網路安全檢查清單

# 主動因應威脅的 57 個提示

## 保護企業的安全是長遠的旅程，而不是最後的終點

您可以決定將防禦措施的重點放在哪裡。可能無法防止入侵，不過可以在入侵發生之前做好充分準備。藉由立即採取動作，您可以確保企業不會輕易成為威脅行動者的目標，而且您可以透過限制攻擊者在您的網路中傳播的能力來盡可能減少網路攻擊事件造成的損害。您需要提前確定企業必須採取哪些措施來消除威脅、恢復正常營運及復原。

下列建議是以即時事件回應案例為依據，並從我們的2022年Unit 42事件回應報告總結而得。這些建議分為多個部分，有助於您集中精力並提高安全計劃的彈性。

## 確保企業安全性的全面建議

### 身分和存取管理 (IAM)

- 儘可能針對 Web 應用程式和多因素驗證 (MFA) 使用單一登入 (SSO) 平台。
- 定期檢視 Active Directory 中新建立的帳戶、信箱和無法識別的群組政策物件。
- 設定伺服器以防止未獲授權的存取和目錄清單。實施強大的存取控制。
- 如果員工被解僱，迅速採取動作撤銷員工的存取權限 (例如，進行中工作階段、權杖、帳戶、MFA 裝置和輪換憑證)，然後驗證存取權限是否已經予以撤銷。確保您保留員工的系統和數據，以備需要調查時使用。
- 將授權帳戶的使用侷限於存在有效業務需求或使用者需要授權帳戶來完成工作任務，而且不要重複使用本機管理員帳戶密碼的情況。
- 針對工作角色不需要管理介面和偵錯工具的任何人停用其訪問。

**七個最常遭受攻擊的產業**是金融、專業和法律服務、製造、醫療、高科技，以及批發和零售。

## 風險、弱點和修補管理

- 確定對於企業最有價值的關鍵資產。這應該包括對關鍵資產進行清點，藉以了解您的最高價值目標在哪裡以及這些目標是否需要任何額外的防護。
- 在實施開放原始碼時，研究開放原始碼以了解是否有任何已發佈的弱點；僅使用經過審查和修補的開放原始碼。
- 對所有面向公開環境的基礎結構進行定期 Web 應用程式/程式碼審查和年度滲透測試，藉以尋找弱點；遵循補救建議。
- 根據最佳實務在您的開發環境中設定安全設定。
- 執行包括設定檢查在內的定期掃描，並且執行定期系統稽核以偵測錯誤設定。
- 實施變更控制通訊協定，要求審查和簽署設定變更。
- 修補管理對於作業系統和內部部署應用程式極為重要；APT 行動者會伺機快速利用弱點。在盡職調查允許的情況下儘快解決新發佈的弱點。

## 數據和軟體安全性

- 了解敏感數據的位置並實施強大的存取控制以保護該數據；定期監控和稽核存取。將敏感數據的存取權限侷限於有需要的企業內部人員和第三方。
- 為筆記型電腦和卸除式裝置實施完整磁碟加密。制定應變計劃以停用遺失或遭竊的裝置。
- 實施和運用能夠定位和/或遠端抹除裝置的行動裝置管理應用程式。
- 建立 DLP 計劃，負責對數據進行分類和標記，並在敏感資訊或其他公司識別的相關資訊離開企業時發出警示。

## 威脅偵測與回應

- 考慮使用憑證入侵偵測服務和/或攻擊範圍管理解決方案來協助追蹤易受攻擊的系統和潛在的入侵。
- 運用 EDR 或 XDR 解決方案，並且確保您的安全作業團隊了解如何運用該技術來保持整個網路的完整可視性。
- 制定事件回應和補救計劃。即使盡最大努力，事件仍可能發生，因此必須訂定經過測試的綜合計劃，藉以確保在事件發生時迅速採取動作。如果您有網路保險 (建議)，請務必將保單的關鍵程序和聯絡人整合到計劃中。

## 其他提示

- 維護日誌儲存庫並定期檢查所有日誌和登入嘗試是否有異常行為模式。確保日誌儲存長達適當的時間以履行任何法律或監管義務。Unit 42 顧問建議儲存一年或更長時間，如果不可能，則至少 90 天。

- 運用日誌彙總系統，例如安全資訊和事件管理 (SIEM) 系統，藉以增加日誌保留、完整性和可用性。
- 每年對包括承包商在內的所有使用者進行定期安全意識訓練。考慮使用值得信賴的訓練平台，該平台允許您將自訂目標納入訓練課程。
- 避免使用扁平式網路。隔離網路和 Active Directory、區隔敏感數據，並且運用安全的虛擬區域網路 (VLAN)。
- 遵循深層防禦方法，在 Web 應用程式堆疊的每一層實施保護措施。這可能包括 Web 應用程式防火牆、作業系統強化、應用程式輸入控制、檔案完整性監控，以及用於數據庫存取和產業標準加密的最低權限使用者帳戶。
- 為員工提供合法展開業務的途徑；單純阻止某些途徑會導致您可能錯過創造性解決方法。
- 考量根據常見的拼寫錯誤或企業名稱的變體來購買網域名稱。威脅行動者將因此更難冒充您的企業。

