



ThreatSonar Plus

全方位端點風險檢測平台

發掘端點關鍵風險，及早防範安全威脅

隨著 AI 代理快速整合至企業端點與工作流程，資安邊界已然改變。在自動化攻擊頻傳的威脅下，企業風險已不再侷限於系統漏洞，更延伸至 AI 代理的權限使用與行為風險。企業需要系統化檢測，同時掌握端點與 AI 代理所帶來的整體風險。

一次檢測，掌握端點與 AI 代理風險

ThreatSonar Plus 為全方位風險檢測平台，以「資產盤點」與「風險偵測」為核心，協助企業在單次檢測中，全面盤點端點資產與 AI 代理使用情況。平台可同時識別系統、軟體、應用程式與 AI 代理，分析其潛在風險，包括資料存取、指令執行與權限配置，同時結合漏洞資訊、風險評分與資產重要性，協助判斷風險優先順序，並將檢測結果運用於後續改善、治理與稽核。

主要效益

- **快速識別端點風險，優先處置**
一站式檢測，全面掌握端點與 AI 代理風險
- **提升修補效率，縮短曝險時間**
比對已遭野外利用的高風險漏洞，及早修補以降低攻擊風險
- **強化設定安全，符合國際標準**
依據 CIS 基準檢查系統設定，提供改善方向
- **涵蓋 SEMI E187，支援合規評估需求**
自動化檢測 SEMI E187 四大面向，評估報告一目瞭然

四步驟快速評估風險



核心特色

AI 代理多維度風險檢測

ThreatSonar Plus 針對 AI 代理帶來的自動化威脅，基於具公信力的 OWASP AI 代理風險分類並採用其 AIVSS 評分機制，提供全方位檢測與評估方案，協助企業掌握從機敏資料暴露到惡意技能與指令的潛在風險。

機敏資料曝險

羅列出 API 金鑰、憑證與機密資料存放位置，掌握端點中可能暴露的機敏資訊。

惡意技能識別

辨識第三方與開放原始碼技能，辨識其中可能夾帶的後門、惡意程式碼，以及下載或執行惡意程式的風險。

隱蔽指令分析

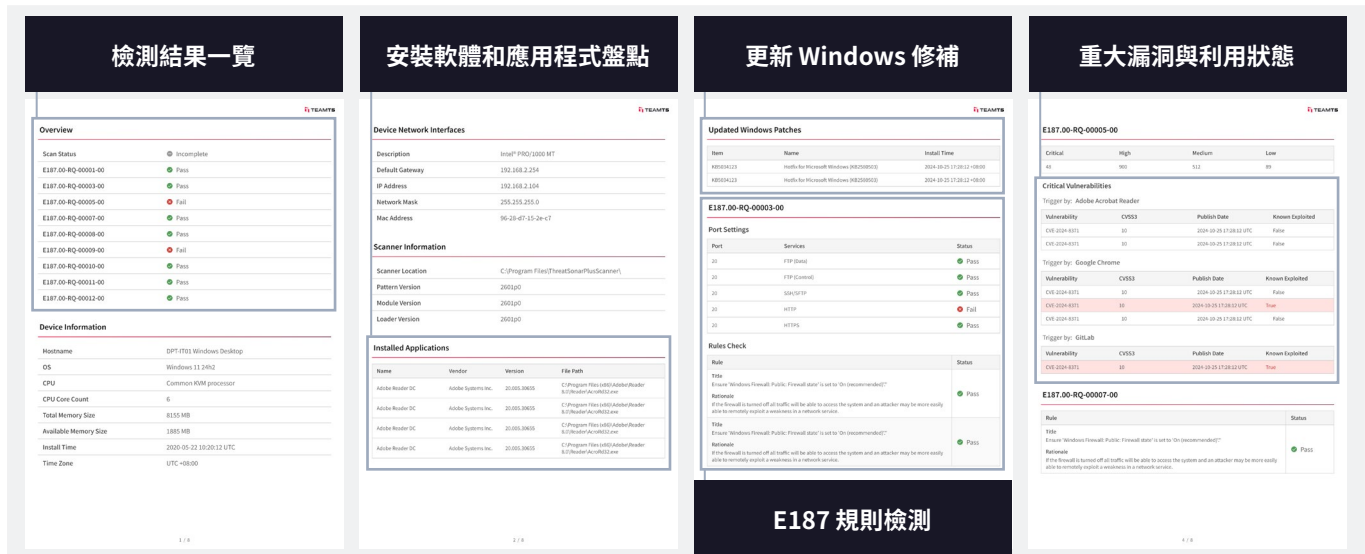
解析 AI 代理相關工具說明與設定內容，找出隱藏指令、危險指令或其他可疑內容。

權限與存取範圍評估

檢視 AI 代理的權限與工作範圍，找出可能超出任務需要的存取設定。

SEMI E187 合規檢測

ThreatSonar Plus 提供自動化風險與合規檢測，涵蓋 SEMI E187 四大安全要求，包括作業系統規範、網路安全、端點防護安全與資訊安全監控，可檢查作業系統支援狀態、網路傳輸協定、連接埠及端點防護設定，快速識別潛在風險與不符合規範項目。完成檢測後，可自動產出標準化合規報告與風險摘要，呈現檢測結果與改善建議，降低人工查核成本，協助半導體設備商掌握設備安全狀態，作為 SEMI E187 合規評估與持續改善依據。



功能

資產全面可視，掌握 AI 代理使用

資產盤點為風險評估的基礎，除涵蓋端點設備、作業系統與應用程式外，亦納入 AI 代理的部署與使用情境。企業可透過檢測建立完整的資產可視性，掌握 AI 代理在環境中的部署與使用狀況，作為後續風險分析與管理依據。

多維風險檢測，全面掌握端點風險

風險偵測涵蓋端點漏洞與 AI 代理使用情形，協助企業全面掌握潛在風險。在 AI 代理風險方面，系統可檢視其相關設定，分析可能涉及的風險。在漏洞偵測方面，系統依據資產資訊轉換為 CPE，並比對 CVE 資料庫，提供完整漏洞資訊與風險評估依據。在安全配置方面，依據 CIS 規範檢查端點設定，確認是否符合安全基準。

彈性部署，適用多元環境

ThreatSonar Plus 提供連線與離線部署模式。連網設備可於檢測後自動上傳結果，離線設備則可透過手動方式匯入分析。同時提供免安裝版本，可透過可攜式裝置執行檢測，不在受測設備上產生任何資料，也不會變更環境設定，兼顧安全性與操作便利性。

關於 TeamT5

v.202609

廣受全球 550 家以上客戶信賴，橫跨政府單位、科技、製造、金融、醫療、軍事、電信等產業。

頂尖專家團隊

團隊成員常在世界級資安會議中發表最新頂尖研究，包含臺灣 HITCON、美國 Black Hat、日本 Code Blue / AVTOKYO、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST，於威脅情資研究與資安先進技術領域擁有世界領先地位。

外界肯定

獲得美國 Bloomberg 及 CNN、日本產經新聞及朝日新聞、韓國 ET News 等採訪報導。更於 2022 年獲得日本三大巨頭投資，包含日本最大創投 JAFCO 集富集團、日本最大跨國企業並在全球皆有商業投資的 ITOCHU 伊藤忠商事，與日本最大資安解決方案提供商 MACNICA。