CITIC TELECOM CPC

TrustCSI™ 3.0

Information Security Services

AI-Driven Cybersecurity Framework

Powered by AI SOC

Identify & Predict

Protect

AI SOC

星智神盾 SIEM-MiiND

Managed Security Service

Detect

Respond & Recover

› Global-Local Intelligent DICT Service Partner

TrustCSI™ 3.0 Powered by AI SOC

TrustCSI™ 3.0 is our upgraded flagship security suite giving you the best possible enterprise protection. It provides superior visibility and control over information risks, with three pivotal areas of focus. Firstly, in an era of more stringent data handling practices, TrustCSI™ 3.0 addresses (C)ompliance to meet even the most stringent evolving requirements. Secondly, it is an easily deployed, low overhead, zero maintenance Managed (S)ecurity Service for navigating an increasingly complex IT landscape of sophisticated threats. Lastly, we leverage cutting-edge AI to infuse (I)nnovation and intelligence to achieve dramatically higher speed, effectiveness, and efficiency in thwarting threats.

As your Trusted TechOps Security Enabler in an era of digital intelligence, we go beyond optimizing reliable protections to fundamentally redefine future security frameworks. Leveraging 2 decades of deep expertise and cutting-edge AI innovation, our self-built SIEM-MiiND — an intelligent SIEM platform that dramatically enhances SOC efficiency, delivering faster, more precise 24/7 threat analysis and monitoring. At its core, our revolutionary AI SOC empowers enterprises to proactively combat evolving cyber risks with next-gen defense capabilities

Your Trusted TechOps Security Enabler

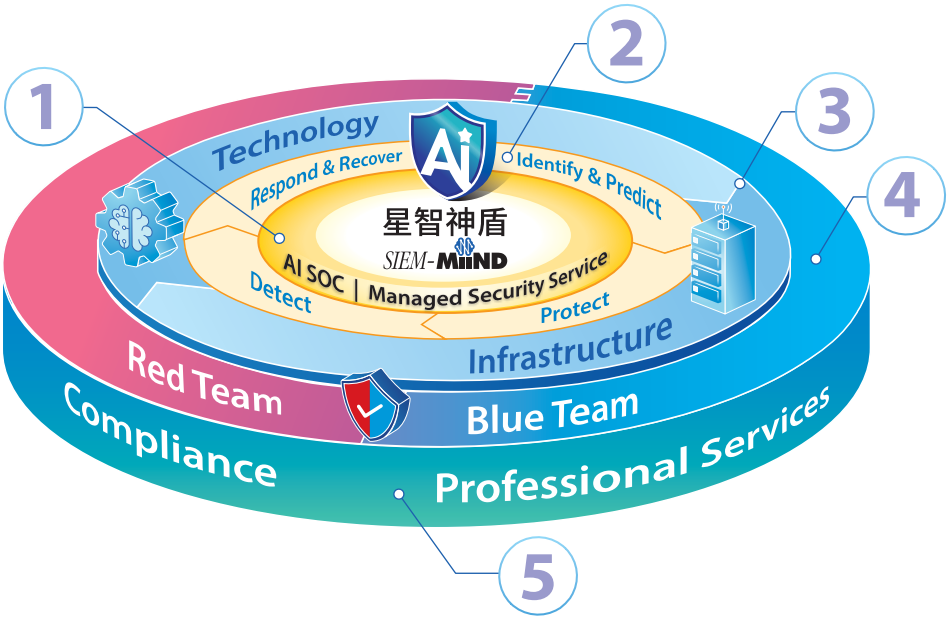
AI-Driven Cybersecurity Framework

Powered by our unparalleled and decades of in-depth experience in cybersecurity and AI-Driven Cybersecurity Framework, we redefine cybersecurity from passive defense to proactive guardianship, enabling enterprises to thrive in an AI-driven landscape

As modern enterprises accelerate their digital transformation, they gain unprecedented opportunities, yet also heighten risks with an expanded attack surface. Meanwhile, AI-powered cyber-threats are more sophisticated than ever. Today, intelligent, comprehensive cybersecurity has never been more crucial.

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 that are empowered by an AI-driven Cybersecurity Framework, enabling your organization to Identify & Predict, Protect, Detect, Respond & Recover effectively from diverse threats.

Our AI-driven Cybersecurity Framework is supported by a dedicated team of security professionals, 3 cross-regional AI-powered Security Operations Centers (AI SOCs), and our self-built advanced security information and event management (SIEM-MiiND) technology. This comprehensive approach focuses on "People," "Process," and "Technology," seamlessly incorporating "AI Red-Blue Cybersecurity Practices" to intelligently identify vulnerabilities within the enterprise IT environment, enabling robust and proactive defense strategies that deliver maximum protection for the enterprise.



AI-Driven Cybersecurity Framework

1 AI SOC: SIEM-MiiND

As the core of our AI SOC, SIEM-MiiND is a self-built intelligent security information and event management (SIEM) platform independently developed by our cybersecurity and innovation R&D team that significantly improves SOC efficiency, enhances data processing capabilities, and enables comprehensive security monitoring.

Improved Response Capabilities

Implements an intelligent security incident detection mechanism, significantly reducing troubleshooting time and enabling actionable recommendations up to 75% faster after the initial email alert (depending on the complexity of the security events)— assisting customers on minimizing losses from business disruptions. SIEM-MiiND also identifies potential threats and issues preventive alerts, lowering the risk of enterprise network attacks.

AI-Powered Chatbot

Provides businesses with an additional inquiry channel beyond the 24/7 hotline, enabling them to promptly and clearly understand the status of security incidents and overall security levels through both online and offline channels, under a secure authentication login mechanism.

