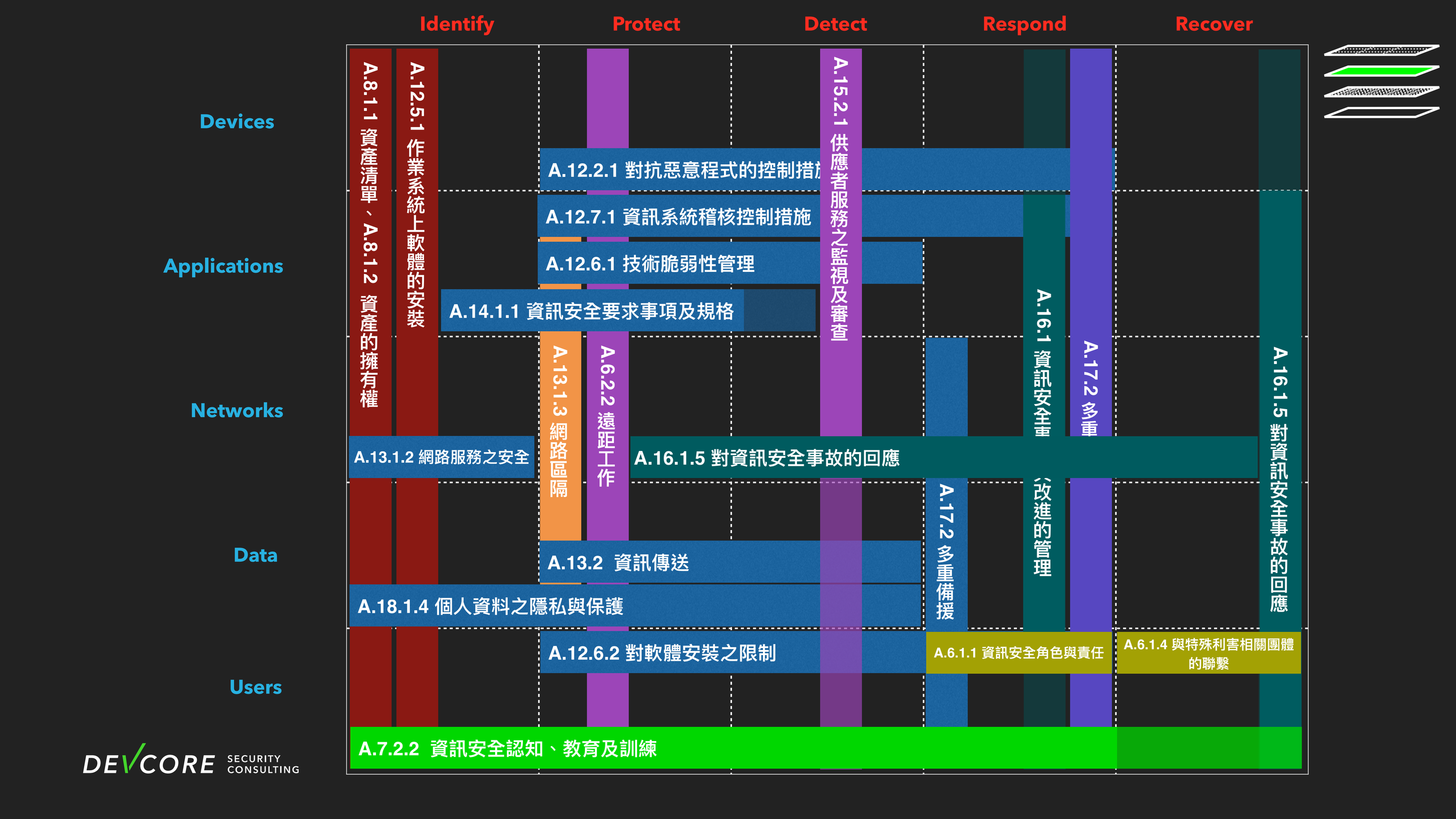

Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
目錄伺服器
設定檢視
網站安全弱點檢測
系統滲透測試
網路安全架構檢視
防火牆連線
設定檢視
應用
程式
防火
牆
防毒
軟體
入侵偵
測及防
禦機制
0-Day
漏洞
網路惡意
活動檢視
資通安全
威脅偵測
管理機制
使用者端電腦
惡意活動檢視
原廠
工具
品質
不良
設置
不當
監控
誤判
雜訊
過多
防禦缺口
資安頂級終極無敵解決方案
DEVCORE
SECURITY
CONSULTING

透過現有的基礎評估更多強化的可能性

- 以現有的標準或框架為基礎
- 挑選同類型視角 (view) 作為互補
  ex：用 CSF 對應 27001
- 從控制措施往上對應支援的流程
  ex：用 CSC 對應 27001
- 用設備及服務補足技術層的不足