**77% 的入侵**疑似是由三個初始存取途徑所引起：網路釣魚、利用已知軟體弱點所進行的入侵，以及暴力破解憑證攻擊 — 主要集中於遠端桌面通訊協定。

## 防止網路釣魚攻擊的建議

- ☐ 營造「安全意識文化」。公司領導階層必須體認到網路安全性和支援的重要性、推廣更豐富的網路訓練計劃，並且強調公司通訊的安全性。
- ☐ 運用受信任的訓練廠商或平台，為企業和員工角色設計課程，並考量威脅行動者方法的快速發展性質。
- ☐ 方便使用者檢舉疑似網路釣魚電子郵件；確保適時審查報告並對此類訊息採取動作。
- ☐ 以視覺方式提醒使用者注意外部寄件者的附件。這可能有助於識別與公司網域類似的詐騙網域。
- ☐ 展開全面的訓練，涵蓋並超越網路釣魚和魚叉式網路釣魚。涵蓋涉及實體安全的其他社交工程問題、防止裝置遺失的業界最佳實務、內部威脅指標等等。
- ☐ 為各個群組量身打造 Web 型模組，這些模組與其角色以及他們可能成為的特定目標相關，以便員工可以更確實發現和避免可能針對他們使用的策略。
- ☐ 每年對所有員工進行全面訓練，並在年中對特定重點領域 (例如進階技術) 進行「更新」。
- ☐ 透過設定目標、達成目標的規則、獎勵或激勵、回饋機制和排行榜，將安全訓練遊戲化，以便更確實吸引員工。企業可以相互競爭。
- ☐ 追蹤網路釣魚測試的領先效能指標，以便您可以根據企業的需要調整網路釣魚的內容和難度。
- ☐ 鼓勵使用者透過以角色為基礎的存取控制進行的檔案共享而不是電子郵件來儲存敏感資訊。

- ☐ 運用掃描附件和訊息內容以及評估寄件者信譽的電子郵件安全解決方案。
- ☐ 使用反詐騙和電子郵件驗證技術，例如寄件者政策架構 (SPF)。
- ☐ 如果正常業務營運不需要，請考慮根據地理區域阻止帳戶登入。
- ☐ 採用進階網路釣魚防護/機器學習解決方案或其他第三方解決方案來偵測和阻止複雜的網路釣魚活動。考慮採取網路釣魚回應活動自動化以減少所需的人為介入。

## 有助於企業保持最新版系統的修補建議

- ☐ 透過自動探索工具清點整個分散式企業中的所有 IT 資產 (包括儲存、交換器、筆記型電腦等)，藉以釐清您必須管理的內容。
- ☐ 優先考量您的修補需求。根據企業風險承受能力，確定哪些弱點是高、中或低風險以及這些風險對於業務而言的優先順序。
- ☐ 訂定定期部署修補程式的排程。考量每月一次的最低頻率，而且可以選擇在必要時不按照週期部署高優先順序修補程式。
- ☐ 在開發 QA 環境中測試您的修補程式，藉以確保這些修補程式在部署到生產環境後不會「破壞系統」。
- ☐ 部署修補程式後，監控這些修補程式的穩定性。這可能也包括監控網路的穩定性。
- ☐ 移除在不再受支援的作業系統上執行的系統。

**65% 的已知雲端安全事件**起因於錯誤設定。

## 保護雲端環境的建議

- ☐ 定期評估在面向公眾網際網路上可以存取或公開哪些數據。
- ☐ 考慮採用攻擊範圍管理解決方案來協助追蹤易受攻擊的系統和未受管理的雲端資產。
- ☐ 運用每個平台的雲端安全專業知識。管理雲端中的安全性需要滿足每個平台細微差別的專業知識。平台愈複雜，不慎洩露數據的錯誤機會愈多。
- ☐ 確保具有雲端控制存取權限的使用者在每個雲端環境中都經過全面訓練。
- ☐ 如果您不具備內部專業知識，或者您的雲端資產特別複雜而且持續變動，請評估您可以選擇的管理型安全服務。
- ☐ 控制對雲端環境的存取。對雲端中 CSP 控制台、API 和 CLI 等雲端控制的存取應該侷限於有需要的人。這種 RBAC 對於儘可能降低設定和其他安全錯誤的風險而言極為重要。

- ☐ 區隔管理和使用者憑證，並且將日常使用者侷限於生產環境。
- ☐ 儘可能實施允許清單，藉以進一步限制對已知和可信任端點的存取。
- ☐ 定期稽核您的雲端數據以了解您有哪些敏感數據及其所在位置。
- ☐ 加密敏感數據 (至少)、區隔敏感數據、使用 RBAC 提供存取權限，並且定期輪換金鑰。評估與雲端供應商一起維護金鑰還是在企業內部維護金鑰對您而言最適當，不過要務必擬定限制金鑰存取和風險暴露的金鑰安全政策。

