# QAX Threat Intelligence Center

Empowering Cybersecurity with Cutting-Edge Innovations

Organizations continue to fight an unbalanced battle on the cyber defense front. Attackers are sophisticated, well-funded, well organized and use highly targeted techniques. Security teams are overwhelmed with the volume of incidents that needs to be investigated. To the point where they struggle to prioritize the threats that pose the greatest risk to the organization.

QAX Threat Intelligence (TI) Center specializes in TI research and production development. We are committed to providing leading threat intelligence capabilities and security operations for national network security, enterprise organizations.

## QAX  Threat Intelligence Center

QAX Threat Intelligence Center is unique in the industry. Developed by 120+ top security researchers around the globe that apply decades of experience to deliver knowledge about adversaries and motivations, intentions and methods.

With continuous proactive risk assessment our solution helps analyst identify and prioritize the most relevant risks. Integration with QAX technology is also available to automatically perform investigations, speed responses, and enable security teams to move from a predictive to a proactive security posture.

QAX Threat Intelligence Center provides consultancy service to assist customers better align TI skills, tools/services and security requirements towards a well-defined & targeted TI strategy.

"QAX provides actionable threat intel to our organization, especially the focused indicators that are most relevant to us. The custom reputation feeds go a long way, allowing alerting when our IP ranges appearing on data web mentions, registration of domain names typo squatting our web properties. "

**YiLi Chen – Chief Security Officer, Bank of GuangDong, China**

## Benefits

**Proactive Threat Hunting & Detection**

Hunt with built-in hunting packages for threat actors

**Prioritize the resources to address the TTPs that matter**

Prioritize the specific threats to your organizations and map the defenses accordingly

**Improve security operation efficiency**

Expedite the threat investigation and IR process

## How It Works

**Collection**

200+ sources ranging from open source, commercial, industry-led, community driven and customer feedback.

**Curation**

Enriched information about the identities, motivations, characteristics and methods of threats, commonly referred to as tactics, techniques and procedures (TTPs).

**Processing**

Aggregation thousands of indicators for enrichment, normalization, deduplication, search and usage in other tools, categorized with alignment to industry-recognized frameworks.

**Dissemination**

Full dissemination methods including data feeds, API service, local TIP platform, APT report, IR service and product integration.

TI INSIDE Program
Threat Intelligence Operations System (TIOS)
Threat Intelligence Platform (TIP)
QAX Security DNS (QDNS)
Threat Analysis Arsenal
Real-Time Threat Monitoring Platform (Threat Radar)
Threat Analysis Platform (TAP)

Machine-Readable Threat Intelligence
TI INSIDE-Threat Intelligence Endogenous Product Solutions
Human-Readable Threat Intelligence
**THREAT INTELLIGENCE CAPABILITY SERVICE**
Localized Threat Intelligence Analysis And Operations System
Cloud-Based SaaS Service Platform

IOC, Indicator Of Compromise
IP Reputation
File Reputation
URL Reputation
Vulnerability Intelligence
APT Intelligence
Security Advisory

## QAX Advantages

**Insight into the adversary group**

Deep understanding of adversarial planning through observation of activity within the attacker's development environment before attacks are launched.

**Rich context to mitigate threats**

Build attack context for the alerts that they face Threat Intelligence is mainly derived from three areas, attacker's environment, response strategy and never-before seen TTPs.

**Actionable Threat Intelligence**

Comprehensive offering that guides tactical security operation actions and strategic security decisions, organizations can better manage risk and response to today's attacks.

## System Requirements

**Operating System:**

Centos 7.5 or above

**Hardware configuration：**

(1)CPU: Intel 4214*2, Main Frequency 2.2GHz，

Number of cores 12，Cache 16.5 MB L3

(2)Memory: 32G*2 DDR4 2133/2400/2666/2933MHz

(3)Hard Disk: 4T SATA*2

(4)Network Card: Gigabit NIC with 4 electrical

ports + 1 10 Gigabit NIC

## About QAX

QAX, the largest cybersecurity company in China, is a leader in global cybersecurity industry, offering next-generation enterprise and national-level solutions. As the official cybersecurity and antivirus software sponsor for the Beijing 2022 Olympic and Paralympic Winter Games, QAX successfully ensured the event's security with unprecedented "Zero Incident" record.