Introduction

QI-ANXIN's NG-SIEM (Next Generation Security Information and Event Management) is a cyber-situational awareness and security operation platform based on big data. It collects massive heterogeneous data from diverse sources and uses techniques like association analysis, machine learning and threat intelligence to provide decision-making support for risk assessment and emergency response for security supervisors and offer security operation tools like threat detection, investigation and response to security operation personnel.

NG-SIEM home page

Features

1. Cutting-edge Big Data Architecture

NGSOC is built on a big data architecture to cope with the challenges of collecting, storing and computing tons of data. NGSOC can process hundreds of billions of data at a speed of 10W EPS to realize querying which respond within seconds, greatly improving the speed and efficiency of security analysis and response.

2. Powerful Threat Detection

NGSOC uses Sabre, a distributed association analysis engine, with 700+ association analysis rules and 100+ semantics and supporting visualization. The DGA detection technology enabled by machine learning could achieve a detection accuracy of 99.94%.

3. Perfect Closed-Loop Security Operation

NGSOC enables life-cycle management of primary security factors such as assets, vulnerabilities and other factors such as alarm and risk assessment using the closed-loop capability from threat detection, visualization, generalization to coordinated response and neutralization.

Values

1. Continuous Monitoring and Awareness of Security Situation in Real Time

NGSOC helps enterprise security supervisors understand the overall security situation of their organizations quickly and in full picture, identifying security priorities to guide security and IT personnel.

2. Comprehensive and Timely Detection of Advanced Threats
Using a variety of new threat monitoring tools with the support of threat intelligence, NGSOC hunts security threats hidden in various logs faster than traditional SIEM products.

3. Respond and Neutralize by Achieving Closed-Loop Management of Threats
NGSOC provides a variety of response and neutralization methods, and notification of different hazards levels and scope of impact in three major forms including "person to person", "machine to person" and "machine to machine".

4. Early Warning and Comprehensive Dynamics Assessment
To help improve organizations abilities of coping with major cyber threat events and emergency responding, NGSOC provides threat early warning that use imported early warning packages to automatically complete the assessment of how widely an organization's network is affected.

Honors

- IDC: Won the first place with the highest market share and capabilities in IDC MarketScape: China Situational Awareness Solutions Market Vendor Evaluation in 2021.
- CCID: Won the first place with the highest market share in 2019-2020 China network Information Security Market Research Annual Report.
- Digital World Consulting: Won the first place in both marketing execution capability and application innovation in Cybersecurity Situational Awareness Capability Guide in 2020.
- CCID: Won the first place with the highest market share in 2018-2019 China network Information Security Market Research Annual Report.
- IDC: Won the first place with the highest market share and capabilities in IDC MarketScape: China Situational Awareness Solutions Market Vendor Evaluation in 2019.

Customers

The following fortune 500 companies are our customers.

国家电网有限公司 (STATE GRID)	中国南方电网有限责任公司 (CHINA SOUTHERN POWER GRID)
国家电力投资集团有限公司 (STATE POWER INVESTMENT)	国家能源投资集团有限责任公司 (CHINA ENERGY INVESTMENT)
中国电力建设集团有限公司 (POWERCHINA)	中国华电集团有限公司 (CHINA HUADIAN)
中国石油化工集团有限公司 (SINOPEC GROUP)	中国中化集团有限公司 (SINOCHEM)
中石油天然气集团有限公司 (CHINA NATIONAL PETROLEUM)	中国建筑集团有限公司 (CHINA STATE CONSTRUCTION)
中国铝业集团有限公司 (ALUMINUM CORPORATION OF CHINA)	中国核工业集团有限公司 (CHINA NATIONAL NUCLEAR)
中国五矿集团有限公司 (CHINA MINMETALS)	中国电信集团有限公司 (CHINA TELECOMMUNICATIONS)
中国联合网络通信集团有限公司 (CHINA UNITED NETWORK COMMUNICATIONS)	中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS)
中国第一汽车集团有限公司 (CHINA FAW GROUP)	中国兵器工业集团有限公司 (CHINA NORTH INDUSTRIES GROUP)
中国交通建设集团有限公司 (CHINA COMMUNICATIONS CONSTRUCTION)	招商银行股份有限公司 (CHINA MERCHANTS BANK)
中国太平保险集团有限责任公司 (CHINA TAIPING INSURANCE GROUP)	民生银行股份有限公司 (CHINA MINSHENG BANK)
首钢集团有限公司 (SHOUGANG GROUP)	中国宝武钢铁集团有限公司 (CHINA BAOWU STEEL GROUP)
中国远洋海运集团有限公司 (CHINA COSCO SHIPPING)	潍柴动力股份有限公司 (WEICHAI POWER)