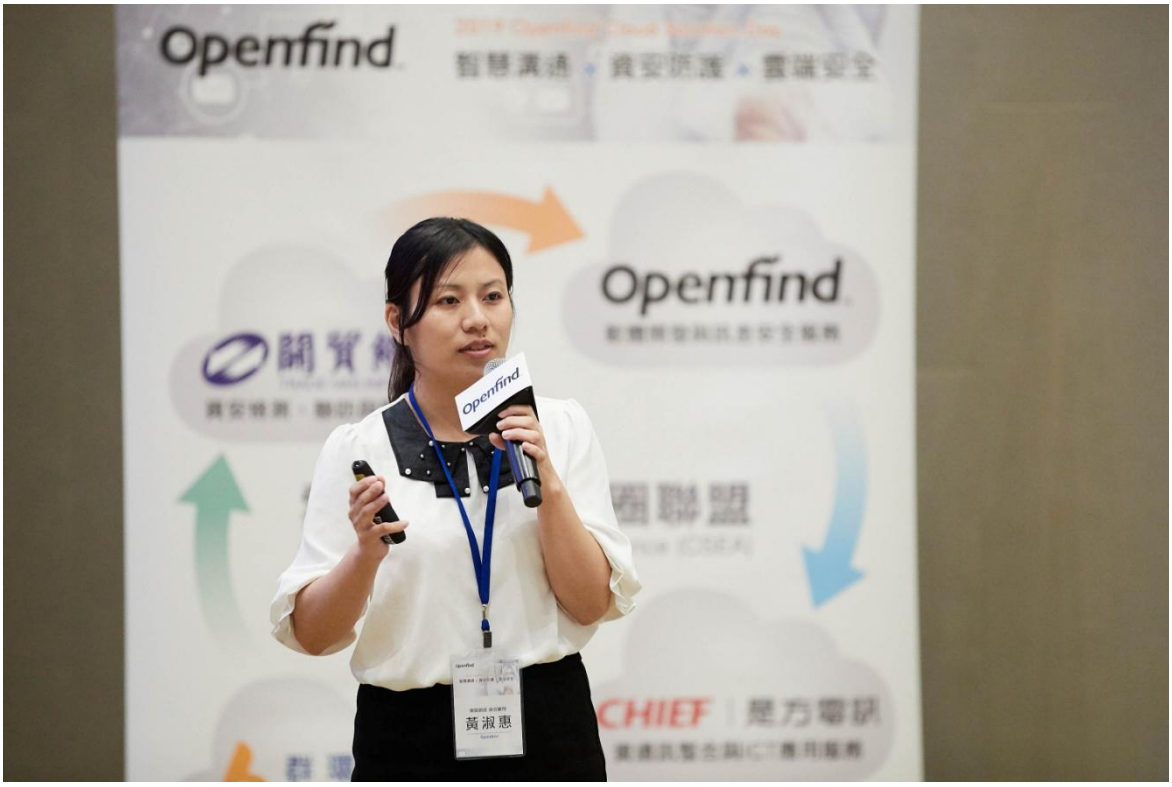
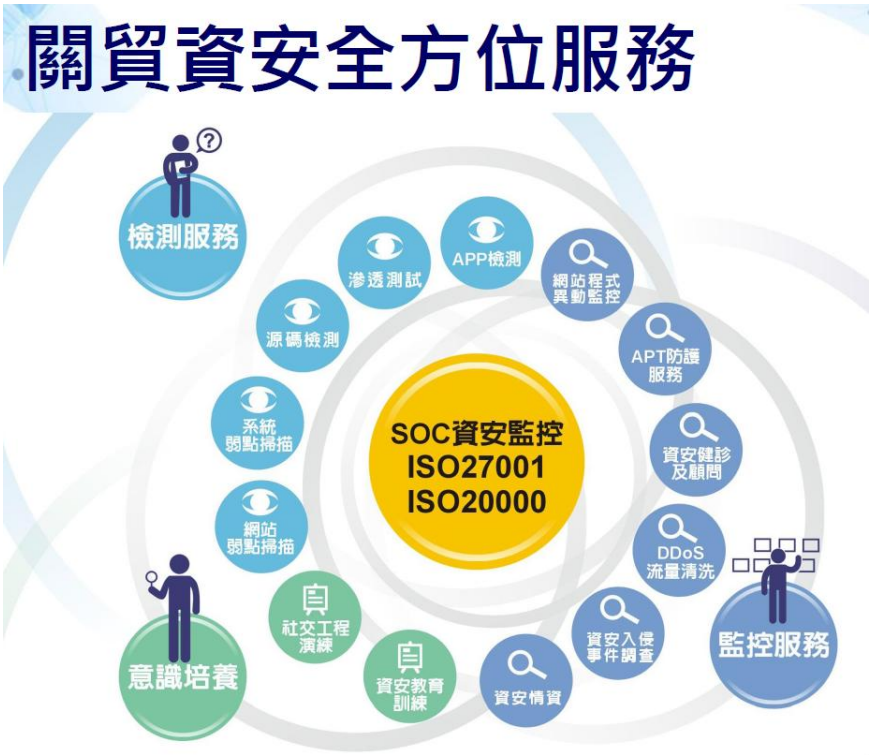
雲端挖礦機？如何防禦與偵測駭客在內網潛行之軌跡？



