出國報告（出國類別：實習）

智慧電網資安防護研習

服務機關：台灣電力公司
資訊系統處
姓名職稱：楊石昇 電腦軟體工程師
派赴國家/地區：美國/舊金山
出國期間：**108** 年 **3** 月 **3** 日～**108** 年 **3** 月 **10** 日
報告日期：**108** 年 **4** 月 **23** 日

摘要

政府於 106 年通過 4 年期的「國家資通安全發展方案」後，行政院為強化我國關鍵基礎設施之資安防護能力，於 107 年 6 月完成立法並公布「資通安全管理法」，同時展開「資安旗艦計畫」及「前瞻基礎建設計畫」，以落實關鍵基礎設施之各項資安防護工作。台電公司為加強智慧電網的資安防護工作，參加由美國在台協會(American Institute in Taiwan)商務組主辦的首屆 AIT RSA 2019 資安研習團，透過關鍵基礎設施之研討會與資通安全專家經驗交流，瞭解國際技術與產業發展現況，作為日後資安計畫規劃與執行之參考。

本次參訪除了參加美國 RSA 資安大會(RSA CONFERENCE 2019)外，還有三場關鍵基礎設施(CI)資安研習會，分別與 NIST(NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)，PG&E(PACIFIC GAS AND ELECTRIC) COMPANY 及 CISO(CALIFORNIA INDEPENDENT SYSTEM OPERATOR)的專家學者及業界先進行交流，藉由他們已經累積數十年的實際經驗， 為我國關鍵基礎設施之資安防護能力及台電公司的智慧電網資安防護工作，提供一套適切可行的參考方案。

目次

壹、出國目的

智慧電網是由傳統電力、資訊及通訊技術三大基礎建設所形成的新型電力網路。由於電力和資訊及通訊技術的結合，使得傳統資通安全必須融入電力網路安全及電力運轉安全考量，方能滿足智慧電網資通安全所需。以配電系統為例，電力網路(饋線)安全由各式保護協調元件的參數規畫以確保；而電力運轉安全則由電力調度自動化系統(SCADA)承擔，因此保護協調系統及電力調度自動化系統需有適當的資通安全考量。本次 RSA 2019 資安研習團，除了解美國最新的資安技術外，也至國外先進電力公司學習智慧電網之資安防護機制及解決方案。

台電公司配合政府政策，期許為智慧型電網的建構者，除透過發電端效率提升外，亦將逐步改善輸配電效率，推動配電端饋線自動化及環路供電建置，並將配合電力科技持續創新，規劃建構智慧型電網，期能進一步提高供電可靠度。在智慧型電網的建設過程中，除了要確保輸配電網路資通安全外，也要提供 AMI 資料傳輸的安全性，而這一部分屬於 OT 資安的範疇，其相關資安規範(例如: NERC CIP、NIST SP 800 及 ISO 27019)的引用及建立也是一大挑戰，因此，藉由本次參訪，培養 IT/OT 複合領域資安防護及稽核的能力，以持續強化本公司資安基礎設施提升 IT/OT 資安能量。

貳、實習參訪過程

本次出國自 108 年 3 月 3 日出發，迄 3 月 10 日返國(共計 8 天)，參加由美國在台協會(American Institute in Taiwan)商務組主辦的首屆 AIT RSA 2019 資安研習團。本次參訪除了參加美國 RSA 資安大會(RSA CONFERENCE 2019)外，還有三場關鍵基礎設施(CI)資安研習會，進行面對面的意見交流，詳細說明如下：

一、美國 RSA 資安大會(RSA CONFERENCE 2019)

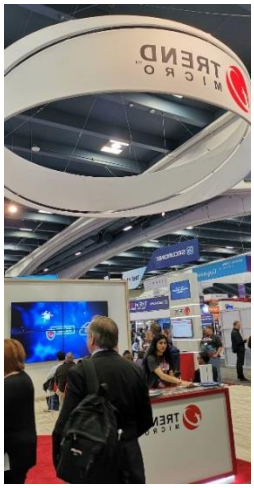
本次參訪地點在美國加州舊金山市中心 Moscone Center。這裡是著名的展覽會場，每年都有很多各行各業的重量級會展及國際級的公司來到這裡發表他們的最新產品。

資安展期間雖然舊金山的天氣不佳時有大雨及低溫強風，但會場內仍是滿滿的參觀人潮，絲毫不受氣候的影響。

RSA 已由原來的演算法，加解密器等資訊產品廠商，走向資安產業，並於最近幾年成功掌握資安產業的發展趨勢，擴大在資安產業的影響力。故近幾年的 RSA Conference 已成為資安產業的年度盛會，並吸引近 700 多家世界各地資安廠商參展及舉辦上百場的研討會及數十場 keynotes，內容涵蓋各領域：除了網路設備商，防毒軟體大廠外，也包含法律、教育、政府管理、技術、商業活動及人才培訓等，可以說是一個很具代表性的資安產業盛會。

（一） 展覽攤位參訪

參展的廠商分布於展場的南館和北館，共約 700 多個參展攤位，現場並提供茶點及免費 WIFI 透過 APP 即時傳送展場訊息，讓參觀者可以隨時掌握展場動態。



參展的廠商除了傳統的網路設備大廠外，也包含了資安防毒等軟體廠商，有很多新創公司來這邊展示新一代的網路資安及雲端資安產品，這些創新的產品概念，也正引領新的資安潮流。

透過和參展廠商的面對面溝通，也發覺下一代的資安防護概念已經跳脫原本被動的下載攻擊特徵碼進行防護，轉變為及時動態產生特徵碼判斷，並利用人工智慧(Artificial Intelligent)及機器學習(Machine Learning)的方式，加強每一次攻擊判斷的準確率，這樣的發展趨勢，確實令人驚艷。在第三部分的出國心得部分，也會針對這樣的發展趨勢，作更進一步的說明。

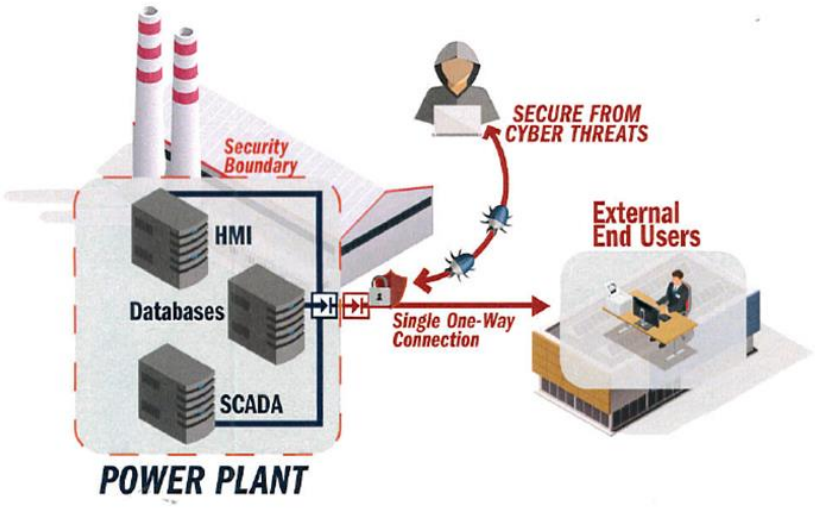
（二） 關鍵基礎設施的資安設備

展場中也有部分廠商從事關鍵基礎設施的資安設備開發，這些產品的設計概念，可以作為我國在建設關鍵基礎設施建置時的參考，例如:IT 與 OT 間的無線網路傳輸資安防護，以及如何利用單向資料傳輸設備來防止駭客攻擊。

