tsti大同世界科技

智慧交通再精準 x 資安來指揮

邱明雄/Shafer Chiou

2017/12/12

大同世界科技副總經理 暨

協志聯合科技總經理

集團公司

大同(股)公司
Tatung Company

2000年5月由大同公司資訊通信業務處分割獨立，成為大同世界科技股份有限公司，並於 2004年3月29日上櫃。

1. 群輝康健成立於2008年7月，前身為大世科系統服務處及系統研發處等部門
2. 2013年1月更名為群輝商務科技公司

- Since 2008

1. 成立於1996年，擁有第二類電信執照。
2. 2015年7月正式併入大同世界科技公司成為100%子公司。

- SaaS 營收、電信暨網路服務
- IaaS/PaaS/SaaS 租賃
- 資安實戰攻防演練課程

成立於2012年，提供呼叫中心及雲計算解決方案、ERP/MES/CRM應用服務專業顧問。

- SaaS 技術支援
- ERP，CRM，MES專業顧問及軟體服務

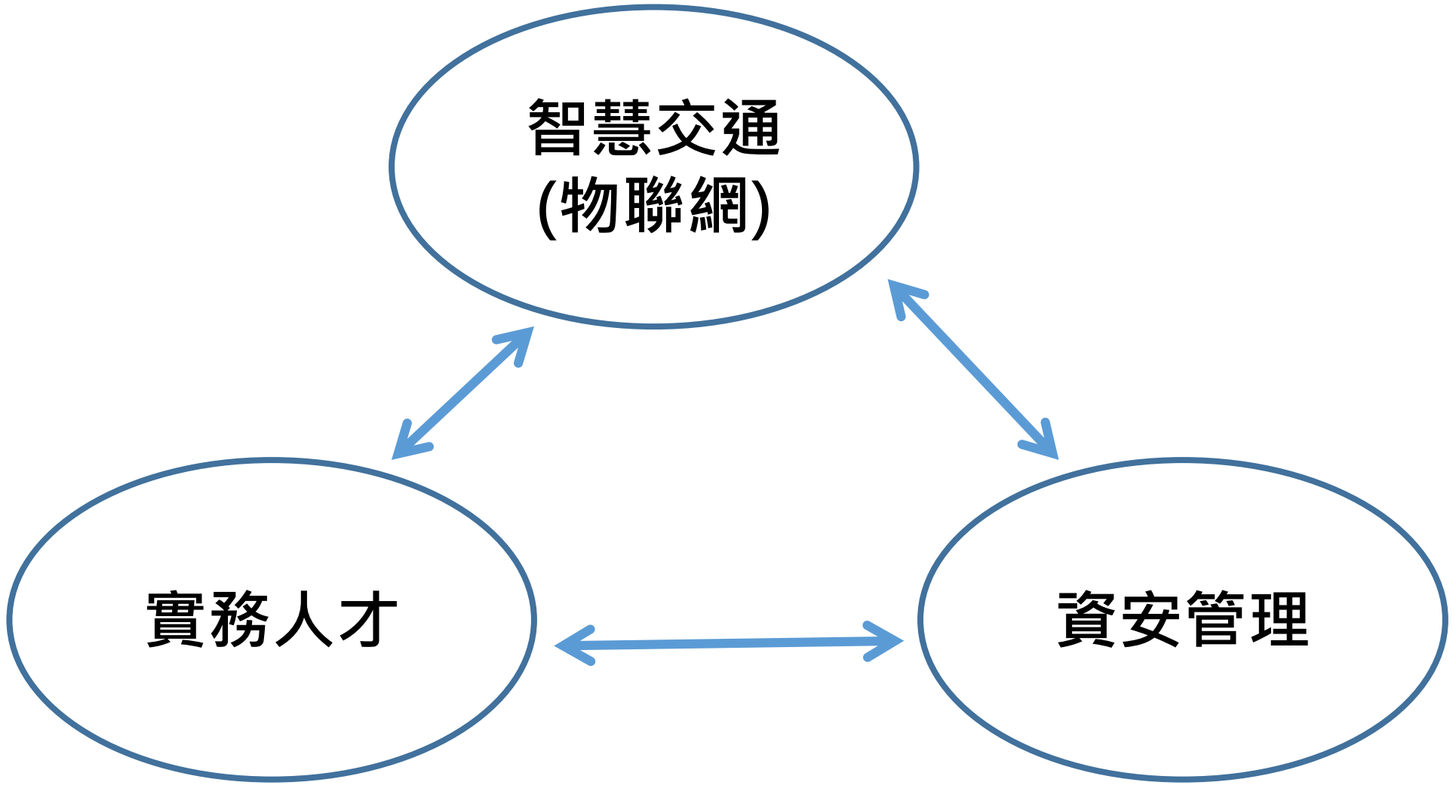
Agenda

一、智慧交通再精準-公務車管理案例

二、資安來指揮-物聯網資安範例

三、資安人才培養

智慧交通再精準 x 資安來指揮



車聯網趨勢

微軟授權車聯網技術專利給豐田，他們在打什麼算盤？

作者 雷鋒網 | 發布日期 2017 年 03 月 24 日 12:41 | 分類 汽車科技, 物聯網, 自駕車 Follow G+ Like 0 Share

3 月 22 日，微軟在官網公告，宣布授權日本汽車製造商豐田一批車聯網技術方面專利，內容包括（車載）識、手勢控制、人工智慧及網路安全工具等。目前具體的專利清單及授權費用未知。

