Unit 42 威脅情報和事件回應服務

情報導向。立即回應。

絕佳體驗

無論是因應入侵還是管理網路風險，我們都了解您面臨的挑戰。Unit 42 安全顧問來自美國政府、執法部門和全球安全公司，已成功處理一些最大規模的數據入侵事件。我們的入侵回應團隊是其中一支最忙碌的團隊，每年回應超過 1,300 起安全事件。我們的風險管理解決方案受到這種絕佳的經驗所啟發，根據我們看到日復一日影響企業的攻擊媒介，我們進行重點評估並確定建議的優先順序。我們的團隊進行數以千計的網路風險評估，並與全球各地的企業合作來識別和緩解網路威脅。

專為速度和效率而打造

我們迅速行動以協助我們的客戶。無論是透過部署進行分析或是提供重要發現，我們都會以最快速度完成所有任務。我們會在幾分鐘內啟動我們的事件回應團隊，整合從鑑識顧問到惡意軟體分析師和團隊主管所需的專業技能組合。我們迅速採取行動以遏制、調查和協調我們的回應。我們與您共同找出跡象並透過關鍵決策進行操作，便於您快速復原業務。在我們的風險管理業務中，我們意識到網路安全支出是一項投資。我們會審慎考量客戶的安全預算的重點，在降低風險的同時達到最佳的投資報酬率。我們按時、按預算交付解決方案，藉以達到最大影響。

持續創新和進階技術促進我們持續發展

在快速發展的威脅形勢下保持領先需要最好的技術和持續的創新。我們為解決客戶的網路安全挑戰而投入的研究、開發和創造力感到自豪。Palo Alto Networks 已經開發並將持續發展一套提供技術支援而且功能相當強大的威脅防禦、偵測和事件回應解決方案。我們整合雲端原生運算和機器學習人工智慧，因此我們的團隊能夠在幾分鐘內，而不是幾天或幾週內，在全球和企業範圍內進行回應。我們的產品有助於 Unit 42 加速部署、以更智慧化的方式進行捕捉、更深入調查並完全遏制。

如需詳細資訊，請造訪 www.paloaltonetworks.com/unit42。

15

平均經驗年數

1,000+

2021 年事項

24/7/365

事件回應

Unit 42 威脅情報和事件回應服務

事件回應

事件回應

BEC 調查

回應企業電子郵件環境遭到未獲授權而進入的情況並從中復原。遏制事件並且確定根本原因、入侵時間和攻擊者活動，然後量化暴露的敏感資訊。

勒索軟體調查

回應勒索軟體攻擊並從中復原。遏制威脅並且確定根本原因、入侵時間和攻擊者活動，然後量化暴露的敏感資訊。如果需要，與威脅行動者協商，取得並驗證解密金鑰，並且制定和實施復原計劃。

雲端事件回應

回應經由雲端發動的攻擊並從中復原。遏制威脅事件。確定初始攻擊途徑、未獲授權存取和外洩的範圍，並確定需要補救的系統範圍。確定並實施其他的防護措施。

Web 應用程式入侵

回應 Web 應用程式攻擊並從中復原。遏制威脅、分析日誌、檢閱程式碼、量化敏感資訊的暴露或遺失，並獲得設計強化對策的建議。

進階持續性威脅 (APT) 調查

回應疑似 APT 事件並從中復原。遏制威脅並且確定根本原因、入侵時間和攻擊者活動，然後量化暴露的敏感資訊。

PCI 調查

回應信用卡數據洩露並從中復原。認識 PFI 程序。遏制威脅並且確定根本原因、入侵時間和攻擊者活動，然後量化暴露的 PCI 資訊。

惡意軟體分析

使用開放原始碼情報、沙箱、反向工程和報告交付來分析惡意軟體樣本，包括惡意軟體的行為和功能。

數據採礦

識別和量化因數據洩露而面臨風險的敏感數據，以便做出通知決策，包括 PHI、PII、PCI 以及其他敏感和受監管的資訊。

網路風險管理

策略諮詢

董事會和資訊安全長諮詢

進行評估和審查以識別網路風險、確立目前狀態概況，並訂定安全策略向高階主管和董事會報告。

併購和收購網路盡職調查

評估人員、程序和技術以識別潛在的紅色旗標、突顯隱藏的網路安全風險，並在併購或收購的背景下獲得對整體資訊安全計劃成熟度的獨立評估。

網路風險評估

基於架構或受監管 (NIST、CIS、ISO、CCPA、HIPAA 等) 的網路安全風險評估，藉以確定控制實施的現狀和落差，並為未來狀態增強的 InfoSec 計劃開發策略計劃。