(關貿網路 資安整合服務部資安顧問 黃淑惠)

關貿網路為財政部持股之資訊服務公司，負責國內重大資訊系統建置及維運，如電子報稅、地政系統、通關網路乃至近期的電子發票系統等，而在多年的資訊系統歷練中關貿網路體會到資安的重要，因而投入心力琢磨資安技術與累積經驗能量。資安顧問黃淑惠說明關貿網路資安服務發展歷程。

資安不外乎「攻、防、人」三要素，對應至資安服務作為即為檢測服務、監控服務以及意識培養工作，而後再展開多種細項工作，如檢測有弱點掃描、滲透測試；監控有異動監控、流量清洗；意識培養則有社交工程演練、資安教育等。



黃淑惠進一步分享近期觀察到的資安趨勢，與過往不同駭客逐漸不採行直接目標攻擊，而是探索可能的脆弱環節從而侵入，並再內部長期潛伏與橫向移動，而後在設定的時間正式發起攻擊。

面對新攻擊趨勢當如何防範？黃淑惠建議企業當換位思考剖析駭客心理，檢視攻擊目標排行榜可發現駭客偏好攻擊防毒伺服器、AD（Active Domain）、版本派送伺服器、WSUS（Windows Server Update Services）等，其共通特性均為權限高、接觸範圍廣，如同兵家必爭之地，一旦入侵成功可獲得高主控權，進而發起攻擊以獲取犯罪經濟效益。

另一排行榜顯示 WannaCry 等勒索軟體是透過何種途徑入侵得逞，調查結果出乎意料，一般認為會是軟體漏洞為大宗，結果是 RDP 遠端桌面協定 63.5%，次之為社交工程 30%，軟體漏洞僅佔 6.1%。欣慰的是遠端桌面與社交工程管道均可事先防範，難以即時防範的軟體漏洞則可透過資安管理措施控制其風險。

黃淑惠也分享其親身經歷的新型態資安威脅事件，即企業被植入數位加密貨幣挖礦程式，企業客戶在發現伺服器運作極慢卻查不出原因後向關貿網路尋求協助。

在進行大量數位採證與相關訪談等逐漸還原駭客攻擊情境與步驟，最初駭客以社交郵件誘使企業內部行政人員開啟執行信件附檔，而後惡意程式自行政人員電腦向內部轉移進而取得 AD 管理權限，而後取得伺服器更新權限，最後將大量挖礦程式派

送到企業內各伺服器中，幾乎耗竭所有伺服器硬體資源與效能。

找出問題根因與發展程序後即可解決問題，同時也遏止更進一步的威脅可能，如駭客可能在後期將伺服器上的使用者資料加密以勒索贖金，然因關貿網路的提前解決而未發生。

透過此一案例黃淑惠提出兩點防禦建議，即快與準，「快」必須儘速通報資安聯防團隊以便對威脅進行樣本分析，「準」則是深入調查根因並提出防禦強化方案。

最後也建議企業當建立資安縱深防禦，挖礦案例的起點為社交工程郵件，因此最前線須進行社交工程演練提高人員防備心，而為了避免威脅於內部移動當對網路設備與伺服器進行日誌分析，另也輔以攝影機與端點防護措施。期許企業別再為惡意挖礦所苦，讓所有已投資的資訊設備均能發揮應有效能。