由於 IT 與 OT 間的無線網路傳輸，因位於開放場域及訊號傳送易被攔截等特性，資安防護的難度便提高了許多。例如:要避免因無線傳輸的漏洞，導致資料中心被入侵的風險，或是不正確的 IoT 設備的設定檔，開啟了後門程式。要改善這種狀況，需要透過無線的資安設備，對每個介於 IT 和 OT 的端點設備進行動態的監控，辨認每個 OT 的端點設備的異常特徵值，以及對資料中心可能造成的風險。同時，對於異常的端點設備，如感測器、現場及時攝影機或是控制器，可以自動進行網路隔離，避免多重風險同時發生，並減緩更進一步的攻擊。例如:由於感測器異常或訊號遭竄改，造成資料判斷錯誤，進而觸發更多異常的控制訊號。以下圖來說明 IT 與 OT 間的無線網路資安防護。

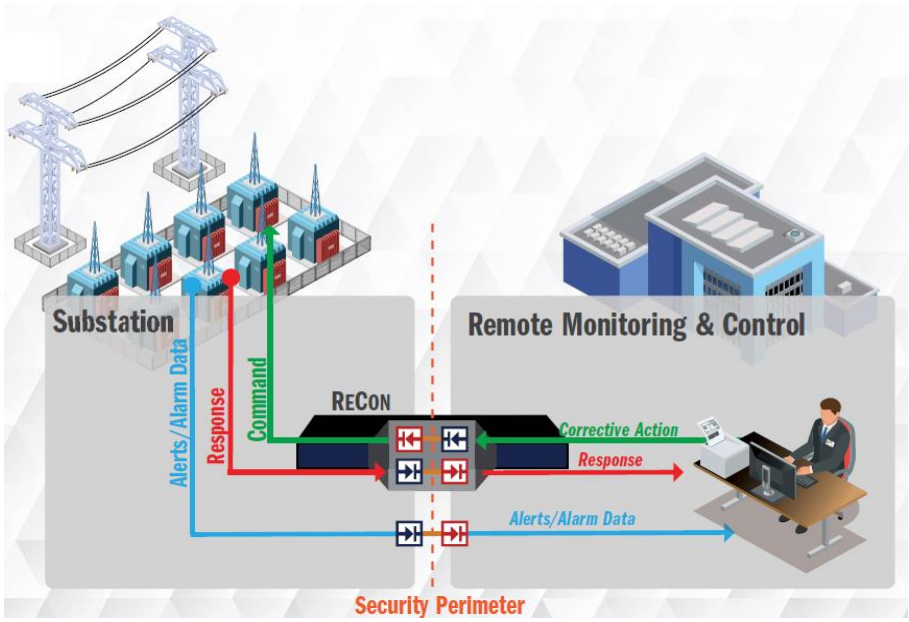
資料來源 https://www.802secure.com/

利用單向資料傳輸設備來防止駭客攻擊：在電廠的 SCADA 系統及控制中心的訊號(HMI)需要透過網路傳輸將資料傳送到外部的 IT 中心，如果所有由電廠的網路傳輸都是單向的連接到外部的 IT 中心，就可以避免駭客連線至電廠內部，同時在外部的 IT 中心也可接收傳輸資料，監控電廠的運作。



資料來源 https://www.owlcyberdefense.com/

傳輸電力的配電設備需透過遠端的控制中心進行監控，一旦收到來自配電設備的警告或是事件訊息，控制中心需要能透過安全的方式傳送指令給配電設備，改變程控設備(PLC)及感應器設定，同時能收到動作完成的確認訊息。這時也可以透過兩次單向資料傳輸，將控制中心的接受訊息與傳送指令分開傳輸，此種模式，可以避免駭客以傳統雙向傳輸模式，提供偽造訊息並發送錯誤指令的風險。



資料來源 https://www.owlcyberdefense.com/

（三）Sandbox 創新比賽

RSA 創新比賽：除了展場及研討會外，現場還有創新比賽，由十數家新創公司，用 5 分鐘時間來闡述自家的產品技術及核心理念，相當精彩。

Axonius 贏得了本次 RSA Conference Sandbox 的冠軍，該公司原本是資訊設備管理軟體公司，但也同時提供資安的解決方案，讓客戶在管理設備的同時，也可以管理設備的資安規則。

管理的資訊設備除了一般的個人電腦也擴及到防火牆、路由器等網路設備，也包括辦公室常見的 WIFI、行動裝置及 IoT 產品，並透過資安規則的設定對管理的資訊產品進行防護。最後，Axonius 也有提供自動化管理功能，監控設備的使用異常行為，以降低資安風險。

二、NIST(NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)參訪

2013 年初，美國總統歐巴馬指示國家標準暨技術研究院（National Institute of Standards and Technology，NIST）與開發網路安全框架的機構或廠商合作，NIST 網路安全框架基於現有標準、指南和實務做法，以降低營運關鍵基礎設施之組織的資通安全風險。近幾年來對於關鍵基礎設施的威脅及發生之風險不斷增加，因此 NIST 網路安全框架也變得越來越重要。藉由 NIST 網路安全框架（NIST Cybersecurity Framework，NCF）與整合 ISO/IEC 27001 資訊安全管理系統，機構或組織皆可由 NCF 評估網路的資訊安全風險，採行合適的管控措施以降低風險。

（一）NIST 研討會

本次研討會是由美國在台協會商務組舉辦，透過與 NIST 部門人員的對談，了解 NIST 除了 Cybersecurity Framework 持續強化之外，也朝新領域如 AI security guidance，quantum machine security guidance 訂定新的標準和準則，讓美國的產業，組織及公司可以有一個依循的規範，當然，NIST 也歡迎世界各國參考他們的規範，以強化自身的資安風險管控。

