互動式網路安全性情境電子書

真實情境。更明智的決策。更強大的防禦。

Dell 對安全性的承諾是我們所有工作的核心。透過分享深入解析、最佳實務與創新技術，本電子書旨在賦予您所需的工具與知識，以領先新興的網路風險。

選擇攻擊情境

網路安全威脅不斷演變，組織需要有效回應以保護其資料。為了讓您的組織做好最佳準備，請讓自己沉浸到真實世界的模擬演練中，盡情瀏覽網路安全策略，以對抗網路攻擊。

探索各種攻擊類型與產業特定挑戰，涵蓋聯邦、州與地方政府、金融服務業與醫療保健業等領域。在過程中，您將發現 Dell 的整合式安全解決方案 (從筆記型電腦與桌上型電腦到企業系統) 如何建構以防護這些威脅。

- 備份滲透 →
- 勒索軟體 →
- 分散式阻斷服務攻擊 (DDoS) →
- 供應鏈硬體 →
- 惡意內部人員 →
- 供應鏈軟體 →
- 中間人攻擊 (MITM) →
- 零時差 →
- 提示/SQL 注入 →

攻擊類型：備份滲透

身為雲端備份服務供應商的管理員，某天晚上您接到一通客戶來電，他們正在嘗試還原一些遺失的資料。

他們已經多次嘗試從您的雲端復原，但復原總是失敗。

您前往辦公室，發現所有電腦螢幕都顯示全部資料已加密，而且要重新取得資料存取權，您需要支付贖金。

測試您的知識 →

攻擊類型：備份滲透

1：縮小攻擊面 2 3 4

您不確定哪些備份系統或客戶受到影響。您的第一步應該是什麼？

- [ ] 通知主管機關
- [ ] 關閉所有系統
- [ ] 嘗試圍堵並隔離威脅
- [ ] 識別您是否有乾淨的備份可供還原

查看正確答案 →

攻擊類型：備份滲透

1：縮小攻擊面 — 2 — 3 — 4

您不確定哪些備份系統或客戶受到影響。您的第一步應該是什麼？

- ✗ 通知主管機關
- ✗ 關閉所有系統
- ✓ 嘗試圍堵並隔離威脅
- ✗ 識別您是否有乾淨的備份可供還原

立即圍堵並隔離威脅可防止進一步擴散或損害，並爭取時間來評估事件範圍，有可能將所有類型的網路攻擊 (包括涉及 AI 的攻擊) 影響降至最低。

下一個問題 →

攻擊類型：備份滲透

1 — 2：偵測及因應網路威脅 — 3 — 4

您的優先事項是讓客戶的資料快速可用。如何達成此目標？

- [ ] 支付贖金
- [ ] 識別勒索軟體類型
- [ ] 通知主管機關
- [ ] 識別哪些資料已遭入侵

查看正確答案 →

攻擊類型：備份滲透

1 — 2：偵測及因應網路威脅 — 3 — 4

您的優先事項是讓客戶的資料快速可用。如何達成此目標？

- ✗ 支付贖金
- ✗ 識別勒索軟體類型
- ✗ 通知主管機關
- ✓ 識別哪些資料已遭入侵

識別遭入侵的資料有助於將復原工作集中在還原最關鍵的客戶資訊上，以利加速資料的可用性，並避免在未受影響的系統上進行不必要的工作。

下一個問題 →

攻擊類型：備份滲透

1 — 2 — 3：從網路攻擊中復原 — 4

您識別出有可供復原的備份。流程中的第一步應該是什麼？

- [ ] 優先還原關鍵系統
- [ ] 使用鑑識分析來確認攻擊已完全圍堵
- [ ] 變更所有密碼並撤銷遭入侵的認證
- [ ] 實施零信任原則

查看正確答案 →

攻擊類型：備份滲透

1 — 2 — 3：從網路攻擊中復原 — 4

您識別出有可供復原的備份。流程中的第一步應該是什麼？

- ✗ 優先還原關鍵系統
- ✓ 使用鑑識分析來確認攻擊已完全圍堵
- ✗ 變更所有密碼並撤銷遭入侵的認證
- ✗ 實施零信任原則

在還原系統之前，您需要確保攻擊已完全圍堵，以協助防止意外重複感染與進一步損害，避免威脅在您的環境中延續或升級。

下一個問題 →

攻擊類型：備份滲透

1 2 3 4：整體最佳實務

有哪些潛在方法可以降低未來發生此情況的風險？

- [ ] 啟用零信任原則
- [ ] 啟用端點偵測與回應 (EDR) 功能
- [ ] 實施不可變的實體隔離備份
- [ ] 以上皆是

查看正確答案 →

攻擊類型：備份滲透

1 2 3 4：整體最佳實務

有哪些潛在方法可以降低未來發生此情況的風險？

- [x] 啟用零信任原則
- [x] 啟用端點偵測與回應 (EDR) 功能
- [x] 實施不可變的實體隔離備份
- [x] 以上皆是

使用多層防禦策略可以降低風險、將損害降至最低，並增強組織韌性，因為沒有任何單一措施本身是足夠的。

查看解決方案 →

攻擊類型：備份滲透

重點回顧

當網路犯罪分子利用備份系統中的漏洞入侵、損壞或加密重要復原資料時，即發生備份滲透。這些複雜的攻擊可能與勒索軟體或惡意軟體部署等其他事件同時發生或緊接著發生，進而擴大對營運和財務的負面影響。

在 Dell，我們相信賦予組織能力，在面對不斷演變的網路威脅時保持韌性。透過我們的尖端解決方案、專業服務與值得信賴的合作夥伴關係，我們在此協助您保護最重要的事物。

深入瞭解我們的解決方案，以及我們如何應對當今最嚴峻的網路挑戰。

探索備份滲透摘要 →

返回情境

PowerProtect 產品組合 ›

我們不可變的、實體隔離及加密備份存放庫，由 AI 驅動的 CyberSense 分析提供支援，確保快速偵測與復原，讓您能夠保持韌性。

PowerEdge 伺服器 ›

透過安全開機、硬體信任根與系統鎖定，Dell 提供您可以信賴的基礎結構來保護您的備份。

受信任的工作空間 ›

SafeBIOS 與 SafeData 保護可降低風險，確保您的備份系統保持未遭竄改，並在您需要時隨時提供。

安全性與復原能力服務 ›

從安全部署到主動事件回應，我們的專家與合作夥伴可協助您建立韌性並更快復原。

網路解決方案 ›

透過網路區隔、多重因素驗證 (MFA) 與最低權限組態，Dell 協助您鎖定存取並保護您的關鍵資料。

攻擊類型：分散式阻斷服務攻擊 (DDoS)

現在是星期二下午，一個州政府機構即將面臨一場風暴。

交通部的 IT 團隊接到大量來自服務人員的電話，他們無法進入任何系統來處理：

- 更新駕照
- 取得道路許可證
- 繳納稅款
- 查看道路狀況
- 啟動緊急應變系統，導致道路清潔人員無法清除積雪/結冰的道路

這一切都是因為他們的系統逾時。

測試您的知識 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1：縮小攻擊面 2 3 4

首先應該在哪裡尋找到底發生了什麼？

- [ ] 檢查網路裝置是否有突然、無法解釋的入站流量激增
- [ ] 檢查網路裝置是否有來自單一或有限數量 IP 位址的異常流量
- [ ] 檢查防火牆或網路可見度工具記錄檔，尋找過多的連線失敗或流量封鎖事件
- [ ] 以上皆是

查看正確答案 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1：縮小攻擊面 — 2 — 3 — 4

首先應該在哪裡尋找到底發生了什麼？

- [x] 檢查網路裝置是否有突然、無法解釋的入站流量激增
- [x] 檢查網路裝置是否有來自單一或有限數量 IP 位址的異常流量
- [x] 檢查防火牆或網路可見度工具記錄檔，尋找過多的連線失敗或流量封鎖事件
- [x] 以上皆是

為了正確診斷大範圍的系統中斷，您需要同時檢閱網路裝置活動與防火牆或可見度工具記錄檔，以快速發現異常模式或封鎖事件。這能實現更快速、更準確的事件回應，因為您可以區分網路事件與基礎結構問題。

下一個問題 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 — 2：偵測及因應網路威脅 — 3 — 4

您懷疑這可能是 DDoS 攻擊。您的第一步是什麼？

- [ ] 透過 DDoS 緩解服務重新導向所有網路流量
- [ ] 啟用 Web 應用程式防火牆 (WAF) 規則以篩選惡意模式
- [ ] 檢查流量激增是否來自合法來源
- [ ] 在內部與外部溝通正在發生的情況

查看正確答案 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 — 2：偵測及因應網路威脅 — 3 — 4

您懷疑這可能是 DDoS 攻擊。您的第一步是什麼？

- ✗ 透過 DDoS 緩解服務重新導向所有網路流量
- ✗ 啟用 Web 應用程式防火牆 (WAF) 規則以篩選惡意模式
- ✓ 檢查流量激增是否來自合法來源
- ✗ 在內部與外部溝通正在發生的情況

在啟用 DDoS 對策之前，必須先驗證流量激增的合法性。這能讓您避免意外封鎖真正的使用者，防止對關鍵利害關係人造成干擾，並確保任何進一步的保護措施適當且精準鎖定目標，進而將對公共營運與整體業務持續性的負面影響降至最低。

下一個問題 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 — 2 — 3：從網路攻擊中復原 — 4

您可以採取哪些步驟來嘗試避免未來的 DDoS 攻擊？

- [ ] 封鎖有問題的 IP 位址
- [ ] 定期執行滲透測試搭配 DDoS 模擬
- [ ] 將所有應用程式移至雲端，因為雲端提供商通常不會遭受 DDoS 攻擊
- [ ] 實施零信任原則

查看正確答案 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 ✓ — 2 ✓ — 3：從網路攻擊中復原 ✓ — 4 ○

您可以採取哪些步驟來嘗試避免未來的 DDoS 攻擊？

- ✗ 封鎖有問題的 IP 位址
- ✓ 定期執行滲透測試搭配 DDoS 模擬
- ✗ 將所有應用程式移至雲端，因為雲端提供商通常不會遭受 DDoS 攻擊
- ✓ 實施零信任原則

主動式滲透測試搭配 DDoS 模擬可識別並強化您的防禦缺口，而零信任原則始終會執行最低權限存取，專注於將風險最小化。這有助於降低干擾關鍵系統的風險，例如緊急應變協調或即時交通號誌控制等必須在攻擊期間保持運作的系統。