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

www.nist.gov/cyberframework/framework



DEVCORE SECURITY CONSULTING

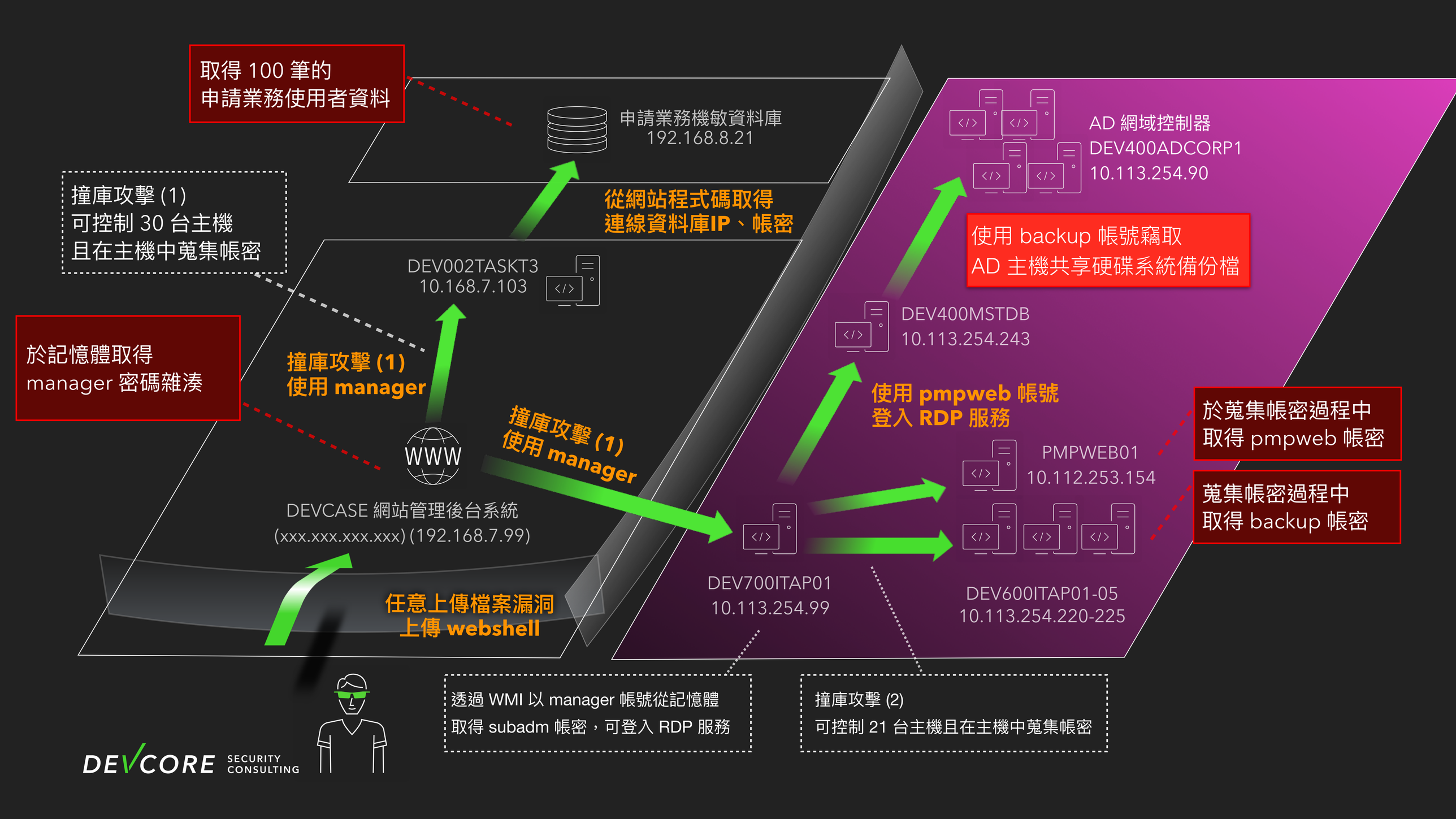
CIS CSC 搭配 CDM

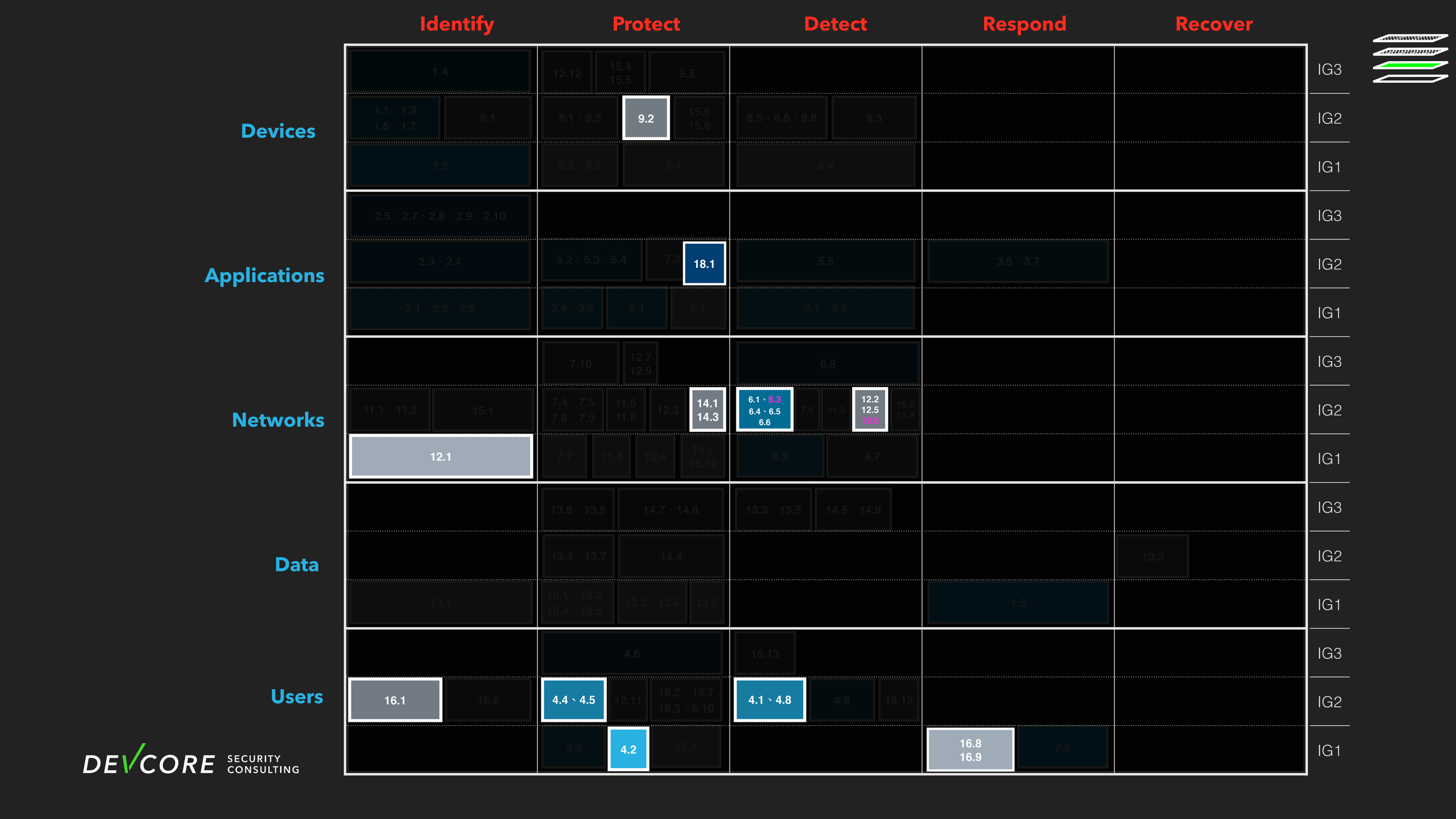
- 基本型：1-6 控制群組
- 基礎型：7-16 控制群組
- 組織型：17-20 控制群組
- IG1：中小型企業、有限的 IT 資產、資料敏感性低、非針對式攻擊
- IG2：中、大型企業、需要保護及管理 IT 基礎設施、保護客戶機敏資料
- IG3：超大型企業、專業分工、機敏資料多、具有法規要求必須保護的資料，遭受攻擊將影響社會發展

DEVCORE SECURITY CONSULTING

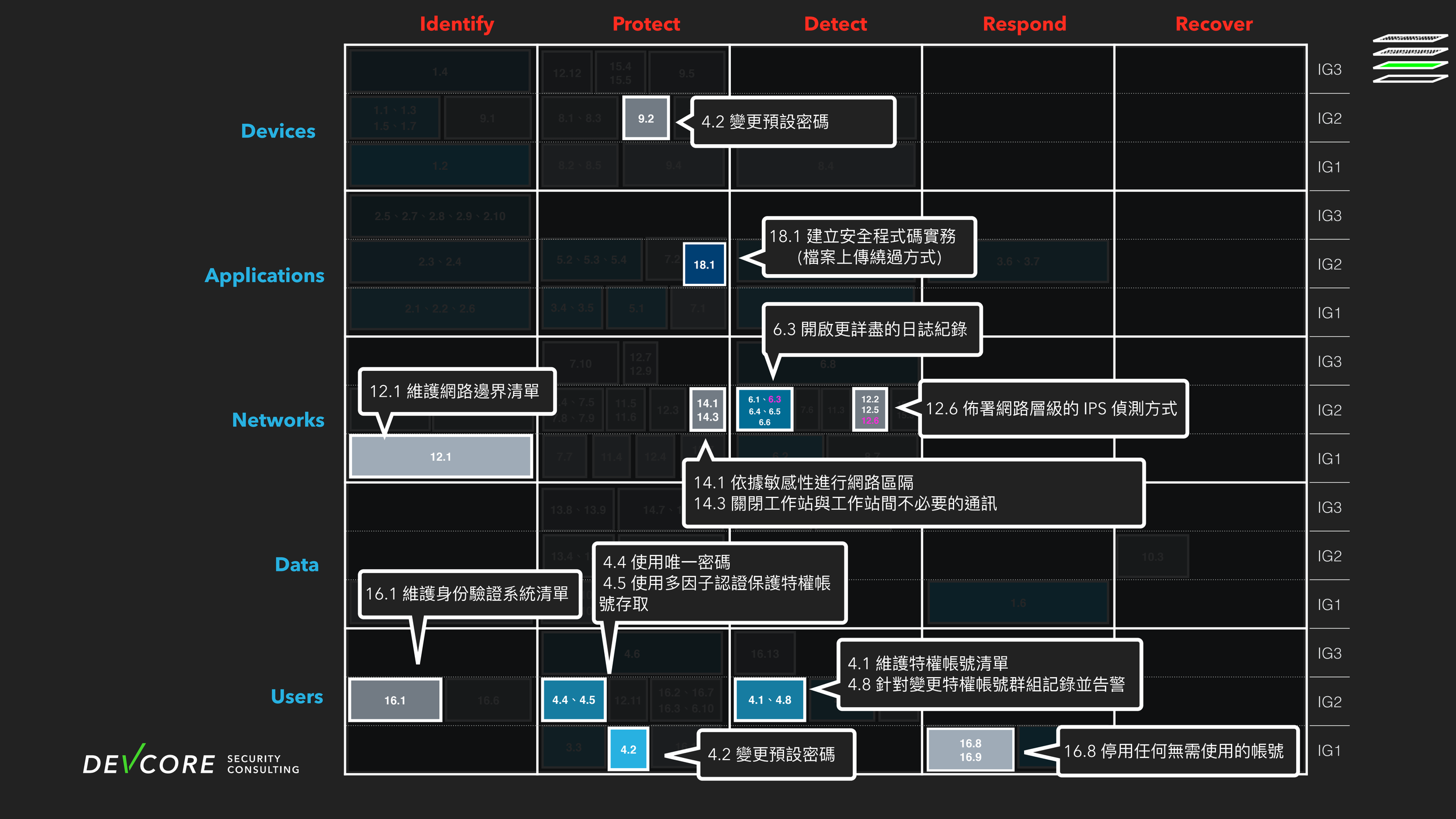
	Identify	Protect	Detect	Respond	Recover	
IG3	1.4	12.12 / 15.4 15.5 / 9.5				Devices
IG2	1.1、1.3 1.5、1.7 / 9.1	8.1、8.3 / 9.2 / 15.6 15.9	8.5、8.6、8.8 / 9.3			
IG1	1.2	8.2、8.5 / 9.4	8.4			
IG3	2.5、2.7、2.8、2.9、2.10					Applications
IG2	2.3、2.4	5.2、5.3 5.4 / 7.2、7.3 / 18.1	5.5	3.6、3.7		
IG1	2.1、2.2、2.6	3.4、3.5 / 5.1 / 7.1	3.1、3.2			
IG3		7.10 / 12.7、12.9 12.10 / 15.8	6.8			Networks
IG2	11.1、11.2 / 15.1	7.4、7.5 7.8、7.9 / 11.5 11.6 / 12.3 / 14.1 14.2	6.1、6.3、6.4 6.5、6.6、6.7 / 7.6 / 11.3 / 12.2 12.5 12.6 / 15.2 15.3			
IG1	12.1	7.7 / 11.4 / 12.4 / 15.7 15.10	6.2 / 8.7			
IG3		13.8、13.9 / 14.7、14.8	13.3、13.5 / 14.5、14.9			Data
IG2		13.4、13.7 / 14.4			10.3	
IG1	13.1	10.1、10.2 10.4、10.5 / 13.2、13.6 / 13.6		1.6		
IG3		4.6	16.13			Users
IG2	16.1 16.6	4.4、4.5 4.7 / 12.11 / 16.2、16.7 16.3、6.10	4.1、4.8、4.9 / 16.12			
IG1		3.3 / 4.2 4.3 / 16.1		16.8 16.9 / 2.6		