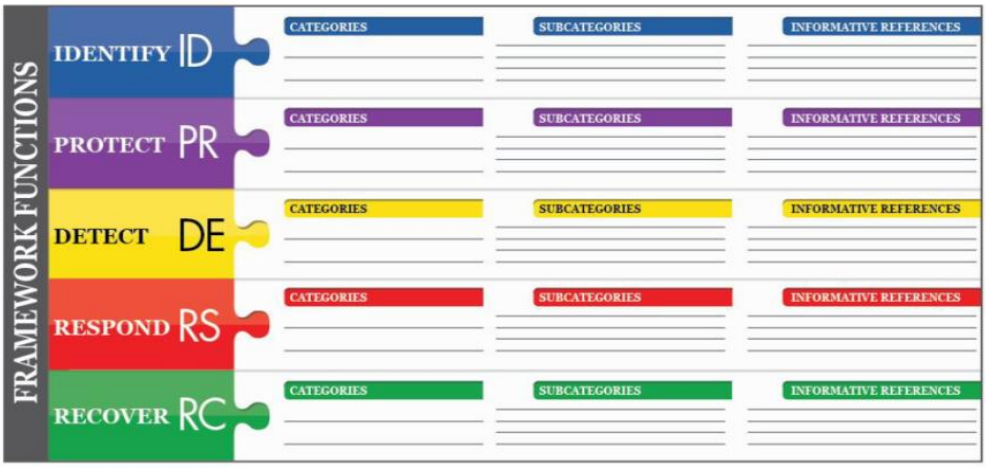
會中 NIST 也提到 Cybersecurity Framework 並非一個產品資安的測試標準，也不是一個資安產品的測試平台，該資安網路框架是提供原則性的資安遵循規範與 ISO 27001 相似，但他們強化了關鍵基礎設施的資安防護，對國家安全和人民生活息息相關的資訊和實體設備安全的風險管理，做了比較明確的指導。

（二）網路安全框架 Cybersecurity Framework

網路安全框架 Cybersecurity Framework 1.0 版是 2013 年 2 月依據 13636 號行動法案，由 NIST 發布的正式官方版本，其重點是改善關鍵基礎設施的

資安防護並為未來的資安規範提供指引。網路安全框架提供了一個比較彈性的方法，去強調資安對網路，實體設備及使用者的影響。該框架可適用於不同組織或機構的特性，例如:資安的要求是注重在 IT (Information Technology)，ICS (Industrial Control Systems)，CPS (Cyber-Physical Systems)，或是連接 IoT(Internet of Things)等設備。該安全框架也可以協助組織或機構去對客戶，員工或是第三方合作夥伴，去強調個人隱私資料對資通安全的影響。

網路安全框架的核心功能包含 5 個部份，包括 ID (Identify) ，PR (Protect) ，DE (Detect) ，RS (Respond) 及 RC (Recover)，如下圖所示：



Framework Core Structure

資料來源: https://doi.org/10.6028/NIST.CSWP.04162018

這 5 個核心功能彼此沒有順序關係,也可以同時進行其中某幾個功能，要視當時的風險管理情況而定。這 5 個功能說明如下：IDENTIFY (ID)是針對組織內部對系統，使用者，資產，資料，及可用性等風險的管理，要有一套明確的做法。例如在下表中，Category 為 AM (Asset Management)資產管理分類，其子分類有包含實體設備和系統在組織中的保管方式，或是子分類為軟體平台或應用系統在組織中的保管方式。同時，這些分類對應到的參考規範，也列在表格最後一欄: 例如常見的 ISO/IEC 27001，ISA (International Society of Automation) 62443 以及 NIST SP (Special Publication) 800。

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5

資料來源: https://doi.org/10.6028/NIST.CSWP.04162018

其他的核心功能像是 Protect (PR)是規範發展一套合適的安全防護措施以確保執行關鍵資料傳遞或服務時，這個過程要有適當的保護。而此一保護措施也包含了資安事件: 如權限控管及資料安全等；核心功能 Detect (DE)是規範要發展並執行適當的資安事件活動辨識方式，以便及時的發現有危險的資安事件，該功能包括像是即時監控，異常事件的發現及處理等；核心功能 Respond (RS)是規範要發展並執行的適當措施，以因應資安事件發生時要採舉的行動或其他潛在的風險，減緩資安事件的影響並避免事態擴大。核心功能 Recover (RC)是規範要發展並執行的適當及有彈性的維護措施，以回復自資安事件中受損或是中斷的服務，這個核心功能目標是要降低資安攻擊的影響，並能儘速恢復正常的服務。

（三） 卓越資安中心 NCCoE(The National Cybersecurity Center of Excellence)

最後，研討會中也提到 NIST 組織下的一個資安機構 NCCoE，透過此一機構提供業界有關資安的顧問服務，專案合作或規範導入等服務。藉由此一方式來推廣資安規範，以期能運用在各行各業中，降低業界導入資安規範的成本。這個模式，也可用於我國資安產業的推廣，經由專責的資安機構，讓產業能與資安相結合。

資料來源: https://www.nccoe.nist.gov/

NCCoE 的願景是提供前瞻的資安防護架構，促進科技的創新和增進經濟的成長。NCCoE 的任務是加速資安科技的推廣，和世界各地的資安機構及創新公司共同合作，提供現今世界一個可靠的標準化資安原則，以符合各行業的資安需求。

該組織未來的目標是提供可行的資安環境，幫助人們可以用更簡單方便低成本的方式，讓他們的數位資料以及數位基礎建設可以更安全。另一方面，也要加速一般公司在合理的預算下接收新的資安防護科技，減輕他們在資安防護上的負擔。最後，是加速資安產業的創新，讓資安新創者可以用更多有創意的方案去解決目前一般公司在資安議題上所遇到的瓶頸和難題。

三、PG&E(Pacific Gas and Electric) Company 參訪

太平洋瓦斯與電力公司簡稱 PG&E，總部位於舊金山的太平洋瓦電大樓，是美國一家提供加州約全州三分之二的區域，天然瓦斯和電力服務等的公用事業公司。本次參訪由 AIT 商務組帶領我方參訪團和 PG & E 的資安部門人員進行會談，另有該公司的資安協力廠商 Paloalto Network 一起參加這次會議，主要內容為 PG&E 的資安相關議題。

