THREATQUOTIENT™

Blueliv.

THREATQ™ AND BLUELIV

Through Blueliv Cyber Threat Intelligence, clients are armed with the ultra-fresh analysis and data needed to protect their assets from the gamut of online threats.

The combination of ThreatQ™ and Blueliv enables the ingestion of real-time threat intelligence to the Threat Library™ with the assurance of helping analysts identify relevant events and reduce noise.

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.

BLUELIV CYBER THREAT INTELLIGENCE

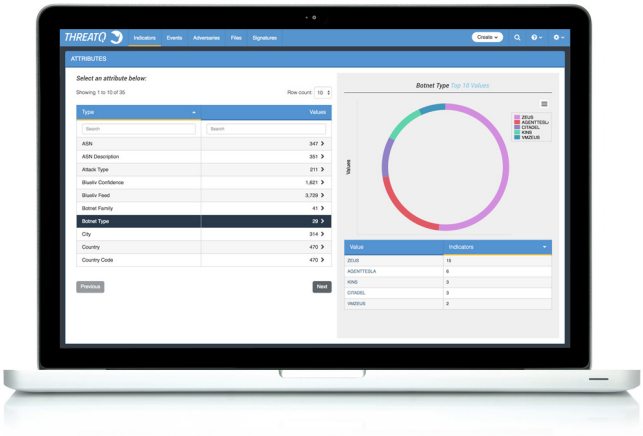
Through Blueliv Cyber Threat Intelligence, clients are armed with the ultra-fresh analysis and data needed to protect their assets from the gamut of online threats. Any organization can track in real-time the threats that are aligned against it and quantify and qualify the attack vectors malicious attackers are using. Every second, Blueliv scours and analyzes hundreds of sources to turn global threat data into targeted, predictive and actionable intelligence that detects, identifies and helps stop cyber threats. Furthermore, Blueliv security experts are able to view threats and attacker characteristics from an unconventional perspective to successfully anticipate intentions and potential outcomes.

INTEGRATION HIGHLIGHTS

Blueliv provides automated, real-time threat intelligence data, ultimately streamlining the delivery of valuable data into ThreatQ for analysis and correlation with network events.

Pairing Blueliv's confidence level with ThreatQ's Scoring System helps analysts reduce the noise and identify relevant events more quickly.

Blueliv's attack feed provides targeted information, making it easier to find, mitigate and contain the attack.



Blueliv Cyber Threat Intelligence Data Feed provides unique intelligence about the following: varied online crime servers conducting malicious activity, infected bot IPs, malware hashes, attacking IPs, hacktivism activities and Tor IPs. The feed is offered as an easy-to-buy solution that provides automated security and high-impact results rapidly. The user can identify what attack vectors malicious actors are using, understand potential indicators of compromise (IOC) and deploy mitigation solutions. The feed provides organizations with the volume, velocity and variety of real-time threat intelligence needed in order to take decisive actions and stay ahead of the cyber threat curve. The feed is relevant to all industry verticals: financial services, insurance, telecom, utility, government, transport, retail organizations, service providers and security vendors.

INTEGRATION USE CASES

The integration supports a variety of use cases such as:

Importing IP and FQDN indicators associated with botnets and crime servers

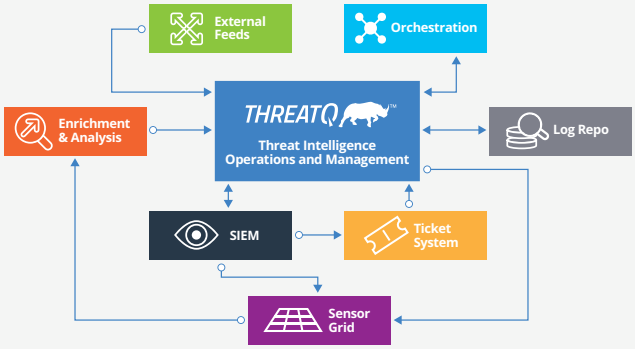
Ingesting hashes and attributes indicating the type, family, architecture and confidence of the malware

Creating relationships between related IPs, hashes and FQDNs

Providing valuable geolocation information for IPs and FQDNs involved in attacks, crime servers and botnets

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 BLUELIV

Blueliv is a leading provider of targeted cyber threat information and analysis intelligence for large enterprises, service providers and security vendors. Its cyber threat platform and feed addresses a comprehensive range of cyber threats to turn global threat data into predictive, actionable intelligence that detects, identifies and helps stop cyber threats. Blueliv's clients include leading bank, insurance, telecom, utility and retail enterprises in Europe, and the company has alliances with leading security vendors and other organizations to share cyber intelligence. Blueliv was named Gartner 2015 Cool Vendor and Go-Ignite winner 2016. Find out more at www.blueliv.com.

TQ_ThreatQ-Blueliv-Solution-Overview_Rev1