善用情資加快回應威脅速度

奇資安引進Recorded Future 助企業強化防護力

現今全球資安防護趨勢走向主動應對的方式，即是透過收集情資的方式，預先針對駭客可能採取攻擊手法進行應對。為此，奇資安所引進 Recorded Future，讓整體資安防護機制更為完善。

採訪／施鑫澤　文／林裕洋

隨著駭客朝向組織化發展，且攻擊手法多元下，不僅讓企業、政府更重視資安防護，也開始透過情資收集與交換，掌握駭客組織的攻擊型態，以便能在惡意程式入侵之前，預先採取相對應的防護措施。在全球資安人才不足的狀況下，企業必須儲備具備情資管道、分析技巧及真偽判斷能力的網路情資分析人才，才能因應資安威脅趨勢，打造可防堵惡意程式入侵的防護機制。

奇資訊保安及網絡（後面簡稱，奇資安）資通安全技術長葉家傑指出，過往企業面對資安威脅的應對方法，泰半採取被動作為，往往要等到被攻擊時才察覺，即便有安裝主動威脅偵測（Threat Hunting）工具，也得等到已爆發駭客攻擊入侵才能回應。然而現今全球資安防護趨勢則走向主動應對的方式，即是透過收集情資的方式，預先針對駭客可能採取攻擊手法進行應對。例如，一個國家要有效建立防禦能力，自然必須掌握潛在威脅國家的攻擊武器種類，才能運用有限預算打造有效的防護機制。所以我們特別引進Recorded Future，助力台灣企業掌握最新資安趨勢，進而讓整體資安防護機制更為完善。

情資重要性日增需建立執行能力

由經驗豐富資安專業人士成立的奇資安，專注於研究最新的網路安全趨勢以及企業組織當今面臨的威脅。該公司憑藉紮實的網路安全和技術知識，投入資安領域的研究和實驗，為企業提供通過高度可客制化的服務。

葉家傑指出，情資就是將資料組合成一種形式，作為後續決策提供所需的參考資訊。若應用在資安領域上，即是將以前看不見的、外部的資訊收集回來，而要處理來自全球各地的不同資訊，則需要一個可處理大量資料的AI 平台，才能建立情資平台，作為企業資安團隊或主管的決策參考。以美國資安培訓機構SANS為例，即指出負責戰略、戰術、操作等不同職務的資安人員，應該具備使用情資做不同決定的能力。由於歐美企業對資安向來較為重視，目前甚至有公司成立Cyber Threat Intelligence （CTI）分析部門，負責透過收集與分析情資找出公司的敵人，再與風險管理的部門討論後續應對方式，避免公司陷入威脅而不自知。

葉家傑表示，若要運用情資進行分析，最大挑戰之一，莫過於在網路眾多資訊中，如何找出與公司相關的資訊，再透過主動分析自身行業風險、主動把準備攻擊的人找出來，再用Risk Based Approach工具協助，這是企業得克服的挑戰之一。畢竟資安工作非常繁瑣，加上駭客攻擊手法多元化，能否有效利用情資進行分析之後，再轉為實際行動，也是資訊人員非常沈重的工作負

奇資訊保安及網絡（奇資安）資通安全技術長葉家傑。

擔。

Recorded Future情資 最全面全球市場受肯定

奇資安代理的Recorded Future，是世界上最大情資公司之一，其雲端情報平台涵蓋對手、基礎設施和目標，可透過持續化的自動資料收集和分析技術，搭配與技術團隊的人工分析服務，提供企業全方位的即時情資顯示。如此一來，企業能在第一時掌握犯罪組織的一舉一動，並且立即採取相對應措施，確保人員、系統和基礎設施安全。

長期以來，Recorded Future一直投入收集全球各地的威脅資料，並透過模型構建和分析等技術，將大量資料轉化為亦於讀取的資訊。該公司是透過文字、圖像和技術來源等，收集和構建對手和受害者之間的資料，並使用獨家研發的自然語言處理和機器學習技術，分析全球數十億設備之間的關聯。截至目為止，Recorded Future已持續收集300多個國家行為者、300萬個犯罪論壇和10,000 個活躍的 C2，以及數十億個域、2.75 億個 IP 和 98,000 個 ASN等。

除此之外，該公司也監控超過 300,000 個組織、200,000 個漏洞、36 億洩露的憑證和 25,000 名 C2 受害者等，以便能掌握最新資安趨勢，並提供給企業作為建構資安防護機制與政策的參考。

「隨著企業的數位化程度日深，背後隱藏資安風險自然也愈高。特別是在現今混合式攻擊手法當道的狀況下，駭客正透過網路、物理、虛假訊息等之間的相互搭配，藉此達到滲透與攻擊防護能力薄弱的目標。」葉家傑解釋：「Recorded Future能提供涵蓋對手、基礎設施和目標等範疇的最全面情資，並持續透過版本的更新與進化，讓企業能掌握最新情資，以便能在破壞對手入侵之前採取最果斷的措施。」

顧問服務能力 強助企業落實情資分析結果

Recorded Future能提供情報非常多元，涵蓋品牌情報、安全運營情報、威脅情報、漏洞情報、第三方情報、地緣政治情報、支付欺詐情報、身份智能、攻擊面情報等，企業可依照營運需求與特性，快速取得所需的情報內容。而隨著公有雲服務成為企業不可或缺的重要後盾，在欠缺合適資安防護機制等狀況下，愈來愈多資訊系統暴露在雲端平台上，也成為駭客鎖定的攻擊目標，因此掌握最新攻擊趨勢也更為重要。相較於其他產品，Recorded Future能提供外部基礎設施的統一視圖，讓企業可根據漏洞、錯誤配置和超出策略的資產等問題，預先對風險最高的資產進行優先級修復，進而達到被攻擊的可能性。

葉家傑表示，我們的雲服務 Recorded Future Intelligence Cloud 獨特地結合持續性的資料收集、大規模圖形分析，以及全球研究團隊的分析敏銳度，提供最完整情資訊息，涵蓋對手、基礎設施等面向，讓企業能藉此達到業務和安全性的目標。此外，透過Recorded Future威脅情報，以及奇資安的資安團隊服務等協助，針對各種威脅進行優先級別排序，預先針對犯罪組織一舉一動採取對應方式，讓有限資安預算發揮最大效益，同時降低資安人員的負擔。

值得一提，由於奇資安在市場上已累積不少用戶與口碑，加上擁有強悍的技術能量與團隊，所以被 APAC CIO Outlook 雜誌評選為亞太區 2022 年度十大最佳資訊安全解決方案公司。