下一個問題 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 2 3 4：整體最佳實務

做為整體事件回應與復原計畫 (IRR) 的一部分，您應該通知誰？

- [ ] 您的法務團隊
- [ ] 您的網路保險廠商
- [ ] CISA (網路安全暨基礎設施安全局)、FBI、MS-ISAC (多州資訊分享與分析中心)
- [ ] 以上皆是

查看正確答案 →

攻擊類型：分散式阻斷服務攻擊 (DDoS)

1 2 3 4：整體最佳實務

做為整體事件回應與復原計畫 (IRR) 的一部分，您應該通知誰？

- [x] 您的法務團隊
- [x] 您的網路保險廠商
- [x] CISA (網路安全暨基礎設施安全局)、FBI、MS-ISAC (多州資訊分享與分析中心)
- [x] 以上皆是

在大規模網路事件期間，請考慮與法務、保險與政府機構協調，處理合規性、理賠與執法事宜。在您確保符合所有法規要求後，貴組織便能有效圍堵、解決事件並從事件中復原。

查看解決方案 →

攻擊類型：分散式阻斷服務攻擊 (DDOS)

重點回顧

DDoS 攻擊是指攻擊者從多個來源發送龐大流量，意圖癱瘓網路、服務或伺服器的正常運行。攻擊者利用殭屍網路發動攻擊，而殭屍網路則是攻擊者遠端控制的受感染裝置網路。

在 Dell，我們結合進階的偵測與緩解技術、專業服務與零信任方法，協助組織對抗 DDoS 攻擊，保持韌性，進而確保快速回應、將干擾降至最低，並強化防禦。

深入瞭解進階的網路韌性策略，以及 Dell 如何協助您保護組織免受 DDoS 攻擊。

探索 DDoS 摘要 →

⌂ 返回情境

網路解決方案 ›

啟用網路區隔、微區隔與最低權限執行，以隔離關鍵資產、限制攻擊擴散，並確保快速圍堵 DDoS。

PowerEdge 伺服器 ›

透過硬體信任根、安全開機、系統鎖定與即時竄改證據，Dell 提供有韌性、高效能的 DDoS 保護與加速復原。

受信任裝置 ›

整合的 SafeBIOS、SecureData 以及自動化偵測與回應可將端點攻擊面減少高達 70%，防止 DDoS 驅動的干擾成為入侵途徑。

PowerProtect 產品組合 ›

加密、不可變與實體隔離的備份環境，由 AI 驅動的威脅分析提供支援，確保快速、經驗證的還原，並在 DDoS 干擾期間維持業務持續性。

安全性與復原能力服務 ›

Manage Detection and Response (MDR)、事件回應與復原 (IRR)、威脅搜捕與韌性架構指導，可增強 DDoS 準備度並強化防禦能力。

攻擊類型：惡意內部人員

現在是星期二早上 8:00。美國一家醫療保健公司的員工剛開始一天的工作。

一位處理高度敏感患者資料的高階員工在辦公室工作到深夜後登入系統。

她注意到前一晚工作的資料夾中有變更。在與團隊確認後，她向 IT 部門提出查詢。

經過調查後，他們發現一名與犯罪集團有關聯的初階 IT 員工誘騙高階員工將 USB Rubber Ducky 插入其裝置，這會將基本輸入/輸出系統 (BIOS) 降級為易受攻擊的版本，進而入侵系統。

測試您的知識 →

攻擊類型：惡意內部人員

1：縮小攻擊面 2 3 4 5

惡意內部人員使用 MITRE 對抗戰術、技術與常見知識 (MITRE ATT&CK) 框架追蹤的兩種方法發起此攻擊。它們是什麼？

- [ ] 信任關係 + 透過可移除媒體複製
- [ ] 社交工程 + 透過可移除媒體複製
- [ ] 社交工程 + 外部遠端服務
- [ ] 信任關係 + 硬體新增

查看正確答案 →

攻擊類型：惡意內部人員

1：縮小攻擊面 2 3 4 5

惡意內部人員使用 MITRE 對抗戰術、技術與常見知識 (MITRE ATT&CK) 框架追蹤的兩種方法發起此攻擊。它們是什麼？

- ✗ 信任關係 + 透過可移除媒體複製
- ✓ 社交工程 + 透過可移除媒體複製
- ✗ 社交工程 + 外部遠端服務
- ✗ 信任關係 + 硬體新增

配合 MITRE ATT&CK 技術，結合人為操縱與透過可攜式儲存裝置複製，攻擊者利用社交工程誘騙高階員工連接 USB Rubber Ducky，透過可移除媒體傳遞遭入侵的資料。

下一個問題 →

攻擊類型：惡意內部人員

1 — 2：偵測及因應網路威脅 — 3 — 4 — 5

為什麼攻擊者需要同時使用這兩種方法？

- [ ] 以全域管理員身分進入網路，以降級基本輸入/輸出系統 (BIOS)
- [ ] 對管理員進行網路釣魚，以允許他們降級 BIOS
- [ ] 變更裝置的網域名稱系統 (DNS) 供應商，以取得一次性網路存取所需的認證
- [ ] 在裝置上安裝惡意軟體，以取得持續網路存取所需的認證

查看正確答案 →

攻擊類型：惡意內部人員

1 — 2：偵測及因應網路威脅 — 3 — 4 — 5

為什麼攻擊者需要同時使用這兩種方法？

- ✗ 以全域管理員身分進入網路，以降級基本輸入/輸出系統 (BIOS)
- ✗ 對管理員進行網路釣魚，以允許他們降級 BIOS
- ✗ 變更裝置的網域名稱系統 (DNS) 供應商，以取得一次性網路存取所需的認證
- ✓ 在裝置上安裝惡意軟體，以取得持續網路存取所需的認證

攻擊者需要使用這兩種方法──透過 USB Rubber Ducky 安裝惡意軟體來入侵裝置，以及使用認證來實現持續的網路存取──以對目標環境建立持續且未經授權的控制。

下一個問題 →

攻擊類型：惡意內部人員

1 2 3：偵測及因應網路威脅 4 5

偵測異常網路活動的其中一種方法是什麼？

- [ ] 應用程式控制
- [ ] 延伸偵測與回應 (XDR)
- [ ] 次世代防毒 (NGAV)
- [ ] 端點電子圍籬

查看正確答案 →

攻擊類型：惡意內部人員

1 ✓ — 2 ✓ — 3：偵測及因應網路威脅 ✓ — 4 ○ — 5 ○

偵測異常網路活動的其中一種方法是什麼？

- ✗ 應用程式控制
- ✓ 延伸偵測與回應 (XDR)
- ✗ 次世代防毒 (NGAV)
- ✗ 端點電子圍籬

由於 XDR 可提供廣泛、相關的可見度，以快速偵測威脅，所以最適合偵測可疑的網路活動，因為它會持續監控並分析跨端點、網路與雲端環境的活動。

下一個問題 →

攻擊類型：惡意內部人員

1 2 3 4：從網路攻擊中復原 5

哪種內建電腦安全性可以偵測到攻擊鏈早期的可疑活動？

- [ ] 安全性資訊和事件管理 (SIEM)
- [ ] 延伸偵測與回應 (XDR)
- [ ] 攻擊指標 (IOA)
- [ ] 角色型存取控制 (RBAC)

查看正確答案 →

攻擊類型：惡意內部人員

1 2 3 4：從網路攻擊中復原 5

哪種內建電腦安全性可以偵測到攻擊鏈早期的可疑活動？

- ✗ 安全性資訊和事件管理 (SIEM)
- ✗ 延伸偵測與回應 (XDR)
- ✓ 攻擊指標 (IOA)
- ✗ 角色型存取控制 (RBAC)

IOA 專注於即時偵測攻擊者行為與可疑活的動模式，使安全性團隊能夠比簽章型方法更早識別出威脅，並在發生重大損害之前進行干預。

下一個問題 →

攻擊類型：惡意內部人員

1 2 3 4 5：整體最佳實務

在找出初始存取方法後，您可以採取哪樣措施來復原並防止未來類似的入侵？

- [ ] 將 BIOS 更新至最新版本
- [ ] 停用 BIOS 降級選項
- [ ] 停用 USB 連接埠
- [ ] 實施精細控制以實現安全的 USB 裝置使用，並防止惡意軟體擴散
- [ ] 以上皆是

查看正確答案 →

攻擊類型：惡意內部人員

1 2 3 4 5：整體最佳實務

在找出初始存取方法後，您可以採取哪樣措施來復原並防止未來類似的入侵？

- [x] 將 BIOS 更新至最新版本
- [x] 停用 BIOS 降級選項
- [x] 停用 USB 連接埠
- [x] 實施精細控制以實現安全的 USB 裝置使用，並防止惡意軟體擴散
- [x] 以上皆是

透過處理不同的攻擊途徑以確保硬體安全且封鎖降級，可以圍堵 USB 型威脅，並在多個點阻止惡意軟體擴散，協助建立全面的多層防禦，復原受影響的系統，並防範未來的入侵。

查看解決方案 →

攻擊類型：惡意內部人員

重點回顧

當組織內部人士濫用其存取權限來洩露資料、中斷營運或擷取敏感資訊，以用於私人、財務或競爭目的時，即為惡意內部人員攻擊。此人可以是員工、承包商、合作夥伴，或任何可以合法存取公司系統和網路的人。

Dell 透過結合進階技術與嚴格的安全協定，防禦惡意內部人員網路攻擊。

深入瞭解進階的網路韌性策略，以及 Dell 如何協助您保護組織免受惡意內部人員攻擊。

探索惡意內部人員摘要 →

返回情境

受信任裝置與基礎結構 ›

內建最低權限、多重因素驗證 (MFA)、角色型存取控制 (RBAC)、雙重驗證與零信任保護，可保護端點與基礎結構，降低內部威脅的風險。

PowerEdge 伺服器 ›

硬體信任根、安全開機、動態 USB 連接埠管理與系統鎖定，可防範竄改並阻止實體或韌體型內部人員攻擊。

PowerProtect 產品組合 ›

不可修改、隔離的備份能確保資料完整性、快速還原，以及早期偵測資料操縱的嘗試，進而從內部人員事件中復原。

安全性與復原能力服務 ›

專家主導的訓練、滲透測試、威脅搜捕、事件回應與入侵復原服務，可強化對內部人員驅動事件的準備度與韌性。

安全性合作夥伴 ›

整合的端點偵測與回應 (EDR)、延伸偵測與回應 (XDR) 與自動化威脅情報，可即時識別、圍堵並緩解複雜的內部威脅。

攻擊類型：中間人攻擊 (MITM)

