

QAX NGSOC SIEM Series

NGSOC SIEM-BD, NGSOC SIEM-LV



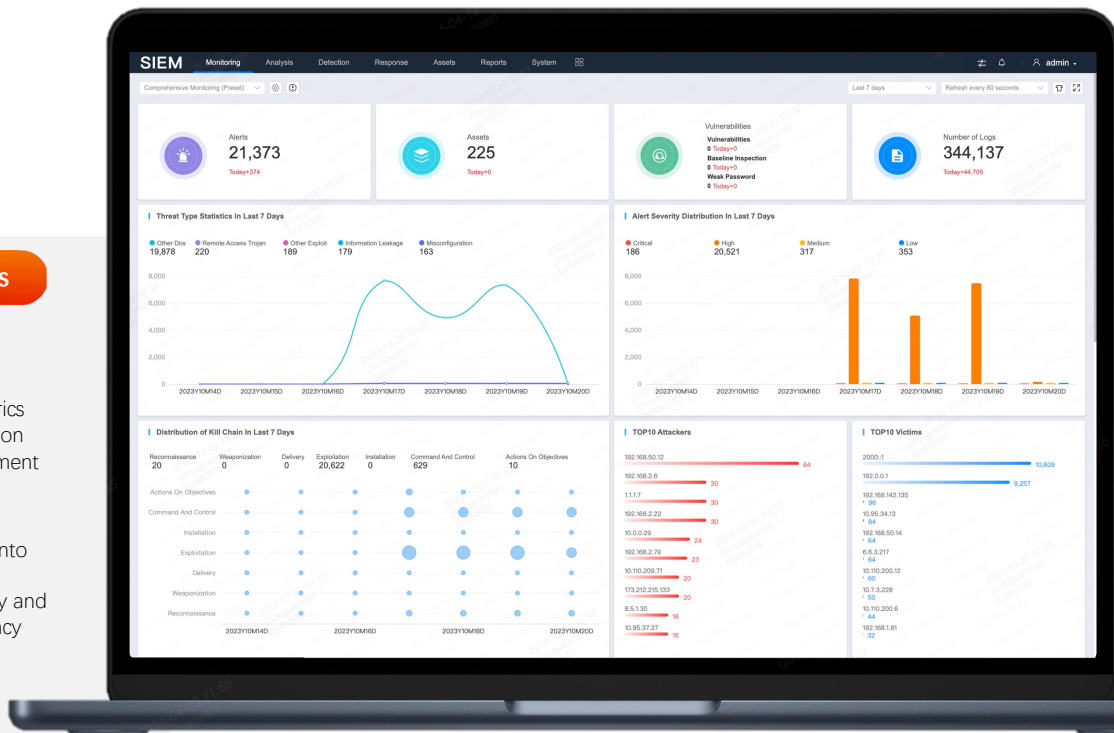
NEW Features

Quantitative Operation

Customizable Metrics measuring Operation Quality & Achievement

Smart Triage


Get alerts triaged into four categories for appropriate priority and thus higher efficiency





Highlights

Secure Business

is the Only Goal of QAX SIEM Solution which helps you:

 **\$4.45 Million***
Save From Loss

 **x8 MTTR***
Enhance Efficiency

 **134%***
Increase Trust

Gartner 2023-2024 SIEM Magic Quadrant Player

QAX SIEM is listed in Gartner MQ published in Q2 2024.

China Top SIEM Player

IDC Report: QAX has the largest market share and is the Top 1 Leader in China SIEM market.

QAX SIEM. Give You Answer, Not Alerts.

The QAX SIEM (NGSOC) series is ideal for realizing Secure Business by providing a centralized platform for SOC team to comprehensively monitor threat trend, aggregate and deeply analyze threat data, command and control resources and response in real time.



Pro Detection

Advanced technologies uncover **known threats** with pattern correlation and **unknown threats** by behavior learning.



TI Driven

Large volume of **Threat Intelligence** enrich all the detection processes to enhance the detection capabilities and efficiency.



Integration

Data Sources, Security Products, and Systems can be all integrated to become a unified monitoring, analysis and command center.



Customization

All the **Parsing Rules, Models, Dashboards, Reports, Notifications**, etc. can be customized to fit the business need.



Automation

Threats can be analyzed by **AI/ML** technology automatically and response work can be executed **automatically** according to response plan.



Visibility

Situation Awareness, Quantitative Metrics, Risk Level of Assets will help to supervise the security level of whole organization and show your value.



Business



Telcom



Aviation



Energy



Finance



Education



Health

SIEM, the Security Information and Events Management system, is the core component of the modern Security Operation Center.

