THREATQUOTIENT™

THREAT INTELLIGENCE PLATFORM:
What, Why and How?

WHAT IS A THREAT INTELLIGENCE PLATFORM?

A threat intelligence platform (TIP) is made up of many primary features which allow an organization to implement a threat-centric approach to security operations which builds on their existing security investments — infrastructure and people. It helps security teams quickly understand the most relevant threats facing the organization, make better decisions and take the right actions faster. While TIPs vary from vendor to vendor, the core features include the ability to:

AGGREGATE

A TIP serves as a central repository for threat data from both external and internal sources. It aggregates global data — from commercial sources, open source, government, industry and existing security vendors — in one manageable location and translates it into a uniform format. It also brings together internal threat and event data from sources including the security information and event management (SIEM) system, log management repository, ticketing systems and case management systems.

CORRELATE AND CONTEXTUALIZE

With all threat data in one place, a TIP correlates events and indicators from inside the environment with external data on indicators, adversaries and their methods to provide context to understand the who, what, where, when, why and how of an attack.

INTEGRATE

As a baseline, a TIP integrates with and automatically exports intelligence on the highest-priority threats to the organization's ecosystem of tools. This includes SIEMs and case management solutions, allowing these technologies to work more efficiently and effectively to deliver fewer false positives, as well as integration with the sensor grid (firewalls, IPS/IDS, Netflow, routers, web and email security, endpoint protection, etc.) to generate and apply updated policies and rules.

ACT

A TIP empowers security operations centers (SOCs), threat intelligence analysts, incident response (IR), and risk management and vulnerability teams with the curated threat intelligence they need to take action quickly against the most relevant threats the organization faces. They can reduce time to detect and respond to threats and gain valuable insights to anticipate threats and become more proactive.

WHY DO YOU NEED A THREAT INTELLIGENCE PLATFORM?

From the boardroom to the SOC, executives and analysts alike can benefit from a TIP as the foundation to threat-centric security operations.

- Chief information security officers can reduce risk, improve defenses and execute on strategic and tactical enterprise goals while staying on budget. They can arm their SOCs, IR teams and threat intelligence analysts with a platform to efficiently structure, organize and utilize threat intelligence across the enterprise.
- Security analysts can improve situational understanding, accelerate detection and response, maximize existing security investments and collaborate more effectively as a team.
- IR teams can automate prioritization of threats and security incidents, accelerate investigations and push intelligence automatically to detection and response tools.
- Threat intelligence analysts can efficiently structure and organize threat intelligence with context and prioritization to build adversary dossiers, make better decisions and take action.

PRIMARY USE CASES FOR A THREAT INTELLIGENCE PLATFORM

THREAT DATA AGGREGATION	Turn threat data into threat intelligence through context and automatically prioritize based on user-defined scoring and relevance.
ATTACK TRENDS	Investigate attacks and track over time using the data to improve defensive posture.
ALERT TRIAGE	Send only threat intelligence that is relevant to reduce the amount of alerts that need to be investigated.
INTELLIGENCE PIVOTING	Utilize campaign, malware and indicator knowledge to identify related attacks and adversaries that may affect operations.
BREACH INVESTIGATION	Support scoping and remediation by correlating artifacts of an investigation with a threat library of related indicators and context.
THREAT HUNTING	Empower teams to proactively search for malicious activity that has not yet been identified by the sensor grid.
INCIDENT RESPONSE	Gain global visibility to adversary tactics, techniques and procedures to improve remediation quality, coverage and speed.
STRENGTHEN SENSOR GRID	Make firewall, IDS, IPS, SIEM and other devices smarter with the most accurate and relevant threat data.
OPERATIONAL ROI	Retrospectively evaluate intelligence sources' value, versus the relevance of their information to incidents experienced.

HOW IS THREATQ™ DIFFERENT FROM OTHER THREAT INTELLIGENCE PLATFORMS?

FLEXIBILITY

Collaboration and sharing are critical to accelerating detection and response. ThreatQ is designed so that all security teams can use and update threat intelligence as part of their existing workflow without changing processes. Using open APIs and at no additional cost, ThreatQ integrates into existing systems — including, but not limited to SIEMs, log repositories, ticketing systems, incident response platforms, orchestration and automation tools — allowing disparate teams to use the tools and interfaces they already know and trust, and still benefit from and act on that intelligence. Organizations can also define custom objects to expand the types of intelligence managed that may be unique to their environment — for example, an indicator of suspicious BitCoin addresses.