一位毫無戒心的客戶在咖啡店連接到免費、不安全的 Wi-Fi，完成共用團隊文件的最後更新。

片刻之後，他們公司的 IT 部門收到來自該員工帳戶的異常登入嘗試通知，以及來自全球多個地點的未經授權資料存取。

經過調查後，他們確認攻擊者已攔截並操縱無線連線，存取敏感資訊。

測試您的知識 →

攻擊類型：中間人攻擊 (MITM)

1：縮小攻擊面　2　3　4

在偵測到異常登入嘗試後，IT 團隊首先應該在哪裡進行調查？

- [ ] 防火牆、入侵偵測系統 (IDS)、入侵防禦系統 (IPS) 記錄檔與延伸偵測回應 (XDR)
- [ ] 受影響員工的筆記型電腦
- [ ] 咖啡店不安全 Wi-Fi 的網路流量
- [ ] 公司系統的驗證記錄檔

查看正確答案 →

攻擊類型：中間人攻擊 (MITM)

1：縮小攻擊面 — 2 — 3 — 4

在偵測到異常登入嘗試後，IT 團隊首先應該在哪裡進行調查？

- ✓ 防火牆、入侵偵測系統 (IDS)、入侵防禦系統 (IPS) 記錄檔與延伸偵測回應 (XDR)
- ✗ 受影響員工的筆記型電腦
- ✗ 咖啡店不安全 Wi-Fi 的網路流量
- ✓ 公司系統的驗證記錄檔

透過分析這些防火牆、IDS/IPS 與驗證記錄檔，IT 團隊可以追蹤未經授權的存取嘗試，評估遭入侵的帳戶，更加瞭解事件的範圍。

下一個問題 →

攻擊類型：中間人攻擊 (MITM)

1 — 2：偵測及因應網路威脅 — 3 — 4

在確認 MITM 攻擊後，IT 團隊應該立即採取什麼行動？

- [ ] 立即將遭入侵員工的裝置從網路中斷線，並將其隔離以進行分析
- [ ] 更新防火牆規則與網路配置，以阻止進一步未經授權的存取行為
- [ ] 重設所有員工帳戶的密碼
- [ ] 停用受影響的系統以防止資料外洩

查看正確答案 →

攻擊類型：中間人攻擊 (MITM)

1 — 2：偵測及因應網路威脅 — 3 — 4

在確認 MITM 攻擊後，IT 團隊應該立即採取什麼行動？

- ✓ 立即將遭入侵員工的裝置從網路中斷線，並將其隔離以進行分析
- ✓ 更新防火牆規則與網路配置，以阻止進一步未經授權的存取行為
- ✗ 重設所有員工帳戶的密碼
- ✗ 停用受影響的系統以防止資料外洩

立即中斷連線並隔離遭入侵的裝置，可阻止攻擊者存取並保存鑑識證據，而更新防火牆與網路規則，則可封鎖進一步的惡意連線，並防範更廣泛的網路環境，免於持續遭到入侵。

下一個問題 →

攻擊類型：中間人攻擊 (MITM)

1 2 3：從網路攻擊中復原 4

哪些預防措施可以減少 MITM 攻擊的漏洞？

- [ ] 強制所有員工使用虛擬私人網路 (VPN)
- [ ] 實施零信任安全性原則，例如多重因素驗證 (MFA)
- [ ] 避免使用公共 Wi-Fi
- [ ] 將透過電子郵件分享的敏感檔案進行加密

查看正確答案 →

攻擊類型：中間人攻擊 (MITM)

1 2 3：從網路攻擊中復原 4

哪些預防措施可以減少 MITM 攻擊的漏洞？

- ✓ 強制所有員工使用虛擬私人網路 (VPN)
- ✓ 實施零信任安全性原則，例如多重因素驗證 (MFA)
- ✗ 避免使用公共 Wi-Fi
- ✗ 將透過電子郵件分享的敏感檔案進行加密

在不安全的網路上強制使用 VPN，可加密員工的網際網路流量以防止攔截，而實施零信任安全性原則與 MFA，則確保每個存取請求都經過持續驗證。

下一個問題 →

攻擊類型：中間人攻擊 (MITM)

1 2 3 4：整體最佳實務

在處理入侵後，您的組織應該實施哪些長期策略？

- [ ] 定期稽核與修補系統
- [ ] 增加網路區隔以隔離敏感資料與系統
- [ ] 部署端點偵測與回應 (EDR) 與 Managed Detection and Response (MDR) 解決方案
- [ ] 為員工實施強健且定期的訓練
- [ ] 以上皆是

查看正確答案 →

攻擊類型：中間人攻擊 (MITM)

1 2 3 4：整體最佳實務

在處理入侵後，您的組織應該實施哪些長期策略？

- [x] 定期稽核與修補系統
- [x] 增加網路區隔以隔離敏感資料與系統
- [x] 部署端點偵測與回應 (EDR) 與 Managed Detection and Response (MDR) 解決方案
- [x] 為員工實施強健且定期的訓練
- [x] 以上皆是

為了防範不同的威脅，這些長期策略結合起來可建立全方位、有韌性的安全性狀態，阻止攻擊者利用缺口，並確保快速且有效地回應入侵行為。

查看解決方案 →

攻擊類型：中間人攻擊 (MITM)

重點回顧

當網路犯罪分子秘密攔截某兩方之間的通訊，例如員工與公司伺服器之間的通訊，或客戶與企業網站之間的通訊，就會發生 MITM 攻擊。攻擊者的目標可能各異，但結果卻如出一轍：信任與安全的雙重崩壞。

在 Dell，我們提供創新、可擴充的安全解決方案，賦予組織能力以消除 MITM 威脅、保護資產，並維持業務完整性，搭配偵測、回應與自信復原所需的工具與專業知識。

深入瞭解進階的網路韌性策略，並瞭解 Dell 如何協助您保護組織免受 MITM 攻擊。

閱讀 MITM 攻擊摘要 →

返回情境

受信任裝置 ›

Dell 透過硬體驗證、韌體保護 (例如 SafeBIOS 與 SafeID)、強健的加密與零信任框架，保護端點與傳輸中的資料。

PowerEdge 伺服器 ›

安全開機、晶片信任根、動態 USB 連接埠管理與系統鎖定，確保硬體完整性，並保護關鍵工作負載免受網路型威脅。

儲存解決方案 ›

靜態與傳輸中的加密資料，結合隔離的快照與快速復原功能，確保檔案保持安全，並可在 MITM 攻擊後快速還原。

PowerProtect 產品組合 ›

不可修改、隔離的備份與 AI 驅動的 CyberSense 分析，能在 MITM 攻擊事件中實現快速復原與可信賴的資料還原。

安全性與復原能力服務 ›

從漏洞評估與使用者訓練，到滲透測試與事件回應，Dell 的專家與合作夥伴提供全方位的支援，以強化您的防禦。

攻擊類型：提示/SQL 注入

您在一家主要透過聊天機器人提供服務的航空公司擔任客戶服務人員。

您開始注意到您和同事接到大量客戶來電，表示他們無法進入自己的常客飛行帳戶，而當他們進入時，發現所有常客飛行里程都消失了。

測試您的知識 →

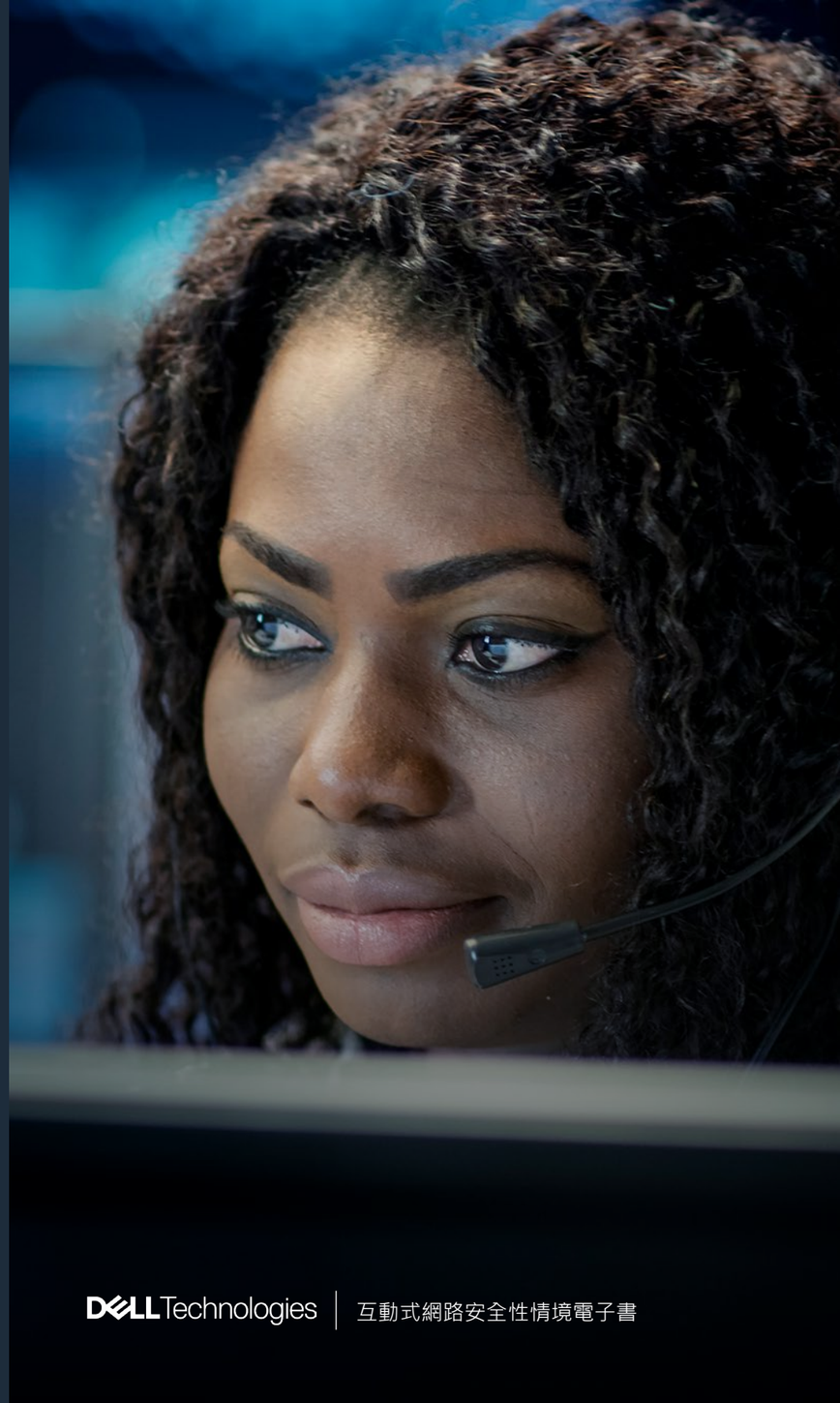
攻擊類型：提示/SQL 注入

1：縮小攻擊面 2 3 4

經過調查，您在記錄檔中看到一些錯誤：*Syntax error in Structured Query Language (SQL) statement or Invalid column name 'admin'* (結構化查詢語言 (SQL) 陳述式中的語法錯誤，或無效的欄名稱 'admin')。這是哪種類型的網路事件？

