財團法人電信技術中心

2018 年 ISRAEL HLS & CYBER

出國報告

服務機關：財團法人電信技術中心資通安全組

出國人員：陳坤裕工程師

派赴國家：以色列

出國期間：107 年 11 月 10 日至 11 月 17 日

報告日期：2018 年 11 月 30 日

出國報告摘要

以色列國土安全與資安會議 (Israel HLS&CYBER 2018) 於 2018 年 11 月 12 日至 2018 年 11 月 15 日於以色列特拉維夫 Israel Convention Center, Tel Aviv 舉辦，此行主要目的為參訪以色列資安廠商，觀摩其核心價值並反思，以裨益本中心執行資安旗艦計畫能更切中要點。

參訪廠商有以色列電力公司 (IEC)、Verient、Radiflow、CyberGym、L7 Defence、CORO.NET、Merlinx、GoldTech、TSG IT Systems、Glassbox、OpenLegacy、Communtake、KAYMERA、Intezer、Radware、Leumi Bank SOC、Gav-Yam Negev Advanced Technologies Park。會議另一個目的是搭建業務交流平台，資安產業是人才驅動的產業，一定要與外部產生關聯，不能閉門造車，如何與產業內的頂尖人物交流並建立業務關係，是一項挑戰。

綜觀而言，此行拓展了我們在資訊安全的視野，也藉由參訪時與講者討論，更深入了解他們產品的概念與細節，取得最新發展趨勢與第一手研究資訊，增進我們對資安產業的理解，明白以色列資安廠商如何應對政策與市場之合理期待，並將這些經驗帶回給資通安全組成員，提升整體資訊安全知識能量。

目次

壹、會議參加目的.....3

貳、會議時間、議程與地點 4

參、會議摘要.....5

肆、心得及建議.....10

壹、會議參加目的

以色列國土安全與資安會議 (Israel HLS&CYBER 2018) 於 2018 年 11 月 12 日至 2018 年 11 月 15 日於以色列特拉維夫 Israel Convention Center, Tel Aviv 舉辦，此行主要目的為參訪以色列資安廠商，觀摩其核心價值並反思，以提升本中心執行資安相關計畫時，能更切中要點。本次行程參與同仁除本中心陳坤裕工程師外，一行還有通傳會蘇思漢簡正、葉世湛分析師與林祐仲技正。

此會議涵蓋之資安議題有 National Security、Cyber Crime、Transportation、Fintech、Manufacturing 與 Enterprise and IOT。此外，大會亦安排我們前往以色列電力公司 (IEC)、Verient、Radware、Leumi Bank SOC 以及 Gav-Yam Negev Advanced Technologies Park 參訪。希望藉由參與此會議與各資安公司參訪，能以更廣泛的層面理解資安議題與其切入要點。

圖 1、HLS& CYBER 2018 涵蓋之會議議題

貳、會議時間、議程與地點

本次會議時間、議程與地點如下所示

- 舉辦日期：2018 年 11 月 12 日至 2018 年 11 月 15 日
- 舉辦地點：主要位於 Israel Convention Center, Tel Aviv，其餘在 IEC、Verient、Radware 與 Leumi Bank 各公司參訪。
- 會議議程：

表 1、HLS & CYBER 議程

2018 年 11 月 12 日	
時間	主題
09:00-12:00	以色列電力公司
14:00-16:00	Verient
18:30-19:00	Registration
19:00-21:30	Gala Evening: Hangar 11, Tel Aviv Port
2018 年 11 月 13 日	
08:30-09:30	Coffee & Registration: Hall 2, Tel Aviv Convention Center
09:30-11:15	Exhibition & Plenary Sessions
11:15-11:45	Coffee Break
11:45-13:00	Exhibition & Plenary Sessions
13:00-14:00	Lunch Break
14:00-18:00	Exhibition, Plenary Sessions & Satellite Events
2018 年 11 月 14 日	
09:00-12:00	Radware
14:00-16:00	Leumi Bank SOC
2018 年 11 月 15 日	
09:00-12:00	Gav-Yam Negev Advanced Technologies Park