Case Study

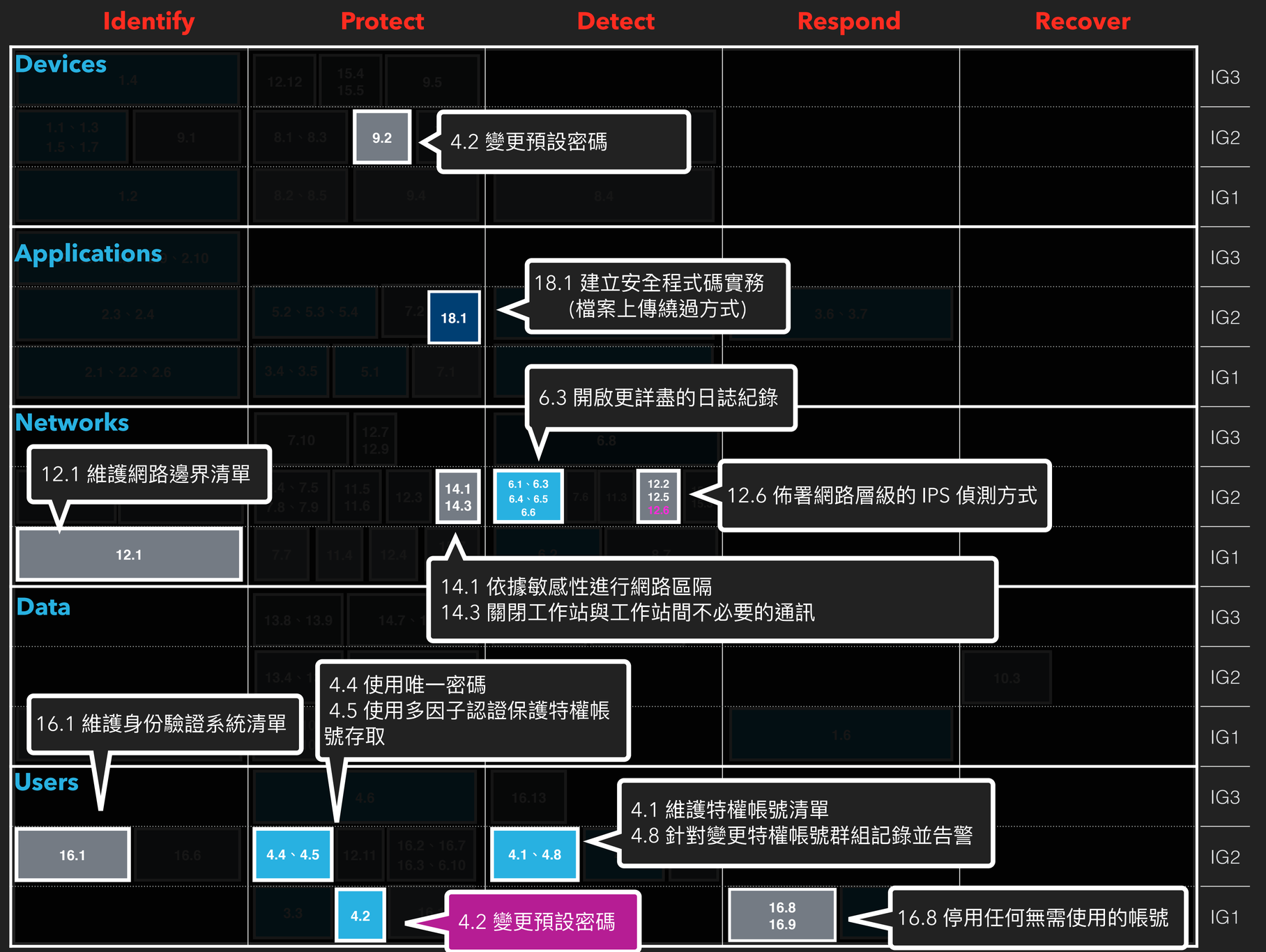

取得 100 筆的
申請業務使用者資料
申請業務機敏資料庫
192.168.8.21
撞庫攻擊 (1)
可控制 30 台主機
且在主機中蒐集帳密
從網站程式碼取得
連線資料庫IP、帳密
DEV002TASKT3
10.168.7.103
AD 網域控制器
DEV400ADCORP1
10.113.254.90
使用 backup 帳號竊取
AD 主機共享硬碟系統備份檔
DEV400MSTDB
10.113.254.243
於記憶體取得
manager 密碼雜湊
撞庫攻擊 (1)
使用 manager
使用 pmpweb 帳號
登入 RDP 服務
於蒐集帳密過程中
取得 pmpweb 帳密
WWW
撞庫攻擊 (1)
使用 manager
PMPWEB01
10.112.253.154
蒐集帳密過程中
取得 backup 帳密
DEVCASE 網站管理後台系統
(xxx.xxx.xxx.xxx) (192.168.7.99)
DEV700ITAP01
10.113.254.99
DEV600ITAP01-05
10.113.254.220-225
任意上傳檔案漏洞
上傳 webshell
透過 WMI 以 manager 帳號從記憶體
取得 subadm 帳密，可登入 RDP 服務
撞庫攻擊 (2)
可控制 21 台主機且在主機中蒐集帳密
DEVCORE SECURITY CONSULTING