- [ ] 認證竊取
- [ ] 提示或 SQL 注入
- [ ] 中間人攻擊
- [ ] 網路釣魚

查看正確答案 →



攻擊類型：提示/SQL 注入

1：縮小攻擊面 — 2 — 3 — 4

經過調查，您在記錄檔中看到一些錯誤：*Syntax error in Structured Query Language (SQL) statement*（結構化查詢語言 (SQL) 陳述式中的語法錯誤）或 *Invalid column name 'admin'*（無效的欄名稱 'admin'）。這是哪種類型的網路事件？

- ✗ 認證竊取
- ✓ 提示或 SQL 注入
- ✗ 中間人攻擊
- ✗ 網路釣魚

「提示或 SQL 注入」是正確答案，因為記錄檔錯誤 (例如「Syntax error in SQL statement」(SQL 陳述式中的語法錯誤)或「Invalid column name 'admin'」(無效的欄位名稱 'admin')) 顯示攻擊者利用聊天機器人的輸入欄位，使用惡意 SQL 程式碼來存取或變更客戶帳戶資料，這些 SQL 注入攻擊的明確技術指標與所描述的可疑活動相符。

下一個問題 →

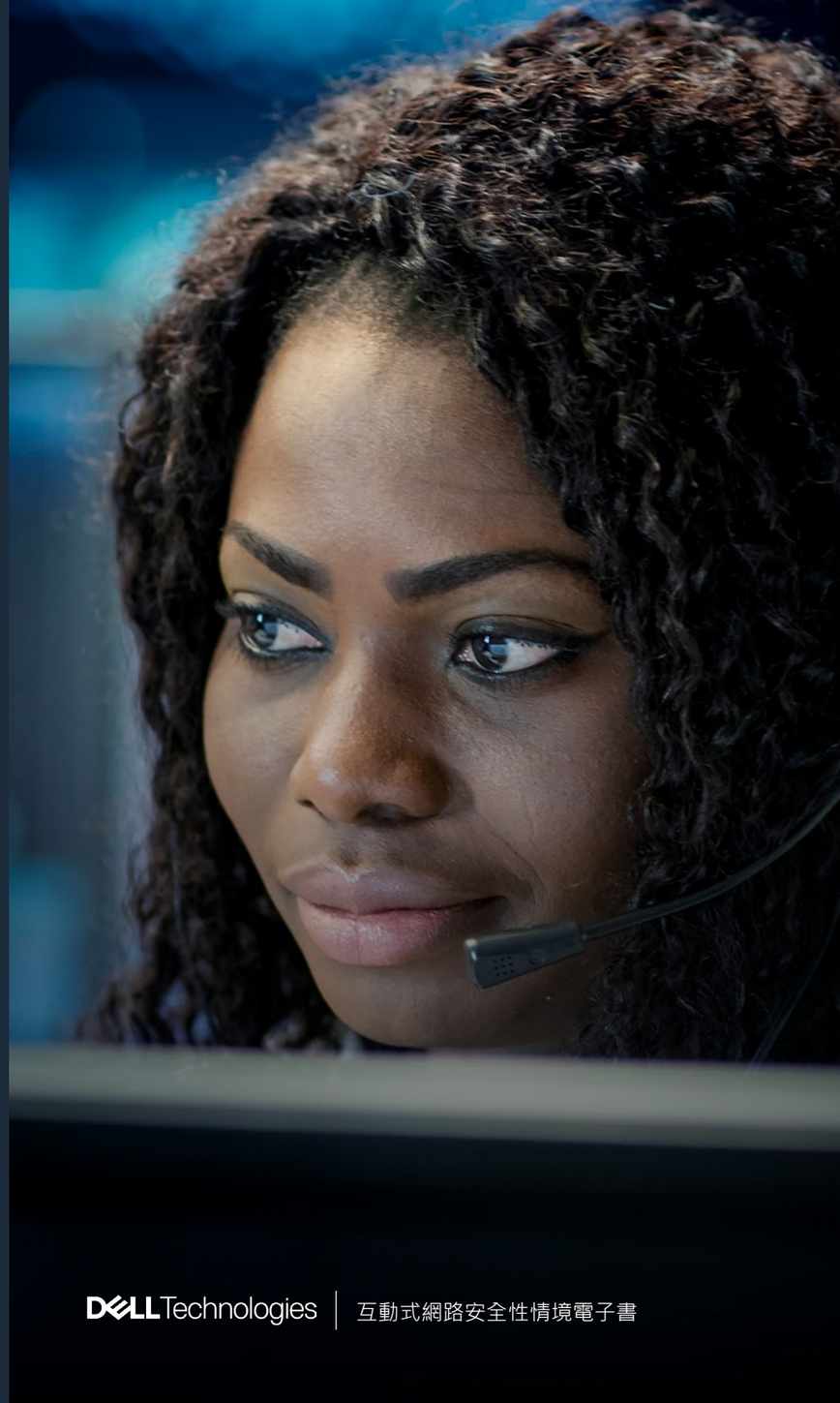
攻擊類型：提示/SQL 注入

1 — 2：偵測及因應網路威脅 — 3 — 4

您意識到您的客戶服務聊天機器人遭受提示/SQL 注入攻擊。您應該怎麼做？

- [ ] 讓機器人離線
- [ ] 調查資料庫記錄檔，尋找未經授權的存取以及被竊取、修改或刪除的資料
- [ ] 遵守所有資料違規揭露法律
- [ ] 以上皆是

查看正確答案 →



攻擊類型：提示/SQL 注入

1 — 2：偵測及因應網路威脅 — 3 — 4

您意識到您的客戶服務聊天機器人遭受提示/SQL 注入攻擊。您應該怎麼做？

- [x] 讓機器人離線
- [x] 調查資料庫記錄檔，尋找未經授權的存取以及被竊取、修改或刪除的資料
- [x] 遵守所有資料違規揭露法律
- [x] 以上皆是

回應提示/SQL 注入攻擊，需要讓聊天機器人離線、調查資料庫記錄檔以尋找未經授權的存取，並確保遵守揭露法律。這些步驟對於停止利用、評估損害以及履行法規與道德義務至關重要。

下一個問題 →

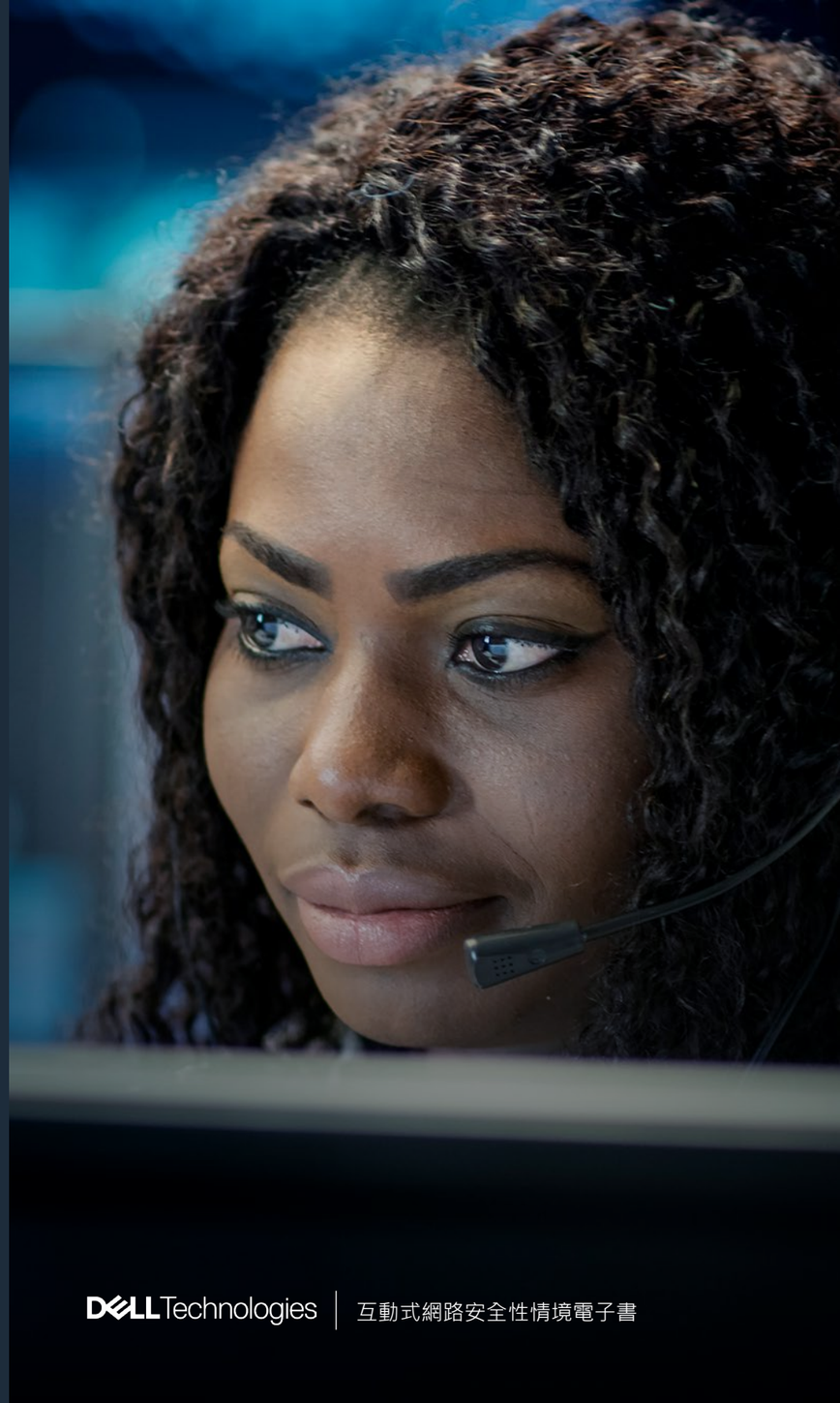
攻擊類型：提示/SQL 注入

1 — 2 — 3：從網路攻擊中復原 — 4

您應該實施哪些功能來協助阻止提示/SQL 注入？

- [ ] 教育開發團隊使用預備陳述式與參數化查詢作為編碼實務
- [ ] Managed Detection and Response (MDR) 工具
- [ ] 實施最低權限存取，例如多重因素驗證 (MFA)、角色型存取控制 (RBAC)、Web 應用程式防火牆 (WAF) 等
- [ ] 區隔後端資料庫/知識庫

