出國報告(出國類別：考察)

RSA Conference 2020 資安研討會

服務機關：桃園國際機場股份有限公司

姓名職稱：彭俊智 助理工程師

派赴國家/地區：美國 舊金山 **Moscone Center**

出國期間：中華民國 **109** 年 **2** 月 **23** 日至 **3** 月 **1** 日

報告日期：中華民國 **109** 年 **4** 月 **14** 日

目次

一、摘要.....3
二、行程紀要.....4
三、參與活動簡要.....4
(一) 聽取 Emerging Threat.....4
(二) 針對 Ransomware 攻擊趨勢探討.....5
(三) Trend Micro XDR：Improving EDR Effectiveness by Adding Email/Network Visibility.....7
(四) IoT 資安測試方式： Building a Comprehensive IoT Security Testing Methodology.....9
四、會後建議方向.....11

一、摘要

RSA Conference 2020 資安研討會是 2020 年全美國最主要也是世界上盛大的資安研討會之一，每年皆能吸引全球 5 萬名與會者參加，今年於 2020 年 2 月 24 日至 2 月 28 日在美國舊金山舉辦，共計 5 天。因為時差(換日線)及班機的關係，2 月 23 日搭乘長榮 BR18 由桃園機場出發並於 3 月 1 日深夜由舊金山搭機返回抵達桃園機場已是 3 月 2 日早上。大會活動與展場地點主要在 Moscone Center 區域，亦為舊金山聯合廣場附近，共分為三個主場地：Moscone South、North 及 West 館，舉辦 Keynotes、 Sessions & Events、Tutorials & Trainings、Learning Labs、Sandbox 以及廠商產品攤位展示等(Booths)等各類活動主題，縱貫整個資安大會的各項活動主要與網路詐騙、加密與加密鏈結、雲端安全、應用程式安全、駭客與威脅、法律安全、AI 與機器學習、行動與 IoT 安全、開放原始碼、資料保全、安全策略與架構等議題，除邀請業界具前瞻性思想的領導者提供演說內容外，並導入產業技術與防護安全的新方法，不僅為科技安全新知傳遞的大本營，亦為資安產業彼此競合關係的管道。本次研討會共分為 24 個主題、以及 2 千位專家演講者，多達 700 場會議及至少 700 家以上的參展廠商，在上述 3 個主要場地同時進行。其中有一項沙盒競賽，每年皆會進行投件並經過審查後，選出最優秀的前幾家新創公司，在年會活動中各進行 3 分鐘的簡報，展示其創新技術以爭取評審優勝。本次參訪活動行程為參加 RSA Conference 舉辦的相關主題研討以及展點廠商所展示的資安防護技術運用；希望藉此次外部參訪，在許多專家、學者的經驗下取其經驗，提升及強化本身專業能力外，亦可適時運用在本公司的資安防護。

二、行程紀要

行程日期	地點	紀要
109.02.23	桃園-舊金山	啟程(BR18) 1950-1450L
109.02.24 至 109.02.28	舊金山 Moscone Center 會議中心	參加 109 年度美國 RSA Conference 資安研討會，強化本機場國際上資安議題與發展趨勢，並藉由該研討會的 Keynotes、Class Track(資安課程)，學習並擷取資料安全、雲端安全、網路攻擊型態防堵等方式，透過展場超過百家國際知名大廠展出最新資訊安全解決方案，企盼建構與整合本公司最適化之機場網路安全策略。
109.02.29	舊金山-桃園	返程(BR7)1220-1810L(+1)

