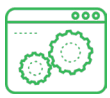
託管的安全協調、自動化與回應

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

嚴密的安全性：專屬的客戶工作負載和資源、SOC 2 認證的服務、伺服器和儲存分離



部署彈性：可選擇託管執行個體的地區、內部部署元件的引擎 (proxy) 連線，以及在複雜的架構中快速設定

高可用性：自我修復的架構、企業級的 AWS 型工作負載、引擎負載平衡

Cortex XSOAR 託管服務

技術的進步讓業務處理變得更加容易，但也為已經負擔過重的 SOC 團隊帶來了許多安全挑戰。隨著威脅面的擴大以及安全產品的增加，安全團隊會收到大量警示 (這很糟糕)，或者因為在不受監控的環境中缺乏可視性而導致發生惡意活動 (這更糟糕)。SOC 因為資源不足而進一步受到阻礙，他們無法有效地配置人員和資金來應對安全警示高峰並處理日常的安全營運和維護。

利用 **Cortex XSOAR 的託管解決方案**，安全團隊可以改善回應時間並提高效率，而不必為基礎結構、維護和儲存投入專用的資源。Cortex XSOAR 將管理和維護基礎結構和平台層，使 SOC 能夠專注於事件回應的關鍵層面。

主要優點

可靠、彈性且可擴充

- 具有高可用性的企業級自行修復 AWS 基礎結構。
- 選擇您偏好的地區以啟動及維護託管的執行個體。
- 加快安全解決方案部署，可將企業/IT 延遲降至最低。

嚴密的安全性和隱私權

- 專屬且隔離的客戶工作負載 (基礎結構、儲存)。
- 鎖定的客戶託管帳戶，與其他 Cortex XSOAR 執行個體隔離。
- SOC 2 合規性服務，伺服器與儲存分離。

降低整體持有成本

- 減少伺服器、軟體、數據中心空間以及網路設備方面的資本支出。
- Cortex XSOAR 將維護並支援整個基礎結構和平台層。

加速事件回應並將其標準化

- 透過編寫的劇本，協調安全產品的動作和流程。
- 以機器的速度自動執行可重複的步驟，同時保留的分析人員的整體控制權。
- 與您的安全團隊即時協作以進行互動式調查。
- 全面持續支援基礎結構和作業系統層級。

paloalto NETWORKS

可靠性

Cortex XSOAR 的託管服務使用結合專屬技術和尖端 AWS 功能的自我修復架構，確保使用者的高可用性。託管服務將 AWS Application Load Balancer 與 EC2 結合在一起，可確保運算要求分散在各個執行個體中，以實現最佳功能。

安全性

Cortex XSOAR 為每個客戶維護一個不同的工作負載，並不斷監控並完善可用性、資源利用率以及備份流程。客戶擁有專屬的資源，不會在任何層級 (工作負載、儲存、Docker 容器等等) 共享基礎結構。客戶託管的帳戶會被鎖定，並與其他 Cortex XSOAR 執行的執行個體分離。Cortex XSOAR 在處理託管執行個體的客戶支援時，還能保持職責分立。只有我們的 DevOps 團隊可以存取作業系統層，客戶成功團隊會在需要作業系統存取權時與 DevOps 團隊聯繫。

彈性

託管解決方案可加快設定速度並將 IT 延遲減至最少，消除企業再加快安全防護面前的障礙。Cortex XSOAR 可以在單一託管服務中支援不同層級的使用高峰，而使用者不必在不同的服務層級和需求之間進行選擇。使用者也可以選擇他們希望啟動和維護執行個體的地區。若要統一雲端和內部部署元件，使用者可以部署引擎 (Cortex XSOAR Proxy 伺服器) 來選擇將透過引擎執行的產品整合。

