

THREATQ™ AND SILOBREAKER

Technology Segment: Threat Intelligence

With the combination of Silobreaker and the ThreatQ Threat Intelligence Platform, organizations can leverage hundreds of thousands of open, deep & dark web sources to contextualize technical indicators and analyze unstructured threat information at scale.

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.

SILOBREAKER

Silobreaker is a SaaS platform for collection, analysis and dissemination of intelligence from unstructured data sources in near-real time. By indexing millions of documents from the web, users can efficiently extract actionable insights from text-heavy content that would otherwise be a manual, time consuming process. Even sources that are traditionally difficult to investigate such as forum posts and pastes, can be quickly parsed and visualized to provide higher quality intelligence relevant to user's needs. With customisable queries, interactive dashboards and the ability for users to collaborate in a single workflow, Silobreaker supports users at every stage of the intelligence cycle. So, stakeholders can make informed decisions based on reliable intelligence to protect their organisation and mitigate risks.

INTEGRATION HIGHLIGHTS

Query Silobreaker's vast dataset on-demand, using intuitive and flexible syntax to pull relevant content into the ThreatQ intelligence platform.

Enrich indicators with insights from a highly customizable pool of relevant data, including news, blogs, feeds, forums, pastes, internal documents, finished intelligence and dark web content.

Extract and correlate on high-relevance entities from Silobreaker documents, including malware, threat actors, attack types and more.

INTEGRATION USE CASES:

The integration supports a variety of use cases such as:

- Monitoring threat actors, malware, attack types, TTPs and other relevant terms across open sources and the deep & dark web.
- Vulnerability tracking, including content related to proof-of-concept code, zero days and exploits.
- Credential monitoring and indicator enrichment for IPs, domains and subdomains.
- Strategic security trends, including novel attack methods and campaigns targeting industry.



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 SILOBREAKER

Silobreaker is a leading security and threat intelligence technology company, that provides powerful insights on emerging risks and opportunities in near-real time. It automates the collection, aggregation and analysis of data from open and dark web sources in a single platform, allowing intelligence teams to produce and disseminate high-quality, actionable reports in line with priority intelligence requirements (PIRs). This enables global enterprises to make intelligence-led decisions to safeguard their business from cyber, physical, and geopolitical threats, mitigate risks and maximise business value.

For more information, visit <https://www.silobreaker.com>