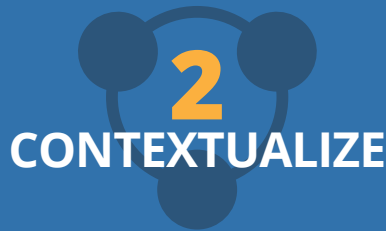


5 STEPS TO MASTERING THE USE OF THREAT INTELLIGENCE



1 AGGREGATE

Automatically consolidate all sources of threat data – *external and internal* – into one location to achieve a single source of truth. Without aggregation, using threat intelligence can become a laborious and unmanageable task.



2 CONTEXTUALIZE

Data is useless without context when you are trying to make rapid and informed decisions. Context provides better understanding of the threat and what it means to your environment.



3 PRIORITIZE

Massive amounts of data can create an overwhelming amount of noise, making it difficult to focus on the intelligence which needs the most attention. Prioritization based on the parameters *you* set is critical to ensure relevance.



4 UTILIZE

Collecting and analyzing threat intelligence is important, but doesn't help the organization until you can utilize it. Automatically applying curated threat data to your environment turns intelligence into better protection and mitigation.



5 LEARN

Continuous threat assessment is crucial to keeping your defenses current. Threat intelligence must be updated and enriched regularly in order to tune your threat library, stay focused on what matters and make better decisions.

INTERESTED IN LEARNING MORE?

Request a Live Demo of the ThreatQ Platform at ThreatQ.com/demo.