QI-ANXIN Threat Intelligence Center— Defend against Threats with inside Intelligence in China

QI-ANXIN Threat Intelligence Center (QAXTIC) is a professional threat intelligence team belonging to QI-ANXIN Group. Based on advanced big data on network security, QAXTIC focuses on developing key technologies on network security. By organizing an excellent team of TOP experts all over the Asian-Pacific region, QAXTIC own the complete and accurate capacity on threat intelligence analysis, and provide relevant service to organizations and enterprises on threat protection of network security.

As one of the largest vendors on threat intelligence in China, QI-ANXIN engages in collecting and analyzing malware and other network data. From independent study, business cooperation, and open sources, QI-ANXIN has accumulated more than 1 trillion files, and years of pDNS data. At the same time, QI-ANXIN continually monitors APT groups on this planet and publishes analysis reports on APT activities (https://ti.qianxin.com/blog/tag/APT/). So far, network security services from QI-ANXIN has covered majority of government sector and large-scale enterprises in China.

01 Massive Machine-readable Threat Intelligence (MRTI)

Indicator of Compromise (IOC)

By monitoring network infrastructure used by cyber attacker, QAXTIC could provide accurate IOCs, which helps enterprises to find out their compromised endpoints and block risk as soon as possible. Threat intelligence can reduce Mean-Time-To-Detect (MTTD) significantly, which brings extra time to implement security measurements of containment, mitigation, and remediation. Furthermore, the actual loss can be controlled in a lower level.

File Reputation

Relying on rich sample resources in the cloud and various technical methods, QAXTIC can judge whether a file is malicious and provide more information like malware type and malware family. By searching for hash value and other indicators, subscribers could obtain results with rich context information, including indicator of compromise (IOC), to stimulate correlation and analysis.

IP Reputation

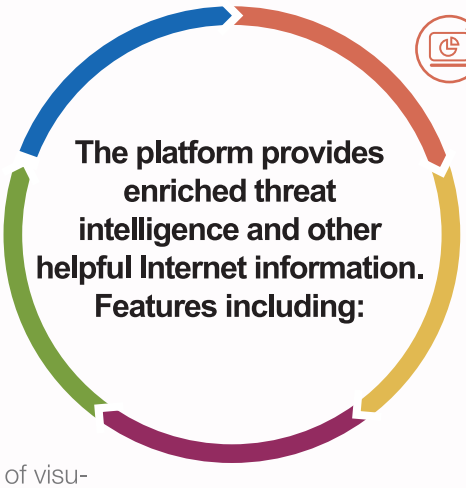
QAXTIC provides details about IP addresses including their location, autonomous system number (ASN), owners type (e.g. enterprise gateway, carrier exit, individual user), malware attributes (e.g. DDoS, botnet, spam, brute force, and scanner), etc. According to a certain IP's malicious attributes, network administrator can block those IPs which has automated attack behaviors such as frequently scanning, credential stuffing attack, etc. By leveraging IP intelligence, network security staffs can classify existing security alarms and obtain more details on attackers.

02 ALPHA Threat Analysis Platform

A SaaS analysis tool provided for security engineers/analysts, can be used for confirming alarms, prioritizing events, acquiring context information of events, and tracing attackers.

Intelligence Supply

Performance data of almost 1 billion individual files in sandbox. Otherwise, ALPHA provides IP reputation of billions of IPv4 address with their attack history.



Data Integration

ALPHA provides massive pDNS data, including information about nodes and scales, and years of records on WHOIS.

Monitoring and Investigation

ALPHA traces thousands of cybercrime groups and malware families, and discovers remote servers used by APT groups.

Visualization Interaction

The platform offers measures of visualized correlation and analysis, which can automatically mine and search related Internet resource, including domain names, IPs, email addresses, attack events, and malware.

Various APIs

ALPHA offers easy-to-use REST APIs for different purposes, including IP reputation, IOCs, and file reputation. It provides excellent efficiency of batch query, and response information sufficient enough at the same time.

03 QI-ANXIN Threat Intelligence Platform (QAXTIP)

This platform is an analysis tool, which helps enterprises use threat intelligence to improve their perception on big data of network security, and find out the real and critical threats from massive alert logs.

QAXTIP has an open products framework and a compatible performance to interoperate with other platforms, such as a SOC or a SIEM. Its strengths on data and functions are following:

High value

QAXTIC has the World-class APT tracking and discovery capabilities, and data comes from the newly discovered and named multiple APT groups. Ahead of other Chinese vendors, QAXTIC has the continuously discovery capabilities to disclose new APT groups.

High accuracy

In results of several users' practical tests, the accuracy is above 99.9%. As they said, it indeed meets the actual needs, and saves time for their security operation team.

Massive quantity

With fast APIs performance, it contains a 60 million IOCs, more than a billion-level IP reputation database, and a billion-level file reputation database.

Threat Intelligence could play a key role in active security defense and is a compulsory course for enterprises to refine their security management.

Twitter: @ RedDrip7 https://ti.qianxin.com ti_support@qianxin.com