THREATQUOTIENT™ FLASHPOINT

THREATQ™ AND FLASHPOINT

The combination of ThreatQ™ and Flashpoint delivers an extensible threat intelligence platform which pulls insights and context from the Deep & Dark Web (DDW) to provide defenders the prioritization, context, customization, prioritization and collaboration needed for increased security effectiveness and efficient threat operations and management.

Utilizing Flashpoint Finished Intelligence and Risk Intelligence Observables datasets and ThreatQ across the security operations center ensures that intelligence is accurate, relevant and timely to their business so organizations get more out of their true security resources: people and infrastructure.

THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization 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,™ an Adaptive Workbench™ and an 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.

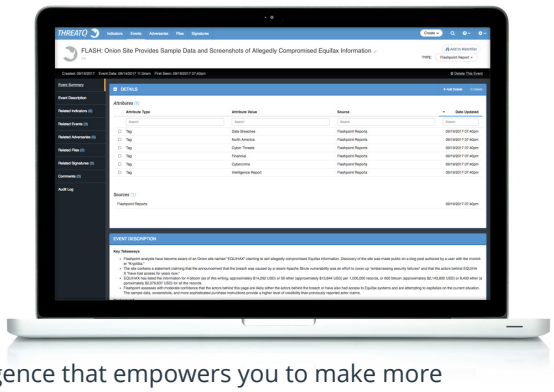
INTEGRATION HIGHLIGHTS

Access Finished Intelligence reports within the Threat Library.

Correlate across data types including actor, campaign and malware.

Help security teams respond appropriately when investigating a threat by providing additional context.

FLASHPOINT INTELLIGENCE PLATFORM



The Flashpoint Intelligence Platform grants access to Flashpoint's expansive archive of Finished Intelligence reports, Deep & Dark Web (DDW) data and Risk Intelligence Observables (RIOs) in a single, finished intelligence experience. Whether you are an intel expert or new to Business Risk Intelligence, Flashpoint's platform delivers relevant intelligence that empowers you to make more informed decisions and mitigate risk across your organization.

INTEGRATION USE CASES

THREAT DATA AGGREGATION & OPERATIONAL INTELLIGENCE

ThreatQ combines, normalizes and contextualizes threat data from both external and internal sources into a Threat Library used across the organization. By using the Finished Intelligence produced by Flashpoint, the integration offers a "state of the threat" landscape to assist security personnel in developing and prioritizing intelligence on emerging threats to the organization. A law firm, for instance, creates alerts about cyber criminals targeting documents held by law firms, allowing them to mitigate risk of exposure and enhance their security protocols. This up-to-date, strategic-level awareness helps create a "what should I care about today" intelligence feed for users.

BREACH INVESTIGATION

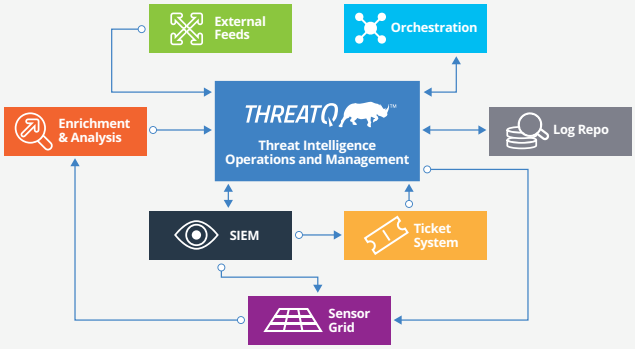
The integration supports the scoping and remediation of a breach by correlating artifacts of an investigation with a Threat Library of related indicators and context. Flashpoint RIOs dataset provides additional context on malicious infrastructure used for reconnaissance and exfiltration. This additional context enables the network defender and intelligence teams to remediate and take relevant action to support their business operations.

INSIDER MISUSE

The Flashpoint RIOs dataset provides visibility into activities and events extending beyond traditional indicator-based datasets. Using this data in ThreatQ, customers monitor RIOs associated with DDW activity for where they might be exposed by misuse, insider threat or policy violations. The SOC monitors within their *client-owned space* (or third-party suppliers, partners, etc.) for users interacting on the DDW or uploading/downloading files. By correlating against internal logs, users have greater visibility into potential insider threats in their environment and a greater understanding of those threat actor's actions.

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 understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

ABOUT FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) to empower business units and functions across organizations with a decision advantage over potential threats and adversaries. The company's sophisticated technology and human-powered analysis enable enterprises and public sector organizations globally to bolster cybersecurity, confront fraud, detect insider threats, enhance physical security, assess M&A opportunities, and address vendor risk and supply chain integrity.

For more information, visit flashpoint-intel.com.

TQ_ThreatQ-Flashpoint-Solution-Overview_Rev1