類別：考察
地區：美國

RSA Conference 2020 資安展與智能城市出國參訪報告

（主辦機關印信）

主辦機關：新北市政府資訊中心

目次

圖次

第一章 目的

RSA Conference 2020 資安展係全球最大規模之資訊安全展，大會活動除資安設備廠商展覽外，相關議題研討會議包含智慧城市物聯網、資通訊應用服務與最新資安服務趨勢，與會包含資訊機關組織、學術團體、高科技資通訊服務公司及資安軟硬體服務廠商。

本次活動係應美國在臺協會 (American Institute in Taiwan，簡稱 AIT)之邀，由國安會諮委李德財博士帶團，國安會、外交部、經濟部、行政院資通安全會報技術服務中心、國家通訊傳播委員會、中央研究院、工業技術研究院、資策會、銀行團體與本市共同出席與會，就美國最新官方資安管理制度(國家標準暨技術研究院 NIST 之 Cybersecurity Framework，簡稱 CSF)、RSA Conference 之國際頂尖資安監控防護中心、SPLUNK 大數據中心(SPLUNK Enterprise)、FireEye 資安作業平台(Helix)、與 Fidelis 資安作業平台(Fidelis Cybersecurity Framework)進行參訪研討，同時參訪展會國際新創團隊。經本次出訪彙整大數據中心、資安決策儀表板、NIST CSF 導入等三大方略，做為本市針對智慧城市與資安防護之問題與解決方式建議。

本次參訪重點：

(一)「國家標準暨技術研究院」(2 月 24 日)：美國國家標準與技術研究院（The National Institute of Standards and Technology，簡稱 NIST）是隸屬於美國商務部(U.S. Department of Commerce)之官方機構，本次應 AIT 之邀，參訪 NIST 舊金山團隊，就網路安全框架(Cybersecurity Framework，簡稱 CSF)進行綜合研討。

(二)「RSA Conference 展會與資安監控防護中心」(2 月 25 日)：RSA 會議是一系列 IT 安全會議，成立於 1991 年，每年在美國，歐洲，亞洲和阿拉伯聯合酋長國舉行。RSA 的名稱是源自於 RSA Data Security，Inc.開發的公鑰加密技術，本年度 RSA Conference 於舊金山 Moscone Center 盛大展出，包含南館(South Center)、北館(North Center)與西館(West Center)。除各大高科技資通訊服務公司及資安軟硬體服務廠商展會活動，亦包含演討會 (KEYNOTES)與新創團隊。

(三)「FireEye 資安作業平台」(2 月 26 日)：FireEye 是一家公開上市的美國網路安全公司，提供用於應對進階網路威脅的自動威脅取證及動態惡意軟體防護服務，如進階持續性威脅（APT）和網路釣魚（Spear phishing）。FireEye 成立於 2004 年，公司總部位於 Milpitas, California(中譯加州米爾皮塔斯)。FireEye 是第一家由美國國土安全部頒發認證的網路安全公司。本次應 AIT 之邀，參加 FireEye 之研討會。

(四)「Fidelis 資安作業平台」(2 月 27 日)：Fidelis Cybersecurity 是一家網絡安全公司，專注於威脅檢測，搜尋和響應高級威脅以及數據洩露。客戶包括 IBM，美國陸軍和美國商務部。Fidelis 提供網絡安全設備，其中包括該公司獲得專利的深度會話檢查體系結構(Deep Session Inspection)。本次應 AIT 之邀，參加 Fidelis 之研討會。

(五)「SPLUNK 總部大數據中心」(2 月 28 日)：Splunk 是一家總部位於美國加利福尼亞州舊金山，該公司生產的軟體可以通過 Web 界面來搜索，監視和分析生成大數據，在可搜索的資料庫中擷取索引和關聯性的即時數據，介以生成圖形，報告，警報，可視化決策儀表板等。本次應 AIT 之邀，參觀 SPLUNK 總部大數據中心與其研討會。

第二章 過程

本 RSA Conference 2020 資安展與智能城市出國參訪，應美國在臺協會之邀，自 109 年 2 月 23 日由臺灣啟程前往舊金山，至 109 年 3 月 1 返國，依序參訪「國家標準暨技術研究院」、「RSA Conference 展會與資安監控防護中心」、「FireEye 資安作業平台」、「Fidelis 資安作業平台」、「SPLUNK 總部大數據中心」等主題分述如下：

一、國家標準暨技術研究院

壹、機構簡介

美國國家標準與技術研究院（The National Institute of Standards and Technology，簡稱 NIST）是隸屬於美國商務部(U.S. Department of Commerce)之官方機構，其使命是促進創新，並透過標準規格制度建立與國際規範認證提升美國產業競爭力。其具體工作範圍包含納米級科學技術，工程學，資訊技術，中子研究，材料測量和物理測量。本次應美國在臺協會之邀，於 2 月 24 日參訪美國國家標準與技術研究院於舊金山之工作團隊，於 Hawthorne Plaza 就 NIST 網路安全框架(Cybersecurity Framework，簡稱 CSF)進行綜合研討。

