Search

Surveillance

Survey

ThreatSonar
Advanced Threat Detecting Platform

端點智能威脅鑑識系統

前言與概述

駭客威脅持續發生，多數客戶受到進階式滲透威脅攻擊(APT)也不斷升高，為過止此類惡意侵入危害，企業每年投注愈來愈多的設備預算與人力，仍難以有效地發覺或扼止問題的發生，當攻擊事件被披露時，往往已是環境遭感染、資料被竊取的情況。

有鑑於此，**Team T5 LAB** 專注於全球威脅情資分析與研究，將其獨特之追蹤、分析、歸納與鑑識的方法論；並結合駭客攻防實際經驗，研發出先進產品【***ThreatSonar* 端點智能威脅鑑識系統】**

產品特色

- ***ThreatSonar*** 採免安裝常駐代理程式(Agent)的方式，可有效降低被攻擊者掌握，反制的風險。
- ***ThreatSonar*** 可支援 yara rule 與 black-list 威脅情資(intel)匯入，以強化整體資安的基礎。
- ***ThreatSonar*** 可支援視覺化的網路(network-hunting)與主機(host-hunting)威脅獵殺，藉以快速視察現況及修復災難。
- ***ThreatSonar*** 採輕量化設計，且不影響系統作業與資源的狀況下約 20 分鐘完成；每小時可檢測 2000 台以上端點。
- ***ThreatSonar*** 具深層執行端點掃描優勢，且可更有效地發現各類惡意程式與威脅軌跡。
- ***ThreatSonar*** 採網頁操作管理，管理介面支援繁中、英、日、韓語系，報告可匯出 CSV

肯定與建議

ThreatSonar 端點威脅智能鑑識系統，榮獲多數 **A** 級政府機關；及國內外企業指定採用，作為資安 SOP 中的『每日』檢測項目；且數量已超過 **20,000**(持續增加中) 端點；來執行設備威脅的檢測。

截至 2016 年底，源自客戶服務過程中，***ThreatSonar*** 發現全球最新且未爆發的 **APT** 攻擊手法；總計超過 **16+**種，**Team T5** 擁有最先進專業的鑑識系統外，更可依遭受的威脅情況與範圍，提供專業感染處置諮詢與修復服務，使強化客戶資安範疇；並降低同質威脅的事件發生機會。

致力於全球資安攻防趨勢；與技術核心的白帽安全專家組成，長期研析各類駭客行為、手法與攻擊工具，並追蹤監控隱匿於暴後的攻擊團體。

成員多數曾任職過知名國際資安大廠，擅長亞太區網路間諜防護，且在 HITCON 台灣駭客年會組織中長期擔任義工，並於各國際頂尖資安研討會中發表成果：美國 Black Hat(四次)、德國 TROOOPERS(兩次)、日本 CODE BLUE(三次)等，並參加多種國際 CTF 比賽獲獎：美國 DEF CON 世界第二名、日本 SECCON 第二名等。

團隊客戶來自於全球百大企業，如：『日本大型電信集團、電機製造商、綜合商社』；『結盟美國、韓國、歐洲知名資安大廠，服務金融產業客戶』；『台灣地區半導體、高科技大廠、公路總局、各大 SOC』。

Search

Surveillance

Survey

技術優勢

智能檢測

- ☆ 全自動規則設定智慧偵測
- ☆ 動(靜)態混合 APT 威脅分析
  ex. 檔案、機碼、系統紀錄、週期性工作、開機磁區、啟動程序、記憶體、執行程序

獨特分析

- ☆ 100+ 種異常動態行為規則
- ☆ 記憶體可疑區塊分析
  ex. dll /代碼注入，rootkit /隱藏程序
  C&C callback / pass-the-hash
- ☆ 3000+種東亞 APT 後門特徵

專家評估

- ☆ 白帽專家制定風險模型
- ☆ 威脅風險等級評估

鑑識追蹤

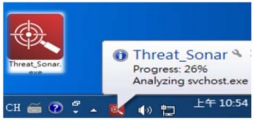
- ☆ 識別威脅技術手法
- ☆ 識別駭客攻擊來源
- ☆ 外部情資整合比對

時間資訊

- ☆ 發掘事件起源及過程
- ☆ 紀錄攻擊手法 TTP 情境

操作容易、高效鑑識

ThreatSonar 端點威脅鑑識系統，採用 **Team T5** 威脅情報指標鑑識引擎，透過企業既有派送機制，執行時少量的網路頻寬及短暫的檢測時間，迅速完成單次鑑識工作，管理員立即可由雲端智能鑑識威脅情報中心取得完整詳細的風險評估報告。