數位時代 BUSINESS NEXT 新聞 觀點 專題 PX酷品 活動 雜誌 創業小聚 數位行銷學院

交通運輸

5G時代最「有感」應用，車聯網進入黃金發展期

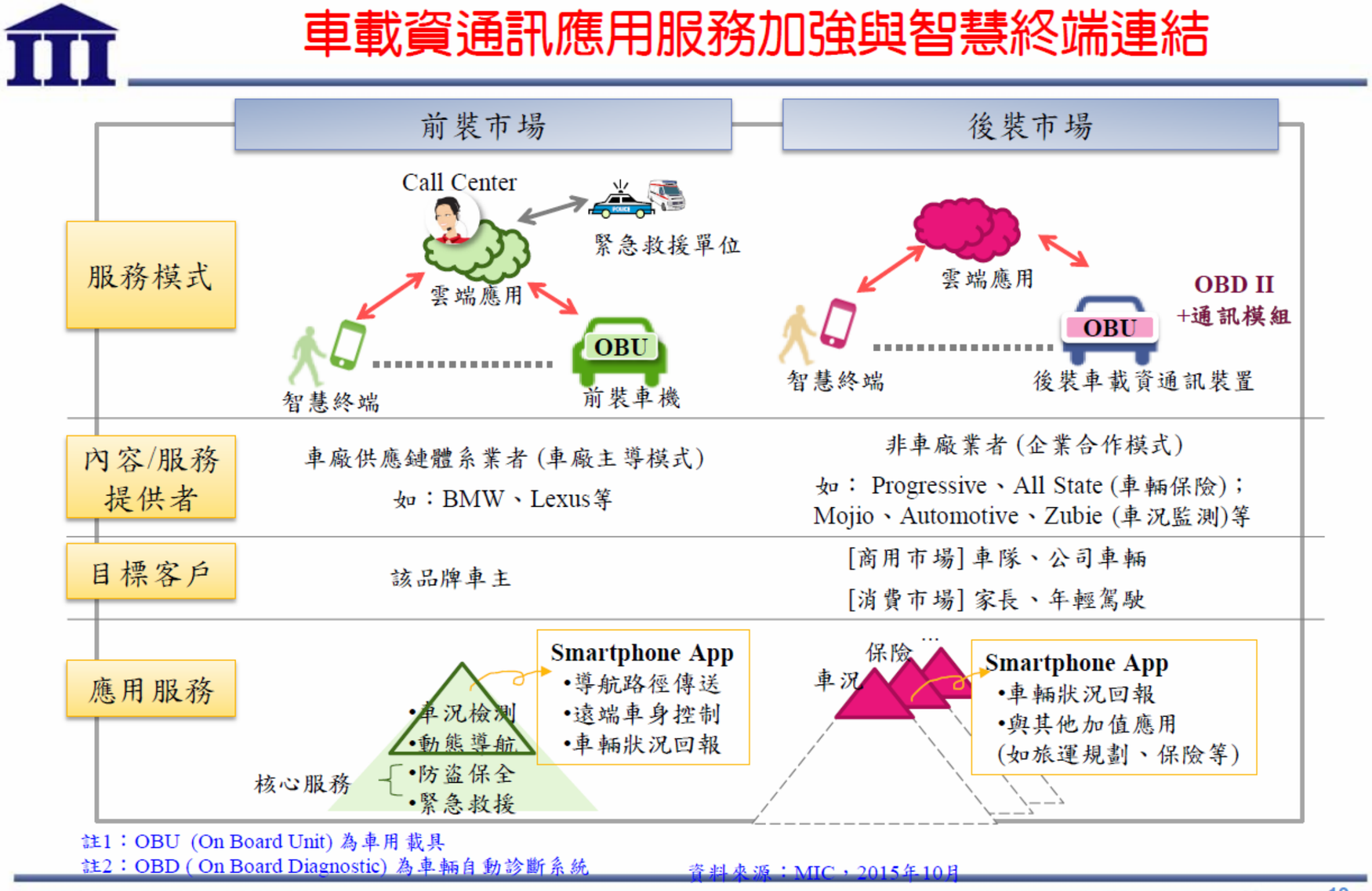
by 曾鑫 2017.10.05

LIFE

TOYOTA、Intel等7企業攜手 為「車聯網」未來結盟

2017-08-13 黃有容 日本 / 車聯網 / 電動車 字級 A- A

物聯網(IoT) 應用

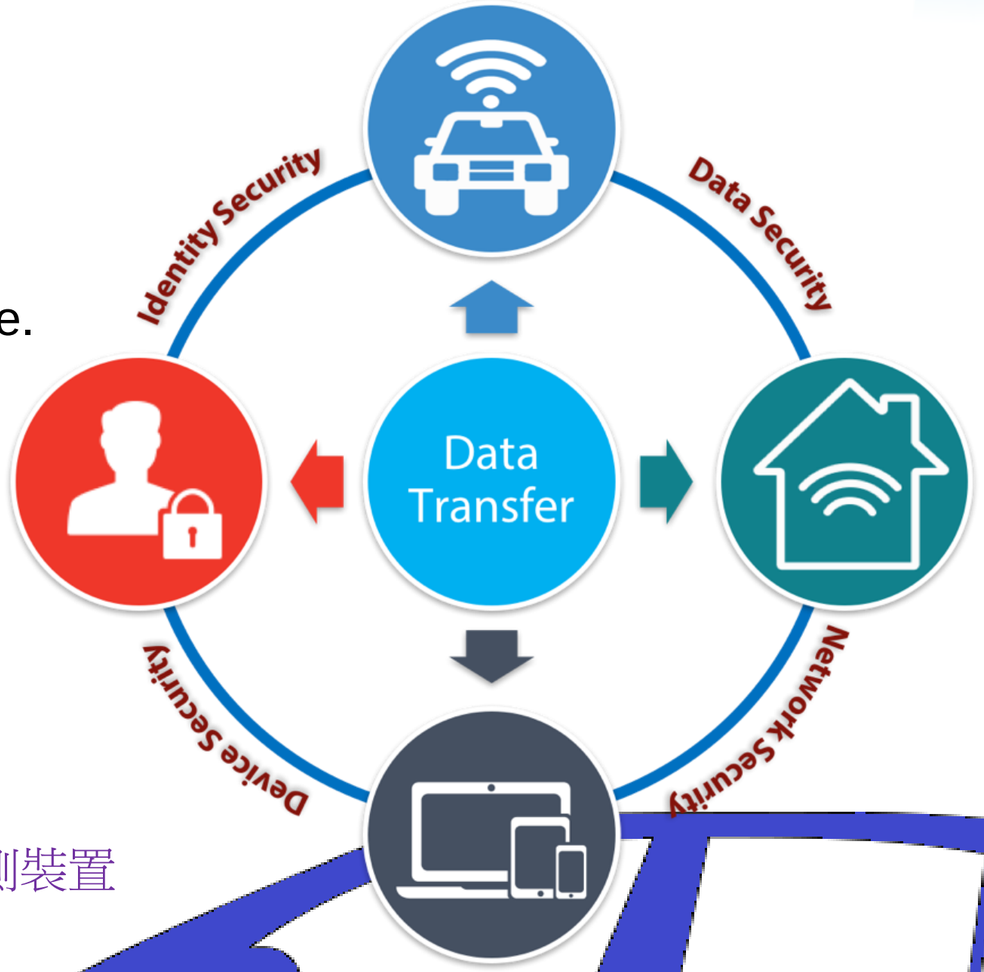


資料蘭園: 2015/11/23
車聯網與智慧交通發展趨勢與機會

車聯網-資安標配

Security solutions providers vary widely in approach, coverage and size.

