
中信國際電訊CPC
CITIC TELECOM CPC
TrustCSI™ 3.0
雲網神盾
CyberSecurity ReDEFINED. SOC4Future
致力提升 安全服務! 技術賦能 重新定義!

ReDEFINED.
SOC4Future
安全賦能重新定義

Your Trusted TechOps Security Enabler

CITIC Telecom CPC is committed to being your trusted TechOps Security Enabler. We fully understand specific digital protection needs across multiple industries, and offer our world class TrustCSI™ managed information security solutions empowered by the SOC4Future strategy to deliver holistic enterprise protection that enables your organization to Identify, Predict, Protect, Detect, Respond and Recover effectively from diverse threats.

Our experienced and certified team of security professionals helps enterprises periodically conduct the "AI-Red/Blue Cybersecurity Practices" to fully ascertain weaknesses in their IT infrastructure landscape and applications to develop effective defense measures for maximum protection. Additionally, our cutting-edge intelligent security service, built on our ReDEFINED cybersecurity framework, world-class infrastructure, award-winning expertise and state-of-the-art technology, proactively safeguards your organization continuously and intelligently.

Cloud Network & Security

Innovative Cybersecurity Framework

Leveraging our decades of in-depth practical experience in information security industry, we redefine a comprehensive cybersecurity framework comprises four pivotal service pillars: Identify & Predict, Protect, Detect, and Respond & Recover, to ensure full protection of enterprises.

Advanced Technologies featuring Dual SIEM

Advanced Dual SIEM platforms revolutionize threat intelligence management, expediting large-scale intelligent data analysis to swiftly detect and respond to emerging threats with delivery of professional analysis reports, catering to diverse security requirements with exceptional speed and efficiency.

Strengthened Infrastructure enabling SOC-as-a-Service

Our "SOC-as-a-Service" is empowered by 3 top-tier self-deployed and managed 24x7 Security Operations Centers (SOCs) in Hong Kong, Guangzhou and Shanghai, and fully managed by certified professional expertise and compliance acumen to deliver unparalleled security analytics and monitoring capabilities.

Embrace Red/Blue Synergy

Through a comprehensive 4-stage Red/Blue Team simulations to "stress test" scenarios and systems with our advanced Security Operations Centers (SOCs) service capabilities, we elevate enterprise employee defense capabilities and identify the potential risks of enterprise for fast remediation, enhancing enterprise-wide rapid response to cyberthreats with proactive holistic defense solutions.

Empowering Secure Operations with Professional Service & Compliance

With our "global-local" approach and certified expertise in compliance, we offer a range of services from consultancy to security device migration and cross-border data compliance, enabling enterprises with unparalleled security in their global digital operations.

創新網絡安全框架

憑藉多年來在信息安全行業的深耕和實踐經驗，我們為客戶從新規劃四個關鍵服務版塊，涵蓋識別及預測、保護、偵測、回應及復原的全面網絡安全框架，使更全面保障企業安全。

先進雙核心SIEM技術平台

先進雙核心SIEM技術平台，重新定義威脅情報管理。通過大規模智能數據分析，迅速偵測和回應新興威脅，並提供專業分析報告，快速及有效地滿足各種安全要求。

強化基礎設施，實現SOC即服務

「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）提供支持。服務由擁有國際認證及合規經驗的專業團隊管理，為客戶提供創新定制的網絡安全分析及監測服務，與全天候資安管理。

擁抱「攻防實踐」協同效應

結合先進的安全運作中心（SOC）服務能力，我們可通過4個階段執行「紅藍隊模擬」網絡攻擊測試，對企業營運環境和系統的攻擊和防禦能力進行全面的「壓力測試」，藉此有效提升員工的安全意識和洞悉企業潛在風險，及早修正。加強主動防守，提升企業整體對網絡安全的全面佈置。

實現安全運營的專業服務和數據合規管理

結合「服務在地、連接全球」的策略及具有數據合規認證的專業團隊，我們為企業提供全面的服務，從咨詢服務到安全設備遷移和跨境數據合規管理，使企業擁有高水平的安全能力，實現全球數碼化運營。

您值得信賴的TechOps信息安全賦能者

中信國際電訊CPC致力成為企業值得信賴的TechOps信息安全賦能者。我們充分了解不同行業的數碼化信息安全需求，通過SOC4Future策略，賦能世界級TrustCSI™信息安全管理服務，有效地識別、預測、保護、偵測、回應及復原各種信息安全措施，為企業提供全面保護。

憑藉豐富的行業實踐經驗，中信國際電訊CPC的安全專業團隊能協助企業定期開展「AI攻防」實踐，全面評估其IT基礎設施環境與應用的風險，並制定有效的防禦措施，以達到最高的安全保障。此外，我們嶄新的智能安全服務，建基於我們重新定義的網絡安全框架、世界級的基礎設施、屢獲殊榮的專業團隊和前沿技術，能主動地為企業客戶提供無間斷及智能保護，成為企業的「雲網神盾」。

雲網神盾

Safeguarding your DX business with Intelligent Cybersecurity Framework

智能網絡安全框架，保護您的 DX 業務

Leveraging our decades of in-depth practical experience in information security industry, we redefine a comprehensive cybersecurity framework comprises four pivotal service pillars: Identify & Predict, Protect, Detect, and Respond & Recover, to ensure full protection of enterprises.

憑藉多年來在信息安全行業的深耕和實踐經驗，我們為客戶從新規劃四個關鍵服務版塊，涵蓋識別及預測、保護、偵測、回應及復原的信息網絡安全框架，使更全面保障企業安全。

Respond & Recover
回應與復原

Identify & Predict
識別及預測

Detect
偵測

Protect
保護

AI-Red/Blue Cybersecurity Practices 「AI攻防」實踐

CITIC Telecom CPC's "AI-Red/Blue Cybersecurity Practices" forms an integral part of enterprises' comprehensive cybersecurity protection.

- The "Red Team" performs all-encompassing assessments and simulations, including asset, strategy and process review, AI identification and vulnerability scanning, penetration testing, simulated phishing email drills, and provides risk assessment analysis to help enterprises to identify potential weaknesses, vulnerabilities and risks.
- The "Blue Team" provides holistic defense services including staff training, risk consultation, application testing, analysis reports, device deployment, response and traceability. Compliment with 24x7 managed services to strengthen defense capabilities against attacks, enabling holistic enterprise protection.

Through the "AI-Red/Blue Security Practices" to "stress test" scenarios and systems, we elevate enterprise employee defense capabilities and identify the potential risks of enterprise for fast remediation, enhancing enterprise-wide rapid response to cyberthreats with proactive holistic defense solutions.

中信國際電訊CPC的「AI攻防」實踐是企業綜合網絡安全保護的重要組成部分。

- 「攻方」執行全方位的評估和模擬，包括：資產、策略與流程梳理、AI識別與漏洞掃瞄、滲透測試、模擬釣魚郵件演練，並提供風險評估分析，以助企業識別潛在的弱點、漏洞和風險等；
- 「防守方」則提供全面的防禦服務，包括人員培訓、風險諮詢、系統測試、分析報告、設備部署、響應與溯源，配合24x7 託管服務，實現攻防互補，安全賦能。

「AI攻防」實踐針對企業營運環境和系統的攻擊和防禦能力進行全面的「壓力測試」，藉此有效提升員工的安全意識和洞悉企業潛在風險，及早修正。加強主動防守，提升企業整體對網絡威脅的全面佈置。

MORE | 更多

中信國際電訊(信息技術)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED
中信國際電訊集團成員

www.citictel-cpc.com