CYBERSEC 2024 臺灣資安大會淺介

蘇柏鳴 / 金融聯合徵信中心 資安部

一、CYBERSEC 2024 資安大會介紹

2024年的臺灣資安大會（CYBERSEC Taiwan 2024）於5月14日至16日在台北南港展覽二館舉行。這是該大會舉辦的第十屆，以「Generative Future」為主題，探討生成式AI及其對資安的影響。此次大會聚焦於AI驅動的演算法、IT架構及應用，帶來前所未有的資安挑戰，吸引超過18000名資安專業人士參加，是歷屆規模最大的一次。

（一）參展規模

(1)共有超過500家全球知名資安品牌參展。

(2)設有1300多個參展攤位，是亞洲規模最大的資安展。

（二）專業論壇和講座

(1)大會舉行超過300場專業演講，涵蓋各種最新的資安議題和技術。

(2)設有30個資安主題論壇，包括「CYBERSEC Global」、「CYBERSEC Arena 資安競技場」、「資安十年歷史牆」等。

（三）特色展區

(1)臺灣資安館：展示本土自主研發的資安技術和解決方案。

(2)Cyber Talent 資安人才專區：旨在培養和挖掘資安人才，促進專業發展。

(3)AIoT & Hardware Security Zone：探索智慧聯網和硬體安全的最新進展。

（四）參展企業

(1)國內企業：中華資安、池安量子、全景軟體、亞利安科技、中芯數據、奧義智慧科技、DEVCORE、達友科技、伊雲谷、鑒真數位、財團法人電信技術中心、工業技術研究院、數聯資安、可立可、邁達特、安碁資訊、Gogolook、聯宏科技、匯智安全科技、TeamT5、關貿網路、TRAPA Security、零壹科技…等。

(2)國外企業：Akamai、Bitdefender、Check Point、Palo Alto、Fortinet、Cloudflare、CrowdStrike、CyberArk、Cybereason、Darktrace、F5、Forcepoint、Forescout、illumio、Imperva、IBM、Proofpoint、Menlo、Microsoft、Keysight、radware、SentinelOne、Splunk、Trend Micro、Thales、SecurityScorecard、Zscaler…等。

圖1 資安十年歷史牆

二、專場演講分享

（一）AI 浪潮衝擊下，如何運用 Splunk 的AI賦能全方位處理各式資安攻擊

(1)講者：Daniel Yeung （Splunk技術經理）

(2)內容摘要

根據「Splunk CISO Report 2023[1]」內容指出，70%的資安長認為 AI 使攻擊者比防禦者更具優勢；還有35%已經在嘗試將其用於網路防禦；83%在勒索軟體攻擊之後向攻擊者付費（直接、通過網路保險或與談判者聯繫），其中超過一半的人至少支付了100,000 美元。

SIEM（Security Information and Event Management）指的是一種資安解決方案，用來集中各種資安產品所蒐集到的Log，進而整合事件告警、關聯分析、產出數據報表，甚至是採取自動化腳本回應等，以輔助資安人員更有效率地建立整體環境可視性並即時排除問題。

- 簡單的規則檢測事件並觸發警報：例如：身份驗證失敗後觸發警報。
- 關聯規則將兩個或多個規則／事件聯接起來，以提升準確檢測：例如在10分鐘內，使用不同使用者之名從同一主機到不同登入目標的多次身份驗證嘗試失敗。如果在