三、參與活動簡要

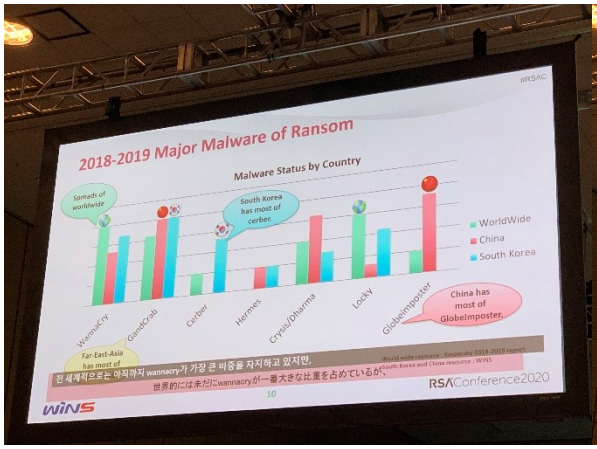
(一) 聽取 Emerging Threat

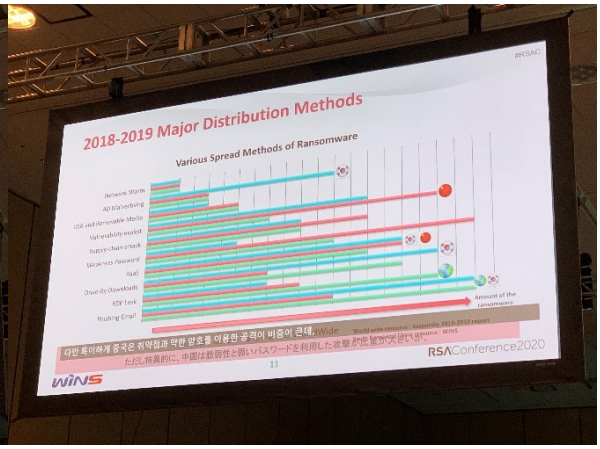
本場次主要是針對 Ransomware 進行相關的對談、經驗分享，從美國兩大的市區的 CIO，一位是洛杉磯市網路安全辦公室的 CIO，另一位是紐約市警局網路安全辦公室的中尉警官，與在場進行分享相關資安經驗。洛杉磯市的 CIO 則是以政府的角度建立資安學院，而紐約市警局亦是有類似資安辦公室，雖然分隔美國東西兩岸，但是在資安角度上彼此就像是每年舉辦的 RSA 研討會方式，自行分享資安上遇到新的攻擊行為或者是探討防

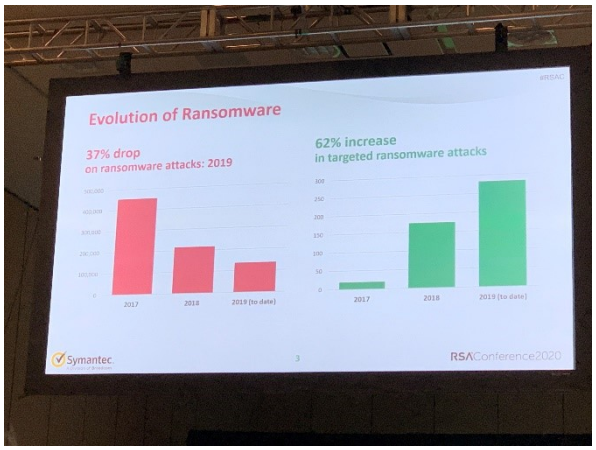
禦手法。

(二) 針對 Ransomware 攻擊趨勢探討

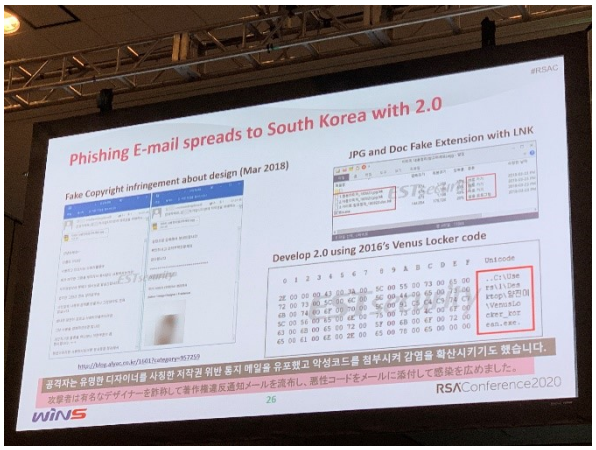
首先由韓國當地的 Win Cert 經理人進行探討 Ransomware 攻擊趨勢與手法，由下圖統計所示，目前中國仍然是攻擊來源的大宗，而攻擊手法前三名依序仍然是電子郵件社交工程、下載到惡意程式、弱點揭露並列第二、再來則是 RAAS(亦為勒索軟體服務)。



