企業需要更智慧平價的資安鑑識服務

網路資訊專訪中芯數據技術長吳耿宏

「為何之前第一銀行、遠東國際商業銀行的資安事件中，資安設備找不到惡意程式？但在事發後，協助處理的專案資安鑑識團隊卻能找到大量惡意程式，並追查出前因後果？」中芯數據技術長吳耿宏先提出一個疑問，試圖讓我們關注現有資安技術服務的限制。

事實上每種資安設備在設計之初已設定一個防禦方向與目標，倘若試圖入侵的一方採取不同的思維角度切入，防禦效果即打折扣，此為其一。其二是資安設備僅對進出企業的協定封包進行分析，若資安可疑特徵僅在於端點(endpoint)部位便很難有效偵測。但對事實上最終的資料處理、資料儲存硬體，才是資安入侵者最終想攻取之地。因此閘道上主要偵測出入侵至端點前的各種攻擊手法，幾乎只是過程，而非目標。

所以在既有設備監控外，強化與補足端點防護才能使資安防護更為全面，吳耿宏解釋。透過端點行為記錄與分析，即可辨識出作業系統與通訊協定的運作是正常或異常。而且資安設備提供的日誌檔、事件資訊僅片段局部，仍然需要專業資安人員串起前後脈絡，才可能拼湊出資安事件的全貌，這也是前述資安事件中設備無法追查出問題，然鑑識團隊人員進入後卻可查出問題的原因所在。

因為每種防護設備都有本身限制，為增加防禦範圍，而不停增加防護設備，其實也帶來新的困擾。吳耿宏接續說，企業為了強化資安防護不斷購買資安設備，但設備愈多產生的警訊也增加，企業需要雇用更多的資安人員去關注警訊。這相當弔詭，按理而言，資安設備當替資訊人員分勞解憂、減少人為心力投入，怎會是設備愈多、人力需求對應增多呢？

人力可貴　要用在刀口上

彙整前面所述，便知道有一個關鍵值得關注，資安設備無法做到百分百防護。但就算專業資安人員能鑑識出資安疑點進而追查出脈絡，然這已是事發後的追查，而且要大量透過人力來進行事後的處理，對於原本已經造成的損失之外，又產生額外的費用，讓整體的損失更是雪上加霜。因此有無可能將相同的人員專業運用在事件初期，提供企業即時的資安鑑識服務呢？

中芯數據針對上述的痛點與疑問提出解方，首先在各端點上安裝系統活動紀錄收集器(Sensor)，由收集器回傳端點行為資訊，將這些資訊匯集至中芯數據的資安營運中心。在營運中心內，由系統對各類系統活動資訊進行分析鑑識，該系統已整合專業鑑識團隊的知識、智慧，以快速且自動化的方式進行人工智慧研判，而後再加上中芯專業人員的研判，最後向企業回報完整事件，包含事發點、事件移轉擴散路徑、事件可能波及影響範疇等，由企業的資訊人員自行決定是否移除該可疑事物。

中芯數據將專業的鑑識工作從事發後拉到事發前，由全人力執行轉成人工智慧式的高度自動化執行，提供企業更智慧、平價的資安鑑定團服務。對企業而言，可說是一套位於遠端資安事件決策支援系統。吳耿宏如此譬喻。唯有如此，企業才能真正精省資安人力資源，也避免在資安問題追查上採無頭緒、大海撈針式的費力搜查。或是沒有任何有效對策之下，不停地重新安裝作業系統。

事實上資訊市場研究機構顧能(Gartner)也在去(2017)年開始強調，現有資安委外管理(Managed Security Services, MSS)服務需要升級，成為更防範於未然的意圖威脅即時鑑識服務(Managed Detection and Response, MDR)。中芯數據亦推出屬於 MDR 範疇的資安防護服務，稱為意圖威脅即時鑑識服務(Intention Prediction as a Service, IPaaS)。

安全記錄不完整等於沒有做

平心而論過去的資安服務 MSS 計費有其背景淵源，以往資安委外服務商有很高的營運成本在網路頻寬費，因而採 EPS(Event Per Second)制。而今頻寬費用已降低，但計價模式依然未變。造成如果要有效分析，必須大量收集記錄，但是越多記錄，代表費用也隨之飆漲，若最終不敵現實考量，仍然只能收集與分析部分資安設備警訊，便會發生疏漏的情況。

而 IPaaS 不僅更詳整辨識、更即時辨識、更智慧與更自動化辨識，且顛覆過往在計價模式。吳耿宏說明，過往的 SIEM 服務多半採 EPS 制，以每秒接收的事件量來計費，通常每秒達 500 以上即屬高階，費率逐漸走高，企業在配置資安預算時便開始遲疑，改考慮折衷配置、部份配置，無法顧及企業內的所有資安設備。相對於此，中芯 PIaaS 服務採訂閱制，依據裝置數目多寡收取年費，遠較前述模式實惠。
此外，若企業期望導入自有 MDR 系統，中芯數據也提供整廠輸出方案，協助其建置，包含智慧自動化鑑識技術、專業鑑識知識等。而吳耿宏再一次強調自動化的重要性，因為在資安鑑識過程中，可能 90%以上的時間都在收集、整理資訊，真正專業研判的時間其實只佔小部分時間，因此如何讓前段程序盡可能以自動化程式取代人工處理，是資安防範能否即時快速與平價的關鍵所在。

正由於人工智慧、大數據分析、自動化的獨到優異性，中芯數據透過從偵測，分析到後續處理的全方位服務方式，已可做到 1 名專責者統管 2 萬台裝置的高擴展性，真正做到人力資源精省。不再需要為大量資安警訊不停忙碌，卻仍苦無有效率的處理對策。透過 IPaaS 服務，企業不再需要煩惱處理資安警訊或事件所消耗的資源，即可有效率的解析攻擊的過程與影響狀況，讓鑑識或事件處理不需要等到損失已經造成，才開始處理。讓資安防護機制真正落實到企業的每個角落。

受訪人簡介

吳耿宏目前擔任中芯數據技術長一職，於 2015 年協助中芯數據正式通過國際標準資安認證機構 IOS27001 認證，促使中芯數據在資訊安全管理上提供資安委外服務流程制度上遵循的基礎。