In modern era, potential risk is threatening every corner of the cyber space. To ensure the cyber security, various security products are deployed by organizations to detect suspicious attacks.

According to Gartner's definition, SIEM aggregates the event data that is produced by monitoring, assessment, detection and response solutions deployed across application, network, endpoint and cloud environments. It means that all the alerts and logs will be ingested into SIEM and be analyzed together.

However, the security operation analysts are overwhelmed by countless alerts and logs among which the real-value ones are hard to find, making the security work more inefficient.

Typical Challenges of CISO & SOC Manager



Poor Detection Capabilities to uncover evolving attack tactics and techniques.



Time Consuming to examine Data Sources scattered in different systems.



Lack of Security Talents to investigate large volume of alerts in short time.



Slow Response due to too many Products & Vendors without centralized management.



Limited Visibility of Comprehensive Security and No Quantitative Management.

What if No Next-Gen SOC?



Monetary and Reputation Loss.



Hidden Threats Never Know.



Lose Governance and Control.

Give You Answer, Not Alerts!

QAX NGSOC, increase your ROI of cyber security construction.

Core Capabilities

Smart Triage

QAX SIEM will examine all the alerts and capture only high-value ones via Security Expert Models and Business Expert Models. The Smart Triage will help analysts get rid of 98% noise and increase work efficiency.

Advanced Analysis

QAX SIEM can detect all suspicious attacks with less false positive, through statistical analysis, correlation analysis, sequential analysis, etc. Besides the out-of-the-box models, analysts can create new models within 3 minutes, without learning difficult query languages.

Incident Management

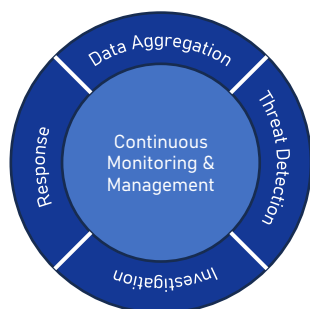
For any highly suspicious incidents, QAX SIEM can gather contextual information automatically, map MITRE ATT&CK knowledge base content, summarize the whole attack process with natural language, and provide specific suggestions, decreasing the MTTR.

Automatic Response

Integrated with various products, the response actions can be identified, defined, orchestrated in the playbooks and executed automatically, which can reduce 92% MTTR.

Out-of-the-box Security Contents

You can directly utilize: 1,000+ Data Parsers; 1,000+ Analytic Rules and Models; 300+ million of internal TI; Integration with QAX TIP; 350+ ATT&CK Techniques; and customized visualizations, dashboards, reports, etc. All the security contents are out-of-the-box, improving the quality of security operation. And they are FREE!



New Features

Quantitative Operation (QO)

Key Value - Visibility

Quantitative Operation is for management and monitoring using key operation metrics collected from TDIR work (Threat Detection, Investigation, Response). Visibility of work quality and achievement are measured and shown via intuitive visuals with which the stakeholders can easily acknowledge the value of security construction, and the manager can make data-driven decision.

Business Challenge

CISO and SOC manager don't have enough metrics controlling the security operation work and showing the value of security investment which normally are invisible and hard to measure.

Product Features

- **20+ Key Operation Metrics:** selected from Gartner, SANS, CNCERT recommendation lists, covering achievement, ROI, efficiency, maturity, risk level, etc.
- **Metrics are customizable:** period coverage, metrics value can be configured.
- **QO Situation Awareness Panel is customizable:** layout and content can be managed.

Smart Triage

Key Value - Efficiency

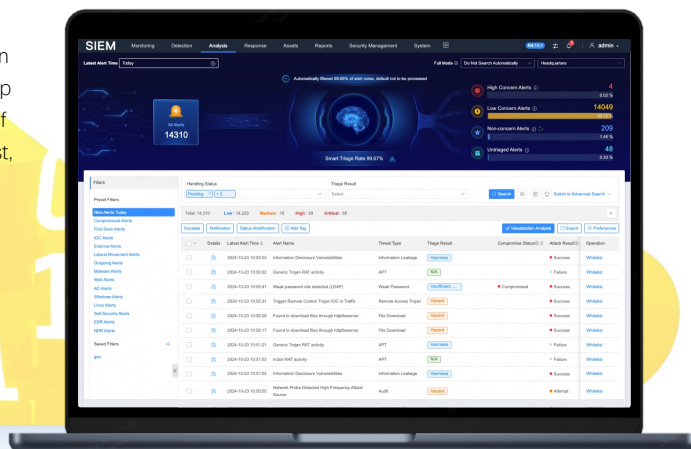
- **98% Efficiency Up** for Alert Triage, beside the threat severity to rely on now the Smart Triage considers the business impact and context information.
- **More Suitable Triage** can be set up via customizable low-code design.
- **Easy Management** for the cleanliness of alert list. The low-concern and non-concern alerts can be handled automatically based on rules.