查看正確答案 →



攻擊類型：提示/SQL 注入

1 2 3：從網路攻擊中復原 4

您應該實施哪些功能來協助阻止提示/SQL 注入？

- ✓ 教育開發團隊使用預備陳述式與參數化查詢作為編碼實務
- ✗ Managed Detection and Response (MDR) 工具
- ✓ 實施最低權限存取，例如多重因素驗證 (MFA)、角色型存取控制 (RBAC)、Web 應用程式防火牆 (WAF) 等
- ✗ 區隔後端資料庫/知識庫

訓練開發團隊使用預備陳述式與參數化查詢，便能從源頭封鎖 SQL 注入攻擊，而執行最低權限存取控制 (例如 MFA、RBAC 與 WAF) 則可透過防止攻擊者提升權限或橫向移動，限制任何嘗試注入的影響。

下一個問題 →

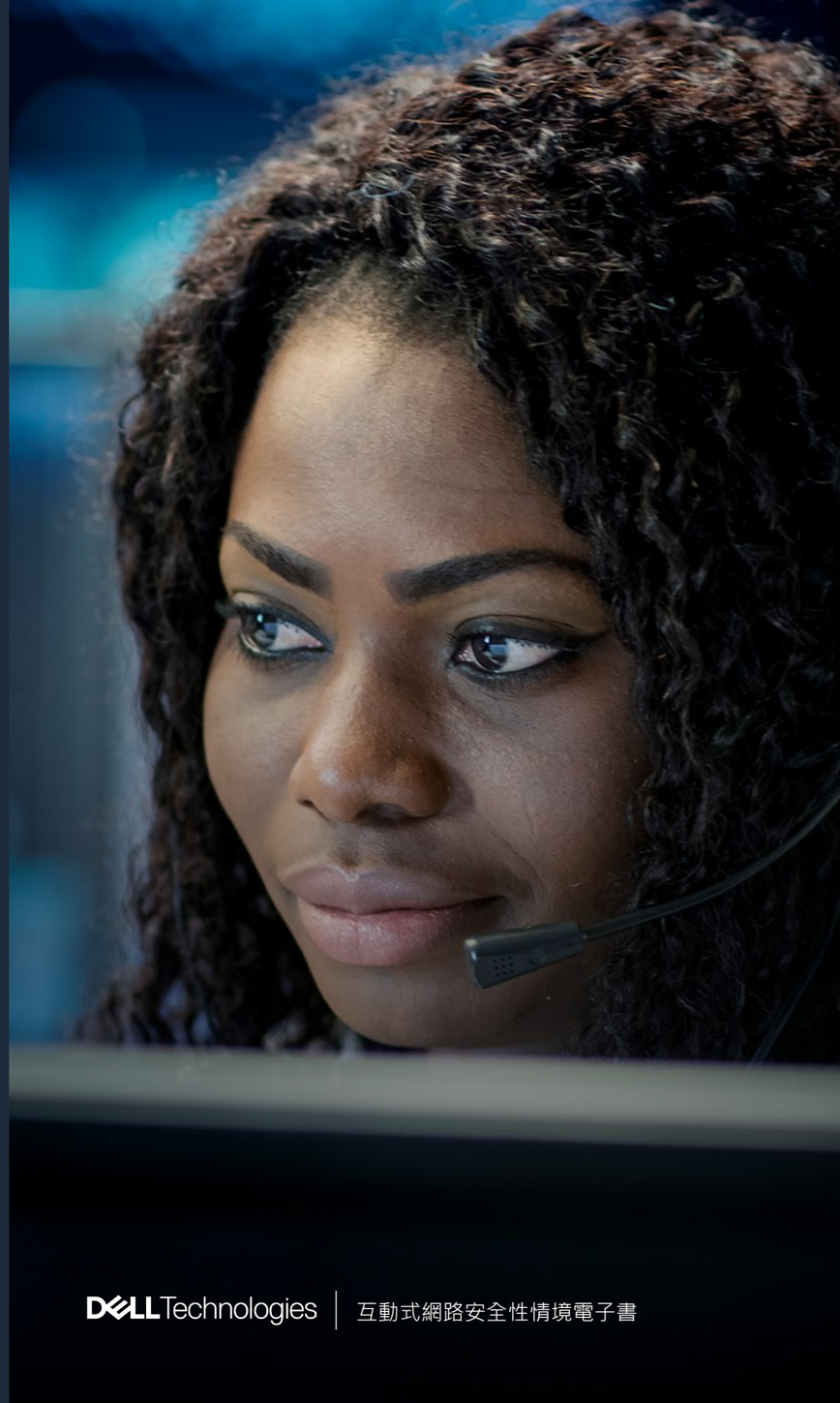
攻擊類型：提示/SQL 注入

1 2 3 4：整體最佳實務

您會採取哪些步驟來取回航空公司客戶的資料？

- [ ] 追蹤被竊取的資料
- [ ] 讓客戶重建其個人資料
- [ ] 向網路攻擊者買回資料
- [ ] 從最近未遭入侵的備份還原，以還原常客飛行里程，並通知客戶他們應該變更密碼並檢查信用卡

查看正確答案 →



攻擊類型：提示/SQL 注入

1 2 3 4：整體最佳實務

您會採取哪些步驟來取回航空公司客戶的資料？

- ✗ 追蹤被竊取的資料
- ✗ 讓客戶重建其個人資料
- ✗ 向網路攻擊者買回資料
- ✓ 從最近未遭入侵的備份還原，以還原常客飛行里程，並通知客戶他們應該變更密碼並檢查信用卡

從最新未遭入侵的備份復原遺失的帳戶資料，有助於維持資料完整性，並減少停機時間。在破壞性注入攻擊後，迅速通知客戶重設密碼並監控信用卡活動，進一步支援法規遵循。

查看解決方案 →

攻擊類型：提示/SQL 注入

重點回顧

提示和 SQL 注入攻擊屢次經證明是網路犯罪分子發動網路攻擊中最具破壞性也最普遍的方法之一。這些攻擊是利用使用者查詢或資料庫系統中的漏洞，讓惡意行為者能操縱伺服器、竊取資料或中斷工作流程。

