精誠軟體服務
SYSTEX Software & Service

資安合規稽查 套件包

資安是個複雜且多變的議題，現今駭客的首要攻擊目標通常為程式漏洞，這是因為企業組織在採用多樣的作業系統、網站和應用程式，但沒有被確實的修補。為強化系統的作業安全性，有效防止惡意攻擊並偵測可疑活動。透過漏洞檢測、安全組態檢測、網站組態檢測及高風險軟體檢測，從中提供全面的可見性評估威脅和漏洞的補救並建議或提供適用的修補程序的資安解決方案，使其不受新興威脅的危害。

商品特色

- **漏洞評估**
  透過工具檢查作業系統漏洞，第三方漏洞，零日漏洞。
- **安全配置評估**
  透過工具檢查默認憑證，防火牆配置，未使用的帳號和群組，特權提升，開放共享。
- **Web服務器配置評估**
  透過工具與 DDoS 相關的配置，未使用的網頁，錯誤配置的 HTTP 標頭和選項，目錄遍歷，過期的 SSL / TLS，跨站點 Scripts。
- **高風險軟體檢視**
  透過工具檢視是否有 End-of-life 軟體，遠程桌面共享軟體及點對點軟體。
- **主機系統網路埠清查**
  透過工具清查各系統已開啟之網路埠。

商品功能

威脅項目	報告產出
軟體漏洞識別	• 列出缺少的修補程序和部署的概述報告，提供企業保護 IT 資產採取修補的依據。
零日漏洞識別	• 列出經識別零日漏洞威脅項目。 • 提供相關資訊或變通做法。例如更改註冊表值，關閉易受攻擊的端口，禁用舊協議等。
系統設定弱點識別	• 列出與標準差異的報告清單。例如：SSL / TLS , UAC 配置…
高風險軟體識別	• 列出已安裝高風險軟體報告。
網頁伺服器設定弱點識別	• 列出檢測到的 Web 服務器配置錯誤項目。 • 提供建議修正建議。
主機開啟已網路埠識別	• 列出環境中已開啟網路埠的主機與對應服務。

精誠軟體服務 聯絡窗口｜(02) 23670188 # 6872 digitalmk@systexsoftware.com.tw 王小姐