DEVCORE SECURITY CONSULTING

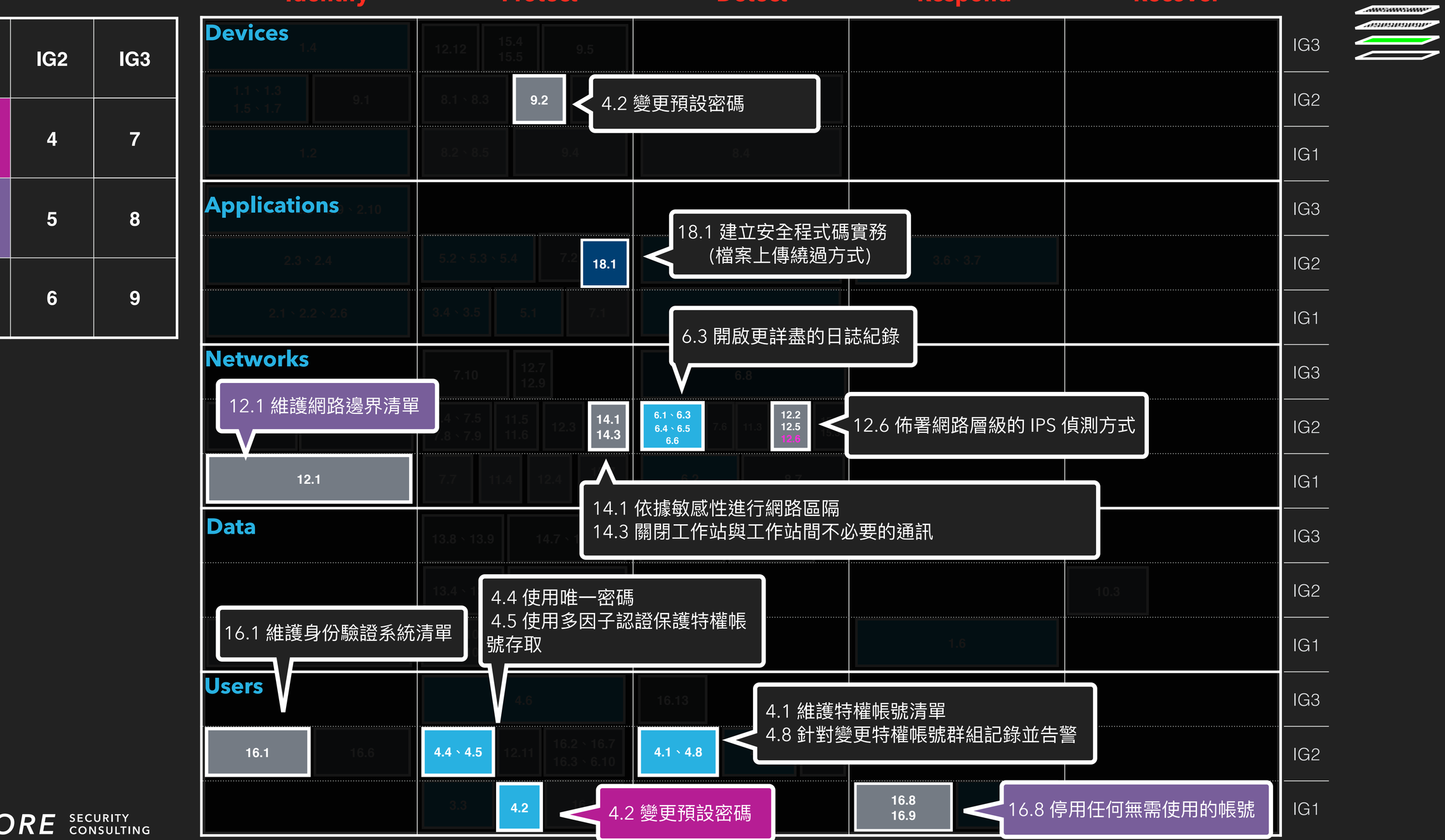

Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
IG3
IG2
IG1
9.2
4.2 變更預設密碼
18.1
18.1 建立安全程式碼實務
(檔案上傳繞過方式)
6.3 開啟更詳盡的日誌紀錄
12.1 維護網路邊界清單
12.1
14.1
14.3
6.1、6.3
6.4、6.5
6.6
12.2
12.5
12.6
12.6 佈署網路層級的 IPS 偵測方式
14.1 依據敏感性進行網路區隔
14.3 關閉工作站與工作站間不必要的通訊
4.4 使用唯一密碼
4.5 使用多因子認證保護特權帳號存取
16.1 維護身份驗證系統清單
16.1
4.4、4.5
4.1、4.8
4.1 維護特權帳號清單
4.8 針對變更特權帳號群組記錄並告警
4.2
4.2 變更預設密碼
16.8
16.9
16.8 停用任何無需使用的帳號
DEVCORE SECURITY CONSULTING

