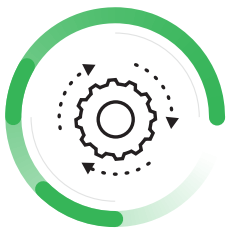
CORTEX XSOAR
BY PALO ALTO NETWORKS

重新定義安全協調和自動化

Cortex™ XSOAR 是全面的安全協調、自動化與回應 (SOAR) 平台，可整合案例管理、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。

SOAR 平台的新主幹



安全協調

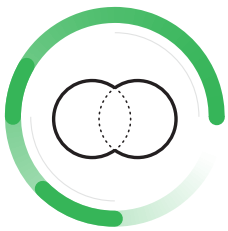
快速、大規模回應事件

- 數以百計的整合
- 數以千計的自動化動作
- 視覺劇本編輯器

案例管理

取得、搜尋和查詢所有安全警示

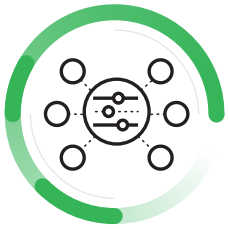
- 自訂事件配置
- 自動文件
- 儀表板和報告



合作與學習

一起合作，提高調查品質

- 虛擬戰情室
- 調查畫布
- 機器學習



威脅情報管理

剖析、管理和處理威脅情報

- 威脅摘要彙總
- 精細指標檢視
- 情報分享與回應

選擇客戶

25%
財星 500 大企業

首要
全球線上支付系統

財星
50
醫療保健組織

財星
100
運動服飾零售商

線上
串流媒體和娛樂巨擘

SOAR 生態系統

平台
370+
整合
可擴充的開放平台

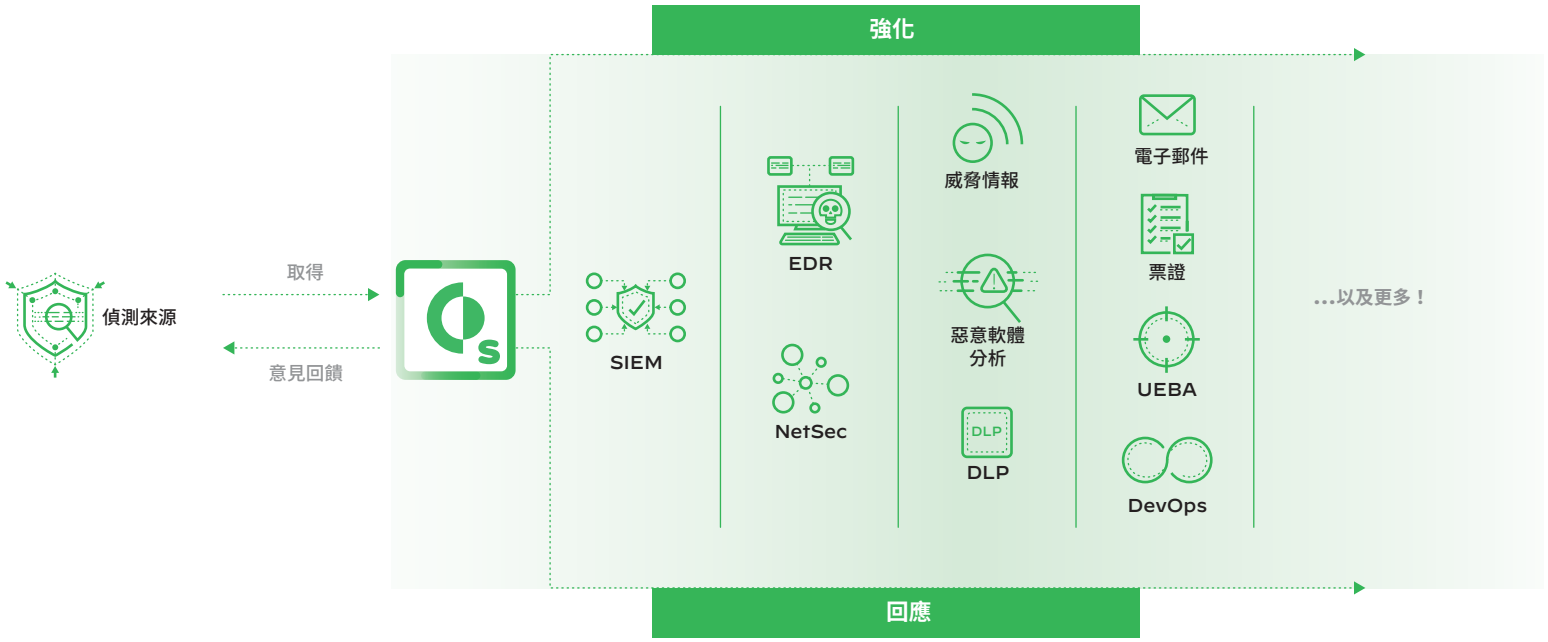
社群
13,000+
成員 (業界最大的 IR 社群)

合作夥伴
100%
通路合作
MSSP 和雲端適用

CORTEX XSOAR
BY PALO ALTO NETWORKS

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行為指標 (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。



Cortex XSOAR 如何提供協助

提高調查品質

使用協作工作區、機器學習和交互關聯

自動進行可重複的步驟

自動進行動作，將事件回應標準化並擴充

整合安全功能

在單一主控台上收集來自多個產品的情報