中信國際電訊CPC

TrustCSI™ Secure AI

用户和企業行為分析(UEBA)，全面監測企業網絡異常

TrustCSI™ Secure AI 模仿生物免疫系統的自我學習機制，為企業網絡防禦提供嶄新方案。TrustCSI™ Secure AI假定企業經常要面對來自內部的威脅，主動偵測各種異常動靜，以行為分析方法及先進的機器學習運算法，快速查找問題根源，評估嚴重程度，再根據分析結果，制定可視化的操作，並預測異常的網絡情況是否足夠嚴重而觸發警報。我們的網絡保安專家利用TrustCSI™ Secure AI實時偵察機構網絡內任何異常情況，包括以前無法探測的＂零日攻擊＂，在攻擊週期的不同階段監測各種潛伏威脅，大大減少客戶控制威脅所需時間，並有效降低攻擊引致的損失。

產品特點

- 單臂式嗅探器 (one-arm sniffer)操作容易，輕鬆部署，額外防護
- 自動調節偵察功能，分辨正常與異常企業網絡行為
- 迅速偵測各種異常情況，例如敏感數據區域內的網絡活動，或不尋常的解密行動
- 網絡保安專家持續優化防禦威脅模型
- 能偵測到傳統規則或特徵比對模式無法偵測的威脅
- 全方位管理方案，包括電郵通知、威脅偵查報告及每日配置備份

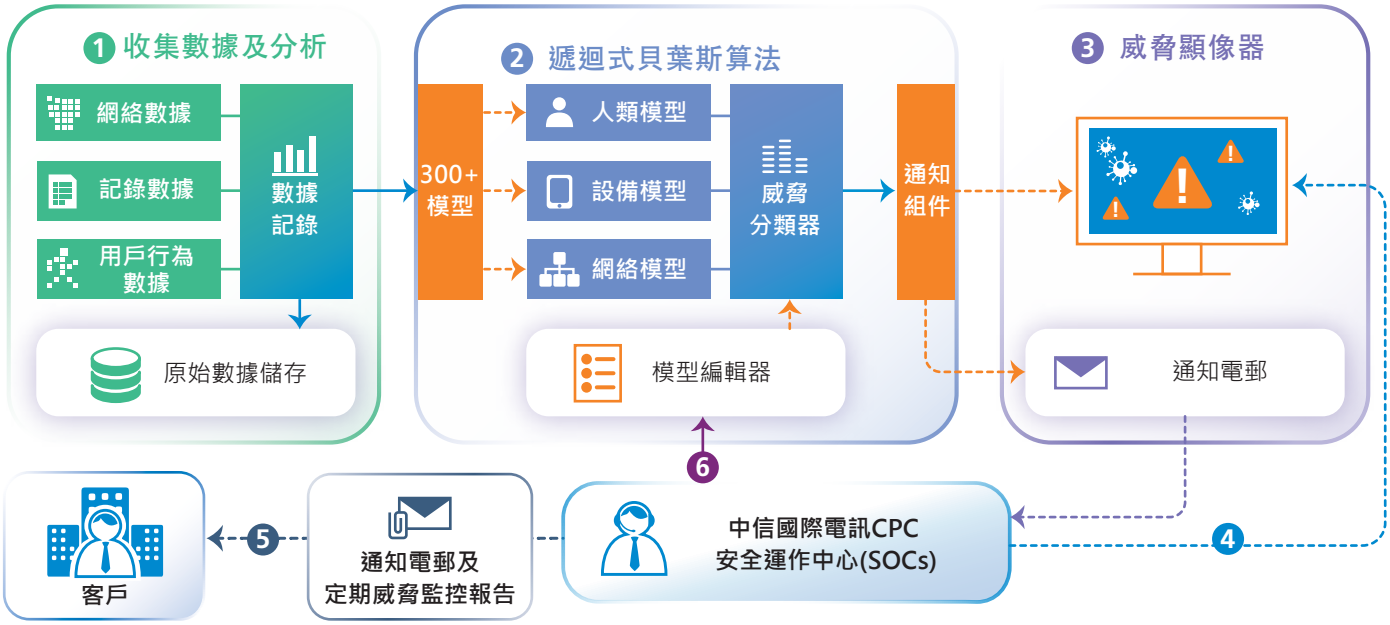
你最可信賴的信息技術方案伙伴

TrustCSI™ Secure AI

競爭優勢

- 基於先進的自啟式行為運算模型
- 全面網絡流量分析，100%可視化網絡動態
- 顆粒度分析涵蓋每個用戶、設備及網絡的活動
- 分析潛伏長時間的威脅事件，並能回放查察
- 智能鑒別正常工作流程來對威脅進行自動分類

TrustCSI™ Secure AI 方案圖示



1. 從網絡核心收集並分析原始流量數據，檢查每個數據包的潛在威脅風險。
2. 整合原數據包的海量分析結果，為網絡上每個用戶和設備的 " 日常模式 " 建模，人工智能地建立基準常態，一旦遇有任何微細異動，即可察覺。
3. 威脅分類器(Threat Classifier)實時分析異動概率，監視異常網絡行為，並確保只向網絡安全團隊發送相關的異常行為信息。
4. 中信國際電信CPC的網絡安全專家仔細檢查每一個偵查到的威脅危機，再按嚴重性及置信度評分及分類。這些分析結果將列入定期威脅偵測報告中，包括網絡行為趨勢圖像及威脅危機分類等。
5. 當發現高級別威脅時，中信國際電信CPC的網絡安全專家會向客戶發出警報；亦會向客戶發出定期報告，有關客戶操作環境的威脅情況。
6. 如有需要，中信國際電信CPC的網絡安全專家也可以通過模型編輯器為客戶創建或優化客戶的網絡安全政策及規則。

用戶得益

- 辨識及阻止包括能夠越過其他網絡安全監控措施的攻擊在內的複雜及隱蔽的網絡攻擊
- 不僅防禦惡意軟件入侵，更可揭露非法使用及其他可疑的用戶行為或滲透活動
- 適用於任何關注內部威脅和其他新興及有針對性網絡攻擊的企業

中信國際電訊CPC

W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
波蘭 T: 48 22 630 63 30
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
拉脫維亞 T: 371 6721 4122
俄羅斯 T: 7 495 981 5676
中國大陸 (Toll Free): 400 880 1222
新加坡 T: 65 6220 6606
立陶宛 T: 370 5264 4303
荷蘭 T: 31 20 567 2000

DHK1802EN