圖 1 參訪美國國家標準與技術研究院舊金山工作團隊

圖 2 我國代表與 AIT 商務官與美國國家標準與技術研究院工作團隊合影

貳、網路安全框架(Cybersecurity Framework，簡稱 CSF)簡介

網路安全框架(Cybersecurity Framework，簡稱 CSF)設計之目的，係透過框架化的流程，提供以風險為導向、持續運作的管理架構，進而幫助組織與企業，都能依據自身環境彈性使用，管理與降低網路安全風險。類似 PMP 之 PDCA 框架，CSF 建立了識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond) 與復原(Recover)，等五大網路安全生命週期的管理策略。

5 大功能下具有 23 個類別與 108 個子類別，方便企業或組織能夠依循這些項目，評估各子類別可採行的安全措施與行動，並提供了許多參考資訊，可以對應到國際共通的標準與指引：

（一）識別(Identify)：包含資產管理、企業環境、治理、風險評估、風險管理策略、供應鏈風險管理；

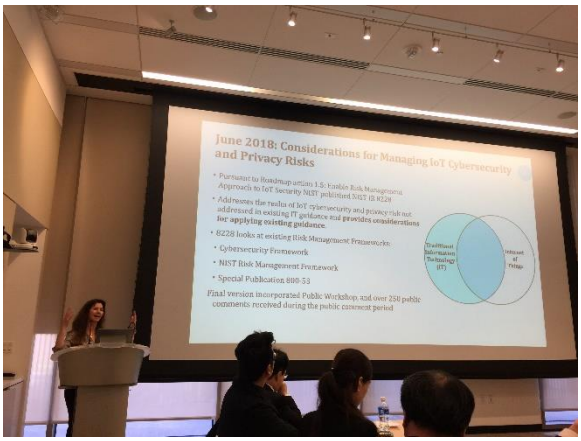
（二）保護(Protect)：身分存取控制、網路安全、意識與培訓、資料安全、資料保護流程與說明、維運與防護技術；

（三）偵測(Detect)：異常與事件、安全持續監控、偵測過程；

（四）回應(Respond)：回應計畫、溝通、分析、減緩、改進；

（五）復原(Recover)：復原計畫、改進、溝通。

NIST 還有提供了 7 個建議步驟，從優先級別與範圍、業務流程目標確認，建立現況輪廓、風險評估、建立目標輪廓，再從優先級別與差異來分析與決定，實施行動計畫。



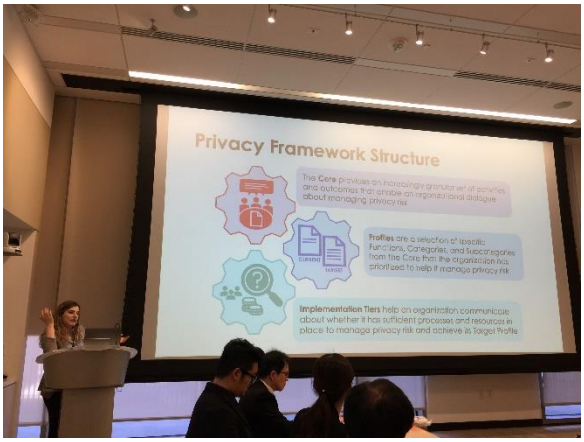


圖 3 美國國家標準與技術研究院分析師進行 CSF 簡報分享

參、網路安全框架與物聯網之關係

適逢物聯網成為智慧城市發展主題，物聯網之資安議題亦成為眾人注目之資安議題。因物聯網設備可透過端點擷取重點資訊，甚至包含個人資料，如何由端點、通訊過程、雲端，到後續之存取管理分析應用皆符合相關資安規範，成為物聯網與資安發展的重點議題。為此，CSF 提供了 7 個建議步驟，在整個 ROADMAP 裡，組織(不論是供應商、服務商、物聯網供應商)皆須依據優先級別與範圍、業務流程目標先行確認建立現況輪廓、風險評估、建立目標輪廓，再從優先級別與差異來分析，以基準線(Baseline)決定並實施行動計畫。