[1] Splunk CISO Report : https://www.splunk.com/en_us/form/ciso-report.html。

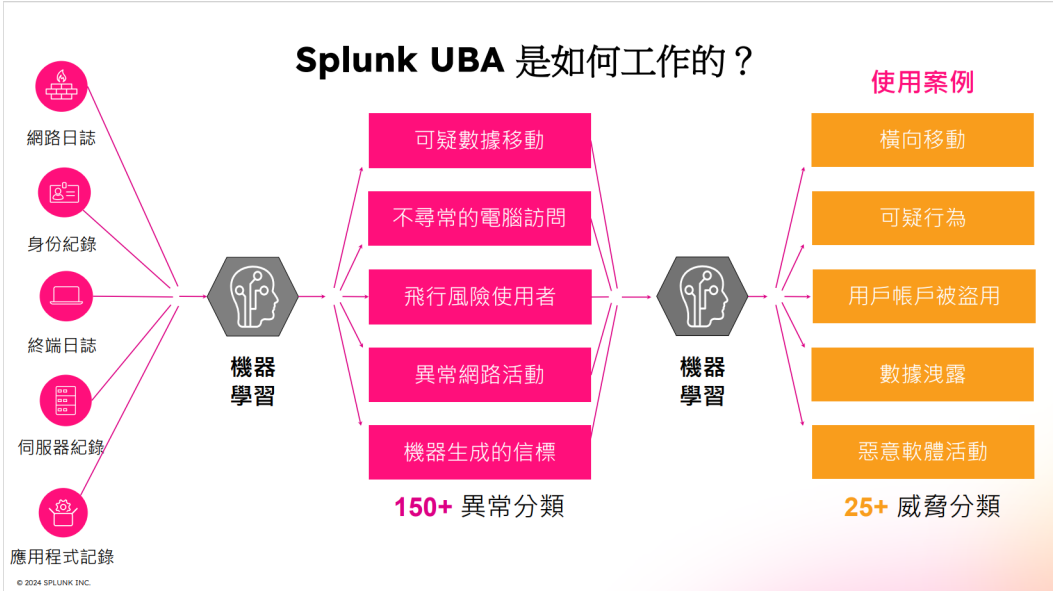
此台主機上於任一目標上成功登錄，將觸發警報。

很多組織目前制定的許多規則和政策都是無效的，CardinalOps[2]研究數據顯示，平均25%的SIEM規則不完整並且永遠不會觸發，這主要是由於未確定提取資料欄位或未發送所需數據的日誌資料，但是，組織完全沒有意識到這些規則不起作用。另外只有15%的SIEM規則佔據了SOC處理的95%工單，這表明一小部分雜訊的規則會產生大量分散注意力的誤報（False Positive）而導致SOC分析師花太多時間處理無意義的告警。

Splunk 使用者行為分析（UBA）使用機器學習檢測進階威脅，增強安全可見性並生成豐富的上下文洞察，以協助資安團隊評估風險並採取快速行動，簡化事件調查，並提高SOC效率。

- 檢測並消除最進階的威脅使用multi-dimensional behavior baselines、dynamic peer group analysis和無監督機器學習檢測異常行為，利用超過200多個異常ML規則和模型來揭示最複雜的威脅。
- 通過豐富的判斷增強安全可見性，以便採取有效行動可視化攻擊多個階段的威脅，以了解攻擊的根本原因、嚴重性和時間線。
- 簡化事件調查，提高SOC效率在到達SOC之前對其進行過濾，讓分析師有時間專注於最緊迫的威脅。

圖2 Splunk UBA[3]



2 CARDINALOPS Research：https://www.securitymagazine.com/articles/94556-enterprise-siems-unprepared-for-84-of-mitre-attck-tactics-and-techniques。

3 資安大會 Slide：https://cybersec.ithome.com.tw/2024/slide。

(3)心得

數據爆炸的時代，雖然掌握越多資料越能從中擷取有用的資訊，但往往也帶來許多雜訊，每天大量的日誌資料要如何有效分析也是需要透過大的工具來協助，不管是ML的分析亦或者是更進階的AI分析，這些都比傳統的規則比對的進入門檻高非常多，資安分析人員必須跟上AI的浪潮才能因應新時代的挑戰。

（二）Defence Together 企業機關零信任架構成熟度評估方法論與實務導入策略

(1)講者：陳君勇（智慧資安技術長）

(2)內容摘要

John Kindervag[4]提出了零信任安全模型，主張：「Never Trust， Always Verify 永不信任，一律驗證！」，零信任架構是長期資安策略，不僅僅是短期資安方案，或購買單一資訊資安產品可以實現的，目前有關零信任架構（ZTA）規範如下：

- 國際：NIST SP800-207、NIST CSF v2.0及CISA ZTMM v2.0。
- 美國：2021年美國總統發布指令，要求美國聯邦政府採用「零信任架構」作為資通安全現代化策略之一，美國預算與管理辦公室並於2022 年1月，制定備忘錄要求各機構在 2024年底前滿足特定的網絡安全標準（ZTA）和目標。
- 國內：政府三階段ZTA導入計畫（111~113）及金管會「金融資安行動方案V2.0」鼓勵導入ZTA。