(1) Identity Security
(2) Data Security
(3) Network Security
(4) Device Security



雲端應用–車隊管理

車載資安系統

車載通訊系統–車間與路側裝置

防盜應用軟體

車內資訊娛樂系統

智能驅動與能源優化

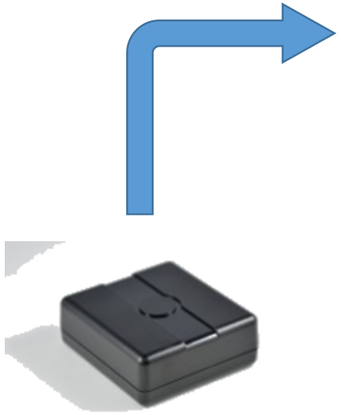
智能馬達

智能電池

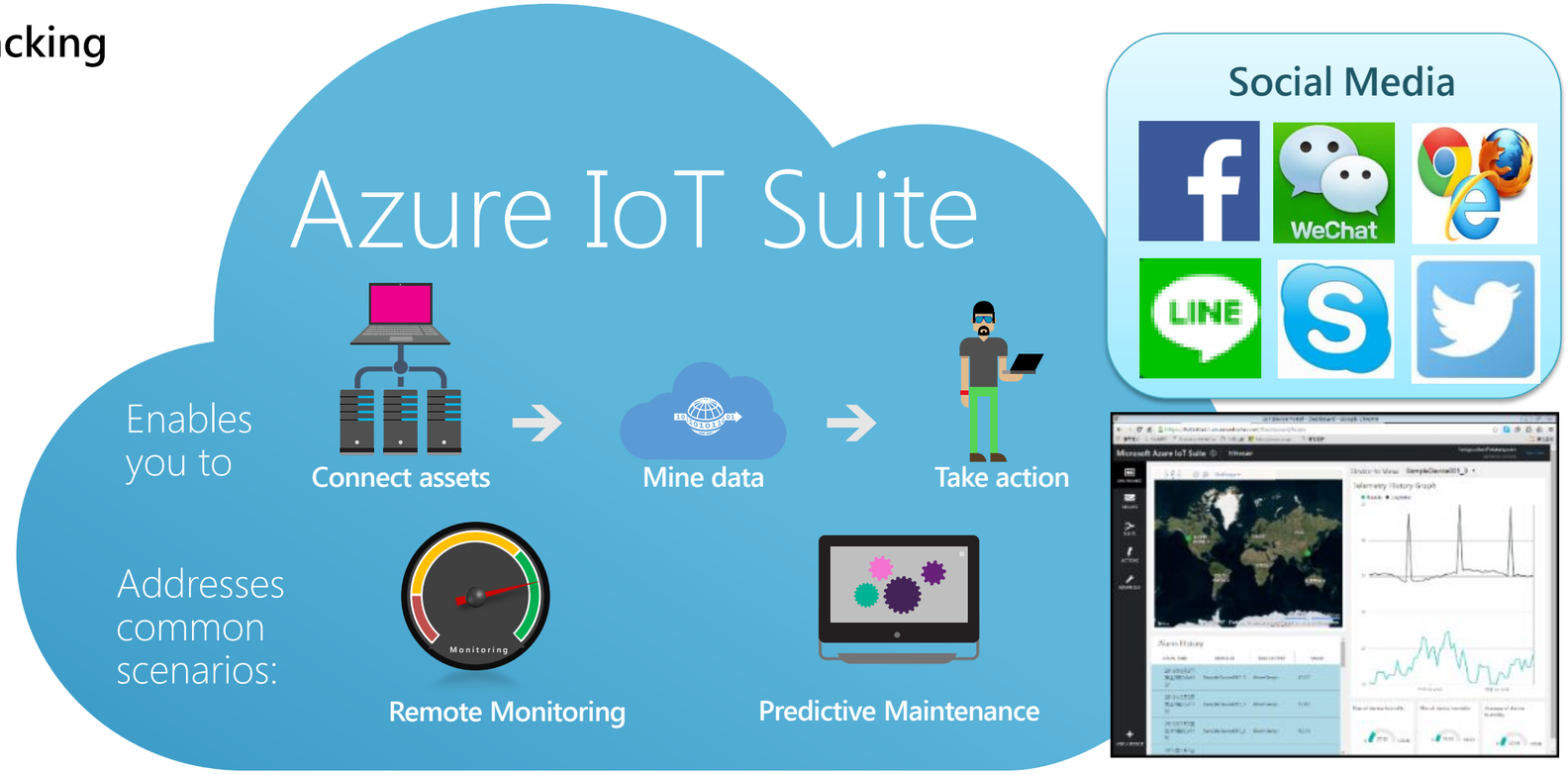
ADAS自動駕駛輔助系統

車聯網–tsti 公務車管理案例

IoT Suite Use Case : Vehicle Tracking



ATBS AT100G_C



Administrator

- Stolen vehicle recovery: Both consumer and commercial vehicles can be outfitted with GPS units to allow police to do tracking and recovery.
- Fleet management: When managing a fleet of vehicles, knowing the real-time location of all drivers allows management to meet customer needs more efficiently.
- Fuel Monitoring: monitor the fuel through tracking device (with help of fuel sensor connected to the device).
- Distance Calculation: calculate the distance traveled by the fleet.
- OBD II - Plug and play interface which provides most of engine diagnostics information.

