中芯數據
Core Cloud Tech.

資安事件回應與處理

意圖威脅即時鑑識系統2019

Server 版/Web Server版/PC標準版/PC專業版/PC白金版

使用 Sentinel 進行事件因應

中芯數據 Sentinel 能讓安全團隊以簡單的方式監控惡意活動，首要工作就是瞭解會遭受最嚴重威脅衝擊的資產與系統。

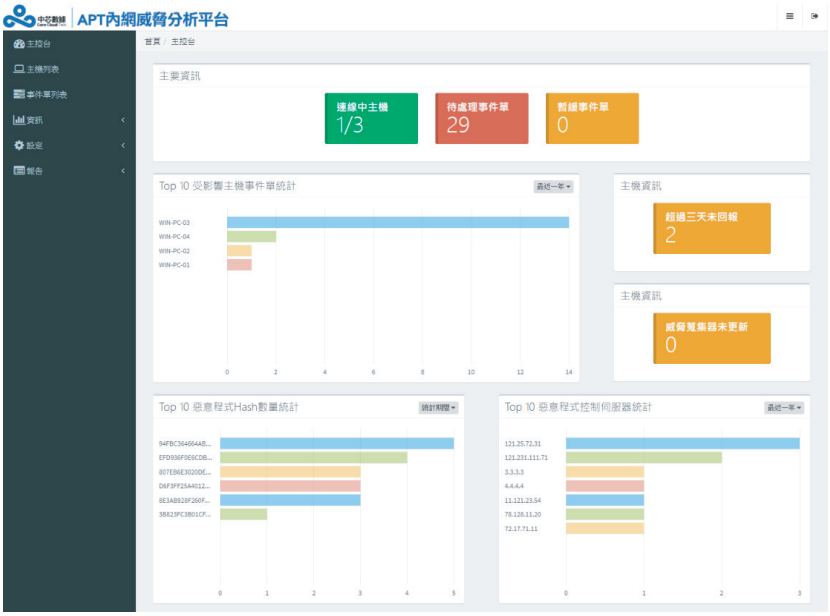
事件處理人員能使用 Sentinel 排除以人工作業進行事件調查，讓團隊能以具高度信心、經過協調的方式因應。Sentinel 能自動處理部分工作，例如停止惡意程式與雜湊，甚至隔離或封鎖端點。同時 Sentinel 的情報引擎仍能為團隊提供事件的重要詳情，包括根本原因以及事件的衝擊範圍。

由於 Sentinel 的核心模組是安裝在個人主機和伺服器端點上，並持續在隱匿模式中蒐集資料，因此敵人無法偵測到，於此情形下，操作人員將能清楚瞭解持續性活動，以及獲得有關行為的相關資訊，包括：

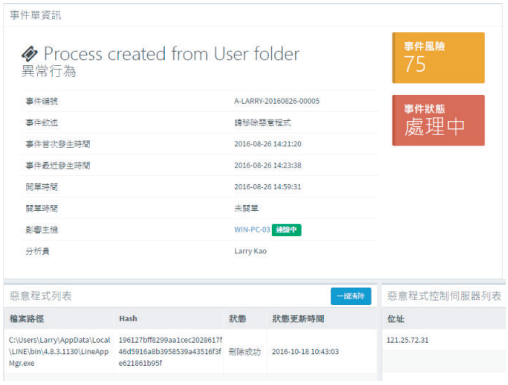
- 即時知悉受感染的系統為何，以及何者的風險最大？
- 這些系統如何受到感染，哪些行為顯示已受到入侵？
- 即時識別攻擊活動的人為因素，無須等待到發現被入侵後，才進行鑑識調查。
- 全面分析偵測到的可疑活動，並指出未及時因應該行為，可能對全部系統造成的短期衝擊和長期關聯性。

主要特色

- 強大搜尋能力：識別單一端點上的內部活動，或搜尋整體企業中的特定行為。
- 可自訂蒐集項目：指定任何行為，找出其於基礎架構中發生的確切時間和位置。
- 即時分析：快速精準地識別及優先排序威脅，以達到最佳的威脅回應。
- REST API：無縫整合企業安全生態系統，可輕易將外部資訊與 Sentinel 整合。
- 修復與封鎖：能依據需求刪除檔案及終止程序、拒絕端點網路存取，並在啟動隔離時設定警報訊息。
- 行為洞察力：擷取程序的命令列引數，能立即瞭解程序的執行時間、方法以及啟用的選項。
- 智慧群組：指定自訂群組，以便能自動依據業務單位將威脅相互關聯，並大量地管理端點。
- 攻擊情報：匯出至常用的SIEM和資料分析系統，提供給安全分析師更多的攻擊情報價值



圖｜ 瞭解您受感染的狀況及風險最大的主機



圖｜ 瞭解事件處理狀態並允許使用者刪除惡意程式

Sentinel 具備強大的功能，能讓安全團隊和因應人員獲得前所未見的洞察力。功能包括多重控制面板畫面以及全面性搜尋，能將情報功能擴及運作中的端點、已分類的威脅、威脅優先排序通知，以及受追蹤的程序。

中芯數據股份有限公司 APT事件處理小組 0809.016.818