保護您的組織免受不斷演變的提示/SQL 注入威脅與攻擊，是 Dell 對網路安全持續承諾的一部分，我們提供偵測、回應與復原所需的工具與專業知識。

探索進階的網路韌性策略，並瞭解 Dell 如何賦予您的組織能力，以防禦提示與 SQL 注入攻擊。

探索提示/SQL 注入摘要 →

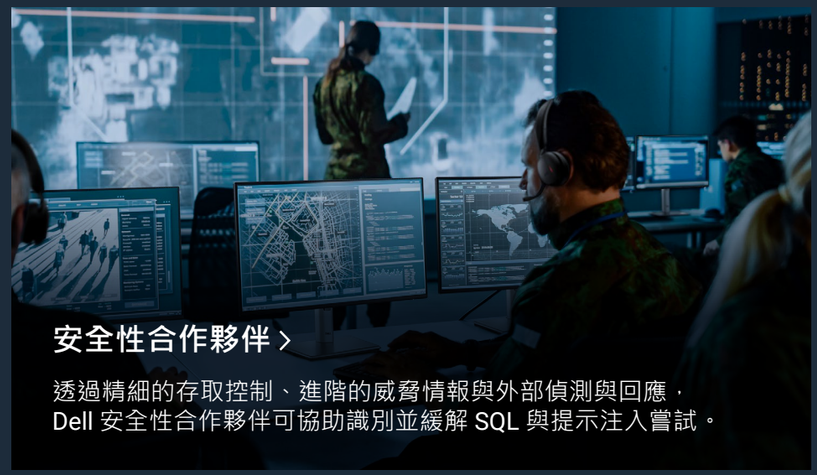
返回情境

受信賴工作空間和受信賴基礎結構 ›

保護端點安全，並降低遭入侵認證在注入攻擊中被利用的風險。

PowerEdge 伺服器 ›

Dell PowerEdge 伺服器具備硬體信任根、安全開機、晶片型安全性與即時組態驗證程式，可確保防竄改的基礎結構僅執行受信賴的程式碼。



安全性合作夥伴 ›

透過精細的存取控制、進階的威脅情報與外部偵測與回應，Dell 安全性合作夥伴可協助識別並緩解 SQL 與提示注入嘗試。

PowerProtect 產品組合 ›

Dell 的不可修改、實體隔離備份與進階的網路復原分析提供受信賴的還原點，確保從資料損毀或外洩中快速復原。

安全性與復原能力服務 ›

從安全開發訓練與滲透測試，到威脅搜捕與事件回應，Dell 的專家與合作夥伴協助驗證保護措施，並快速修復注入攻擊的傷害。

攻擊類型：勒索軟體

您是一位 IT 專業人員，在以連線醫療系統聞名的區域醫院工作，該系統包括電子健康記錄 (EHR)、智慧型輸液幫浦與放射影像，全部連接到集中式網路。

昨晚，多個系統同時開始當機。到了早上，臨床人員回報無法存取患者記錄。

以下勒索訊息出現在多個終端機上：

「已對您的檔案加密。在 72 小時內支付 20 個比特幣，否則將公開患者資料。」

測試您的知識 →

攻擊類型：勒索軟體

1：縮小攻擊面 2 3 4

服務台收到超過 100 個檔案加密與應用程式錯誤的報告。安全記錄檔顯示來自內部網域帳戶的異常檔案重新命名活動。您的第一步是什麼？

- [ ] 立即支付贖金以還原關鍵服務
- [ ] 通知執法單位與法律顧問
- [ ] 開始重新映像所有受影響的端點
- [ ] 將受感染的系統從網路中斷線

查看正確答案 →

攻擊類型：勒索軟體

1：縮小攻擊面 — 2 — 3 — 4

服務台收到超過 100 個檔案加密與應用程式錯誤的報告。安全記錄檔顯示來自內部網域帳戶的異常檔案重新命名活動。您的第一步是什麼？

- ✗ 立即支付贖金以還原關鍵服務
- ✗ 通知執法單位與法律顧問
- ✗ 開始重新映像所有受影響的端點
- ✓ 將受感染的系統從網路中斷線

立即中斷連線並隔離受感染的醫院系統。可阻止勒索軟體擴散、保護關鍵醫療裝置與敏感患者資料、保存調查證據，並爭取寶貴時間進行協調回應與復原。

下一個問題 →

攻擊類型：勒索軟體

1 — 2：偵測及因應網路威脅 — 3 — 4

事件回應團隊發現攻擊可能從遭入侵的帳戶開始，該帳戶用於存取無多重因素驗證 (MFA) 的伺服器。以下哪項是導致攻擊的主因？

- [ ] 過時的防毒軟體定義
- [ ] 暴露的電子健康記錄 (EHR) 資料庫
- [ ] 遠端存取缺乏 MFA
- [ ] 電子郵件篩選功能太弱

查看正確答案 →

攻擊類型：勒索軟體

1 — 2：偵測及因應網路威脅 — 3 — 4

事件回應團隊發現攻擊可能從遭入侵的帳戶開始，該帳戶用於存取無多重因素驗證 (MFA) 的伺服器。以下哪項是導致攻擊的主因？

- ✗ 過時的防毒軟體定義
- ✗ 暴露的電子健康記錄 (EHR) 資料庫
- ✓ 遠端存取缺乏 MFA
- ✗ 電子郵件篩選功能太弱

遠端存取缺乏 MFA，讓伺服器有遭到入侵的風險，因為攻擊者可以使用竊取或猜測而得的認證登入，而無需額外的驗證步驟。有了 MFA，即使帳戶遭入侵，仍需要第二個因素，因而大幅降低未經授權存取的風險。

下一個問題 →

攻擊類型：勒索軟體

1 2 3：從網路攻擊中復原 4

醫療人員現在依賴紙本工作流程。今天預定手術的患者無法在系統中驗證。支援醫院營運的最佳短期行動是什麼？

- [ ] 重新啟動核心資料庫伺服器以嘗試重新初始化
- [ ] 即使是六個月前的內容，仍啟用所有舊備份
- [ ] 啟用醫院的手動停機程序，並向緊急應變團隊呈報
- [ ] 讓人員根據個案情況決定如何進行

查看正確答案 →

攻擊類型：勒索軟體

1 2 3：從網路攻擊中復原 4

醫療人員現在依賴紙本工作流程。今天預定手術的患者無法在系統中驗證。支援醫院營運的最佳短期行動是什麼？

- ✗ 重新啟動核心資料庫伺服器以嘗試重新初始化
- ✗ 即使是六個月前的內容，仍啟用所有舊備份
- ✓ 啟用醫院的手動停機程序，並向緊急應變團隊呈報
- ✗ 讓人員根據個案情況決定如何進行

啟用手動停機程序並向緊急應變團隊呈報，可確保立即延續關鍵的臨床工作流程、保護患者安全，並建立驗證與記錄照護的標準化流程。這種方法可將錯誤降至最低、有效管理風險與資源，並支援專家安全地還原數位系統。

下一個問題 →

攻擊類型：勒索軟體

1 2 3 4：整體最佳實務

當地媒體已報導此事件。領導階層想知道是否應該發布公開聲明，而法務部門詢問有關健康保險流通與責任法案 (HIPAA) 義務的問題。最適當的下一步是什麼？

- [ ] 在取得更多資訊之前公開否認事件
- [ ] 發布新聞稿指責第三方 IT 廠商
- [ ] 通知監管機構並開始內部入侵通知程序
- [ ] 立即支付贖金並避免公眾關注

查看正確答案 →

攻擊類型：勒索軟體

1 2 3 4：整體最佳實務

當地媒體已報導此事件。領導階層想知道是否應該發布公開聲明，而法務部門詢問有關健康保險流通與責任法案 (HIPAA) 義務的問題。最適當的下一步是什麼？

- ✗ 在取得更多資訊之前公開否認事件
- ✗ 發布新聞稿指責第三方 IT 廠商
- ✓ 通知監管機構並開始內部入侵通知程序
- ✗ 立即支付贖金並避免公眾關注

根據 HIPAA 與州法律的要求，迅速向主管機關與受影響的個人回報受保護健康資訊的入侵狀況，可確保法規遵循、法律保護與最佳實務透明度，以防止法律與聲譽損害，進而履行強制性揭露義務，並與患者、員工與利害關係人建立適當的溝通。

查看解決方案 →

攻擊類型：勒索軟體

重點回顧

勒索軟體是一種惡意軟體，會阻斷對電腦系統或資料的存取，直到受害者支付贖金。這是最具破壞性的網路攻擊類型之一。全球百分之五十的組織在過去一年內都遭受過至少一次的勒索軟體攻擊，勒索軟體攻擊後的平均停機時間為三週，導致嚴重的營運中斷。

在 Dell，我們優先透過零信任框架、端點保護與網路區隔來保護您的組織，以封鎖勒索軟體進入並限制其擴散。透過專家主導的事件回應規劃，我們協助您保持韌性並從攻擊中快速復原。

深入瞭解進階的網路韌性策略，並瞭解 Dell 如何協助您保護組織免受勒索軟體攻擊。

探索勒索軟體攻擊摘要 →

返回情境

受信賴的基礎結構 >

透過硬體驗證、多重因素驗證 (MFA)、角色型存取控制 (RBAC) 與零信任框架，在基礎結構層級封鎖勒索軟體。

網路與 PowerEdge 伺服器 >

限制勒索軟體移動。具備網路區隔、安全開機、晶片信任根、動態 USB 連接埠管理與系統鎖定。

受信任的工作空間 >

整合 SafeBIOS、SafeID、SafeData 與端點偵測與回應 (EDR) 工具，在裝置層級提供主動威脅情報、即時偵測與自動化惡意軟體圍堵。

PowerProtect 產品組合 >

透過不可修改、實體隔離的備份、智慧型網路復原分析與快速還原功能，保護關鍵資料，以防止勒索並實現韌性。

安全性與復原能力服務 >

與 CrowdStrike 等專家合作，協助進行評估、漏洞管理、安全性意識訓練、滲透測試與事件回應。

攻擊類型：供應鏈硬體

您的公司在全球辦公室推出 500 台全新筆記型電腦。為了加快速度，您將映像與硬體準備工作外包給第三方 IT 物流廠商。他們直接將預先設定組態的機器運送給員工。

幾天之內，您收到多通來自現場的電話，表示：

- 多重因素驗證 (MFA) 要求被繞過或無法正常運作。
- 安全性團隊看到多個時間詭異的未經授權管理員登入。
- 他們還看到來自應該離線的使用者的虛擬私人網路 (VPN) 流量。

測試您的知識 →

攻擊類型：供應鏈硬體

1：縮小攻擊面 2 3 4

一名員工回報在未嘗試登入時收到多重因素驗證 (MFA) 推送通知。您組織的安全儀表板顯示登入來自具有公司發放資產標籤的裝置。安全營運中心 (SOC) 團隊最合乎邏輯的第一步是什麼？

- [ ] 遠端停用使用者的帳戶，並抹除其筆記型電腦
- [ ] 將登入 IP 和裝置指紋與其他已知遭入侵的使用者進行比較
- [ ] 向 HR 呈報，假設使用者有過失
- [ ] 發布全公司警報，立即變更密碼

查看正確答案 →

攻擊類型：供應鏈硬體

1：縮小攻擊面 2 3 4

一名員工回報在未嘗試登入時收到多重因素驗證 (MFA) 推送通知。您組織的安全儀表板顯示登入來自具有公司發放資產標籤的裝置。安全營運中心 (SOC) 團隊最合乎邏輯的第一步是什麼？

- ✗ 遠端停用使用者的帳戶，並抹除其筆記型電腦
- ✓ 將登入 IP 和裝置指紋與其他已知遭入侵的使用者進行比較
- ✗ 向 HR 呈報，假設使用者有過失
- ✗ 發布全公司警報，立即變更密碼

當您的 SOC 團隊判斷可疑活動是屬於範圍更廣的攻擊，還是孤立攻擊時，即可快速辨識模式、針對事件回應，以及圍堵進一步的風險，這是識別供應鏈硬體攻擊時的合乎邏輯第一步。

下一個問題 →

攻擊類型：供應鏈硬體

1 — 2：偵測及因應網路威脅 — 3 — 4

您的事件回應團隊發現多台受影響的筆記型電腦執行的 SSD 韌體版本與官方廠商版本資訊不符。端點偵測回應 (EDR) 未顯示惡意程序。這最可能表示什麼？

- [ ] 來自 IT 廠商的組態錯誤
- [ ] 一種會自我刪除的新型勒索軟體
- [ ] 韌體層級的供應鏈入侵
- [ ] 映像期間的正常行為

查看正確答案 →

攻擊類型：供應鏈硬體

1 — 2：偵測及因應網路威脅 — 3 — 4

您的事件回應團隊發現多台受影響的筆記型電腦執行的 SSD 韌體版本與官方廠商版本資訊不符。端點偵測回應 (EDR) 未顯示惡意程序。這最可能表示什麼？

- ✗ 來自 IT 廠商的組態錯誤
- ✗ 一種會自我刪除的新型勒索軟體
- ✓ 韌體層級的供應鏈入侵
- ✗ 映像期間的正常行為

多台筆記型電腦上未經授權的 SSD 韌體，未被 EDR 偵測到且與官方發布版本不符，表示蓄意的硬體或韌體竄改——這是韌體層級供應鏈入侵的標誌。

下一個問題 →

攻擊類型：供應鏈硬體

1 2 3：從網路攻擊中復原 4

您已隔離 100 台疑似具有惡意 SSD 韌體的裝置。您需要決定如何繼續進行，而不驚動可能具有遠端存取權的攻擊者。最好的下一步是什麼？

- [ ] 關閉所有裝置並將它們運送至鑑識部門
- [ ] 在系統執行時進行即時記憶體傾印並調查
- [ ] 通知第三方廠商他們已遭入侵
- [ ] 抹除所有裝置，並在全球向所有使用者重新發放全新的筆記型電腦

查看正確答案 →

攻擊類型：供應鏈硬體

1 — 2 — 3：從網路攻擊中復原 — 4

您已隔離 100 台疑似具有惡意 SSD 韌體的裝置。您需要決定如何繼續進行，而不驚動可能具有遠端存取權的攻擊者。最好的下一步是什麼？

- ✗ 關閉所有裝置並將它們運送至鑑識部門
- ✓ 在系統執行時進行即時記憶體傾印並調查
- ✗ 通知第三方廠商他們已遭入侵
- ✗ 抹除所有裝置，並在全球向所有使用者重新發放全新的筆記型電腦

