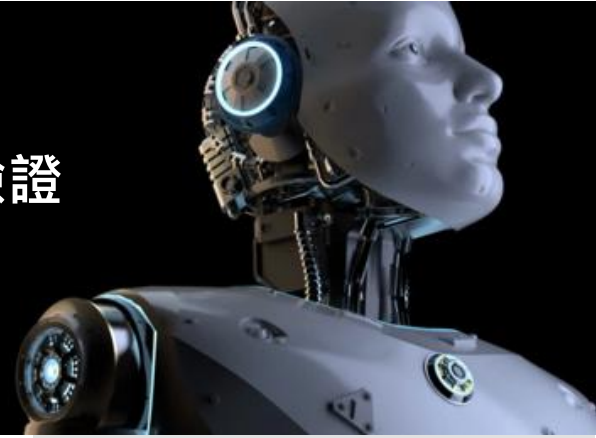


RidgeBot® AI 驅動的全天候安全驗證

CISO 信賴的 AI 安全平台，7x24 全天候保護您的企業



許多組織會利用滲透測試來驗證網路安全狀況。在這類測試中，安全測試人員扮演攻擊者的角色，盡全力嘗試入侵組織的資訊環境，以尋找任何漏洞，並分析這些漏洞在真實駭客攻擊中被如何利用。

在現今攻擊者不斷開發新的漏洞和攻擊方法的情況下，企業的安全團隊和專業的「滲透測試人員」面臨巨大的壓力。Ridge Security 正在透過智慧資安驗證機器人 RidgeBot® 改變遊戲規則。RidgeBot® 結合了對威脅、弱點與漏洞利用技術的集體知識，並配備最先進的駭客攻擊技術，RidgeBot® 就像真正的攻擊者，持續不懈地尋找、利用漏洞並記錄其發現結果。RidgeBot® 自動化滲透測試，使其能夠以更經濟的方式運行，並具備大規模測試的能力，它們在定義的範圍內運作，應對高度複雜的環境結構。

- 提升安全測試的覆蓋範圍與效率
- 降低安全驗證成本
- 持續保護 IT 環境
- 提供可執行且可靠的結果，滿足不同團隊角色的需求

在漏洞被利用之前先將其揭露

RidgeBot® 讓您在攻擊者利用漏洞之前率先發現它們，搶占先機。不同於傳統掃描工具僅辨識風險，RidgeBot® 可以更進一步——安全、實際地執行漏洞利用，提供真實、確切的入侵證據。透過 AI 驅動的持續滲透測試，RidgeBot® 模擬駭客手法，挖掘可能導致資安事件的弱點。在最終的結果階段，提供您可執行的報告，幫助您優先處理並修補關鍵威脅，避免發展成代價高昂的安全事件。

RidgeBot® 可自動掃描、驗證並安全地測試您 IT 環境中的漏洞，提供確切的證據。讓您不用再依賴猜測，消除誤報——RidgeBot® 透過明確、資料佐證的證據，向您分析防禦系統的弱點。別等攻擊發生才行動，透過 RidgeBot® 搶先應對網路威脅，確保您的資安防線萬無一失。

RidgeBot® 與眾不同

- ✓ 全自動且持續運行
 - ✓ 無代理、即插即用
 - ✓ 零誤報風險發現
 - ✓ 可排程或依需求執行
 - ✓ 無需高技能專業人員
-
- 超過 36,000 筆外掛程式資料庫
 - 比人工測試快 100 倍
 - 已測試超過 100,000 項資產
 - 已對 1,000 個以上網站進行滲透測試



用 RidgeBot®達成持續威脅暴險管理 (CTEM)

傳統的安全評估無法跟上漏洞被利用的速度，一次性的測試是不夠的，企業需要持續自動驗證自身的安全狀態，以實現「持續威脅暴險管理 (CTEM)」目標。

2022 年 Gartner 首次提出「持續威脅暴險管理(CTEM)」架構，旨在以駭客視角管理企業暴露的風險面。CTEM 透過識別、評估、排序、驗證和修復攻擊風險，幫助組織在攻擊者利用漏洞之前，主動管理內外部威脅的影響。RidgeBot®支援 CTEM 架構，可提升您的安全性與運作效率。