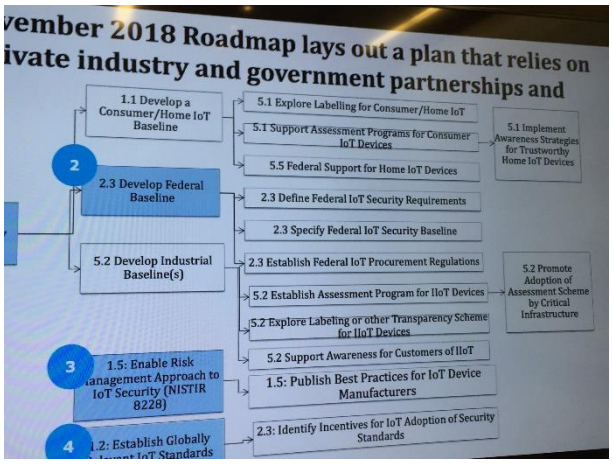


圖 4 CSF 物聯網之資安防護措施簡報分享

二、RSA Conference 展會與資安監控防護中心

壹、展會環境介紹

RSA 會議是一系列 IT 安全會議，成立於 1991 年，每年在美國，歐洲，亞洲和阿拉伯聯合酋長國舉行。RSA 的名稱是源自於 RSA Data Security，Inc.開發的公鑰加密技術，該技術成立於 1982 年，RSA 加密協定源自於技術發明者 Rivest，Shamir 和 Adleman。RSA 會議除展會以外，還進行教育，專業網路和獎勵計畫，例如 RSA 數學卓越獎（正式稱為 RSA 會議數學卓越獎），以表彰該領域的傑出人士和組織

本年度 RSA Conference 於舊金山 Moscone Center 盛大展出，包含南館(South Center)、北館(North Center)與西館(West Center)。南館(South Center)與北館(North Center)之地下空間為主要展場，包含各大高科技資通訊服務公司及資安軟硬體服務廠商；西館(West Center)為演討會地點，由學術團體進行資安新知研討(KEYNOTES)；另北館(North Center)二樓開放提供新創團隊進駐。

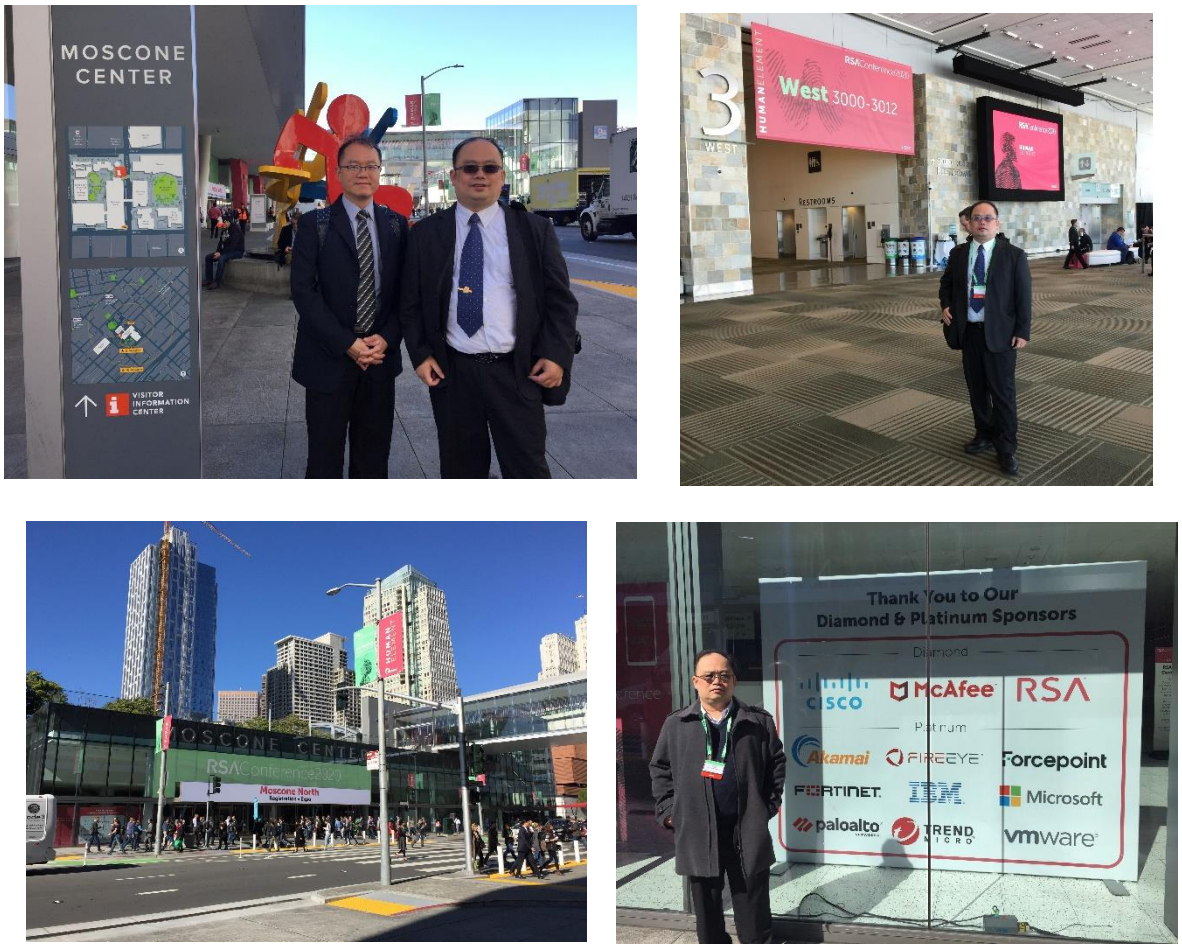


圖 5 RSA Conference 2020 展會

貳、參訪資安監控防護中心(Security Operation Center，簡稱 SOC)

