THREATQUOTIENT™ corelight

THREATQ™ AND CORELIGHT

Technology Segment: Enrichment And Analysis

With the combination of Corelight and the ThreatQ threat intelligence platform, organizations can operationalize threat intelligence to generate high-value, contextual, real-time alerts.

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.

CORELIGHT

Corelight runs on Zeek, the powerful, open-source network analysis tool that has become a global standard. Thousands of the world's most critical organizations use Zeek to generate actionable, real-time data to help defend their networks. Zeek extracts over 400 fields of data in real-time, directly from network traffic. It covers dozens of data types and protocols from Layer 3 to 7 about TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. This information can be matched against intelligence data from ThreatQ to augment Corelight's network security data to identify threats.

Corelight Sensors—available in physical, cloud and virtual formats —vastly simplify the challenges deploying open-source Zeek. They offer excellent performance, combine the capabilities large organizations need with high-end, out-of-band hardware and a specialized version of the open-source Zeek network security monitor.

INTEGRATION HIGHLIGHTS

Distribute simple and automated third-party indicators of compromise from ThreatQ to Corelight

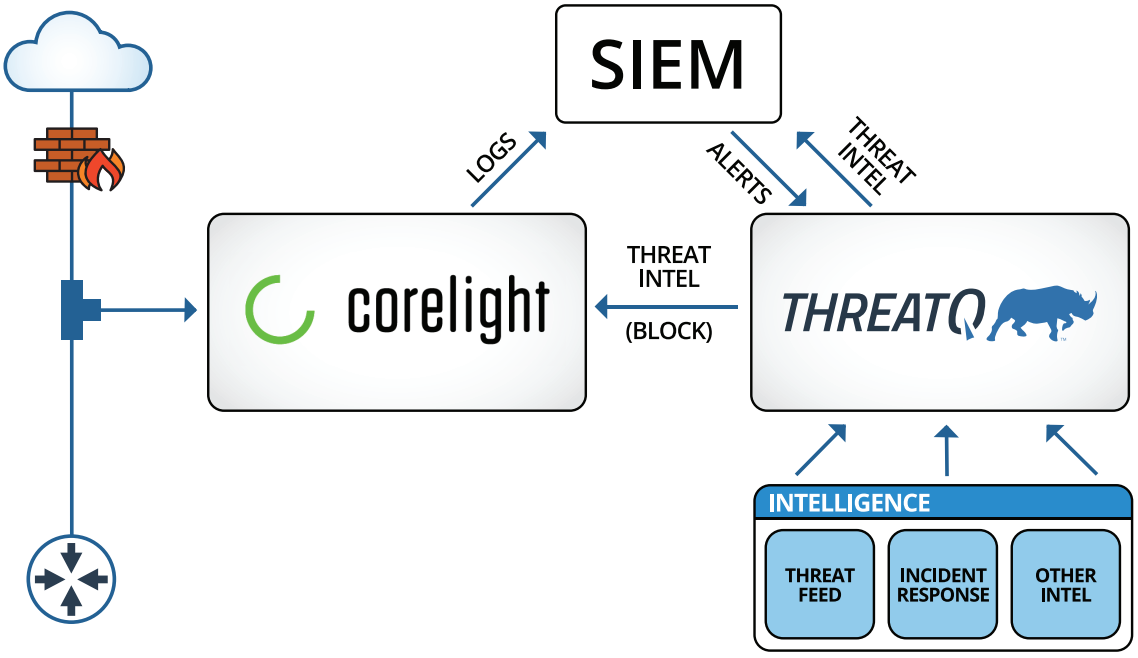
Operationalize any threat indicator for real-time visibility and situational awareness

Add incredible amounts of context to indicators, providing actionable insights for your SOC and response teams

INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- Leverages ThreatQ as a single source of truth, along with Corelight's network visibility, to alert on any IOC in real time vs. post-mortem.
- Use ThreatQ as a prioritized, single source of truth for Corelight to make informed networking decision.



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 , APAC and MENA.

For more information, visit https://threatquotient.com.

ABOUT CORELIGHT

Corelight delivers powerful network traffic analysis (NTA) solutions that help organizations defend themselves more effectively by transforming network traffic into rich logs, extracted files, and security insights. Corelight Sensors are built on Zeek (formerly called "Bro"), the open-source NTA framework that generates actionable, real-time data for thousands of security teams worldwide. Zeek has become the 'gold standard' for incident response, threat hunting, and forensics in large enterprises and government agencies worldwide. Corelight makes a family of physical, cloud and virtual network sensors that take the pain out of deploying open-source Zeek and expand its performance and capabilities. Corelight is based in San Francisco, California and its global customers include numerous Fortune 500 companies, large government agencies, and major research universities.

For more information, visit https://www.corelight.com.

TQ_ThreatQ-Corelight-Solution-Overview_Rev1