（一）PG&E 研討會

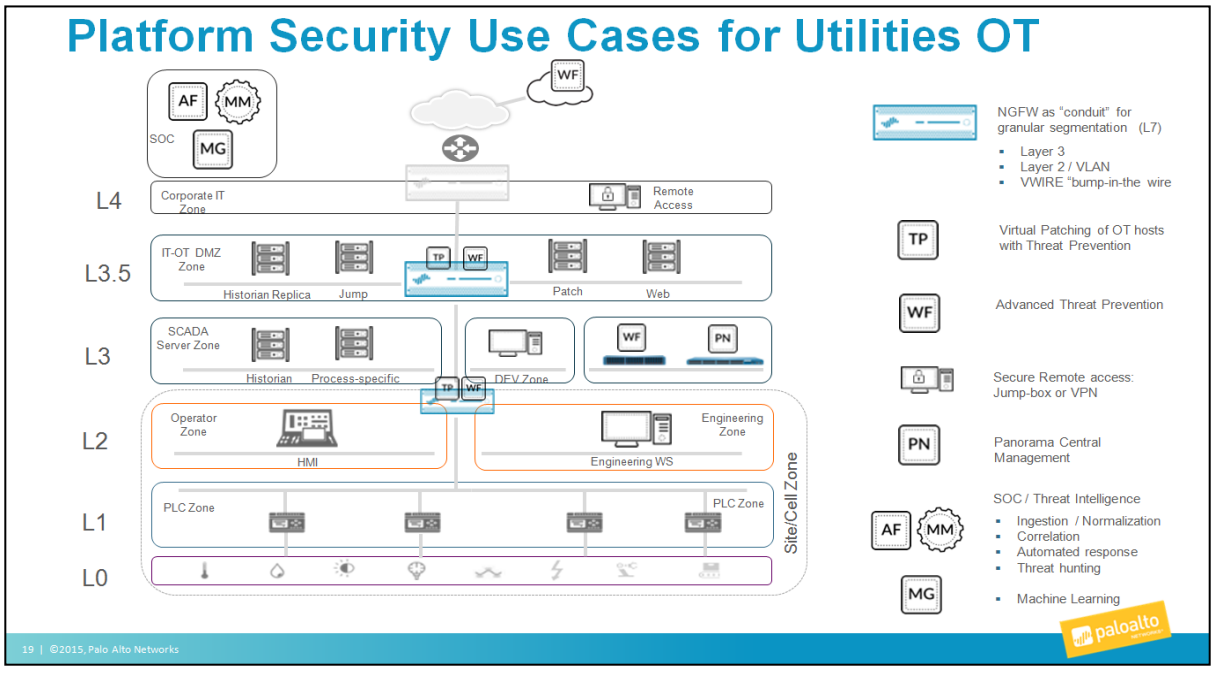
研討會中 PG&E 及 Paloalto Network 各自進行了公司簡介之後，由 PG&E 的資安主管介紹該公司的資安團隊和業務以及如何與 Paloalto Network 等協力廠商合作進行 PG&E 的資安業務。PG & E 的資安部門共 150 人，初期的資安團隊重點，在於全公司的風險及資產管理，將風險較高的資安議題優先處理，並且簡化作業流程以降低資安風險，當然，過程中也與資安廠商討論適合的解決方案，提供 PG&E 資料傳輸及營運作業的方案以避免資安威脅。

現在 PG&E 的資安業務已由初期的資安防護建置，邁向提供新的資安技術服務，就以下幾點說明: a.網路 AI 導入(network intelligence)：利用 AI 的技術加強網路的資安防護，由過去被動式資料庫更新，轉為主動辨識有高度資安風險的特徵值。b.全方位的監控(monitoring)：將 IT/OT 的端點設備資料透明化，可以同時監控兩者的即時動態資料，以防止異常事件發生 c.資安自動

化(automation)：將以往資安事件的分類與查檢，利用 AI 演算法自動判讀及處置，降低人為的負擔並提高準確率 d.遵循最新的 Cyber Security standard：依據政府資安部門提供的最新標準，更新資安防護作業或是更新設備，同時，e.與當地的資安協力廠商或是其他電力事業公司共同努力合作，打造更安全的資安環境。

研討會上也提出關於臺灣推展智慧電網時 IT/OT 間的資安建議，PG&E 的資安主管也提到，IT/OT 走向網路是不可避免的趨勢，因此在全公司都有高度共識下，推展了 SCADA 系統的數位化，加強網路資料傳輸的安全性以及設定資安防護的優先順序，尤其是在最前端的工作單位要能有效溝通，才能讓整個進度順利完成。對於協力廠商，也要遵守 Cybersecurity Framework 上的規範，從訂定合約，組裝測試及驗收，都要能符合規範上的要求。

（二）智慧電網的資安防護架構



PG&E 的資安防護架構示意圖(如上圖所示)主要分為五個部分: 1.OT 設備(包含輸配電等工作場域)，2 為 SCADA/HMI 設備 3.IT/OT DMZ 區域 4.企業內部 IT 環境 5.SOC 資安監控及管理。

在 OT 設備(上圖 L0~L2)中，包含感應器，PLC 控制單元，電腦機房和工程用區域都以防火牆在內部以虛擬網段切割，各自有防護區域並由防火牆提供整體資安防護。在 SCADA/HMI 設備(上圖中 L3)中，亦由兩組防火牆設備作實體網段分割，因其需要讀取來自 OT 設備的資料，並能傳輸至 IT/OT DMZ 區，故在架構上為獨立的實體網段，以便能同時能承接不同場域的 OT 設備，由 SCADA/HMI 作資料集中控管並回傳至 IT/OT Zone。在 IT/OT DMZ 區域(上圖中 L3.5)則包含了備份資料中心，企業網站及軟體更新派送等服務，一方面作為資安防護的非軍事區(DMZ)避免直接來自網際網路的攻擊，另一方面也提供基礎的資安服務或是放置易受網路攻擊的服務(如企業網站)。

在企業內部 IT 環境(上圖中 L4)，則透過防火牆和網際網路作連結，在這個區域內包含員工電腦及各項裝置(如印表機，WIFI)都在 SOC 端點防護的管控中，其他如 VPN(虛擬私有網路)連線，也都納入 SOC 監控中，SOC 也提供資安規則的發布，即時更新每個端點的防護功能，同時，SOC 的功能也加入機器學習及自動防護等概念，讓資安防護的人力資源配置和防護精準度都可以大幅度的改善。

在 IT/OT 的資安防護上，業界多建議 IT 與 OT 的 SOC 能合併一起，不要分開設置，保持資料監控和資安防護的一致性，也同時避免疊床架屋的網路防護架構，造成更多漏洞的產生。並且，利用新的資安科技運用在現有的設備上，不但可以降低資安建置成本，也可以發揮更多的效益。這幾年世界各國的關鍵基礎設施(如烏克蘭電廠)頻遭駭客攻擊，除了瞭解這些受害案例的原因之外，也要能隨時注意會造成資安漏洞的地方，並加以防範，才能作好資安防護的工作。

四、CISO(California Independent System Operator)參訪

加州電力調度中心(California Independent System Operator，CISO)建立於 1998 年，負責營運加州約 80%與部分內華達州地區的電力市場以及管理電網可靠度之非營利公共組織。當天拜訪時，行銷主管告知，目前再生能源裝置容量約占全系統容量的 59%，又以太陽光電為主要來源，而當大量太陽光電併入電網改變了系統負載的型態，白天太陽光電抵銷大量負載，而到了傍晚因太陽光電無法再發電而導致負載突升，因此，CISO 的電力調度可以說是十分具挑戰性。

（一）CISO 研討會

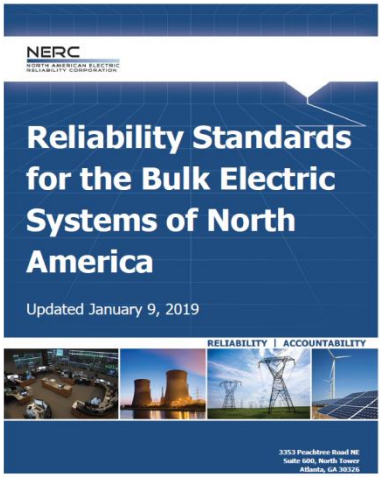
本場研討會除了介紹 CISO 的資安團隊業務內容及工作模式外，研討的主題著重在 CISO 的 SCADA 資安架構以及如何遵照NERC CIP 的規範，運用在 CISO 的資安防護上。

