THREATQUOTIENT™

splunk> phantom

THREATQ™ AND SPLUNK® PHANTOM

With the combination of Splunk Phantom and the ThreatQ platform, organizations can enable defenders to work more effectively and to better inform end-to-end security operations and incident response workflows.

The Splunk Phantom App for ThreatQ enables customers to use the ThreatQ Threat Library™ as a customized enrichment source throughout the full incident response workflow and empowers analysts to make decisions based on highly detailed information and 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 PHANTOM

Splunk Phantom automates enterprise security operations. In the face of problematic trends, including the dramatic increase in volume of attacks, severe shortages in qualified personnel, growth in the diversity and complexity of IT security environments, and investors and regulators holding management to task for breaches, Splunk Phantom arms security operations with the automation and orchestration solutions that ready them to defend their company's business.

INTEGRATION HIGHLIGHTS

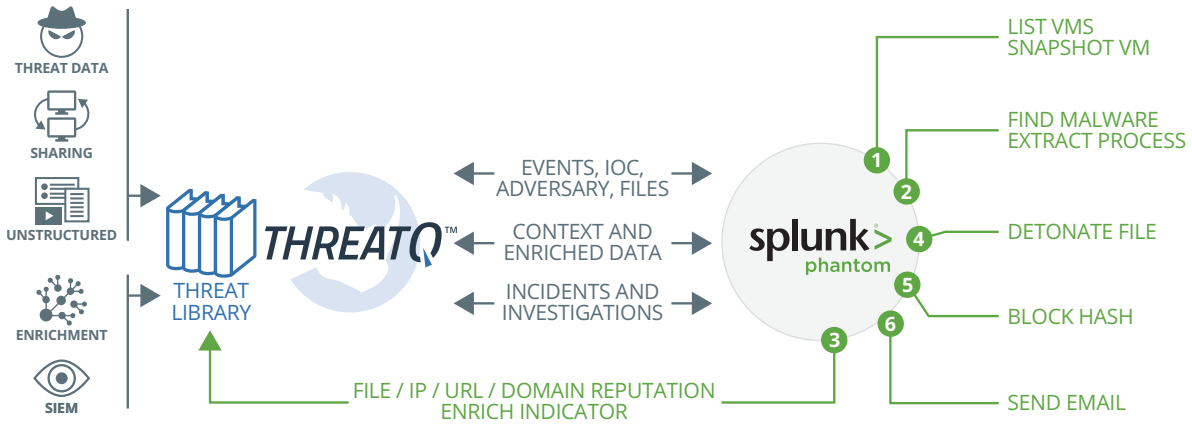
Allows Splunk Phantom to pull in enrichment from the ThreatQ Threat Library into playbooks and create new indicators, events, adversaries and files

Enriched data from the ThreatQ Threat Library enables contextual decision-making based on the results

Automates incident response workflow: preparation; detection and analysis; containment, eradication and recovery; post-incident activity

Combine actions to investigate and track spearphishing activities between Splunk Phantom and ThreatQ

THREATQ / SPLUNK PHANTOM SOLUTION DIAGRAM



SPLUNK PHANTOM-SUPPORTED ACTIONS	
test connectivity	Validates the asset configuration for connectivity
run query	Queries ThreatQ and grabs attributes
create ioc	Creates IOC in ThreatQ
get related iocs	Queries ThreatQ for related IOCs
create event	Creates an event within ThreatQ, including related indicators
create adversary	Creates adversaries in ThreatQ
upload file	Uploads files from vault in current container
domain reputation	Gets attributes, related indicators and related adversaries
ip reputation	Gets attributes, related indicators and related adversaries
email reputation	Gets attributes, related indicators and related adversaries
url reputation	Gets attributes, related indicators and related adversaries
file reputation	Gets attributes, related indicators and related adversaries
update status	Changes indicator status in ThreatQ
create attribute	Creates attributes in ThreatQ
upload spearphish	Creates a spearphish event within ThreatQ, including attachments
create task	Creates a task within ThreatQ and relates it to the corresponding event
create investigation	Creates an investigation within ThreatQ, including all related indicators, tasks and events

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 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-Phantom-Solution-Overview_Rev1