

TREND VISION ONE™

Security Operations (SecOps)

藉由 XDR、代理式 SIEM 和代理式 SOAR 來主動偵測、調查及回應威脅，讓駭客無所遁形

讓您的資安營運中心 (SOC) 擊敗威脅、贏得勝利

資安團隊肩負著保護企業免於潛在威脅的重責大任，但卻經常人力不足、預算有限，就連工具也是零零散散。身心俱疲的情況稀鬆平常，而跨團隊合作帶來的摩擦大於成效。然而，資安事件的代價正不斷攀升，根據 Ponemon Institute 和 IBM 發表的「2024 年資料外洩成本報告」(Cost of a Data Breach Report 2024)，**2023 年一起資料外洩的平均成本已達到 445 萬美元**，創下歷史新高。所以，那些緩慢、零散或被動的資安防護再也沒有生存空間，傳統的資安事件管理 (SIEM) 系統用起來既昂貴又難以擴充，而且過度仰賴手動調校和調查。它們非但不能加快回應速度，還會讓 SOC 團隊淹沒於複雜性和雜訊當中。

SOC 團隊不僅需要可視性，還需要明確性、優先次序判斷，以及迅速而協調的行動。我們的 Trend Vision One™ Security Operations (SecOps) 解決方案將我們屢屢獲獎的 XDR、代理式 SIEM 以及代理式資安自動化協同及回應 (SOAR) 整合在一起，讓 SOC 團隊能專注在最重要的事情上。當威脅快速挺進時，您的 SOC 團隊將更快反應。

用主動式功能超越傳統被動式防護

專為未來而打造

SecOps 能快速安裝並無縫整合，採用最現代化的技術，以更低的成本提供卓越的資安功能，確保您一開始就具備長期的擴充性和效率。

大型語言模型 (LLM) 的優勢

將您的結構 (schema) 當成一種語言，透過 AI 來了解資料背後的意圖，進而減少手動建立規則的需求。



Trend Vision One™ 平台讓我們有機會將所有資訊匯集到單一地點，並讓我們
的資安團隊能夠處理整個環境的所有違規情況和事件，無須在不同 IT 部門之間奔走。

Samer Mansour
副總裁暨資安長
Panasonic North America



無可匹敵的 XDR 基礎

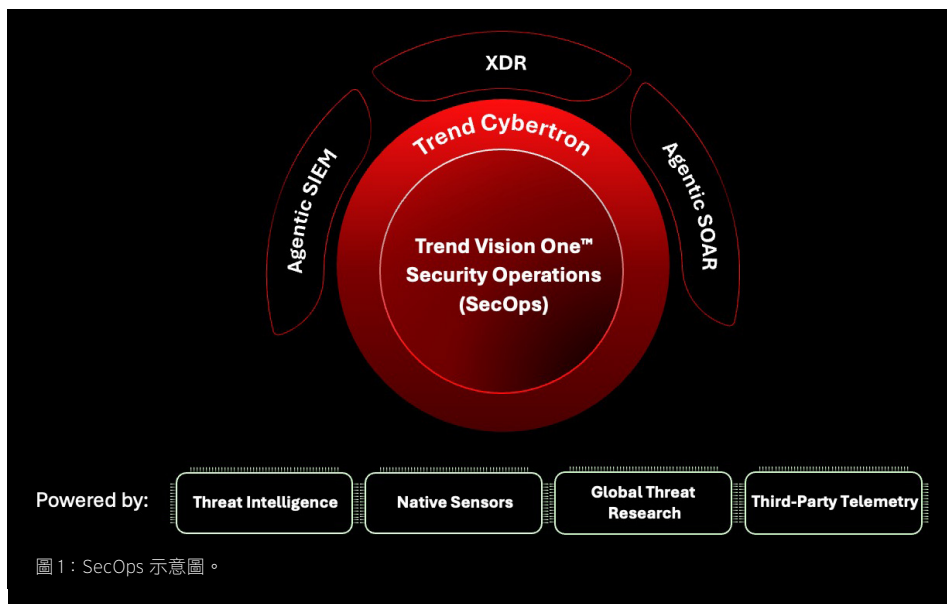
SecOps 是以我們先進的原生感測器為後盾，提供涵蓋所有防護層的全方位可視性。它能消除傳統 SIEM 在偵測上的嚴重漏洞，提供更好的防護並減少盲點。