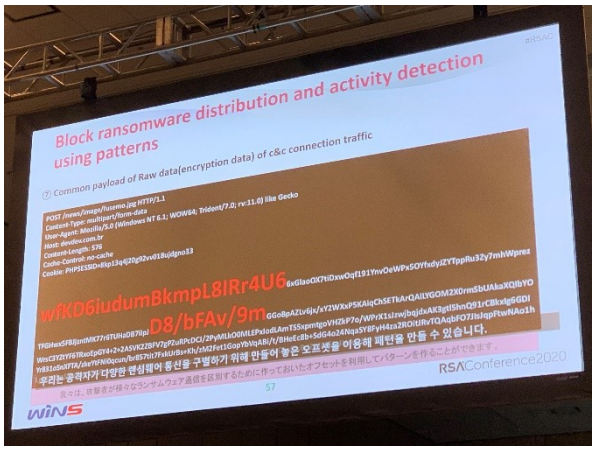




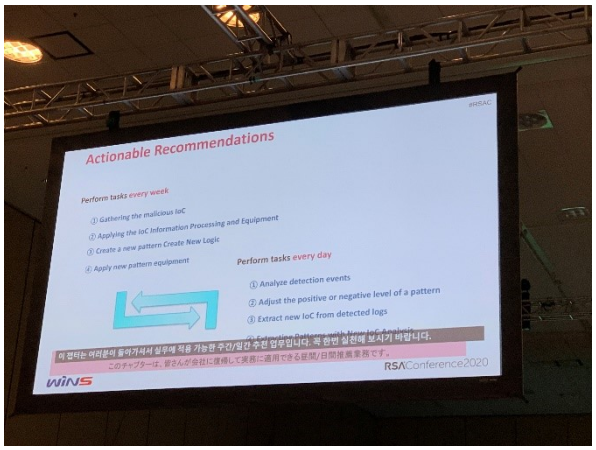
釣魚郵件的手法，還是以 html 或是假檔案為主，如下圖所示。



我們該如何預防或是防堵，則可以透過分析該檔案的二位元原始資料剖析，可以看到標頭的特徵值則為固定不變，但是實際上該檔案的檔名是相同的，如下圖。

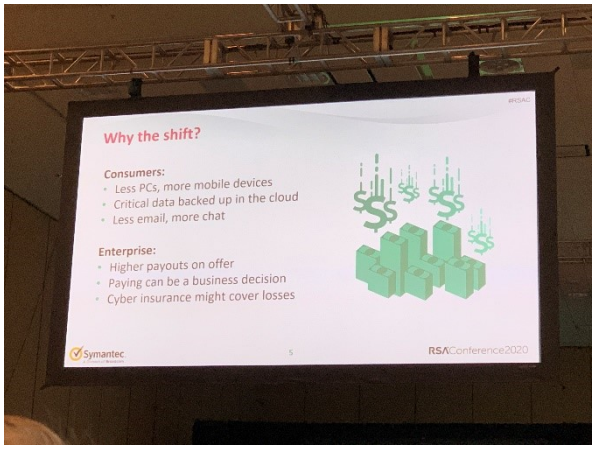


透過定義出惡意程式的妥協指標(Indicators of Compromise)，並從日常維運紀錄(LOG)中進行分析攻擊模式(Patten)，迭代方式修正，促使收斂攻擊，如下圖所示。

