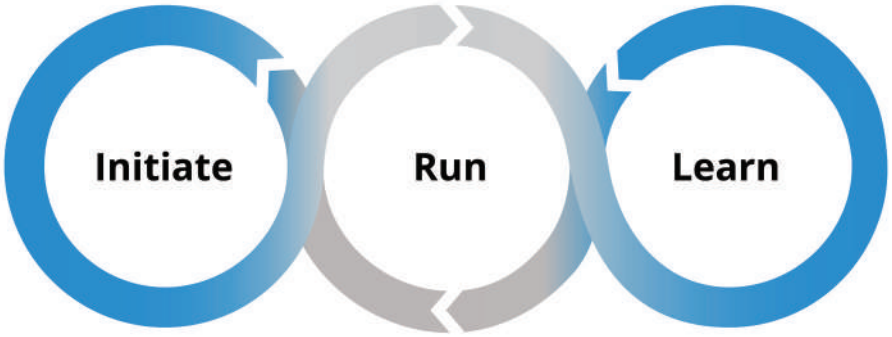
THREATQUOTIENT

DATASHEET

# ThreatQ TDR Orchestrator

ThreatQ TDR Orchestrator is the industry's first solution to introduce a simplified, data-driven approach to Security Automation, TIP and TDIR that accelerates threat detection and response across disparate systems, resulting in more efficient and effective security operations.

With the shortage of security personnel, automation has become a key strategy to offload repetitive tasks and empower humans to conduct advanced security operations tasks more efficiently. Automation has been looked at as defining a process and the steps needed to complete that process. This approach ignores the fact that automation is much more than just running the process. In reality, there are three important stages of automation to define and address:




**Initiate** – Define what should have actions taken upon it and when those actions should occur.

**Run** – Perform the course of action or defined process through to completion.

**Learn** – Record what is learned for analytics and to improve future response.

## BENEFITS & HIGHLIGHTS

A data-driven approach is easier to set-up and maintain, uses fewer resources and provides a number of other benefits including:

Reduce playbook runs by 80%

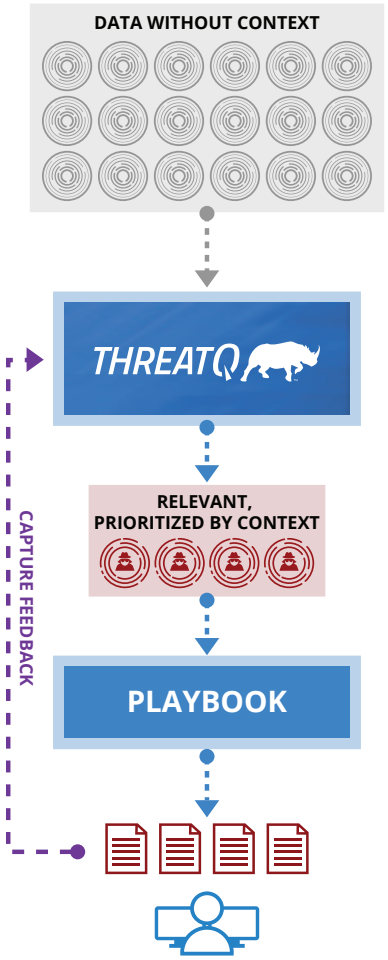
Ensure output is relevant and high priority

Learn from the actions taken, and improve over time

Easy to configure and run with existing tools

Harness Generative AI and natural language processing

ThreatQ TDR Orchestrator puts the "smarts" in the platform and not the individual playbooks by using Smart Collections™ and data-driven playbooks. The application of Smart Collections and data-driven playbooks provides for simpler configuration and maintenance, and provides a more efficient automation outcome. This approach further addresses all three stages of automation – Initiate, Run and Learn – easily and efficiently by enabling users to curate and prioritize data upfront, automate only when relevant, and simplify actions taken. It can be used to complement other playbook capabilities through ThreatQuotient's ecosystem, partners or users can define data-driven playbooks within the ThreatQ Platform. To improve the platform "smarts", it will also capture what has been learned to improve data analytics, which in turn improves the initiation stage of automation.




## THREATQ SMART COLLECTIONS™

A ThreatQ Smart Collection is a dynamic data set based on defined criteria that improves detection and response by automatically:

- Generating dashboard analytics
- Controlling data shared via ThreatQ Data Exchange feeds
- Sharing data with select ThreatQ integrations to support a wide range of use cases
- Launching automated workflows in the ThreatQ Orchestrator

For example, a Smart Collection could be defined for indicators sighted on the network with a threat score between 6 -10 and related to a specific adversary like APT28. The same Smart Collection could update dashboards, share data across integrations or platforms, and trigger an automated enrichment whenever new sightings are detected that meet the criteria.

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence 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. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit www.threatquotient.com.



Sales@ThreatQ.com • 703.574.9885