Cortex XSIAM

AI 驅動的安全作業平台

SOC 的需求已經改變。企業需要花費很長時間才能偵測到安全事件，而當他們偵測到安全事件時，也需要花費很長時間才能進行補救。結合最近的監管要求和威脅行動者在幾小時內實施點對點攻擊，這對企業帶來巨大的風險。

挑戰：SOC 的需求已經改變

這個核心問題是 SOC 目前所面臨三個基本挑戰的結果：

1. 孤立的工具和數據

企業通常儲存大量的安全和應用程式數據，這些數據永遠不會聚集在一個地方，更不用說以標準化的方式用於威脅偵測和回應。分析師需要調查威脅時，他們會花太多時間在工具之間切換來尋找所需的資訊。結果導致 SOC 的營運複雜度。

2. 弱式威脅防禦

大量孤立的數據加上繁重的偵測工程要求，讓識別安全事件之間的關係變得困難，甚至不可能。企業通常依賴靜態關聯規則來識別惡意活動，但這通常會導致較高的誤判率和遺漏威脅。而且由於安全警示是多個工具中互不關聯的數據點，SOC 不得不手動關聯事件。這最後導致必須大規模阻止威脅。

3. 嚴重依賴手動作業

脫節的數據、獨立的工具以及缺乏對 AI 和自動化的有效使用，導致 SOC 需要大量的手動工作和備援。這種規模問題表示 SOC 不可能對所有傳入警示做出回應，而且他們很難確定首先處理哪些警示的優先順序。除了分析師的倦怠和工作不滿之外，這還導致威脅偵測和補救的嚴重延遲。

解決方案：重新思考與轉變安全營運

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；統一的工作流程使分析師能夠提高工作效率；嵌入式智慧和自動回應可以在最少的分析師協助下阻止攻擊。

與傳統安全營運不同，現代 SOC 藉助 AI 和自動化來處理大量數據集，而不是依靠人力判斷以及為了應付過往威脅所設計的規則。

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，這將改變安全營運的遊戲規則。它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，可以更輕鬆地載入各種數據來源，而無需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，而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 模型超越傳統的方法，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。

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。透過將多個產品集中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。

XSIAM 統一同級最佳的安全營運功能，包括 EDR、XDR、SOAR、ASM、UEBA、TIP、SIEM 等等。Cortex XSIAM 還集中所有安全數據，並使用專為偵測和阻止已知和未知安全事件而設計的機器學習數據模型。透過 XSIAM，自動化數據整合、分析和回應動作，分析師能夠專注於重要的事件。

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

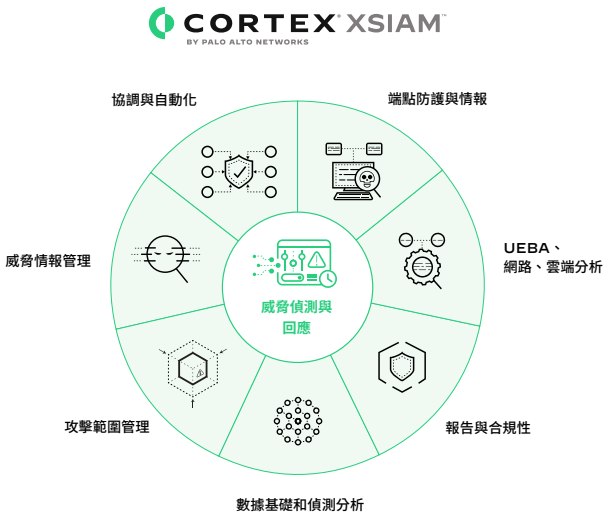

圖 1：Cortex XSIAM

簡化的數據上線程序可讓 SecOps 團隊輕鬆地新增數據來源，擴充的數據模型則可以規範化數據並建立關聯性，以進行「讀取時建立結構描述」的數據存取。Cortex XSIAM 也會自動整合端點、網路、雲端、身分和其他數據，讓其能夠精準地偵測進階威脅，並透過跨數據見解簡化調查程序。

Cortex XSIAM 透過智慧警示分組和根本原因分析提供每次攻擊的完整情況，因此分析師能夠快速地調查事件。內嵌的自動化可強化警示、回應惡意活動，並且在低風險警示排入佇列之前預先將其關閉，讓分析人員能夠注意在少數需要人為介入的威脅上。Cortex XSIAM 為 Palo Alto Networks 本身的 SOC 提供支援，每個月都能縮減超過 1 兆個事件，讓分析人員每天都只需要處理少數幾個事件。

