User benefits

Identifies and stops even the most sophisticated and hidden cyberattacks which manage to penetrate other network security measures.

Goes beyond malware protection, and uncovers unauthorized usage and other suspicious human behavior and infiltration activity.

Ideal for any business concerned about insider threats and other modern sophisticated and targeted cyberattacks.

CITIC TELECOM CPC

User and Entity Behavior Analytics (UEBA) for anomalous enterprise activity detection

Your Global Local ICT Solutions Partner

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

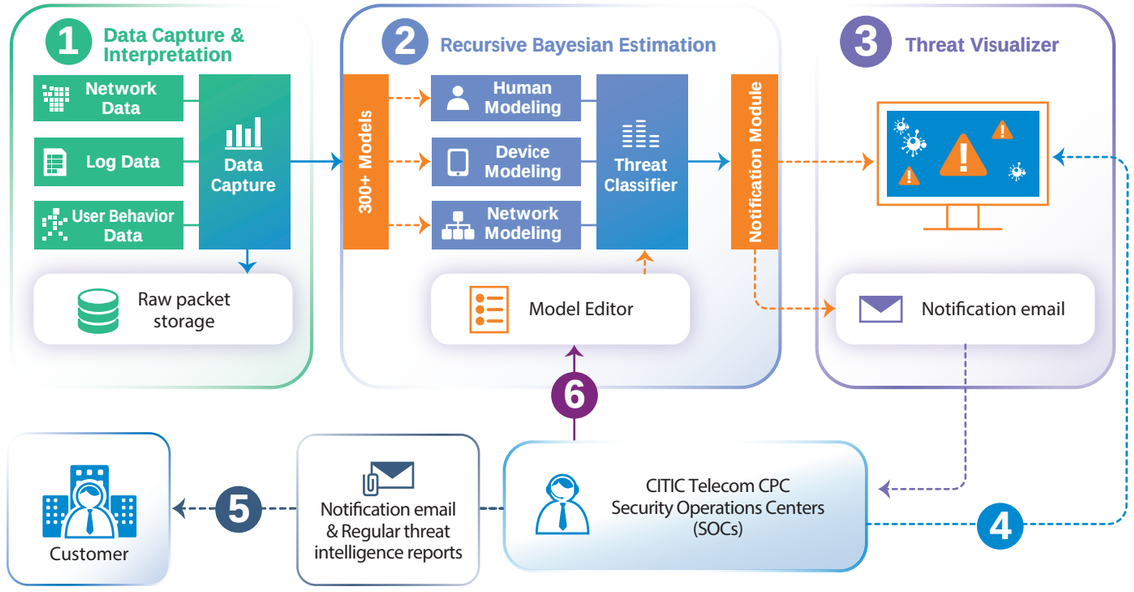
TBA2010EN

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

Combined with behavioural approach and advanced machine learning algorithms to quickly identify all anomalous activities

TrustCSI™ Behavior Analysis Service brings a new approach to enterprise cyber defense, inspired by self-learning biological immune systems. Under this key service, we have **TrustCSI™ Secure AI** which actively investigates all anomalous activities and identifies threats using the behavioural approach and advanced machine learning algorithms to quickly hone in the root cause and severity of the anomaly detected, formulate findings into actionable insight and predict whether any anomalous network behaviour is significant enough to cause alarm. With TrustCSI™ Secure AI, our cyber security analysts can detect real time anomalies within the organizations network, including previously unknown "zero-day" attacks and, provide visibility of emerging threats at various stages during the attack life-cycle. They shorten the time it takes for customers to contain threat and limit the extremity and cost of an attack when it occurs.

A self-learning cyber AI solution to detect and analyse attacks with regular reporting and security policy fine-tuning services



Highlights

- Easily add protection via hassle-free one-arm sniffer deployment
- Adaptively investigates and learns about normal and anomalous enterprise network activities
- Quickly detects behavioral anomalies, such as activity in a data-sensitive area of the network or unexpected decryption
- Continuous fine-tuning of threat modeling by certified cyber-security analysts
- Advanced detection that traditional rule & signature - based approaches do not work
- Fully managed solution includes notification emails, threat intelligence reports and daily configuration backup

Competitive Edges

- Sophisticated heuristics automatically develop behavioural approach mathematical models
- Comprehensive traffic analysis and 100% visibility of network activity
- Granular analysis covers activities from every individual user, device and network
- Analyzes events over long timeframes, with playback capability
- Automatic classification of threats, with intelligent awareness of normal workflow and collaboration

1. Raw traffic data from the network core is collected for analysis, with every packet examined to uncover potential threat risks.
2. This detailed packet-level analysis is massively aggregated to build "life pattern" models for every human user and device on the network, establishing baseline norms for Artificial Intelligence to discern subtle deviations as they emerge.
3. Anomalies are probabilistically assessed in real-time by a Threat Classifier, delivering unprecedented network behavior visibility and ensuring only the most relevant are presented to the security team for consideration.
4. Every detected threat is carefully examined by CITIC Telecom CPC's Security Analysts, then classified and scored in terms of severity and confidence. This analysis is used for network trend visualization and categorizing threat types, and is included in regular threat intelligence reports.
5. CITIC Telecom CPC Security Analysts alert the customer to high priority threats as they occur, and provide regular reports on the threat status of the customer's environment.
6. CITIC Telecom CPC Security Analysts can also create or fine-tune the customer's own security policies and rules via a model editor when necessary.