Cortex XSIAM

AI 驅動的安全作業平台

Cortex® XSIAM™ (擴充式安全情報和自動化管理) 是針對現代安全作業中心 (SOC) 的 AI 驅動的安全作業平台，利用人工智慧和自動化的力量從根本上改善安全成果並達成安全轉型。透過將多個產品整合到專為安全營運而建置的單一平台中，降低風險和營運複雜度。

SOC 的需求已經改變

SOC 的要求已經演變。企業面臨安全事件偵測和補救時間延長的問題。再加上最近的監管入侵通知要求以及威脅行動者在數小時內快速執行點對點攻擊，這對企業帶來重大風險。

每次入侵發生後，安全團隊都會成功調查事件，發現入侵方法、受影響的系統和遭竊的數據。問題出現了：如果您擁有了解事件後詳細資料的資訊，為什麼不在此類事件發生之前採取主動措施來預防或阻止呢？

這個問題的答案在於 SOC 現今面臨的三個主要挑戰：

1. 孤立的工具和數據

太多的工具來完成一項工作並不一定有幫助。不同的網路安全工具會導致工作流程效率不彰 (在多個產品和多個主控台之間切換)，進而導致認知負荷增加和對威脅的潛在監督增加。缺乏整合還會阻礙即時威脅偵測並延遲事件回應，同時維護多個工具會佔用大量資源，並會增加營運複雜度。大多數企業都擁有大量的安全和應用程式數據，但數量太多，而且存在於不同的地方。網路數據儲存在防火牆中，端點數據存在於端點偵測與回應 (EDR) 中，驗證數據存在於單獨的日誌中，而其他關鍵資訊可能永遠不會離開應用程式特定的日誌。更糟的是大約半數的企業表示他們尚未將雲端作業連線到 SOC，因此一切仍然是中斷連線的數據點。

2. 弱式威脅防禦

僅依靠靜態關聯規則和廣泛的偵測工程 (由於數據量巨大而加劇) 在識別整個環境中的安全事件之間有意義的關係方面提出重大挑戰。在這種情況下，警示顯示為中斷連線的數據點，需要 SOC 團隊進行手動關聯工作。不過，這種方法經常導致偵測不準確，其特徵是誤判率偏高。該過程的脫節性質阻礙安全基礎結構的有效性，突顯出需要更先進和調適型威脅偵測方法來減少誤判並增強整體安全狀況。

3. 嚴重依賴手動作業

大量互不相關的數據和不同的工具導致大量警示需要 SOC 進行調查和解決。在處理這些警示時，SOC 分析師很難確定首先處理哪些警示的優先順序，並且通常需要手動關聯各種數據來源和工具中的事件，才能找出他們需要處理的內容。通常，他們可能正在調查多個不同的警示，卻不知道這些警示與單一事件有關。這會導致冗餘和手動工作，進而延長偵測和補救安全事件的平均時間。

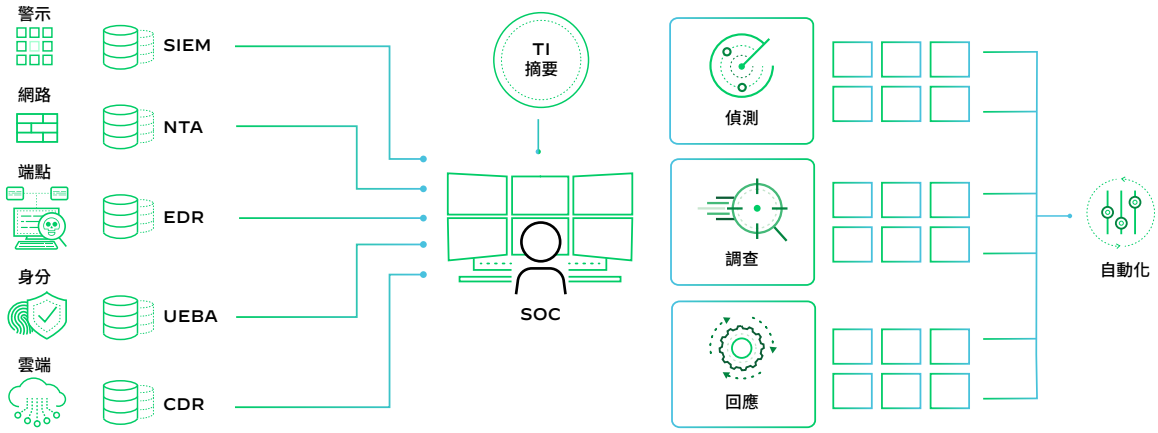

圖 1：孤立安全營運

解決方案：重新思考並達成安全營運轉型

現代 SOC 必須建立在新的架構之上：廣泛且自動化的數據整合、分析和分類。這就是為什麼整合式平台對於簡化流程和提高效率至關重要。在現今快步調的數位環境中，簡化營運複雜度至關重要。透過將各種系統和工具整合到一個集中式解決方案中，企業可以消除孤島並達成營運的統一檢視。

