THREATQUOTIENT™

splunk>

THREATQ™ AND SPLUNK®

The Splunk and ThreatQ integration allows security operations center (SOC) analysts to make prompt incident decisions and raise alerts with scored intelligence and extraction of context.

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.

SPLUNK

Splunk is the industry-leading platform for machine data. Machine data is one of the fastest-growing, most complex areas of big data. It's also one of the most valuable, containing a categorical record of user transactions, customer activity, sensor readings, machine behavior, security threats, fraudulent activity and more.

Splunk collects all your machine data from wherever it's generated, including physical, virtual and cloud environments. It enables you to search, monitor and analyze your data from one place in real-time. Troubleshoot problems and investigate security incidents in minutes. Monitor your end-to-end infrastructure to avoid service degradation or outages. Gain Operational Intelligence with real-time visibility and critical insights into customer experience, transactions and other key business metrics. Splunk is available as a software download or cloud-based service that makes your machine data accessible, usable and valuable across the organization.

INTEGRATION HIGHLIGHTS

- Ingest Splunk Data into ThreatQ
- Provide Rich Context Incidents and Indicators to Splunk
- Cross-correlate Incidents and Indicators
- Configuration and Customization of Data Extraction from and to Splunk
- Allows Collaboration with Investigations
- Allows Running Commands in Real-Time

THE INTEGRATION OF THREATQ AND SPLUNK SOLVES COMMON SECURITY OPERATIONS CHALLENGES

EXTRACTING CONTEXT FOR DATA

PROBLEM

During investigations, SOC analysts need details on indicators of compromise (IOCs) — maliciousness, severity, relationship for infinite data with no context. Gathering all this information is time-consuming and mostly manual.

SOLUTION

After ingesting incidents from Splunk Enterprise Security, ThreatQ uses the Threat Library™ to give analysts relevant context about the threat objects associated with an incident. Analysts can view and cross-correlate in both ThreatQ and ThreatQ Investigations.

CUSTOMIZATION AND PERSONALIZATION OF ENDLESS DATA AT HAND

PROBLEM

SOC analysts struggle with scoring, marking data and determining patterns from Splunk's endless data.

SOLUTION

SOC analysts can quickly determine the relevance, risk or impact of a single alert or series of alerts within Splunk interfaces. The ThreatQ add-on provides personalization and context via a company's calculated indicator score, status and sources. Additional context is also available via a direct link to the ThreatQ Threat Library, along with the ability to add information, context or indicators to the Threat Library directly from Splunk. Correlated Splunk sightings are forwarded to the Threat Library based on per-indicator events and allow for the automatic modification of the score or prioritization of an indicator within the Threat Library. This leads to better and more guided hunting by threat analysts along with the potential for automatic mitigation or prevention of threats within the security architecture.

NOT EVERYTHING IS IMPORTANT — NOISE REDUCTION

PROBLEM

Analysts have to deal with too many false alarms.

SOLUTION

The ThreatQ Splunk integration allows analysts to directly impact detections, preventions and other team context-based decisions through direct Splunk actions of marking IOCs as true positives, false positives or marking an IOC as whitelisted. This information is directly applied to the Threat Library and impacts the customer's personalized scoring policy and the automatic dispersal of intelligence to the security architecture.

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.

Copyright © 2019, ThreatQuotient, Inc. All Rights Reserved.

ABOUT SPLUNK

Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future.

For more information visit: https://splunk.com.

TQ_ThreatQ-Splunk-Solution-Overview_Rev1