	IG1	IG2	IG3
基本型 1-6	1	4	7
基礎型 7-16	2	5	8
組織型 17-20	3	6	9



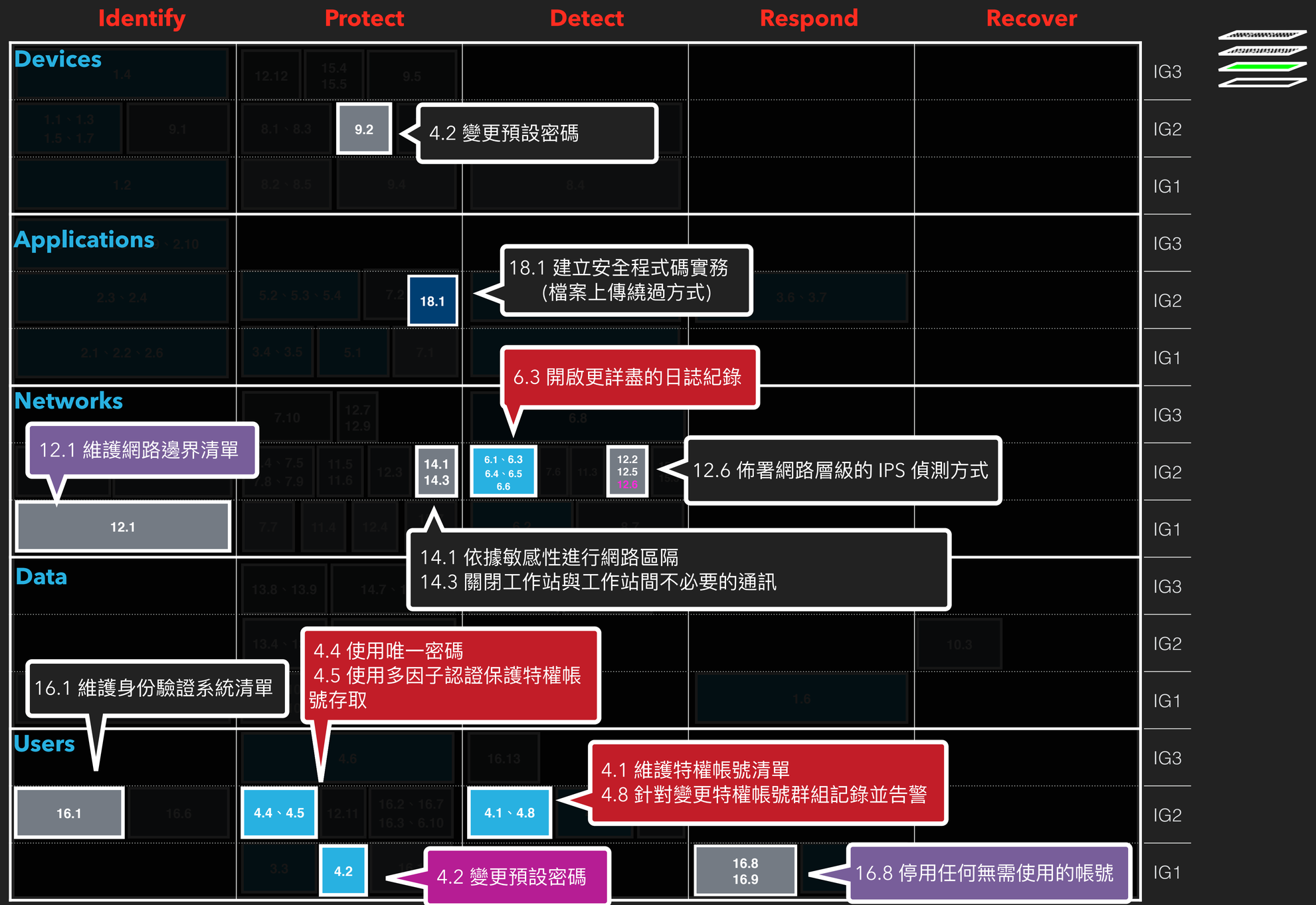
DEVCORE SECURITY CONSULTING

	IG1	IG2	IG3
基本型 1-6	1	4	7
基礎型 7-16	2	5	8
組織型 17-20	3	6	9



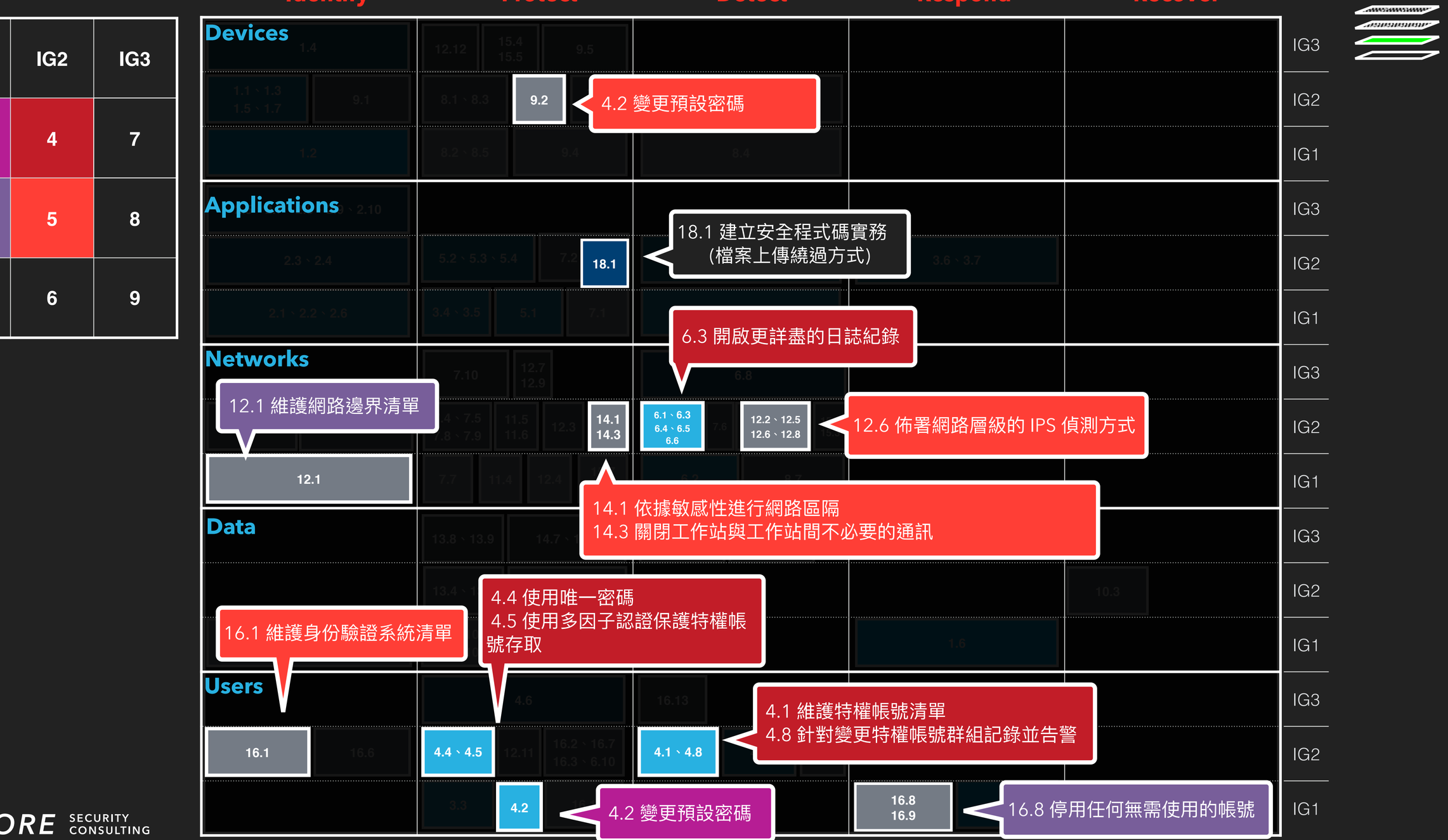
DEVCORE SECURITY CONSULTING

	IG1	IG2	IG3
基本型 1-6	1	4	7
基礎型 7-16	2	5	8
組織型 17-20	3	6	9



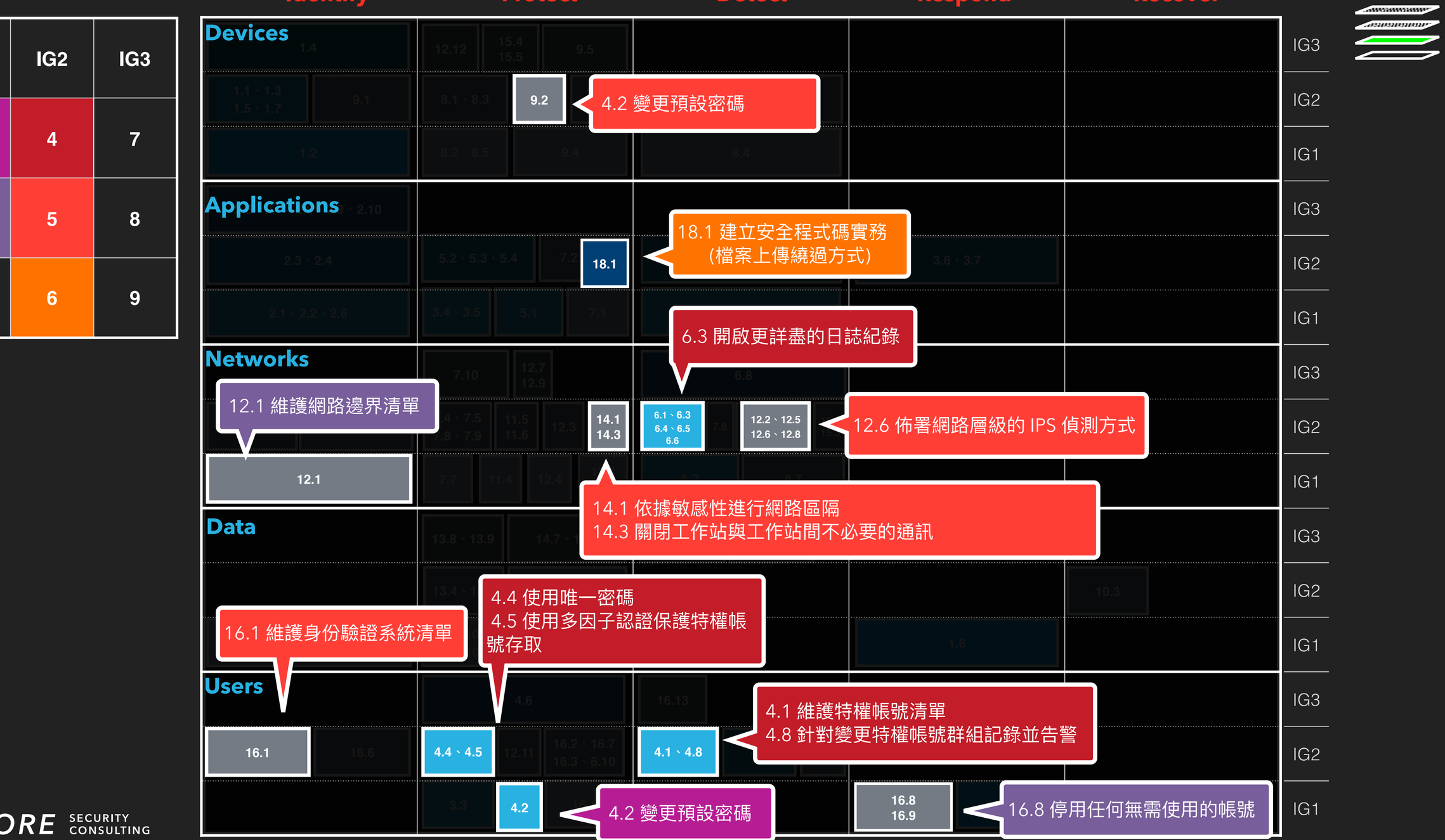
DEVCORE SECURITY CONSULTING

	IG1	IG2	IG3
基本型 1-6	1	4	7
基礎型 7-16	2	5	8
組織型 17-20	3	6	9



DEVCORE SECURITY CONSULTING

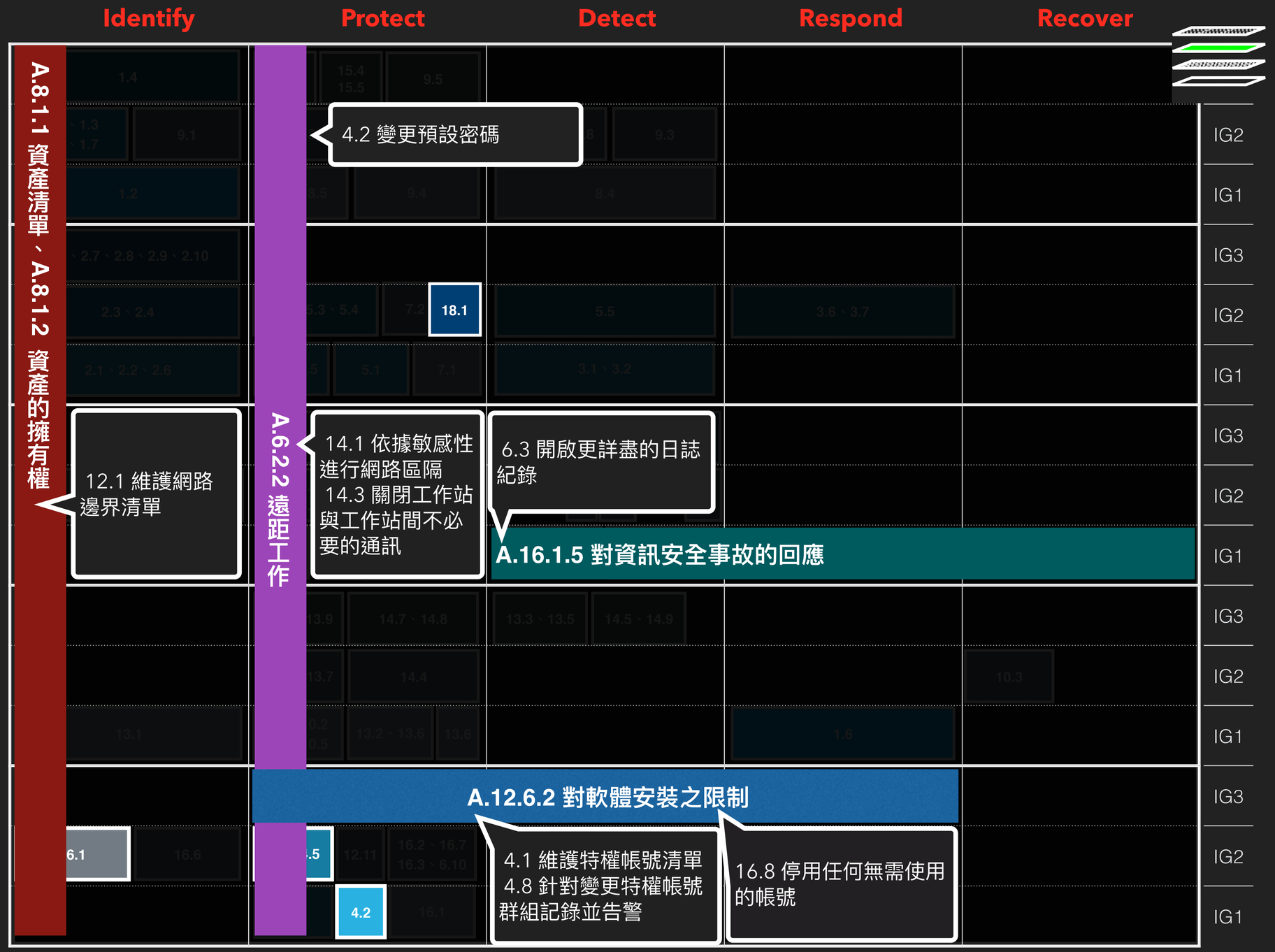
	IG1	IG2	IG3
基本型 1-6	1	4	7
基礎型 7-16	2	5	8
組織型 17-20	3	6	9