車聯網–tsti 公務車管理

公務車管理-預約

公務車預計時程登錄

日期 2017/11/20

申請人 洪泰原

車號 RAR-0516

新增 離開

- 請選擇
- RAR-0516
- RAY-9195
- RAY-9201
- RBS-8792

掌握使用人員與車輛狀態

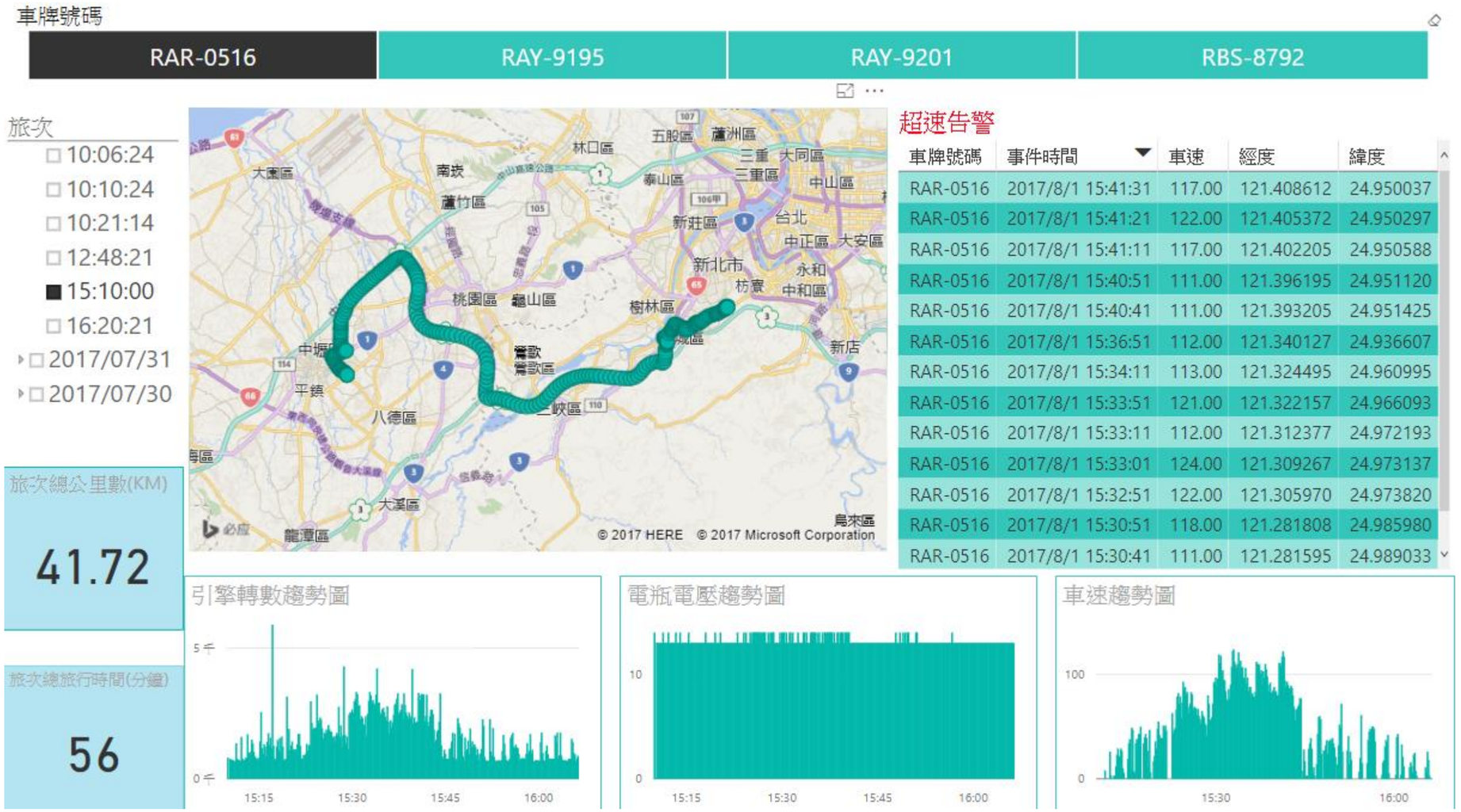
公務車預訂查詢

日期區間 2017/11/20 ～ 2017/11/20 查詢 新增

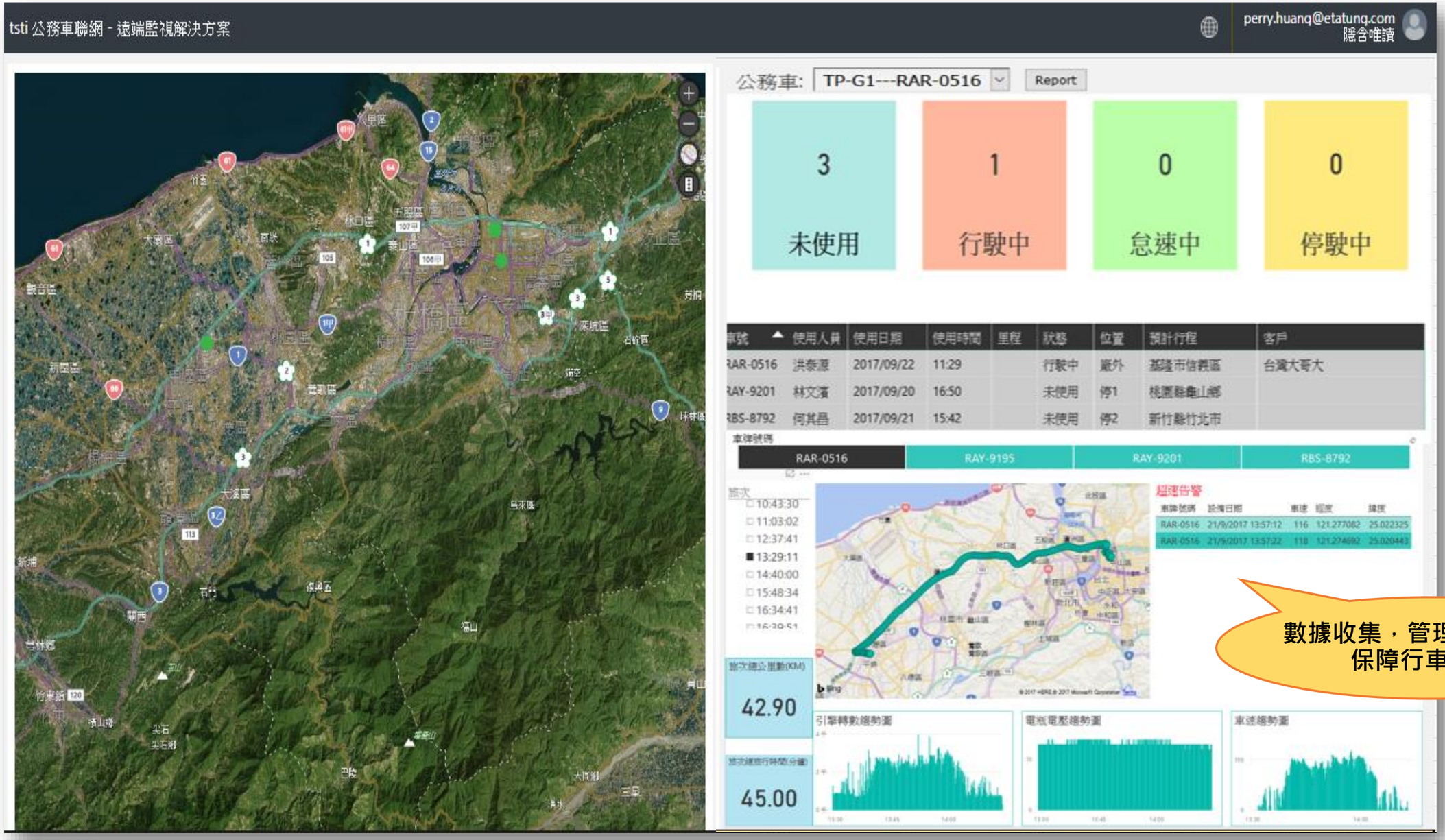
#	日期	車號	申請人	縣市	區	地點	客戶名稱	使用時間
編輯	2017/11/20	RAY-9195	李汪勳	桃園縣	桃園市		DHL	09:00~17:00
編輯	2017/11/20	RAR-0516	洪泰原	新北市	泰山區		台灣大哥大	09:00~17:00
編輯	2017/11/20	RAR-0516	洪泰原	台北市	內湖區		台灣大哥大	09:00~17:00
編輯	2017/11/20	RAR-0516	洪泰原	新北市	土城區		台灣大哥大	09:00~17:00
編輯	2017/11/20	RAY-9201	蕭維良	新竹縣	寶山鄉		敘碁	09:00~17:00
編輯	2017/11/20	RBS-8792	陳億榮	桃園縣	桃園市	華南銀行	富邦	09:00~17:00

