THREATQUOTIENT™

AT A GLANCE: THREATQ™ SCORING

Most organizations have plenty of threat data and threat intelligence, yet they still don't feel they are adequately protected. What's missing is a way to prioritize the data based on the requirements of a particular organization. This allows security teams to minimize false positives and focus on what matters. ThreatQ's scoring feature addresses this challenge.

> *"ThreatQ's customer-defined Scoring is huge. We currently have one false positive per month, whereas, eight months back, we had ten per day."*
>
> *— Threat Intelligence Manager*
> *Fortune 500 Technology Customer*

WHAT IS SCORING?

Scoring represents the measure of "threat risk" facing an organization based on the calculated intersection derived from supporting internal and external intelligence.

As each day passes, threat intelligence platforms (TIPs) are automatically absorbing hundreds, thousands or potentially millions of indicators, forcing teams to quickly define an "all in panoramic-view" scoring strategy. Without a comprehensive scoring capability, no TIP can fully address the data overload problem that plagues security operations and threat intelligence teams.

ThreatQ™ provides the first highly customizable, intelligence-scoring platform, allowing teams to define scoring parameters that the platform will use to automatically re-score providers' intelligence as it enters their ThreatQ system. The result is a customer-driven score based on their own views of the world and NOT that of the provider.

WHY SCORING IS IMPORTANT

To squeeze every ounce of benefit from threat intelligence, it is critical the intelligence conform to the vantage point and mission of the team operationalizing it. The ability to customize the threat intelligence score allows teams to re-align external intelligence to their own risk posture, prioritize threats to their organization (while removing noise at the same time) and be more efficient in deploying the right intelligence to the proper tools.

REAL RISK SCORES

Many intelligence providers and "blackbox" TIPs include a threat score. Those scores aren't specific to an organization or vertical, but rather, a generic global risk score. This leads companies to a false sense of control over risk and a misallocation of resources because that adversary, attack or indicator might not even be targeting their industry. Generically calculated scores that don't factor in the unique requirements of an organization can lead to the loss of a team's valuable time tracking down intelligence with a high score that does not pose a threat to that organization. This can also expose an organization to additional risk due to not prioritizing relevant intel.

PRIORITIZATION

Indicators trigger alerts which, in turn, initiate analyst investigations. However, alerts are generally not created equal and teams end up wasting a significant amount of time chasing ghost alerts (false positives). A customer-defined scoring methodology allows the team to dictate their own risk posture based on their resources, tools and other team priorities.

HOW IT WORKS

The ThreatQ scoring feature allows security teams to redefine how scores are calculated. Teams can score on a scale of -10 to 10, based on parameters they determine. These parameters are driven by multiple factors, including:

1) SOURCES

The security team's level of trust in the source publishing the information and the number of corroborating sources are fundamental to the evaluation of the maliciousness of the information.

- All indicators must have a source (internal [ticketing system, sandbox, etc.] or external)
- All attributes have a source
- Multiple sources can increase or decrease the risk score based on the historical fidelity of the source

2) INDICATOR TYPE

The indicator type maps back to how a customer leverages specific indicators for detection or blocking. Indicator types have different life cycles based on the team and resources, etc. For example, a team may not be able to operationalize certain hash types due to various constraints, but may still want to ingest them for peripheral analysis/investigation purposes. So, those hashes would receive a threat score of 0 or even a negative number.

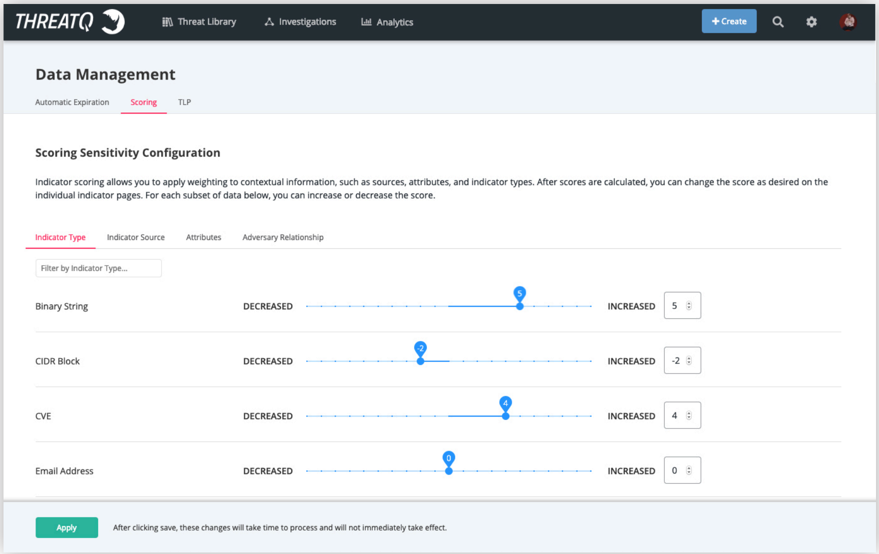
3) INDICATOR ATTRIBUTES OR CONTEXT

An indicator's context is a key contributor to an indicator's threat score because it helps characterize the type of threat. Most attributes can be broken down into three categories, including describes the indicator, describes the attack, or describes the adversary. Each of these plays a critical part in the indicator's threat score.

4) ADVERSARY ATTRIBUTION

Indicators associated with adversary groups are another mechanism to weigh the risk levels of an indicator. The scoring of the various individual adversaries provides security teams with a granular ability to help score the risk of indicators stemming from a specific adversary.

An initial baseline scoring policy is important, but organizations also must be able to constantly reevaluate that policy as new data and context become available. Additional intelligence gained over time could raise or lower the threat score depending on the weights and priorities the security team assigns to the different factors. With the ThreatQ scoring feature, security teams can redefine, recalculate and reevaluate threat scores, ensuring the scoring methodology remains aligned to the organization's risk posture and based on resources, tools and other priorities.



Data Management

Scoring Sensitivity Configuration

Indicator scoring allows you to apply weighting to contextual information, such as sources, attributes, and indicator types. After scores are calculated, you can change the score as desired on the individual indicator pages. For each subset of data below, you can increase or decrease the score.

Binary String	DECREASED	5	INCREASED	5
CIDR Block	DECREASED	-2	INCREASED	-2
CVE	DECREASED	4	INCREASED	4
Email Address	DECREASED	0	INCREASED	0

After clicking save, these changes will take time to process and will not immediately take effect.

Scoring Configuration in ThreatQ

THE VALUE

ThreatQ's scoring capability gives security teams greater control over how they allocate resources and helps maximize the benefit from threat intelligence. They can:

- Prioritize threats to the organization
- Filter out the noise and reduce instances of false positives
- Continuously re-align intelligence to their own risk posture
- Optimize the use of internal resources and tools
- Assess the value of intelligence feeds for investment

CONCLUSION

Scoring is a critical component for any team because it sets the day-to-day pace, aligns teams to a mission and supports efficiency across resources, allowing teams to appear bigger than they are. But to be truly effective, the scoring methodology should be transparent and customizable using parameters the team sets. ThreatQ's scoring capability offers a chance for teams to take back control of their intelligence efforts and redefine intelligence based on their own risk levels.

ABOUT THREATQUOTIENT™

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit https://threatquotient.com.