PARTNER SOLUTION OVERVIEW — ENRICHMENT & ANALYSIS

THREATQUOTIENT™

Reservoir Labs

THREATQ™ AND R-SCOPE® BY RESERVOIR LABS

Threat Intelligence provides an organization with an incredibly valuable tool to identify and remediate threats. Equally important, and often overlooked, is the platform on which you deploy and operationalize your threat intelligence.

The joint solution of ThreatQ and R-Scope by Reservoir Labs enables you to operationalize threat intelligence from ThreatQ's Threat Library™ to generate high-value, contextual, real-time alerts.

THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, prioritization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a Threat Library, Adaptive Workbench™ and Open Exchange™ to ensure that intelligence is accurate, relevant and timely to their business. With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure.

R-SCOPE BY RESERVOIR LABS

R-Scope was designed from the ground up to provide the best network security tool to fuel your Next-Gen Security Operations Center (SOC). R-Scope sensors power threat hunting and response for many of the world's premier incident response (IR) and SOC teams. R-Scope provides an incredible amount of visibility into your network, as well as critical security functionality, such as fully customizable file object extraction, selective packet capture and behavioral analytics.

R-Scope provides the ideal platform for operationalizing your threat intelligence. The security methods and tools you choose are crucial to ensuring the effectiveness of your threat intelligence. R-Scope makes it easy to consume and operationalize any type of threat indicator, including IP, domain, file attributes & hash, and certificate information.

INTEGRATION HIGHLIGHTS

Operationalize any threat indicator for real-time visibility and situational awareness.

Add incredible amounts of context to indicators, providing actionable insights for your SOC and response teams.

Customize notifications specific to your environment and use cases, including complex conditional alerting.

Simple and automated distribution of third-party indicators of compromise from ThreatQ to R-Scope.

R-Scope does more than generate hundreds of network, file, application and protocol data points. It also includes a fully programmable and stateful analytics engine that allows your team to create meaningful alerts when an indicator of compromise triggers, rather than flooding your SIEM with noise. This is crucial in both identifying real threats, as well as ensuring a quick response.

INTEGRATION USE CASES

The Integration supports a variety of use cases, such as:

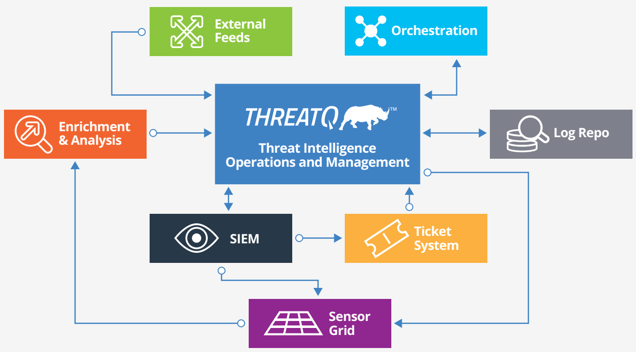
Create conditional rules to avoid unwanted chatter. For example, only generate an alert if the user successfully establishes a network session to a phishing site.

Leverage R-Scope's network visibility to alert on any IOC in real time vs. post-mortem. IP's, domains, certificates, file hashes.

Extract deep insights from R-Scope metadata to feed into ThreatQ for high-precision, environment-specific alerting.

OPEN EXCHANGE ARCHITECTURE

ThreatQ's Open Exchange provides an extensible and flexible environment for analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other formats of structured and unstructured data, along with an SDK and APIs for custom connections.



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 additional information, please visit threatquotient.com.

ABOUT RESERVOIR LABS

Reservoir Labs is a premier research and development firm headquartered in New York City that provides advanced network security solutions to both commercial and government customers. Our team of experts conducts thought-leading research, develops novel technologies and creates advanced solutions for today's most challenging security problems.

Find out more by visiting www.reservoir.com