網路安全的人力層面

想像最壞的情況。

假設整個資料中心因精密的勒索軟體攻擊而關閉。銷售、客戶服務和財務部門無法運作。您是資深 IT 主管，負責恢復系統，但難以找到合適的解決方案。

您的團隊本來就人手不足，已經連續工作數週，幾乎沒有休息或休假時間。部分從業人員甚至**連續工作長達 36 小時**都沒休息。您開始擔心疲勞可能導致決策有誤，對復原工作本身造成負面影響。

因此，您迫切需要能立即投入的額外人力，來協助解決問題，不過該在哪裡找到這些人力？

這個情況可能聽起來很像小說的開頭，但其實是 Dell 客戶的親身經歷，並凸顯現今網路安全環境的一大問題：人力因素。

最新資料顯示，業界面臨近 500 萬名資安專業人力短缺。當您從更早階段著手採取解決方案，事件發生時就不會迫切需要資源。

從建立和培養人才庫開始

要確保擁有所需人力，第一步是建立人才庫：

大學招募和實習
與當地大學和技術學校合作，可獲得穩定的新進人才來源。這些員工能隨著時間成長為高影響力的團隊成員。

長期訓練與開發
雖然時間和預算持續面臨壓力，網路安全專業人員必須跟上工具和威脅的變化。

專注於留才
業界需要大量優秀從業人員，特別是有攻擊應對經驗的人員。若無法留住頂尖人才，他們會改投入其他公司。

團隊再強大，也可能無法承受管理攻擊的壓力，因此請提前規劃，先找好額外支援以備不時之需：

評估第三方人力
網路安全諮詢和人力派遣公司會在日常營運和事件期間協助您的團隊。即使當下沒有需求，也能與這類公司合作，這樣就能在需要時立即獲得這些人力。

Dell 提供多項服務來強化現有團隊戰力，包括虛擬 CISO (vCISO)、事件回應和網路安全諮詢。

善用 AI
善用網路安全工具內建的全新 AI 功能，例如記錄分析、異常偵測、低階警示分類或專業訓練。這些功能可填補資源缺口並解決作業需求，甚至能讓團隊成員專心處理更高階的任務。

網路攻擊期間的人力挑戰最嚴峻

如本文一開始的假設情境所示，重大網路攻擊可能癱瘓組織，讓主要系統和業務營運停擺。攻擊期間的每分鐘都會導致公司損失金錢，因此網路安全團隊將承受解決問題的巨大壓力。

確保團隊盡可能掌握最新資訊，將直接影響其事件回應成效和相關壓力。

請記住，不只是資安專業人員，其餘所有員工也都必須接受安全性訓練，因為他們是第一道防線。

本文開頭的故事指出一個核心難題：網路防禦人員終究是人類，而人類有極限，因此即使是能力最強大的專業人員，超過極限時也會失敗。精神疲勞、壓力和倦怠是現今網路安全環境的一大問題。

雖然這個問題沒有單一解方，但以下策略可發揮很大效用：

建立強大的團隊和人才庫
建立有備援人力的強大團隊，才能從根本解決精神疲勞、壓力和倦怠，避免這個問題變成緊急狀況。

從人力層面制定攻擊應變計畫
事件回應計畫非常重要，其中必須規劃人員管理方式、排班和休息時間。

利用第三方人力

外部網路安全顧問可以協助您增強團隊戰力。例如，Dell 的事件回應服務會在數小時內，派遣專家團隊到現場立即準備評估、控制並開始修復。我們已協助許多客戶順利度過網路攻擊。

AI 能提供協助，但不是萬靈丹

在增強網路安全工具和程式方面，AI 具有重大潛力，從預測分析到制定專屬訓練計畫都將提供支援，甚至主動防止威脅擴散。

更重要的是，AI 或許還能在事件發生期間，為防禦人員提供即時支援系統。只要使用歷來攻擊資料訓練，機器學習模型即可根據類似的過往事件，提出行動建議。

將自然語言處理技術導入網路安全工具後，分析師將能直接與系統互動、找出威脅並部署解決方案。

此外，AI 也可以監控行為模式，標出人類分析師可能因疲憊而經常出錯的時機，並提示換班或安排他人接手。

雖然網路安全工具正快速整合越來越多精密 AI 工具，但許多最強大的功能仍在開發中。請記住，至目前為止，AI 無法取代經驗豐富且技能熟練的從業人員，**尤其是有攻擊應對經驗的人員**。

運用 **AI** 的建議：

瞭解工具如何協助安全性作業

詳細分析 AI 工具並導入合適的地方，才能發揮最大效用。將 AI 用於偵測進階威脅、自動處理重複性任務或管理身分，都可以很快獲得成效。

制定計畫，以便未來導入新 AI 功能

瞭解新功能何時可用、為團隊帶來哪些助益，並制定導入計畫。

將 AI 納入人力規劃

隨著自動化減少手動任務，安全性團隊人力也需要提升。您可能需要更高階的人力來分析和處理安全性資訊，而非編譯資訊。請隨之調整招募和發展策略。

如果 AI 尚未成為您網路安全營運的關鍵一環，這項技術對相關作業的重要性仍將越來越高。不過請記住，任何技術都無法取代技能熟練且經驗豐富的從業人員。目標應該是使用 AI 自動化作業並提升人力效率，最終防止攻擊並將攻擊發生後的影響降到最低。

推進網路安全成熟度：一步一步來

與網路安全作業一樣，解決人力因素是過程，而非終點。只要逐步努力，即使前進一小步都能帶來改變，並隨著時間累積。重要的是，技術和安全工具再強大，最終仍不會超越操作人員。

> 在實務上，有合作夥伴能隨時提供事件回應、修復和復原服務，是最佳的做法。”
>
> ***Jason Rosselot***
> *Dell Technologies* 網路安全部門副總裁兼業務部門資安長

能夠協助的 Dell 產品和解決方案

精選 Dell 解決方案	說明
事件回應服務	由業界認證網路安全專家組成的團隊，隨時協助組織迅速應對網路攻擊事件。我們會與您共同消除威脅，直到恢復正常營運。
網路安全諮詢服務	透過專家指導，協助您發現並解決安全性策略的盲點、保護資產和資料，以及實現持續監控和治理。
vCISO	虛擬資安長和網路安全專家，可協助找出和管理風險，並指導組織做出策略性決定。
Managed Detection and Response	提供跨端點、網路和雲端的監控、威脅偵測、調查和快速回應功能，協助組織減少手動工作及簡化日常安全性作業。客戶可選擇偏好的 XDR 平台 (Secureworks® Taegis™ XDR、CrowdStrike Falcon® XDR 或 Microsoft Defender XDR)，並獲得專家指導、季度報告和每年最多 40 小時的事件回應服務。

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

DELL Technologies