參、會議摘要

此次本中心資安組派員前往 ISRAEL HLS & CYBER 2018，主要目的為參訪以色列資安廠商，觀摩其核心價值並反思，以提升本中心執行資安相關計畫時，能更切中要點。下面為參展廠商之產品摘要、參訪廠商之心得摘要及相關背景介紹：

- 以色列電力公司 (IEC)
    - 公司簡介

      以色列最大的電力供應公司，政府擁有該公司 99.85%的股權為國營事業。該公司提供發電站的建立、維護和運行；送電和配電網等業務。亦是唯一的綜合電力公司，其裝機容量約佔以色列總發電量的 80%，並傳輸和分配以色列的絕大部分電力。因政治環境以致不使用核能發電，主要使用天然氣發電，少部分使用煤發電。
    - 參訪心得

      該公司以風險為考量擬定資安防禦策略。其中提到較關鍵點如下：1. 公司的資安人員要比操作人員更瞭解各層面的技術細節。2. 員工的待遇及管理制度不健全，將造成該名員工洩漏機敏資料。3. 資安演練係以建置實際設施及系統實施攻防演練，以確保演練真實性。4. 公司花費許多的時間及人力達到系統不中斷及迅速恢復。
- Verint
    - 公司簡介

      Verint 成立 20 餘年，係資安解決方案的專業顧問，並為組織提供了重要的見解，使決策者能夠預測、應變及採取行動。該公司的產品組合係利用機器學習技術和進階分析，將資訊轉化為洞察力。迄今超過 180 個國家的 10,000 多家組織，包括財富雜誌所列百大公司 80%和政府機構都使用 Verint Actionable Intelligence 解決方案。
    - 參訪心得

      介紹主要公司產品 TPS(Threat Protection System)係透過原有資安設備(如:防火牆、入侵偵測防禦系統、防毒系統)及額外安裝於終端設備(如個人電腦、伺服器)情報蒐集軟體所提供資訊及網路流量封包，經過系統的判斷機制(演算法、情資資料庫等)處理後，產出有意義的資訊供資安人員後續判斷。另外，除上述使用固定特徵判斷資安事件外，並使用人工智慧解析駭客行為模式，當網路行為符合更多的前述行為模式時，就更有可為視為網路攻擊行為。

- Radiflow
    - 提供國防基礎設施 (如：電力、水庫與交通運輸系統)之安全評估服務。該公司會先審視網路架構、相關設施，將潛在問題描繪出後，提出測試計畫。隨後啟動監控與分析網路流量，並提出可能被攻擊之弱點。
- CyberGym
    - 透過客製化建立與企業相仿之資訊環境，並利用 Red team 實際找出已存在或潛在資安威脅，將此邏輯以教育訓練方式傳授給企業資訊人員，使其擁有駭客思維，從攻擊角度思考如何防禦。
- L7 Defence
    - 監聽網路流量並使用 AI 分析判斷出惡意行為後，動態回饋調整阻擋規則。
    - 為達到良好效能，網路監聽可僅取樣 5%，並卸載低使用率之阻擋規則。
- CORO.NET
    - 針對在家或非常駐辦公室工作者，提供一套確保工作者進行遠端連線時，亦能透過安全網路遠端工作。
    - 該公司提供之產品，亦結合 google map，以視覺化方式讓使用者理解附近無線網路之安全性，如產生安全疑慮，將會對使用者示警。
- Merlinx
    - EAGLE: 利用中間人技術(Man in the middle，MITM)，在使用者及 Wi-FI AP 中監聽，取得經 Wi-Fi AP 傳輸的資料流，並可將木馬程式注入使用者端，對使用者進行監聽。(使用小到可放入被包的中間人攻擊套件取得經 Wi-Fi 傳輸的資料流，就算是加密的資料也可經解密後萃取出有意義的資料。)
    - MARS: 可遠端控制受感染的裝置並執行特定指令。
    - 這兩項產品只提供政府司法警察機關使用，並不賣給民間企業。
- GoldTech
    - 該公司之產品光學 IFF(Identification Friend or Foe)主要利用熱能信標(Thermal beacon)，做到敵我識別，同時利用高功率的可見紅外線雷射指標器，可標示攻擊目標，以利友軍發起精準之飽和攻擊。
    - 該公司也製造軍用高解析度之數位視訊記錄器，以及移動式軍用通信電臺車輛，可隨時隨地架設起 20 米的直立鐵架，可乘載 900 公斤之重量。

