新一代智能安全运营中心
(AI SOC)

CITIC TELECOM CPC

TrustCSI™ 3.0
云网神盾

信息安全管理服务

全新 AI SOC 网络安全框架

AI SOC 赋能

识别及预测 | 保护 | AI SOC 星智神盾 SIEM-MIND 托管式安全服务 | 侦测 | 回应与复原

› 服务在地 连接全球的数智通讯服务伙伴

中信国际电讯(信息技术)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED
中信国际电讯集团成员
A member of CITIC Telecom International

TrustCSI™ 3.0 云网神盾 AI SOC 赋能

TrustCSI™ 3.0 云网神盾是我们优化的信息安全旗舰解决方案，为您的企业提供最佳保护。方案针对三个关键领域，全面检视及控制信息风险。首先，在现今需求严格实践数据处理的时代，TrustCSI™ 3.0云网神盾强调合规性(Compliance)以符合最严谨的法规要求。其次，此方案易于部署、低前期投入成本、零维护的安全管理服务(Security)，应对日益复杂的IT环境中衍生的威胁。最后，我们利用先进的人工智能，注入创新(Innovation)和智能能力，显著提升阻截威胁的速度、成效和效率。

作为您在数智化时代值得信赖的 TechOps 信息安全赋能者，我们不仅致力于优化防护，更专注于从根本上重新定义未来网络安全框架。凭借二十年的深厚专业积淀与前沿AI应用，我们自建了星智神盾(SIEM-MiiND)，一款可大幅提升SOC营运效率的智能安全信息和事件管理(SIEM)平台。作为AI SOC 的核心，SIEM-MiiND 能提供更快速、更精准的 24/7 全天候威胁分析与监控，赋能企业以前瞻性的主动防御能力，全面对抗不断演变的网络风险。

您值得信赖的TechOps信息安全赋能者

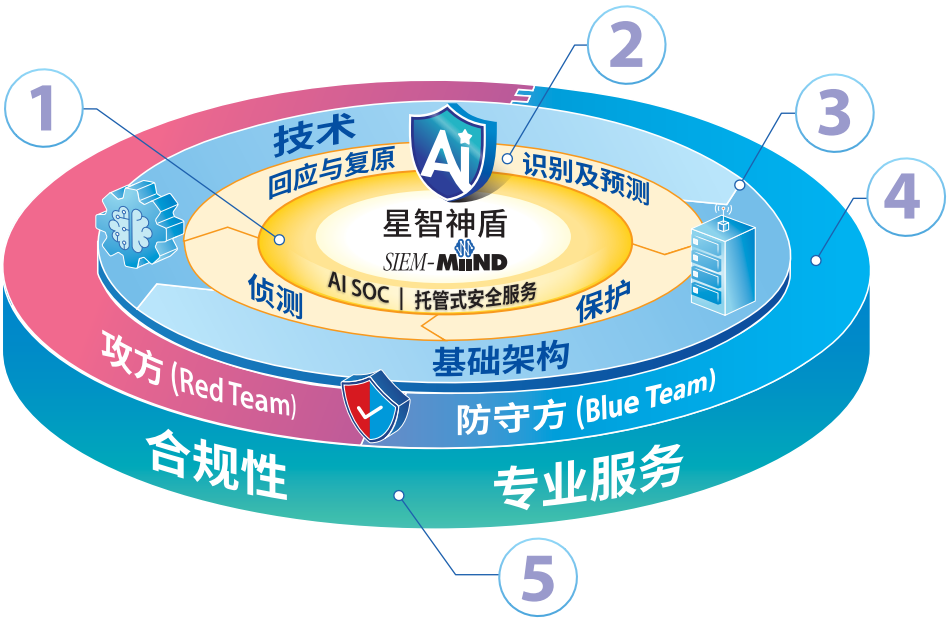
全新 AI SOC 网络安全框架

凭借累积多年信息安全的服务经验，通过全新 AI SOC 网络安全框架，我们将网络及信息安全由被动式保护转化为主动式防御，协助企业轻松应对数智化时代瞬息万变的网络威胁，减低安全风险。