Business Challenge

It's common that the CISO and SOC manager face the lack of professionals but a huge number of alerts to check. Security experts are not easily available, leading to the capacity pressure especially when attack volume going up. How to distinguish the most important alerts to investigate and response to let the most professional is the biggest challenge.

Product Features

- **Triage Categories:** Smart Triage can categorize alerts into four categories, High-Concern, Low Concern, Non-concern, and Untriaged Alerts. The security experts can focus on high-concern alerts first. The high-concern alert may have huge unfavorable impact on business. A straightforward example of high-concern and low-concern alerts: the same brute force attack targets on CEO's account or an intern account would make a big difference.
- **Customizable Model:** The Smart Triage relies on triage models. The security experts and business experts can work together to construct models that suitable to specific business nature. Low-code design is friendly to get on board.
- **Auto-handling:** For low-concern and non-concern alerts, the team can set up the auto-handling plan of response, such as whitelist, false positive, ignored, to save time and make the alert list clean.





Key Features

Key Features · Data Aggregation

Data Ingestion

Various data sources can be aggregated into NGSOC SIEM. 1,000+ data processing rules are out-of-the-box and can be automatically mapped to the data sources. Besides, the DIY rules such as parsing, filtering, enriching can be created easily for new data sources. It is the fundamental supporting all the detection, investigation, and response work.

Threat Intelligence

TI is useful to detect threats in short time. NGSOC has inside TI knowledge base to refer. QAX Threat Intelligence Platform can be integrated natively. Customized TI can be imported as well to empower the detection process and give more context information for threat hunting.

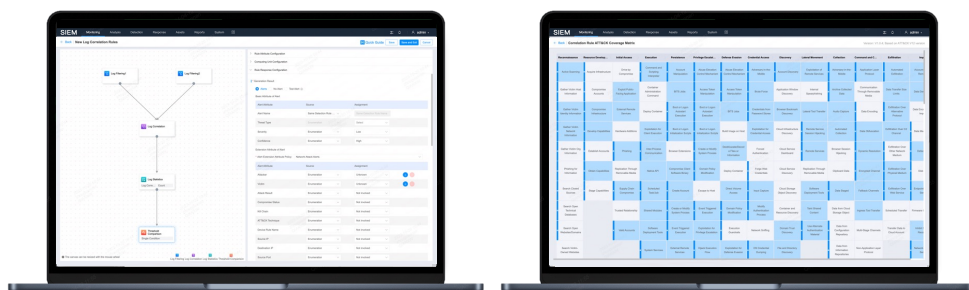
Risk & Asset Mgmt.

Risk level is calculated based on ongoing threats, vulnerability exposure, and asset nature. The algorithm is customizable, and the risk status and trend can be examined in different level. Vulnerability scanning reports can be imported, CAASM solution can be integrated.

Key Features · Threat Detection

Correlation Analysis

Correlation Analysis aims at detecting deeper threats by considering correlated logs and alerts information. It is based on SABRE engine, the QAX self-developed distributed real-time analysis engine, which is the first one and still the best one in China. 1,000+ out-of-the-box models are provided covering more than 350 MITRE ATT&CK cases. In addition, with the low-code design, the modeling team can easily create models according to the security policy.

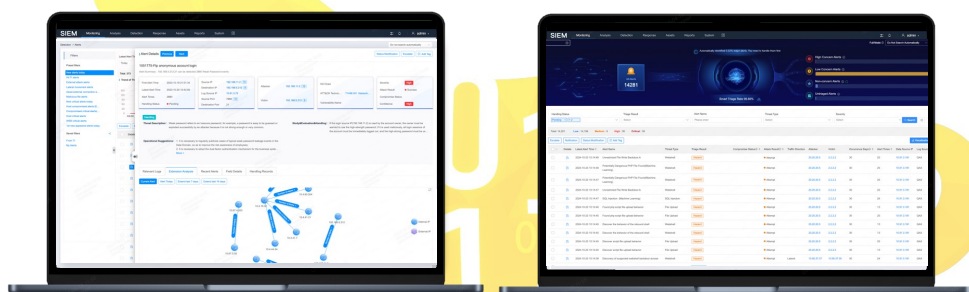


Behavior Analysis

Abnormal Entity Behaviors can tell the unknown threats. Based on ML algorithms, the abnormal behaviors can be found out of the ordinary baseline learned from past records. The baseline space can be generated for a single entity or a group of entities to make the behavior learning more reasonable and reliable.

