Vendor Question List for Threat Intelligence Platforms

A threat intelligence platform (TIP) empowers SOCs, threat intelligence analysts, incident response, risk management and vulnerability teams to not only respond to events and alerts, but to also anticipate threats and become more proactive. The key to enabling this is that the TIP serves as the central repository for all threat data from both external and internal sources - fostering collaboration, better decision making, proactive measures and accelerated detection and response. The platform must be able to help you understand, prioritize, and act upon the most relevant threats facing your organization

This list outlines the essential questions you need to ask a threat intelligence platform vendor prior to making a decision. Use this as a quick reference and download the Buyer's Guide to Threat Intelligence Platforms to get more details.

Ingest Data

- How many out-of-the-box commercial feeds and open source feeds do you have?
- Do customers have the ability to enable/disable individual feeds?
- Do customers have the ability to enable/disable components of a feed? (i.e., I only want to import intelligence associated with industries x, y, and z.)

Context

- Are customer-initiated or customer-defined IOC context shared across the vendor's other customers?
- If an indicator was seen more than once, does the subsequent sighting of the indicator override the prior sightings?
- Am I able to define custom attributes to fit the needs of our organization (i.e., Bitcoin addresses, Twitter handles, SWIFT code)?

Scoring

- Can customers customize scoring based on their own organization, team, resources and capability without those customizations being broadcasted to your other customers?
- Can I design the scoring algorithm to determine what information it is based on?
- Do you support negative scores?
- Can I control the score associated to feeds?

Expiration

- What is the vendor's approach to expiring intelligence?
- Can I adapt the expiration methodology to align with my customized scoring and capabilities of my sensor grid technologies?
- Can the TIP automatically adjust expiration dates based on parameters I set?

Correlate Internal and External Data

Do we need to pay more for API use for integrating internal and external data?

If bidirectional data is enabled, does your company have ownership rights to my company's data within the system?

To address the integrations I need, must I open additional ports on the firewall?

Integrations

Do I need to pay extra for API use for integrations?

Do you have bidirectional integration with all the SIEMs, ticketing systems and vulnerability management solutions?

What other tools do you support with bidirectional integration?

Do I need to engage professional services to handle integrations?

Does SIEM information become shared information?

Notifications

Can an analyst create an alert list within your dashboard on any object in the system?

Is the alert notification within the UI, email, or another third-party client (e.g., Slack, HipChat, RSS feed, etc.)?

Export

Does the export include the most common out-of-the-box file formats (e.g., CSV, JSON, CIF, etc.)?

Can an analyst export any object and any supporting context?

Does the export support a scripting language to allow comprehensive control over the type and format of information being exported (i.e., can an analyst define what intelligence is being exported and output it in a technology specific format within a single UI)?

Can an analyst configure multiple export feeds (i.e., by sensor technology, per geographic location or to support daily exploratory research)?

Sharing and Collaboration

Can the TIP serve as a shared workbench for all members of the security team?

Are we able to integrate the collaborative functionality into our existing workflow? If so, how and is there additional cost involved with this integration?

Can we opt-in and opt-out of sharing data with a vendor or community?

Is the shared data anonymized and how?

If data is shared, how is it used by the vendor?

Is the TIP vendor assuming ownership rights to any data shared within its platform?

Deployment Options

- Am I the sole owner of my data?
- Is my data being co-mingled with other customers in a multi-tenant environment?
- What capabilities do I lose if I do not deploy an on-premise integration server?
- If a cloud provider's infrastructure goes offline, what functionality is lost?
- Can you share copies of your quarterly third-party performed penetration tests?

Pricing Models

- Is there a cost per integration or API with each defense system? If so, what is that cost?
- Is there a cost associated with integrating custom data or IOCs?
- What is the total cost of ownership given my business requirements?
- Are there additional costs associated with a private instance of cloud-based deployment?
- Can we adjust the number of user licenses without penalty?
- Is there an unlimited users license option?
- Is there special pricing for managed security services (MSSPs)?

Support

- Are there various methods to contact support?
- What SLAs are offered in regard to support tickets?
- How do I update support tickets?
- How can I escalate an issue?
- How are features requests handled and how quickly are they addressed?
- How are bug reports handled and how quickly are bugs typically resolved?
- What is the RMA policy? (If applicable)

ABOUT THREATQUOTIENT™

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system.

For additional information, please visit threatq.com.

TQ_Vendor-Question-List-for-TIPs_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885