1 共1頁 1 - 6 共6筆

公務車管理-旅次規劃與實際比較



公務車管理-彙整分析



數據收集，管理駕駛行為，
保障行車安全

公務車管理-整合智能客服中心

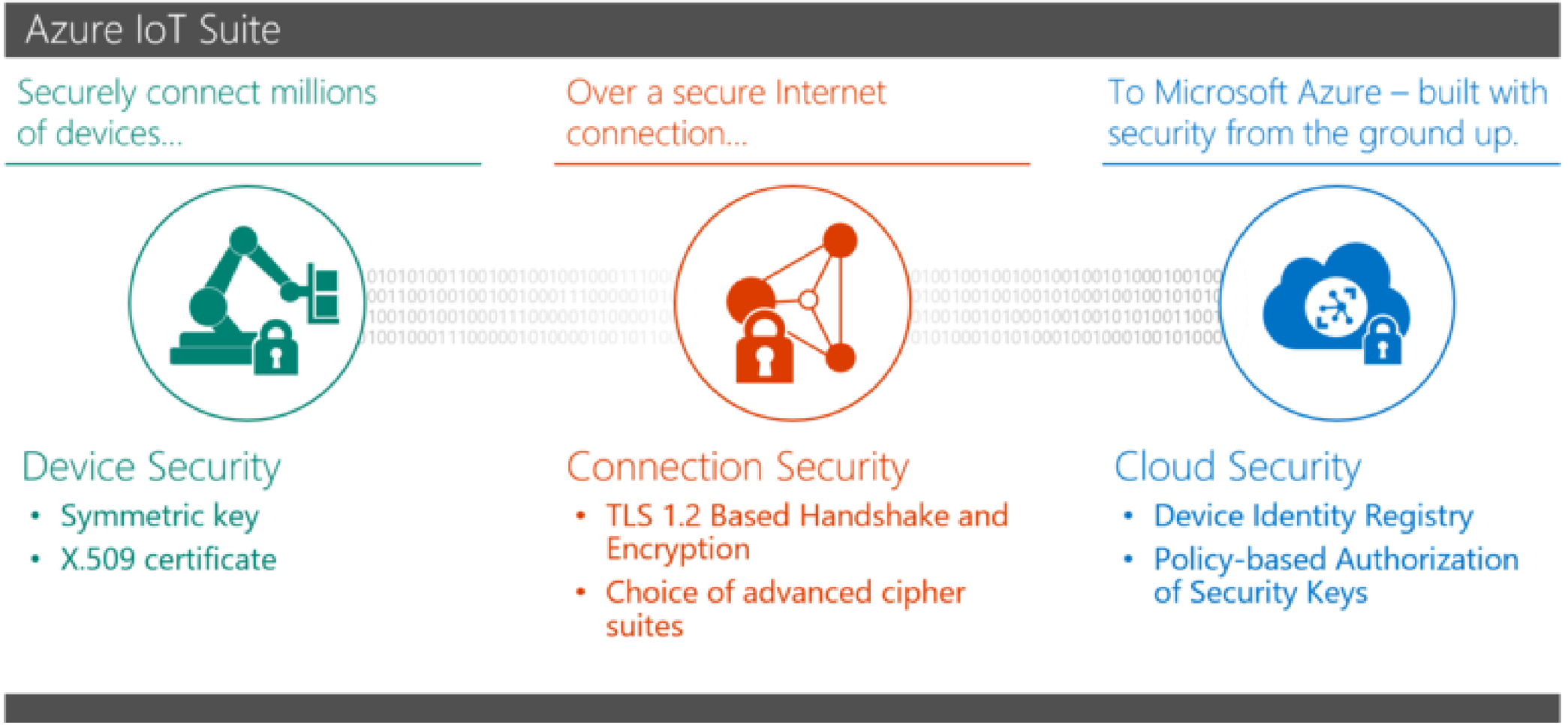
Agenda

二、資安來指揮-物聯網資安範例

物聯網資安

範例：**Azure IoT** 資安

- **Device Security**: Securing the IoT device while it is deployed in the wild.
- **Connection Security**: Ensuring all data transmitted between the IoT device and IoT Hub is confidential and tamper-proof.
- **Cloud Security**: Providing a means to secure data while it moves through, and is stored in the cloud.



物聯網-資安來指揮

Threat Model(威脅型態) : STRIDE

- Spoofing(詐騙): Impersonating something or someone else.
- Tampering(竄改): Modifying data or code.
- Repudiation(否認): Claiming not to have performed an action.
- Information Disclosure(揭露): Exposing information to someone not authorized to see it.
- Denial of Service(拒絕服務): Denying or degrading service to users.
- Elevation of Privilege(特權): Gain capabilities without proper authorization

Component	Threat(威脅)	Mitigation	Risk	Implementation
Device IoT Hub	TID	(D)TLS (PSK/RSA) to encrypt the traffic	Eavesdropping or interfering the communication between the device and the gateway	Security on the protocol level. With custom protocols, we need to figure out how to protect them. In most cases, the communication takes place from the device to the IoT Hub (device initiates the connection).