CISO 的資安團隊主要分為法規及網路設備兩個部門，前者會檢視聯邦或是州政府要求的關鍵基礎設施規範，定訂要遵循的作業流程及資安設備的架構；另一組網路設備組則負責實際設備的管理及資安事件監控，並根據資安要求設有異地緊急應變中心，兩者在業務上相互配合，以因應各種可能的駭客攻擊事件。

CISO 的 SCADA 中心以防火牆和企業內部的 IT 設備作實體網路區隔，以防護在 SCADA 內部的程控設備，監控設備以及連線到各電廠的即時資料，並且還有儲存歷史資料的資料庫；在企業內部的 IT 設備則以防火牆和網際網路作實體網路區隔，如有員工要透過網際網路連線至企業內部，則需要透過 VPN 以二階段驗證方式連接企業內部 IT 設備，如要再連接至 SCADA 中心，還要額外透過 Jump 主機，同時再作一次二階段驗證，才能讀取 SCADA 內部的資料。

在會中 CISO 主管也提到，他們遵循的法規主要為 North American Electric Reliability Corporation (NERC)，源自於聯邦法規 FERC，是電力基礎設施的規範，其中 Critical Infrastructure Protection (CIP)與資安防護有關，例如: CIP005 提供防火牆的防護措施，CIP006 提供實體設備的防護說明。

（二）關鍵基礎設施防護 NERC-CIP (Critical infrastructure protection)



NERC(North American Electric Reliability Corporation)北美電力可靠性公司是一家非營利性國際監管機構，其任務是確保北美高容量電力系統的可靠性。NERC 負責美國，加拿大及墨西哥下加州的一部分，位於該地區的電力系統運營商皆需要滿足其安全標準，包括網路資通安全。

關於關鍵基礎設施保護（CIP）安全標準：

NERC 關鍵基礎設施保護（NERC-CIP）規定了大容量電力系統的最低安全要求標準以及電力系統資安問題的規則，包括使用軟體漏洞評估工具測試和修復關鍵資產的安全問題。以下圖 CIP-003-7 文件為例，其定義安全管理管控，在文件中會說明要達成的目標，適用範圍及細項說明。

CIP-003-7 - Cyber Security — Security Management Controls

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003-7
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
   - 4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

資料來源: https://www.nerc.com/pa/Stand/pages/cipstandards.aspx

NERC CIP-003 "安全管理控管" 中，要求網路管理員或負責的單位能夠改善或精進保護關鍵網路資產的現有策略；其他文件例如:NERC CIP-002 "識別關鍵網路資產" 要求識別和記錄電力系統中的所有關鍵網路資產，這種方式可以幫助管理者或組織了解在關鍵網路資產受到損害時，可能發生的影響和損害。

肆、出國心得

本次參加在美國舊金山地區舉辦的 RSA Conference 2019 大會，現就參訪研討之見聞並與不同領域人員意見交流以及上述關鍵基礎設施與智慧電網之資通安全相關應用，心得如下：

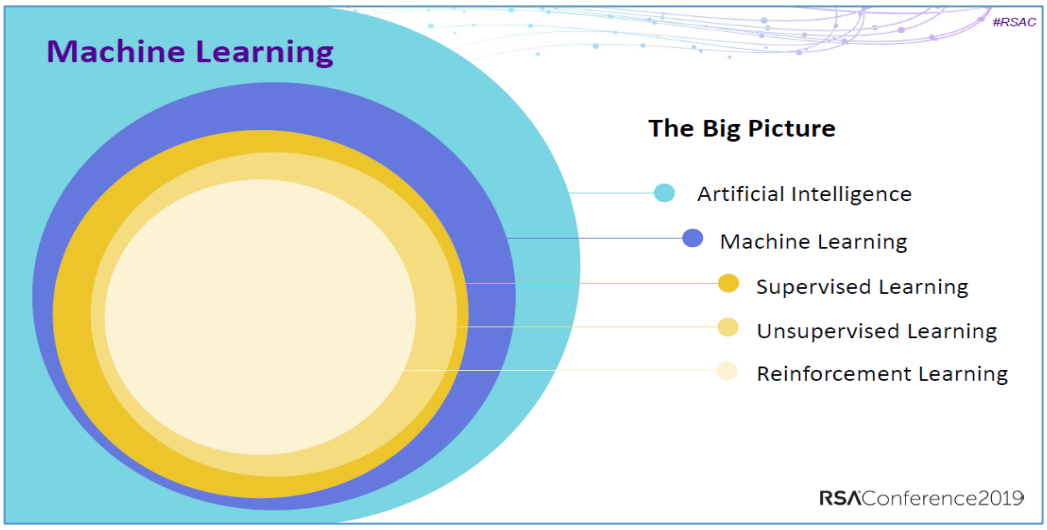
(一) IT/OT 將以雲端端點防護為主流:

雲端端點防護 cloud native endpoint protection platform (SaaS) 是次世代端點防護主流，在本次展覽中已有多家資安大廠投入相關領域，在美國包含許多領域之藍籌股公司，像是金融服務、能源、石油天然氣、電信業、零售業與科技產業，以及國際間的政府機關也都陸續採用。雲端端點防護提供威脅自動化偵測與資安事件前後之對照服務。透過訂閱模式的偵測軟體配置，提供設備端點之資安服務。雲端端點防護整合次世代防毒(Next-Generation Anti-Virus)、端點偵測與回應(Endpoint Detection & Response)和全方位的威脅獵捕(Threat Hunting)服務，並透過端點監控與回應，增加企業資安團隊的效率以及提供更精確的監控。

其次，在 IT/OT 和網路環境中，如果發生違反政策的流量或資安漏洞被利用時，可利用新的技術將可疑流量引入虛擬誘餌網路(Decoy Network)，以進行下一步的資安威脅情報收集。大多數駭客都會尋找阻力最小的路徑，並嘗試各種可用於入侵組織內部的電腦或是 IT/OT 設備的網路連線通道、文字記錄檔和資料庫等。虛擬誘餌網路設計，在駭客試圖破壞之前為其提供「合法」的活動區域作為誘餌區，並在資安資料庫中留下他們的搜尋的路徑、使用的工具及執行過的軟體。之後，將其連接到 Secure 雲端，觀察其實際攻擊的手法和運作模式的特徵值，作為異常入侵時的判斷數據以防止類似攻擊手法再度發生。因此，虛擬誘餌網路結合 Secure 雲端，可以進行攻擊隔離，從而降低組織的資安風險。

(二) 人工智慧與機器學習技術大量運用在資安產品上

次世代的網路資安設備在本次展覽中也廣泛的出現，主要的亮點就是透過人工智慧與機器學習技術來精進資安防護的精準度，而使用這些技術的資安設備和以往使用資料庫或是被動式特徵碼等前一世代的產品已有明顯的區隔和差異。人工智慧包含使用強大的演算法來讓電腦可以比人類更準確、更有效地完成任務，也替自動化及其他關鍵流程開啟了大門，使用人工智慧讓硬體可以用自己的方式思考。另一方面，機器學習更進一步地讓電腦不僅能夠完成以前需要人為干預的工作，還可以根據這些工作經驗，用於改善工作的效率並自我學習。