輕鬆追蹤威脅

我們的 Trend Companion™ AI 網路資安顧問會引導分析師完成調查。它能提供 AI 驅動的洞見，將日常作業自動化，進而減少手動作業。如此一來，您的 SOC 團隊就能專心處理高優先次序的威脅、加快回應速度、提升整體效率。

了解您的資料。有意義地採取行動。

第一套以語言來思考而非單靠記錄檔的代理式 SIEM



輕鬆擷取第三方資料

輕鬆擷取分析資料（用於偵測及追蹤）與歸檔資料（用於合規及長期保留）。隨時跟上您不斷演變的環境，即時擷取任何類型的記錄檔，不論規模大小。

可化為行動的資料可觀察性

利用語言式交叉關聯與 AI 驅動偵測來排除雜訊，將多樣化的監測資料變成有意義的洞見，無須動手就能解析資料或建立規則。

簡化報告與合規作業

原生支援記錄檔保留、稽核與合規報告，全都在單一主控台上，讓您輕鬆達成合規要求。

簡化並擴大資料保留

採用可擴充的彈性策略來妥善保存重要資料而不拖慢營運速度，讓您安心達成合規與資料保留要求。



2024 年 MITRE ATT&CK™ 企業防護評測 (Enterprise Security Evaluation) 結果：

- 100% 分析涵蓋率：所有主要步驟 (16/16)
- 100% 分析涵蓋率：Linux 和 MacOS 所有子步驟
- 100% 分析涵蓋率：伺服器平台 (Windows/Linux) 所有子步驟
- 99% 分析涵蓋率：所有子步驟 (79/80)

建置涵蓋每一層面的強大原生威脅防護

- 端點偵測及回應 (EDR)：藉由深度的端點可視性與即時交叉關聯，在邊緣偵測及攔截威脅。
- 網路偵測及回應 (NDR)：揭露您網路上未受管理與不受控裝置上所隱藏的威脅。
- 雲端偵測及回應 (CDR)：藉由全方位的雲端偵測來保護工作負載、容器及叢集。身分偵測及回應 (ITDR)：標記危險的使用者，

將遭到入侵的身分列為早期威脅訊號。

- 電子郵件偵測及回應 (EmDR)：透過行為式電子郵件分析來偵測針對性攻擊與帳號被盜。
- 資料偵測及回應 (DDR)：追蹤機敏資料的移動，立即揭露資料被嘗試外傳的情況。