CUSTOM SCORING/PRIORITIZATION

The volume of indicators published today outstrips the capabilities most defensive technologies have to actually monitor. In addition, all intelligence is not created equal; what poses a threat to one organization may not to another. ThreatQ reduces the noise for more efficient and effective security operations. Customers can customize scores and automatically prioritize intelligence for their specific environment based on parameters the organization sets around indicator source, type, attributes and context, as well as adversary attributes. Security teams can change scoring ranges for greater granularity and automatically recalculate and re-prioritize intelligence as new data, events and learnings are added.

INTEGRATIONS

Bidirectional integrations (data flowing into and out of the TIP) are the wave of the future because they offer a full-circle automated capability. ThreatQ supports bidirectional integrations with all of the security technologies in an organization's ecosystem. This allows analysts to make significantly faster and better decisions using the data already at their fingertips. Some of the key use cases include integration with:

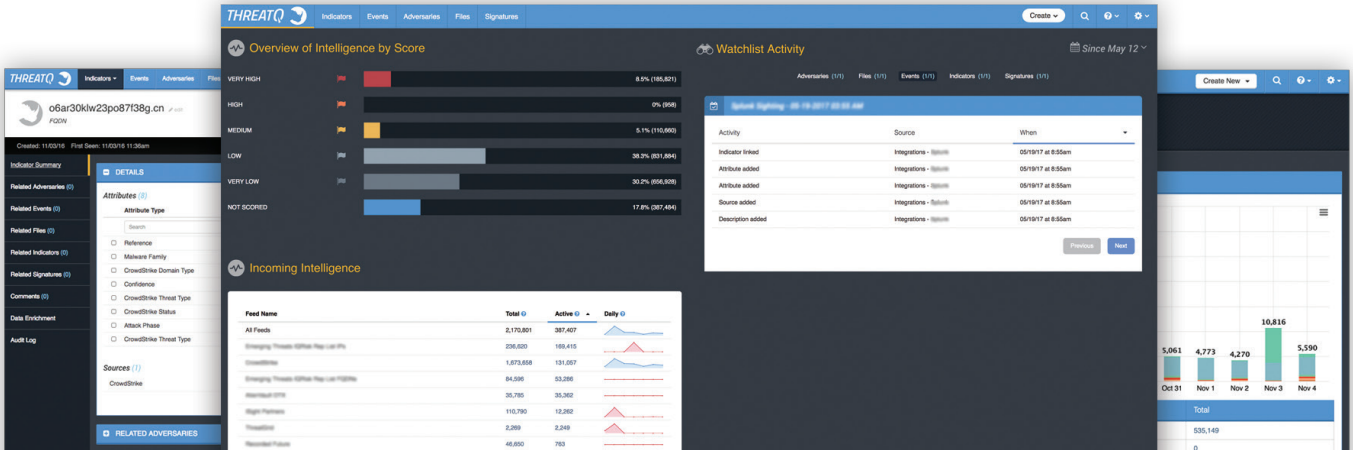
- SIEMs or log repositories to increase efficiencies of these systems, reduce false positives and simplify "rear-view mirror" investigations
- Ticketing systems to enrich and jumpstart investigations with deeper intelligence
- Vulnerability management solutions to discover possible attack routes, prioritize patching and continuously re-adjust to stay ahead of the adversary

DATA OWNERSHIP

Sharing enriched threat data externally, such as with technology vendors and Information Sharing and Analysis Centers (ISACs), helps strengthen defenses across a larger community of users. However, organizations must have a clear understanding of how much of their information these groups will share and with whom. ThreatQ provides granular controls over what, when and how much data is shared. Deployment options also impact data ownership. In contrast to a cloud-based platform that typically stipulates customers surrender their data which can even be repackaged by a vendor as part of their own data feed, ThreatQ is an on-premise platform that allows organizations to maintain complete data ownership rights.

INVESTIGATIONS

ThreatQ Investigations is the first cybersecurity situation room designed for collaborative threat analysis, shared understanding and coordinated response. Built on top of the ThreatQ threat intelligence platform, it embeds visualization and documentation in a shared environment for greater understanding and focus throughout the analysis process. It accelerates investigations and improves collaboration among and across teams and enables team leaders to direct actions, assign tasks and see the results unfold in near real time.



CONCLUSION

The average cost of a data breach globally is now nearly $4 million and “mega breaches” of more than 1 million records cost $40 million and more.* Organizations need to do more to accelerate their security operations, but investing in another threat feed, point product or new process to address the latest threat isn’t the answer. With the right threat intelligence platform, organizations can maximize the use of their existing threat and event data, security technologies and people to achieve more faster. They can understand high-priority threats, make better decisions, accelerate detection and response, and proactively reduce risk in the future.

**Source: 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute*

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_What-Why-How_Rev1

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