THREATQ™ AND RST CLOUD

Technology Segment: Enrichment and Analysis Intel Feeds

RST Cloud integrates with ThreatQuotient to deliver key features: RST Threat Feed provides TAXII collections of Indicators of Compromise (IoCs) of different risk levels with context, attribution to threat and adversary, while RST Report Hub offers intelligence reports from multiple sources. RST Noise Control helps filter out known-good observables to reduce noise during detection or prevention. Additionally, RST IoC Lookup enriches indicators like IPs, Domains, URLs, and Hashes with context such as threat attribution and risk scores. RST Whois API further enriches Domains and URLs with registration data.

THREATQ BY THREATQUOTIENT™

The ThreatQuotient solutions make security operations more efficient and effective. The ThreatQ data-driven threat intelligence platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

THREAT INTELLIGENCE KNOWLEDGE COLLECTION BY RST CLOUD

RST Cloud brings intelligence data into the ThreatQ Platform through the integration of:

RST Threat Feed: Provides various TAXII collections of Indicators of Compromise (IoCs) with different risk scores.

RST Report Hub: Offers a TAXII collection of intelligence reports from hundreds of different sources, analyzed and parsed by the RST Cloud engine.

RST Noise Control: Checks if an indicator or collection of indicators is likely to be known-good and may generate noise when used for real-time detection, or cause issues when applied for prevention.

RST IoC Lookup: Enriches indicators of interest (IP, Domain, URL, Hash) with context data such as threat attribution, environmental context, and risk score.

RST Whois API: Enriches a Domain or URL with domain registration data.

INTEGRATION HIGHLIGHTS

Access a comprehensive collection of IoCs, enriched with context and scoring

Streamline public threat intelligence research directly into your ThreatQ Platform, ensuring you never miss critical threat reports, articles, and blog posts

Quickly determine if an indicator of interest is known-good or known-bad, with additional context to support the verdict

INTEGRATION USE CASES:

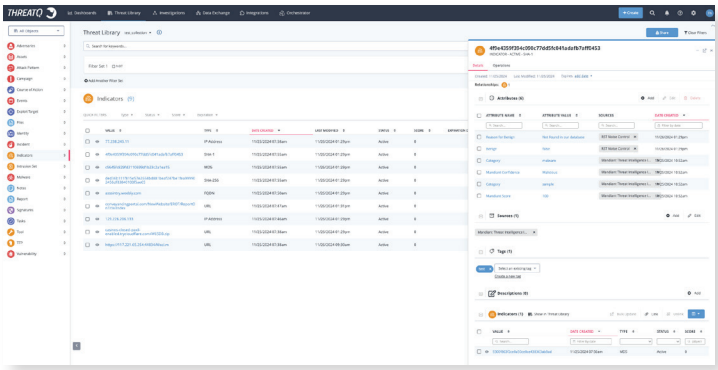
The integration supports a variety of use cases such as:

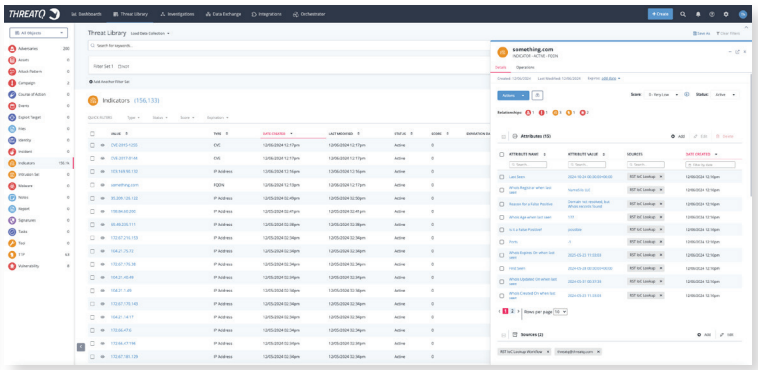
Public Threat Reports collection automation: no need to copy manually or extract IoC, threat actors, TTPs, malware names and their relationships from public threat reports, articles, and blog posts anymore. RST Report Hub brings them all pre-processed and ready to use for detection and threat hunting activities.

Threat Intelligence Management: CTI analysts face the challenge of managing millions of threat data points every day from multiple sources in various formats, all of which need to be operationalized. This includes external data from commercial sources, open source, industry, and existing security vendors, as well as internal data. RST Cloud CTI services provide ready-to-use data from a wide range of threat intelligence sources, delivered in an analyzed, pre-processed, and structured format, enriched with valuable context and risk assessment.

Threat Hunting: Threat hunting involves proactively and continuously searching for abnormal activity in networks and systems to detect signs of compromise. The key challenge is pinpointing the most relevant data to form accurate hypotheses. RST Report Hub streamlines this process by offering a comprehensive knowledge base, enriched with relevant CTI insights, detailed threat reports, and a refined approach to filtering the threat landscape.

Incident Response and Alert Triage: When an event or alert is escalated to an incident, it gains additional resources and visibility. Swift action is essential to assess the scope, impact, and required measures for mitigation and recovery. However, gathering all the necessary information can be challenging, as it often involves manual effort and data in various formats from multiple teams and tools. RST Cloud enrichment APIs streamline this process by providing experts with valuable insights, determining whether an observable is known-good or known-bad, the reasoning behind the verdict, and offering additional data to support confident decision-making and efficient incident triage.





ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that 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 integration marketplace, data management, orchestration and automation capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. For more information, visit www.threatquotient.com.

ABOUT RST CLOUD

RST Cloud is a leading provider of comprehensive cyber threat intelligence services, offering innovative solutions to enhance threat detection, analysis, and response. Through partnerships and advanced AI-powered tools, RST Cloud delivers actionable intelligence that strengthens organizations' security postures.

For more information, visit www.rstcloud.com