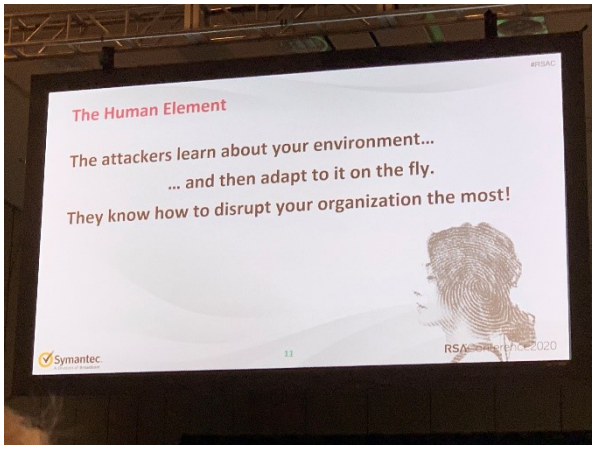


另一方向為主動的備份策略，除了異地以外亦可採取雲端的方式；再者為針對目前保險

公司所推出的資訊安全保險進行適時規避，但所費不貲，也不失為方法之一。

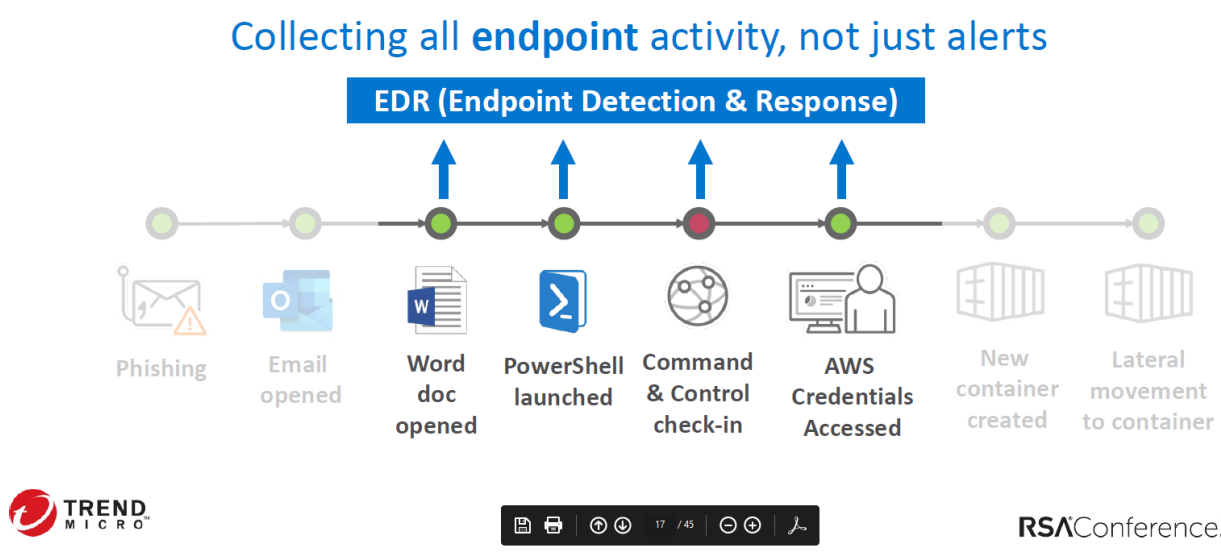


駭客攻擊不再只是單純的破壞，而是融入你我生活的一部分，甚至比你更清楚公司組織架構，進而蠶食鯨吞公司機敏資料變現。

