Cortex Xpanse：威脅回應中心

威脅回應中心可以成為您的單一控管中心來進行更有效的弱點管理，以協助您成功地防禦新興威脅。

安全團隊必須能夠在解決新弱點和暴露的同時，管理其不斷變化且分散的攻擊範圍。我們的研究顯示，幾乎有一半企業的攻擊範圍基礎結構每個月都會發生變化。

在這個不斷演變的形勢中，要識別出關鍵暴露並排定補救工作的優先順序變得極為困難。在發生例如 Log4j 和 3CXDesktopApp 等網際網路緊急狀況期間，這樣的挑戰會特別的明顯，因為這些面向公眾的暴露可能會導致入侵行動的成功率大幅提升。

當發生網際網路緊急狀況時，企業往往會將其所有資源轉移到暴露的評估上，這包括查看過時的資產目錄、手動更新的試算表和其他互不關聯的來源，但這些資訊不但不夠全面，也可能不符現況。在此同時，攻擊者會在 CVE 公告發佈後的幾分鐘內開始尋找任何可入侵的暴露。

安全團隊通常難以因應新興威脅，也無法有效掌握可能會對其網路造成影響的最新弱點。安全團隊需要集中化平台來檢閱、研究、評估及補救任何已發生的新威脅，確保其網路能夠防禦最新的 CVE。

Expander 威脅回應中心的設計可為安全團隊提供一站式服務來檢視、研究、評估及補救新的威脅。其所提供的控管中心檢視可以根據嚴重性、修補程式可用性、武器化和地緣政治等各種因素，來突顯不同的弱點。威脅回應中心能協助企業有效防禦新興威脅並保護其攻擊範圍。

使用案例

檢視新興威脅：存取經彙整的事件清單以有效掌握任何最新弱點。

研究威脅：取得詳細的弱點資訊，包括 CVSS 評分、摘要、作用中警示、入侵詳細資訊以及對應的 CVE。

評估影響：針對每個弱點分析作用中警示、受影響的業務單位以及指派的人員。

補救規劃：利用補救建議、入侵後果和其他資源來制定全面的規劃以因應各種威脅。

它如何運作？

威脅回應中心會根據如弱點嚴重性、修補程式可用性、武器化和地緣政治等因素，編譯一份與新型和新興威脅有關的彙整事件清單。然後其會將此資訊與存在於企業環境中的 CVSS 評分、摘要、作用中警示以及對應的 CVE 等詳細資訊進行結合，根據受影響的業務單位進行影響評估。

Cortex Xpanse 安全研究團隊會與其他 Palo Alto 安全研究人員合作，當新的關鍵弱點公佈時立即採取行動，以確保 Xpanse 客戶能夠儘快獲得可視性 – 在大部分的情況下都能在公佈後的幾小時內完成。

