THREATQUOTIENT

EXECUTIVE BRIEF

Choosing an Enterprise Grade Threat Intelligence Platform (TIP)

Overall Considerations

When making a decision to implement a Threat Intelligence Platform (TIP) it is important to consider the profile, quality and future potential of the partner that you select. With more than 2,000 security companies in the industry today, not all technology vendors are equal, nor do all vendors have the strength to deliver on the promises that they make.

Making an investment in a threat intelligence platform is an important decision, as a TIP becomes a core part of your existing security investment, fusing together disparate data sources, tools and teams to prioritize threat risk and accelerate threat detection and response.

First and foremost, the decision to pursue a threat intelligence platform project should be viewed as a journey, not a simple product purchase, and we urge you to carefully choose the organizations that you partner with for this strategic technology.

When making an investment in this category we suggest that you consider a number of factors:

- **Platform Maturity, Architecture & Capabilities**
- **Services, Implementation & Post Sales Support**
- **Users & Customer Base**
- **Company History, Team & Ability to Execute**

Platform Maturity, Architecture & Capabilities

As with any security investment, the maturity, architecture, and capabilities of a TIP are critical in the decision. Because a TIP becomes a core part of your security infrastructure, it's important for the platform to be stable and scale to the needs of your organization while connecting the disparate data sources and tools used by your security technologies and teams.

Development on the ThreatQ Platform began in early 2013, well in advance of other competing products entering the market. This is significant as the team could focus on making sound architectural decisions which ultimately resulted in an Enterprise Grade Threat Intelligence Platform from the start. As the market has matured with more companies offering solutions, these architectural decisions and the ten plus years of learning and experience have increasingly become an important

ABOUT THREATQUOTIENT

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data.

ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

differentiator as companies evaluate ThreatQ versus competing TIP providers.

An Enterprise Grade Threat intelligence Platform is scalable and stable with a broad ecosystem of integrations supporting a wide range of use cases.

A focus on data empowers teams to quickly identify the threats that matter most before taking action. The ThreatQ DataLinq Engine powers a TIP that is more scalable, easier to manage, and yields a better outcome at a faster pace. With a fully customizable data model, no other company can offer the same degree of flexibility in handling data. The ThreatQ core platform capabilities like dynamic scoring, prioritization, and no-code automation are best-in-class thanks to the ThreatQ data-driven approach.

Development on the ThreatQ Platform began more than a decade ago. Currently at Version 5, the platform demonstrates a level of stability and maturity beyond competing products. Perhaps best proven by being selected as the TIP for many of the largest companies and government agencies in the world. ThreatQuotient also maintains open communication with intelligence feed partners to receive early notification of changes that may affect integrations allowing these changes to be proactively tested and updated if required. Further, enterprise software demands platform resiliency, and resiliency takes a solid QA and development process. Factors such as these have enabled ThreatQuotient to earn and retain certifications like SOC2: Type 2 SOC Level 2.

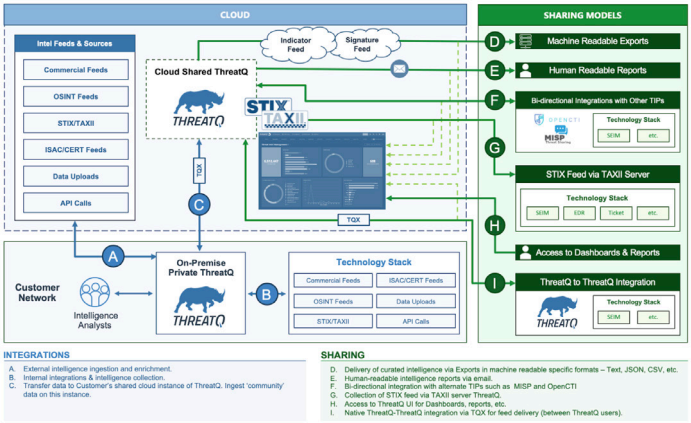
A broader reach across the security infrastructure means better visibility and context for users; this plus the ability to bring the data together on one platform simplifies the challenge of quickly understanding the threat and taking action to neutralize it.

