Cortex：從點對點進行主動安全作業

安全作業中心 (SOC) 已運作約 15 年，但直到過去五年來才變得相當重要。隨著防禦網路攻擊的需求以及採用集中式安全作業 (SecOps)，安全團隊遭遇的挑戰包括缺乏合格員工 (員工、技能與知識)、預算限制，以及市場上複雜解決方案的阻礙。

攻擊將變得更為頻繁、複雜且昂貴，這由不斷增加的勒索軟體所驅動。遺憾的是攻擊可能長期不被發現，導致停留時間增加，並延緩調查、緩解或補救。儘管作業缺乏效率的原因在各個企業中不盡相同，常見的問題包含：

- 對其裝置、應用程式、網路和系統的可視性受到限制。
- 不知道需要保護哪些資產
- 不了解要使用哪個工具，以及如何將其與現有基礎結構整合

為了因應全球規模的威脅並維持靈活度，安全團隊逐漸改用全面的雲端交付解決方案。此方法可實現安全作業的嚴格控制、安全狀況的整體檢視，以及整合式同級最佳產品，適用於資產探索、弱點評估、威脅偵測、行為監控、情報以及自動化回應。

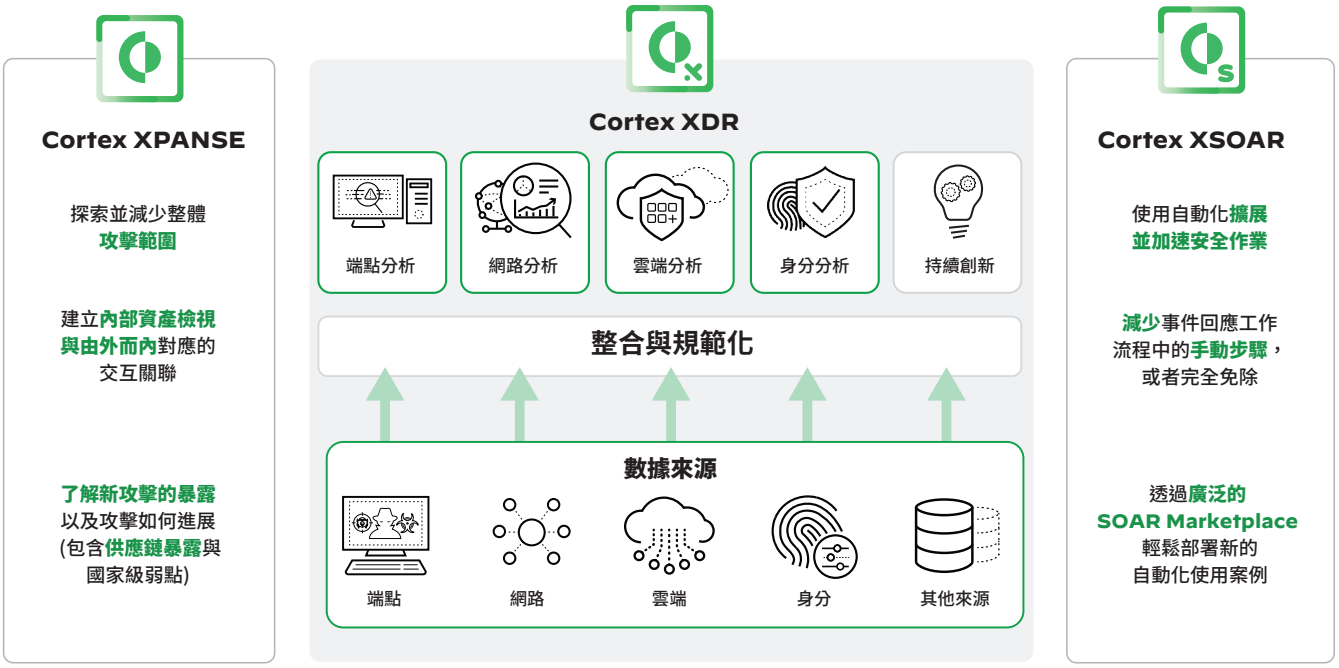

圖 1：適用於安全作業的點對點工作流程自動化

Cortex Xpanse：連接網際網路的資產探索與緩解

雲端與遠端工作的興起代表著攻擊範圍持續移動、變化，而且變得更加複雜。此外，掃描技術的進步讓攻擊者能更快速且輕鬆地掃描整個網際網路以找出攻擊途徑，並揭露出各種遭廢棄、惡意或錯誤設定的資產，這些資產可能會淪為攻擊者用來入侵的後門。攻擊範圍管理解決方案的部署，可針對企業的外部攻擊範圍提供持續的評估。

Cortex® Xpanse™ 可針對企業面向網際網路的全球雲端資產和暴露提供完整且準確的目錄，以持續發現、評估並緩解外部攻擊範圍，以及評估供應商風險，或評定所收購公司的安全性。

探索您的攻擊範圍：自動清點所有連接網際網路的資產以尋找未知風險。

防範勒索軟體：在攻擊者之前先探索暴露的遠端存取。

基礎結構監管：監控統合環境的安全性。

雲端安全：避免雲端蔓延並集中強制執行雲端政策。

第三方盡職調查：識別出供應商和所收購公司之間關係所衍生的風險。

Cortex XSOAR：安全協調、自動化與回應，外加威脅情報管理

任何 SOAR 解決方案的核心就是能夠針對需要最小程度人力介入的安全事件來設定優先順序並建立簡化的工作流程。SOAR 平台帶來效率提升，可在單一平台中自動化程序並降低事件調查的複雜度。

