Cortex Xpanse 主動回應模組

使用自動化主動解決您的攻擊範圍風險
來降低安全事件的頻率和嚴重性

問題

全球攻擊範圍持續擴大和變化。[1]由於缺乏可視性、欠缺業務脈絡以及無法根據警示採取行動，安全團隊正在盡力管理持續擴大的攻擊範圍。這似乎是不可能完成的任務，不過事實並非如此。

您的關鍵 IT 基礎結構負責產生數百萬美元的營收。因此，您的安全團隊可以運用現成的自動化來解決攻擊範圍風險，而不是因應拼湊多個不同解決方案來克服這些安全障礙的挑戰。

藉由主動回應模組，您的安全團隊能夠超越攻擊範圍可視性，自動解決您的攻擊範圍暴露問題。您的團隊可以使用自動化來抵禦網路攻擊。

您的 SOC 可以部署 Cortex Xpanse 主動回應模組：

- 減少分析師花在機械式調查任務上的時間 (例如，在不同的系統中進行搜尋、提交票證等)。
- 簡化分析和後續步驟建議，藉以簡化擴展 SOC 的路徑。
- 保留透過臨時調查發現的脈絡，藉以獲得新的見解並提高未來調查的效率。
- 深入了解您的團隊以往使用哪些補救路徑來簡化補救決策。

主動回應模組

對於許多負責補救攻擊範圍風險的企業來說，持續存在的挑戰是確定未知資產的所有權和業務脈絡是極度手動且耗時的任務，可能跨越多個團隊，包括 IT、SecOps 和 DevOps。

許多企業擁有一些世界上最大規模、最複雜和極度敏感的網路，例如國防部、美國軍方的所有六個分支、衛生與公眾服務部，以及多家財星 500 大公司，為了解決其中的可視性、脈絡和補救挑戰，這些企業選擇採用 Cortex Xpanse。隨著新的主動回應模組推出，您的團隊現在可以運用 Palo Alto Networks 領先業界的自動化、協調和補救專業知識。

輕鬆展開自動化進程

企業可以使用主動回應模組輕鬆展開自動化風險降低進程。每個警示都會觸發精心設計的調查劇本，藉以為分析師強化、脈絡化並呈現所有可用的補救選項。成功補救事件之後，也會提供即時驗證。

