中信國際電訊CPC AI 構建企業網絡安全新防線

|ezone.hk 編輯部|31-08-2026 00:00|

當人工智能全面滲透商業運作，網絡安全的戰場亦隨之徹底改變。黑客早已借助 AI 工具自動挖掘系統漏洞、降低攻擊門檻，令網絡威脅以更快速度、更大規模潛現，面對這場攻守之間的智能化角力，企業所需的已不再是傳統被動監控的安全運作中心（SOC），而是能主動出擊、以 AI 對抗 AI 的全新防禦體系，中信國際電訊 CPC 憑藝深耕香港逾 25 年的豐富經驗與前瞻性的 AI 技術部署，多年來獲獎無數，彰顯品牌厚實的創科軟硬實力，在今屆「e 世代品牌大獎」中更榮獲「最佳 AI 安全運作中心供應商」大獎。

SIEM-MiiND 星智神盾 以本地 AI 大模型賦能 SOC

中信國際電訊 CPC 的 AI SOC 核心，建基於本地部署的智能安全信息及事件管理平台「SIEM-MiiND 星智神盾」。平台名稱中的「ii」代表智能創新（Innovation）與智慧思維（Intelligence），體現中信國際電訊 CPC 的前瞻性 ICT-MiiND 策略，將創新技術、算力算法與大數據無縫融合。

SIEM-MiiND 由中信國際電訊 CPC 自行部署的本地 AI 大語言模型（LLM）支撐，確保客戶數據全程留存於受控環境，杜絕敏感資訊外洩，平台每天處理數千萬的安全事件，透過 AI 自動完成告警關聯分析與威脅研判，並以 AI 驅動的 SOAR 劇本實現秒級安全回應，同時將關鍵警報處理時間縮短，最高可達 50%，大幅提升整體 SOC 效能。

中信國際電訊 CPC 網絡安全顧問劉俊生指出，面對黑客借助 AI 自動化降低攻擊門檻的嚴峻局勢，企業必須以「以 AI 對抗 AI」方能確守數碼命脈。

從專家主導到 AI 賦能 重新定義 SOC 效能

傳統 SOC 依賴大量安全分析人員三班輪值，成本高昂之餘亦難以跟上威脅演變速度，SIEM-MiiND 從根本上改變了這一模式，將重複性高、耗時的查找與分析工作交由 AI 自動處理，安全專家則得以專注於制定網絡安全策略等決策性工作，新客戶接入時間亦由過往的數天縮短至數小時，大幅提升服務效率。

AI SOC 的核心突破之一，在於對「假陽性（False Positive）」的智能過濾。傳統環境下，系統警報的假陽性比率可高達八至九成，劉俊生指出，SIEM-MiiND 能學習每位客戶的正常操作習慣，結合其風險暴露面自動研判警報真偽，令 SOC 工程師得以將精力集中於真正需要即時處理的安全威脅，大幅提升應對效率與準確度。

AI SOC 託管式安全服務，融合智能自動化與核心大模型算法，為企業提供無縫且強韌的深層次安全防護。

隨著生成式 AI 普及，網絡攻擊的技術門檻已大幅降低，以往只有頂尖技術人員才能執行的滲潤攻擊，如今借助 AI 工具即可獲得詳細的攻擊思路，令潛在威脅的數量與複雜度呈幾何級增長，劉俊生強調，應對之道只有一個：以 AI 對抗 AI，SIEM-MiiND 同時整合國內外威脅情報，透過強大的 AI 大模型進行深度分析，有效預測未來攻擊趨勢並加速回應速度。

國際認證與人才支援 破解資安人才荒困局

香港網絡安全人才長期供不應求，自行組建全天候輪值 SOC 團隊成本極高，中信國際電訊 CPC 的世界級安全運作中心已獲 ISO9001、ISO14001、ISO20000、ISO27017 及 ISO27001 等多項國際認證，專業安全專家團隊亦全數持有 CISA 及 CISSP 等國際資格，以業界最佳規範處理威脅事件，讓企業可需自建龐大安全團隊，即可享有全天候的頂級防護。

AI 的引入同步改變了人才需求結構，劉俊生指出，具備基本 IT 及網絡知識的人員，配合 AI 工具輔助，已能承擔相當程度的 AI SOC 工作，與此同時，SOC 從業員的核心價值亦轉型為更強的客戶溝通能力，具備豐富行業知識，深入理解客戶業務風險、在事故發生時迅速協助應對，是目前 AI 未能取代之處。

AI SOC 結合一系列前沿智能創新方案，包括 AI 滲透測試、AI 可視化安全解決方案及 AI 安全風險，為企業構建多元化立體防線。

量化風險見真正 ROI 跨境合規一體管理

劉俊生建議企業以量化方式評估安全投資：衡量受保護資產的實際價值，對比 AI SOC 服務成本，方能作出理性決策。一旦遭受勒索軟件攻擊，企業數據癱瘓、系統全面癱瘓，損失往往遠超任何防禦投入。

