網路安全必備指南：

如何因應現代網路威脅

數位世界已成為危險的荒野，每次點擊、下載或登入都可能觸發隱藏的網路陷阱。

當今的網路環境比以往任何時候都來得危險，勒索軟體、DDoS 攻擊、網路釣魚詐騙和備份滲透等威脅變得更先進。駭客現在還會利用 AI 巧妙突破傳統防禦措施，將以往的隨機攻擊轉為經過縝密計算的威脅，持續造成廣泛損害。

Dell 從客戶回報的事件中發現，駭客正利用 AI 發動攻擊，透過抓取社群媒體資訊來偽造有說服力的訊息，連最具網路安全意識的員工都可能受騙。這種情況相當令人擔憂。

這些案例清楚地警示，先進技術讓攻擊者能以前所未有的準確性來操弄、欺騙及滲透組織。

要在這個敵人環伺的環境中安全前進，組織必須採取全方位網路安全策略，也就是結合尖端工具、主動策略和警覺文化的生存工具包。本指南將探討這類策略的組成要素，協助組織建立韌性防禦機制，來應對當今最緊迫的網路威脅。

保護組織的關鍵：零信任架構

在現今的 AI 驅動威脅環境中，採用零信任架構不再是可有可無。攻擊者正在使用 AI 自動偵察環境及竊取認證，還會快速調整技術，導致傳統防禦措施成效減弱。零信任基於「假設入侵」的思維運作，會持續驗證每個存取要求並實施嚴格的身分驗證流程，以降低風險。

透過主動監控使用者、裝置和應用程式，零信任能降低未經授權存取和資料外洩的可能性。這是現代化的統一身分管理方法。

保持營地安全：縮小攻擊面

縮小攻擊面對於防禦 AI 驅動威脅至關重要；端點、API 和供應鏈漏洞都是經常遭利用的攻擊面。端點和 API 做為網路的進入點，經常成為部署惡意軟體或竊取敏感資料的目標。

保護這些區域需要分層防禦策略，包括強式身分驗證、傳輸中資料加密、定期漏洞測試、端點偵測與回應 (EDR) 工具、修補程式管理和裝置強化。此外，還可透過端點監控解決方案和持續威脅偵測，即時識別及阻止惡意活動。

組織必須採用主動策略來保護軟體供應鏈和開發生命週期。強制執行最小權限存取原則，可確保只有經過授權的使用者和應用程式能與關鍵系統互動；自動化威脅偵測與回應，則能在漏洞出現時快速加以處理。

跟隨經驗豐富的荒野追蹤者：主動威脅偵測與回應

AI 驅動攻擊善於利用漏洞及模仿正當行為，還會動態調整來規避安全措施，因此難以偵測。為了對抗這些複雜威脅，組織不能只是採取被動措施，而是需要進階威脅偵測系統搭配快速回應能力。透過運用 AI 和機器學習，安全團隊可以分析行為模式、偵測異常並即時回應威脅，在重大損害發生前解決問題。

有效的偵測與回應系統必須接收大量營運資料，以便發現風險並觸發自動化回應。這種威脅情報也會自我累積，進而讓系統更聰明，能夠主動識別及對抗新興敵對戰術。

在暴風雨前練習搭建庇護所：事件回應與復原

雖然預防攻擊是第一步，但組織必須抱持攻擊不可避免的心態來保護自己，以盡量降低攻擊造成的損害為目標。有效的策略應包含兩個部分：

- 完善的事件回應與復原 (IRR) 計畫。
- 以備份關鍵資料和應用程式為核心的技術措施。

事件復原計畫應顧及所有方面。由於強力攻擊很可能會癱瘓公司大部分甚至全部作業，這類計畫應涵蓋公司中每個部門面對網路事件的行動。這類計畫還應說明組織將如何與內部和外部溝通，並預先編寫溝通範本以便隨時可用。此外，必須定期更新和維護計畫。最後，計畫成效取決於演練頻率，必須確保每個人在攻擊發生時，都能依直覺立即採取行動。

從技術角度來看，組織首先應該確定最低可行公司 (MVC) 作業的樣貌：哪些系統即使採用紙本作業，也必須保持運作？維持銷售業務是否至關重要？客戶服務呢？

確定後，就應該圍繞這些層面，建立備份和復原機制。能復原已知的良好資料，不僅有助於組織快速恢復營運，還可避免不肖人士企圖挾持資料來威脅組織。此外，現代化 IR 策略必須超越傳統方法，將 AI/LLM 系統 (如聊天機器人和虛擬代理程式) 視為第一級資產，復原順序與付款系統或客戶資料相同。