RSA Conference 資安監控防護中心布建於舊金山 Moscone Center 盛大展出北館(North Center)地下室，本次應美國在臺協會之邀，於 2 月 25 日由 Director Charles Lim 與 Vice President George Lee 介紹該防護中心。

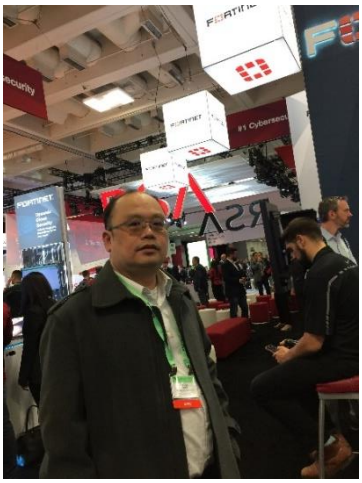
圖 6 參訪 RSA Conference 資安監控防護中心

RSA Conference 資安監控防護中心以儀表板之方式，即時反應大會系統對內與對外網路狀況，將聯網狀況以 IP、行為等以國別、地域別等進行即時化反應，同時就潛在威脅(TREND)與 PORT 連結異常以時軸進行儀表板顯示，即時反應大會資安現況。

參、參訪展會廠商

RSA Conference 展會於於 2 月 25 日上午 10 點開始展覽至 27 日下午，於南館(South Center)與北館(North Center)之地下空間展示各大高科技資通訊服務公司及資安軟硬體服務廠商，進行自由參觀。

（一）FORTINET：包含其防火牆與網路設備



（二）
VMWARE：包含其虛擬伺服器平台

（三）RADWARE：包含其防火牆與網路設備

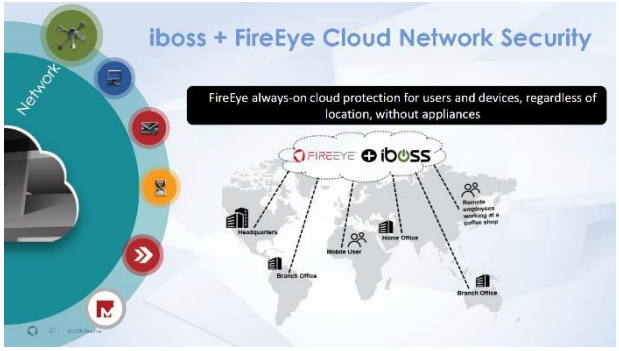
四、FireEye 資安作業平台

FireEye(中文翻譯火眼)是一家公開上市的美國網路安全公司，提供用於應對進階網路威脅的自動威脅取證及動態惡意軟體防護服務，如進階持續性威脅（APT）和魚叉式網路釣魚（Spear phishing）。FireEye 成立於 2004 年，公司總部位於加利福尼亞州米爾皮塔斯。FireEye 是第一家由美國國土安全部頒發認證的網路安全公司。

本次應美國在臺協會之邀，於 2 月 26 日參加 FireEye 所舉辦之研討會，就該公司之產品進行說明。

本次重點服務介紹如下：

- FireEye Helix：資安監控作業平台，提供組織掌控從警示到修復的所有事件。FireEye Helix 整合不同的資安工具以擷取資安投資中未被開發的潛力。
- FireEye Network Security 以及 Forensics：一種進階的威脅防護和漏洞偵測解決方案，可以全面了解世界上最複雜的攻擊，保護網絡，資產和使用者，保護已知和未知威脅。
- FireEye Endpoint Security：全面的端點解決方案，透過多個組合引擎保護使用者，阻止惡意軟體和攻擊，偵測進階攻擊，並提供由世界領先的前線回應者開發的及時回應工具和技術。
- FireEye Email Security：一種電子郵件保護解決方案，藉由了解攻擊和攻擊者的第一手知識，阻止電子郵件攜帶的威脅，在造成任何傷害之前停止它。該解決方案不僅可以阻止惡意軟體攻擊和可疑的 URL，還可以阻止網絡釣魚和模擬技術。
- FireEye Expertise On Demand：預付費的年度訂閱，提供靈活的按使用付費存取 FireEye 行業認可的安全專業知識，確保您在最需要的時候獲得所需的功能。
- FireEye Threat Intelligence：超智慧服務組合凌駕於僅僅只是增加資安產品的效能，高度情景資訊組織來增加安全產品的阻擋功能，組織需要建立主動防禦，確定警報優先級別，分配資源和改善對事件的回應速度。
- FireEye Managed Defense：是一種託管偵測和回應（Managed Detection and Response, MDR）的管理防禦服務，結合了業界公認的網絡資安專業知識、FireEye 技術和無與倫比的豐富攻擊者知識，可以在攻擊者生命週期的早期偵測到威脅，並有助於將入侵的影響最小化。
- FireEye Mandiant：世界知名資安事件回應和評估，增強和轉型諮詢服務，以保護重要的組織資產。Mandiant 能夠降低業務風險，其深入了解攻擊者行為，利用獨家的威脅情報和專門技術成功達標。



