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.

## 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 MUST BE CUSTOMIZED TO YOUR ENVIRONMENT

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

Lots of intelligence providers and "blackbox" TIPs include a threat score. But, those scores aren't specific to you or your vertical, but, rather, a generic global risk score. This leads

> "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*

companies to a false sense of risk management and a misallocation of resources because that adversary, attack or indicator might not even be launched against your industry, although it steals cycles from your team because the provider generically scored it high.

## 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.

## THE VALUE

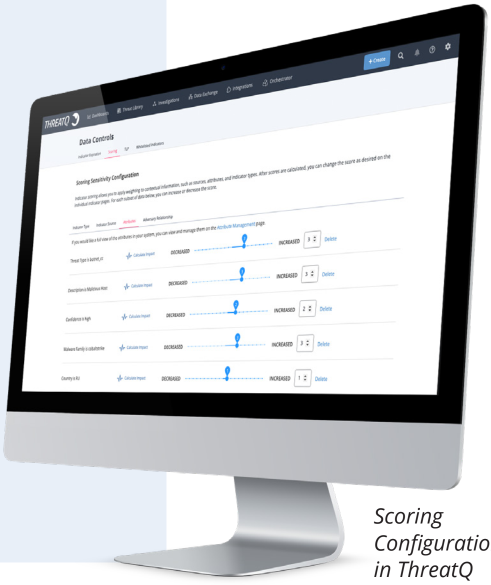
ThreatQ's scoring capability gives security teams greater control over how they allocate resources and helps maximize the benefit from threat intelligence. They can:

- 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. The ability to automatically consume and deploy threat intelligence has led the industry to a crossroads – those who blindly operationalize it feeling the pain of chasing ghosts, and teams who overlay the intelligence with their own insights to build stronger defenses. Which one are you?

To learn more about how to take a strategic approach to operationalizing threat intelligence through scoring that aligns to your environment, contact us at info@threatq.com for a demo.



Data Controls

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.

If you would like a full view of the attributes in your system, you can view and manage them on the Attribute Management page.

| | | | |
|---|---|---|---|
| Threat Type is botnet_cc | DECREASED | INCREASED | 3 |
| Description is Malicious Host | DECREASED | INCREASED | 3 |
| Confidence is high | DECREASED | INCREASED | 2 |
| Malware Family is cobaltstrike | DECREASED | INCREASED | 3 |
| Country is RU | DECREASED | INCREASED | 1 |

*Scoring Configuration in ThreatQ*

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations 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. For more information, visit www.threatquotient.com.