THREATQUOTIENT™

INTEL471

THREATQ™ AND INTEL 471

Intel 471 is the premier provider of cybercrime intelligence curated by infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks.

With the combination of Intel 471 Cybercrime Intelligence and the ThreatQ threat intelligence platform, organizations are afforded real-time insight of existing and emerging threats within the cybercriminal underground and are equipped with proactive capabilities to mitigate impact to their organizations, assets and people. Centralizing adversarial and malware intelligence in tandem with ThreatQ's platform affords organizations an ability to simplify complex security threats by automatically integrating the right intelligence across their security ecosystems to inform security decision makers.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates 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.

CYBERCRIME INTELLIGENCE BY INTEL 471

Intel 471 is the premier provider of cybercrime intelligence curated by infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks. Adversary Intelligence is focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks. Malware Intelligence leverages our underground access to provide timely data and context on malware and adversary infrastructure.

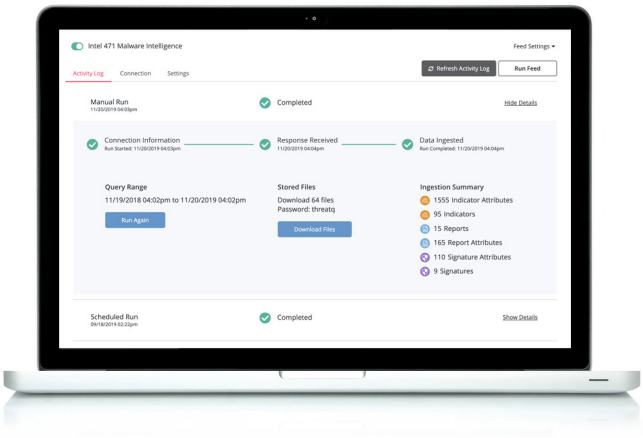
INTEGRATION HIGHLIGHTS

Proactively enrich, correlate and prioritize observables of critical relevance within ThreatQ spanning threat actors, malware, exploits and nefarious infrastructure from Intel 471's Adversary, Malware Intelligence, Vulnerabilities and Alerts with Watcher's Groups.

Ingest, research and analyze Intel 471 Intelligence to reveal actionable threat data to customize ThreatQ support to SOAR, SIEM, investigative alerting and reporting.

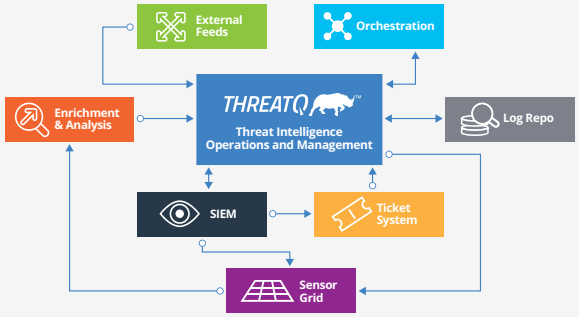
Accurately identify and eliminate unnecessary, duplicative and irrelevant threat data to equip organizations to enhance security defense in-depth posture to disrupt and block attacks before they are carried out.

Centralize adversarial, malware intelligence, vulnerabilities and alerts in tandem with ThreatQ's platform to simplify complex security threats by automatically integrating the right intelligence across security ecosystems to inform security decision makers.



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.



INTEGRATION USE CASES

The integration supports a variety of use cases such as:

INCIDENT RESPONSE AND HUNTING

With ThreatQ's integration of Intel 471 Malware Intelligence, the ability to move beyond traditional correlation and pivoting of malware used by financially motivated cybercriminals is realized. Additional IOCs (file- and network-based) and associated tools used by the threat actors deploying the malware are revealed to equip the organization to enhance policies and rules to hunt for malicious activity and tools across their infrastructure.

FRAUD DETECTION AND MITIGATION

Pairing Intel 471's deep access into the cybercriminal underground with ThreatQ's industry-leading capability to operationalize intelligence, organizations are equipped with early access of advanced fraud tactics and methodologies where they are able to proactively detect and mitigate business impact. Together, Intel 471 and ThreatQ provide organizations the intelligence and course of actions to protect profitability by validating or improving fraud controls and countermeasures.

PATCH AND VULNERABILITY MANAGEMENT

Intel 471 delivers insight on vulnerabilities being discussed, pursued and weaponized within the cybercriminal underground. This intelligence on vulnerabilities being targeted for exploitation, along with ThreatQ's management to investigatively query data associated with an organization's attack surface, enables the prioritization of vulnerabilities most relevant and impactful to business operations.

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 and APAC.

For additional information, please visit threatquotient.com.

ABOUT INTEL 471

Intel 471 is the premier provider of cybercrime intelligence for leading intelligence, security and fraud teams. Our adversary intelligence is focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks. Our malware intelligence leverages our adversary intelligence and underground capabilities to provide timely data and context on malware and adversary infrastructure. Intel 471 is comprised of intelligence operators and native speakers located where cybercriminals formerly operated with impunity and without consequence. Our pedigree is unmatched built on experience from operating in the intelligence services, military, law-enforcement and private companies across the globe.

For more information, visit intel471.com.

TQ_ThreatQ-Intel-471-Solution-Overview_Rev1