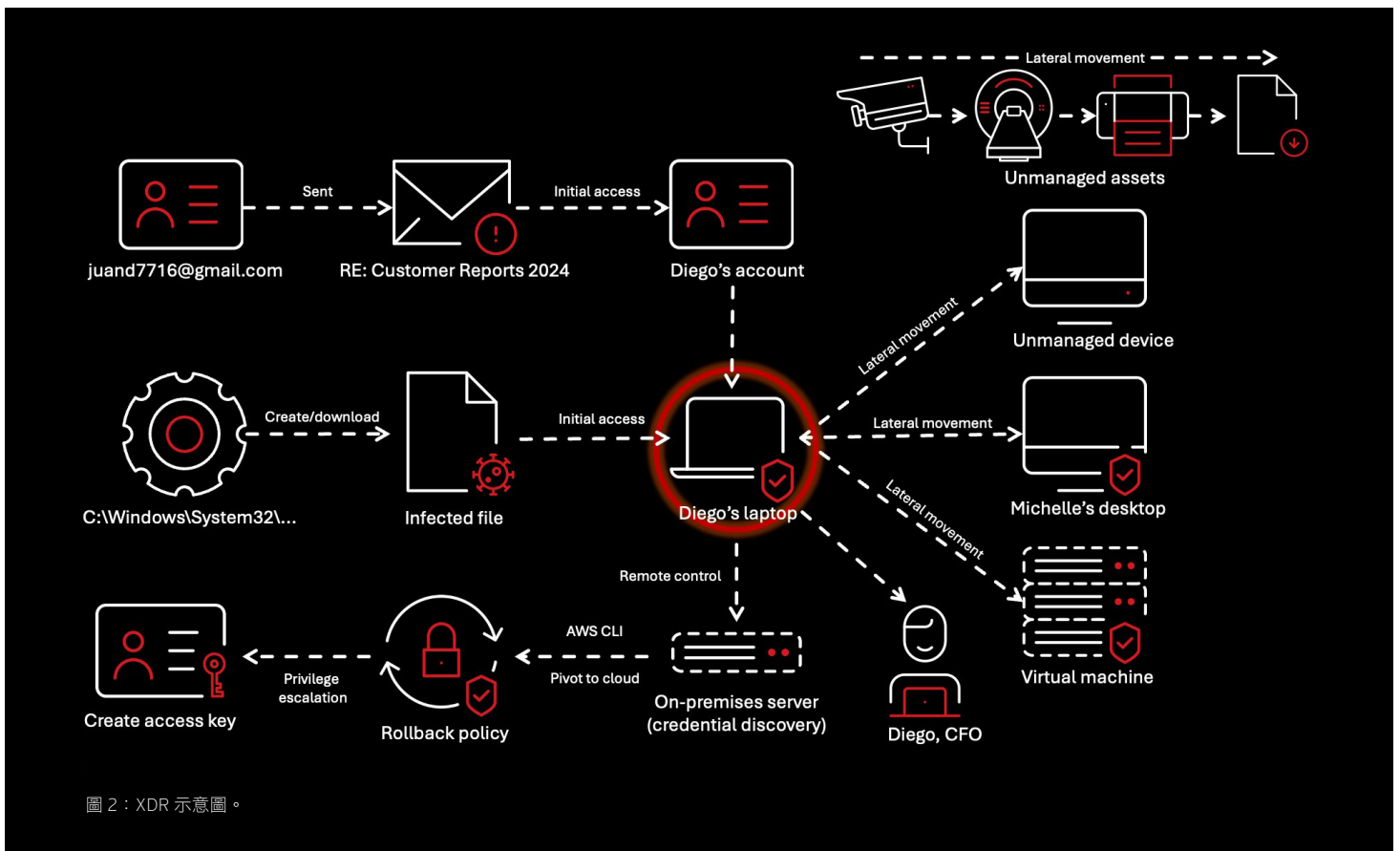


圖 2：XDR 示意圖。

使用代理式 SOAR 來重新定義事件回應

更少雜訊、更快行動，讓 SOC 的每個動作都發揮更明確的價值。

AI 驅動的調查

我們的工作台 (Workbench) 具備自動化優先次序判斷與 AI 功能，能摘要事件、指引後續行動，並點出最重要的事情，從收到警報到採取行動，SOC 團隊完全不需臆測。

端對端 SOC 自動化

從分類到解決，重複性的工作都能透過 AI 和彈性的案件管理來減輕負擔並最佳化。SOC 團隊將專心處理衝擊，而非忙於手動作業。

環環相扣的生態系

我們的代理式 SOAR 是專為串連而打造，能與現有的工作流程和系統整合，同時還提供開放的 API、客製化應變腳本 (Playbook) 以及即時協調。

會事先思考的工作流程

我們的代理式 SOAR 讓分析師透過直覺的 AI 輔助工作流程來發掘威脅並快速判斷情境，減少手動來回切換。



主動式防護就從這裡開始

Trend Vision One 是唯一將資安曝險管理、資安營運以及強大的多層式防護集中在一起來協助您預測及防範威脅、並加速實現主動式資安成效的企業網路資安平台。

關於趨勢科技

趨勢科技為網路資安全球領導廠商，致力建立一個安全的資訊交換世界。憑藉著數十年的資安專業、全球威脅研究以及持續不斷的創新，Trend Vision One 企業網路資安平台運用 AI 來保護全球數十萬家企業機構及數百萬一般使用者，涵蓋雲端、網路、裝置及端點。[TrendMicro.com](https://www.trendmicro.com)

©2025 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、Trend Micro 標誌、t 字球形標誌、Trend Vision One 及 Trend Companion 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。Trend Micro、Trend Micro 標誌與 t 字球形標誌註冊於美國專利與商標局。[SB00_Security_Operations_Solution_Brief_250625TW]

如需有關我們蒐集哪些個人資料的詳細內容和理由，請參閱我們的網站上的「隱私權聲明」：[trendmicro.com/privacy](https://www.trendmicro.com/privacy)

申請免費 30 天試用
[TrendMicro.com/trial](https://www.trendmicro.com/trial)