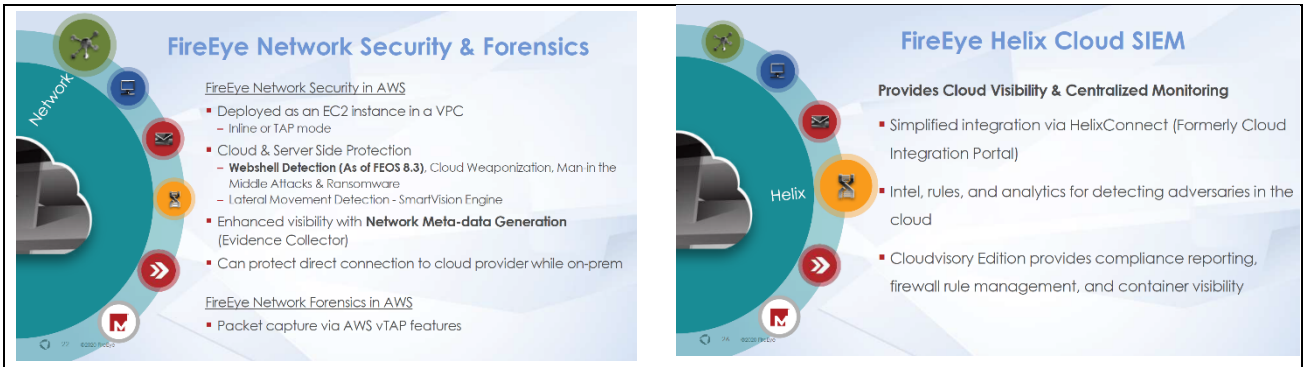


圖 7 FireEye 資安服務研討會

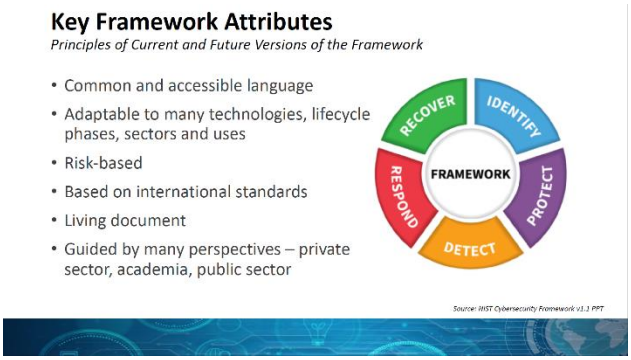
五、Fidelis 資安作業平台

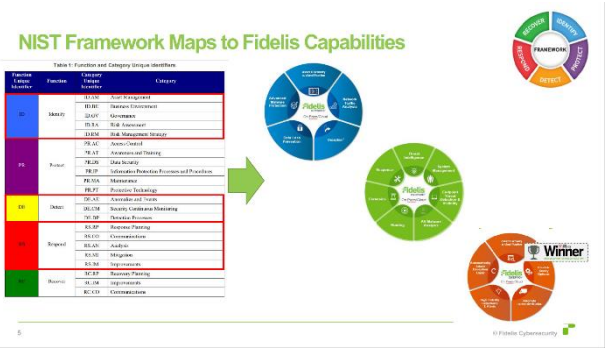
Fidelis Cybersecurity 是一家網絡安全公司，專注於威脅檢測，搜尋和響應高級威脅以及數據洩露。客戶包括 IBM，美國陸軍和美國商務部。Fidelis 提供網絡安全設備，其中包括該公司獲得專利的深度會話檢查體系結構(Deep Session Inspection)。該公司聲稱其技術優勢在於網絡流量檢查的速度和準確性。本次應美國在臺協會之邀，於 2 月 27 日參加 Fidelis 所舉辦之研討會，就該公司之產品進行說明。

