Spirent **SecurityLabs**

Spirent **SecurityLabs**

Comprehensive security testing and monitoring services

利用我們的專業知識識別並減緩漏洞

測試並分析您的網路、應用程式和設備的安全性和合規性至關重要。但是，內部資安測試不一定需要內部人員來測試。

由持證專家提供的客製化服務

Spirent SecurityLabs 提供各種綜合性的託管測試服務，由經過認證的經驗豐富的專業人員提供。我們的安全顧問作為您內部安全團隊的延伸，主動識別漏洞並減輕風險。透過 SecurityLabs 專家來增強您的團隊可以幫助您優化人員配置，補充內部專業知識，並通過獨立的協力廠商測試和報告促進合規性。SecurityLabs讓您接觸到經驗豐富、獨立的測試專家團隊；他們擁有與您公司類型、規模和產業相符的豐富經驗，並擁有符合您特定需求的認證。

我們的測試專業人員可以協助您進行以下工作：

- 手動滲透測試 測試網路基礎設施、Web和行動裝置應用程式、嵌入式設備和原始碼
- 自動掃描和報告 通過一個獨特的統一 SaaS 平臺進行自動掃描和報告，提供對組織 IT 基礎設施的掃描、分析和監控的持續可見性
- 合規性 通過獨立的、定制的、自動化的、隨需測試實現持續合規性的測試（PCI、GDPR、GLBA、HIPPA、SOX等）和CTIA IoT
- 特定漏洞測試 涵蓋各行業和地理區域的行業特定漏洞測試
- 提供諮詢服務 從實施最佳實踐的測試方法到潛在攻擊情景的風險分析到緩解策略，客製化的掃描配置，以符合客戶預算和測試需求

Case Study

客戶使用場景案例

大型區域醫院

對醫療設備、應用程式、外部和內部網路進行滲透測試

•對大規模IP範圍/基礎架構進行網路滲透測試（Class-B大小的網路，數千個用戶）

•採取適當的預防措施，內部協調，避免對實時臨床系統和患者安全造成影響

•伺服器端和客戶端漏洞測試

•執行了嵌入式醫療設備測試和移動應用程式測試，幫助識別漏洞並建議補救措施

國際鐵路公司

紅隊測試

•使用徹底的偵查過程識別隨機的內部功能變數名稱

•侵入外部網路，並在遠端獲取內部網路訪問權的同時不觸發任何IDS / IPS /防火牆 / AV / SIEM警報

•繞過各種安全控制，入侵內部網路，獲取對關鍵資料和系統的訪問權

金融服務公司

滲透測試

• 大型 IP 範圍/基礎架構的外部網路滲透測試

• 在內部進行適當協調以避免對實時系統產生影響

• 執行非認證和認證的 Web 應用程式滲透測試，以幫助識別漏洞並提出修復建議

政府機構

外部滲透測試、內部滲透測試、無線網路評估

•主要和次要數據中心的外部網路滲透測試和漏洞掃描

•內部網路、伺服器和用戶端系統的滲透測試和漏洞掃描

•無線網路安全評估和偽裝訪問點偵測/映射

About Us

www.spirent.com

Youtube: @spirentvideos

Terillogy Technology CO., LTD

www.terilogy.com.tw

新北市中和區中正路920號7樓

sales@terilogy.com.tw

02-2226-6269

Spirent SecurityLabs Certifications

為什麼SecurityLabs獨特？

SecurityLabs的顧問們深入研究網路安全，不斷擴展其專業知識的深度和廣度。我們實施和測試先進的方法，探索新興領域，如無人機、物聯網和加密貨幣，並擁有多個行業部門的經驗，包括**汽車、醫療保健、工業系統（ICS/SCADA）**等。

We do not work for you; we work with you

提高安全性需要您的內部團隊和我們的顧問之間的積極合作。我們會主動與你的團隊分享我們的知識和經驗。

SecurityLabs已被委託測試許多政府系統的安全性，包括關鍵國家基礎設施的元素，如電信、能源和公用事業以及運輸，我們擁有測試機密和軍事系統所需的安全許可證。

手動滲透測試能力

Web應用程式 - 在所有關鍵領域進行網路應用程式的全面滲透測試和任何相關的主機，如輸入驗證、注入、釣魚、身份驗證機制、會話安全、加密使用、策略合規性等等。

行動裝置應用程式 - 對行動設備應用程式的二進制代碼進行滲透測試，以動態分析和設備端安全性，以揭示與敏感數據儲存在緩存中，未加密數據儲存在設備上、日誌文件、Crash logs、SQL注入、不受限制的文件上傳會話安全、加密使用、支持的密碼、中間人等方面有關的安全漏洞。

網路和無線 - 對網路/無線進行深入掃描和滲透測試，以發現有關不安全的服務器配置、預設系統密碼、已知漏洞的未打補丁服務器、Rogue access points、War Driving、Eavesdropping、不安全的防火牆配置、不安全的通訊、資訊泄漏和不當錯誤處理方面的可利用漏洞。

靜態代碼分析 - 代碼審查服務是白盒測試的一部分，用於識別難以找到的漏洞，例如緩沖區溢出、SQL注入漏洞、後門、身份驗證繞過和授權邊界等。我們使用諸如污點分析和數據流分析之類的技術，在“靜態”（非運行）原始碼中檢查這些漏洞。

進階測試能力

紅隊 - 我們可以通過挑戰其策略，流程和IT系統並引入對抗方法來評估整個組織的安全性。紅隊測試始終是以目標為驅動的，模擬現實世界的情況，例如複製敏感資訊、訪問受保護的範圍等。紅隊測試使用各種物理，電子和社交工程技術，試圖利用您的人員和任何物理弱點來獲取進入設施的權限。

物聯網和嵌入式設備（POS/ATM/汽車）——嵌入式設備的滲透測試包括設備硬體評估、韌體提取和逆向工程、通信分析（有線和無線）、加密分析、任何相關Web服務的分析以及用於可利用的漏洞（例如身份驗證繞過、授權邊界、注入攻擊等）的設備管理應用程式。

About Us

www.spirent.com

Youtube: @spirentvideos

Terillogy Technology CO., LTD

www.terilogy.com.tw

新北市中和區中正路920號7樓

sales@terilogy.com.tw

02-2226-6269