Cortex XSOAR

重新定義安全協調、自動化與回應

對於處理大量的警示和無窮無盡的安全任務，安全團隊需要更多人員和可擴充的程序。分析師將時間浪費在操作不同的主控台進行數據收集、判斷是否誤報，以及在事件的整個生命週期中執行重複性手動任務。面對愈來愈嚴重的技能短缺問題，安全領導者應該將更多時間用來訂定重要的決策，而不是陷入被動且分散的手動回應中。這並非解決之道。

安全營運轉型

您的 SOC 團隊能透過統一自動化、案例管理、即時協作及威脅情報管理來簡化安全營運。這代表您可在 Cortex XSOAR 的幫助下，管理所有來源的警示、使用劇本將程序標準化、處理威脅情報，而且能對幾乎所有使用案例自動做出回應。

商業優勢

藉由 Cortex XSOAR，貴企業將能夠：

- 將事件回應程序擴充和標準化。
- 縮短解決時間並提高 SOC 效率。
- 提高分析師的工作效率並增強團隊學習能力。
- 透過現有威脅情報投資立即達到投資報酬率。

為什麼選擇 Cortex XSOAR？

可透過自動化事件回應來改善 SOC 效率

藉由 Cortex XSOAR 實現事件回應工作流程及重複性任務的自動化，使分析人員能夠專注於處理最關鍵的事件。使用預先定義的劇本或輕鬆自訂自己的劇本來自動化 SOC 使用案例，例如指標強化、警示重複數據刪除、網路釣魚回應、勒索軟體回應、威脅情報摘要管理、惡意軟體調查，甚至是員工入職和離職等 IT 營運。

體驗更好的效能、可靠性和可擴充性

Cortex XSOAR 現在提供雲端原生 SOAR，可自動擴充以支援未來的成長，並透過快速部署來加速實現投資回報率。完全整合到 Cortex 平台的 Cortex XSOAR 是透過統一的使用者介面提供，因此可實現工作流程管理的易用性和一致性。

取得、搜尋和查詢所有安全警示

當複雜的即時調查需要分析人員介入時，必須確保他們能夠進行極為迅速的搜尋、查詢和調查，並透過 Cortex XSOAR 在單一平台上整合任何來源的警示、事件和指標以加快事件回應速度。

一起合作，提高調查品質

協作調查功能提供強大的工具套件來協助分析人員相互協助、執行即時安全命令，並自動記錄所有動作以了解每個事件的脈絡。由機器學習驅動的助理可以學習平台中採取的動作，並提供分析師指派和執行動作命令的指南。

滿懷信心且迅速地針對威脅情報採取行動

進行原生威脅情報管理，並透過劇本驅動的自動化功能整合威脅情報彙總、評分和分享。可將額外的第三方威脅情報進行分層以更有效地揭露及排定關鍵威脅的優先順序，藉此增強內建、高真實性的威脅情報。

圖 1：Cortex XSOAR 的價值

Cortex XSOAR 的運作方式

在執行可自動化、由程序驅動的劇本以強化並回應事件之前，Cortex XSOAR 會從偵測來源 (例如安全資訊和事件管理 (SIEM) 解決方案、網路安全工具、威脅情報摘要和信箱) 擷取彙總的警示和入侵指標 (IoC)。這些劇本在技術、安全團隊和外部使用者之間進行協調，藉以實現集中的數據可視性和行動。

簡單且可擴充的部署

Cortex XSOAR 的雲端原生 SaaS 環境可進行快速部署以獲得即時投資報酬率，為任何規模的客戶提供支援。我們也提供內部部署。

對於管理型安全服務供應商 (MSSP)，Cortex XSOAR 可透過數據區隔和和可擴充架構支援完全多租用戶環境。MSSP 可以在 Cortex XSOAR 上進行管理型服務營運，為客戶提供頂級產品並發揮內部團隊的最佳生產力。對於現有 Cortex 使用者來說，XSOAR 可以輕鬆整合到其他 Cortex 解決方案中，並從同一平台提供。