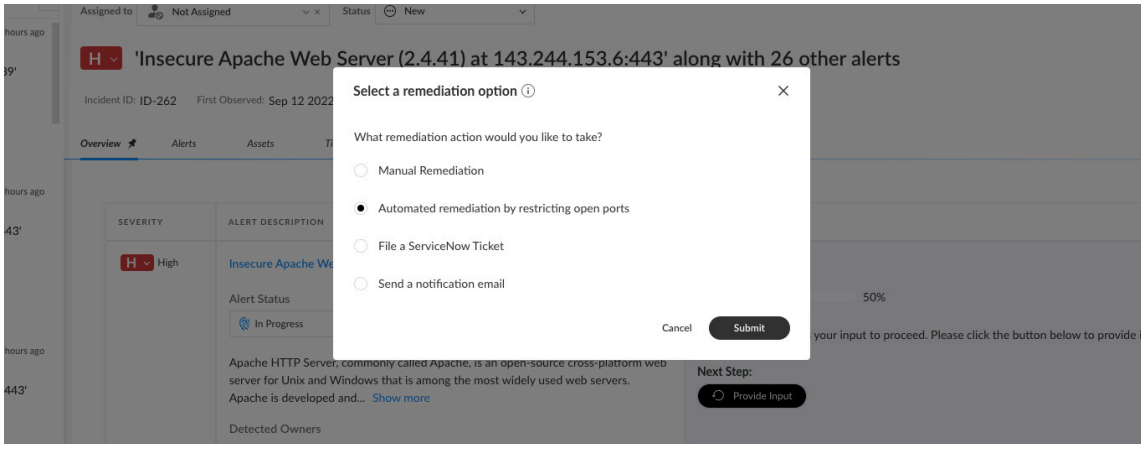

圖 1：分析師有多種選擇可用來解決攻擊範圍風險

您的分析師可以手動選擇或定義補救路徑標準，藉以指示應如何處理特定風險或一組風險，這是否表示：

- 提交具有強化脈絡和逐步補救指導的票證。
- 通知偵測到的服務擁有者。
- 透過限制開放連接埠或修改服務設定自動解決風險。
- 讓分析師透過其他方式解決。

1. *2022 年 Cortex Xpanse 攻擊範圍威脅報告*，Palo Alto Networks，2022 年 7 月 12 日。

超越單純的攻擊範圍可視性

與市場上的其他工具不同，Cortex Xpanse 的主動回應模組不僅有助於企業找到未知的風險，也可以修復這些風險。大多數企業需要三週以上的時間來掃描、尋找和修復攻擊範圍的事件，而惡意執行者會在宣佈新的關鍵 CVE 後 15 分鐘內開始尋找弱點。[2]主動回應模組透過下列方式協助弭平差距：

- 自動連接到您的所有安全和 IT 工具以收集適用的脈絡。
- 使用機器學習分析收集到的數據，為分析師提供關鍵見解。
- 透過授予選擇補救路徑的精細控制，讓安全團隊控制本身想要如何解決各種類型的風險。
- 包括內建的補救劇本，藉以消除關鍵的攻擊範圍風險，例如暴露的遠端桌面通訊協定 (RDP) 伺服器和不安全的 OpenSSH。
- 透過重新掃描資產來驗證補救是否成功。
- 透過稽核所採取的每項行動並將調查詳細資料匯總到實用的儀表板和報告中，確保您的安全團隊在控制之中。

運作方式

在自動補救劇本執行期間，Xpanse 將先收集已知的詳細資料和識別碼，並且透過可用的整合將這些與任何相關的脈絡資訊相結合，包括 Amazon Web Services (AWS) 等雲端供應商或 ServiceNow 等 IT 資產管理工具、弱點管理解決方案和其他資源。

圖 2：自動解決您的攻擊範圍風險

2. *2022 年 Cortex Xpanse 攻擊範圍威脅報告*，Palo Alto Networks。

所有這些原始資訊接著會經過分析以進行關鍵字比對，並且使用機器學習來識別關鍵脈絡，例如服務擁有者、服務是否是生產部署的一部分，以及有關數據敏感性或目的的其他任何資訊。該分析也將確定是否可以採取自動補救動作。

如果尚未啟用全自動補救，則會向分析人員顯示已收集的所有資訊的摘要，以及可以選擇的可用補救或通知選項。在 AWS EC2 執行個體上進行 RDP 自動補救的情況下，Xpanse 將運用 AWS EC2 API 修改受影響執行個體的安全群組，藉以阻止對暴露的連接埠進行的連接埠存取。

補救完成後，Xpanse 將進行輕量化連接埠掃描，立即驗證該服務無法再透過網際網路存取。最後，Xpanse 將產生所有調查結果、提供的決策和採取的行動有關的摘要，以便分析師和管理人員可以了解任務的完成情況。