## 使用 Cortex 支援安全作業

眾所週知，安全作業需要顧及人員、程序和技術的微調平衡。為此，我們想要介紹一整套專為 SOC 設計的安全解決方案。

Cortex 產品組合提供點對點的安全解決方案，有助於您提高整個安全作業的偵測和作業效率。這些技術為我們的 Palo Alto Networks SOC 和全球數以千計的 SecOps 提供支援。

**Cortex XDR** 透過跨越網路、雲端、端點和幾乎任何數據來源提供領先的端點保護和企業範圍的威脅偵測與回應，有助於企業免於遭受攻擊。專利的行為和機器學習式分析可精確查明迴避性威脅，並提供您需要的情報，以便在發生入侵之前做出回應。不要等到攻擊發生後才發現其中的關聯；在入侵發生*之前*加以防禦。

**Cortex XSOAR** 為您的 SOC 提供單一平台來管理事件和自動化工作流程，藉以盡可能提高營運效率。檢查清單中列出的任何手動和重複的程序都適合自動化。藉由針對使用者存取控制、網路釣魚回應、弱點管理、雲端安全等關鍵程序的 900 多個預建自動化套件，XSOAR 可以做為您在 SOC 中的虛擬合作夥伴，藉以加快事件回應並且減輕分析師的日常工作量。

**Cortex Xpanse** 知道您的雲端總是持續變化，並且暴露出安全漏洞。攻擊者只需要一個漏洞就可以入侵您的網路。Xpanse 持續監控您的攻擊範圍，為您提供面向網際網路的雲端資產和錯誤設定的最新清單。在攻擊者探索之前探索影子 IT。

其具備點對點的原生整合和互通性，使 SOC 團隊可以透過 Cortex 生態系統之間的持續協力以消除各種威脅循環。這三種產品也會合作監控威脅形勢並提供最強大的偵測、回應和調查功能：

- Cortex XDR 和 Xpanse 可針對網際網路攻擊範圍、端點、雲端和網路提供絕佳的可視性和偵測能力 (包括遠端工作者)。
- Cortex XDR 可以運用 XSOAR 自動進行惡意軟體調查和回應。
- Cortex Xpanse 和 XSOAR 協同運作，使用 Xpanse 資產資訊自動偵測事件並且自動補救新探索的資產。
- Cortex XSOAR 從所有 Palo Alto Networks 產品和其他數百種安全工具中獲得警示和威脅情報，藉以促進事件調查並推動自動化事件回應。

## 使用 Unit 42 MDR 全天候偵測與回應網路攻擊

Unit 42 安全專家運用本身多年保護企業的經驗來監控您的環境並找出可疑活動。我們的分析師運用 Cortex XDR 彙總來自端點、網路、雲端的安全遙測數據，識別來源並運用高真實性威脅情報和人工智慧分析來防禦、偵測與回應最進階的威脅。

Unit 42 MDR 團隊使用專屬程序、基礎結構和擴充的組合，透過加速偵測、回應和威脅捕捉來迅速阻止可能影響企業的惡意活動。

### 使用 Unit 42 聘用團隊在幾分鐘內開始進行回應

當您識別出入侵行為後立即開始計時。如果您不立即遏制入侵並確定根本原因，攻擊者將再次回到您的環境中。

藉由 Unit 42 聘用團隊，我們的專家將透過快速撥號成為您的團隊之外的延伸，可協助您更迅速做出回應，藉此盡可能減少攻擊的影響，並且更迅速恢復業務。

## 接下來呢？XSIAM 可以滿足未來需求

雖然 Cortex 產品能夠滿足可視性、防護和自動化的關鍵 SOC 要求，但是大多數企業仍然需要 SIEM 做為 SecOps 的核心元件。不過 SIEM 產品未能進行有效的集中威脅偵測與回應，導致分析師必須面對毫無止境的警示和手動流程。安全團隊需要集中平台，將多個安全功能整合並自動化到單一的基礎解決方案中，並且能夠看見企業整體的安全數據。

擴充式安全情報和自動化管理 (XSIAM) 能夠滿足這個需求，運用人工智慧驅動的自動化功能徹底改善安全成果，並實現手動 SecOps 模式的轉型。透過建構智慧數據基礎和自動化統一的 SOC 功能，XSIAM 可加快回應速度、因應威脅，並顯著簡化分析師活動。

如需 Cortex 產品套件如何提供同級最佳威脅偵測、防禦、攻擊範圍管理和安全自動化功能有關的詳細資訊，請下載我們的白皮書：

使用 Cortex 建立虛擬 SOC 平台

現在如何規劃未來的 SOC

參閱 Unit 42 2022 年事件回應報告，更深入了解現今的網路威脅形勢，以及威脅行動者偏好使用的策略。

paloalto NETWORKS

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_cybersecurity-checklist-57-tips_112222