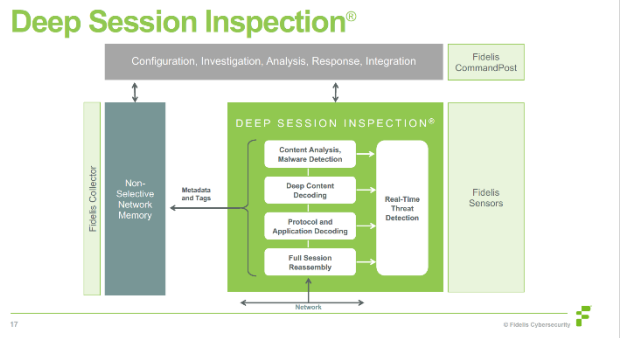
Fidelis Cybersecurity 解決方案對應美國國家標準技術研究所(NIST)所擬定的網路安全框架，分別研發對應服務，以進行識別(資產盤點，企業生態網路環境，風險設備，風險管理策略)、偵測(異常行為與告警事件，持續監控，程序偵測)、反應(反應處理，連線通訊管控，攻擊分析，拖延駭客進攻時間，全面還原)

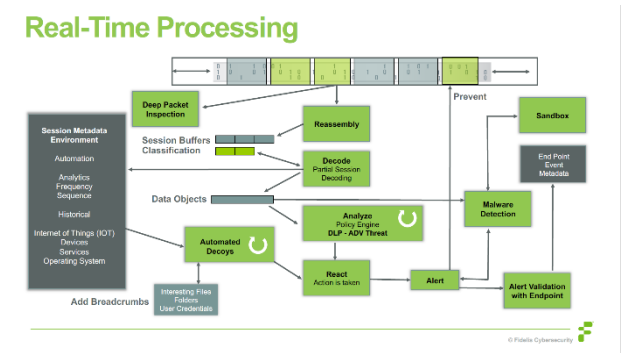
- Fidelis Network 進階式威脅阻斷 ： 通過獲得專利的 Deep Session Inspection 技術即時地對設備、作業系統、應用程式、端口、通訊協議和網絡服務器上的網絡流量自動進行解碼、分析來偵測威脅和防止資料外洩，透過不斷發現和分類所有資產來了解客戶自身的網路環境及最有可能的被攻擊者入侵的路徑。所有的封包內容都會被萃取成元數據並儲存在資料庫中，一旦新型攻擊手法的威脅情資更新後，系動將自動地對歷史元數據進行回溯性分析查找威脅和異常行為，提供駭客入侵軌跡、攻擊手法，完成鑑識採證。
- Fidelis Endpoint 端點偵測與事件反應：使用領先業界的 AV 引擎阻擋惡意程式並透過機器學習模型防止惡意行為，可整合威脅情資增強防護能力，如 IOC 和 YARA 等。安裝代理程式協助客戶瞭解端點狀況以及已安裝的軟體清單，提供 MITRE CVE 和 Microsoft KB 報告，快速反應端點弱點狀況。持續收錄端點上所有的活動行為並進行即時和回溯性分析。自動執行 Script 資料庫和劇本功能協助分析師針對事件達到終止程序，收集或刪除文件、網路隔離、鑑識採證、瞭解事件發生的完整上下文、快速完成調查並將端點恢復到良好的配置。

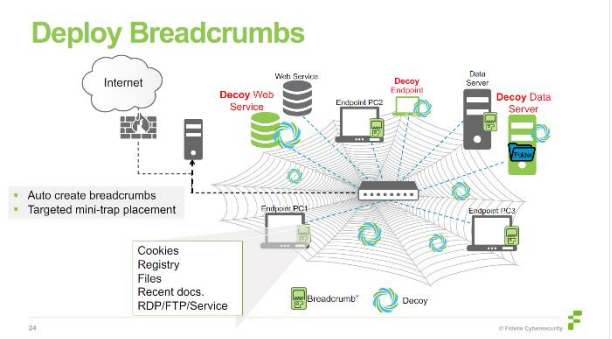
- Fidelis Deception 駭客誘捕科技：透過流量分析持續地映射客戶的網絡環境地形圖旨在消除盲點，減少駭客攻擊面，防護設備類型包括所有可控管及不可控管的資產、舊系統、影子 IT、企業物聯網、醫療、OT 產業設備等。基於客戶真實網絡環境並且隨著更動而不斷地適應，自動並且大量地以最少的資源和時間部署高擬真誘捕設備在網絡中偵測橫向移動的惡意程式和攻擊者。於真實設備中植入麵包屑(Breadcrumb)誘使攻擊者轉移注意力至誘捕陷阱進而觸發高真實度告警，並進行監視、瞭解駭客攻擊手法、拖延入侵者的進攻時間、阻斷駭客狙殺練的各個階段，達到即早即告警的效果。