The ThreatQ breadth and depth of integrations enables ingestion of any data source and bi-directional integrations with SOC tools and technologies. Commercial feeds, open source feeds, ISAC feeds, proprietary data, structured and unstructured data can be consumed by the platform and stored for continuous access via the Threat Library, a single source of truth for threat detection and response data and related context. By storing and prioritizing the data collected from previous detections, investigations and incidents, the Threat Library serves as organizational memory and learns and improves over time. The ThreatQ marketplace provides integrations to more than 400 security products and services with the extensibility to develop others as needed.

ThreatQ works with your existing processes and technologies to make your people and technologies more efficient. The platform gives security operation teams the ability to address a number of popular use cases including: Threat Intelligence Management, Threat Intelligence Sharing, Incident Response, Alert Triage, Threat Hunting, Phishing Analysis, and Vulnerability Prioritization.

THREATQ SMART COLLECTIONS

ThreatQ Smart Collections are core to providing scalability on the platform. Users can quickly create highly refined data collections using flexible filter controls, and then use these Smart Collections to drive analysis in dashboards, investigations in ThreatQ Investigations, automations in ThreatQ TDR Orchestrator, sharing across a community of users and much more.



ThreatQ supports integration and sharing across a wide range of technologies fostering collaboration without restrictions.

Services, Implementation & Post Sales Support

The complexity of an enterprise's security environment and the diversity of its security technologies means that deployment of a Threat Intelligence Platform involves upfront planning and subsequent implementation. While many organizations may possess an internal capability to implement and deploy a TIP, others will rely on the company they choose to partner with for this strategic platform. When selecting a TIP provider, it is important to consider the support and implementation services that a vendor can offer. To put it in simple terms, is the vendor easy to work with and do they show the flexibility to adapt to your processes and commitment to shared success?

ThreatQuotient provides a number of delivery services either directly or indirectly through a growing network of integration partners. The objective of a TIP is to accelerate threat detection and response, and our objective is to assist you with the planning and implementation to deliver on that mission.

Professional Services:

ThreatQ provides professional services for clients at all levels of security operations and threat intelligence maturity. The team leverages industry-leading practices and expertise from personnel with decades of combined commercial and government threat intelligence and operational cybersecurity experience.

The services provide the core capabilities to assess, design, and build data-driven threat intelligence functions. The Professional Services team identifies the people, processes, and technologies necessary to effectively integrate intelligence into security operations and cyber risk management programs. These services enable the enterprise to transition from traditional signature-based monitoring, detection, and response to an external threat-focused operations program.

Customer Success:

ThreatQ's Customer Success Team is committed to a proactive approach to ensure clients continue to see increasing value from their investment as their needs change and evolve. Beginning with an onboarding process, a dedicated Customer Success Engineer will meet with clients on a regular scheduled basis. The CSE endeavors to understand the challenges a client is facing today as well as future goals, setting milestones and tracking progress along the way. Having this type of relationship allows Customer Success to act as the client's advocate within ThreatQ.

Training & Certification:

Education is a cornerstone of cybersecurity, and our dedication to fostering knowledge has routed in ThreatQ Academy. This educational platform serves as a hub for professionals seeking to deepen their understanding of threat intelligence. Offering courses, resources, and certifications, ThreatQ Academy is ThreatQuotient's commitment to our clients and partners to evolve along with them in their pursuit to protect their information technology assets. ThreatQ Academy provides standard training modules as well as custom-tailored learning solutions that can meet virtually any operational need and be accessible when they are needed.

Certification through ThreatQ Academy is an important investment. In the constantly changing cybersecurity landscape where threats are always advancing, having certified professionals on the team can make an impactful difference. First, certification serves as a means to develop team members into experts in threat intelligence. It equips them with the knowledge and skills required to effectively identify, assess, and mitigate cybersecurity threats. This not only enhances their capabilities, but also bolsters the organization's defenses.

Certification also helps in identifying skilled personnel within the team, allowing organizations to leverage their expertise for specific tasks and projects. Beyond these advantages, it also instills a sense of confidence and trust among clients and partners, knowing that the organization is committed to upholding the highest standards of cybersecurity through certified professionals. In essence, the ThreatQ Academy certification programs are a strategic investment in both the team's competence and the organization's security posture.

