Gemini Enterprise 產品介紹

資安事件分析的挑戰

現今的資安分析人員承受了太大的責任與壓力，面對接踵而來的資安事件與海量的日誌卻必須限時解讀、分析、關連並重現事件發生經過。傳統的資安事件管理工具如 SIEM 已經毫無招架之力，新興的日誌分析工具似乎總是還缺少點什麼，總是沒辦法最有效的解決資安分析人員的問題。

關鍵字搜尋仍然不夠

新世代的資安事件分析工具多半具備能海底撈針的巨量資料搜尋能力，能在海量的系統與資安日誌中快速搜尋蛛絲馬跡，這的確減輕了分析人員的負擔。但是資安分析人員仍然需要仰賴自身的專業能力，在各種資料來源與格式中下達關鍵字搜尋著相關連的線索，在異質資料關聯分析的能力上顯然還不足以協助解決資安分析人員的困擾。

事件關連分析的侷限

另一方面，傳統的 SIEM 長於資安事件關連分析但是撰寫與維護關連規則顯然是所有使用者的痛，專業門檻高而資安事件樣態的改變也快導致維護成本高昂，於是缺乏關連規則維護的 SIEM 變成了毫無用處的擺設面對劇烈變化的資安環境跟不上腳步。此外複雜的關聯規則缺乏互動性，只能應用已經撰寫好的關聯規則，空有規則偵測能力卻不能彈性運用讓資安分析人員難以利用來做為輔助分析的利器。

資料視覺化的挑戰

資料視覺化是輔助資料分析的重要手段，不僅問題呈現簡明易懂也提供足夠程度的操作互動性；但是對於資安分析人員來說資料視覺化不僅僅是各種圖表的呈現或是華麗的視覺特效，更重要的是視覺化呈現的方式決定了能發掘的資安問題與能分析的範圍。目前市面上的數據分析多半是基於統計分析的視覺化呈現，無法進行回溯與關聯分析，而異質資料之間的關聯分析與根因的回溯分析僅只有限、經過設計過的鑽探(Drill-down)路徑或是關聯規則始終缺乏一個最適合於關聯與回溯分析的資料視覺化呈現方式。

產品簡介

Gemini Enterprise 是集合了資安分析師與數據分析師的智慧研發而成，以極為創新的型態提供市場上前所未見的資安事件分析解決方案。Gemini Enterprise 可以從常見的 SIEM 平台如 ArcSight, Splunk 等擷取剖析出所需的資料與相關的屬性，運用獨特的人工智慧技術自動識別出資料之間的關聯性，這些被 Gemini Enterprise 自動串連起來的資料就能極快的協助資安分析人員追查事件發生的成因以及被影響的範圍。
Gemini Enterprise 從既有的資料儲存中萃取分析所需的資料，因此能夠很容易的與企業既有的日誌管理系統進行整合，企業無需為 Gemini Enterprise 重複收集日誌進行分析。Gemini Enterprise 也可以被視為既有 SIEM 的加值分析服務，能夠輔助強化 SIEM 的分析能力，使 SIEM 具備全新角度的資料分析能力而既有的資安投資也不會浪費。

獨特優勢

自動識別資料與建立關聯

Gemini Enterprise 利用經長期學習的人工智慧成果，能夠從各種資料來源中自動識別超過 1600 種與 IT 或 Security 相關的資料類型，理解這些資料的意義與用途以及與其他資料類型的關聯性，無需人工轉譯或建立對照關係。

視覺化資料關聯呈現

繁複的資料以不同資料類型之間的關聯形式呈現，以不同的顏色與箭號表達資料屬性與之間的因果關係一目瞭然的訴說著資料背後的故事。

直覺式的資料關聯探索

直覺的互動式資料探索介面從一個資料元素展開探索，透過資料之間的關聯性描繪出有價值的資料關聯地圖，發掘出事件的牽涉範圍與因果關係，全程不需要搜尋語法或複雜操作，具有極低的技術門檻與學習曲線。

分析案例管理

每個發掘描繪完畢的資料地圖可以加入註解儲存成一個又一個的分析案例。這些保存的分析案例不僅以極低的專業門檻保存了事件分析的經驗與知識，避免資安分析人員的知識斷層還能幫助管理階層更結構性的理解不同事件的全貌。

案例分享與再利用

儲存的分析案例可以分享給其他人補充或更新累積與完善事件分析的知識，這些不斷累積的分析案例能夠提昇資安分析人員的能力，加速未來的資安事件調查效率，消弭因職務或人員異動帶來的知識銜接斷層。

突出效益

快速找出根本原因

Gemini Enterprise 透過直覺化的互動式操作介面不需要搜尋語法沒有技術門檻，從與事件相關連的資料元素開始探索，利用資料之間的因果關聯進行回溯分析，便能夠很快的找出事件的根本原因。

重現資安事件發展脈絡

經過探索完畢的資料地圖呈現出完整的事件脈絡，包含完整涉及的資料範圍事件之起始成因，與一步步的事件演進以關聯圖的視覺化型態來呈現能幫助資安分析人員，乃至於高階管理人員快速理解完整的資安事件發展脈絡。

擴展 SIEM 的分析能力

雖說傳統的 SIEM 在即時互動分析上有諸多限制，但是已經進行的資安投資無需拋棄。企業僅需增添 Gemini Enterprise 並與既有的 SIEM 整合便能立即擴展 SIEM 的即時互動分析能力，讓 Gemini Enterprise 帶來 SIEM 並不具備的嶄新資安視角。