CTEM 目標	RidgeBot® 功能	優點
資產發現與盤點	自動對應網路、Web 應用程式、OT/IoT、API 和雲端環境的攻擊面。	消除盲點，確保所有資產皆受管理，不留任何漏洞。
持續攻擊面測試	AI 驅動的滲透測試與漏洞利用，內建超過 36,000 種外掛程式。	持續發現安全缺口，降低合規風險。
威脅模擬和風險驗證	模擬真實駭客攻擊行為（入侵與攻擊模擬(Breach and Attack Simulation, BAS)及紅隊演練）。	將安全團隊專注於真正的威脅上而不是誤報，進而提高工作效率。
自動修補與回應	根據漏洞可被利用程度與業務影響確定風險的優先順序，並與 DevOps 或 SecOps 系統整合。	優先修補高風險漏洞，加快應對速度並降低資安事件成本。
適應性安全與威脅情報	AI 驅動的即時安全驗證，且與 MITRE ATT&CK 框架對應。	主動防禦不斷演變的威脅，讓安全防護始終領先一步。

速度很重要，網路威脅發展迅速

RidgeBot®比它們更快



無需繁瑣的操作也可以擁有無懈可擊的安全防護

不同於傳統的滲透測試或掃描技術，RidgeBot®可 7x24 持續評估、辨識、驗證並優先處理整個 IT 環境中的威脅。作為一個全自動、AI 驅動的持續威脅管理平台，RidgeBot®不僅能發現漏洞，還可以利用漏洞讓您了解潛在危害，協助您優先修補關鍵風險。

網路和應用程式測試

- > 掃描並驗證作業系統、資料庫和應用程式的各種外掛程式。
- > 在攻擊者行動之前，先行識別可被利用的網路服務漏洞。
- > 安全地的模擬真實攻擊，驗證風險暴露情況。

登錄身分驗證後的 Web APP 測試

- > 以真實使用者登入進行深入的安全評估。
- > 辨識身份驗證缺口、會話劫持(Session Hijacking)風險及 OWASP 前十大威脅。
- > 模擬真實的攻擊路徑，提供入侵證據與風險優先排序分析。

登錄身分驗證後的 API 測試

- > 驗證並測試 API，揭露端點與資料交換中的安全漏洞。
- > 偵測漏洞，如身份驗證失敗、注入攻擊與錯誤設定。
- > 透過安全地模擬攻擊來驗證漏洞可利用性，確保 API 整合安全無虞。

RidgeBot®全自動執行攻擊測試流程。當它連接到您的 IT 環境時，RidgeBot®會自動偵測網路中所有不同類型的資產，透過漏洞資料庫深入分析目標系統。一旦發現漏洞，RidgeBot®會使用內建的駭客技術與攻擊模組，對漏洞發起真實攻擊測試，如果攻擊成功，該漏洞將被驗證，並完整記錄整個攻擊過程。RidgeBot®提供您詳盡的風險評估與優先排序分析，並提供漏洞分析、修補建議與風險報告。

與傳統掃描的主要差異

比人工測試快

100 倍

特徵

漏洞驗證

誤報

改善資安態勢

傳統掃描

無

常見

受限的

RidgeBot®

有

消除誤報

持續的

將安全挑戰轉變成斷行行動

自動滲透測試



監控一切，保護一切

全面資產發現

RidgeBot®會自動識別裝置、應用程式和網站，因此您可以全面了解您的 IT 環境，確保所有資產受到保護。

風險性漏洞管理

安全控制驗證

資產管理



比攻擊者先發現並修復漏洞

主動漏洞掃描

利用 RidgeBot®的 AI 偵測發現隱藏的弱點，確保您的安全團隊專注於真正的威脅，而非誤報。



透過真實測試驗證風險

遵循白帽原則並驗證風險

藉由安全的 AI 驅動攻擊模擬，了解哪些漏洞真正可被利用，幫助您優先處理需要修復的問題。



更智能的威脅偵測，更強的安全防護

AI 驅動的漏洞識別

利用進階的載荷測試與風險模型，偵測真實世界的攻擊模式，提升企業對未知威脅的預警與防禦力。



掌握整面攻擊面

持續暴露管理

無論是依照需求還是排程執行，RidgeBot®監控您整體 IT 環境，包括 IP、網域、應用程式、資料庫及 OT 裝置，確保沒有任何盲點。



將資料轉化為可執行的建議

智能報告與修復建議

RidgeBot®提供已經過排序、明確的建議，幫助您更快速地進行修復並達到更強的安全防護，協助團隊迅速應對並降低風險。



模擬攻擊，真實防禦

真實的入侵模擬

RidgeBot®模擬多向量網路攻擊，向您展示駭客如何入侵，讓您及時強化防禦，防患於未然。



專注最大的風險，而非最吵雜的警報

自動化風險優先排序

即時將攻擊鏈和駭客的潛在入侵路徑視覺化，確保您的團隊優先處理最關鍵的威脅。

代理商 欣盟科技有限公司

SPHINXTEC 欣盟科技

all about data security

Tel: 03-6682708

<https://www.sphinxtec.com/>

CustomerCare@sphinxtec.com