THREATQUOTIENT™

AT A GLANCE: THREAT LIBRARY

Most organizations have plenty of threat data and security tools, yet they still don't feel they are adequately protected. What's missing is a way to make sense of and better use of what they have. What they need is a customized threat library.

A customized threat library aggregates into a central repository the millions of threat-focused data points security teams are bombarded with every day. It augments and enriches that global threat data with internal threat and event data from the company's own tools, including the security information and event management (SIEM) system, log management repository and case management systems. This provides context for automatic scoring and prioritization of threat intelligence based on parameters that the teams set. By removing the noise and reducing the risk of false positives, users can focus on the data that really matters to their organization.

A customized threat library becomes an enterprise's single source of truth for answering security questions, including:

- Why was this indicator blocked?
- How should we defend against this malware family?
- Is that indicator part of an opportunistic drive-by or something more targeted?
- Have we seen this indicator before?

The ability to answer questions like these defines a security-driven threat library. It not only benefits threat intelligence analysts, the security operations center (SOC) and the incident response (IR) team, but is something that the security architecture can leverage as a force multiplier to maximize the value from its existing security operations tools and teams.

HOW IT WORKS

A threat library should do three things.

1. Serve as an organized, indexed and searchable location for structured and unstructured security information from external and internal sources.

Structured intelligence includes data from potentially dissimilar locations over structured routes. These could be threat feeds and indicators; CVEs or other vulnerability information; tools, techniques and procedures (TTPs); adversary briefs; signatures or rules; email messages or malware samples. All threat intelligence platforms can accept this information. The differentiation comes with the type of control organizations have over that data to score it, tag it and correlate it with other pieces of relevant data. Data collected into the threat library needs to be personalized and context-specific to the company or network it is being used to protect. It needs to be relevant, reference information that can then be prioritized automatically based on parameters the user defines.

2. Be easily accessible not only from a native interface, web or otherwise, but it should also provide enterprise-wide systems with access to the data through APIs or other easily accessible means.

Users must be able to access the data from whatever tool they are using as part of their current workflow without having to stop what they are doing and access another interface. For example, an IR team member working on a case should be able to see the context from the threat library within the

tool they are using. If they need more data, they should be a click away from getting related information within the threat library. They should also be able to update and change data as their investigation progresses. If something was previously labeled malicious but is now known to be benign, they should be able to label it as a false positive and the library should be modified immediately.

3. Automatically aggregate and normalize data while maintaining a consistent trail of information on what has been added or modified, by whom and when.

A threat library should maintain an audit history so that users can ensure the right feeds are on, the right enrichment is occurring and the right scoring policy is in place. With visibility into all the activities associated with an indicator – including the who, what, when and why – security teams can understand how past decisions were made and make further refinements. This might include changing scores and feeds and automatically re-prioritizing as further analysis dictates. As teams add more data and context, they can continuously tune the threat library. Over time, the threat library becomes the organization's threat memory, learning and providing greater knowledge for security operations.

THE VALUE

A threat library is the heart of security operations. It allows users to handle integrations from any source – structured or unstructured, internal or external. They can validate how the threat data is scored and prioritized to ensure they aren't missing valuable context. And because threat intelligence is being catalogued, the entire security operations team can understand the context to use it more effectively.

As the library self-tunes, it enables situational understanding, better decision making and automated actions that accelerate security operations in a wide variety of use cases. For example, applying curated intelligence to existing SIEM solutions for alert triage allows these technologies to perform more efficiently and effectively – focusing on the alerts that are high priority and delivering fewer false positives. Security teams can also use it to be anticipatory and prevent attacks in the future – automatically sending intelligence to the sensor grid (i.e., firewalls, IPS/IDS, routers, web-proxies, email security, endpoint, etc.). Orchestration and automation tools can be used with greater confidence and reliability because they are automating relevant, prioritized data, rather than repeatedly executing the same playbook or tasks.

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_Threat-Library_At-a-Glance_Rev1