目前金融機構主管機關研訂金融「零信任架構導入參考指引」，發展「零信任成熟度模型及評估指標（ZTMM）」，評估後再依評估結果導入零信任架構提升資安防護，初期可以優化及整合既有資安管理機制為優先，不以導入新產品解決方案為必要，並建議導入規劃如下：

- 風險導向，高風險場域先行。

  初期導入以規模於可控範圍、減少影響面並可獲致實質補強效益為原則，建議以高風險及低衝擊之場域為優先。
- 循序漸進，擇基礎原則先行。

  根據 NIST、CISA及資安院 所訂定之導入框架、原則或標準，考量實務可行性，建議參採其評估方法論，盤點高風險場域之完整存取路徑（即身分、設備、網路、應用程式、資料5大面向），先行以補強脆弱點，嗣後再考量依CISA 成熟度模型逐步強化。
- 資源整合，動態監控支援信任推斷。

  事件日誌整合分析、建立信任推斷機制及發展自動協作機制。

[4] 零信任概念提出者: https://www.linkedin.com/in/john-kindervag-40572b1/。

零信任成熟度模型（ZTMM）評估內容，分為五大支柱，Identity、Devices、Networks、Applications & Workloads及Data，前三項各有7個功能問項，後兩項各有8個功能問項，共7x3 + 8x2 = 37項功能問項，每個支柱「三個橫向跨域協奏」包括可視化與分析（Visibility）、自動化及協防指揮（Automation and Orchestration）及資安治理（Governance），並將成熟度分成四個Level，傳統（Traditional）、初始（Initial）、進階（Advanced）及最佳（Optimal），每個實施梯度對保護能力、實現細節和技術複雜性都提出了更高的要求。

圖3 零信任成熟度模型（1/3）[5]

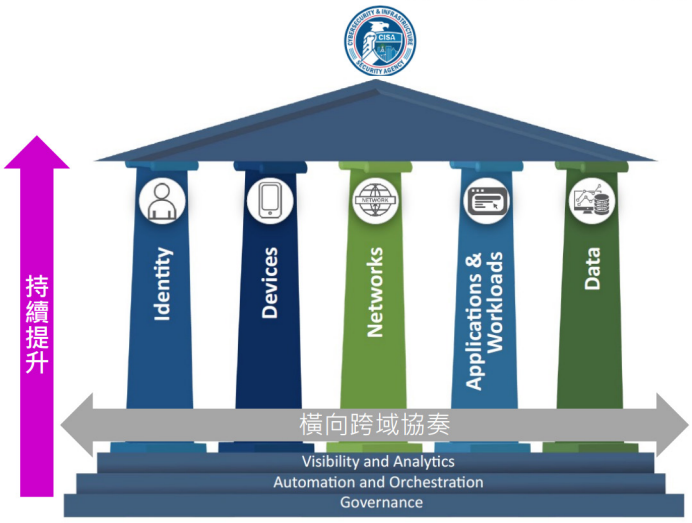
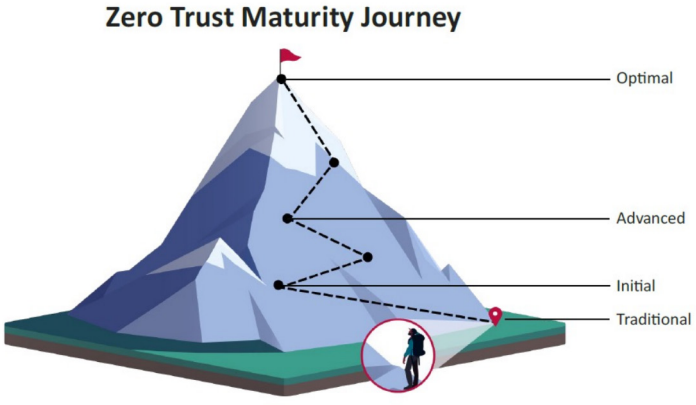