物聯網-資安來指揮

Azure IoT資安範例-大同智慧家電雲服務

Agenda

三、資安人才培養

資安實戰攻防演練課程(3天)

線上報名: http:cybersecurity.com.tw

地點：台北市中山區中山北路三段22號 (報到區域:大同公司1F)

廣告企畫製作

打造台灣第一座 企業級資安實戰攻防演練中心

目前臺灣已經成為全球最容易受到網路攻擊的目標之一，面對駭客或網軍環伺的嚴峻考驗，駭客鎖定目標已不侷限於政府部門、金融業、高科技產業，而是各產業甚至個人都面臨到來自網路的威脅（Cyber Threat）。所以，企業更面對不可避免的網路威脅與挑戰，須要從人、科技和流程加以整合，才能有效因應網路威脅。

企業如何從網路威脅偵察、事件分析、資安風險的評估和管控，進而主動出擊防範威脅於未然，皆需要企業高層關注資安人員的培育與訓練。目前較具規模的企業大多已導入資訊安全管理系統(ISMS)並取得認證，這是企業維護資訊安全的基礎，然而在面對真實的網路攻擊（威脅）時，絕大多數取得(ISMS)認證的人員可能都因為沒有足夠的應變操作戰能力而束手無策，因此，提升人員之資安應變作戰能力，讓企業能安然度過網路攻擊（威脅），要有一套完整攻防實戰學習環境，從實際攻防實戰演練過程中，來建立各企業更有效的資安防禦機制。

攻防實戰學習環境的演練，類似戰爭遊戲(WAR-GAME)或棋為兵棋推演，提供一個類似企業面臨各種網路威脅的真實環境，讓資安人員於攻防演練過程，學習到正確的應對經驗，在演練過程中，會有專業從旁協助，於攻防演練完成後會深入檢討過程之應對技巧有哪些可以改善或做得更好。譬如在面對勒索軟體、進階持續性滲透威脅(APT)攻擊或阻斷服務式(DDOS)攻擊，都需要透過實際情境訓練來提升資安人員之偵防能力，並研擬與實施不同情境下的防禦措施，目標為培育企業資安人員具備充裕的防禦作戰能力。

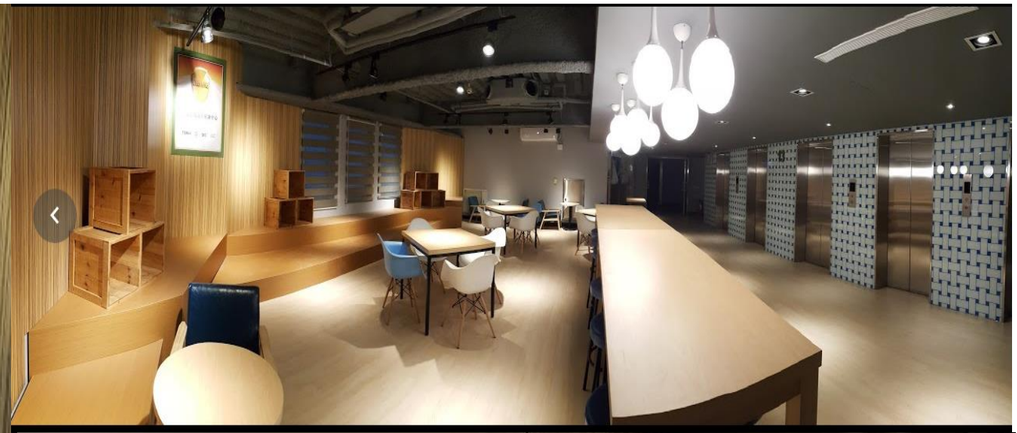
大同世界科技(股)公司及協志聯合科技(股)公司董事長沈柏延表示，基於網路攻擊事件層出不窮，讓企業營運面臨嚴峻挑戰，培養具備專業防護能力的資安人員，藉由各式攻擊模擬，以提升其因應網路攻擊的防護知識，進而養成高階資安防護技術與專業的資安設備與安全軟體應用之能力，達到阻擋進階持續性滲透攻擊威脅，才能減少駭客入侵的機會與企業的損失，並確保營運不中斷。

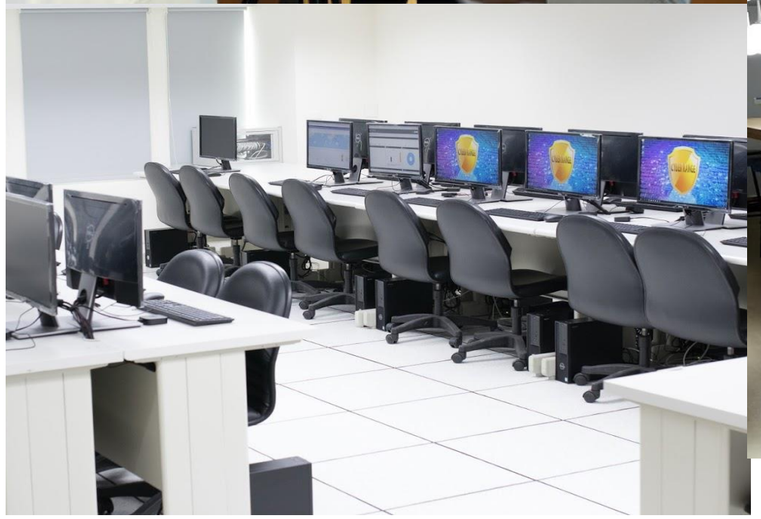
沈柏延表示，由大同世界科技(股)子公司協志聯合科技(TISNet)技轉美商思科(Cisco)數位韌性實戰服務(Cyber Range Service)，打造台灣第一座企業級資安實戰攻防演練中心，提供駭客級攻防演練實戰的培訓課程，透過深入了解駭客思維與攻擊脈絡，為企業培養資安人才，提昇企業全面的資訊安全防護力。