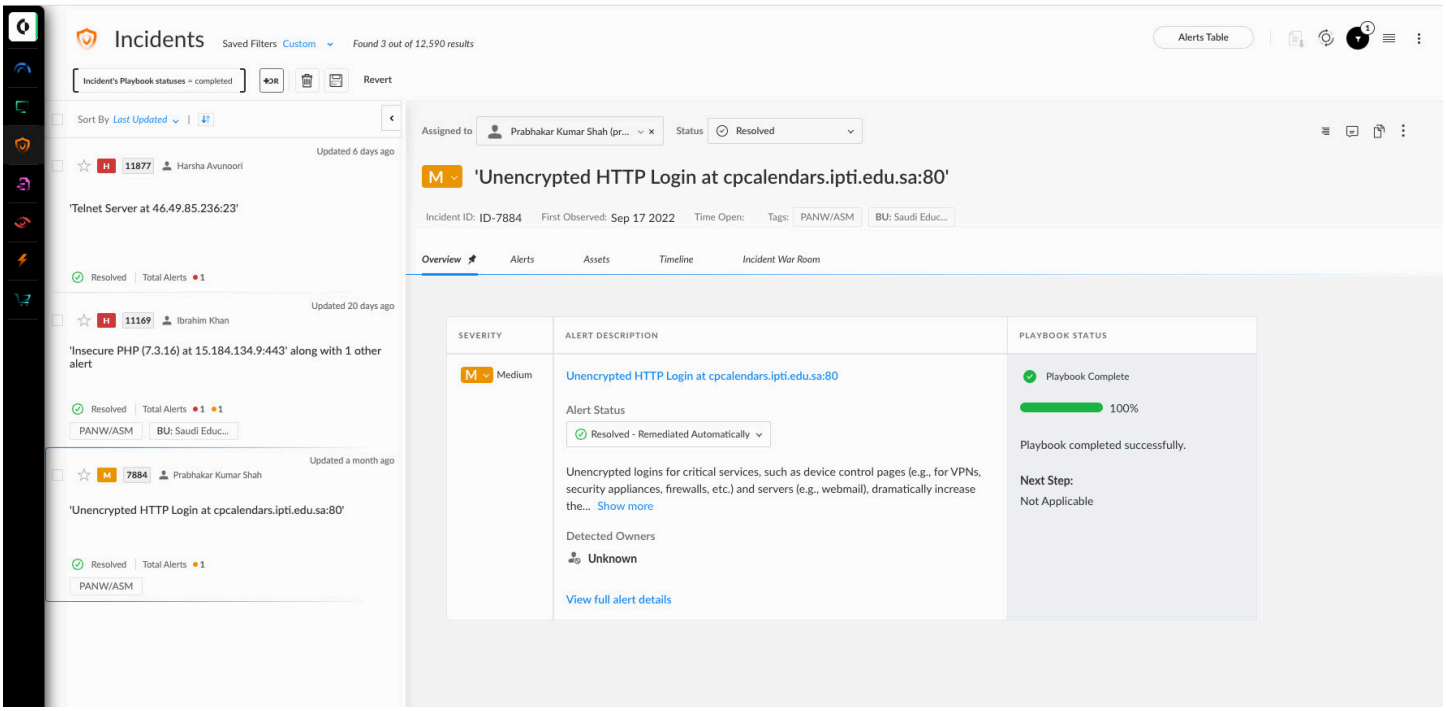

圖 3：檢視風險的自動解決進度

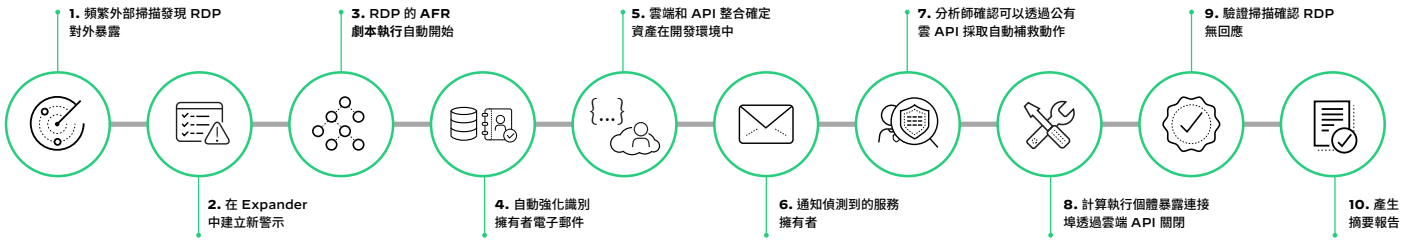

圖 4：使用主動回應模組消除雲端 RDP

主動回應模組解決的使用案例：

- 對於暴露的 RDP 執行個體移除網際網路存取，這些執行個體是勒索軟體的閘道。
- 對於不安全版本的 OpenSSH 執行個體移除網際網路存取，這可用於權限提升。

雖然近年來企業的攻擊範圍急遽增加，不過企業的安全團隊並未隨之擴充。企業需要找到有效的方法來降低風險並且了解持續增加和日益複雜的攻擊範圍。

主動回應模組進一步推動 Xpanse 的願景，協助企業主動發現風險、確定風險優先順序並自動降低風險，藉以降低安全事件的發生頻率和嚴重程度。若要深入了解，請觀看 Cortex Xpanse 示範。

主動回應模組免費試用！

在 2023 年 6 月之前，主動回應模組提供給 Cortex Xpanse Expander 客戶免費社群試用，此後將成為必須購買的附加模組，以主動降低攻擊範圍的風險。

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 號台北南山廣場 34 樓

cortex_ds_xpanse-active-response-module_121222