- TSG IT Systems
    - 使用影像分析引擎分析監視器即時拍得的影像，再經規則引擎分析切割出來的影像後，對可疑行為發出警示。
    - 也可分析過去錄製的歷史影像。
- Barrel
    - 透過 Email、uber 帳單等方式蒐集個人資料， 經切塊拆分成各種類型的資料並加密後，透過區塊鏈 smart contract 的方式提供給客戶分析統計使用。
    - Barrel 的客戶並無法直接取得個人資料，僅能使用 Barrel 提供的介面分析出使用者的特性提供公司策略運用。
- Glassbox
    - 該公司之產品主要目的為分析使用者在網站上之行為 (如：點擊 A 連結後，再點擊 B 連結)。此公司分析之方法為建立相關腳本，並比對使用者行為與腳本是否有差異，若有不同，則提供使用者實際行為之所有相關資訊，反饋給企業，讓企業重新設計網頁瀏覽流程，達到精準訊息之傳遞或提高銷售業績。
- OpenLegacy
    - 許多企業 (例如：銀行) 至今使用老舊 大型主機(mainframe) 系統。對資訊人員而言，升級與維護是艱鉅的課題，此公司之產品提供一套中介服務，嫁接在企業舊有系統上，企業可透過此中間層提供之接口進行系統功能之新增與修改。
- COMMUNTAKE
    - 與 KAYMERA 公司提供類似之集中控管服務。差異為，KAYMERA 公司專注在軟體面，而 INTACTPHONE 公司則兼顧硬體，駭客拿到使用者手機後，亦無法破解入侵。
- KAYMERA
    - 提供一集中管理系統，管理使用者之終端手機 (使用者手機需安裝 agent)。資安人員可透過此系統調整終端手機內 App 使用之權限，並建立相關的 rule，確保使用者不受資安威脅。
- Intezer
    - 將 DNA 概念引用至惡意程式中，建立惡意程式 DNA 資料庫。分析系統將欲分析之惡意程式先採集其 DNA，並從 DNA 資料庫中比對，找尋該惡意程式是否源自某惡意程式家族。
    - 該公司分析系統亦有脫殼技術 (unpacked)，會先偵測惡意程式是否使用加殼技術，若有，則將該惡意程式脫殼，隨後再採集 DNA 進行比對。
    - 若遇到無法偵測出之加殼技術，則該系統會動態運行此惡意程式，並將相關程序從記憶體中取出，再採集 DNA 進行比對。

- Radware
  - 公司介紹

    Radware 係為協助公司建置網絡安全和模擬資安防護的應用解決方案，並提供資安軟硬體服務及最安全的雲端服務中心等。
  - 簡報重點
    - 3G / 4G 訊息集中在核心網路伺服器(Core Network Server)，而 5G 把能在 Edge 處理掉的事情儘量在 Edge 處理(稱為邊緣運算)，好處是訊息可以不用經過層層關卡送回到核心網路處理而造成塞車，壞處則是使用者容易因為誤動作或惡意目的對系統造成破壞，或者是邊緣伺服器容易被駭客攻擊造成資料洩漏。
    - 在 5G 網路中 IoT 的運用將更為活耀，但也同時帶來威脅。IoT 裝置通常因為成本低，因此沒有良好的軟體設計，造成資安防護能力不足，容易淪為駭客跳板或變成 Botnet 執行 DDoS 攻擊的工具，也有駭客利用 IoT 來作為 Digital Currency : 虛擬貨幣的挖礦工具。
    - Radware 的產品 DefensePro 是結合 Dos 防護、行為分析、IPS 的攻擊緩解設備，透過行為分析技術來進行攻擊緩解，除了可防護網路層攻擊外，還可以針對第七層的內容進行檢查，並提供 IPS 防護功能，可說是一台多功能的資安設備。葉分析師世湛提問，現今 DDoS 攻擊常達到 10Gps 甚至 100Gps ，造成連外頻寬被塞滿，而不是網路設備被擊垮時，除了跟 IASP 購買清洗流量的服務外，是否還有其他做法時，該公司表示無法處理。
    - Radware 的產品哲學是迅速的 Mitigate (減輕) 傷害，而不求完全地解決問題。在處理新型態攻擊產出新阻擋規則時，他們使用「修改規則->量測->修改規則->量測」的反覆流程，在有限的時間內，最後產出一組可接受，但可能並非最佳的規則，在最大化減輕新型態攻擊造成之損害狀況下，讓使用者感受最少的限制使用服務。此一務實思維值得學習。

