Qi An Xin SkyEye New Generation Threat Sensitive System

Qi An Xin SkyEye New Generation Threat Sensitive System (referred to as SkyEye system) is a sophisticated solution that provides customers with cybersecurity services and products, specialized in offense and defense penetration and data analysis, focusing on threat detection and response. Based on network traffic and terminal EDR logs, SkyEye system uses threat intelligence, rules engine, file virtual execution, machine learning and other technologies to accurately detect the intrusion behavior of known advanced network attacks and unknown network attacks against hosts and servers in the network. It also uses the local big data platform to store and query traffic logs and terminals logs, and analyze, investigate, backtrack events utilizing threat intelligence and attack chain analysis. Combined with border NDR, terminal EDR, and automated orchestration, the threat can be blocked in time.

CUSTOMER VALUES

Accurate detection of advanced threats

Compared with traditional security detection solutions, SkyEye system can quickly and accurately detect cyber threat attacks with high accuracy and low false positive rate.

Rapid response to major security incidents

Based on the context of threat intelligence, Skyeye system can help security operators to detect, identify and respond to major security incidents, such as Eternal Blue, APT Incident, NotPetya, BlueKeep, Sodinokibi.

Traceback and analysis of cyber attacks

SkyEye system is capable of restoring and storing the metadata of network traffic, which can help users to trace back the network attacks that have occurred, and analyze the attack path, infected surface, and information leakage.

Compliance with upgraded requirements on cybersecurity

SkyEye system meets the upgraded cybersecurity requirements v2.0 for network attack detection and analysis, especially for new network attacks and APT attacks.

PRODUCT FEATURES

Advanced threat detection

By using threat intelligence, file virtual execution, intelligent rule engine, machine learning, and other technologies, SkyEye system can detect and identify advanced network attacks and new types of network attacks, covering: APT attacks, ransomware, WEB attacks, Remote Access Trojans, botnets, stealing Trojans, spyware, network worms, mail phishing, and other advanced attacks. All these threats detected in the network can be clearly shown through visualization technology.

Abnormal behavior detection

Based on network traffic data, SkyEye system uses big data analysis and machine learning technology to build a detection model of network abnormal behavior. With multiple scenarios like built-in unconventional service analysis, login behavior analysis, email behavior analysis and data behavior analysis, SkyEye system detects and identifies new types of attacks and internal violations.

Alarm response

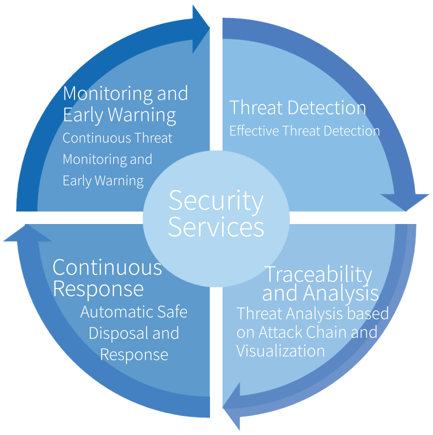
For each attack alarm, SkyEye system provides enterprise users with functions such as listing, counting, querying and investigating. SkyEye system supports analyzing alarms based on ATT&CK tags and the synergy between terminal EDR linkage and firewall NDR linkage, helping security operators quickly identify and respond to alarm incidents.

Attack traceback analysis

SkyEye system supports forensic analysis of full packet, and visual analytics for clues (Threat Hunting), which can present the completion process of an attack for enterprise users, and help users perform retrospective and in-depth analysis of network attacks.

Threat Sensitive
Asset Awareness
Vulnerability Assessment
Threat Intelligence

SOAR
EDR
NDR


Monitoring and Early Warning
Continuous Threat Monitoring and Early Warning
Threat Detection
Effective Threat Detection
Security Services
Continuous Response
Automatic Safe Disposal and Response
Traceability and Analysis
Threat Analysis based on Attack Chain and Visualization

Traffic
Terminal
Server
Mail
Sandbox
Third-party Logs

Monitoring Center
Threat Hunting
Forensic Analysis of Full Packet
Web Breach Detection
Threat Analysis of All Network Traffic

PRODUCT ADVANTAGES

Leading APT detection and tracking capabilities

Qi An Xin Threat Intelligence Center is monitoring more than 40 domestic and foreign hacker organizations that launched APT attacks against government agencies, scientific research, large enterprises, and other organizations in China, dating back to 2007.

Leading threat intelligence capabilities in China

Based on multi-dimensional, global data collection capabilities, cloud-based big data automated processing complemented with the top security research team's manual operations helps to provide users with accurate threat intelligence. Context-based intelligence helps users analyze, investigate, and respond to alerts in time.

Strong synergy

Through linkage of terminal EDR, firewall NDR, and SOAR, SkyEye system helps users quickly locate infected hosts and malware, blocks threats promptly, improving the response and handling capabilities of network attacks.

Computing and retrieval capabilities for massive data

SkyEye system innovatively uses search engine technology as the core technology for local data storage and retrieval, which can greatly improve retrieval performance, provide enterprises with fast search capabilities of terabyte-level of data, and provide solid technical support for local large-scale data retention, attack evidence retention and query, and real-time correlation analysis.

Rich industry cases

SkyEye system has served for more than 1000 customers across all provinces in China. Successful application cases can be found in public security organizations, finance, government ministries, telecom operators, petroleum and petrochemical, power, education, medical and other industries, helping customers identify and respond to more than 100 APT attacks. During the periods of 19th National Congress of the Communist Party of China, the Belt and Road Summit and the Two Sessions, as well as the offensive and defensive drills, on-site safety experts monitored the attack behavior more than 300,000 times through SkyEye system, discovered thousands of exploits, and effectively assisted users to strengthen and protect hundreds of servers according to the attack information, receiving more than 100 letters of thanks from users.