新一代智能安全運作中心
(AI SOC)

CITIC TELECOM CPC

TrustCSI™ 3.0
雲網神盾

信息安全管理服務

全新 AI SOC 網絡安全框架

AI SOC 賦能

識別及預測 | 保護 | AI SOC 星智神盾 SIEM-MiiND 託管式安全服務 | 偵測 | 回應與復原

› 服務在地 連接全球的數智通訊服務伙伴

TrustCSI™ 3.0 雲網神盾 AI SOC 賦能

TrustCSI™ 3.0 雲網神盾是我們優化的信息安全旗艦解決方案，為您的企業提供最佳保護。方案針對三個關鍵領域，全面檢視及控制信息風險。首先，在現今需求嚴格實踐數據處理的時代，TrustCSI™ 3.0雲網神盾強調合規性(Compliance)以符合最嚴謹的法規要求。其次，此方案易於部署、低前期投入成本、零維護的安全管理服務 (Security)，應對日益複雜的 IT 環境中衍生的威脅。最後，我們利用先進的人工智能，注入創新(Innovation)和智能能力，顯著提升阻截威脅的速度、成效和效率。

作為您在數智化時代值得信賴的 TechOps 信息安全賦能者，我們不僅致力於優化防護，更專注於從根本上重新定義未來網絡安全框架。憑藉二十年的深厚專業積澱與前沿AI應用，我們自建了星智神盾（SIEM-MiiND），一款可大幅提升 SOC 營運效率的智能安全信息和事件管理（SIEM）平台。作為AI SOC 的核心，SIEM-MiiND能提供更快速、更精準的 24/7 全天候威脅分析與監控，賦能企業以前瞻性的主動防禦能力，全面對抗不斷演變的網絡風險。

您值得信賴的TechOps信息安全賦能者

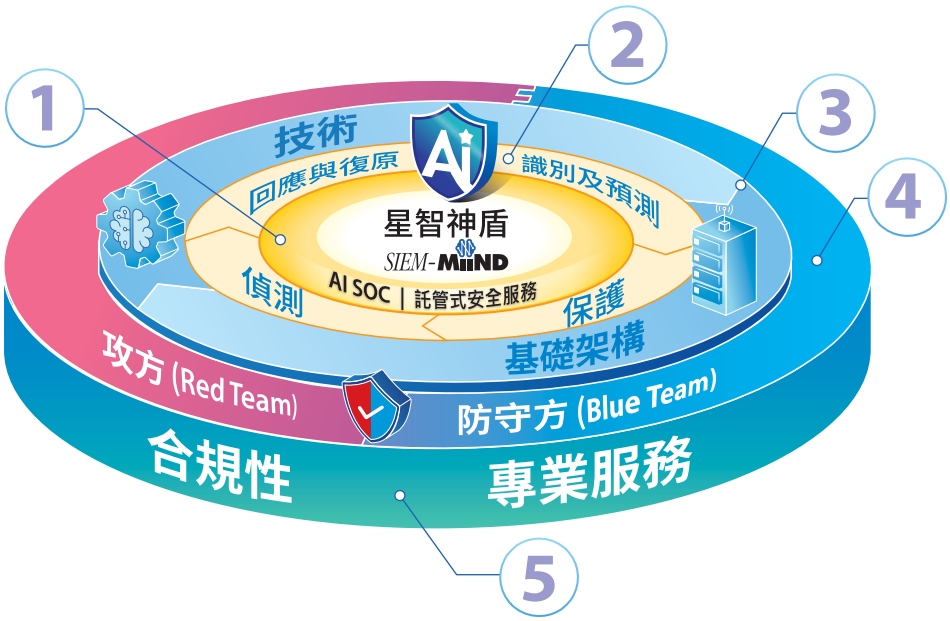
全新 AI SOC 網絡安全框架

憑藉累積多年信息安全的服務經驗，通過全新 AI SOC 網絡安全框架，我們將網絡及信息安全由被動式保護轉化為主動式防禦，協助企業輕鬆應對數智化時代瞬息萬變的網絡威脅，減低安全風險。