為什麼選擇 Cortex XSOAR

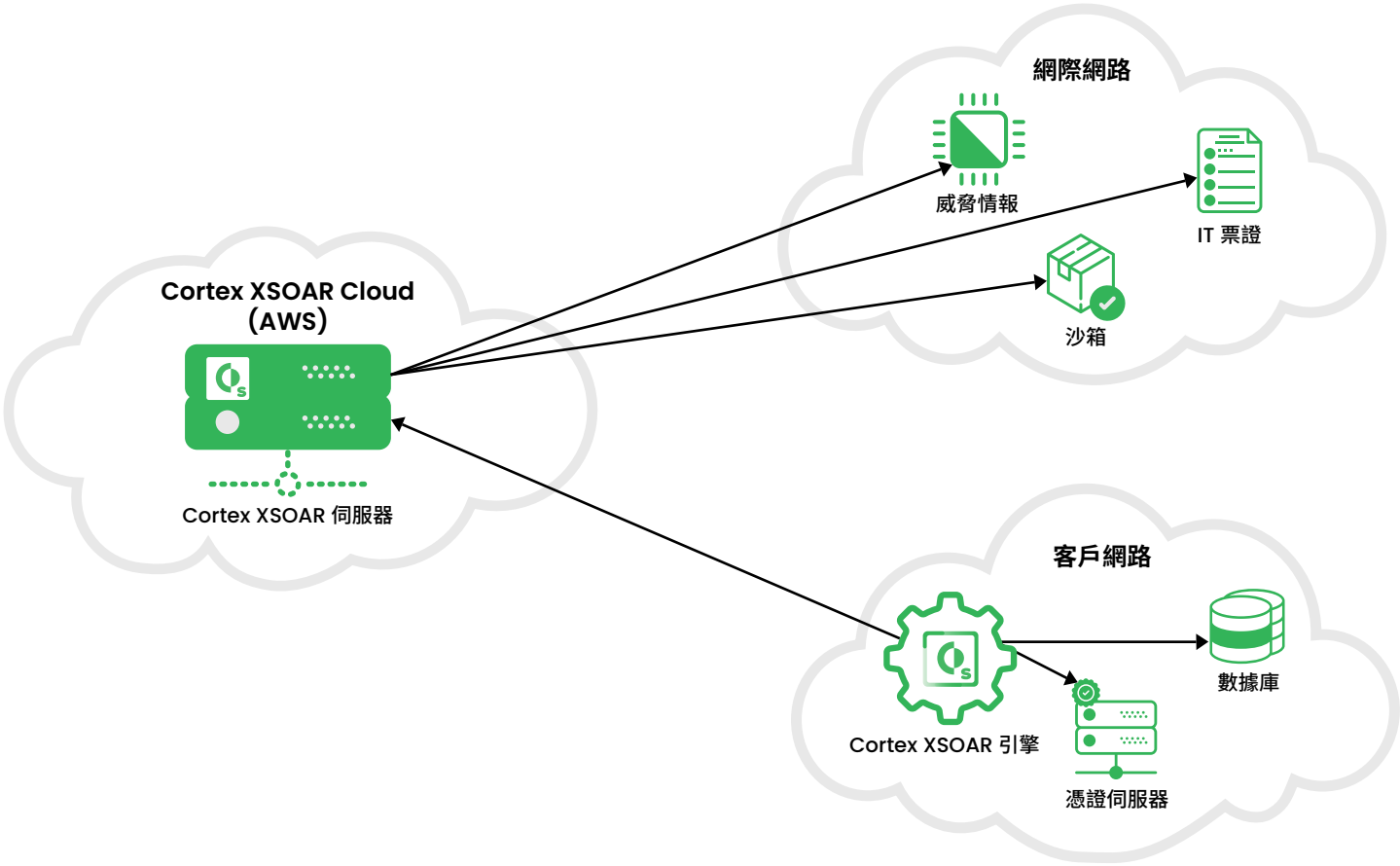
Cortex XSOAR 是一個安全協調、自動化與回應 (SOAR) 平台，可統一案例管理、自動化、即時協作和威脅情報管理，以便在整個事件生命週期中為安全團隊提供服務。

安全團隊可以使用 Cortex XSOAR，從多個來源取得警示，並啟動編寫好的，可在其安全產品之間進行協調的自動化回應流程。若要深入瞭解 Cortex XSOAR，請參閱我們的型錄。

Cortex XSOAR 引擎

Cortex XSOAR 引擎是在內部部署安裝的 Proxy 伺服器，可在不影響任何防火牆或網路限制的情況下，實現各種安全環境的統一功能。使用者可以從 Cortex XSOAR 介面下載引擎，並選擇要透過引擎部署的整合。引擎和 Cortex XSOAR 伺服器之間的所有通訊都是透過 HTTPS 進行的。

Cortex XSOAR 託管服務——架構



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