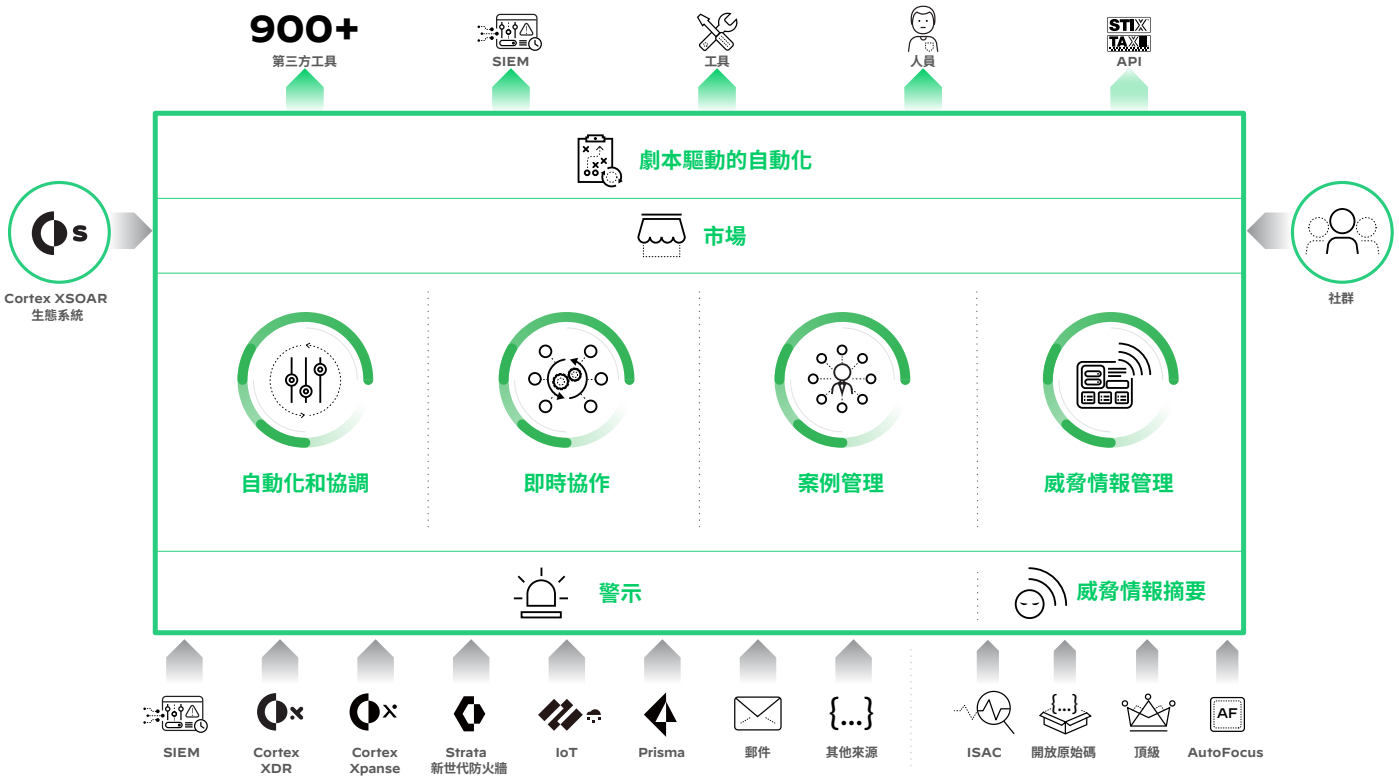

圖 2：Cortex XSOAR 平台

整裝待發，邁向成功

我們業界領先的客戶成功團隊致力於協助您不斷強化安全狀況，並充分運用 Cortex XSOAR 實作。

標準版成功計劃包含在每個 Cortex XSOAR 訂閱中，可提供自我引導式的資料和線上支援工具，協助您快速啟動和執行。您也可以選擇升級至頂級版成功計劃，它可提供指引式上線訓練、自訂研討會、全天候技術電話支援，並且能夠與客戶成功團隊聯絡以提供個人化的體驗，確保您實現最佳的投資報酬率 (ROI)。

令 Cortex XSOAR 與眾不同的原因？

廣泛的生態系統和使用案例

Cortex Marketplace 是業界最廣泛的 SOAR 社群，可透過 Cortex Marketplace 提供 900 多種整合方式，並針對最常見的使用案例提供許多立即可用的劇本。

協作

內建協作功能 (例如戰情室)，可促進跨部門和跨職能的團隊合作以快速解決複雜事件。

整合式威脅情報管理

Cortex XSOAR 將原生威脅情報緊密整合至統一的工作流程中，同時將各種警示與其來源和編譯的威脅情報數據進行配對，以自動執行適當的回應。

開始您的 Cortex XSOAR 30 天免費試用。使用單一使用案例自動化安全營運來展開安全自動化旅程。

立即試用：https://start.paloaltonetworks.com/sign-up-for-community-edition.html。

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