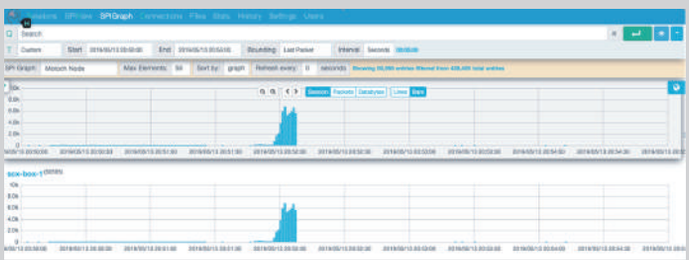
SecuTex 先進資安威脅防禦系統

產品介紹

SecuTex Network Protection



SecuTex Network Protection 先進資安威脅防禦系統

提供企業網路流量封包側錄、保存、檢索功能，可協助還原資安攻擊事件現場。
支援黑名單(惡意Domain/IP地址)及IDS偵測威脅功能，快速匡列潛在受駭主機清單。提供整合性資安儀表板，即時掌握整體風險態樣，更可自訂可疑活動偵測規則，同時具威脅偵測與事件調查鑑識能力。

1. 高擴展性高彈性的資料處理架構

本產品採分散式管理架構，透過單一管理介面(SecuTex Portal)集中式控管多台側錄偵測設備(SecuTex Box)，可因應企業需求佈署在各網路節點，SecuTex Box支援即時流量處理與高效之封包分析與索引機制，可偵測黑名單連線紀錄與異常異常連線行為，統一於SecuTex Portal作呈現，並可透過SecuTex Portal自訂黑名單(惡意Domain/IP)及異常連線行為的特徵值(IDS特徵)派送至SecuTex Box進行比對，亦可針對系統異常狀態，設定主動告警通報機制，相關訊務流量統計藉由圖像化儀表板呈現。

2. 有效率的事件現場重建與軌跡還原

SecuTex Box可使用應用層通訊協定、連線開始時間、連線結束時間、來源網際網路位址、來源網際網路連接埠、目標網路位址、目標連接埠、連線會話(Session)傳輸封包數量、會話傳輸封包資料量等條件排序。資安專家可依特定連線Session資訊(Session ID 或是Community ID Flow Hashing)搜尋並匯出條件相符連線之PCAP封包檔案。

SecuTex Box提供檢索流量軌跡之功能，檢索功能支援可以封包協定之欄位值(例如：來源IP地址、目的IP地址)當作條件進行查詢，且支援關鍵字和常規表示法(Regular Expression)檢索機制。

中華資安國際 CHT Security
www.chtsecurity.com
SERVICE@CHTSECURITY.COM 02-2343-1628 | 04-2369-2220 | 07-262-6260