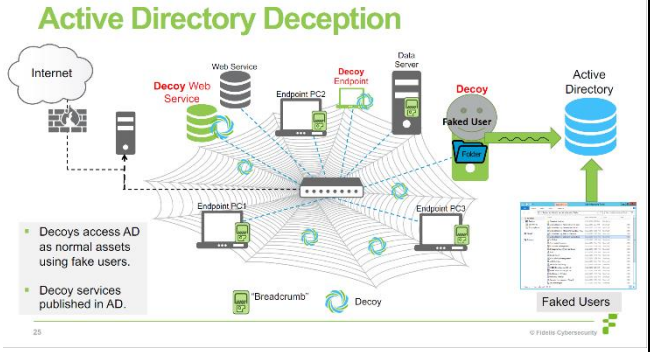


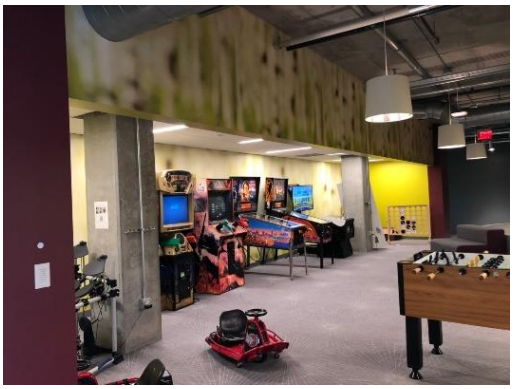
圖 8 Fidelis 資安服務研討會

六、SPLUNK 總部大數據中心

本次應美國在臺協會之邀，於 2 月 28 日驅車前往 SPLUNK 總部，並參訪其大數據中心。本次參訪由該公司負責 Security 市場之總裁 Haiyan Song 主持並簡報，Splunk 專注於數據引擎，並建立分析平台，以結構化、非結構化等機器數據(log)產生分析、告警之資料報告。

其重點如下：

- 搜索、關聯、調查：具有專利的 Splunk 搜索處理語言（SPL），直觀且功能強大。自動將各類數據格式，提供 140 多種命令,可以統計搜索、計算指標、甚至在滾動時間窗內查找特定條件。放大和縮小的時間線以自動揭示趨勢、峯值和蘊含的模式，並且可以以鑽取深入細節。
- 鑽取分析：通過使用即時搜索和時間線控制深入分析前後的所有數據,快速顯示趨勢峯值和異常。只需輕點鼠標,就可利用 Splunk 的獨特字段提取功能找到任何數據字段內的任何值,以跟蹤事件序列和快速實現"大海撈針"。無論是否正在調查一個安全警報,分析業務中斷的根源,或調查潛在數據泄露,都會在幾秒鐘到幾分鐘而不是幾小時或幾天內得到答案
- 監控告警：將搜索轉化爲實時告警,通過電子郵件或 RSS 自動觸發通知,執行修復操作,向系統管理控制檯發送 SNMP 陷阱或在服務檯生成故障票據。告警可基於各種閾值、基於趨勢的條件和其他複雜標準而觸發。在出現告警時獲得其他信息,協助運維人員更快進行根本原因分析並找到問題的解決方案
- 報表和儀表盤：使用同一界面搜索實時和歷史數據。使用熟悉的搜索命令來定義、限制或擴大搜索範圍,並跨越多種數據源進行關聯以發現新的現象。關聯基於時間的數據、外部數據、位置、子搜索或連接跨越多種數據源。搜索幫助提供鍵入提示建議和上下文幫助,方便使用搜索處理語言（SPL™）的所有高級特性



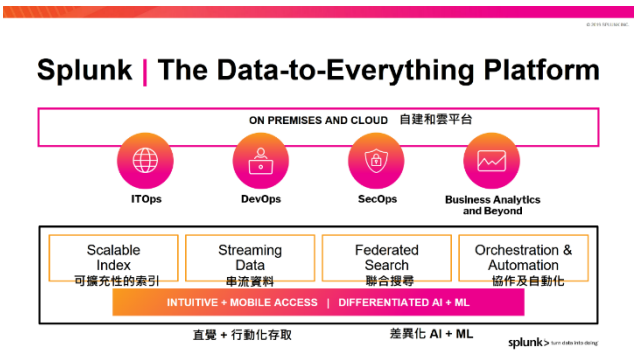


圖 9 SPLUNK 資安服務研討會

第三章 心得

壹、NIST CSF 觀念導入

NIST 之 CSF NIST 之網路安全框架(Cybersecurity Framework，簡稱 CSF)雖尚未經過 ISO 認證為國際標準，但依據過往經驗應會於近期成為國際標準，甚至有可能成為我國後續資安法遵參考依據。比較起 BSI 或相關 ISMS 資安管理制度，CSF 有更明確的指引 GUIDELINE 與 ROADMAP，以識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond) 與復原(Recover)等五大網路安全生命週期的管理策略，搭配 23 個類別與 108 個子類別，以具體的優先級別與範圍、業務流程目標確認，建立現況輪廓、風險評估、建立目標輪廓，再從優先級別與差異來分析與決定，實施行動計畫，方便企業或組織依循。

目前本府並無導入該安全框架之規劃，惟相關精神，例如五階段分析、風險與範疇識別，CHECKLIST 分析等精神，皆可以提供我們進行資安管理制度導入之參考，並進行適度調適。

