THREATQUOTIENT™

KELA

THREATQUOTIENT™ AND KELA

Technology Segment: Cybercrime Threat Intelligence

ThreatQuotient's threat intelligence platform, ThreatQ, offers a customizable solution so customers can maintain a knowledge base of vulnerabilities and exploits used by cyber criminals and state actors. KELA's tailored threat visibility, combined with cybercrime attack surface intelligence, arms you with highly contextualized intelligence, as seen from the eyes of attackers, thus enabling proactive network defense.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of 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.

KELA CYBERCRIME INTELLIGENCE PLATFORM

KELA's Cybercrime Intelligence Platform is a unique combination of cybercrime attack surface intelligence presenting targeted intelligence specific to a Customer and a cybercrime investigation capability that supports dedicated threat hunting, incident response and intelligence analysis.

Cybercrime attack surface intelligence capability allows Customer to create a profile of assets to monitor inside of the cybercrime underground. The targeted threat intelligence that is captured and then sent to ThreatQ as a dedicated feed of intelligence that is specific to Customer and associated entities. It is possible to create multiple feeds for different entities.

The Cybercrime Investigations module is accessible directly through KELA's cybercrime investigation area or via dedicated enrichments (Operations) that are included with the ThreatQ user interface.

INTEGRATION HIGHLIGHTS

Contextualized intelligence from the cybercrime underground that reduces noise and ensures customers are always looking only at the most relevant information and detect threats before they become attacks.

Access cybercrime sources through KELA's unique security data lake in a safe and secure manner. KELA's security data lake contains a combination of data automatically collected from various cybercrime underground sources and intelligence insights provided by cybercrime intelligence subject matter experts.

Large ecosystem of integrations. ThreatQ is designed to integrate with third-party infrastructure. This enables ThreatQ to quickly integrate with existing security tools and processes and make intelligence from KELA actionable within your environment.

THREATQ THREAT INTELLIGENCE PLATFORM

ThreatQ is designed to aggregate intelligence from multiple sources, provide analytics functions, intelligence scoring and integrate with third-party tools. Adding ThreatQ as part of the solution ensures that Customer has the flexibility to extend the intelligence monitoring capabilities to include third-party sources such as OSINT, VirusTotal and Domain-Tools. ThreatQ also includes an extensive ecosystem of integrations that can be utilised to ensure that captured intelligence from KELA and other sources can be used effectively. Examples of integrations include Ticketing Systems, SOAR platforms and SIEMs.

Users would leverage ThreatQ as the primary interface point daily. KELA's cybercrime investigations platform may be used as an enrichment interface point when more detail is required, particularly in Incident Response, Threat Hunting and Intelligence Analysis use-cases or when specific RFIs are required.

INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- Cybercrime Threat Intelligence
- Cybercrime attack surface monitoring
- Insider threat intelligence
- Fraud Detection

- Brand Protection
- Third Party Intelligence
- Vulnerability Intelligence
- Law Enforcement

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform 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 data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit: www.threatquotient.com.

ABOUT KELA

An award-winning cybercrime threat intelligence firm, KELA's mission is to provide 100% actionable intelligence on threats emerging from the cybercrime underground to support cybercrime prevention. Our success is based on a unique integration of our proprietary automated technologies and qualified intelligence experts. Trusted worldwide, our cybercrime threat intelligence and cybercrime attack surface intelligence technology automatically penetrates the hardest-to-reach corners of the internet to provide you with unique, contextualized, and actionable insights. Our solutions infiltrate underground places your team can't reach and thoroughly learn your unique requirements to uncover direct threats to your organization. KELA's tailored threat visibility, combined with cybercrime attack surface intelligence, arms you with highly contextualized intelligence, as seen from the eyes of attackers, thus enabling proactive network defense.

For more information, visit: www.ke-la.com.

THREATQUOTIENT™