Cortex XSOAR 案例管理

CORTEX XSOAR
BY PALO ALTO NETWORKS

- **完整的案例管理：**多來源警示取得、集中式事件佇列、全方位的 SLA 追蹤和指標、證據收集與日誌記錄、行動應用程式支援。
- **專為完全自訂而設計：**適用於事件類型和安全角色的自訂流程與配置、適用於程序工作流程的彈性劇本、小工具驅動的儀表板和報告。
- **持續改進與學習：**以機器學習的方式，對於事件負責者/任務指派、相關事件，以及經常執行的安全命令提供深入見解。

以安全為中心的案例管理

在威脅不斷升級並複雜化的形勢下，SOC 員工面臨著全面的挑戰。其中一個主要挑戰是在適用於大量攻擊的標準化事件回應，與適用於複雜的一次性攻擊的自訂回應之間找到平衡。此外，SOC 員工也缺乏對持續改進和學習的關注，大部分時間用於處於日常事件。

這就是 Cortex XSOAR 的用武之地。我們的完整案例管理功能結合安全協調和自動化，可以在攻擊不斷增加的情況下，更快地進行分類、回應和協調。它專注於自訂功能 (從精細的指標和回應工作流程到事件流程和欄位)，可讓使用者針對攻擊類型量身打造自己的回應方式。機器學習提供的見解還可以幫助使用者持續學習，並提供有關事件負責者、任務指派、相關事件以及經常執行之命令的建議。整合式威脅情報管理可自動取得、彙總並調整威脅摘要數據，以便在調查期間增加脈絡。

主要優點

流程一致、透明且經過記錄

- 劇本驅動的回應動作與調查查詢。
- 自動記錄所有調查和歷史搜尋。
- 搜尋調查、指標和證據。
- 以精細的方式追蹤事件和分析人員指標。

量身打造的事件可視性和監控功能

- 自訂事件取得規則集和來源。
- 獨特的事件專用欄位、檢視與回應工作流程。
- 以分析人員層級追蹤任務指派和回應動作。
- 針對事件子集進行快速切換搜尋和查詢。

提高分析人員的工作效率並增強團隊學習能力

- 以視覺方式對應相關事件，快速偵測出重複項目。
- 支援即時協作與無結構性的調查。
- 以機器學習的方式，提供對於任務分析人員比對、負責者與回應動作的見解。
- 行動應用程式，可隨時隨地管理案例。

部署彈性且可擴充

- 解決方案可以使用雲端託管式部署或內部部署。
- 利用數據彙總和可擴充架構，支援完全多租戶環境。
- 引擎 Proxy 可處理區隔的網路。
- 多層設定可改善負載管理。

paloalto NETWORKS

完整的案例管理

Cortex XSOAR 的平台可管理事件生命週期的所有層面：

- 多來源警示取得，其中包含集中式事件佇列，以及針對各個攻擊類型的劇本驅動的回應。
- 直覺的拖放式劇本，可將 SOC 流程自動化，並將工作流程標準化。
- 自動記錄所有事件和調查，以進行全方位的 SLA 追蹤。
- 中央指標儲存庫，可針對指標和威脅捕捉活動進行切換搜尋。
- 行動應用程式，可隨時隨地提供個人化的儀表板、任務清單，以及可執行的事件動作。
- 跨 Windows/Mac/Linux 作業系統的一次性代理程式，可從端點收集數據。

端對端自訂

Cortex XSOAR 的彈性讓使用者可以量身打造對攻擊的回應：

- 自訂事件類型、簡化的資料分類與對應，可實現集中的警示可視性。
- 量身打造的事件流程與配置，對於每個事件類型和安全角色，都具備完整的存取控制。
- 強大的搜尋和查詢功能，可快速深入探究事件子集。
- 全方位的儀表板和可自訂的報告，可將效能與封存結果量化。

智慧型自動化與協調

Cortex XSOAR 的案例管理與跨人員、流程和技術的劇本協調緊密結合在一起：

- 與數據強化工具、威脅情報摘要、SIEM、防火牆、EDR、沙箱、鑑識工具、通訊系統等等進行數百個開放且可擴展的整合。
- 動態劇本，可透過手動任務與分析人員互動，透過郵件回應和分析與最終使用者互動。
- 建立新的劇本任務/區塊，並將其帶到整個劇本中的彈性。
- 劇本執行的即時視覺化，以進行任務管理和疑難排解。

持續學習

Cortex XSOAR 的機器學習可提高 SOC 效率，並可讓團隊隨著每次攻擊而變得更加聰明：

- ChatOps 支援的虛擬「戰情室」，分析人員可以在該處即時協作並執行安全動作。
- 相關事件調查工具套件，可提供跨時間的可自訂相關事件圖。
- 內部的安全機器人 (DBot)，可協助執行命令、建議事件負責者和任務指派。
- 可從外部安裝的聊天機器人，允許對 Slack 進行鏡像調查。
- 證據收集，並以豐富的文字標記和可反白顯示的筆記自動記錄。

CORTEX XSOAR
BY PALO ALTO NETWORKS

適用於事件管理的 Cortex Xsoar

統一的平台

可統一案例管理、安全協調、協作與威脅情報管理的完整平台

完全的自訂性

在取得來源、事件類型、事件配置、回應劇本和報告方面的彈性

持續學習

以機器學習的方式，提供對於事件負責者、分析人員任務比對和分析人員動作的見解

彈性部署

內部部署和雲端託管式部署，其中包含完全多租戶環境和三層隔離

智慧型自動化

透過劇本，結合包含數百項整合和數千個動作的自動化任務和手動任務

SLA 信賴

進行自動記錄，提供完整的 SLA 追蹤、精細的分析人員和事件指標，以及儀表板和報告

Cortex XSOAR Community Edition

若要體驗 Cortex XSOAR 的功能，請試用免費的 Community Edition。提供 30 天的企業授權，這是測試 Cortex XSOAR 的絕佳方法。註冊免費的 Community Edition

關於 Cortex XSOAR

Cortex XSOAR 是業界領先的安全協調、自動化與回應平台，可統一案例管理、自動化、即時協作和威脅情報管理，以便在整個事件生命週期中為安全團隊提供服務。藉由 Cortex XSOAR，安全團隊可以將程序標準化、自動執行可重複的任務，並管理整個安全產品堆疊中的事件，藉以縮短回應時間，並提高分析師的工作效率。如需詳細資訊，請造訪 https://www.paloaltonetworks.com/cortex/xsoar

paloalto NETWORKS