貳、SIEM 解決方案導入

本次展會有多家廠商都建立了完整的 SIEM 解決方案。所謂 SIEM(Security information and event management)，很類似我國之 SOC，但在 SOC 之外，他又明確定立了相關資安管理與通報之工作指引，包含數據整合、關聯分析、緊急通報、決策儀表板、法遵、LOG 保留、鑑識等，說明如下：

(一)數據整合：日誌管理可整合來自網絡，安全性，服務器，資料庫，應用程序等許多來源的數據，從而能夠合併受監視的數據，從而有助於避免丟失關鍵事件。

(二)關聯分析：查找通用屬性資料，並將事件鏈接。包含各項跨平台整合介面技術，以便將數據轉化為有用的資訊。關聯分析是整個 SIEM 解決方案的安全事件管理部分的功能。

(三)緊急通報：相關事件的自動分析

(四)決策儀表板：工具可以獲取事件數據並將其轉變為資訊圖表，以幫助查看模式或識別未形成標準模式的活動。

(五)法遵：可以使用應用程序來自動收集法規遵從性數據，生成適合現有安全性，治理和審計流程的報告。

(六)LOG 保留：採用歷史數據的長期存儲，以促進數據隨時間的關聯，並提供合規性要求所需的保留。長期保留日誌數據在法醫調查中至關重要，因為在發生漏洞時不太可能發現網絡漏洞。

(七)鑑識：能夠根據特定條件跨不同節點和時間段搜索日誌。這減輕了在您的腦海中聚集日誌信息或搜索成千上萬個日誌的麻煩。

目前本府已經有導入 SOC，惟整體覆蓋度、LOG 保留與整合度不佳，且缺乏關聯分析與通報整合服務系統，加以決策儀表板等即時資安服務狀況無法掌握，尚待改善。

參、其他資安防護機制心得

本次 RSA Conference 資安參訪，除了參訪到美國最新官方管理制度，同時看到近期重點方向，包含決策儀表板、海量即時分析等外，同時部分廠商之專利技術，也可引為參考：例如 Deep Session Inspection 相對於過往的 PACKET(封包)分析，即時地對設備、作業系統、應用程式、端口、通訊協議進行解碼、分析來偵測威脅和防止資料外洩，值得借鏡。

第四章 建議

新加坡「智慧國 2025(smart nation) 」計畫，除設立「智慧國與數位政府辦公室」外，並列舉「數位經濟行動架構」、「數位政府藍圖」及「數位整備藍圖」的三大目標，並致力發展結合交通運輸、公共安全、保健服務等智慧科技，可為我們新北市政府推對智慧城市之借鏡如下所示：

本次 RSA Conference 2020 資安展參訪，在美國在臺協會邀請下參訪國家標準暨技術研究院、RSA Conference 之國際頂尖資安監控防護中心、SPLUNK 大數據中心，並參加 FireEye 與 Fidelis 資安研討會，列舉「建立本府之決策大數據中心」、「建立本府之資安防護戰情儀表板」及「NIST CSF 網路防護框架觀念導入」三大方略，做為本市針對智慧城市與資安防護之問題與解決方式建議：

- 建立本府之決策大數據中心
  目前之數據決策，多以結構化的資料庫，並且受限於介面管理與資料流程，缺少即時化分析。本次參訪美國業界之大數據中心，可透過搜索處理語言，以獨特字段提取功能滾動查找特定條件，快速實現海量搜尋的功能，進一步達到即時搜尋與大數據分析，可為本府參考借鏡。
- 建立本府之資安防護戰情儀表板
  目前本府已經有導入 SOC，惟整體覆蓋度、LOG 保留與跨平台整合度尚待改善，且缺乏關聯分析與通報整合服務系統，加以無法透過決策儀表板等即時資安服務進行視覺化掌握。建議可透過 SIEM 之概念，導入完整之解決方案，將數據整合、關聯分析、緊急通報、決策儀表板、法遵、LOG 保留、鑑識等，以制度化方式導入相關工具、軟硬體服務，建立系統化資安管理與通報之工作指引。
- NIST CSF 網路防護框架觀念導入
  NIST 之 CSF NIST 之網路安全框架(Cybersecurity Framework，簡稱 CSF)雖尚未經過 ISO 國際認證，且尚未成為我國資安法遵；但比較起 BSI 或相關 ISMS 資安管理制度，有更明確的指引 GUIDELINE 與 ROADMAP。本府可參考其識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond) 與復原(Recover)等五大網路安全生命週期的管理策略，搭配 23 個類別與 108 個子類別，以具體的優先級別與範圍、業務流程目標確認，建立現況輪廓、風險評估、建立目標輪廓，再從優先級別與差異來分析與決定，實施行動計畫，並將相關精神導入資安管理制度，並依本府實際需求與狀況進行適度調適，以為借鏡。