Enhanced Detection Capabilities

Conducts preliminary analysis of vulnerabilities and potential Indicators of Compromise (IOCs) proactively to reduce threats to enterprise networks.

Optimized Rule Sets

Through AI technology, detection thresholds are adjusted based on the customer's historical data and new attack scenarios, and new rule sets are continuously created for the log data of newly added devices, tailoring and fine-tuning rule sets for the customer.

2 SOC4Future Strategy

The SOC4Future strategy harnesses a comprehensive four-stage framework to deliver holistic enterprise protection:

1). **Identify & Predict:** By utilizing a suite of comprehensive assessment and identification services covering systems, applications, network infrastructure, and critical assets to identify and mitigate security risks.

2). **Protect:** Through partnering with top-tier security technology providers globally, ensures robust safeguards against rising threats through top-tier security solutions and expert management of security infrastructure.

3). **Detect:** Reinforced by our three cross-regional AI SOCs and the advanced SIEM-MiiND platform, we elevate enterprises' ability to quickly and effectively identify and respond to the increasing frequency and sophistication of cybersecurity events.

4). **Respond & Recover:** Leveraging threat intelligence, orchestrating and automating incident resolution to minimize resolution time with detailed post-incident report also pinpoint root cause and support actional future planning.

3 SOC-as-a-Service for Cross-border Protection

The "SOC-as-a-Service" paradigm embodies the future of intelligent cybersecurity. We deliver unparalleled security analytics and monitoring capabilities via our AI-driven, top-tier security analytics and monitoring capabilities. The "SOC-as-a-Service" concept is empowered by 3 AI-driven self-built 24x7 Security Operations Centers (AI SOCs) in Hong Kong, Guangzhou and Shanghai. This security stack is fully managed via our "global-local" approach, with certified professional expertise and compliance acumen to provide innovative customized security solutions worldwide. We help our customers achieve unrivaled digital security and peace-of-mind in an evolving digital landscape.

4 Red/Blue Simulation Synergy

A proactive security approach to enhance an enterprise's cybersecurity cycle from reactive defense to proactive guardianship. AI-Red/Blue Cybersecurity Practices cover the entire service stack, from staff training, offensive and defensive drills to network protection solutions, security strategy and service consultation. The Red Team conducts comprehensive AI-powered assessments and simulations, while the Blue Team offers all-encompassing defense services, enhancing enterprise-wide cyber-threat awareness and response.

5 Optimized Professional and Compliance Services

We offer our customers the unique competitive edge of a hybrid "global-local" approach, seamlessly optimizing world-class technical knowledge and facilities, with extensive local business insights. Together with certified expertise in compliance, our scope encompasses a comprehensive range, from consultancy services to Security Device Migration and Cross-Border Data Compliance. With global reach and advanced TechOps capabilities, we are empowering customers with unparalleled trust and security in their digital operations.

Seamlessly Extend Protection to Network and Cloud

Secure Access Service Edge (SASE) for today's Distributed Enterprises

In today's dynamic, digitalized economy, businesses need evolved IT solutions to stay competitive. A Secure Access Service Edge (SASE) is an architecture leveraging a user-friendly SD-WAN orchestrator tool to streamline network traffic across evolving edges (from headquarters to branch offices, datacenters, and cloud edges). This total managed solution simplifies and secures infrastructure while boosting agility and scalability. Businesses can operate without compromise. Applications are responsive, and the entire infrastructure is cost-effectiveness for any user, anytime, anywhere.

All-in-one Email Security and full range of Cloud Backup for Business Continuity

The modern ultra-connected business environment exposes companies to one of the most prevalent cyberattacks: Email, through which over 90% of successful cyberattacks occur. To secure this vulnerability, our O365 backup with advanced email security solution provides an ever-vigilant 24x7 managed service to safely fortify your organizational email.

Beyond email, other systems need protection, especially with businesses increasingly adopting virtualization, cloud computing, and cloud applications into mission critical workflows, and important digital assets extending beyond physical organizational premises. To safeguard these, we offer comprehensive backup solutions encompassing onsite and offsite, virtual machine, and physical server backup, all to preserve precious data and maintain operational resilience.

Identify & Predict	• Code Review Service • AI Visual Security • Vulnerability Assessment Service • Penetration Test Service • Asset Identification Service
Protect	• Versatile Managed Cloud Backup & DR Solution (BRR) • Secure Access Service Edge (SASE) • Managed Unified Threat Management (UTM) • Managed Next-Generation Firewall (NGFW) • Managed Web Application Firewall (WAF)
Detect	• Network Traffic Analysis • Managed Security Services (MSS) • Endpoint Detection & Response (EDR) • Secure AI (UEBA)
Respond & Recover	• Threat Hunting • Versatile Managed Cloud Backup & DR Solution (BRR) • Security Orchestration, Automation and Response (SOAR) • Security Incident Response (IR)
AI SOC	• 3 AI SOCs for cross-border protection • Self-built SIEM-MiiND platform for next-generation threat protection • Local 24 x 7 certified security professionals • ISO27001 International best practice
Professional Services & Compliance	• Security Device Migration Service • China Cybersecurity Law MLPS 2.0 Compliance Service • Security Device Migration Service • Cross-Border Data Compliance Assessment Service

TrustCSI™ 3.0

CITIC Telecom CPC

W: www.citictel-cpc.com
Asia Pacific: info@citictel-cpc.com
Europe and CIS: info-eu@citictel-cpc.com

Hong Kong T: 852 2170 7101
Japan T: 81 3 5339 1968
Estonia T: 372 622 33 99

Mainland China (Toll Free): 400 651 7550
Malaysia T: 603 2280 1500
Poland T: 48 22 630 63 30

Singapore T: 65 6220 6606
The Netherlands T: 31 20 567 2000

TSF2510EN