此外，大規模阻止威脅是企業的首要任務。透過 AI 驅動的成果，企業可以主動偵測並減輕潛在風險，確保數據和系統的安全性。

此外，自動化優先的方法可以加快事件補救速度，減少手動工作量和回應時間。透過利用自動化，企業可以快速解決問題、儘可能減少停機時間並優化整體營運效能。

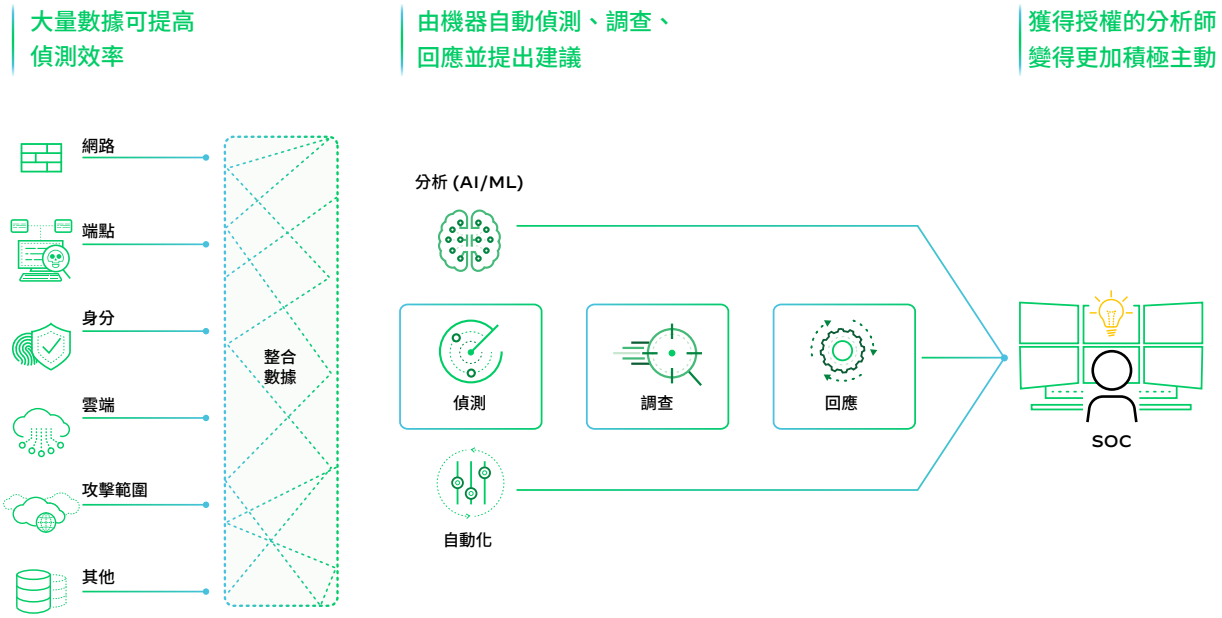

圖 2：轉型後的 SOC

Cortex XSIAM

Cortex® XSIAM™ 是現代 SOC 的 AI 驅動安全作業平台，利用人工智慧和自動化的力量來簡化安全營運、大規模阻止威脅並加速事件補救。透過將多個產品整合到專為安全營運而建置的一體化平台中，降低風險和營運複雜度。

Cortex XSIAM 旨在解決 SOC 目前和未來面臨的獨特挑戰。透過將數據和工具整合到單一 AI 驅動的平台中，SOC 可以簡化安全營運、大規模阻止威脅並顯著加速安全成果。

Cortex XSIAM 的建置考量三個目標，使無法解決的問題在 SOC 中迎刃而解：

1. 透過整合式平台簡化安全營運

將 XDR、SOAR、ASM 和 SIEM 等 SOC 功能整合到單一平台中，將徹底改變安全營運的遊戲規則。如此消除主控台切換的麻煩，提供簡化的體驗。該平台提供廣泛的整合支援，可以更輕鬆地加載各種數據來源，完全不需要進行大量的工程和基礎結構工作。因此，SOC 能夠輕鬆獲得更多與安全相關的數據，進而增強其分析能力。此外，該平台確保原始數據的連續收集、整合和標準化，而不僅僅是發出警示。這讓 SOC 團隊能夠進行卓越且簡化的調查，讓他們能夠更快速且更有效地識別和補救威脅。