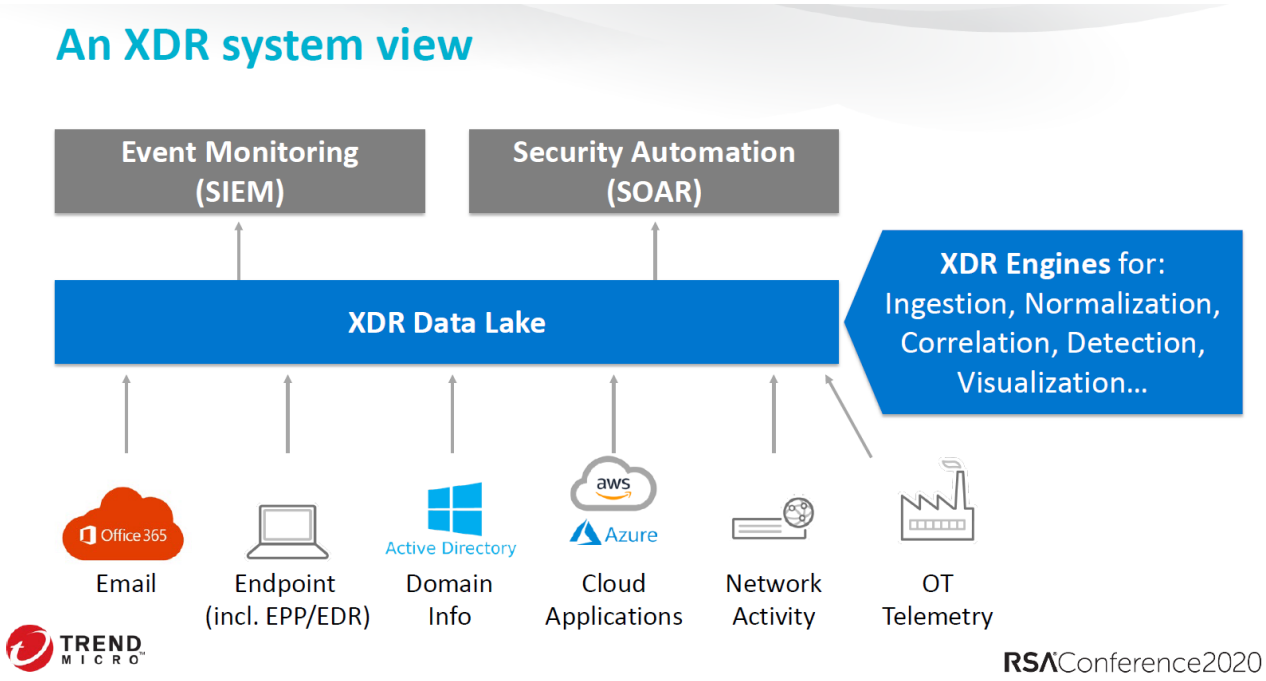


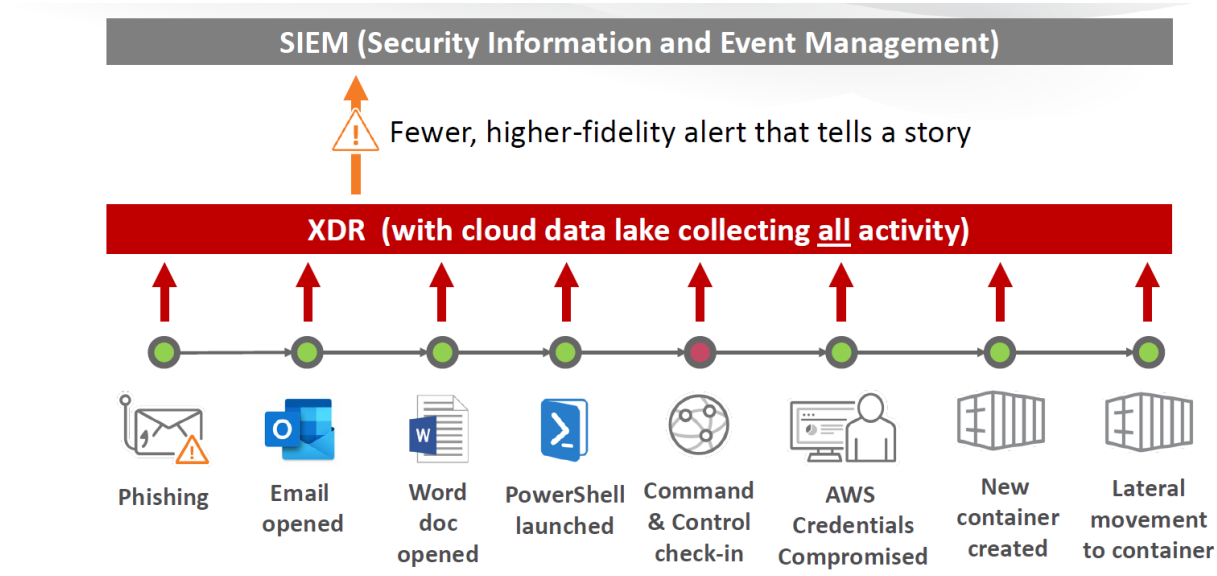
(三) Trend Micro XDR：Improving EDR Effectiveness by Adding Email/Network Visibility