隨著現代企業加速數碼轉型，他們獲取了新機遇，但亦因攻擊層面擴大而增加風險。同時，由AI驅動的網絡威脅日益複雜。因此，構建智能且全方位的網絡安全防護，已是刻不容緩。

中信國際電訊CPC致力於成為您值得信賴的TechOps信息安全賦能者。我們充分了解不同行業獨特的數碼化信息安全需求，全新AI SOC 網絡安全框架，賦能世界級TrustCSI™信息安全服務，為企業提供全面保護，有效地識別、預測、保護、偵測、回應及復原各種網絡安全事件，為企業提供全面保護。

我們的智能網絡安全框架是由專業的安全專家團隊、3 個跨區域智能安全運作中心（AI SOCs），以及自建的智能安全信息和事件管理平台「星智神盾」（SIEM-MiiND）組成。這一全方位智能網絡安全框架聚焦於「人才」、「流程」與「技術」三大核心，並完美融入「AI攻防」實踐，以智能化手段精準識別企業 IT 環境中的潛在漏洞，打造強韌並具前瞻性的主動防禦策略，為企業提供最大程度的安全保障。



全新 AI SOC 網絡安全框架

1 新一代智能安全運作中心：星智神盾 (SIEM-MiiND)

作為AI SOC的核心，星智神盾是我們資訊安全及創新研發團隊自主自建的智能安全信息和事件管理平台，具有更高效的資料處理能力和全面的安全監控能力:

提升響應能力

構建了智能化的安全事件檢測機制，大大縮短故障排查時間，在發出初步警報郵件後，可較以往快高達75%提供進一步細化的安全建議（視乎安全事件的複雜程度），幫助客戶有效減少了業務中斷帶來的損失。星智神盾亦會針對潛在威脅並發出警報通知，降低企業網絡被攻擊的風險。

智能聊天機器人

為企業提供24/7熱線外的新增提問渠道，在安全認證的登入機制下，讓企業更及時透過線上線下途徑清楚了解安全事件現況及整體安全級別。

增強檢測能力

透過主動地對漏洞和潛在的入侵指標（IOC）進行初步分析，減低對客戶網絡造成威脅。

優化規則集

通過AI技術，根據客戶的歷史資料和新的攻擊情景，調整偵測閾值，並就新增設備的日誌資料自動及持續創建新規則集，為客戶量身訂做和微調規則集。

2 SOC4Future 安全策略

SOC4Future 安全策略運用了全面的四階段測試框架，為企業提供全方位的安全保障：

1). **識別及預測:** 運用一系列全面的評估與識別服務，覆蓋系統、應用程式、網絡基礎架構及關鍵資產，以精準識別並化解安全風險。

2). **保護:** 透過與全球頂尖的安全技術供應商合作，利用一流的安全解決方案與專家級的安全基礎架構管理，確保強韌的防禦實力，抵禦日益增加的威脅。

3). **偵測:** 憑藉三個跨區域的 AI SOCs 和先進的 「星智神盾」智能安全信息和事件管理(SIEM) 平台，全面提升了企業快速有效地識別、應對日益頻繁和複雜的網絡安全事件的能力。

4). **回應與復原:** 運用威脅情報，協調並自動化處理安全事件，最大限度地縮短解決時間，並提供詳細的安全事件後報告，以找出根本原因並支援未來行動計劃。

3 面向未來的SOC即服務

SOC-as-a-Service（SOCaaS)服務體現了未來的智能網絡安全。我們通過基於人工智能驅動的先進安全分析和監控能力，提供出色及優化的安全分析和監控服務。「SOC即服務」(SOC-as-a-Service)由位於香港、廣州和上海的3個頂級自建及管理的7x24安全運作中心(SOC)支持。透過我們擁有國際認證、和合規知識及經驗的專業團隊，提供「服務在地、連接全球」的創新及客製化的安全解決方案，幫助客戶在不斷變化的數碼化環境中，達至數碼安全。

