Security Incident Response (IR)

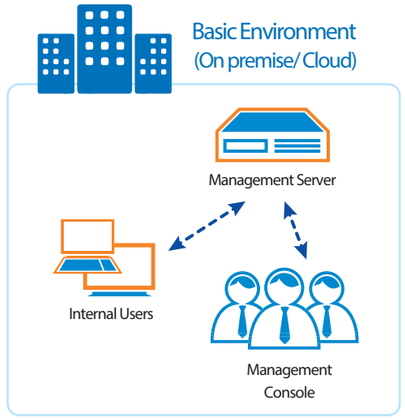
Generally, security incidents occur without warning. Even in the case of discovery, an organization might not have sufficient resources or knowledge to effectively handle and neutralize the attack, resulting in great and sustained damage. CITIC Telecom CPC's Security Incident Response (IR) is a rapid response service with a 24x7x365 highly trained security team to promptly take professional action to investigate and remediate attacks on behalf of the customer. A subsequent detailed "Post Incident Report" will be furnished when the situation has been resolved.

Highlights

- 24x7x365 Dedicated Incident Response Team promptly handles security incident investigation, remediation planning and attack mitigation.
- Memory and hard disk forensics with detailed report on methodology and findings, for presentation to management or legal purposes.
- Detailed "Post Incident Report" including root cause analysis, procedural review, learnings and insights, recommendations for improvement.
- Adaptive Response Framework for initiating automated workflows.

Endpoint Detection & Response Service (EDR)

TrustCSI™ Endpoint Detection & Response Service (TrustCSI™ EDR) is a complete endpoint security solution built for a new era of business. It delivers real-time enterprise protection across the complex modern threat landscape. Diverse imminent endpoint threats (such as phishing, ransomware, and malware) can be instantaneously minimized, with autonomous detection and remediation, diminishing costly breach impacts. With TrustCSI™ EDR, you can quickly and easily protect your organization, keeping its operations running smoothly, with a single, efficient, and cost-effective endpoint security solution.



Highlights

- **Stop Attacks Before They Occur** - Prevent attacks from even beginning to harm your organization by leveraging Next Generation Anti-Virus (NGAV), anti-malware, anti-phishing, sandboxing etc.
- **Runtime Detection and Protection** - When attacks happen, TrustCSI™ EDR's automated full remediation is instantly triggered, even when offline.
- **High Visibility Attack Investigation and Response** - Auto-generated detailed forensics reports provide better system visibility and advanced diagnostic analytics.
- **Automated Rapid Remediation** - Automatically perform specific response activities based upon predefined rules, to block or remediate specific incidents and reduce the workload on incident response teams.
- **Professionally Managed 24x7 SOC** - CITIC Telecom CPC's security experts provide round-the-clock monitoring and managed services to detect and prevent endpoint security attacks with accurate and timely alerts.

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
Russia T: 7 495 981 5676
Taiwan T: 886 2 6600 2588
Malaysia T: 603 2280 1500
Poland T: 48 22 630 63 30
The Netherlands T: 31 20 567 2000
Mainland China (Toll Free): 400 651 7550
Singapore T: 65 6220 6606

CITIC TELECOM CPC

TrustCSI™

Threat Detection & Response Service

Safeguard your Enterprise with Pinpoint Accuracy and Availability

Global-Local Intelligent DICT Service Partner

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
A member of CITIC Telecom International

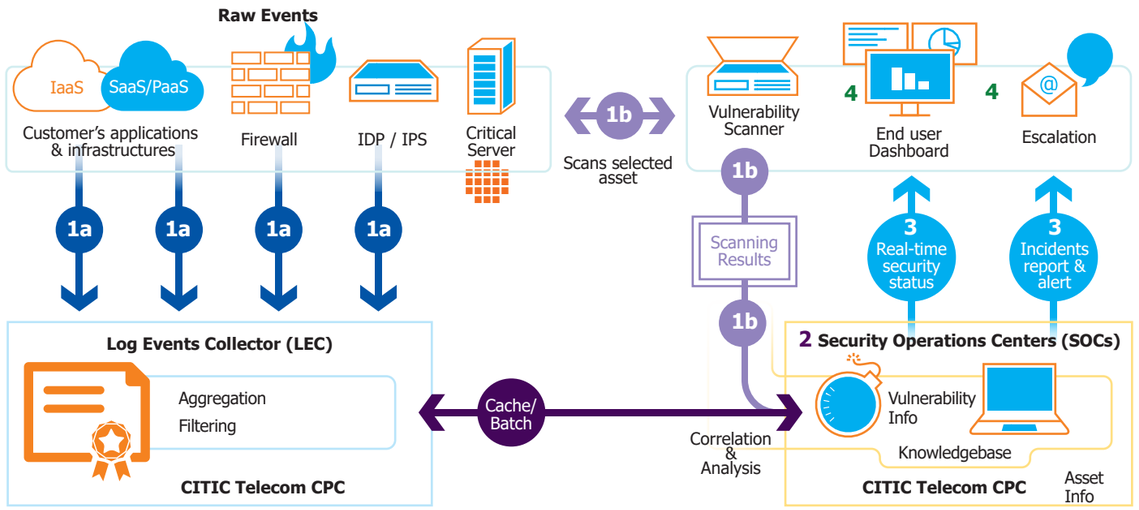
www.citictel-cpc.com

As organizations gain agility, efficiency, reach and competitiveness via digital transformation initiatives, they also become more vulnerable to new threats. Networks that are larger and more functional attract more frequent and sophisticated attacks that are harder to detect. While automated security tools can serve as the basis of enterprise protection, common solutions such as anti-virus software are too slow to respond to the constant stream of zero-day threats and advanced malware. To achieve a more robust security posture requires a highly trained world-class security team that is always on guard round-the-clock. This is the basis of TrustCSI™ Threat Detection & Response Service.