過去從 LOG 蒐集、SIEM 與 SOC 等等設備或服務皆為針對主機設備進行資料蒐集與分析，趨勢科技發展出 EDR，從行為和事件的端點偵測及回應，資訊人員可以得到的不只是入侵方式，亦能夠對正在發生的細節進行分析並了解各種不同的威脅和攻擊類型，讓資訊或資安人員能夠及時有效地關聯資訊並做出回應。但 EDR 只針對特定端點進行監控，倘駭客透過其他方式進入，例如 Email、雲端服務攻擊甚至為透過 OT 或其他技術，則難以偵測；

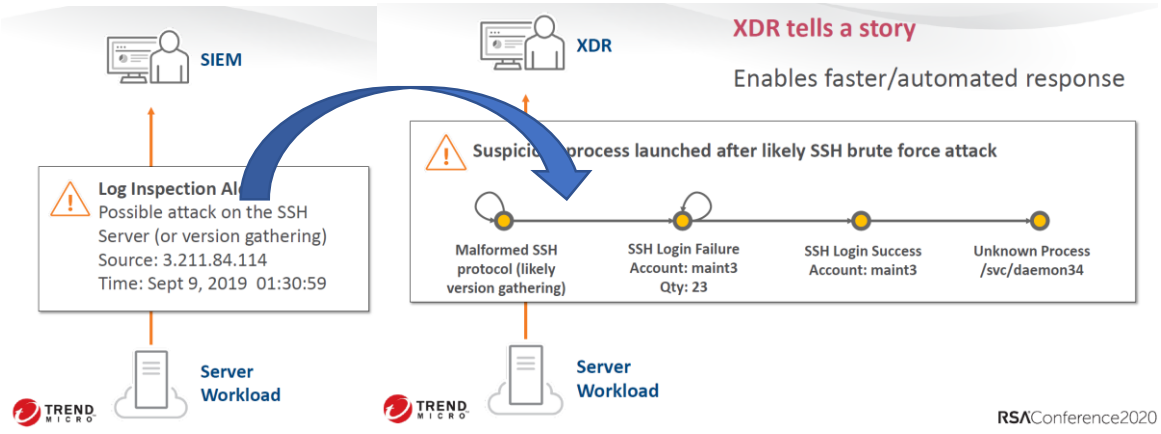


故目前發展出 XDR，針對的是跨層級，範圍涵蓋網路端、閘道端、主機端、用戶端，甚至是第三方技術，如下圖所示。XDR 結合 SIEM 雙平台整合界接，由 XDR 整合與資料(LOG)等進行正規劃再行整合進 SIEM。