與將產品操作和最佳化工作交給客戶的舊型 SOC 解決方案不同，XSIAM 則是受益於 Palo Alto Networks Unit 42 研究團隊所提供的持續更新。Palo Alto Networks 專家從 90,000 多個客戶收集威脅情報、更新機器學習 (ML) 偵測模型，並自動將最新的保護分發到 Cortex XSIAM 部署。來自整個威脅威脅形勢的見解有助於保護客戶免於遭受快速發展的最新進階威脅。在融合先進的技術與共享的情報和研究後，Palo Alto Networks 就能共同分擔保護客戶永續經營的責任。

AI 驅動的安全作業平台

Cortex XSIAM 利用人工智慧 (AI) 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。

應用 AI 來推動更好的安全成果依賴良好的數據。Cortex XSIAM 透過集中、整合和最佳化數據，讓 SOC 完全控制從端點到雲端的企業安全性，特別是用於偵測和防禦安全事件。

Cortex XSIAM 使用人工智慧，利用數千個成熟的機器學習數據模型，旨在快速且準確地識別惡意安全事件。這些模型是基於從數萬個環境中學習到的行為而建立，有助於區別異常活動與惡意活動。這顯著減少誤判並提高偵測和防禦能力，在攻擊演變為安全事件之前加以阻止。

Cortex XSIAM 分析提供基於技術的情報，允許將多個警示整合並分組為較少數量的事件。這些事件充分強化相關脈絡，可以透過自動化解決，也可以對分析師提供利用 AI SmartScoring 系統定義的適當嚴重性分類 (嚴重、高、低等)。

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。

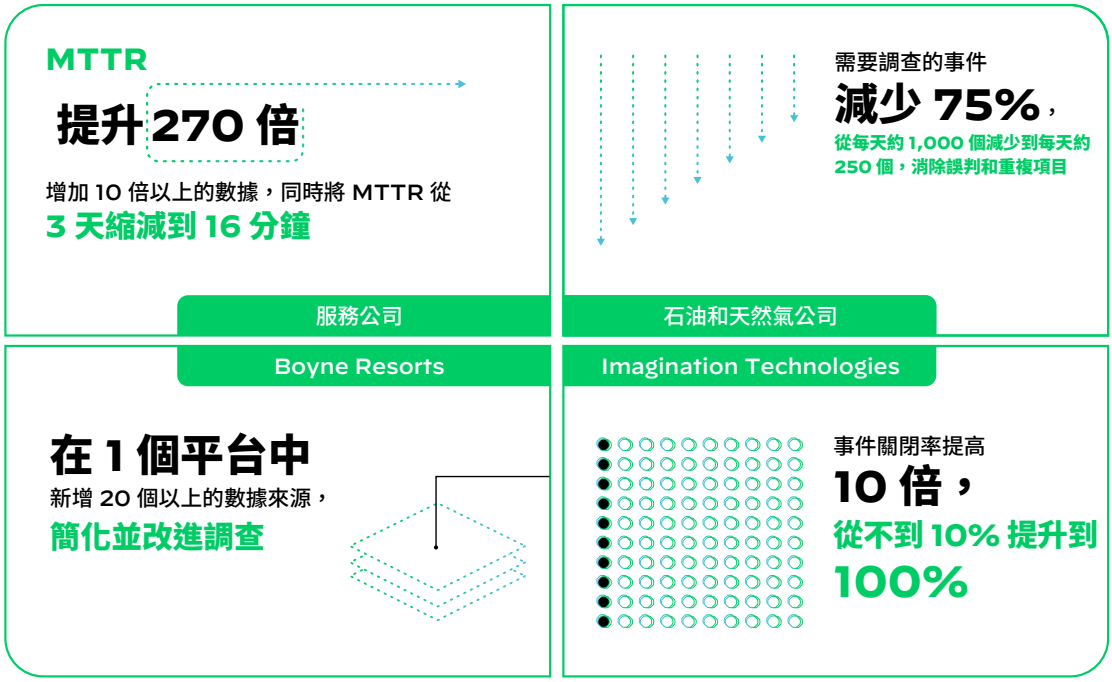

圖 2：Cortex XSIAM 客戶提高 SOC 效率，同時提高整體可視性

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 能夠攝入更多數據來源，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

造訪 Cortex XSIAM 頁面或立即連絡客戶經理安排示範並了解 XSIAM 的實際應用。

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機構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。

資源

- Cortex XSIAM 電子書
- Cortex XSIAM 說明中心
- 客戶案例：Imagination Technologies 利用 Cortex XSIAM 達成 SOC 營運轉型
- 客戶案例：石油和天然氣公司利用 Cortex XSIAM 部署 AI 驅動的 SOC

關於本型錄

本文中提供的技術或專業主題相關的資訊僅供一般參考，可能會有所變更，並不構成法律或專業建議，也不保證適用於特定目的或遵從適用法律。

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

cortex_ds_cortex-xsiam_102523