從上圖我們可以得知，雖然人工智慧和機器學習經常會放在一起討論，但它們並不是相同的概念。今日的科技及分析領域中許多最先進的作法都應用了人工智慧（AI）與機器學習（ML），這些創新方法所能進行的技術應用，讓資安設備的軟硬體能夠根據具體效能指標來做出準確的預測。

利用人工智慧與機器學習（無論是單獨使用或互相結合）應用在資安領域的技術上，相關人員及管理者都必須了解如何將其應用在業務上及所可能帶來的優勢。除了產業法規遵循外，重要的是將這些進階作法加入資安安全防護的一環，與其他已有的保護措施相互合作。

(三) 資通安全自動化

雲端技術、人工智慧和機器學習，讓資安自動化的理想正逐漸成形，正確的自動化工具實際上可以提供更高品質的資安防護，並加強對整個網路安全流程的監督。專業的資安人員在早期很容易感覺到他們比機器更能正確處理緊急的資安事件，但隨著駭客攻擊類型，頻率和復雜性的轉變，人為監控已無法有效處理，故資安自動化在產業界已經默默的進行中。

近年來，許多最重大的網路資安事件都來自人為因素。即使是最熟練的 IT 專業人員也不時會犯錯誤。不幸的是，一些錯誤的成本可能會非常昂貴。資安自動化的優點之一，即是透過這種機制將資通安全防護工作中的人為因素可以降到最低。

最後，資通安全的決策者或管理者面臨的最大挑戰之一，是面對重大的資安事件時，能即時對後續的危機處理進行決策。因此資安自動化的另一個好處是它能夠收集海量資料進行大數據分析，確定關鍵數據的優先等級，從而協助資通安全的決策者或管理對重大資安事件進行管理。

(四) RSA 今年度主題「BETTER」

RSA 今年度主題是「BETTER」：創造更好的資安環境。由於資訊產業的快速演變，讓資安的議題日漸重要，但以往訂定的法律，或是產業規範已漸漸跟不上資安的演變，例如：金融業有來自比特幣造成的金融安全問題，或是像電廠之類的關鍵基礎設施屢遭駭客破壞，這些問題已非現有的法律所能規範和保障，因此，在本次的參訪過程中，來自政府，學界及產業界的專業人士都認為，要打造更好的資安環境，要從社會制度面去做進一步的改善。

在網路安全日益受到威脅的今日，個人數位資料的保護已成為重要課題。但為了資通安全，匿名制的會員，交易及付費方式將會受到嚴格的檢視，取而代之的將會是實名制的身分驗證，而個人資料要如何安全的在網路上使用，除了有個人資料運用的問題，也有隱私上的爭議。這些問題，除了透過技術上的改善之外，也必須透過法律來做更明確的規範。

資安的問題也衍伸出另一個議題，就是網路信賴的程度。在早期網際網路時期，是沒有任何限制，任何使用者或是任何設備都可以信賴收到的資料是正確且可相信的，然而，數十年快速的發展結果，造成駭客肆虐並威脅到網際網路環境，現今網路信賴度的維持，除了使用者要以實名制的方式管理，所有組織和企業內部的 IT/OT 設備，也要有自己的”可識別的身份”，例如: 每台電腦都有自己的 ip 或是 mac address，這些資料必須要經過管理者確認，並登記在資安設備上，如此，該設備才是合法的可受信賴的資料來源。

最後，在多場會議的專家學者討論及交換意見中，資通安全在技術發展的同時，也應注意資通安全推廣的重要性，透過社會教育方式，可以將技術與研究成果相關資訊散布給一般民眾，用簡單且淺顯易懂的言論，讓民眾養成資安的警覺性。國際間各項研究都著重在培養資安人才，本次與會可發現資安教育已從美國的高中及社區學習中展開，且相關學者也有年輕化的趨勢，國內在積極進行各項關鍵基礎設施的建構時，也應著手培養不同世代之參與人員，以確保國家資通安全得以永續經營。

伍、建議

本次參加於 3 月 4 日至 3 月 8 日在舊金山舉行全美最重要的資安大會 RSA Conference 2019 及關鍵基礎設施機構參訪，就與會經驗與實習心得，相關建議如下：

一、 加強參加國際資通安全之研討會，可瞭解國際技術與產業發展現況，透過與國際專家經驗交流，可作為公司 IT/OT 資安計畫規劃與執行之參考，亦有助於確保公司資通安全技術能與國際接軌。

二、 未來關鍵基礎設施的資通安全即為國防的一環，需強化社會教育並透過宣傳、互動媒體、公開演說及大型研討會等，增加民眾對智慧電網資安議題之瞭解，亦可藉此傳達智慧電網相關技術的發展現況，以提升民眾對智慧電網之用電觀念，以及對相關知識的瞭解。

三、 資通安全防護為長期發展計畫，且涉及多項網路通訊，資訊領域與各工程專業領域間之整合，為確保相關專業技術、研究成果及經驗能順利傳承，以及培養整合管理之人才，應持續培育相關人才庫。

陸、附錄

RSA Conference 2019 簡要議程

As always, we thank you for being here and contributing to the critical cybersecurity conversations that take place at RSA Conference each and every year. It is our mission to bring cybersecurity professionals together to forward the industry and empower the collective "we."

This year's theme is, to put it simply, *Better*. Which means working hard to find better solutions. Making better connections with peers from around the world. And keeping the digital world safe so everyone can get on with making the real world a better place.

RSA Conference is the time and the place to remind us to make security a top priority—this week, but also every day. A better, safer world is ahead when we have the drive, the strength and the vision to work together to create it. We hope you find inspiration in the brilliantly led sessions and keynotes, the cutting-edge technology in our Expo, and of course, the innovations showcased in RSAC Innovation Sandbox, RSAC Sandbox, RSAC Early Stage Expo and our brand new program, RSAC Launch Pad, taking place on Tuesday afternoon.

Thank you for being a part of this Conference. Enjoy the week of learning and networking ahead—and don't forget to enjoy social time with your peers at the many special events throughout the week. We're already looking forward to RSA Conference 2019 Asia Pacific & Japan in Singapore on July 16-18 and encourage you, or your colleagues in that part of the world, to join us there for deep, rich, regional and global cybersecurity conversations.

Until next time, let's continue the conversations on *RSAConference.com* and through social media using *#RSAC*.

Sincerely,

Linda Gray Martin
Director and Chief of Operations
RSA Conference

Download our Mobile App

Download the RSA Conference 2019 Mobile App to stay up-to-date with all the Conference activities happening throughout the week. Build your own personalized schedule, participate in polls for select sessions, and find your way around the RSAC Campus—which includes the Moscone Center and Marriott Marquis—with our maps. Visit ***www.rsaconference.com/app1*** or scan this QR code to get started.