獨特技術、無所遁形

Team T5 獨創的記憶體鑑識技術，具備各種啟發式規則，可逐一分析記憶體內容；是否潛藏駭客威脅工具或軌跡，再透過軌跡間的橫向通訊觸發行為，完整勾勒出端點設備遭遇駭客攻擊的感染鏈與時間軸，並使管理者更加精準掌握，可能遭受駭客攻擊的發生來源與擴散途徑，為日後安全強化措施制定正確有效的方案。

訂購資訊

☑ 企業授權

- **ThreatSonar 軟體產品企業授權**
  - 管理軟體使用授權序號 (支援 VM 版本)
  - 端點軟體使用授權數 30 EP
  - 威脅名單更新與軟體版本升級一年授權
- **Endpoint 使用授權數 1~250 EP**
- **Endpoint 使用授權數 251~999 EP**
- **Endpoint 使用授權數 1000+ EP**
- **TS 管理主機硬體 S1 (max. 500 EP)**
- **TS 管理主機硬體 S2 (max. 2000 EP)**
- **TS 管理主機硬體 S3 (max. 5000 EP)**
- **TS 管理主機維護保固**
- **威脅名單更新與軟體版本升級(年授權)**

☑ 雲端授權 (年授權)

- **ThreatSonar 雲端服務授權**
  - 含雲端平台專屬使用帳戶一組
  - 含端點軟體使用授權數 10 EP
- **Endpoint 使用授權數 1~1000 EP**
- **Endpoint 使用授權數 1000+ EP**
- **Endpoint 使用授權數 5000+ EP**

☑ 計次服務

- **ThreatSonar 計數服務授權**
  - 含端點授權 500 EP
  - 計量方式依報告為主
  - 本授權不得權利非法轉售

☑ 專業服務

- **IRS 端點掃描服務**
- **IRS 端點威脅鑑識服務**
- **IRS 端點威脅處置服務**
- **IRS 端點綜合研析報告**
- **IRS 端點進階試驗服務**
- **APT 研析顧問專案服務**
- **上述服務說明詳端點安全服務表**

- **系統支援**
  - Windows XP、Vista、7、8、10
  - Windows Server 2003 、2012

SECDigit
數位安全雲專家

可以信賴的專業資安服務團隊

Search

Surveillance

Survey

ThreatSonar Advanced Threat Detecting Platform

IRS 端點安全服務

類別	服務名稱	內容說明
IRS-Endpoint (複選)	端點安全掃描服務	☆ 提供 Threat Sonar 端點智能威脅鑑識系統 ☆ 提供端點風險評估報告 ☆ 最低訂購數量 200 端點，未達此量以最低數量計價
	端點威脅鑑識服務	☆ 提供日誌紀錄分析 ☆ 提供惡意程式分析
	端點威脅處置服務	☆ 執行內網擴散感染檢測 ☆ 執行端點感染移除作業
	端點綜合研析報告	☆ 受感染時間軸、來源者、方法、路徑、弱點... ☆ 受感染區域範圍與安全現況 ☆ 提供完整災情分析與損害評估及威脅處置報告
IRS-Adv. Lab (單次)	惡意程式逆向進階服務	☆ 採用 IDA Pro 專業工具蒐集追蹤 ☆ 提供程式逆向服務建議報告 ☆ 採工時計價標準
	網路流量側錄進階服務	☆ 客戶協助環境設定與架設 ☆ 提供 APT Box (封包蒐集)與 TAP 裝置 ☆ 提供封包蒐集與中繼站分析 ☆ 提供 APT 網路流量側錄分析報告
	網路封包解密進階服務	☆ 針對 pcap(網路封包檔) 中的流量 ☆ 提供傳輸封包中的加密資訊破解
	檔案解密處置進階服務	☆ 提供程式破解、檔案解密 (如:ZIP、RAR 加密...等)
APT-Consultant	APT 研析顧問專案服務 (Call)	☆ 威脅攻擊定期更新服務 ☆ 威脅樣本檢測判讀服務 ☆ 系統威脅安全監控服務 ☆ 威脅操作模擬分析服務 ☆ 威脅報告專案分析服務 ☆ 緊急救援分析處置服務