CORTEX XDR

藉著統一網路、端點與雲端數據，來追蹤與阻止隱匿性攻擊

商業優勢

- **自動發現隱匿性攻擊：**運用機器學習、行為分析和自訂偵測規則持續偵測威脅。
- **阻止警示麻痺與損害：**在幾秒內驗證安全警示，透過減少待處理項目提升分析師生產力和士氣。
- **縮短平均識別時間 (MTTI)：**結合精確的攻擊偵測與快速的警示分類，可大幅縮短停留時間。
- **縮短平均控制時間 (MTTC)：**在沒有多年經驗的情況下，調查及正確回應外部攻擊和內部威脅。
- **使用 Cortex 增加目前投資的投資報酬率：**透過受信任的應用程式生態系統解決所有安全需求，同時將現有基礎設施當做感測器和執行點。

打破孤島，簡化調查過程

安全團隊通常缺乏阻止攻擊所需的可視性與自動化。端點偵測與回應 (EDR) 和網路流量分析 (NTA) 等孤立的工具會收集大量數據，但它們也迫使分析師在控制台之間轉來轉去忙於驗證各種威脅，進而增加複雜度並減慢調查速度。面對網路安全專業人員的短缺問題，團隊必須簡化其作業，否則他們將難以調查及阻止攻擊。

快速偵測、調查及回應威脅

Cortex XDR 偵測與回應可將網路、端點和雲端數據原生整合在一起，以阻止精密的攻擊。運用行為分析，它可藉著行為分析來識別針對網路的未知與高度迴避的威脅。機器學習與 AI 模型會發現包括受管理與未受管理裝置在內所有來源的威脅。

Cortex XDR 透過提供每個威脅的完整狀況以及自動揭露根本原因，加速警示分類和事件回應。透過將不同類型的數據整合在一起並簡化調查，Cortex XDR 可縮短安全作業每個階段 (從分類到威脅捕捉) 所需的時間與經驗。與執行點緊密整合，可讓您快速回應威脅，應用透過調查獲得的知識，進而在未來偵測類似的攻擊。

使用 Traps 抵禦已知及未知的威脅

優異的安全性始於嚴密的保護。Cortex XDR 內嵌的 Traps™ 端點防護與回應使用多種預防方法來保護端點，防禦惡意軟體、勒索軟體和入侵。Traps 和 Cortex XDR 一起為您的所有數位資產提供一致的預防、偵測與回應。與雲端威脅情報原生整合，確保您的所有網路、端點和雲端安全產品的預防措施協調一致。

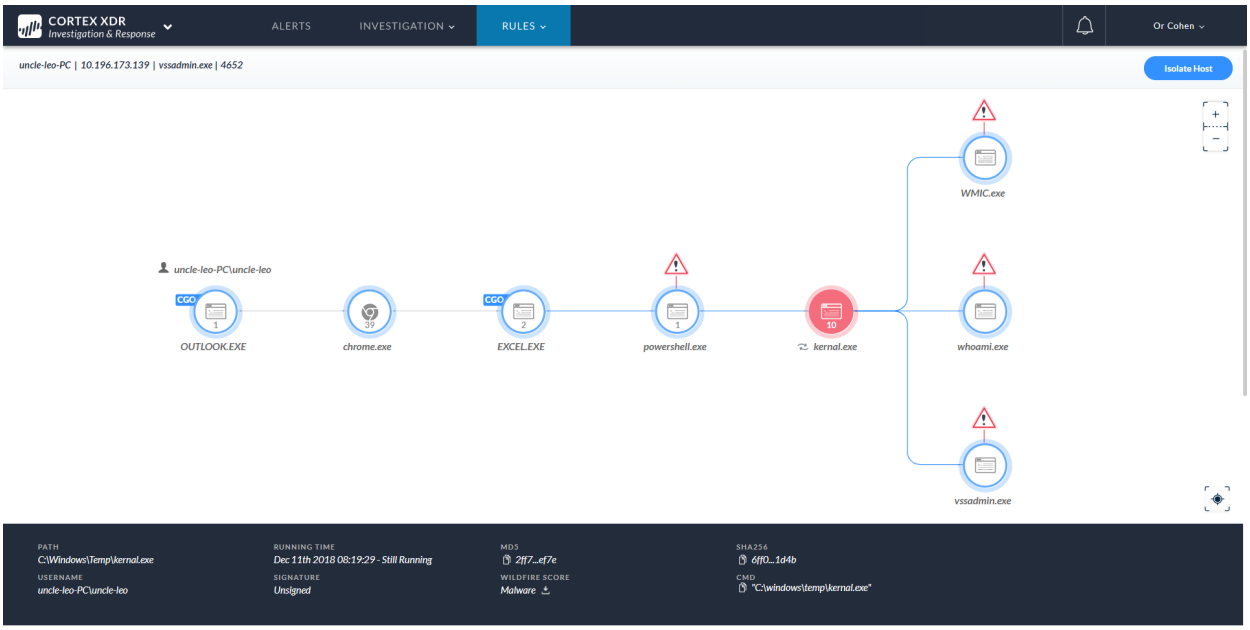

圖 1：Cortex XDR 儀表板

主要功能

取得完整的可視性

將網路、端點和雲端數據相互關聯，以簡化偵測與回應。Cortex XDR 透過自動將從您的網路、端點和雲端資產收集到的數據相互關聯，節省數小時的手動分析時間。它會在 Cortex Data Lake (可擴充又有效率的雲端數據儲存) 中將不同的數據類型整合在一起，以準確偵測攻擊並簡化調查。