DEVCORE SECURITY CONSULTING

控制措施層對應到程序層

- 找出缺少的程序
- 發現待補強的防禦縱深機制
- 設備 + 程序 + 流程才能降低弱點被利用的可能性



DEVCORE SECURITY CONSULTING

回饋至風險評鑑

藉由 CSC 盤點的弱點

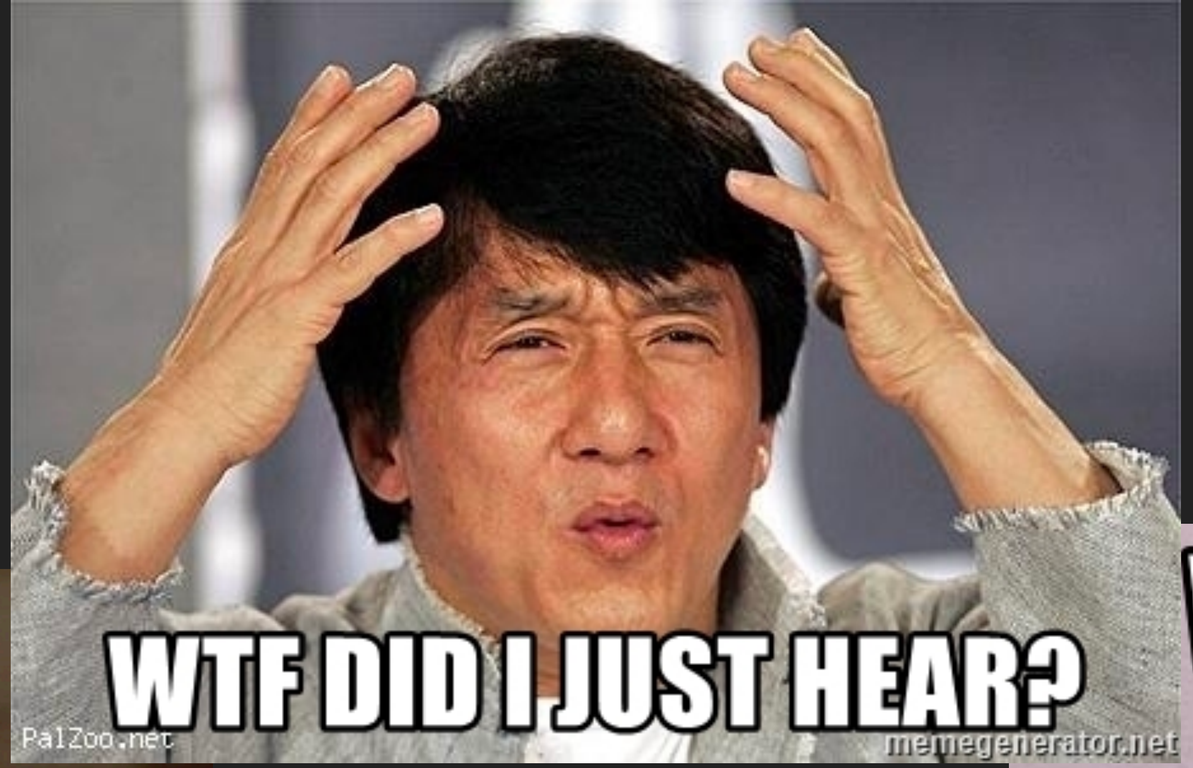
透過資安事件、稽核、紅隊演練
判斷情勢，反應真實威脅

資產名稱	資產價值	威脅	弱點	衝擊等級	可能性	風險等級	控制措施降低可能性	企業承受的風險
SW - 核心系統	3	網站攻擊	程式撰寫不良	3	1	9	3	27
SW - 核心系統	3	勒贖軟體	預設密碼	3	2	18	3	27
SW - 核心系統	3	網站攻擊	網路分隔不良	3	2	18	3	27
DA - 重要電子紀錄	2	勒贖軟體	RDP 攻擊	2	2	8	3	12
DA - 重要電子紀錄	2	勒贖軟體	社交工程	2	2	8	2	8
SW - 內部老舊系統	1	網站攻擊	無法上 patch	2	2	4	2	4

安全層次 (Security Level)

安全層次	方式	優點	缺點
基本安全 組織管理及維運安全	資安標準 資安框架	• 標準化、容易實作 • 提供基礎安全指引	不易反映真實威脅
基礎安全 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	• 無法反映組織全貌 • 不易呈現漏洞組合利用
組織型安全 防範已知攻擊、針對曾發生的資安事故進行改善	BAS	• 完全真實 • 確認當下控制措施、管理及維運狀況	• 不易掌握全貌 • 不易重現攻擊
強韌型安全 防範未知或針對式攻擊	紅隊演練 資安事故	• 針對特定攻擊類型優先驗證 • 節省資源	不易辨識出攻擊者族群及手法
真實型安全 最大化安全防護	紅隊演練 資安事故	最大化發現可能的問題，如：設備組態、人員疏失、管理制度	全面性系統問題，不易於短時間解決

大家剛剛學到了什麼？


WTF DID I JUST HEAR?
PalZoo.net
memegenerator.net


DAFUQ
DID I JUST HEAR?
memegenerator.net


WTF DID I
JUST HEAR
memegenerator.net

大家剛剛學到了什麼？

幫各位複習一下。

EXECUTIVE

Risk Frameworks (SANS)

- NIST 800-39、NIST 800-30
- ISO 27005、CIS RAM

PROCESS

Program Frameworks (SANS)

- NIST Cybersecurity Framework
- ISO 27001

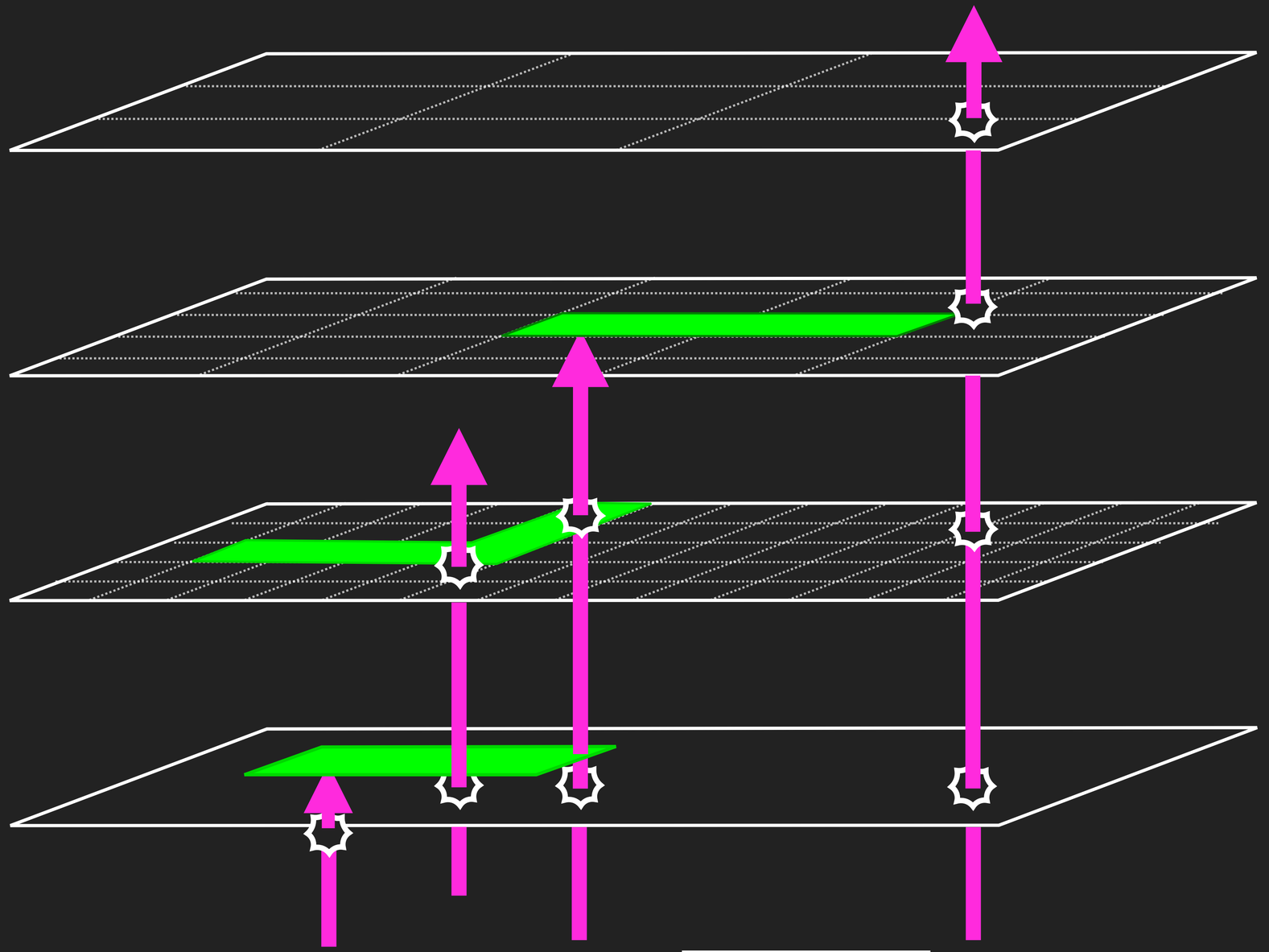
PROCEDURE

Controls Frameworks (SANS)

