Datasheet

ThreatSonar

TEAMT5

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 代理賦予端點存取資料與執行指令的能力，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，並結合漏洞資訊、風險評分與資產重要性，協助判斷風險優先順序。

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**
  追蹤漏洞、提供修補建議，降低零時差攻擊風險
- **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，滿足合規需求**
  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

有哪些資產？	已存在的風險？	需優先關注的風險？	如何精準處置？
資產盤點 掌握環境內有哪些端點設備、安裝軟體、作業系統與 AI 代理使用情況。	**掌握風險** 辨識漏洞、錯誤設定與 AI 代理的潛在風險。	**輕重緩急** 依威脅等級，掌握風險處置優先順序，提升效率。	**應對決策** 提供風險說明與修補措施建議，協助後續處置與應對決策。

核心特色

AI 代理多維度安全防護

ThreatSonar Plus 檢測 AI 代理帶來的自動化威脅，提供從機敏資料保護到惡意指令追蹤的完整防護方案。

機敏資料防護

自動識別 API 金鑰、憑證及機密資料存放位置，防止 AI 代理執行任務時誤用或外洩核心資產。

惡意技能偵測

深度分析第三方 AI 技能，精準辨識隱藏後門與惡意邏輯，確保自動化工具鏈安全合規。

隱蔽指令分析

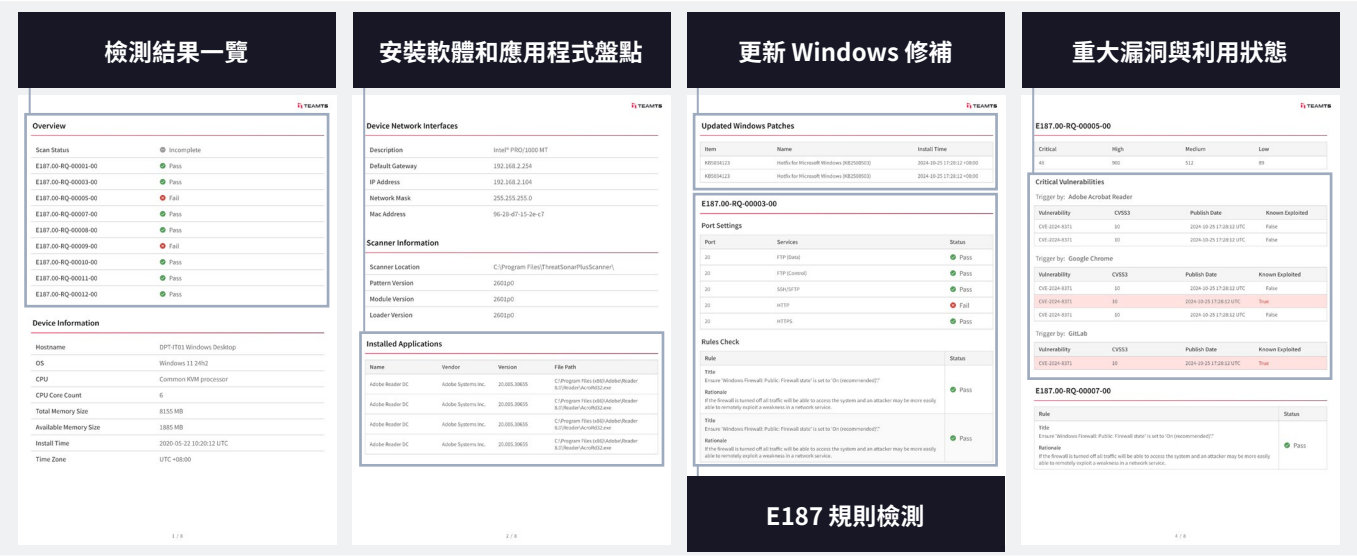
即時監控 AI 生成的系統指令，攔截潛在的惡意行為與指令注入，阻斷自動化攻擊跳板。

最小權限控管

評估並限制 AI 代理的存取範圍，確保其嚴格遵循最小權限原則，消除資安管控盲區。

SEMI E187 合規檢測

ThreatSonar Plus 的自動化風險評估，完整涵蓋 E187 的四大檢測項目——作業系統規範、網路安全、端點防護安全、與資訊安全監控。可檢查作業系統是否仍受原廠支援、分析網路傳輸協定（如 HTTPS、SFTP）與連接埠設定安全性。
根據檢測結果，自動產出標準化報告與風險摘要，藉此協助半導體廠商快速發現並修補漏洞，達成 SEMI E187 的合規要求。



功能

全域資產與 AI 代理盤點

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。

整合式風險偵測與威脅分析

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，系統可檢視其設定與行為模式，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，易於操作

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，兼顧安全性與操作便利性。

關於 TeamT5

v.202605

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。

Tel 02-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA