THREATQUOTIENT™

SYNCURITY
Built by Analysts, For Analysts

THREATQ™ AND SYNCURITY™

The combination of ThreatQ and Syncurity allows SOC and incident handling workflows to decrease the time needed to handle alerts and prioritize risk in mutual customers' environments.

Syncurity and ThreatQ enable customers to reduce time to detect, contain and remediate threats by reducing analyst time spent hunting down IoC information.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates 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.

IR-FLOW™ BY SYNCURITY™

Syncurity delivers an agile security orchestration, automation and response platform that reduces cyber risk. The company makes security operations centers (SOCs) more efficient and effective using tightly integrated alert and incident response workflows. The Syncurity IR-Flow solution is built by analysts for analysts to deploy within hours, and calibrates easily to the differences of every customer environment. IR-Flow uniquely incorporates humans into decision-making, and generates a detailed, immutable system of record for reporting, audit and compliance.

The integration between Syncurity and ThreatQ results in a one-two punch that accelerates accurate alert handling based on the TI curation provided by ThreatQ, combined with IR-Flow's ability to automate and/or semi-automate SOC triage and incident handling workflows. The solutions combine to decrease alert dwell time and more quickly assess and prioritize risk in joint customers' environments, because analysts spend less time hunting down IoC information across multiple sources/systems. ThreatQ and IR-Flow combine to create a holistic system of record that provides measurable decreases in time-to-detect (MTTD), time-to-contain (MTTC) and time-to-remediate (MTTR).

INTEGRATION HIGHLIGHTS

Enrich an IR-Flow alert with context from ThreatQ via a TQ indicator search.

Create an indicator in ThreatQ from an IR-Flow alert or incident.

Add an indicator from IR-Flow to a ThreatQ watchlist.

Mark an existing indicator in ThreatQ as a False Positive in ThreatQ.

INTEGRATION USE CASES

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

Check the existence of an indicator in ThreatQ and, if not present, add indicator to ThreatQ and, optionally, a ThreatQ watchlist.

Enrich Alerts and actions in IR-Flow Alerts from ThreatQ to decrease time spent convicting or acquitting an indicator.

Keep the IoC relationships up to date between IR-Flow and ThreatQ for scoring, prioritization and quicker identification of true/false positives in both products.

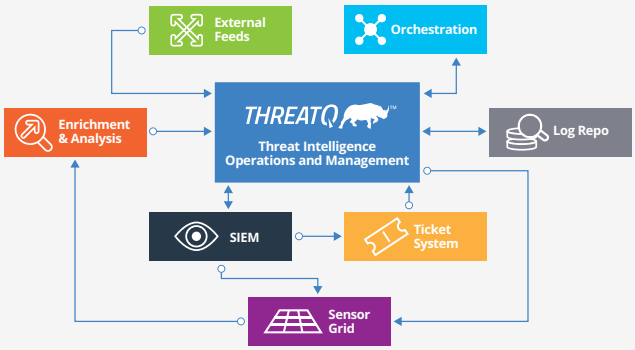
Create an associated event in ThreatQ from an incident in IR-Flow, enrich the incident with context from ThreatQ and inform the self-tuning Threat Library™.

Auto-escalate IR-Flow alerts into incidents based on known bad indicators, and auto-close alerts based on known good indicators in alerts.

Leverage IR-Flow's Triage Scoring Engine™ to rank unknown indicators as high priority automatically.

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 SYNCURTY™

Syncurity optimizes and integrates people, process and technology to realize better cybersecurity outcomes. Syncurity's award-winning and patent-pending IR-Flow™ platform accelerates security operations teams by delivering an analyst-centric incident triage and response platform.

For more information, visit https://www.syncurity.net.

To learn more about how Syncurity's customers are leveraging the IR-Flow platform, please visit https://www.syncurity.net/resource-center/case-studies.

TQ_ThreatQ-Syncurity-Solution-Overview_Rev1