Datasheet

ThreatSonar ANTI-RANSOMWARE

TEAMT5

洞悉網路威脅攻擊
完整端點縱深防禦

ThreatSonar Anti-Ransomware 威脅鑑識分析與回應平台

企業、政府和組織資安團隊在防護、偵測與應對威脅攻擊時，面臨多重挑戰，例如：

- 如何有效地將縱深防禦擴展至端點，達到有效佈署多層次的威脅偵測與防禦解決方案？
- 在有限的威脅偵測能力下，面對進階攻擊、零時差漏洞被利用，該如何因應？
- 面對可疑威脅和攻擊事件，如何有效地在第一時間應變與調查，即時緩解事件造成的影響？

五大效益

- **有效資安防護**
  高偵測覆蓋率，精準阻擋潛在威脅。
- **縮短應變時間**
  自動分析入侵威脅，加速事件處理。
- **緩解警報疲勞**
  協助資安人員過濾雜訊，將時間專注在高風險事件。
- **減輕人力偵測負擔**
  自動化智慧威脅獵捕，主動發現環境中潛伏的威脅。
- **事件緩解，減少損失**
  防堵橫向移動，修補威脅損害。

情資驅動端點安全防護，強化防禦威脅攻擊

TeamT5 團隊長期研究全球威脅情資與追蹤惡意程式，深知企業、政府與組織的資安威脅防禦需求，開發 ThreatSonar Anti-Ransomware 威脅鑑識分析與回應平台，以領先情資持續預測未來攻擊，並全時監控異常行為，聚焦防堵進階持續性威脅（APT）、惡意軟體（malware）與勒索軟體（ransomware）。一旦偵測到威脅入侵，發出即時警告、阻斷攻擊行動，有效回應威脅事件，降低入侵造成的損害。

藉由 ThreatSonar Anti-Ransomware 平台，可實現符合 NIST CSF 網路安全框架的資安部署，達到完整縱深防禦。

Identify 識別	Protect 保護	Detect 偵測	Response 回應	Recover 復原
藉由威脅情資，掌握威脅與端點風險的全貌	針對已知與未知威脅行為，提供自動化的威脅防護，事前阻斷威脅	透過即時偵測或排程掃描，及早發現可疑檔案或行為	事件管理與報告一目瞭然，提升管理效率，快速進行事件處置	系統回復運作，並藉由事件分析結果進一步改善資安防禦對策

核心特色

端點全面防禦

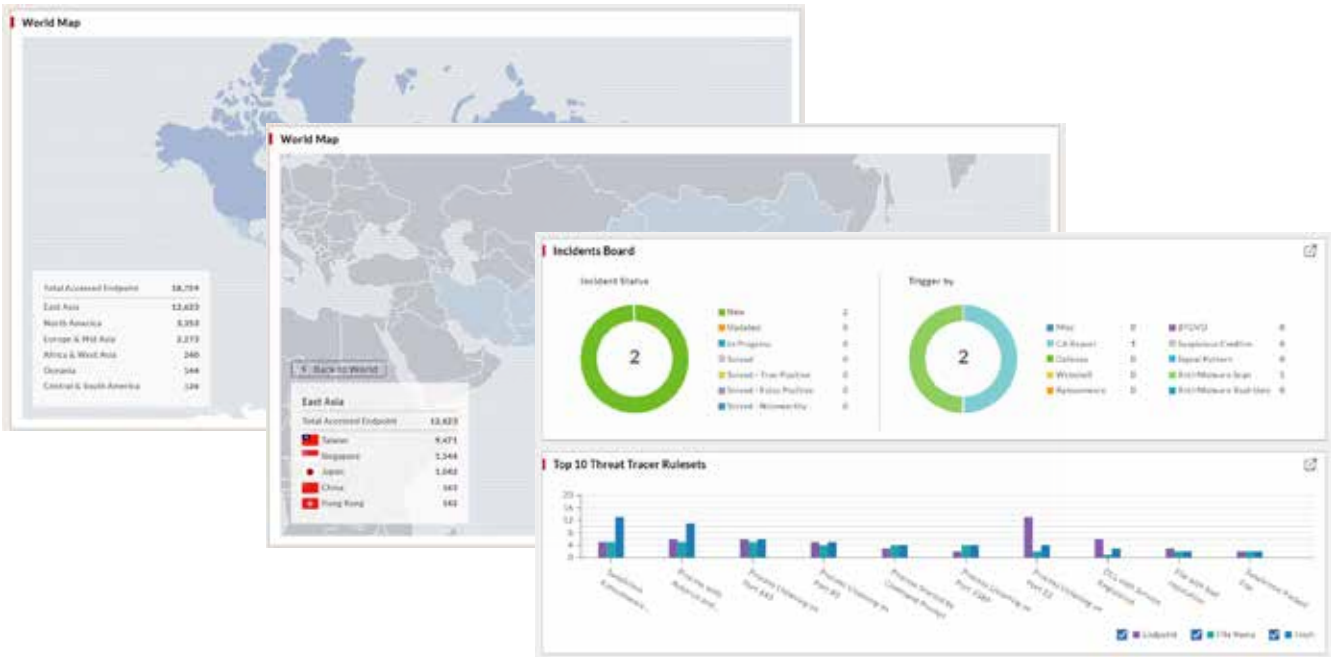
- 結合 Anti-Ransomware 與 Anti-Malware 的 EDR 平台，多層次防護
- 藉由引擎自我學習機制，自動判斷常用程式或新進惡意程式，有效掃描被加密檔案
- 行為分析提升精準防禦，降低誤報
- 全時監控，即時阻擋加密勒索攻擊，保護備份檔案安全

自動化防禦與主動獵捕雙管齊下

- 惡意程式與惡意行為雙重偵測
- 自動化防禦快速過阻已知威脅
- 主動獵捕未知攻擊手法

高效、彈性部署

- 單一掃描程式，快速部署，避免系統衝突
- Anti-Malware 資料庫自動更新，不中斷日常運行
- 支援雲端與落地部署，滿足不同部署需求



功能

對應 MITRE ATT&CK® 加速調查攻擊行為，強化資安策略

當攻擊發生時，可即時對應 MITRE ATT&CK® 框架，透過其已知的技術和戰術的關聯，資安團隊可即時掌握攻擊行為過程中的戰術、技術和程序（TTP），查看自身對某些惡意族群的防範措施是否確實。

可視化網路攻擊鏈，快速識別事件軌跡

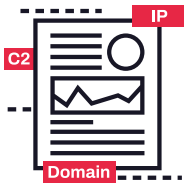
藉由圖像化攻擊發生路徑，查找事件軌跡，並且根據事件資訊標籤，方便資安事件分析人員快速識別，並深入了解攻擊者的行為，進行緩解處置。

時間軸呈現事件全貌，縮短事件調查時程

可透過 Timeline 事件時間軸，呈現先後事件紀錄分析，加速調查事件軌跡。時間軸呈現方式有兩種，一為以節點為主體，查看單一節點執行的時間序；二是以事件為主體，查看報告內每個事件發生的時間序。

ThreatSonar 如何全面防堵勒索攻擊？

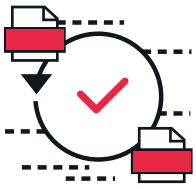
事前保護 → **事中偵測** → **事後處置**



情資
風險精準預測

端點
監控新進程式

阻擋
即時自動阻斷



還原
保護備份檔案

關於 TeamT5

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

v.202605

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA