奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

QI-ANXIN Terminal Threat Detection and Response System

QI-ANXIN Terminal Threat Detection and Response System (EDR) is a new generation of terminal security products driven by threat intelligence. It supplements the deficiency of traditional terminal security products in the defense against advanced threats by continuously monitoring terminal activity behavior, detecting security risks, conducting in-depth investigations of threat risks, and providing remedial responses. It achieves better results and faster efficiency against high-level threats, reduces high-level threats, and ultimately achieves its goals.

SECURITY CAPABILITIES

Collection

- Based on the large data storage technology, the undifferentiated collection of terminal behavior data across the network is achieved.
- Full details of collection can be refined to users, hosts, assets, and processes.

Respond

- Based on SkyC2, realize the collaborative linkage between EDR, Skyeye and Skylar, and realize the second level disposal of threat behavior.
- The response mode supports process blackout, terminal isolation, etc.

Detection

- Combine threat intelligence, abnormal traffic detection, terminal behavior detection, and other technical means to identify threat clues.

Analysis

- Based on the relevance analysis engine and visualization technology, the threat can be presented throughout the network.
- Combined with specific scenarios and other attack processes, further enrich global information such as threats.

CUSTOMER VALUES

Through the effective integration of terminal big data collection, storage, detection, investigation and other functions with external threat intelligence, QI-ANXIN Terminal Threat Detection and Response System can help users detect and find hidden advanced threat events more quickly, more easily identify abnormal security conditions and restore the truth of the threat, so as to reduce the cost of threat management and the time and cost of risk response.

PRODUCT FUNCTIONS

Collection and storage of terminal safety

It can continuously collect the safety-related data of the terminals of the whole network, and summarize the collected terminal safety data to the big data analysis platform in real-time for unified storage and management.

Advanced threat detection and warning

Combined with QI-ANXIN big data threat intelligence, threat hunting and other methods, it can quickly retrieve the terminal behavior of the whole network, accurately locate and generate alarms for advanced threat events.

Web: https://en.qianxin.com

GlobalPartner@qianxin.com

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

Investigation and analysis of threat events

Provides the ability to search large data for terminal security, and can conduct in-depth drill-through analysis of threat events, restore the timeline of threat events. Trace its source, analyze the extent of the impact, damage, and other related information.

Fast response to threats

Once the scope of impact is determined, the threat event can be quickly responded to, and the local risk terminal can be quickly isolated and disposed of.

PRODUCT ADVANTAGES

Advanced Threat Hunting Technology

Advanced threat hunting technology centered on artificial intelligence behavior engine covers office PCs and servers for high precision and multi-dimensional advanced threat hunting.

Big data analysis platform with high performance

It can retrieve and analyze a large number of terminal datasets in real-time to help users manage the centralized terminal datasets.

Real-time integration of threat intelligence

Receive real-time threat intelligence from cloud of QI-ANXIN, and convert the information into related indicators, associate with the network terminal behavior data, and locate the collapsed terminal quickly.

Powerful Platform for Investigation and Analysis

Provides the ability to track, analyze, and investigate threats. Deep mining is based on threat events and related terminal context information to discover the network killer chain and restore the truth of events.

Rich means of response and containment

It provides a fast response to high-level threat events, and integrates terminal security management systems to counter threat containment and security repair for different types of risks.

USE SCENARIOS