使用 AI 來自動化攻擊偵測

使用行為分析來找出隱匿性攻擊。Cortex XDR 會自動指出主動攻擊，讓您的團隊在損害發生之前進行分類並控制威脅。運用機器學習，Cortex XDR 會持續剖析使用者與裝置行為，以偵測攻擊的異常活動跡象。透過檢查專為分析而建立的龐大數據，Cortex XDR 可偵測認證竊取和通道 DNS 威脅等攻擊，幾乎無法從標準威脅日誌或高階網路流量數據中識別這些攻擊。自動化偵測會每天全天候運作，讓您高枕無憂。

使用強大的搜尋工具捕捉威脅

發現隱藏的惡意軟體、針對性攻擊和內部威脅。您的安全團隊可以搜尋、排程及儲存查詢，以識別難以發現的威脅。靈活的搜尋功能可讓您的分析師捕捉威脅並搜尋入侵指標 (IoC)，而無需學習新的查詢語言。透過將 Palo Alto Networks 中的威脅情報與一整組網路、端點和雲端數據相結合，您的團隊可以捕捉惡意軟體、外部威脅和內部攻擊，無論事件是在進行中還是發生在過去皆可。

立即調查事件

自動揭露每個警示的根本原因。使用 Cortex XDR，您的分析師只要按一個按鈕，即可分析所有來源的警示，進而簡化調查。Cortex XDR 會自動揭露與每個警示相關聯的根本原因、信譽和事件序列，從而降低準確驗證所需的經驗需求。所有攻擊活動的鑑識時間表為事件調查提供了可操作的細節，使分析師能在幾秒鐘內確定範圍、損害和後續步驟。

協調執行點的回應

透過快速準確的補救來阻止威脅。Cortex XDR 可讓您的安全團隊從單一主控台立即控制網路、端點和雲端威脅。透過與執行點緊密整合，您的分析師可以快速阻止惡意軟體散播、限制針對裝置發動的網路活動以及更新威脅防禦清單 (例如惡意網域)。透過 Cortex XDR，您可以迅速關閉進階攻擊，同時從現有投資中獲取更多價值。

調整防禦以阻止未來的攻擊

使用行為規則偵測攻擊者的策略、技術和程序。透過 Cortex XDR，您的團隊可以應用每次調查獲得的知識，縮小您的攻擊範圍並簡化未來的調查，將您的安全態勢從被動轉變為主動。您的分析師也可以針對您的網路設計獨一無二的精細行為規則，用來偵測惡意活動。靈活的資訊警示可透過識別可疑行為並使複雜事件易於瞭解，來改善時間表分析。

取得業界領先的端點防護

使用單一代理程式進行端點威脅防禦與數據收集。您的 Cortex XDR 訂閱包括無限制的 Traps 代理程式，可提供最佳的端點防護。Traps 可讓您透過阻擋惡意行為與技術，阻止已知和未知的惡意軟體、入侵和勒索軟體。與 Palo Alto Networks WildFire® 惡意軟體防禦服務整合的雲端惡意軟體分析，可提升準確性和涵蓋範圍。Traps 代理程式會記錄所有端點活動，轉送到 Cortex Data Lake 進行分析，並協調回應。

使用雲端交付輕鬆部署

幾分鐘內即可開始使用。作為雲端應用程式，Cortex XDR 提供簡單、零接觸部署，無需部署新的內部部署日誌收集器或感測器。它會使用您現有的 Palo Alto Networks 產品當做感測器和執行點，進而減少需要管理的產品數量。如果您是新客戶，只需部署一種感測器類型 (例如新世代防火牆或 Traps) 即可使用 Cortex XDR 偵測及阻止威脅。Cortex XDR 建立於業界唯一的開放式 AI 型持續性 SOC 平台 Cortex 上。它藉由自動化和前所未有的準確性，在全新層級上簡化安全作業並顯著改善安全性成果。