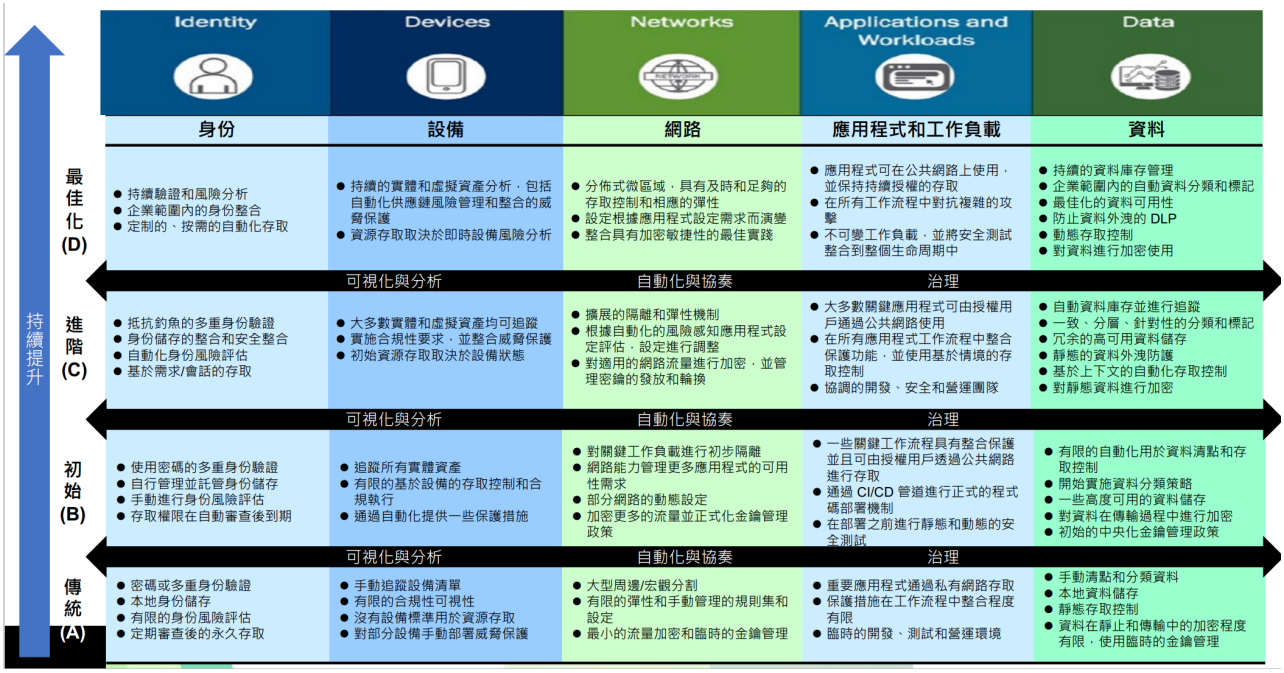
圖4 零信任成熟度模型（2/3）[6]



[5] 資安大會 Slide：https://cybersec.ithome.com.tw/2024/slide。

[6] 資安大會 Slide：https://cybersec.ithome.com.tw/2024/slide。

圖5 零信任成熟度模型（3/3）[7]



(3)心得

目前政府提出由三階段方式導入（身分驗證、設備驗證及信任推斷），但筆者覺得零信任架構是架構問題，不管是範圍跟階段皆應該有一慣性及整體性的考量，並非導入單一產品或簡單用階段式方式導入，而零信任成熟度評估可以在考量整體系統架構及業務運作後，界定出範圍及標的，透過成熟度評估來審視標的五大面向執行的等級到何種程度，再思考後續如何依需求（不是每個場域的五個面向要求皆相同）在實作面提升相關成熟度，會是比較務實的做法。

三、結論

資安大會已經是第10屆舉辦了，一路走來資安發展的面向越來越多元也越來越複雜，雲服務衍生的資安議題、零信任議題、資安人才培育、各種法規議題及目前最火紅的AI議題…等，資安世界變得更複雜了，所以需要更好的整合、更高度自動化及智能化；資安防護工作就是像是一場攻防戰爭，近代戰爭史上發生不少技術代差所導致的壓倒性戰爭，資安防護工作也是，唯有跟上趨勢發展才能確保資安工作的有效。

[7] 資安大會 Slide：https://cybersec.ithome.com.tw/2024/slide。