資安實戰攻防演練中心的技術涵蓋15類安全技術及管理情境(SIEM、Big Data、CSIRT、Cloud Security、Wireless Security、Web Security、Mail Security、NetFlow、Cyber Threat Defense、DNS、WiFi、FW / IPS 等)；另包含各種類型的攻擊手法(超過100種)、劇本及應用，並會持續更新攻擊和威脅情境，整合安全情報資料 / 惡意網址及軟體資料庫。

實戰演練課程(Cyber Range Workshop)依組織資安等級分別規劃3天及5天的演練課程，另外也可配合企業需求提供客製化包班課程，實戰演練課程的情境包含防火牆及入侵攻擊、網頁、網站攻擊、電子郵件攻擊、網路安全行為攻擊、身分認證攻擊、無線安全攻擊、虛擬安全攻擊、安全分區防禦攻擊、阻斷式服務攻擊、進階持續性滲透威脅(APT)攻擊、複合式攻擊、複合式ATP攻擊模組等。

實戰攻防演練中心 官網 http://cybersecurity.com.tw/ | 企業級資安實戰攻防演練中心 台北市中山北路三段22號13F
協志聯合科技(股)公司 聯絡人 黃小姐 (02)2509-5463 SunnyLu@tisnet.com.tw | 大同世界科技(股)公司 聯絡人 黃小姐 (02)2509-5627 LindaHuang@betatung.com



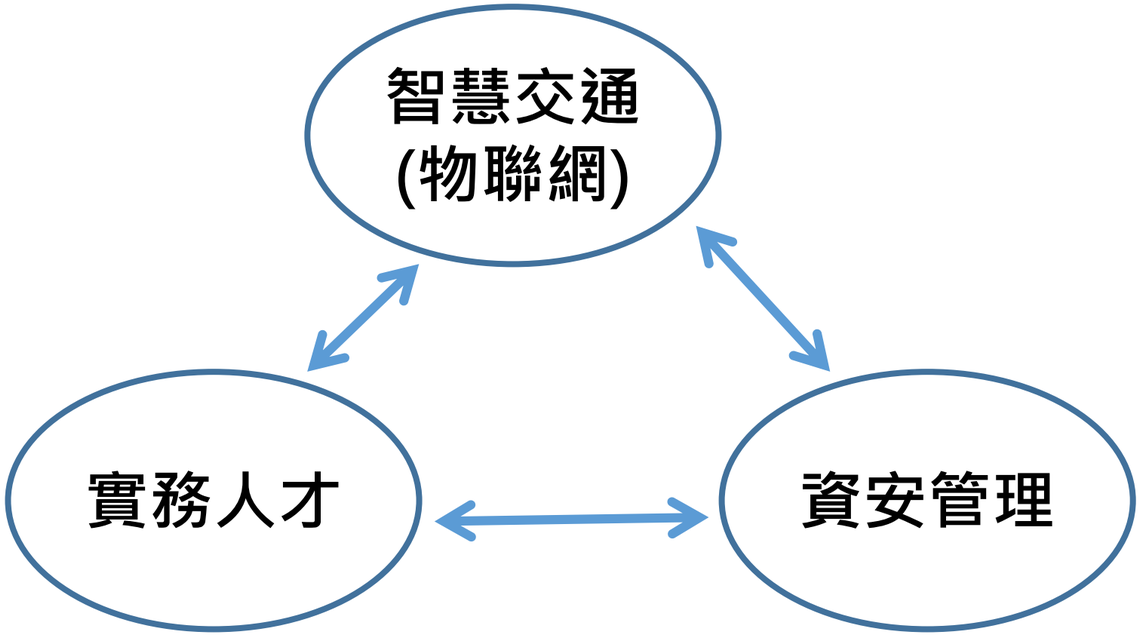


資安實戰攻防演練課程-課程大綱

日期	內容
Day 1 上午	Cyber Range架構簡介及情境演示 電腦安全事件應變小組(Computer Security Incident Response Team, CSIRT)實務介紹
Day 1 下午	安全性資訊與事件管理(Security Information and Event Management, SIEM)概述 實戰演練：初階攻擊與防禦、含背景流量之混和式攻擊
Day 2 上午	防火牆(Firewall)及入侵防禦系統(IPS)簡介 實戰演練：5個相關攻擊情境
Day 2 下午	入侵技術簡介 網頁及電子郵件安全 實戰演練：5個相關攻擊情境
Day 3 上午	網路威脅防禦簡介 實戰演練：5個相關攻擊情境
Day 3 下午	無線網路安全 實戰演練：含背景流量之混合式攻擊 實戰競賽：藍隊(防禦方)競技

資安實戰攻防演練課程-預計達成效益

智慧交通再精準 X 資安來指揮



Q A

www.etatung.com