SERVICE BRIEF

THREATQUOTIENT™

THREATQ™ PARTNER INTEGRATION PROGRAM

The power of the ThreatQ platform lies in its open, extensible architecture, allowing for strong integration and interoperability with the tools you use today and the tools you may be considering across a broad spectrum of services.

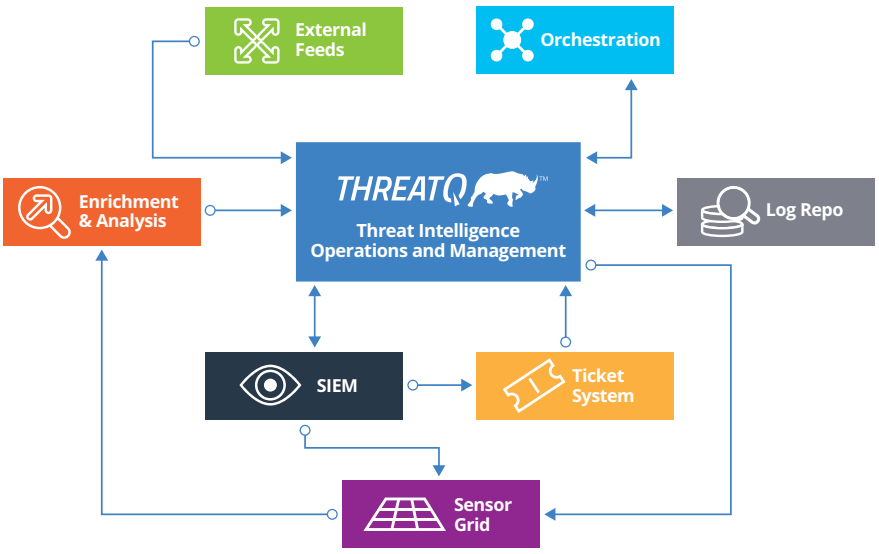
ThreatQuotient's™ Partner Integration Program is a robust ecosystem that leverages the ThreatQ Open Exchange™ through a software development kit (SDK), easy-to-use application programming interfaces (APIs) and a comprehensive set of industry-standard interfaces to fully integrate with the equipment, tools, technologies, people, organizations and processes that protect your business.

The Open Exchange allows the ThreatQ platform to populate the Threat Library™, enrich that data and connect to other systems in your environment, sharing data within the business processes of your organization. These integrations and operations minimize the administrative work analysts have to do and helps them focus on improving security posture.

OPEN EXCHANGE

OPEN EXCHANGE ARCHITECTURE

Your security posture depends on your ability to process potential risks to your business as they emerge. This includes the ability to rapidly ingest millions of indicators at high frequency and distribute accurate and relevant intelligence to the systems and people that protect your assets. ThreatQ's Open Exchange allows analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting along with an SDK and APIs for custom connections.



OPEN EXCHANGE PARTNERS AND INTEGRATIONS

The Open Exchange includes out-of-the-box integrations with most of the popular intelligence feeds for external data, systems for enrichment and analysis, SIEM and log repositories to include internal data, as well as orchestration tools, ticketing systems and sensors, so you can use relevant intelligence to strengthen your defenses. With over 50 commercial partners and more than 100 open source feed integrations, the Partner Integration Program helps drive coordinated threat operations and continues to grow.

CYBER THREAT INTELLIGENCE FEEDS

ThreatQ works with commercial, open source, government, industry, internal and custom intelligence feeds. The platform is format-agnostic and supports standard interfaces for ingestion and exporting. This feed data populates our Threat Library, so you can better understand threats, profile adversaries and improve team collaboration.

ENRICHMENT AND ANALYSIS

Context is critical to understand threats and determine relevance. ThreatQ provides in-platform access to several leading commercial and open source tools to enrich and contextualize threat data. Correlated events can be supplemented with additional information around IP geolocation, registrar, files, domains and URLs. Use standard tools built into the platform or incorporate your own tools as part of the enrichment process.

SIEM AND LOG DATA

The addition of internal events from SIEMs and log repositories is important for context, relevance and priority. ThreatQ integrates with these solutions to combine this internal data with external threat data, providing you with a greater understanding of threats, better focus and faster detection within your environment.

ORCHESTRATION

ThreatQ provides connectivity to security automation and orchestration tools so you can execute playbooks that you've already created. Events can be stored in the Threat Library for continual analysis and tuning. Orchestration tools can also query the ThreatQ Threat Library serve as a customized enrichment source.

CASE MANAGEMENT / TICKETING

Automating the incident response process via ticketing systems is common practice. ThreatQ integrates with leading commercial and open source ticketing systems, with the Threat Library serving as a customized enrichment source. Through this integration, you gain value from existing investments in systems and training while still realizing the benefits from intelligence stored within the ThreatQ platform.

SENSORS

Once threat intelligence is known to be relevant to your infrastructure, it is important to distribute this intelligence to your sensor grid to harden defenses. ThreatQ can send specific actions, rules or signatures to network and endpoint security solutions – firewall, IDS/IPS, Web proxy, advanced malware protection, etc. – or other devices via APIs. Actions can be configured and automated based on parameters you set.

SUPPORTED FORMATS

- STIX/TAXII
- XML
- JSON
- PDF
- Email
- CSV
- Additional formats of structured and unstructured data

For more information and a current list of integrations. visit www.threatq.com/integrations.

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

TQ_ThreatQ-PIP-Program-Overview_Rev2