主動式評估

入侵評估

尋找歷史或目前的入侵指標，藉以識別未獲授權的存取或活動 (跨越雲端、電子郵件、端點) 曾經進行的證據。

安全作業中心 (SOC) 評估

設計和建立新世代 SOC 的設計和諮詢服務。

雲端安全評估

評估目前的雲端運算或服務工作負載控制、安全設定和政策，藉以識別網路安全風險。

供應鏈風險評估

評定和評估基於廠商的供應鏈網路安全風險，藉以識別和減輕供應鏈攻擊的威脅。

BEC 整備評估

有針對性的網路安全風險評估著重於防禦 BEC 和其他基於電子郵件的攻擊所需的控制以及人員、程序和技術。

勒索軟體整備評估

開發控制增強功能、補救建議和最佳實務劇本，藉以達到勒索軟體整備的目標狀態。

事件模擬

桌面演習

使用基於產業特定威脅和實際入侵的自訂情境，與主要相關各方一起模擬您對嚴重數據安全事件的回應。

紫隊演習

透過與 Unit 42 協同作業來確定警示落差、調整防禦並增強安全作業實務，藉此強化您的安全計劃。

Unit 42 威脅情報和事件回應服務 (續)

事件回應

數位鑑識

數位調查

對於從數位媒體收集的資訊，使用科學方法進行鑑識收集、分析、復原和報告，藉以確定該媒體上發生什麼情況或該媒體如何遭到利用。

內部威脅和離職員工調查

對於授予其他忠誠員工的權限遭到濫用的情況進行調查，包括識別存取或濫用的數據和/或內部人員採取的非必要動作。

結構化數據調查

收集和分析 SQL 和 NoSQL 數據庫環境，包括外部日誌。

專家證人/證詞/訴訟支援

審查數位證據和探索，並在報告、陳訴、證詞或公開法庭證言中向事實審理者提供專家意見。

網路風險管理

滲透測試

透過應用威脅行動者用來獲得未獲授權的存取並在遭入侵的環境中取得立足點的策略、技術和程序，對企業的技術控制和網路安全進行壓力測試。

入侵整備審查

評估有效因應威脅所需的人員、程序和技術，以及策略路線圖，藉以達到入侵整備的目標狀態。

安全諮詢和威脅情報

安全程式設計

為您的 InfoSec 計劃設計監管架構、營運模型和路線圖，包括政策和標準、控制架構和深層防禦政策。

虛擬資訊安全長

臨時或兼任資訊安全長，負責識別網路風險並開發和改善您的 InfoSec 計劃。虛擬資訊安全長將訂定網路安全策略，並與 IT、安全和執行團隊合作，回答有關公司安全狀況的問題。

事件回應計劃開發

評估和諮詢服務著重於您的團隊是否準備好防禦、偵測、回應勒索軟體攻擊並從中復原。

專家威脅簡介

這份策略威脅簡介提供 Unit 42 分析師依據端點、網路和雲端的數據深度和廣度自訂的威脅形勢檢視。

Unit 42 聘用團隊

當企業面臨嚴重的網路事件時，您是否已經做好準備？您的回應速度，以及工具和劇本的有效性，將決定您復原的速度。透過快速撥號聯絡世界級 Unit 42 事件回應和網路風險管理團隊，藉此擴展團隊的能力。

從涉及惡意內部人員的案例到有組織的犯罪集團和國家威脅，Unit 42 每年進行 1,000 多次事件回應調查。Unit 42 聘用團隊在您最需要的時候透過預先確定的服務層級協定 (SLA) 為您提供深入的鑑識和回應專業知識。

您也可以為合約期間的主動 Unit 42 網路風險管理服務分配您的聘用團隊時間。我們值得信賴的顧問可以協助您的團隊制定安全策略、進行技術控制評估和達到整體計劃成熟度。

關於 Unit 42

Palo Alto Networks Unit 42™ 匯聚世界知名的威脅研究人員，成立一支由事件回應人員和安全顧問組成的精英團隊，成為情報導向、立即回應的企業，誠摯協助客戶主動管理網路風險。藉由提供領先業界的威脅情報所累積的深厚聲譽，Unit 42 擴大了服務範圍，可提供最進階的事件回應和網路風險管理服務。我們的顧問將成為您值得信賴的顧問來評估和測試您的安全控制措施以因應正確的威脅、透過威脅知情的方法轉變您的安全策略，並在創紀錄的時間內回應事件。請造訪 paloaltonetworks.com/unit42。

獲得網路安全保險計劃認可

Unit 42 名列 70 多家主要網路安全保險公司的認可廠商名單。如果您需要使用與網路保險索賠相關的 Unit 42 服務，Unit 42 可以允諾與保險公司簽訂的任何適用首選名單費率。關於適用的名單費率，只需要在請求服務時通知 Unit 42 即可得知。

遭到攻擊？

如果您認為自己可能遭到入侵或發生緊急事態，請聯絡 Unit 42 事件回應團隊。

- 在 start.paloaltonetworks.com/contact-unit42.html 填寫表單。
- 撥打北美洲免費電話：866.486.4842 (866.4.UNIT42)，歐洲、中東和非洲：+31.20.299.3130，英國：+44.20.3743.3660，亞太地區：+65.6983.8730，或日本：+81.50.1790.0200。
- 傳送電子郵件至 unit42-investigations@paloaltonetworks.com。

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

unit42_ds_threat-intel-incident-response-services_012423