PLAN YOUR EXPERIENCE

SUNDAY / MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
EXPO

AGENDA AT-A-GLANCE

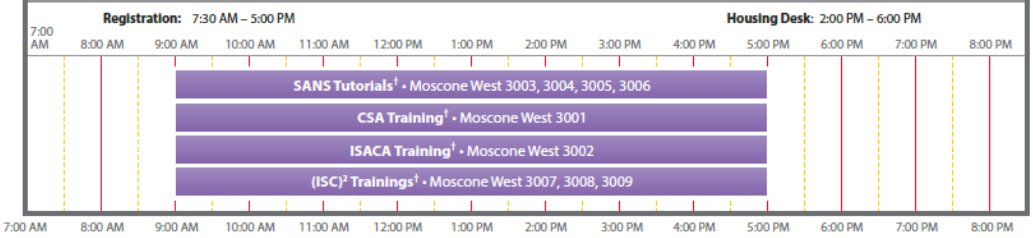
SATURDAY, MARCH 2

Registration: 2:00 PM – 6:00 PM

SUNDAY, MARCH 3

Registration: 7:30 AM – 5:00 PM

Housing Desk: 2:00 PM – 6:00 PM

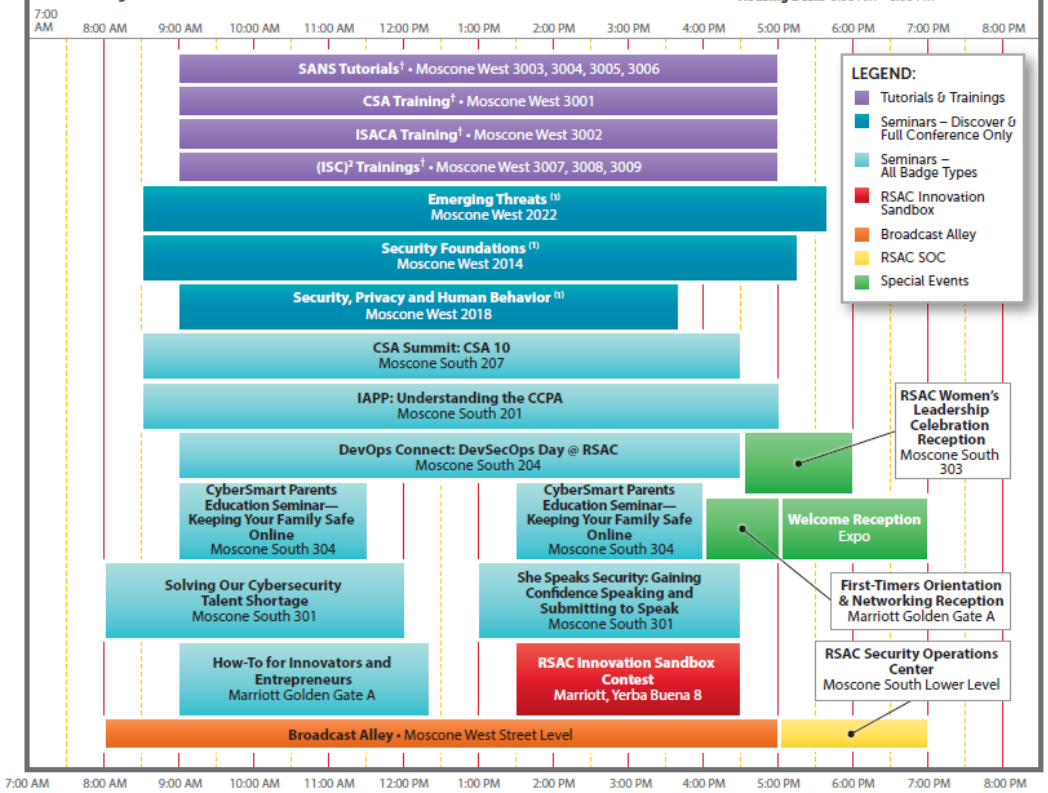


MONDAY, MARCH 4

Registration: 7:00 AM – 7:00 PM

Bookstore: 8:00 AM – 7:00 PM

Housing Desk: 8:00 AM – 6:00 PM

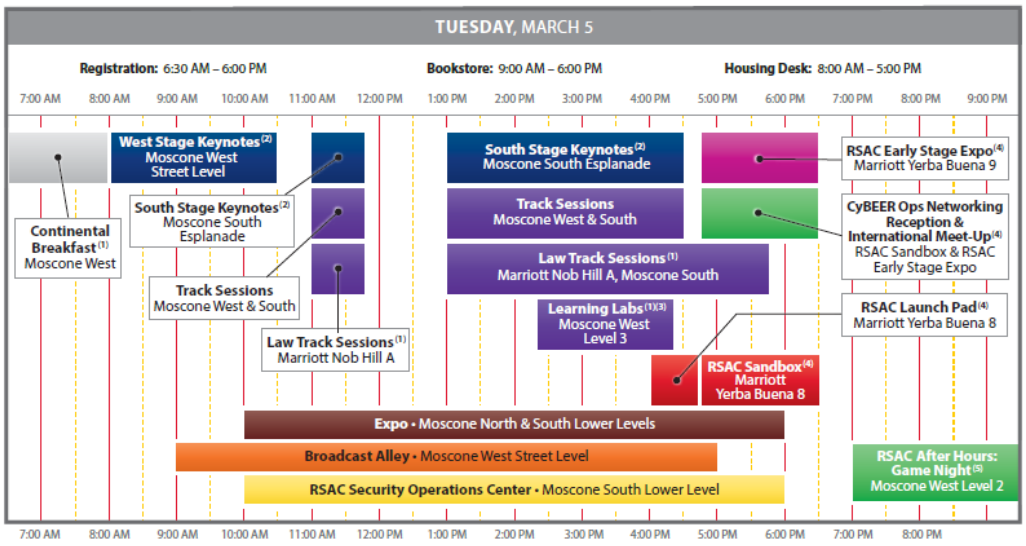


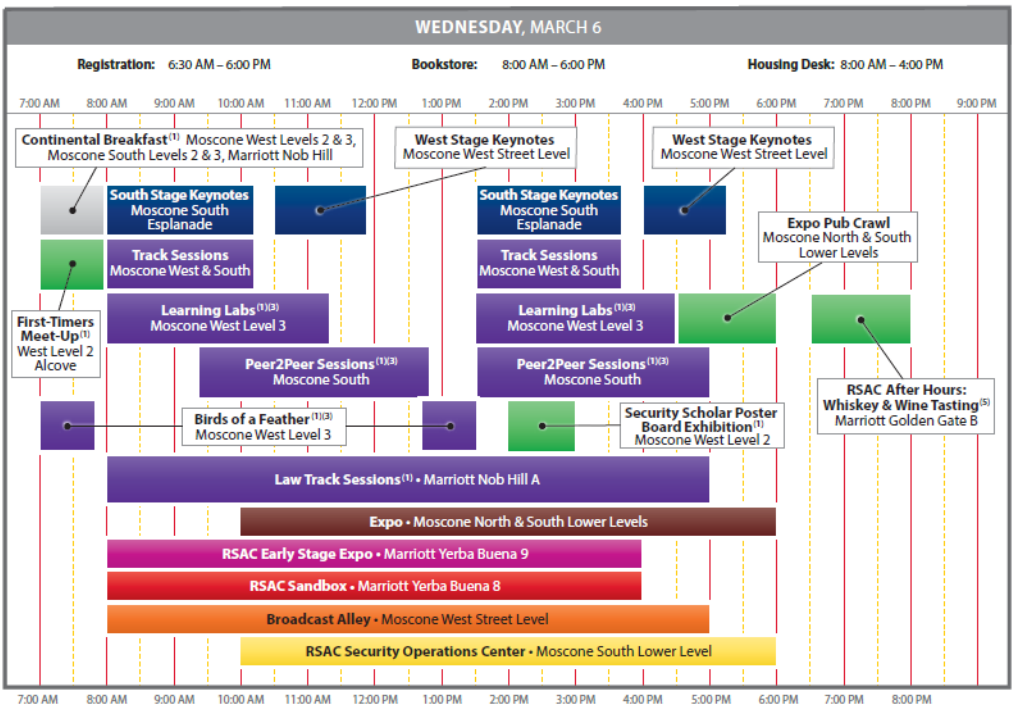
For room locations see maps on pages 8–11.

† SANS Tutorials and CSA, ISACA and (ISC)² Trainings are offered for an additional fee. *(1) Open to Full Conference and Discover Pass holders only.*

Sessions and speakers are subject to change; please visit www.rsaconference.com/us2019 for the most up-to-date information.

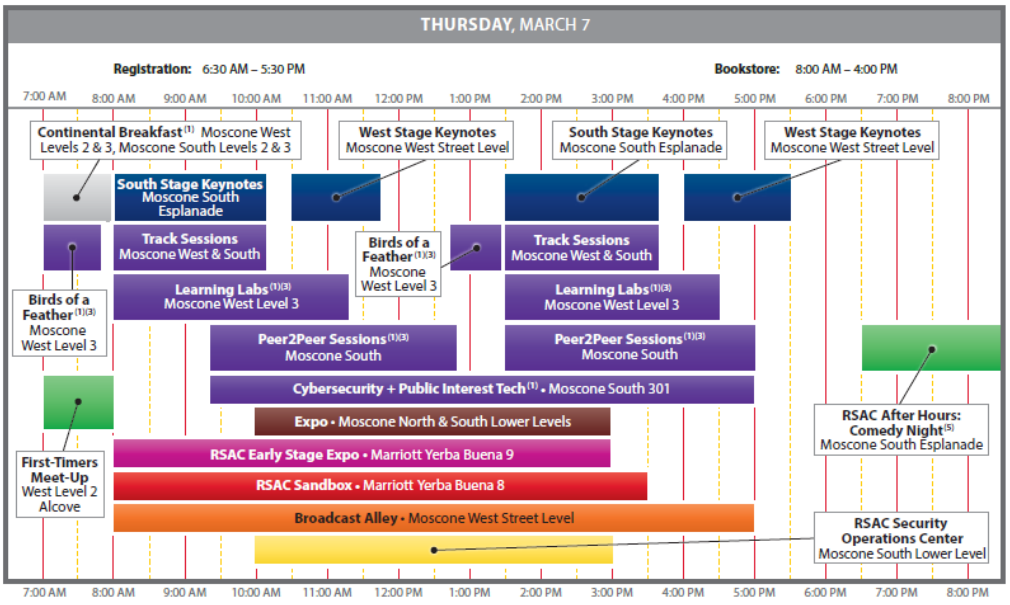
AGENDA AT-A-GLANCE



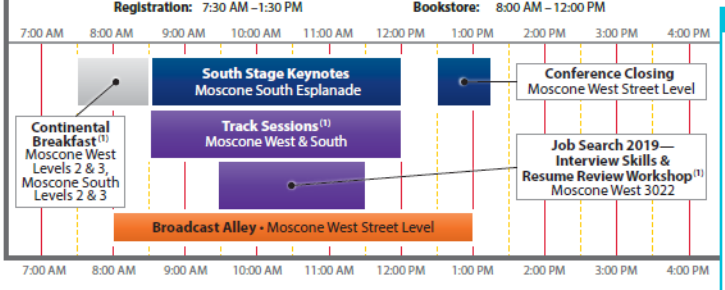


AGENDA AT-A-GLANCE

THURSDAY, MARCH 7



FRIDAY, MARCH 8



LEGEND:

- Keynotes
- Sessions
- Expo
- RSAC Early Stage Expo
- RSAC Sandbox
- Broadcast Alley
- RSAC SOC
- Special Events

Notes:

(1) Open to Full Conference Pass holders only.

(2) Open to Full Conference and Discover Pass holders only.

(3) Limited seating. No press permitted in Peer2Peer sessions, Birds of a Feather sessions and Learning Labs.

