端點威脅偵測應變系統

面臨國際駭客多變化的針對型攻擊，組織中資安部門準備好了嘛?

台灣近年嚴重的資安事件發生時間，根據統計都是下班或是假期時間，加上長時間的潛伏期，令企業難以防範。同時，資安事件發生的當下，需要經驗豐富的專家針對資安系統發出的警報進行分析，甚至對當下的資安威脅調查與處理，這都是企業亟欲達成但是迫於現實考量無法達到的目標。

國際知名的資訊顧問的公司 GARTNER 建議 ：
“企業應使用 MDR 服務，增加 24*7 威脅偵測與事件調查與反應資安的能量，利用 MDR 服務來彌補現有資安操作的空隙，例如弱點掃瞄與日誌監控管理下的時間差 “。

端點威脅偵測應變系統簡介

端點威脅偵測應變系統，利用高靈敏度的端點偵測與應變解決方案，全時保護企業組織內重要 PC 與 Server 伺服器等端點主機，並結合了巨量的國際與本土資安情資，即時的情資驅動威脅偵測與主動獵捕可疑威脅，既使是進階長期潛伏或最新零日的可疑威脅，也能有效感知，自動協助採取應變動作，當下中止駭客惡意活動，徹底根除組織內潛伏的惡意行為，確保真正的企業組織資訊安全。

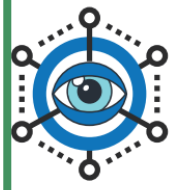
防毒防駭威脅偵測

AI人工智慧驅動威脅獵捕，整合國內外最新情資，偵測受託端點內的運作程序，自動阻斷惡意攻擊行為，保護端點主機與資料安全。

自動調查分析

系統全時監控託管端點，自動阻斷惡意威脅。

全平台支援 統一監控



支援所有主流的端點作業系統，對外服務網站主機與個人電腦都可統一納管。一鍵佈署端點監控程式，如同資安專家即刻進駐，協助資安事件應變處理。

SOC服務連動阻斷

可與SOC服務介接整合，藉由MDR託管端點的高可視性，快速關聯分析，識別高風險端點，抵禦潛在APT威脅。

https://www.chtsecurity.com/ 02-2343-1628 service@chtsecurity.com

中華資安國際 CHT Security

中華電信

端點威脅偵測應變系統

知名 EDR 方案與巨量情資高效偵測威脅

採用國際知名的 EDR(Endpoint Detection and Response) 解決方案，同時結合 EPP 端點 Antivirus 防毒引擎在同一個端點應用程式，同時可以防衛、偵測並採取應變處理於已知的惡意程式與未知的可疑威脅，有效防堵最新不斷改變攻擊手法的資安威脅。偵測能力的關鍵核心，是結合國際即時情資來源與國內發生最新的本土情資，自動驅動偵測檢查在受託端點內詳細的系統資訊與運作程序等多樣的入侵指標，清楚判定威脅並當下自動阻斷惡意攻擊威脅，徹底保護端點主機。

Out Of Box 的彈性架構與服務

威脅偵測應變系統的保護範圍不限內網，即使是帶出公司組織外的攜出 NB 都可以一一保護，中控主機可以建置於 On Premise 或私有雲端，企業所有端點一次全部保護到位。

一鍵佈署端點監控 Agent ，不須重新開機，立即啟用完整專家監控保護，沒有繁瑣人工的設定的需要，如同組織內立即進駐資安專家團隊，即刻進駐資安專家的火力支援。同時，監控 Agent 支援全部的主流的端點作業系統，無論個人 PC 或是對外服務網站主機都可於同一中控主機納管。

資安專家遠端調查與到場調查應變

一旦風吹草動，系統若能判定是已知威脅，則立即阻斷，並由專家重複驗證並通報，並在短時間找出完整的橫向滲 透軌跡，期使是駭客橫向移動，縮減應變處理時間，大大減低資安風險。

服務支援的託管端點系統

-Windows Server 2008 R2 - 2019 &Windows 10-8 (64&32bit)

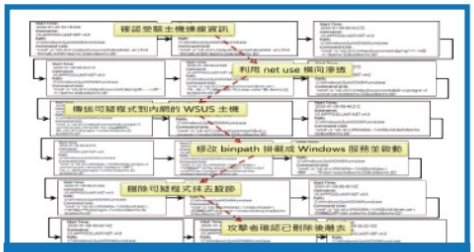
Mac OS 10.9 above(64Bit only)

Linux RHEL & CentOS 6 (above)

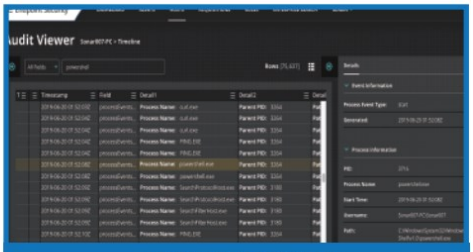
與 SOC 服務高相容性與整合優勢

可與 SOC 服務相互介接，藉由端點威脅偵測應變系統下的託管端點的資安高可見性，與 SOC 通報互補並快速深掘問題端點，有效遏阻問題，並減低 SOC 通知數量與追蹤問題的時間。

視覺化威脅管理平台



所有行為全紀錄



一鍵隔離即時阻斷

https://www.chtsecurity.com/ 02-2343-1628 service@chtsecurity.com