淺介Cyber-Defense Matrix（CDM）

蘇柏鳴 / 金融聯合徵信中心 資安部

Cyber-Defense Matrix這是由曾經在美國銀行擔任首席安全科學家的Sounil Yu在2016 RSA Conference所發表的一種安全模型，是一個檢視企業內部資安整體狀況很好的方法論，以更全面的方式檢視目前資安防護是否有缺漏或重複投資的部分；該模型結合了NIST Cybersecurity Framework（CBF）[1]的操作功能：識別（Identify）、保護（Protect）、檢測（Detect）、回應（Respond）和恢復（Recover），並新增了資產類別：設備（Device）、應用程序（Application）、網絡（Network），數據（Data）和使用者（User）。

所謂「工欲善其事，必先利其器」，資安防護也必須依靠資安產品供應商的支援，但市面上的資安相關產品眾多，我們很難對於資安產品所能提供的效益有效地用一個方法及準則來評估，造成在產品購買上的困難，為解決這狀況，可以透過Cyber-Defense Matrix 5X5的矩陣，將所有已導入之資安產品/防護歸入其中，讓產品屬性及功能面可以一目瞭然，在RSA Conference 2020中，前美國銀行首席安全科學家Sounil Yu的簡報裡將資安防護產品類型作了以下分類示範（如圖1）。

資安防護產品分類示範

1. 識別（Identify）

Configuration管理、漏洞掃描器（Vulnerability Scanner）、靜態應用程式安全（SAST）、動態應用程式安全測試（DAST）、資產管理系統（Asset Management）、模糊測試（Fuzz testing）、Data Audit、Data Discovery、Data Classification、網路漏洞掃描、電子郵件社交工程演練（Phishing）。

2. 保護（Protect）

身分識別與存取管理（IAM）、主機入侵防禦系統（HIPS）、網頁應用系統防火牆（Web Application Firewall，WAF）、程式執行階段自我保護（Runtime Application Self-protection，RASP）、防火牆、入侵偵測系統（Intrusion Detection System，

1 https://www.nist.gov/cyberframework/framework。

IDS）、入侵預防系統（Intrusion Prevention System，IPS）、代碼化技術（Tokenization）、資料遺失防護（Data Loss Prevention，DLP）、文件權限控管（DRM，Digital Rights Management）及安全意識（Security Awareness）。

3. 檢測（Detect）

端點偵測回應（Endpoint Detection and Response，EDR）、DDoS Mitigation、暗網偵測（Dark Web）、內部威脅（Inside Threat）、使用行為分析（Behavioral Analytics）。

4. 回應（Respond）

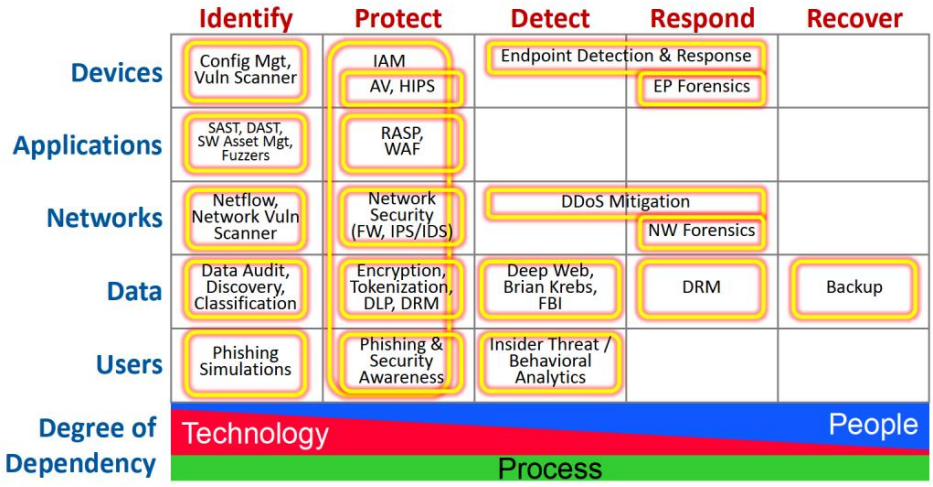
端點偵測回應（Endpoint Detection and Response，EDR）、DDoS Mitigation、端點及網路鑑識（Forensics）、文件權限控管（DRM，Digital Rights Management）。

5. 恢復（Recover）

資料備份（Data Backup）。

在圖中各式各樣的防護方式／產品類型被分配在這個矩陣中，因為有些防護方式是跨功能的，例如EDR產品不僅有偵測的功能，同時也能偵測威脅後做反應及處置。

圖 1 Cyber-Defense Matrix 範例



如前所述，Cyber-Defense Matrix是一個檢視企業內部資安整體狀況很好的方法論，以更全面的方式檢視目前資安防護是否有漏缺或重複投資的部分；舉例來說，假設目前組織已經有建置安全訊息和事件管理（Security Information Event Management，SIME）平台來蒐集日誌（Log），但目前市場上新型態的資安產品像是以色列的IntSights[2]及CyberInt，可以提供結合在暗網蒐集到的威脅情資，另外還有能高度自動化回應的SOAR（Security Orchestration, Automation and Response）平台，這時候就可以考量自己組織的需求，來評估是否引進這些更新型態的產品，防護效果跟整體防護的必要性跟緊急性是否為目前優先導入選項，畢竟不是每個企業都有預算把所有資安設備買齊，在預算有限的狀況瞭解自己組織面臨到主要的威脅是什麼，需要的是怎樣的防護等級及類型的產品，才能將資源最大效益化。

2 IntSights彙整暗網與內部動態，打造企業專屬威脅情。https://www.ithome.com/review/131827。