【E政府-資安研討會】：資料外洩保防-常見危安攻擊解析流程表

時間	議程／講師	
9:00-9:30	報到	
9:30-9:40	開場	
9:40-10:20	政府面對 APT 資安事件處理的真正挑戰 資安負責人員皆會面臨事件處理的挑戰，但周旋於大量從資安設備發出的警報終至疲於奔命，導致現今的處理程序已經幾乎流於形式。而 APT 問題日益嚴重，如何讓安全團隊獲得絕佳的資訊分析，將巨量資安情報擴及運作中的端點與伺服器，提供可追蹤的資安事件處理資訊。中芯數據 APT 偵測與處理解決方案，將與您深度探討政府面對 APT 資安事件處理的真正挑戰！！	吳耿宏 中芯數據 資深資安顧問
10:20-11:00	主題演說 1：政府資安政策說明	李維斌 台北市政府資訊局 局長
11:00-11:20	休息	
11:20-12:00	資安禍首-特權帳號 特權帳號與密碼非常強大，它允許任何人以匿名方式登入並取得系統與資料的完整控制權，此一弱點可能讓企業財務與商譽蒙受巨大損失。造成特權帳密難以管理的原因。 一般企業有成千上萬的特權帳號散佈在所有系統中。人工手動更新與管理需花費可觀的人力與成本。管理員與程式用帳號(內嵌、編譯而無法更改的帳號密碼)普遍存在於所有軟、硬體，包括虛擬設備中。特權帳號的管理與使用為所有稽核單位、法規必要的檢查項。	彭國達 力悅資訊 經理
12:00-13:30	午餐	
13:30-14:10	APT2.0,新世代防禦技術全面剖析新攻擊手法	陳銓耀 Palo Alto Networks 技術顧問
14:10-14:20	休息	
14:20-15:00	小心！APT 攻擊隨時在，深入探討並擬定有效解決方案。 1. APT 技術看似簡單，卻是非常有效的攻擊行為。 2. 在網際網路中的任何環節，都能成為攻擊起點，進而深入網路竊取資料等不 法行為。	盧惠光 台灣二版 高級產品經理
	3. 實際演練攻擊流程並提供應對方法，進一步了解 APT 防護。	
15:00-15:20	休息	
15:20-16:00	資料竊取防護案例分享 為確保政府機關重要的機密資訊建立完整的防護堡壘，抵禦資料安全威脅，必須使用最新的安全技術、最完整的安全政策與能夠確保嚴格執行的安全程序，以建立萬無一失的安全策略。Websense 資安專家將協助政府機關因應複雜的環境架構，有效抵禦進階攻擊與資料竊取，提供即時的防護。	陳志遠 Websense 台灣區技術經理
16:00-16:10	休息	
16:10-16:50	主題演說: 吳其勳 / iThome 電腦報周刊總編輯	
16:50	賦歸	