2. 透過 AI 驅動的成果大規模阻止威脅

立即可用的 AI 模型超越傳統方法，可以連線各種數據來源的事件，並提供對於單一位置的事件和風險的全面概觀。這讓企業能夠增強其偵測、分析和回應能力。透過利用警示分組和 AI 驅動的事件評分，Cortex XSIAM 無縫連接低可信度事件，將其轉化為高可信度事件。這種優先順序基於整體風險，因此安全團隊能夠有效地集中精力。

3. 透過自動化優先的方法加速事件補救

憑藉 Cortex Marketplace 中數百個經過試驗和測試的內容套件，SOC 可以最佳化整個安全計劃的流程和互動。透過自動化先前的手動任務，嵌入式自動化可以節省回應事件或管理風險（例如攻擊範圍暴露）的時間和精力。此外，使用者可以根據自己的特定需求靈活地新增、自訂或修改自動化。該平台還提供自動觸發的警示特定劇本，確保安全任務及時執行，風險得到解決，甚至在分析師介入之前就可以解決。此外，XSIAM 從分析師的手動操作中學習，並為未來的自動化提供建議。這種持續學習過程增強平台自動解決事件的能力，進而隨著時間的推移提高效率和準確性。

全新的安全營運設計可以協助您：

- **重新定義** SOC 架構以採用自動化優先的方法
- **統整**同級最佳 SOC 功能以改善分析人員體驗
- 將多個不同產品**整合**成單一平台
- 將 SOC **擴展**至雲端以取得完整可視性
- 透過著重於重要事件來**提高**分析師的工作效率

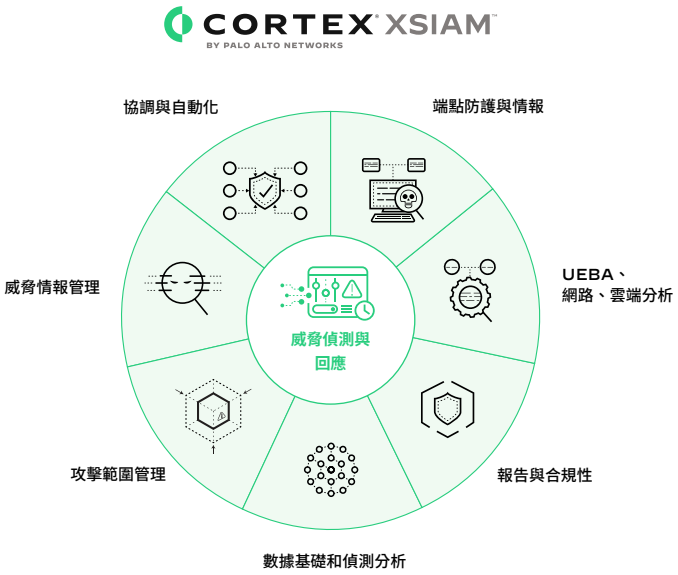

圖 3：Cortex XSIAM

關鍵整合功能

Cortex XSIAM 會將這些關鍵 SOC 產品功能整合至單一的統合式平台：

安全資訊和事件管理 (SIEM)

包括日誌管理、關聯和警示、合規性報告* 以及其他常見 SIEM 功能。

威脅情報平台 (TIP)*

提供完整的 TIP 功能來管理 Palo Alto Networks 和第三方摘要，並自動將這些摘要對應到警示和事件。

擴展的偵測與回應 (XDR)

整合端點、雲端、網路和第三方遙測以達到自動偵測和回應。

端點偵測與回應 (EDR)

包括完整的端點代理程式和雲端分析後端，藉以提供端點威脅防禦、自動回應以及對任何威脅調查有用的深度遙測。

攻擊範圍管理 (ASM)*

包括嵌入式 ASM 功能，可以提供資產目錄的整體檢視，包括針對已發現面向網際網路的資產發出的內部端點和弱點警示。

身分威脅偵測與回應 (ITDR)*

將 UEBA 功能與增強的身分威脅模組結合，藉以有效偵測、防禦和回應內部威脅、數據外洩、可疑橫向移動等威脅。

使用者與實體行為分析 (UEBA)

使用機器學習和行為分析以針對使用者和實體進行剖析，對於顯露出帳戶入侵或惡意內部人員的行為發出警示。

安全協調、自動化和回應 (SOAR)

包括強大的 SOAR 模組和市場，用於建立和協調與 Cortex XSIAM 一起使用的劇本。

雲端偵測與回應 (CDR)