功能

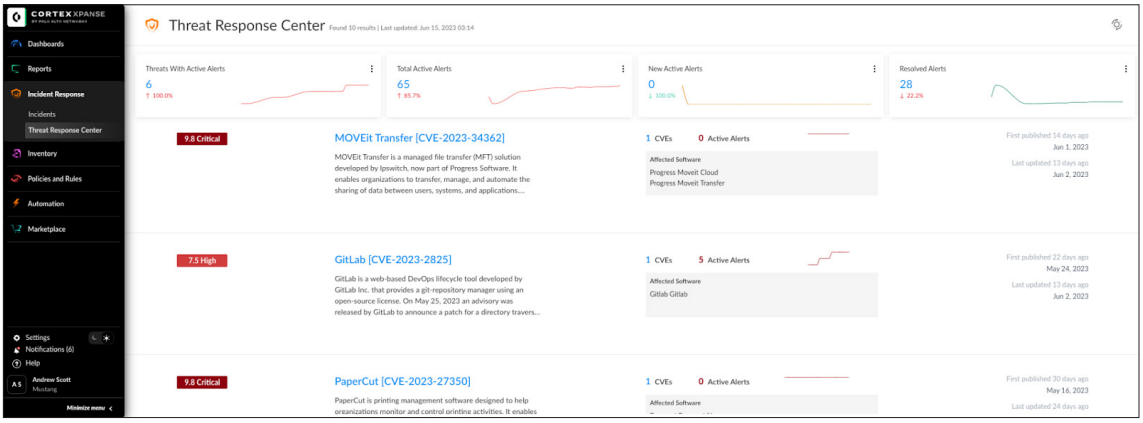

圖 1：控管中心檢視

威脅回應中心的控管中心檢視可作為一種集中化儀表板，針對會影響企業的新興威脅和弱點強調相關的關鍵資訊。控管中心檢視強調：

- **弱點嚴重性**：使用 CVSS 評分顯示每個弱點的嚴重性，協助安全團隊識別優先順序較高的威脅。
- **弱點摘要**：顯示每個弱點的簡短摘要，提供威脅的概況與其潛在影響。
- **大範圍的影響**：顯示與特定威脅有關的作用中警示數量，藉此表示弱點對於企業網路的影響程度。

- **修補程式可用性**：顯示已識別的弱點是否有可用的修補程式或更新，讓安全團隊能根據此規劃其補救策略。
- **武器化**：強調弱點是否已武器化 (例如，威脅行動者是否會在其攻擊行動中主動入侵)。
- **地緣政治因素**：考量各種地緣政治因素，例如進階持續威脅 (APT) 團體是否會使用弱點展開針對性的攻擊。