随着现代企业加速数字转型，他们获取了新机遇，但亦因攻击层面扩大而增加风险。同时，由AI驱动的网络威胁日益复杂。因此，构建智能且全方位的网络安全防护，已是刻不容缓。

中信国际电讯CPC致力于成为您值得信赖的TechOps信息安全赋能者。我们充分了解不同行业独特的数字化信息安全需求，全新AI SOC网络安全框架，赋能世界级TrustCSI™信息安全服务，为企业提供全面保护，有效地识别、预测、保护、侦测、回应及复原各种网络安全事件，为企业提供全面保护。

我们的智能网络安全框架是由专业的安全专家团队、3个跨区域智能安全运营中心（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）组成。这一全方位智能网络安全框架聚焦于「人才」、「流程」与「技术」三大核心，并完美融入「AI攻防」实践，以智能化手段精准识别企业IT环境中的潜在漏洞，打造强韧并具前瞻性的主动防御策略，为企业提供最大程度的安全保障。



全新 AI SOC 网络安全框架

1 新一代智能安全运营中心：星智神盾 (SIEM-MiiND)

作为AI SOC的核心，星智神盾是我们信息安全及创新研发团队自主自建的智能安全信息和事件管理平台，具有更高效的数据处理能力和全面的安全监控能力:

提升响应能力

构建了智能化的安全事件检测机制，大大缩短故障排查时间，在发出初步告警邮件后，可较以往快高达75%提供进一步细化的安全建议（视乎安全事件的复杂程度），帮助客户有效减少了业务中断带来的损失。星智神盾亦会针对潜在威胁并发出告警通知，降低企业网络被攻击的风险。

增强检测能力

透过主动地对漏洞和潜在的入侵指标（IOC）进行初步分析，减低对客户网络造成威胁。

智能聊天机器人

为企业提供24/7热线外的新增提问渠道，在安全认证的登入机制下，让企业更及时透过在线及线下途径清楚了解安全事件现况及整体安全级别。

优化规则集

通过AI技术，根据客户的历史资料和新的攻击情景，调整侦测阈值，并就新增设备的日志资料自动及持续创建新规则集，为客户量身订做和微调规则集。

2 SOC4Future 安全策略

SOC4Future 安全策略运用了全面的四阶段测试框架，为企业提供全方位的安全保障：

1). **识别及预测:** 运用一系列全面的评估与识别服务，覆盖系统、应用程式、网络基础架构及关键资产，以精准识别并化解安全风险。

2). **保护:** 透过与全球顶尖的安全技术供应商合作，利用一流的安全解决方案与专家级的安全基础架构管理，确保强韧的防御实力，抵御日益增加的威胁。

3). **侦测:** 凭借三个跨区域的 AI SOCs 和先进的「星智神盾」智能安全信息和事件管理(SIEM) 平台，全面提升了企业快速有效地识别、应对日益频繁和复杂的网络安全事件的能力。

4). **回应与复原:** 运用威胁情报，协调并自动化处理安全事件，最大限度地缩短解决时间，并提供详细的安全事件后报告，以找出根本原因并支援未来行动计划。

3 面向未来的SOC即服务

SOC-as-a-Service(SOCaaS)服务体现了未来的智能网络安全。我们通过基于人工智能驱动的先进安全分析和监控能力，提供出色及优化的安全分析和监控服务。「SOC即服务」(SOC-as-a-Service)由位于香港、广州和上海的3个自建及管理的7x24安全运作中心(SOC)支持。透过我们拥有国际认证、和合规知识及经验的专业团队，提供「服务在地、连接全球」的创新及客制化的安全解决方案，帮助客户在不断变化的数字化环境中，达至数字安全。