4 擁抱「攻防實踐」協同效應

以積極主動策略，將整個網絡安全循環從被動轉為主動。「AI攻防」實踐涵蓋全棧安全服務，從員工培訓和攻防演練，到網絡保護解決方案、信息安全策略和服務諮詢。攻方執行由AI驅動全方位的評估和模擬測試，而守方則提供縝密的防禦保障，確保全面提升企業對網絡風險的嚴密佈置。

5 優化的專業及合規服務

我們為客戶提供具獨特競爭優勢的「服務在地、連接全球」混合方案模式，無縫融合世界一流的技術知識和設施，以及廣泛的本地業務豐富經驗。另外，我們擁有認證的合規專業知識，我們的業務範圍涵蓋從諮詢服務到信息安全設備遷移和跨境數據合規評估。 憑藉全球覆蓋和先進的TechOps能力，賦能客戶高信任度和安全性的數碼化營運。

無縫擴展網絡和雲端保護

分散式企業的安全存取服務邊緣方案

在現今瞬息萬變的數碼化商業環境下，企業需要具彈性的IT解決方案來保持競爭力。安全存取服務邊緣方案（Secure Access Service Edge，SASE）利用簡單易用的SD-WAN編排工具，簡化不斷變化的網絡邊緣（從企業總部到分支辦公室、數據中心和雲端)的網絡流量管理。這項全面管理解決方案，簡化並保護基礎設施，同時提升靈活性和可擴展性。企業可以持續營運，提升應用程式能力及體驗，以及確保整個基礎設施具成本效益地為任何用戶隨時隨地提供服務。

全方位的企業郵件安全和雲端備份，實現業務持續營運

電子郵件攻擊是現今緊密互聯的商業環境下，企業最常見的網絡攻擊之一，超過90%的成功網絡攻擊都是通過電子郵件。為了堵塞此漏洞，我們先進的O365備份和電子郵件安全解決方案，提供24/7全天候的管理服務，以安全加固企業的郵件系統。

除了電子郵件外，企業也需要全面保護其他系統，尤其是隨著企業在各項關鍵任務的工作流程中，越來越多採用虛擬化、雲端運算和雲應用，部分重要的數碼資產已經超出企業的實體業務範圍。為了保護這些資產，我們提供全面的備份解決方案，包括現場和異地備份、虛擬機器備份和實體伺服器備份，以保護企業重要的數據及業務彈性。

識別及預測	• 代碼審查服務 • AI資訊安全威脅識別平台 • 漏洞評估服務 • 滲透測試服務 • 資產梳理服務
保護	• 郵件防護服務 • 安全存取服務邊緣 (SASE) • 統一威脅管理 (UTM) • 託管式新世代防火牆 (NGFW) • 託管式網站應用程式防火牆 (WAF)
偵測	• 網絡流量分析 • 託管式安全服務 (MSS) • 端點偵測及回應 (EDR) • 用戶和企業行為分析 (UEBA)
回應及復原	• 威脅搜捕服務 • 多功能託管式雲備份及災難復原解決方案 (BRR) • 安全編排及自動化回應 (SOAR) • 安全事件回應 (IR)
智能安全運作中心 (AI SOC)	• 3 個智能安全運作中心 (AI SOCs) 提供跨區域保護 • 自主自建的智能安全信息和事件管理平台「星智神盾」(SIEM-MiiND) 解鎖新一代網絡安全防禦 • 具認證的安全專業人員提供7x24在地服務 • ISO27001國際認證的最佳實踐
專業服務及合規	• 信息安全設備遷移服務 • 中國網絡安全法– 網絡安全等級保護2.0合規諮詢服務 • 雲端專業服務 • 跨境數據合規評估服務

TrustCSI™ 3.0

中信國際電訊CPC

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

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99

中國大陸 (Toll Free): 400 651 7550
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30

新加坡 T: 65 6220 6606
荷蘭 T: 31 20 567 2000

TSF2605TC