- NIST 800-53
- CIS Critical Security Controls

TECHNOLOGY VIEW

Defense Appliance / Service



EXECUTIVE

Risk Frameworks (SANS)

- NIST 800-39、NIST 800-30
- ISO 27005、CIS RAM

PROCESS

Program Frameworks (SANS)

- NIST Cybersecurity Framework
- ISO 27001

PROCEDURE

Controls Frameworks (SANS)

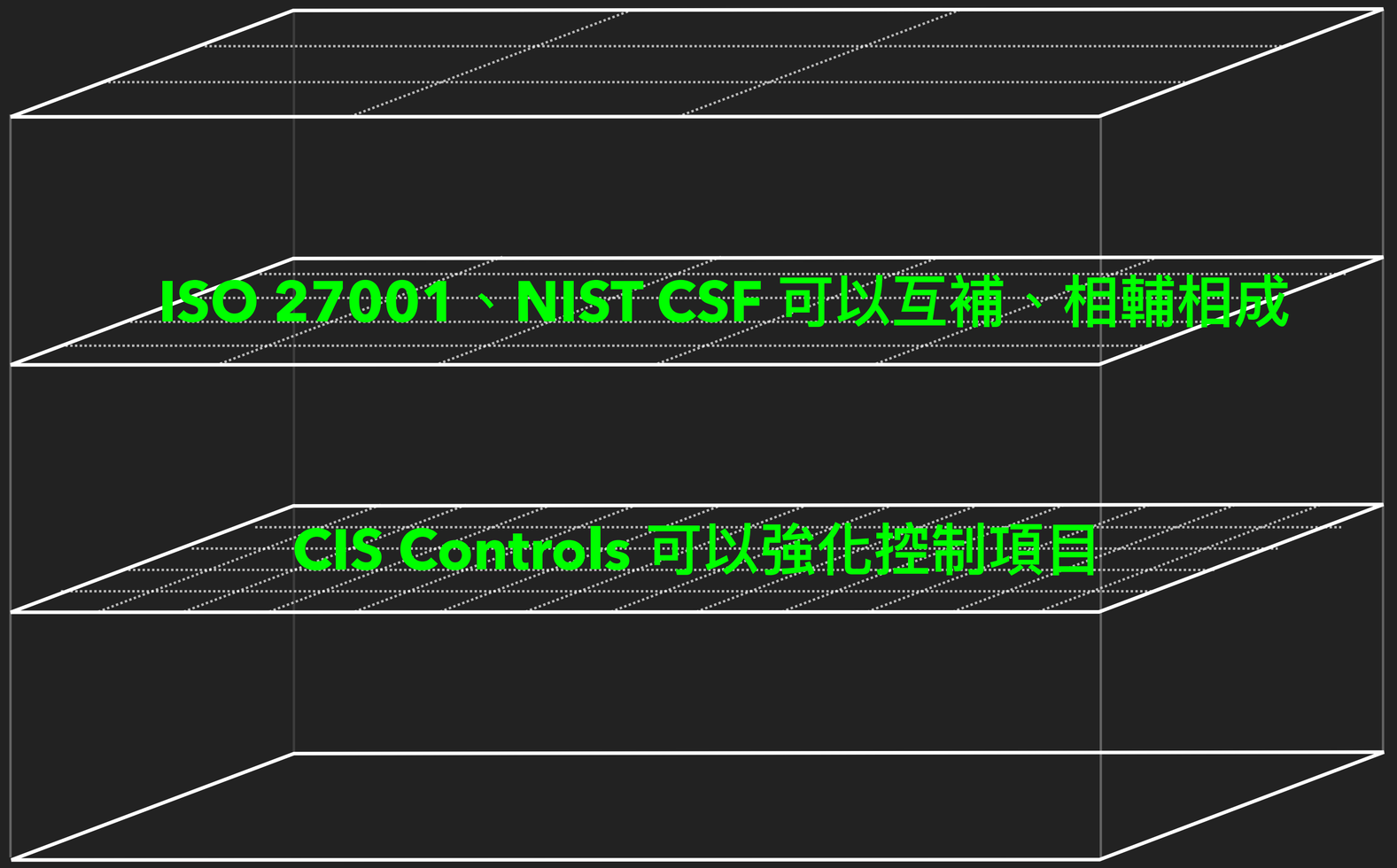
- NIST 800-53
- CIS Critical Security Controls

TECHNOLOGY VIEW

Defense Appliance / Service

DEVCORE SECURITY CONSULTING

ATTACKER'S VIEW **MITRE ATT&CK**



EXECUTIVE

Risk Frameworks (SANS)

- NIST 800-39、NIST 800-30
- ISO 27005、CIS RAM

PROCESS

Program Frameworks (SANS)

- NIST Cybersecurity Framework
- ISO 27001

PROCEDURE

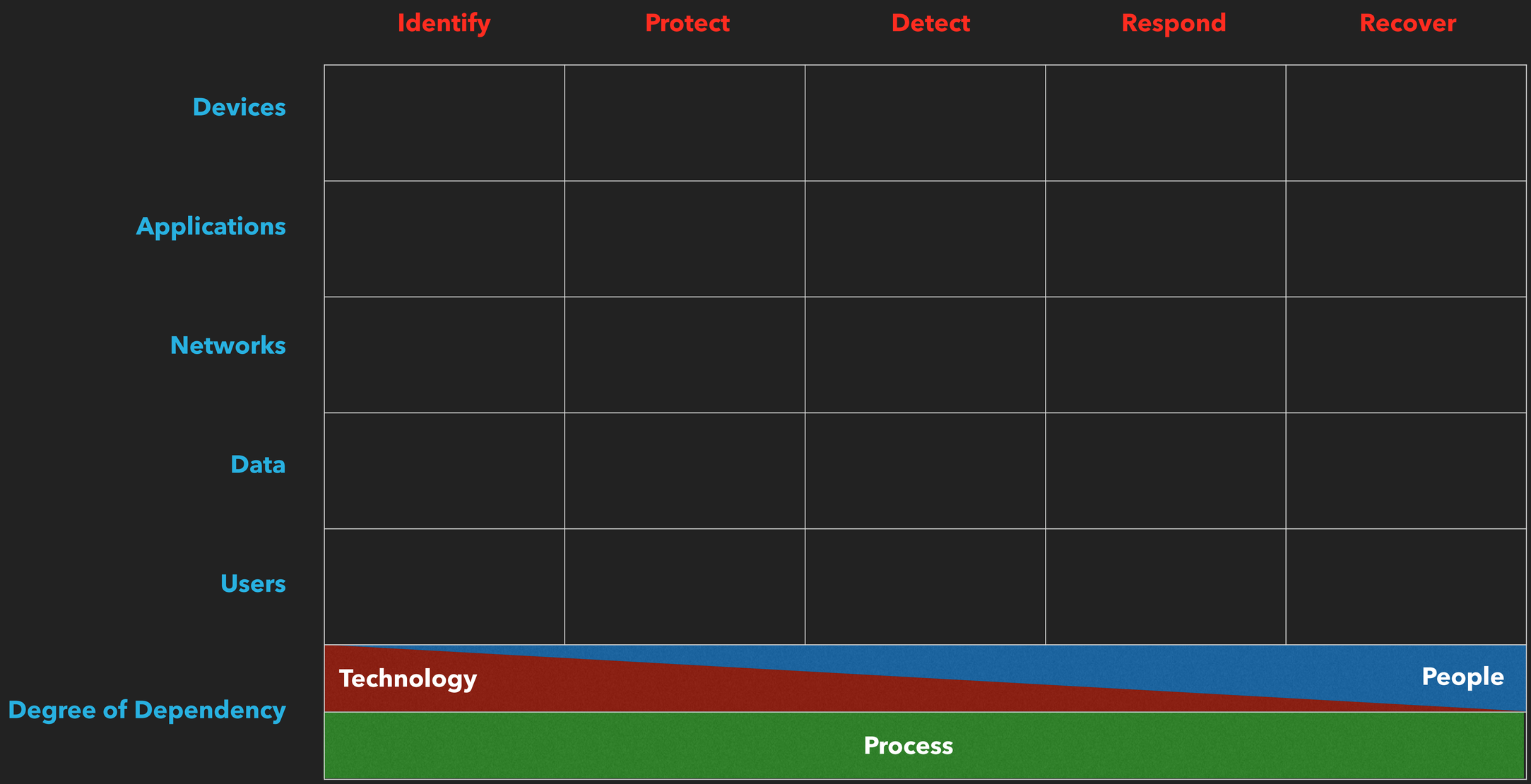
Controls Frameworks (SANS)