即時記憶體傾印對於保存揮發性證據 (例如活躍的惡意軟體與 rootkit) 至關重要，在證據遺失或攻擊者察覺之前，揭露隱藏的威脅與存取點，即可針對事件回應。

下一個問題 →

攻擊類型：供應鏈硬體

1 2 3 4：整體最佳實務

您的資訊安全長要求提供此攻擊如何進入您環境的摘要。您需要向執行團隊提供簡明的解釋。您應該如何解釋此攻擊？

- [ ] 病毒是從網路釣魚連結意外下載而來
- [ ] 我們遇到網路組態錯誤，允許外部存取
- [ ] 惡意韌體是在筆記型電腦佈建期間透過遭入侵的硬體廠商引入
- [ ] 我們的一位開發人員將不安全的程式碼推送到生產環境

查看正確答案 →

攻擊類型：供應鏈硬體

1 2 3 4：整體最佳實務

您的資訊安全長要求提供此攻擊如何進入您環境的摘要。您需要向執行團隊提供簡明的解釋。您應該如何解釋此攻擊？

- ✗ 病毒是從網路釣魚連結意外下載而來
- ✗ 我們遇到網路組態錯誤，允許外部存取
- ✓ 惡意韌體是在筆記型電腦佈建期間透過遭入侵的硬體廠商引入
- ✗ 我們的一位開發人員將不安全的程式碼推送到生產環境

不符的韌體版本與缺乏活躍惡意軟體，確認這是源自廠商的韌體層級攻擊，而非使用者錯誤或組態錯誤。

查看解決方案 →

攻擊類型：供應鏈硬體

重點回顧

近年來，供應鏈攻擊大幅增加。透過在生產、運輸或部署過程中篡改實體裝置，或發現軟體供應商的弱點，攻擊者可以獲得注入惡意元件或代碼、損壞系統或洩露機密資料的方法。受害者的範圍從小型企業到全球企業，結果包括嚴重的財務損失、客戶信任受損和法律後果。

Dell 緩解供應鏈硬體攻擊的方式，是透過整合嚴格的廠商風險評估及嵌入零信任原則，同時持續執行裝置驗證和獨立的完整性檢查。我們在整個生命週期中強化硬體完整性。

深入瞭解進階的網路韌性策略，瞭解 Dell 如何協助您保護組織免受供應鏈硬體攻擊。

探索供應鏈硬體攻擊摘要 →

⌂ 返回情境

供應鏈保證 ›

透過進階的來源追溯、防竄改物流與透明採購，Dell 的供應鏈確保硬體、韌體與供應商在到達您的組織之前經過嚴格驗證。

安全元件驗證 (SCV) ›

在工廠與安裝期間對電腦元件進行加密驗證，可確保真實性、偵測隱藏的變更，並緩解供應鏈竄改風險。

受信賴工作空間和受信賴基礎結構 ›

硬體型的驗證與持續韌體完整性檢查保護端點，在未經授權的變更或惡意植入成為威脅之前向您發出警報。

資產追蹤和 ProSupport Suite 搭配 SupportAssist ›

全方位資產追蹤、即時監控裝置來源以及主動完整性驗證，可確保快速異常偵測與全機隊的安全性。

安全性合作夥伴：採用 AI 技術的偵測與回應 ›

AI 驅動的安全性工具實現持續監控、鑑識調查，以及自動化圍堵竄改或異常的裝置行為，確保對供應鏈威脅迅速採取行動。

攻擊類型：供應鏈軟體

您的公司提供醫院使用的雲端型分析軟體。您的後端服務依賴於一個廣泛使用的開放原始碼記錄程式庫，該程式庫由 GitHub 上值得信賴的第三方開發人員維護。

在您的開發團隊不知情的情況下，攻擊者入侵了 GitHub 帳戶並插入惡意更新，其中包含設計用於以下目的的隱藏程式碼：

- 外洩環境變數，包括應用程式介面 (API) 金鑰與 JavaScript 物件表示法 Web 權杖 (JWT) 密鑰
- 當特定 IP 發出請求時建立反向 Shell
- 除非遠端觸發，否則保持休眠狀態

測試您的知識 →

攻擊類型：供應鏈軟體

1：縮小攻擊面 2 3 4

您的 API 突然開始向關鍵客戶回傳 500 錯誤。雲端監控標記出從容器化服務連到從未見過網域的連出連線。您的第一個回應是什麼？

- [ ] 停用容器的所有連出網路流量
- [ ] 重新啟動受影響的服務，以清除任何記憶體問題
- [ ] 檢查 GitHub 儲存庫中最近的程式碼提交
- [ ] 聯絡該網域的託管供應商

查看正確答案 →

攻擊類型：供應鏈軟體

1：縮小攻擊面 — 2 — 3 — 4

您的 API 突然開始向關鍵客戶回傳 500 錯誤。雲端監控標記出從容器化服務連到從未見過網域的連出連線。您的第一個回應是什麼？

- ✓ 停用容器的所有連出網路流量
- ✗ 重新啟動受影響的服務，以清除任何記憶體問題
- ✗ 檢查 GitHub 儲存庫中最近的程式碼提交
- ✗ 聯絡該網域的託管供應商

停用容器的所有連出網路流量，可立即封鎖攻擊者透過遭入侵的記錄程式庫外洩敏感資料或建立遠端存取，即時隔離您的環境，並爭取關鍵時間進行調查、保護 API 金鑰與密鑰，並防止休眠攻擊機制的啟動。

下一個問題 →

攻擊類型：供應鏈軟體

1 — 2：偵測及因應網路威脅 — 3 — 4

您的工程主管確認應用程式在問題開始前三天從 GitHub 自動拉取程式碼。該版本尚未在任何公開資料庫中標記為惡意。最負責任的即時行動是什麼？

- [ ] 透過 GitHub 直接聯絡程式庫維護者
- [ ] 刪除所有本機專案相依性並重建
- [ ] 等待常見漏洞與揭露 (CVE) 後再採取進一步行動
- [ ] 回復到最後已知安全的程式碼版本

查看正確答案 →

攻擊類型：供應鏈軟體

1 — 2：偵測及因應網路威脅 — 3 — 4

您的工程主管確認應用程式在問題開始前三天從 GitHub 自動拉取程式碼。該版本尚未在任何公開資料庫中標記為惡意。最負責任的即時行動是什麼？

- ✗ 透過 GitHub 直接聯絡程式庫維護者
- ✗ 刪除所有本機專案相依性並重建
- ✗ 等待常見漏洞與揭露 (CVE) 後再採取進一步行動
- ✓ 回復到最後已知安全的程式碼版本

回復到最後已知安全的程式碼版本，可立即移除遭入侵的更新、消除攻擊者的立足點，並還原營運完整性，以主動圍堵風險並保護敏感資料。

下一個問題 →

攻擊類型：供應鏈軟體

1 — 2 — 3：從網路攻擊中復原 — 4

分析可確認程式庫正在外洩 API 金鑰與雲端認證。您已識別出使用遭入侵版本建置的多個容器。在您的圍堵策略中，哪個步驟最關鍵？

- [ ] 在受影響的環境中撤銷並輪換所有認證
- [ ] 使用更新的作業系統 (OS) 映像重新映像容器
- [ ] 抹除開發團隊的筆記型電腦
- [ ] 為 GitHub 儲存庫提交撤除通知

查看正確答案 →

攻擊類型：供應鏈軟體

1 — 2 — 3：從網路攻擊中復原 — 4

分析可確認程式庫正在外洩 API 金鑰與雲端認證。您已識別出使用遭入侵版本建置的多個容器。在您的圍堵策略中，哪個步驟最關鍵？

- ✓ 在受影響的環境中撤銷並輪換所有認證
- ✗ 使用更新的作業系統 (OS) 映像重新映像容器
- ✗ 抹除開發團隊的筆記型電腦
- ✗ 為 GitHub 儲存庫提交撤除通知

撤銷並輪換認證是雲端入侵後的第一個關鍵步驟，封鎖攻擊者存取服務、停止資料竊取，並保護系統，無論入侵範圍如何。

下一個問題 →

攻擊類型：供應鏈軟體

1 2 3 4：整體最佳實務

您必須向技術長與法務/合規團隊解釋發生了什麼事。最準確且清晰的解釋是什麼？您如何總結此事件？

- [ ] 我們的內部持續整合與持續部署/交付 (CI/CD) 工具失敗，允許部署錯誤的程式碼
- [ ] 第三方軟體相依性遭到入侵，我們的自動化作業將其拉入生產環境
- [ ] 開發人員在倉促發布的版本中納入未經測試的程式碼
- [ ] 攻擊者暴力破解了我們的 GitHub 儲存庫

查看正確答案 →

攻擊類型：供應鏈軟體

1 2 3 4：整體最佳實務

您必須向技術長與法務/合規團隊解釋發生了什麼事。最準確且清晰的解釋是什麼？您如何總結此事件？

- ✗ 我們的內部持續整合與持續部署/交付 (CI/CD) 工具失敗，允許部署錯誤的程式碼
- ✓ 第三方軟體相依性遭到入侵，我們的自動化作業將其拉入生產環境
- ✗ 開發人員在倉促發布的版本中納入未經測試的程式碼
- ✗ 攻擊者暴力破解了我們的 GitHub 儲存庫

根本原因是供應鏈攻擊：攻擊者入侵了第三方軟體相依性，而自動化建置流程直接將惡意更新拉入生產環境，進而影響應用程式的完整性與敏感環境，並凸顯可信賴外部相依性中惡意更新的風險。

查看解決方案 →

攻擊類型：供應鏈軟體

重點回顧

供應鏈軟體網路攻擊利用軟體更新、第三方整合與開發環境中的漏洞，嵌入在網路中擴散的惡意程式碼。這些攻擊可能導致大規模資料違規、營運中斷，並入侵整個生態系統，影響各種規模的企業。

