CITIC TELECOM CPC

TrustCSI™ Threat Hunting

Proactively Arrest Attacks and Reveal Concealed Intruders

Faced with increasing variety, sophistication and frequency of network threats, organizations are seeking better ways to protect enterprise infrastructure. Traditional passive defenses, such as anti-virus solutions and firewalls, while still vital, are no longer sufficient by themselves to combat the breadth and depth of modern malicious attacks. Companies are increasingly shifting towards more proactive security measures, such as Threat Hunting, to address gaps that conventional strategies inadequately cover. To address this evolving need, CITIC Telecom CPC's **TrustCSI™ Threat Hunting** service provides businesses with an innovative defense mechanism that proactively safeguards their digital landscapes.

HIGHLIGHTS

- Proactively prevents damage by identifying and neutralizing hidden threats before their activation.
- Immediate threat hunting capabilities in response to Indicators of Compromise (IOCs) and Indicators of Attack (IOAs), ensuring swift identification and response to potential security threats.
- Enables security staff to trace attack vectors and pinpoint stealthy, even previously unidentified, exploits employed by hackers.
- Facilitates security staff to develop enhanced mitigation strategies, leveraging key findings to preempt and prevent future potential cyberattacks.

TrustCSI™ Threat Hunting

Proactively Arrest Attacks and Reveal Concealed Intruders

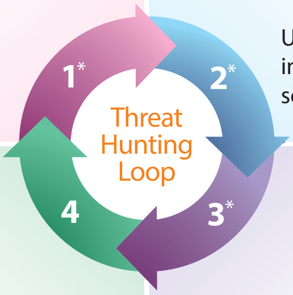
4-tiered Threat Hunting Loop to reveal concealed intruders

Create Hypotheses

Develop hypotheses based on available information and intelligence.

Investigate via Tools and Techniques

Utilize advanced tools and techniques to thoroughly investigate the identified threats by our certified security professional.



Inform and Enrich Analytics

Harness the advanced capabilities of CITIC Telecom CPC's 24/7 Security Operations Center (SOC) to enhance analytics with valuable insights for improving threat detection and response capabilities, ensuring robust security measures for your organization.

Uncover New Patterns and TTPs

Uncover new patterns and Tactics, Techniques, and Procedures (TTPs) employed by adversaries.

***Step 1-3 can be provided by TrustCSI ™ Endpoint Detection & Response Service (EDR):** Existing TrustCSI™ EDR customers can benefit from these features without the need for additional deployment or provisioning.

Your 24x7 In-house Private Investigator

While the benefits of Threat Hunting are clear, enterprises face significant hurdles in adoption. Manually implementing such a security measure is resource-intensive and costly, necessitating the hiring of staff with the right skillsets, otherwise false negatives could ironically elevate the enterprise risk profile. Instead, CITIC Telecom CPC offers a better alternative of a managed security solution via TrustCSI™ Threat Hunting service , ensuring any organization, even smaller scaled enterprises, can harness the compelling advantages of cutting-edge Threat Hunting without high complexity or cost.

User Benefits

- For existing TrustCSI ™ Endpoint Detection & Response Service (EDR) customers, no extra deployment or provisioning required.
- Avoiding disruptive nuisance alerts associated with traditional penetration tests.
- Delivers clear, comprehensible findings to your security staff, presented by our experienced security analysts.
- Swiftly processing vast network traffic data to identify suspicious activities.

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