Cortex XSIAM 分析陣列包括旨在偵測雲端數據異常並發出警示的專業分析，例如雲端服務供應商日誌和雲端安全產品警示。

管理、報告與合規性

集中管理功能簡化網路作業。強大的圖形報告功能支援合規性、數據取得、事件趨勢、SOC 效能指標等等的報告。

* 透過額外授權和模組提供。

Cortex XSIAM 提供真正的成果

雖然 Cortex XSIAM 正在為 Palo Alto Networks SOC 帶來指數級改善效益，但是我們的主要目標是透過創新來超越網路威脅，以便客戶能夠充滿信心地接受和部署我們的技術。最近的客戶成功指標證明 Cortex XSIAM 正在做到這一點。

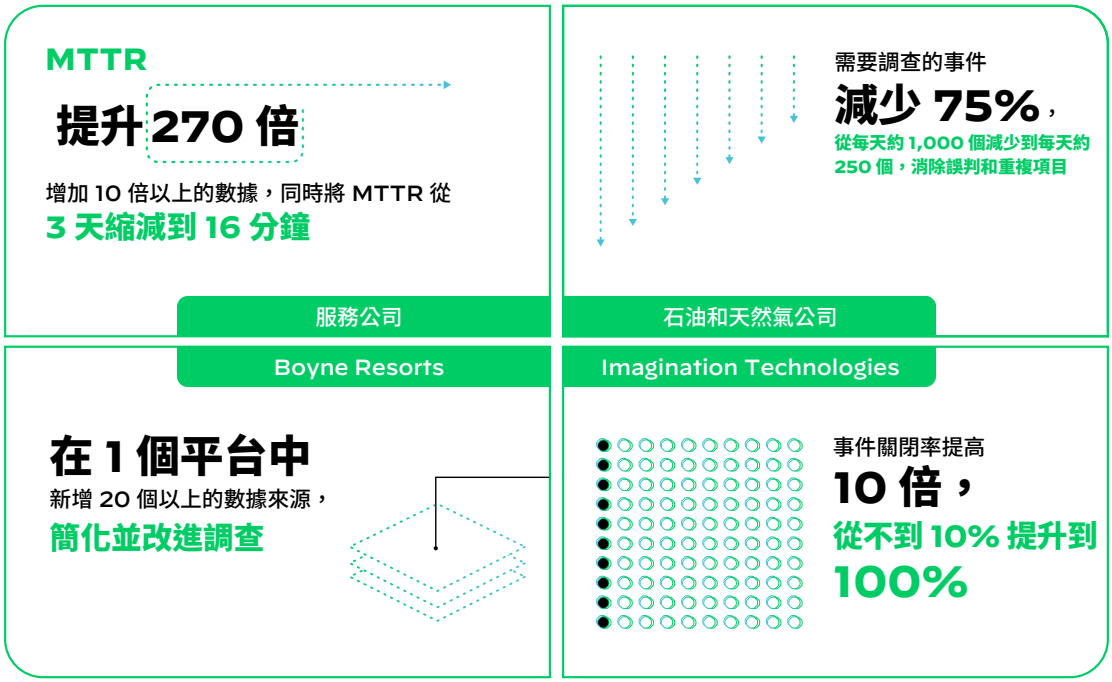

圖 4：Cortex XSIAM 客戶提高 SOC 效率，同時提高整體可視性

Cortex XSIAM 的優勢：

- 提高偵測和防禦能力，**在攻擊成為事件之前加以阻止**
- 讓 SOC 能夠擷取更多數據來源，同時**將回應時間從幾天縮短到幾分鐘**
- **提高事件結束率並且儘可能減少**需要手動調查和補救的**事件數量**
- 簡化數據上線和**降低基礎結構的複雜度**
- 為安全從業人員提供**從被動式安全轉向主動式安全**所需的知識和能力

招募管理型服務專家

Unit 42® 團隊運用多年保護全球企業和政府的經驗全天候監控您的環境並尋找可疑活動。憑藉 10 多年惡意軟體分析得出的業界領先威脅情報，每天新增超過 3,000 萬個新的惡意軟體樣本和 5000 億個事件，我們的 Unit 42 專家可確保您領先於新興威脅。Unit 42 託管式偵測與回應 (MDR) 和託管式威脅捕捉 (MTH) 服務很容易就能夠新增到您的 Cortex XSIAM 訂閱中。

Unit 42 託管式偵測與回應

Palo Alto Networks Unit 42 託管式偵測與回應 (Unit 42 MDR) 服務提供一支由世界級分析師、威脅捕捉專家和研究人員組成的團隊，他們為您調查和回應攻擊，因此您的團隊能夠快速擴展並著重於更具策略性的任務。Unit 42 MDR 包含託管式威脅捕捉。

Unit 42 託管式威脅捕捉

Palo Alto Networks Unit 42 託管式威脅捕捉 (Unit 42 MTH) 服務提供一支由世界級分析師、捕捉專家和研究人員組成的團隊，他們將主動搜尋進階威脅並提供詳細報告，讓您安心無憂。

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 6F-1