Dell 致力於打造網路韌性，強調透明度、安全開發與持續監控，同時維持強健的事件回應計畫，以確保快速復原與利害關係人溝通。

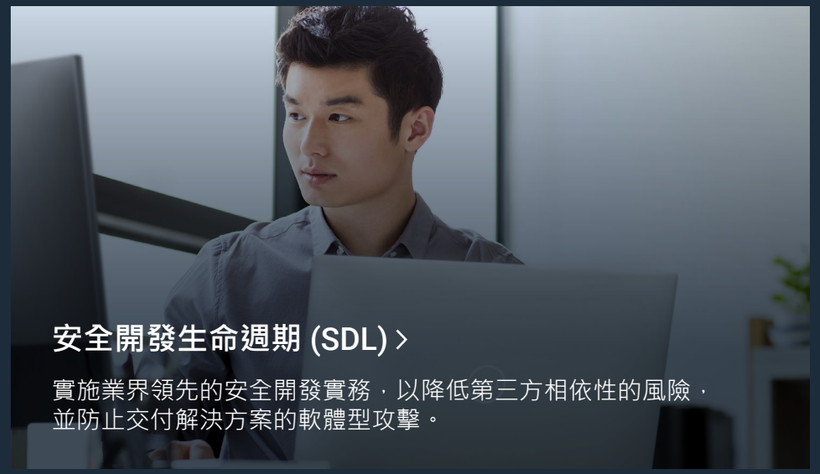
深入瞭解進階的網路韌性策略，並瞭解 Dell 如何協助您保護組織免受供應鏈軟體攻擊。

探索供應鏈軟體攻擊摘要 →

返回情境

供應鏈保證 ›

透過進階的來源追溯、防竄改物流與透明採購，Dell 的供應鏈確保硬體、韌體與供應商在到達您的組織之前經過嚴格驗證。



安全開發生命週期 (SDL) ›

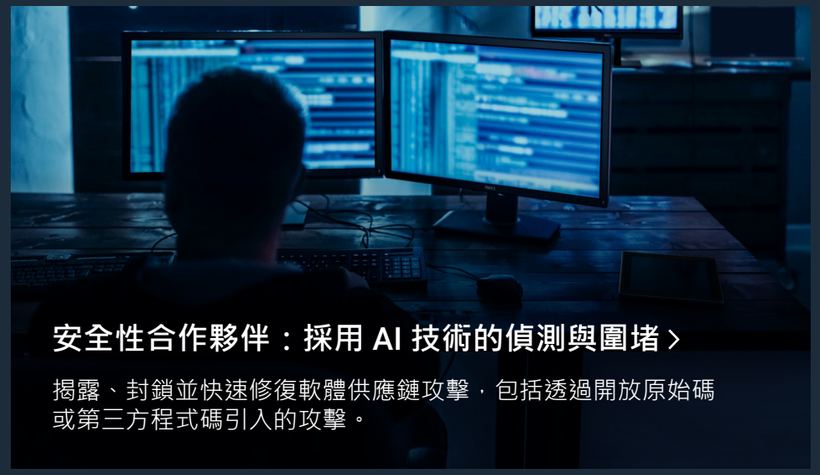
實施業界領先的安全開發實務，以降低第三方相依性的風險，並防止交付解決方案的軟體型攻擊。

受信賴工作空間和受信賴基礎結構 ›

SafeBIOS、SafeID 與 SafeData 提供硬體驗證，協助確保端點僅執行可信賴的程式碼，並提供未經授權或惡意軟體修改的快速偵測。

資產追蹤和 ProSupport Suite 搭配 SupportAssist ›

即時監控裝置與軟體，可快速偵測與回應經供應鏈引入的異常狀況。



安全性合作夥伴：採用 AI 技術的偵測與圍堵 ›

揭露、封鎖並快速修復軟體供應鏈攻擊，包括透過開放原始碼或第三方程式碼引入的攻擊。

攻擊類型：零時差

您是一位監控公司驗證記錄檔的安全性分析師。最近有使用者回報，即使並未分享認證，其帳戶也有未經授權的存取狀況。

在調查記錄檔時，您發現以下活動：

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

同時，一位安全性研究人員識別出應用程式介面 (API) 中的漏洞：

- JavaScript 物件表示法 Web 權杖 (JWT) 永不過期。
- 權杖儲存在本機儲存位置，而非 HTTP-only Cookie。
- 未強制執行多重因素驗證 (MFA)。

測試您的知識 →

攻擊類型：零時差

1：縮小攻擊面 — 2 — 3 — 4

做為安全性團隊，由於沒有警報響起，因此您懷疑這是零時差攻擊，請問要如何確認這一點？

- [ ] 將所有使用者登出其系統
- [ ] 識別記錄檔的重要異常驗證行為
- [ ] 致電其他公司的朋友，看看他們是否遇到相同問題
- [ ] 嘗試與其他安全性異常活動連結

查看正確答案 →

攻擊類型：零時差

1：縮小攻擊面 — 2 — 3 — 4

做為安全性團隊，由於沒有警報響起，因此您懷疑這是零時差攻擊，請問要如何確認這一點？

- ✗ 將所有使用者登出其系統
- ✓ 識別記錄檔的重要異常驗證行為
- ✗ 致電其他公司的朋友，看看他們是否遇到相同問題
- ✓ 嘗試與其他安全性異常活動連結

找出異常驗證行為 (例如異常登入次數、認證重複使用或來自非典型裝置的存取)，並將其與其他異常安全活動 (例如資料存取異常或權限提升) 連結，可確認經協調的零時差攻擊。

下一個問題 →

攻擊類型：零時差

1 — 2：偵測及因應網路威脅 — 3 — 4

由於漏洞未知，安全性團隊必須在調查時限制損害。如何做到？

- [ ] 在系統範圍內使所有驗證工作階段失效
- [ ] 將所有資源集中在攻擊的進入點
- [ ] 僅強制執行多重因素驗證 (MFA) 登入
- [ ] 依賴目前的靜態防火牆或 Web 應用程式防火牆 (WAF) 規則

查看正確答案 →

攻擊類型：零時差

1 — 2：偵測及因應網路威脅 — 3 — 4

由於漏洞未知，安全性團隊必須在調查時限制損害。如何做到？

- ✓ 在系統範圍內使所有驗證工作階段失效
- ✗ 將所有資源集中在攻擊的進入點
- ✓ 僅強制執行多重因素驗證 (MFA) 登入
- ✗ 依賴目前的靜態防火牆或 Web 應用程式防火牆 (WAF) 規則

這些行動共同強化安全性並降低風險，同時切斷攻擊者存取，讓安全性團隊可以調查並解決根本漏洞。

下一個問題 →

攻擊類型：零時差

1 2 3：從網路攻擊中復原 4

Dell 電腦具有安全開機、信賴平台模組 (TPM)、基本輸入/輸出系統 (BIOS) 密碼保護與 SafeBIOS 等技術。這些如何在零時差攻擊中提供協助？

- [ ] 防範竊取應用程式介面 (API) 權杖的認證傾印攻擊
- [ ] 防止具有實體存取權的攻擊者繞過作業系統 (OS) 安全性，安裝竊取驗證權杖的惡意軟體
- [ ] 確保攻擊者無法操縱 BIOS 設定以削弱 OS 安全性，這可能導致 API 工作階段劫持
- [ ] 以上皆是

查看正確答案 →

攻擊類型：零時差

1 — 2 — 3：從網路攻擊中復原 — 4

Dell 電腦具有安全開機、信賴平台模組 (TPM)、基本輸入/輸出系統 (BIOS) 密碼保護與 SafeBIOS 等技術。這些如何在零時差攻擊中提供協助？

- [x] 防範竊取應用程式介面 (API) 權杖的認證傾印攻擊
- [x] 防止具有實體存取權的攻擊者繞過作業系統 (OS) 安全性，安裝竊取驗證權杖的惡意軟體
- [x] 確保攻擊者無法操縱 BIOS 設定以削弱 OS 安全性，這可能導致 API 工作階段劫持
- [x] 以上皆是

這種分層方法提供的全方位保護可針對零時差攻擊，這些攻擊的目標包括 BIOS、韌體、認證與系統組態。透過防止操縱、未經授權存取與認證竊取，即使攻擊者發現新漏洞，這些技術仍然有效。

下一個問題 →

攻擊類型：零時差

1 2 3 4：整體最佳實務

嘗試防止零時差攻擊發生的最佳方法是什麼？

- [ ] 不要使用開放原始碼軟體
- [ ] 利用零信任原則
- [ ] 保持所有內容修補完好，包括作業系統 (OS)、韌體、應用程式介面 (API)、程式庫與容器
- [ ] 在公司周圍架設電氣化閘門，以阻擋威脅行為者

查看正確答案 →

攻擊類型：零時差

1 2 3 4：整體最佳實務

嘗試防止零時差攻擊發生的最佳方法是什麼？

- ✗ 不要使用開放原始碼軟體
- ✓ 利用零信任原則
- ✗ 保持所有內容修補完好，包括作業系統 (OS)、韌體、應用程式介面 (API)、程式庫與容器
- ✗ 在公司周圍架設電氣化閘門，以阻擋威脅行為者

如果存在未知漏洞或未修補的系統，零信任原則可自使用者與裝置移除隱含信任、強制執行持續驗證、僅限制對必要資訊的存取，並圍堵對手移動，來防止零時差攻擊，大幅降低組織面對未發現威脅的風險。

查看解決方案 →

攻擊類型：零時差

重點回顧

零時差攻擊是指在有可用的修補程式或修正之前，利用軟體或硬體中未公開的安全性漏洞。攻擊者會利用這段有機會的時間，因此通常會在漏洞被發現和解決之前，造成大範圍的中斷。

Dell 透過零信任控制、網路區隔、快速圍堵與使用者教育來應對零時差攻擊，進一步強化對新興威脅的防禦。

深入瞭解進階的網路韌性策略，並瞭解 Dell 如何協助您保護組織免受零時差攻擊。

探索零時差攻擊摘要 →

返回情境

受信賴工作空間和受信賴基礎結構 >

防禦端點與基礎結構。透過 SafeBIOS、SafeID、SafeData 保護與零信任框架 (例如多重因素驗證 (MFA) 與角色型存取控制 (RBAC))，Dell 提供分層防禦以限制利用路徑，並確保硬體驗證。

PowerEdge 伺服器 >

安全開機、晶片信任根與 SmartFabric 網路區隔會限制橫向移動，確保僅有受信賴的程式碼在您的基礎結構上執行。

安全性合作夥伴 >

進階的威脅情報、Managed Detection and Response (MDR)、延伸偵測與回應 (XDR) 與精細的存取控制，協助在零時差攻擊擴散之前偵測、搜捕並圍堵。

PowerProtect 產品組合 >

不可變的備份、隔離的網路復原存放庫與 AI 驅動的 CyberSense 分析，確保在零時差入侵後快速還原與恢復韌性。

安全性與復原能力服務 >

從修補程式管理到事件回應，Dell 的專家提供快速圍堵、鑑識調查與韌性規劃，以對抗零時差威脅。


DELL Technologies