Cortex XSOAR 提供點對點事件與安全作業程序生命週期管理，可協助公司加速安全作業、減少調查和回應安全威脅所需的時間。所有規模的安全團隊皆可透過利用廣泛的廠商整合及超過 725 種預先建立的內容套件 (透過 XSOAR Marketplace 提供)，最大化企業涵蓋範圍，從而協調、自動化並加速 SecOps 工作流程的事件回應。

藉由 XSOAR，安全團隊可以從各種威脅情報來源存取集中化威脅情報庫，包括戰術 (電腦可讀取) 到策略來源 (以報告為基礎)，提供自動將威脅資訊對應至事件的能力，以及透過自動化來實用化威脅情報。

自動化和協調

快速、大規模回應安全事件：

- 數百種產品整合
- 數千個安全動作
- 直覺式、視覺劇本編輯器

案例管理

將跨產品、團隊和使用案例的流程標準化：

- 與案例管理工具整合的即時 ChatOps
- 依事件類型區分的自訂檢視
- 可自訂的儀表板和報告

即時協作

一起合作，提高調查品質：

- 虛擬戰情室可處理每個事件
- ChatOps 和即時安全動作
- 自動記錄劇本和分析人員動作

威脅情報管理

完全控制您的威脅情報摘要：

- 自動化重複性的每日指標管理工作
- 藉由現有威脅情報摘要獲得即時投資報酬率
- 透過事件回應決策獲得信心

Cortex XDR：端點威脅防禦、端點偵測和回應、行為分析，以及託管式偵測與回應

Cortex XDR 是一種取代 SIEM 且可行性更高的替代解決方案，它可提供深植在端點威脅偵測和回應中的威脅偵測、調查、回應和捕捉，並且可以隨著企業數據的移動而擴充至雲端環境中。一旦您防禦端點上可能會遇到的攻擊，Cortex XDR 便能提供專注於事件的偵測和回應，也就是自動化證據收集、進行相關警示的分組、將這些警示置於時間表中，揭露根本原因以加快各種技能層級的分析人員進行分類和調查的速度，藉以提供專注在事件上的偵測和回應能力。

Cortex XDR 可透過適用於 Windows® 與 Linux 主機的世界級 EDR，在端點與主機阻止攻擊：

- AI 驅動的本機分析與定期更新的機器學習式行為分析
- 一套端點防護功能，例如裝置控制、主機防火牆，以及磁碟加密
- 廣泛的防護模組，可抵禦執行前和執行後的入侵

Cortex XDR 與第三方緊密整合，提供更好的分析、更快的回應功能 — 不可或缺的功能，企業在回應事件時最多可以使用 45 種工具。[1]

安全團隊使用 Cortex XDR 以更有效率且更有效的方式阻止攻擊、消除盲點、縮短調查時間，最後改善安全成果。Cortex XDR 能夠在關鍵階段阻止攻擊序列，例如可在執行階段將其阻斷以避免攻擊手法得以持續而造成更廣泛的橫向損失，最後安全團隊找到了這個解決方案「中途攔截這些攻擊」。

藉由分析偵測進階攻擊：透過 AI、行為分析和自訂偵測規則來發現威脅。

專注於事件而非警示：透過顛覆性的統一事件引擎避免警示麻痺，以智慧的方式將事件相關警示分組。

調查速度快了 8 倍：透過使用根本原因分析獲得攻擊的完整狀況，迅速驗證威脅。

在不降低效能的情況下停止攻擊：使用輕量化代理程式可獲得最有效的端點防護。

達到最大投資報酬率：使用現有基礎結構進行數據收集和控制，將成本降低 44%。

1. *2020 年網路彈性企業報告*，Ponemon Institute，2020 年 6 月 30 日，https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839。

各個優點結合為龐大優勢

Cortex 產品組合提供點對點安全解決方案，可確保涵蓋每個安全程序步驟。

Cortex Xpanse 在一開始便可確保您的企業對於整個攻擊範圍和風險擁有全面且最新的檢視。這不僅包含潛在暴露的檢視，也能輕鬆檢視資產是否受到 Cortex XDR 保護。此外，Xpanse 可以使用來自 Cortex XDR 的數據，以提供關於遠端工作者環境安全的關鍵資訊。

由於 Xpanse 或 Cortex XDR 會探索新風險與威脅，Cortex XSOAR 可減少手動人工作業，以補救風險並回應威脅。透過 Cortex XSOAR，新探索到的資產或暴露警示可自動傳送至負責的相關各方，以確保僅負責處理問題的人員才會收到警示通知。

Cortex 是業界最全面的安全作業產品組合，包含點對點解決方案，可確保企業採取主動而非被動安全。安全作業始於攻擊範圍管理，以取得資產與風險的完整可視性，進而獲得同級最佳防禦、偵測和端點回應，以及強大的自動化功能以減少人工作業。透過採用產品組合方法，團隊可受益於整合式解決方案，以提供持續防禦與不間斷的風險管理。

如需關於 Cortex 產品套件如何提供同級最佳的威脅偵測、防禦、攻擊範圍管理，以及安全自動化功能的資訊，請下載我們的白皮書：

使用 Cortex 建立虛擬 SOC 平台

現在如何規劃未來的 SOC_

造訪我們的產品頁面：

Cortex Xpanse

Cortex XSOAR

Cortex XDR

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