- NIST 800-53
- CIS Critical Security Controls

TECHNOLOGY VIEW

Defense Appliance / Service

OWASP Cyber Defense Matrix

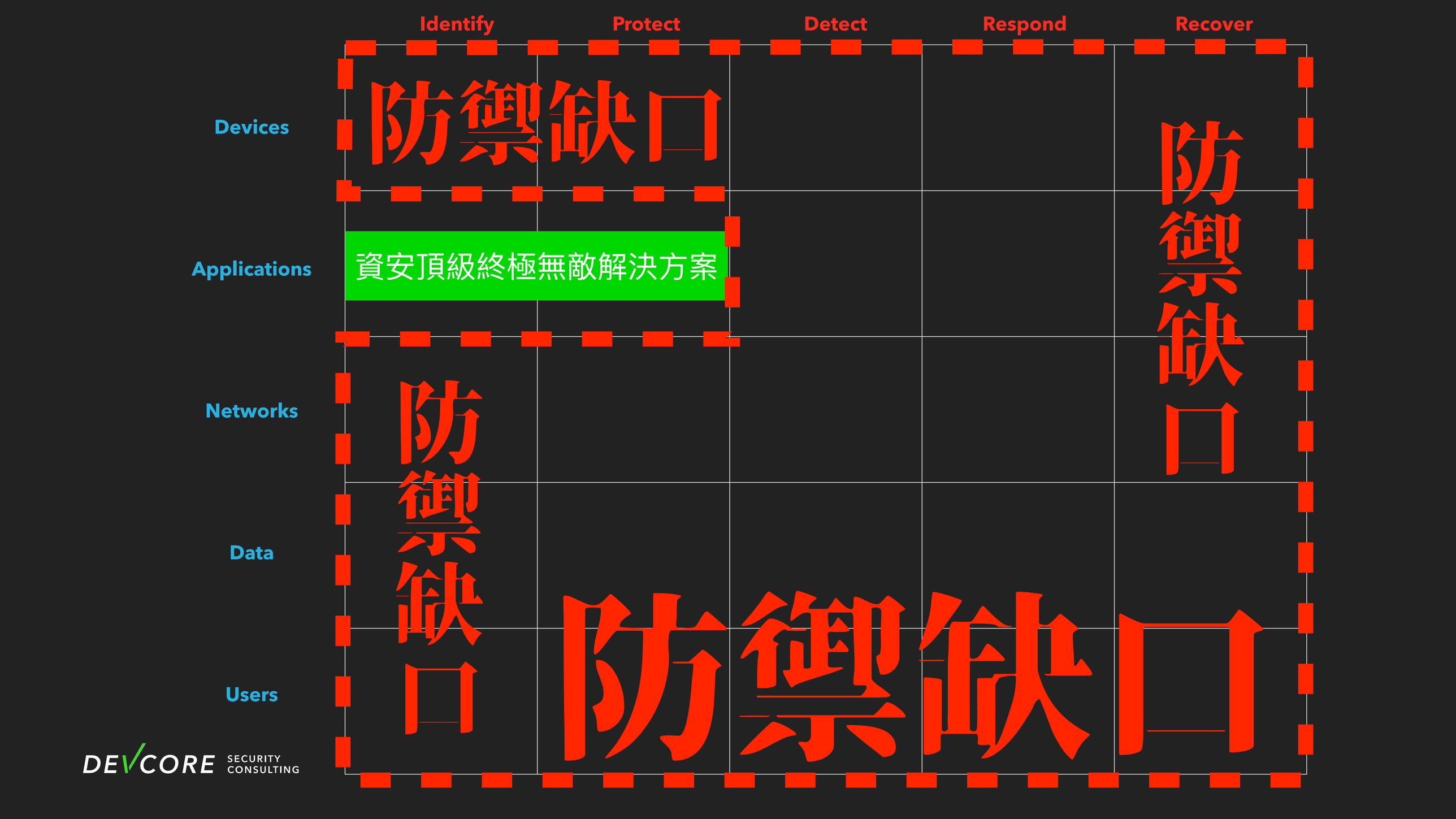


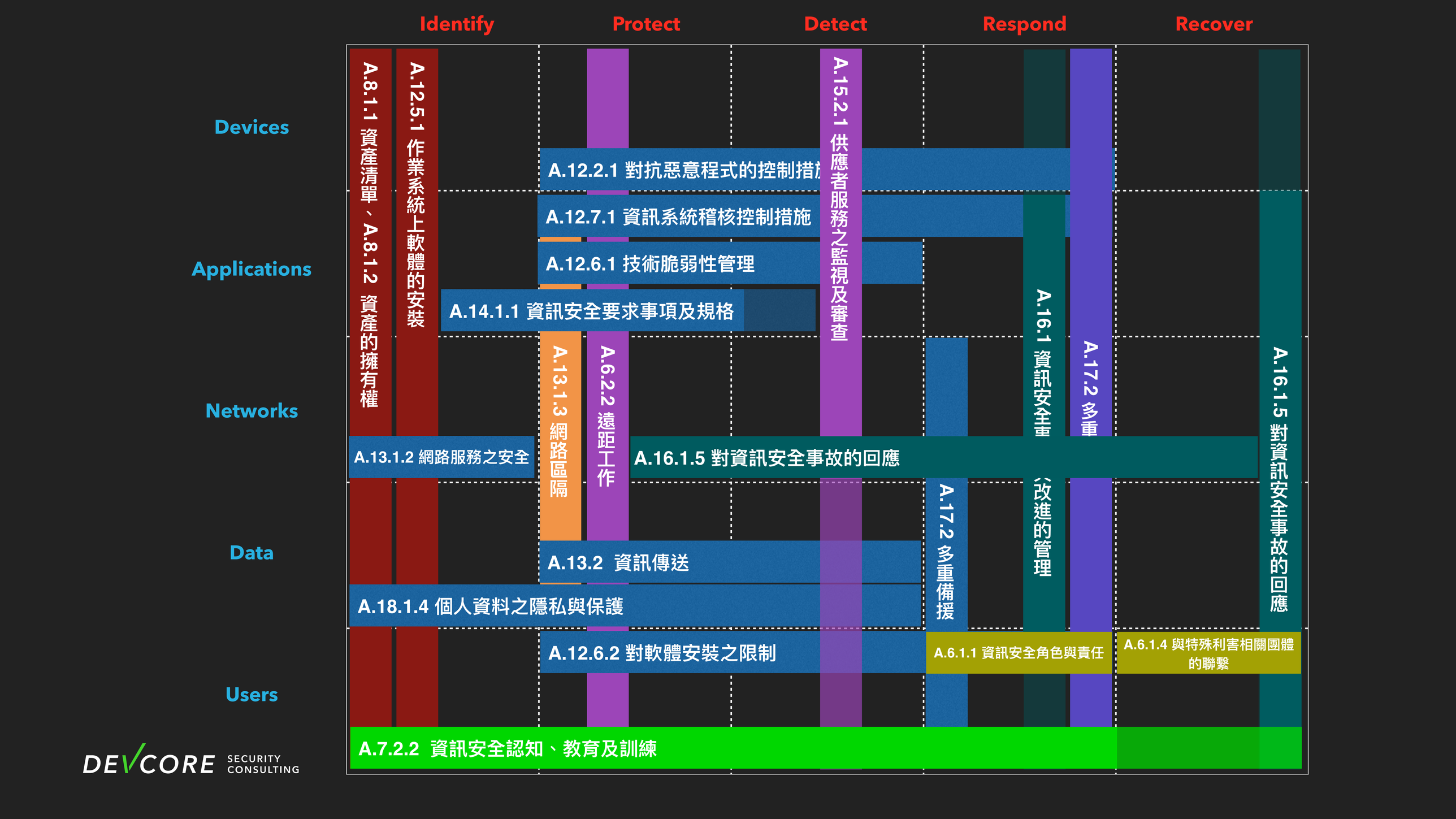
https://owasp.org/www-project-cyber-defense-matrix/

DEVCORE SECURITY CONSULTING

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications	資安頂級終極無敵解決方案				
Networks					
Data					
Users					

DEVCORE SECURITY CONSULTING


Identify
Protect
Detect
Respond
Recover
Devices
Applications
Networks
Data
Users
防禦缺口
防禦缺口
資安頂級終極無敵解決方案
防禦缺口
防禦缺口
防禦缺口
DEVCORE SECURITY CONSULTING



DEVCORE SECURITY CONSULTING

Takeaways

- 資安不能一直應急（短期），要放遠規劃（中長期）
- 資安策略很重要，活用框架工具幫助你擬定長期資安策略
- 資安策略要由上往下規劃，由下往上回顧精進
- 框架與標準沒有絕對，重點在使用的方法
- Special thanks to PK & HITCON Review Board

DEVCORE
SECURITY
CONSULTING

重新檢視你的防禦現況，
建構真實威脅下的防禦策略

Q&A

戴夫寇爾股份有限公司
contact@devco.re
02-2718-0156