4 拥抱「攻防实践」协同效应

以积极主动策略，将整个网络安全循环从被动转为主动。「AI攻防」实践涵盖全栈安全服务，从员工培训和攻防演练，到网络保护解决方案、信息安全策略和服务咨询。攻方执行由AI驱动全方位的评估和模拟测试，而守方则提供缜密的防御保障，确保全面提升企业对网络风险的严密布置。

5 优化的专业及合规服务

我们为客户提供具独特竞争优势的「服务在地、连接全球」混合方案模式，无缝融合世界一流的技术知识和设施，以及广泛的本地业务丰富经验。另外，我们拥有认证的合规专业知识，业务范围涵盖从咨询服务到信息安全设备迁移和跨境数据合规评估。 凭借全球覆盖和先进的TechOps能力，赋能客户高信任度和安全性的数字化营运。

无缝扩展网络和云端保护

分散式企业的安全存取服务边缘方案

在现今瞬息万变的数字化商业环境下，企业需要具弹性的IT解决方案来保持竞争力。安全存取服务边缘方案（Secure Access Service Edge，SASE）利用简单易用的SD-WAN编排工具，简化不断变化的网络边缘（从企业总部到分支办公室、数据中心和云端)的网络流量管理。这项全面管理解决方案，简化并保护基础设施，同时提升灵活性和可扩展性。企业可以持续营运，提升应用程式能力及体验，以及确保整个基础设施具成本效益地为任何用户随时随地提供服务。

全方位的企业邮件安全和云端备份，实现业务持续营运

电子邮件攻击是现今紧密互联的商业环境下，企业最常见的网络攻击之一，超过90%的成功网络攻击都是通过电子邮件。为了堵塞此漏洞，我们先进的O365备份和电子邮件安全解决方案，提供24/7全天候的管理服务，以安全加固企业的邮件系统。

除了电子邮件外，企业也需要全面保护其他系统，尤其是随着企业在各项关键任务的工作流程中，越来越多采用虚拟化、云端运算和云应用，部分重要的数字资产已经超出企业的实体业务范围。为了保护这些资产，我们提供全面的备份解决方案，包括现场和异地备份、虚拟机器备份和实体伺服器备份，以保护企业重要的数据及业务弹性。

识别及预测	• 代码审查服务 • AI资讯安全威胁识别平台 • 漏洞评估服务 • 渗透测试服务 • 资产梳理服务
保护	• 邮件防护服务 • 安全存取服务边缘 (SASE) • 统一威胁管理 (UTM) • 托管式新世代防火墙 (NGFW) • 托管式网站应用程式防火墙 (WAF)
侦测	• 网络流量分析 • 托管式安全服务 (MSS) • 端点侦测及回应 (EDR) • 用户和企业行为分析 (UEBA)
回应及复原	• 威胁搜捕服务 • 多功能托管式云备份及灾难复原解决方案 (BRR) • 安全编排及自动化回应 (SOAR) • 安全事件回应 (IR)
智能安全运营中心 (AI SOC)	• 3 个智能安全运营中心 (AI SOCs) 提供跨区域保护 • 自主自建的智能安全信息和事件管理平台「星智神盾」(SIEM-MiiND) 解锁新一代网络安全防御 • 具认证的安全专业人员提供7x24在地服务 • ISO27001国际认证的最佳实践
专业服务及合规	• 信息安全设备迁移服务 • 中国网络安全法–网络安全等级保护2.0合规咨询服务 • 云专业服务 • 跨境数据合规评估服务

TrustCSI™ 3.0

中信国际电讯CPC

W: www.cititel-cpc.com
亚太区: info@cititel-cpc.com
欧洲及CIS: info-eu@cititel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
爱沙尼亚 T: 372 622 33 99
中国大陆 (Toll Free): 400 651 7550
马来西亚 T: 603 2280 1500
波兰 T: 48 22 630 63 30
新加坡 T: 65 6220 6606
荷兰 T: 31 20 567 2000

TSF2605SC