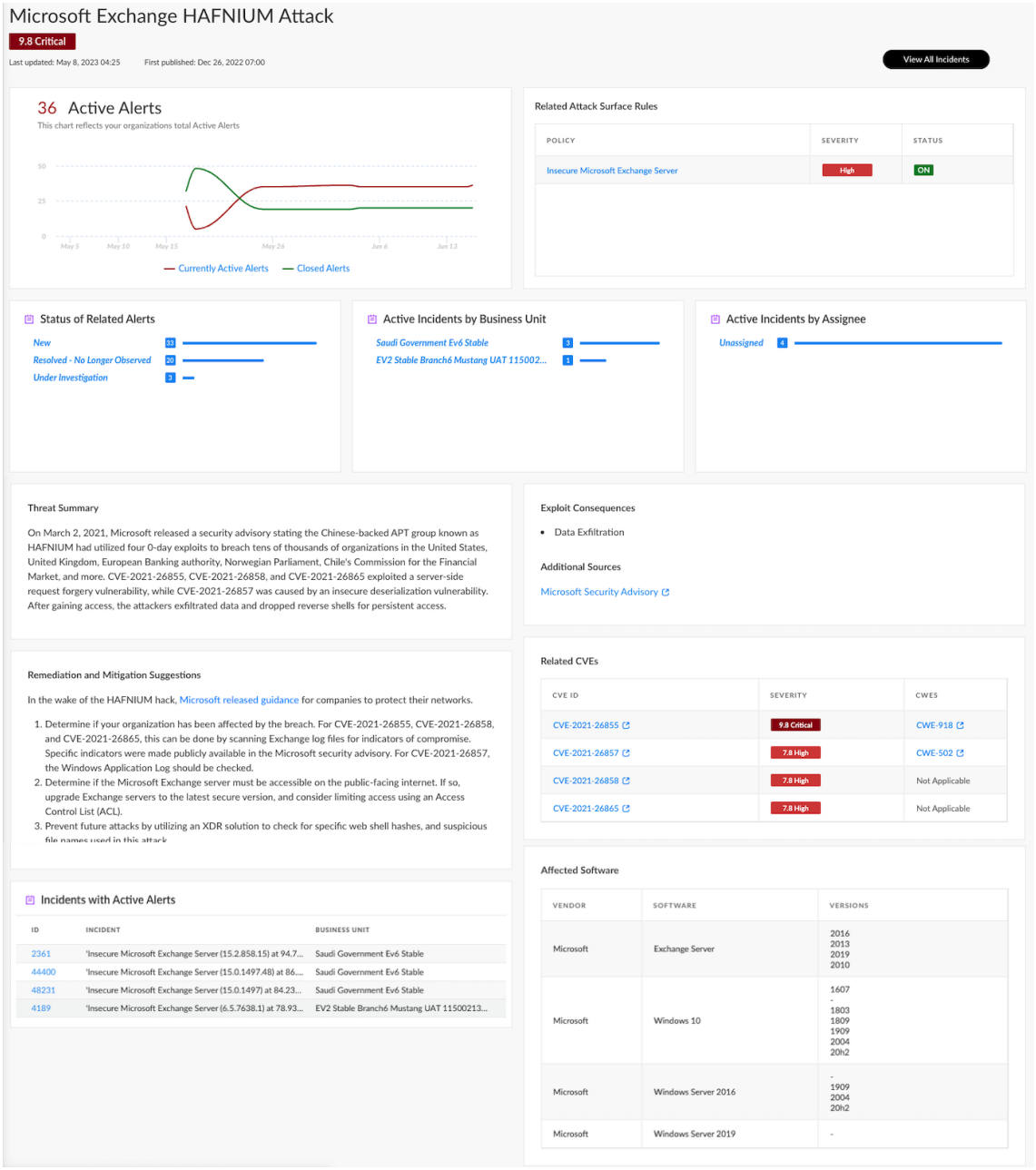

圖 2：詳細檢視

- **警示摘要**：顯示與弱點有關的作用中警示數量，並且追蹤其在某段時間的狀態，例如調查中或已解決等狀態。
- **補救進度**：顯示企業中的補救工作進度，包括已關閉事件、指派的人員，以及對於不同業務單位的影響。
- **威脅情報摘要**：提供弱點摘要、其嚴重性 (CVSS 評分) 以及與威脅有關的任何其他資訊。
- **補救和緩解建議**：針對建議的補救步驟和緩解措施提供指導方針以解決已識別的弱點。

- **入侵後果：**顯示一旦弱點遭到入侵所可能產生的潛在風險和後果。
- **其他的資訊來源：**列出外部資源與連結以收集與威脅有關的進一步資訊，讓安全團隊能研究及深入了解該弱點。
- **相關 CVE：**顯示對應至特定威脅的一般弱點和暴露 (CVE)，針對弱點形勢提供更廣泛的脈絡。
- **作用中警示：**提供與弱點有關的作用中警示連結，讓安全團隊能輕鬆地調查及解決每個事件。

威脅回應中心能協助您的團隊回答下列問題：

1. 就最近引起注意的弱點來說，我的企業是否會受到影響？
2. 目前有哪些新興威脅和弱點會影響我們的企業網路？
3. 這些新興威脅會造成哪些入侵後果和潛在風險？
4. 哪些業務單位和資產會受到這些新興威脅所影響？
5. 我們會在安全團隊中指派誰來處理與新興威脅有關的特定事件？
6. 我們應該採取哪些補救和緩解步驟來解決這些弱點？
7. 這些已識別的弱點是否有任何適用的修補程式或更新？
8. 目前我們對於每個弱點的補救工作進度為何？其成效又是如何？

在現在不斷演變的威脅形勢中，安全團隊需要強大的解決方案來解決新的弱點，並且排定不同補救工作的優先順序。Cortex Xpanse 威脅回應中心會提供單一控管中心來檢視新興威脅、研究各種弱點、進行影響評估並規劃補救。企業可利用 Cortex Xpanse 透過 Expander 提供的威脅回應中心來主動防禦各種威脅，並維護一個安全的攻擊範圍。

關於 Cortex Xpanse

Cortex® Xpanse™ 是一種主動攻擊範圍管理解決方案，可協助企業主動發現、了解和因應所有連線的系統和公開的服務中的未知風險。Xpanse 保護超過 200 家大型企業和數個政府機關。若要深入了解如何保護您的攻擊範圍，請造訪 Cortex Xpanse。

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