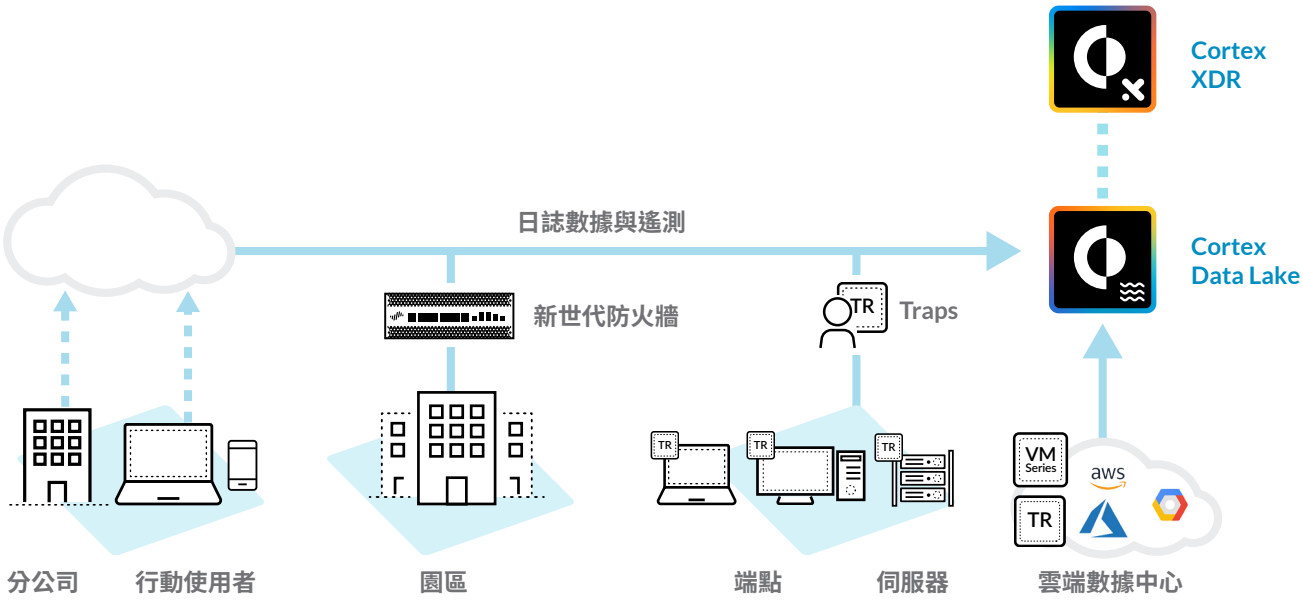

圖 2：分析所有來源的數據以進行偵測與回應

營運優勢

實現跨網路、端點和雲端數據的可視性：大規模收集網路、端點和雲端數據並相互關聯，以便用於偵測、分類、調查、回應及捕捉。

全天候自動偵測精密攻擊：使用始終開啟的機器學習和自訂規則，偵測進階持續性威脅和其他精密攻擊。

消除警示待處理項目：使用自動化的根本原因分析和時間表檢視來簡化調查，進而減少評估及分析警示所需的技能。

大幅減少誤判警示：應用從每個調查獲得的知識，調整行為偵測規則及加速未來的分析，進而減少雜訊和風險。

提高 SOC 生產力：藉著整合整個網路、端點與雲端環境的警示分類、調查和回應，將操作流程精簡至單一主控台。

在不影響業務的情況下修復：以外科手術般的精確度關閉攻擊，同時消除使用者或系統停機時間。

消除進階威脅：保護您的網路免於惡意內部人員、政策違規狀況、外部威脅、勒索軟體、無檔案和專門感染記憶體的攻擊，以及進階零時差惡意軟體。

增強您的安全團隊的防護能力：透過偵測 IoC、異常行為和惡意的活動模式，來中斷每個攻擊階段。

Cortex XDR 功能	
自動化的警示調查	自訂行為式偵測
根本原因分析	受監管和無需監管的機器學習
事件回應	惡意軟體和無檔案攻擊偵測
事件控制和復原	針對性攻擊偵測
事件後的影響分析	內部威脅偵測
威脅捕捉	有風險的使用者行為分析
IoC 和威脅情報搜尋	使用 Traps 防禦惡意軟體、勒索軟體及入侵

技術規格	
交付模式	雲端交付的應用程式
數據保留期間	30 天至無限期數據儲存

作業系統支援

Traps 支援 Windows®、macOS® 和 Linux 作業系統的多種端點。若需要系統要求與受支援作業系統的完整清單，請前往 Traps 相容性矩陣。

Cortex XDR Pathfinder 最低需求：2 CPU 核心、8 GB RAM、128 GB 精簡佈建儲存空間、VMware ESXi™ V5.1 或更高版本，或者 Microsoft Hyper-V® 6.3.96 或更高版本的超級管理器。

Cortex XDR 授權包括：

- Cortex XDR – 分析應用程式
- Cortex XDR – 調查和回應應用程式
- Traps 端點防護與回應
- Cortex XDR – Pathfinder 端點分析服務 (Traps 的無代理程式替代品)

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓

cortex-xdr-ds-022219