



黑貓資訊 ICT 資安檢測

全面檢測資安風險，確保產品安全合規

隨著企業數位轉型加速，硬體、軟體與網路服務的安全性變得至關重要。企業在開發與部署過程中，往往因隱藏漏洞、供應鏈風險、未驗證 API 介面等問題，導致資料外洩、系統入侵、惡意程式植入，進而影響營運安全。

黑貓資訊提供 ICT 資通訊安全檢測服務，透過弱點掃描、滲透測試、韌體分析、病毒掃描、程式碼檢測等技術，協助企業全面評估產品與系統的資安風險。我們運用國際資安標準（如ISO 27001、OWASP、NIST），確保檢測結果符合業界規範，並提供詳細報告與修補建議，協助企業強化資安防護。

透過專業檢測，企業可有效降低資安風險，確保產品安全無虞，提升市場競爭力，確保數位轉型與智慧應用的穩健發展。

測試標準與遵循規範



服務功能與特色

服務項目	簡介	功能特色
弱點掃描	 快速檢測安全漏洞 提供修補建議	利用自動化弱點掃描工具，檢測系統與Web應用程式中的已知安全漏洞，提供完整風險報告與修補建議，確保產品在開發與部署前即具備良好的安全性。
滲透測試	 驗證漏洞風險 強化防禦策略	透過模擬駭客攻擊手法，針對網路服務、API、Web 應用程式進行滲透測試，驗證產品是否存在可被利用的漏洞，並提供詳細的攻擊路徑分析與防禦強化建議。
韌體分析	 檢測潛在風險 確保設備安全性	針對 ICT 設備進行韌體安全檢測，分析是否存在預設密碼、金鑰明文、不安全函式等潛在資安風險，確保設備符合資安標準與法規。並能透過韌體逆向解碼SBOM，確認開源元件是否存在已知漏洞或授權問題
病毒掃描	 偵測隱藏威脅 確保系統無後門風險	利用惡意程式檢測技術 -YARA rule，搭配防毒軟體，針對韌體、應用程式、可執行檔進行病毒與惡意程式掃描，偵測是否遭受感染或潛藏風險，確保產品無後門程式或隱藏攻擊機制。
源碼掃描	 預防漏洞風險 確保開發階段符合資安標準	透過程式碼靜態分析技術 (SAST)，針對 Web 應用程式、行動應用、後端伺服器進程式碼安全檢測，找出 SQL 注入、跨站攻擊 (XSS)、權限驗證漏洞等程式碼層級問題，確保開發階段即符合資安最佳實務。

