Acronis Security Services

抵禦現代網路威脅

資料是世界上最珍貴的資源。資料賦予組織實現目標的能量，對組織而言至關重要，因而成為複雜性、數量均不斷增長的網路攻擊覬覦的目標。

為了因應攻擊，許多組織正利用與日俱增的各式安全解決方案。然而，當今的防毒軟體仍會漏阻 57% 的攻擊。技術顯然已不足以防範網路攻擊，實施更全面的安全策略刻不容緩。事實上，每當 IT 基礎架構異動 (例如：部署新的業務應用程式、BYOD 裝置，或是使用雲端服務)，都需要對安全計劃進行審視，因為異動可能會觸發新的攻擊媒介。

組織須應對的課題是，越來越多的法規要求公司制定以隱私為主的程序，或執行強制性安全評估。即便如此，對所有員工逐步培養關鍵技能以及習慣，仍屬當務之急：依據高層主管們的說法，有 47% 的漏洞歸咎於人為錯誤。

複雜又精心策劃的網路攻擊層出不窮，許多前所未見的惡意軟體攻擊持續被開發及運用。組織雖然無法防止每一次攻擊，但可以透過及時偵測攻擊以限縮災害及潛在損失的範圍，並採取行動確保未來不再發生相同的入侵事件。

ACRONIS SECURITY SERVICES

多年來，Acronis 始終提供業界領先的網路資安防護技術。藉由推出 Acronis Security Services，Acronis 也進而提供更全面的網路資安策略。我們目前供應的安全單一產品內容含括了技術、人員與程序，能解決組織 (不限規模) 當前所面臨可靠度、易用性、隱私、真實性與安全的挑戰。

ACRONIS SECURITY SERVICES 優點

安全評估

- 提升組織的安全狀態
- 將修復成本降至最低
- 符合產業法規的要求
- 維持網路資安策略暨藍圖與業務目標一致
- 制定明確的 IT 投資決策
- 訂定減輕風險的修復計劃

安全意識

- 提高人員迎戰網路攻擊的準備程度
- 降低人為錯誤的風險
- 確保遵循法規與既定程序
- 減少請求安全相關支援的次數

事件回應

- 確保業務持續性
- 限縮安全漏洞的損害程度
- 減輕網路攻擊造成的財務與信譽風險
- 將系統停機時間縮到最短

ACRONIS SECURITY ASSESSMENT SERVICE

與時俱進，同步遵循不斷推陳出新的法規，備戰持續攀升的數位威脅。審視您的安全計劃、IT 基礎架構以及預防和偵測控制措施，以利識別安全漏洞與弱點。取得我們網路資安專家的建議，剷除以您的資料為目標的所有攻擊媒介。

您擁有的服務將包含：

- 風險評估 - 依據產業標準 (例如 NIST、ISO/IEC 27001) 評估您目前的安全狀態。評估您的網路資安成熟度以及與第三方相關的風險。凸顯可能形成弱點的安全漏洞。
- 弱點掃描 - 主動識別網路、應用程式和端點中的已知弱點以限縮 IT 環境的攻擊面，進而確保安全的軟體開發生命週期。
- 滲透測試 - 為了識別網路、行動裝置、Web 及應用程式的攻擊媒介，我們的網路資安專家不僅將演練攻擊是如何進行，也會嘗試利用漏洞並繞過安全控制，存取敏感資料。
- 社交工程 - 針對以網路釣魚等技術 (利用電子郵件、電話、媒體投放或實體存取等人為操作方式) 進行的網路攻擊，評估員工克服攻擊的準備程度。
- 修復 - 取得決策摘要和詳細報告，包括合規性以及解決問題、減輕風險的修復計劃 (依據評估技術提供)。

ACRONIS SECURITY AWARENESS TRAINING

安全意識培訓由頂尖的網路資安專家依據您的業務需求量身打造並授課，能推動員工效率最佳化、減輕各種威脅 (包括社交工程入侵)，同時減少因必須先「詳閱本書」而導致的所有延遲。

您擁有的服務將包含：

- 依角色進行培訓 - 針對一般員工、IT 人員、開發人員和高層管理團隊，分別提供從基礎至專家等級的課程，包含合規性培訓以及專為輔導員工準備 CISSP、CEH、CCSK 等證照考試所設計的單元。
- 多重授課選項 - 利用超過 700 個線上單元進行培訓，或依據您的業務和使用者需求量身打造實體課程。

ACRONIS INCIDENT RESPONSE SERVICES

發生安全事件時，Acronis 的網路資安分析師和漏洞調查人員會提供即時的回應。透過對環境與漏洞的肇因進行全面、整體的評估，提供您深入的分析。回應內容也包含提供詳細的修復計劃，確保採取適當的行動進行復原，並協助您的公司管理法規的要求以及任何信譽損失。

您擁有的服務將包含：

- 識別受損資產 - 查明受損的資源，同時找出、分析潛在的受損系統，以利瞭解漏洞的完整範圍。
- 業務持續性 - 隔離威脅，防止威脅擴散。
- 鑑定 – 分析根本原因並收集、保留證據，例如使用 HDD 影像、網路追蹤和記憶體傾印，以進行後續調查和出庭。
- 修復報告 - 取得有關攻擊的詳細報告，包含來源、主機、應用程式、惡意軟體分析和風險概況。我們的專家將規劃並執行詳細的藍圖，確保事件完全修復。報告中也提供了預防未來再發生類似攻擊的建議步驟。
- 成本效益 - 每年可將未使用的事件回應時數轉換為其他服務。