Users, Customers & Partners

The quality and profile of a vendor's customer base is a reflection on the company itself. Sophisticated enterprise customers perform rigorous diligence on a vendor in a number of areas prior to a purchase. This includes deep technical review, platform security, financial viability, insurance requirements, and the checking of existing customer references.

ThreatQuotient is proud to protect some of the world's most prestigious Fortune 500 companies and federal government agencies.

ThreatQuotient reference accounts such as US DOD, PWC France/CIX-A, and the Saudi investment Bank characterize the size and caliber of our client list which also includes well known names in technology, healthcare, manufacturing, retail, financial services, energy, and the federal government.

While strict non-disclosure and confidentiality agreements and our code of ethics prohibit us from publishing a full list of customers, we are happy to organize individual reference calls with those specific to your industry as needed.

ThreatQ Community also provides a private cybersecurity community focused on intelligence sharing globally. ThreatQ Community includes hundreds of members from a wide range of industries and regions that are committed to sharing threat intelligence as a means of helping to level-up the collective group's threat detection and response capabilities. Community membership includes a hosted instance of the ThreatQ Platform with more than 50 open-source threat intelligence feeds, and the opportunity to collaborate with fellow community members.

In addition to managing the threat intelligence and data for protecting specific organizations, the ThreatQ Platform is deployed as a back-end system in multiple large Systems Integrators, MSSP (Managed Security Service Provider) and MDR (Managed Detection & Response) companies.

Partnerships:

Collaboration is key to delivering a positive experience for users and customers, and partnering with industry leaders such as Thales and ATOS has empowered us to extend our reach, leverage diverse expertise, and deliver enhanced solutions. Through these partnerships, we aim to fortify our commitment to our customers by providing cutting-edge technologies and comprehensive security solutions tailored

> **"ThreatQ Smart Collections are core to providing scalability on the platform. Users can quickly create highly refined data collections using flexible filter controls, and then use these Smart Collections to drive analysis in dashboards, investigations in ThreatQ Investigations, automations in ThreatQ TDR Orchestrator, sharing across a community of users and much more."**
>
> **- Tyler Greer, Cyber Threat intelligence Lead, LPL Financial**

to their evolving needs.

Company History, Team & Ability to Execute

We have seen an influx of well intentioned and passionate entrepreneurs enter the cybersecurity industry in recent years. Driven by a crowd of investors who wish to place a bet in the security market, new companies and teams are created almost weekly. It is important to consider the quality, profile, track record, and the team's ability to execute. Consider factors including whether they built and operated a successful company before, recruited and retained top talent, and developed technology deployable by large enterprise customers.

The ThreatQuotient team has built some of the biggest names in cybersecurity which demonstrates a deep understanding of the cybersecurity problem, the importance of innovation and the value of long-standing relationships with customers and partners. A successful, experienced team brings a track record of building trust with users while delivering unique security operations solutions that address the latest trends with a measured approach.

Recognition is a testament to a company's unwavering pursuit of excellence. We are honored to have recently received several prestigious awards, such as Washington Post Top Workplaces, Cybersecurity Breakthrough for Overall SOAR Platform of the Year, and Cyber Defense Magazine Market Leader in Threat Intelligence acknowledging our innovation, commitment to security, and contributions to the industry with our threat intelligence platform. These accolades serve as validation for our tireless efforts in delivering top-tier solutions and services that make a tangible difference in safeguarding against cyber threats.

Conclusion

Selecting an Enterprise Grade Threat Intelligence Platform (TIP) is a strategic decision of considerable importance. It's essential to choose a partner with a robust and mature platform, offering extensive capabilities and strong post-sales support. A focus on a data-driven approach, scalability when handling data, and integration with existing technologies are crucial for effective threat detection and response. Building a partnership with a provider like ThreatQuotient, with its proven track record, industry recognition, and commitment to innovation and security, ensures that your organization is equipped with a powerful platform to make security operations more data-driven, efficient and effective.

For further information including references from financial institutions partnering with ThreatQuotient, contact us at **www.threatq.com/demo/**

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence platform helps teams prioritise, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

Sales@ThreatQ.com • 703.574.9885
TQ-DTS17-0124-01