- Leumi Bank SOC
    - 公司介紹

      Leumi 是以色列最古老的銀行，也是中東地區領先和最大的公司之一。該銀行如今在以色列全國擁有 250 家分行，並在主要金融交叉點設有分支機構和辦事處。該銀行為所有客戶提供銀行服務，從家庭，中小型企業到大型企業。 這些服務通過專門的業務線提供，每個業務線專門為具有類似特徵和需求的客戶提供銀行和金融服務。
    - 簡報重點
        - Leumi 建立了自己的資安監控中心(Security Operation Center，SOC)，此 SOC 整合了四個監控部門，亦稱為融合中心(Fusion Center)，分別負責銀行實體網路及 ATM 監控的 Physical Center、負責銀行網路服務資安事件監控的 Cyber Center、負責內部實體安全控管的 Security Center、負責內部網路防火牆、IPS 等資安防護設備監控的 Monitoring Center。Leumi 銀行的 Fusion Center 在必要時，可以針對所有 ATM 進行遠端封鎖。而且 Leumi 有培養自己的駭客，協助銀行提升資通安全防護能力。
        - Leumi 的 Cyber Security 任務宣言為：在提供有效及差異化防護及資訊情報風險管理(Risk Management)使資安威脅及風險容忍能達到一致時，促成及提升企業策略。
        - Leumi SOC 的建置廠商 ACID Co Founder Yariv Maroely 表示，他們會從社群網路，網路聊天室，暗網(Dark Net)等來源自動蒐集可能的新形態攻擊，並產出對應處理方
        - Leumi 的精神標語為：勇敢領導、謙虛學習。

肆、心得及建議

本中心資通安全組今年指派陳坤裕工程師隨同國家通訊傳播委員會一起參加 HLS & CYBER 2018 會議。在出國前皆針對會議議題資料進行情蒐，也很感謝資通安全組內同仁與我多次討論，使我可在出國前對出訪任務有先期的認識。

綜觀而言，此行除獲取以色列資安廠商最新產品資訊外，最大收穫便是習得以色列人的精神。參訪 Leumi Bank SOC 時，該公司大廳陳列標語「It's kind of fun to do the impossible」，著實呈現以色列人不畏困難，勇於挑戰之膽量。此外，在 Gav-Yam Negev Advanced Technologies Park 聽取以色列國防軍簡報時，他們提到：「We don't like to change. But we have to change. Because it's survival」，這也顯示出以色列人在艱困環境下，不斷鞭策自己改變以求進步。也因如此，以色列才能在四面環敵且天然資源缺乏下，創造出許多驚人成就。這一切若再歸納，核心即是「務實、勇敢與決心」。

此行坤裕深受啟發，對自主研發資安技術之決心更加堅定。雖人物力等研發資源匱乏，但這正是落實以色列精神的最佳時機。坤裕定戮力完成研發任務，為中心貢獻己力。

下圖由左至右為：NCC 葉世湛分析師、NCC 林佑仲技正、NCC 蘇思漢簡正及 TTC 陳坤裕工程師。