Smart Triage New

The Smart Triage model can tell the SOC team which ones are most valuable based on security knowledge and the business policy. This is essential for the team with limited capacity.





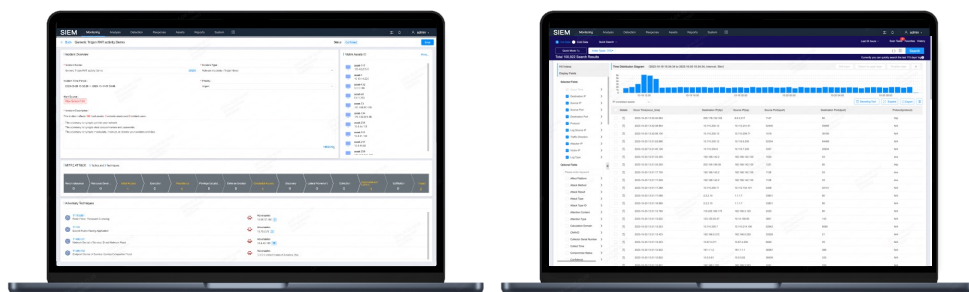
Key Features · Incident Investigation

Incident Workbench

Related alerts can be automatically gathered into an incident to investigate. Useful tools can be found in incident workbench such as MITRE ATT&CK mapping and knowledge base, artifacts and evidence locker, automatic generated brief for the incident, and intelligent suggestion, etc.

Log Search

Threat hypothesis can be verified by researching logs. QAL (QAX Analysis Language) and Lucene Language can be utilized to do the hunting. Billions of logs can be retrieved in seconds. Results can be drilled down, filtered, and visualized to better understand the threats.



Key Features · Command & Control

Response Plan

For fixed response procedure, actions can be designed and stored in response plan. When a typical attack being confirmed, the automatic response can be triggered which can save large amount of time from manual work. All responsive products can be integrated with QAX SIEM.

Key Features · Continuous Monitoring

Situation Awareness (SA)

It's essential for the SOC management team to know the macro-level security situation and make data-driven decisions then command strategically. The interactive visualizations can show the info in real-time in different themes: Comprehensive Operation, External Threats, Internal Threats, etc.

Quantitative Operation New

20+ quantitative metrics can be selected and customized in panel to solve the common headache of security operation management, that is, the work cannot be easily measured and controlled.

Chart, Dashboard, Report

Charts can be created based on log and alert data, and various visualizations can be selected. Customizable dashboards and reports can be created with charts. 100+ templates are provided. Reports can be generated periodically.

System Operation Workbench

All the main services, nodes, clusters status will be shown in a unified page so that the maintenance team can easily notice the system issue. Automatic health check tasks can be scheduled to unitize robot to examine the system health periodically.





Deployment
Available In



On-Prem



Virtual



Cloud

QAX NGSOC SIEM Series Specs

QAX SIEM has 2 versions: LV and BD, abbreviation for Light-Version and Big-Data. The main differences are Process Capacity and Cold/Offline Storage.

Dimensions	NGSOC SIEM-LV	NGSOC SIEM-BD
Target Customer Size	Small	Large, Medium
Process Capacity (EPS)	Max 15,000	Unlimited
Minimum Nodes in Cluster	1	3
Max Nodes Scalable	2	Unlimited
Hot Storage - Traffic Log	✓	✓
Hot Storage - Security Log	✓	✓
Cold Storage - Traffic Log	✗	✓
Cold Storage - Security Log	✗	✓
Archive	✓	✗
Log Sources	Min 50	Min 50
TI Update	✓	✓
Vulnerability Knowledge Base Update	✓	✓
AI QAX-GPT Support	✓	✓

* Note: NGSOC SIEM-LV cannot upgrade to SIEM-BD. SIEM-BD is the most common choice since the need for SOC grows as business volume expands.

A Standard Server Specs

The NGSOC SIEM is mainly installed in local server directly or virtual machine. The vendor of server is not required which can be prepared by customers as long as the critical resources are met including CPU, Mem, and Storage.

Here is the specs info of one standard server QAX can provide:

Dimensions	Spec	Quantity	Note
CPU	16 Cores	2	Physical Cores, 2.4 GHz
Mem	32 G	8	256G in total, DDR4
System Disk	960 G	2	SSD, Raid 1
Data Disk	4 T	12	48T Hard Disk, Enterprise-level SATA 3.5-inch
Network ports	GE port	4	
	SFP+	2	2 multimode optical modules included
	USB 3.0	2	
Other ports	D-Com	1	
	IPMI	1	
	VGA	1	
Height	2 U	1	
Power		2	Including Redundant dual power supply