要對抗進階威脅，IR 計畫必須兼顧自動化與人工檢查。務必瞭解系統全面中斷時，組織將如何運作。如果必須回到紙本作業，該怎麼辦？

人人都須參與：員工意識

員工是網路威脅的第一道防線，就像在危險荒野中前進的生存團隊一樣，每個成員在識別風險和保護資源方面都扮演關鍵角色。為了強化這道防線，組織必須制定完善的員工意識提升計畫，例如包含進階網路釣魚、深偽技術等 AI 特定威脅的攻擊模擬計畫。

最理想的計畫，是結合持續教育、開放溝通、實際模擬和共同責任文化。只要從第一線員工到高階主管，人人都瞭解傳統和 AI 驅動威脅，組織就能隨時保持警覺、充分掌握單位環境的威脅態勢。透過培養團隊合作意識並做好防護準備，組織不僅能預防不斷演進的網路風險，還能建立韌性防禦機制來對抗潛在攻擊。

對抗 AI 驅動攻擊並保持韌性的最佳實務

為了對抗 **AI** 驅動攻擊並保持韌性，組織需要主動的策略性做法。以下是 **10** 個最佳實務：

零信任架構

須透過持續驗證、嚴格存取控制和網路分段，在授予存取權前確保每個使用者和裝置都經過驗證，以阻止及圍堵快速移動的 AI 驅動攻擊。

嚴格的漏洞與修補程式管理：

自動化掃描並快速修補作業系統、韌體、應用程式、API 和第三方軟體。

強化身分識別與存取管理：

部署強大的身分驗證 (MFA、RBAC) 並強制執行強式密碼原則，以降低網路釣魚和認證填充攻擊的成功率。

偵測及監控 **AI** 驅動威脅：

以採用 AI/ML 的行為和異常偵測技術，即時捕捉細微或自動化威脅。

自動化資產探索與清點作業：

持續探索及監控所有資產，包括雲端、IoT 和影子 IT，以避免潛在暴露風險。

自動化事件回應：

根據自動化應對手冊，快速隔離、圍堵和修復威脅，將攻擊者潛伏時間降至最低。

微分段與網路存取控制：

分段並隔離網路與工作負載，防止攻擊者橫向移動並圍堵威脅。

定期實際模擬與持續改善：

進行沙盤推演、紅隊演練和網路釣魚模擬；根據結果更新 IR 計畫和偵測模型。

端點與 **API** 強化：

使用進階端點保護 (EDR/XDR) 和安全 API 閘道；強化身分驗證、速率限制、輸入驗證和加密。

不可變更的實體隔離備份和復原機制：

維護備份並防止篡改，以確保乾淨快速地復原資料。在理想情況下，應採用實體隔離並定期測試。

DELL Technologies

Dell Technologies：帶您穿越未知領域的嚮導

組織需要正確的工具和專業知識，才能防禦進階網路威脅，並預防不斷演變的風險。在現今複雜的網路安全環境中，完善的策略是保護資料、系統和聲譽的關鍵。Dell Technologies 正是這方面的理想選擇。我們提供量身打造的全方位解決方案套件，可滿足各種規模的組織需求。

從安全供應鏈、先進威脅偵測和端點保護到安全資料管理，Dell 都能為貴企業提供抵禦現代網路攻擊所需的技術。Dell 團隊具備業界領先的專業知識，會與您密切合作，制定專屬安全策略。

組織可以藉助即時監控、自動化威脅回應和零信任架構等 Dell 功能，確保能隨時主動應對威脅並維持韌性。

無論是應對勒索軟體、網路釣魚攻擊或法規遵循要求，Dell Technologies 都能協助您在現今的威脅環境中自信前進。與 Dell 共同保護企業，在數位時代下蓬勃發展，確保以安全高效的方式營運，為未來任何挑戰做好準備。

> 事件回應計畫必須有紙本可供參考，因為在攻擊期間系統可能無法存取。”
>
> ***Rachel Tyler***
> *Dell Services* 網路安全諮詢顧問

能夠協助的 Dell 產品和解決方案

精選 **Dell** 解決方案	說明
Dell Trusted Infrastructure	結合 Dell 伺服器、網路、儲存和網路韌性解決方案，打造現代化、安全、有韌性的創新基礎。
網路韌性	專為保護資料及確實安全復原而設計的全方位解決方案組合，包括設備、軟體和服務型產品。
網路安全服務	一套服務組合，可協助您跨工作負載開發並導入全方位安全策略。服務內容包括諮詢服務、vCISO、Managed Detection and Response、滲透與弱點測試，以及事件因應與復原。
Dell Trusted Workspace (端點安全性)	一套內建和選用附加功能組合，專為保護商用 PC 而設計。根據安全供應鏈實務建構而成，內建功能包括 SafeBIOS 和具備 TPM 的 SafeID。選用附加功能包括 SecureD 元件驗證、具備 ControlVault 的 SafeID，以及合作夥伴軟體 CrowdStrike 和 Absolute，可最大化工作空間安全性。

造訪 dell.com/cybersecuritymonth，瞭解如何解決當今一些主要的網路安全挑戰