(4) Open to Full Conference Pass holders, Tuesday One-Day Full Conference Pass holders, Press and CyBEER Ops ticket holders only.

(5) Open to Full Conference and Discover Pass holders, and Full Conference One-Day Pass holders for their day of admittance only. Choose one among the three RSAC After Hours events offered.

For room locations see maps on pages 8–11.

Sessions and speakers are subject to change; please visit www.rsaconference.com/us2019 for the most up-to-date information.

INFO DESK HOURS

Sunday	
South Street Level	7:30 AM – 5:00 PM
West Street Level	7:30 AM – 5:00 PM
Monday	
North Lower Level	4:30 PM – 7:00 PM
South Street Level	7:00 AM – 7:00 PM
West Street Level	7:00 AM – 6:00 PM
North Expo, South Expo	5:00 PM – 7:00 PM
Marriott Marquis	7:30 AM – 5:00 PM
Tuesday	
North Lower Level	9:30 AM – 6:00 PM
South Street Level	8:00 AM – 4:15 PM
West Street Level	6:30 AM – 7:00 PM
North Expo, South Expo	10:00 AM – 6:00 PM
Marriott Marquis	10:30 AM – 6:00 PM
Wednesday	
North Lower Level	9:30 AM – 6:00 PM
South Street Level	7:30 AM – 6:00 PM
West Street Level	6:30 AM – 6:00 PM
North Expo, South Expo	10:00 AM – 6:00 PM
Marriott Marquis	7:30 AM – 6:00 PM
Thursday	
North Lower Level	9:30 AM – 3:00 PM
South Street Level	7:30 AM – 4:00 PM
West Street Level	6:30 AM – 6:00 PM
North Expo, South Expo	10:00 AM – 3:00 PM
Marriott Marquis	7:30 AM – 6:00 PM
Friday	
South Street Level	8:30 AM – 12:30 PM
West Street Level	8:00 AM – 2:00 PM