在跨境業務層面，中信國際電訊 CPC 的兩地三中心網絡覆蓋香港、上海及廣州，憑藉應對中國內地的網絡安全等級保護、歐洲 GDPR、新加坡個人資料保護法規及香港企會局、證監會要求的豐富合規經驗，協助企業無論身處何地均能符合當地監管標準。

行業定制靈活部署 前瞻 IoT 時代新挑戰

不同行業的安全需求截然不同：金融機構要求最高強度的數據中心防護；零售企業則重視泛終端設備網絡的全面覆蓋，中信國際電訊 CPC 的 AI SOC 採用模組化架構，針對不同行業與規模制定相應的監控規則與響應機制，展望未來，隨著 5.5G 網絡及物聯網裝置日益普及，平台已部署應對 IT 與 OT 雙軌安全框架，系統自動學習客戶及裝置的正常使用規律，一旦出現異常行為即時警示，確保企業始終維持最高警戒。

在 AI 賦能攻防兩端的新時代，中信國際電訊 CPC 以 SIEM-MiiND 星智神盾為核心，結合跨境網絡基建、深厚合規經驗與行業定制能力，為企業構築超一道智能、靈活且持續進化的數碼防線，助各行各業在數碼轉型的道路上走得更穩、更遠。

覆蓋香港、廣州、上海的一體化管理架構，助跨境企業在無縫連通雲網資源的同時，輕鬆滿足各地合規要求。

總結

網絡威脅的本質已然改變，攻擊者借助 AI 無休止地尋找破口，企業的安全防線亦必須即被動應對蛻變為主動預判。中信國際電訊 CPC 以 SIEM-MiiND 星智神盾為技術核心，整合本地部署大語言模型、秒級 SOAR 自動回應與全天候威脅情報分析，配合跨境基建與多項國際認證，打造出一套真正以「AI 對抗 AI」為理念的企業級防禦生態。劉俊生指，安全投資的價值從不在於平靜時的開支，而在於危機爆發時能否守住企業的數碼命脈，正是這份對客戶業務的深刻理解，令中信國際電訊 CPC 在人才荒、合規壓力與新興技術威脅三重夾擊下，仍能持續為各行各業提供切實有效的定製化保護。

*Source: 中信國際電訊CPC

最新內容

香港即時天氣報告＋天文台未來9天香港天氣預報 香港各區氣溫一覽
香港交通消息實時更新｜隧道實時路面情況+主要幹道估計行車時間
日本天氣預報：東京、大阪、京都等地未來 7 天氣溫預測 全國各地氣溫及降雨預報
台灣天氣預報 | 台北/台中/桃園/新北/高雄市今日+未來7天天氣預測
國產手機又變貴？記憶體漲價「非常離譜」 旗艦機計劃量狂劈 5 成！Q4 恐迎價格高峰【附售價預測】
海關發現出幫制通知書！XPower一「尿袋」無線充電溫度可飆至131度 呼籲市民立即停用【廠方有回應】
Excel F1 至 F12 功能鍵教學！打工仔必學 12 個快捷鍵組合 事半功倍提升效率
多次度假可改善心臟健康？大學研究：放假愈多代謝綜合症風險愈低
Google 免費兒童英語 App《Read Along》！語音識別技術即時糾音 9 種語言任揀
修改 DNS 突破封網教學！Windows、iPhone、Android 改用 1.1.1.1 零成本解鎖被封網站

Q1：黑客已經用 AI 攻擊，傳統 SOC 真的不夠用嗎？企業應該點樣應對？

A：黑客已借助 AI 自動挖掘漏洞、降低攻擊門檻，令威脅以更快速度、更大規模潛現，傳統被動監控的 SOC 難以跟上，企業需要能「以 AI 對抗 AI」的主動防禦體系，中信國際電訊 CPC 的 SIEM-MiiND 星智神盾正是為此而設，透過本地 AI 大模型自動完成告警關聯分析、威脅研判與秒級 SOAR 回應，最高可將關鍵警報處理時間縮短 50%。

Q2：導入 AI SOC 後，真的可以減少假陽性警報，並解決資安人才荒嗎？

A：可以，傳統環境下假陽性比率可高達八至九成，SIEM-MiiND 會學習每位客戶的正常操作習慣，自動研判警報真偽，讓工程師專注處理真正威脅，同時，具備基本 IT 及網絡知識的人員配合 AI 工具已能承擔相當工作，企業毋需自建龐大全天候團隊，即可享有獲多項國際認證的頂級防護。

Q3：投資 AI SOC 的回報如何衡量？對跨境企業又有什麼實際幫助？

A：中信國際電訊 CPC 網絡安全顧問劉俊生建議以量化方式評估——比較受保護資產的實際價值與服務成本。一旦遭受勒索軟件攻擊，損失往往遠超防禦投入。另外，中信國際電訊 CPC 的兩地三中心（香港、上海、廣州）架構，加上豐富的跨境合規經驗（包括內地等保、GDPR、新加坡 PDPA 及香港金管局 / 證監會要求），可助企業在不同地區輕鬆符合監管標準，真正做到一體化管理。