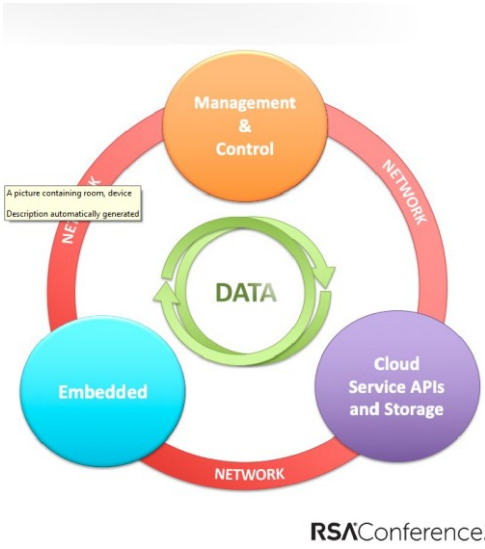


另一方面，過去的 SIEM 無法取得所有資訊或攻擊軌跡，而 XDR 可以完整蒐集並分析出攻擊來源、後續滲透軌跡、使用帳號等等資訊，如下圖所示。

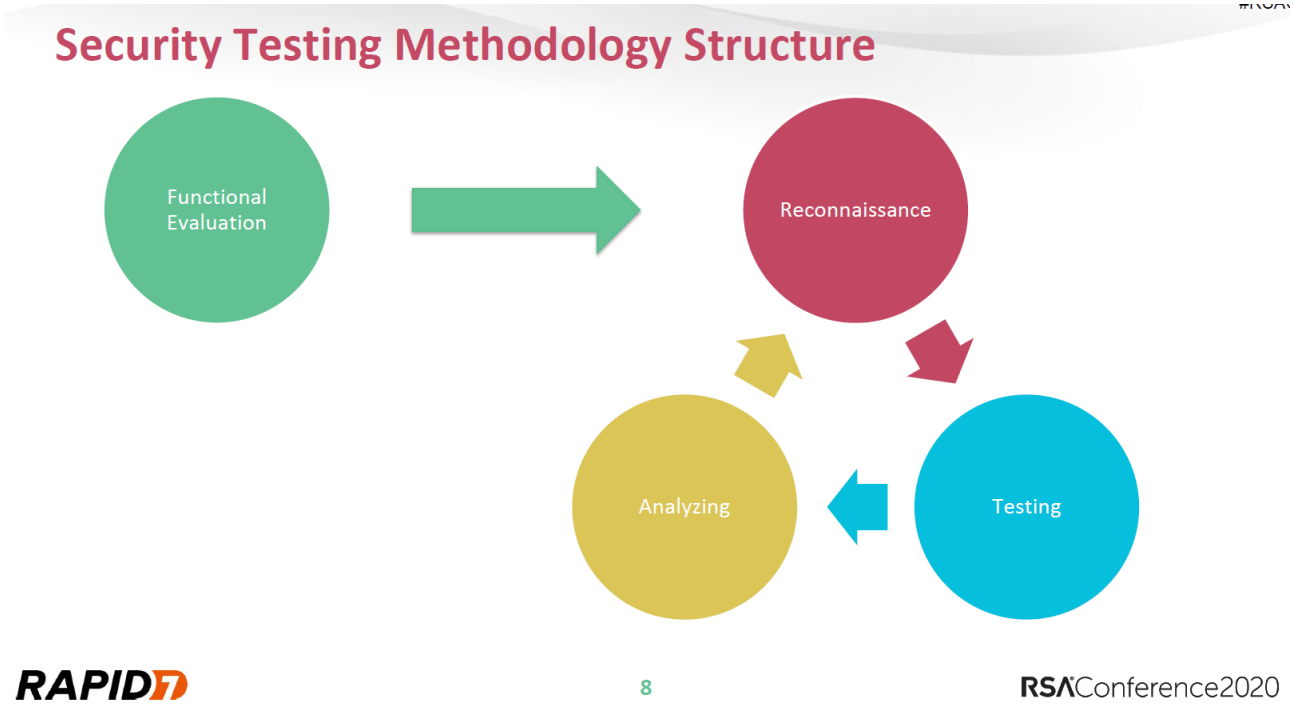


(四) IoT 資安測試方式： Building a Comprehensive IoT Security Testing Methodology

該場次由 Rapid7 的技術顧問進行探討時下 IoT 的資安測試方法。首先 IoT 的生態主要是圍繞著三大主軸，嵌入式系統、雲端服務、管理控制，彼此藉由網路進行溝通，形成 Internet of Things。



安全測試的方法由 4 大面向構成，功能面(Functional)、偵查面(Reconnaissance)、測試面(Testing)與分析面(Analysis)，彼此關係如下圖所示。



功能面：應該要了解該 IoT 設備的主要功能、相關元件與元件之間溝通的協定與通訊方式。

偵查面：

FCC ID：具有無線通訊的物件，通常都會取得 FCC(Federal Communication

Commission)的認證，是為美國政府獨立的審查機構，若該物件通過審核，FCC 會發予一個 FCC ID。

使用手冊：充分了解與閱讀該 IoT 設備使用手冊是必須的。

電子元件列表：要了解該物件所使用的電子元件品牌、規格、型號等等。

產品歷程：猶如軟體開發原始碼，每次發行正式版本都會有該產品先前的發布歷程，IoT 設備毅然。

弱點：依據上述的電子元件列表，反查 CVE 資料庫，取得該電子元件目前是否有弱點存在，若有則請廠商提出修補程式或相關解決方案。

測試面：依據弱點測試、功能驗證與 IoT 相關生態影響三大主軸進行探討。

