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

# QI-ANXIN SOAR Security Orchestration, Automation and Response System

## ——Intelligent Orchestration and Automatic Operations

As a security orchestration, automation and response system with advanced technology, complete functions, and practical security operations in China, QI-ANXIN SOAR can help enterprises and organizations sort out the complex security operations (especially security response) processes into tasks and playbooks, convert distributed security tools and functions into programmable applications and actions, and coordinate the team, tools and processes with the orchestration and automation technology.

## CUSTOMER DEMAND

### Five pain points for customers who really value security operation

**Too much work but not enough people**

Insufficient personnel and limited skills
Too much work to do

**Alert fatigue**

Too many alerts to handle
Which is more important? "Alert fatigue"

**Slow response**

Long response time and too much manual work
Difficult to stop loss in time

**Loss of knowledge**

Operational knowledge is mastered by individual
Hard to pass on and accumulate

**Lack of collaboration**

Fragmentation of operational tools
Lack of collaboration among people, tools, and processes

## CORE FUNCTION

**QI-ANXIN SOAR** includes 8 core functions: orchestration and automation management, application management, alert management, advanced alert analysis, case management, war room, ticket management and support management. Among which, advanced alert analysis and war room are optional functions.

### Orchestration and Automation Management

- Visual playbook editor
- Playbook management
- Script management
- Job scheduling management
- Orchestrator based on workflow engine

### Application Management

- Application integration framework
- Application Management
- Application instance configuration management
- Automated application execution engine

### Alert Management

- Alert collection and preprocessing
- Alert triage
- Alert investigation
- Alert automation response
- configuration management

### Advanced Alert Analysis (Optional)

- Alert enhancement
- Alert correlation analysis
- Alert correlation rule management

### Case Management

- Case list
- Case handling
- Artifacts management
- COA management
- Case handling process records and reports

### War Room (Optional)

- Operations team formation
- ChatOps Operation
- Operations Process Visualization

### Ticket Management

- One-time ticket management
- Periodic ticket management
- Ticket lifecycle management

### Supporting Function

- User and authority management
- Platform security
- Open interface
- Other support functions

## PRODUCT FEATURES


- **Security Capacity Orchestration:** Combine decentralized security tools and capabilities with teams and processes;
- **Security Process Automation:** automate the execution of security process and reduce manual participation as much as possible;
- **Intelligent Alert Response:** intelligent alert triage, investigation and response;
- **Case Management Collaboration:** Constantly track the major security incidents by team cooperation, record the whole process, and make review and summary with the case and war room;
- **Open System Architecture:** open and extensible software framework, highly customizable operation process, and friendly and convenient integration of security tools and products.

## PRODUCT VALUE

- **Resource integration and collaborative connection:** organically integrate scattered tools, personnel, and processes and resources required for security operations to realize the connection and collaboration between people and tools, and tools and tools.
- **Automatic operation, load reduction and efficiency increase:** the security operation process or its fragments can be transformed into orchestrated security playbooks and executed as automatically as possible to greatly reduce the workload and improve the efficiency of the security operations personnel.
- **Enhanced alert and rapid triage:** the security operations personnel can investigate and enhance alerts more easily, and perform alert triage more quickly, thereby improving the quantity and quality of alert handling per unit time.
- **Quick response and timely remidiation:** With the orchestration and automation, the security operations personnel can respond quickly and reduce the average response time.
- **Dynamic confrontation and continuous optimization:** Security operations personnel can dynamically adjust and combine playbooks according to practice. The system can automatically record the operation records of all the confrontation processes, which is convenient for summary and continuous optimization afterwards.
- **Human efficiency improvement and efficient measurement:** the automation and digital measurement of the security operation effect can be realized through orchestration and automation to improve the operation level, and the knowledge of experienced security operations personnel can be solidified, deposited, shared, and continuously optimized.