onward SECURITY
a DEKRA company

DEKRA

企業資安健診

針對網路、系統及人員等面向，提供360度全面向的資安檢測服務，藉此強化資安管理制度，並解決資安防護問題，防範潛在的威脅和攻擊，確保企業整體的安全性。

網路安全防護

- 網路惡意活動檢視
- 網路架構檢視

人員安全防護

- 電子郵件社交工程

系統安全防護

- 系統設定與更新檢視
- 網站與系統安全檢測
- 惡意程式檢測

服務特色

涵蓋資安健診3大構面，包括網路安全、系統安全及人員安全防護。

結合自動化工具與人工分析作業，提供專業健診報告與修正建議。

擁有深度檢測技術與專業資安團隊，具政府、金融、工控等產業資安經驗。

彈性化資安健診服務，根據客戶現況及需求，提供客製化方案選擇。

健診項目

系統安全防護

網站與系統安全檢測

針對網站、主機及連網設備等，進行弱點檢測，掃描是否存在已知CVE安全漏洞，與設定不當所造成的安全問題。

系統安全防護

惡意程式檢測

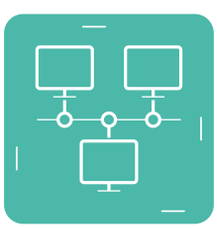
檢視個人電腦與伺服器主機是否存在惡意程式。

系統安全防護

系統設定與更新檢視

依「政府組態基準」所公布安全性檢視之內容為主，以確認機關對於組態設定之落實。

網路安全防護



網路架構檢視

透過網路架構圖呈現網路現狀、網路設備與伺服器的相對位置區域和其IP配置，以供系統管理者未來管理使用。

網路安全防護

網路惡意活動檢視

透過網路封包監聽與網路設備記錄檔分析，瞭解組織網路是否有異常連線狀態。

人員安全防護

電子郵件社交工程

模擬駭客釣魚郵件，檢測員工的資安風險意識及進行行為分析，並提供教育訓練，降低人為失誤造成的資安風險。

進階方案

滲透測試

透過駭客思維，嘗試繞過現有防護機制，找出更多邏輯上的安全問題，協助企業客戶驗證與測試內外部資訊系統的安全強度，瞭解受測目標面臨的安全性威脅、發掘潛在的資安問題，並提供改善建議方案。

紅隊演練

提供單一系統的安全防護強度，並且強調企業邊界網路的防護廣度。以情境為導向的演練目標設定，由安華聯網擔任攻擊方(紅隊)角色，整合情資蒐集、漏洞工具及駭客攻防等技術，驗證企業資安維運團隊(藍隊)對於網路攻擊的偵測與回應能力。

DDoS攻防演練

模擬真實駭客攻擊，能同時控制超過1,000台來自全球超過30個國家的主機進行DDoS攻擊，同時執行多種第四層與第七層網路攻擊手法，並根據客戶需求設計自定義執行時間長度、流量大小、連線數量及封包內容，最高可達同一時間1T的流量。

安華聯網科技(DEKRA德凱集團成員)
Contact us - contract.onward@dekra.com
Learn more at - www.onwardsecurity.com