CITIC Telecom CPC created TrustCSI™ Threat Detection & Response Service (TDRS) to serve as an enterprise's holistic IT security task force, leveraging cutting-edge IT security technologies and CITIC Telecom CPC's multiple Security Operations Centers (SOCs) equipped with high availability and disaster recovery functionality. TrustCSI™ Threat Detection & Response Service enables 24x7x365 pervasive visibility across the entire enterprise network, achieving faster threat detection and response to defeat the cyber criminals' advanced new intrusion and camouflage techniques such as packing, encryption, polymorphism, and others.

Advanced Security Information & Event Management Technology (SIEM 2.0)

The new generation of SIEM technology can identify broader range of devices, applications and data to detect and resolve new intrusion incidents.



1a. Raw event logs (Customer's applications & infrastructures, firewall, IDP/IPS, critical server etc.) sent to CITIC Telecom CPC LEC for filtering and aggregation, then passed to CITIC Telecom CPC's SOCs.

1b. Vulnerability Scanner scans selected assets regularly and delivers scanning results for storing in knowledge base.

2. CITIC Telecom CPC's SOCs utilize SIEM 2.0 (Security Information and Event Management) engine for correlation and analysis between meta-log and knowledgebase. Correlated results are classified in appropriate categories and attributed risk levels.

3. In the event the severity of a correlated security event exceeds normal parameters (as agreed with the customer), CITIC Telecom CPC's security specialists activate incident response mechanism. Customers can examine full details via online end-user portal (dashboard).

4. Online TrustCSI™ MSS portal gives customers a complete picture of real-time security status, including full security event handling details, latest security related RSS news feeds from around the world and detailed monthly reports

Designed to be world-class end-to-end service, CITIC Telecom CPC's TrustCSI™ Threat Detection & Response Service are backed by the best in People, Process and Technology

World-class Security Professionals

Dedicated to service excellence, CITIC Telecom CPC's professional IT security experts are some of the best professionals in Asia Pacific, all highly trained and competent across a wide range of industry security domains, including CISA, CISSP and CompTIA Security+ and other certifications.

World-class Security Operations Centers (SOCs)

Built upon carrier-class infrastructure, CITIC Telecom CPC's Security Operations Centers (SOCs) are equipped with cutting edge technologies, including specialized IT security equipment. They are multiple-certified in ISO9001, ISO14001, ISO20000, ISO27017 and ISO27001 Information Security Management System, and following ITIL best practices.

World-class Security Information and Event Management (SIEM) Technology

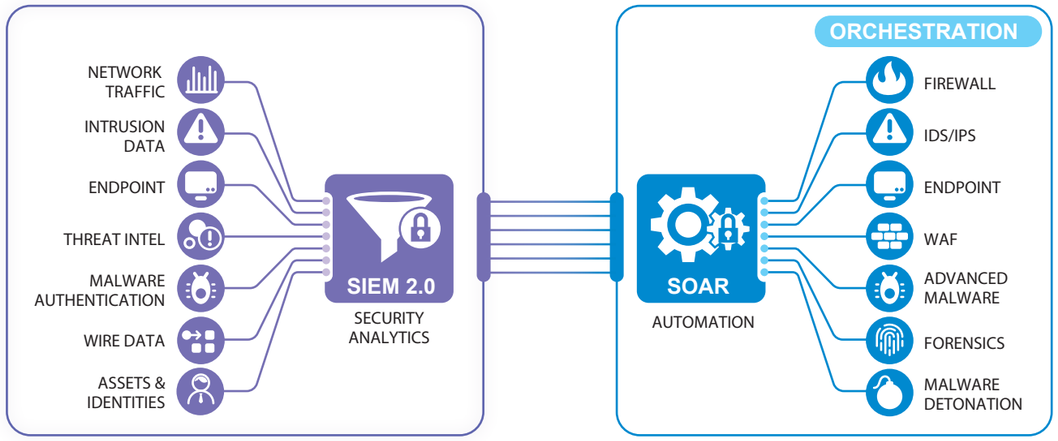
TrustCSI™ MSS is powered by a state-of-the-art correlation and classification SIEM engine, tracking billions of real-time events every second, every day, to help IT security professionals rapidly identify and remediate threats. Damage or theft of digital assets is quickly neutralized or minimized.

TrustCSI™ Threat Detection & Response Service

comprises the Security Orchestration, Automation and Response (SOAR) service, Incident Response (IR), and Endpoint Detection & Response Servce (EDR):

Security Orchestration, Automation and Response (SOAR)

SOAR is a fusion of IT security technologies and processes, consolidating multiple sources of warnings and data regarding attacks, then performing deep analysis to ascertain best practices remediation to mitigate impacts. It leverages standardized workflows to streamline defining, prioritizing, and driving incident response to simplify the process, with automation playbooks that speed up response and eliminate errors, thus overall dramatically improving efficiency. CITIC Telecom CPC's security professionals use both precedent playbooks from previous real-world incident responses, and tailor-made playbooks to address unique customer needs. Via SOAR, a single pane of security control is utilized across the entire environment.



Highlights

Automatically respond to security alerts based on pre-defined playbooks or workflows, speeding up incident response.

Supports integration with 200+ common brand assets including network devices, security devices, servers, endpoints, applications, and more.

Professional playbook customization service based on customer requirements, with trackable and auditable record.

Advanced monthly report with more details & customized monitoring dashboard which is easy to access & with clear visualization.