弱點測試：可參考 OWASP TOP 10、注入攻擊等等

功能驗證：機密性、可驗證性與 Session 管理等。

該場會議後半部有針對 IoT 相關電子元件的測試方式，但該方法已經趨近於建立電子元件測試實驗室的規格，故僅供參考。

四、會後建議方向

基於參與研討會，後續有幾點本公司後續可以採納之處。

(一)　第一點

攻擊者入侵的方式不再是瀑布式攻擊，而是特定且遣伏的 APT 方式進行，手法仍以 Email 詐騙的方式進行為大宗，故每年交通部所進行的 2 次社交工程演練外，建議本公司自行委外辦理額外社交工程演練，並將點擊者進行 1 次完整教育訓練後，擇期再行演練，俾利資安落實與居安思危的體悟。

(二)　第二點

過去我們在資安設備防護不外乎是 IDS/IPS、防毒、防火牆等耳熟能詳的設備或服務，

未來應朝向以下短、中、長期落實。

1. 短期－各系統應完整落實 WINDOWS UPDATE 與防毒系統建置，達到最基本的資安要求。
2. 中期－應於各系統落實作業系統 LOG 與應用系統 LOG 建置，統一收容與適時備份，並分析是否存在惡意行為，俾利在短時間發現異常並予以因應。
3. 長期－基於參訪，應該導入類似 TREND MICRO XDR 的跨層級的防護機制，並結合 SIEM 進行告警機制，俾利資安人員可蒐集完整攻擊來源與入侵軌跡，進而可作為數位證據與保全，達到最終的防護。

(三)　第三點

IoT 是目前也是未來的發展趨勢，交通部目前業已發函所屬相關單位，應該每年進行 OT 設備進行資訊資產盤點，尤其是針對具有通訊性質的 OT(亦為 Internet of Things, IoT)。各業管單位於採購具資通訊性質設備皆請廠商提出該設備是否通過 FCC 認證、使用手冊、是否使用危害國家資通安全之電子元件等等證明；並於每年定期檢視設備原廠是否有最新的韌體進行安全性更新。具資通訊之設備的無線傳輸視其必要性進行資料加密保護，避免資料外洩或不當利用。