Trust**CSI**™ SOC | Security Operations Center

Around-the-clock Security Risks Monitoring Services

CITIC Telecom CPC, a leading provider of ICT solutions in Greater China and Asia Pacific, offers an integrated suite of information security services to multinational companies and business enterprises. Grouped under the name TrustCSI™, the services are driven out of world-class **Security Operations Centers (SOCs)** in Hong Kong which are certified with ISO9001, ISO20000, ISO27001 and ISO27017. CITIC Telecom CPC's SOCs are built on top of the company's carrier-grade Network Operations Centers (NOCs), equipped with advanced SIEM technology and managed by certified security expertise. Apart from providing professional training, CITIC Telecom CPC crafts necessary security policies, procedures and processes to ensure the highest standards of services delivery.

HIGHLIGHTS

➢ 24 x 7 around-the-clock monitoring services for real-time threat analysis and handling

➢ Quick identification of obfuscated attacks before they can do any harm

➢ Elimination of false positive through advanced SIEM log correlation and classification technology

➢ Increase productivity of IT staff by releasing them from tedious security monitoring tasks

➢ Real-time and centralized reporting via the online TrustCSI™ end-user portals

> **Global-Local Intelligent DICT Service Partner**

Best Practices of CITIC Telecom CPC's Security Operations Centers (SOCs)

Powerful ArcSight SIEM Technology

CITIC Telecom CPC's SOCs composed of powerful SIEM (Security Information and Event Management) technology for effectively correlating billions of logs daily from different security devices to identify real-time threats timely and accurately.

Professional Team

Certified with CISA, CISSP and CompTIA Security+, our security experts provide proactive threat monitoring and remediation servies to ensure effective risk mitigation.

Consistent and Certified Process

Certified with ISO9001, ISO20000, ISO27001 and ISO27017, CITIC Telecom CPC brings consistency in handling and managing threats and policies across your enterprises.

Online TrustCSI™ End-user Portal

Through TrustCSI™ online portal, enterprises can get an overview of their security status in real-time, including the details of security event handling information.
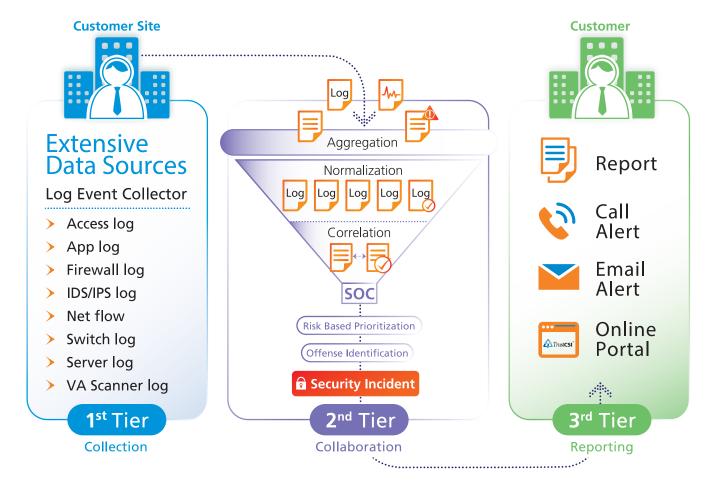
3-Tier Security Operations Architecture

1st Tier | Collecting logs from customers' various security devices for processing initial monitoring, filtering and aggregation.

2nd Tier | Utilizing the SIEM technology for correlating and classifying logs in our SOCs.

3rd Tier | Sending alerts to enterprises if real threats have been identified through email. Customers could download reports and view their real-time security status through TrustCSI™ end-user portals.

Customer Site

Customer

Extensive Data Sources

Log Event Collector

- ❯ Access log
- ❯ App log
- ❯ Firewall log
- ❯ IDS/IPS log
- ❯ Net flow
- ❯ Switch log
- ❯ Server log
- ❯ VA Scanner log

Log

Aggregation

Normalization

Log Log Log Log Log

Correlation

SOC

Risk Based Prioritization

Offense Identification

🔒 **Security Incident**

Report

Call Alert

Email Alert

Online Portal

1st Tier
Collection

2nd Tier
Collaboration

3rd Tier
Reporting