THREATQ™ AND INTEL 471

Technology Segment: Intelligence Feeds

With the combination of Intel 471 Cybercrime Intelligence and the ThreatQ 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 the 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 THREAT INTELLIGENCE BY INTEL 471

Intel 471's unparalleled global intelligence capability consists of automated collection systems and human intelligence teams that sit across 14 countries to provide near real-time coverage of threat actor and malware activity. Intel 471's Cybercrime Intelligence offers broad coverage across four core focus areas:

Adversary Intelligence: ongoing automated collection, human intelligence reporting, and high-fidelity alerting of top-tier cybercriminals targeting and affecting nearly every industry and geography across the globe

Malware Intelligence: analysis and near real-time monitoring of malware activity and command & control infrastructure providing a steady stream of technical indicators, campaign reporting and deep technical insights on the top malware families deployed threat actors

Vulnerability Intelligence: regular vulnerability reporting and ongoing monitoring of the precursors of exploitation such as actor interest, exploit status, weaponization and productization and much more

Credential Intelligence: ongoing monitoring and alerting of compromised credentials associated with your employees, VIPs, customers and third-party suppliers and vendors

INTEGRATION HIGHLIGHTS

Proactively enrich, correlate and prioritize critical data within ThreatQ spanning threat actors, malware exploits and nefarious infrastructure from Intel 471's Adversary and Malware Intelligence.

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

Accurately identify and eliminate unnecessary threat data, enabling organizations to enhance security defense posture and disrupt and block attacks before they are carried out.

INTEGRATION USE CASES:

Incident Response and Hunting

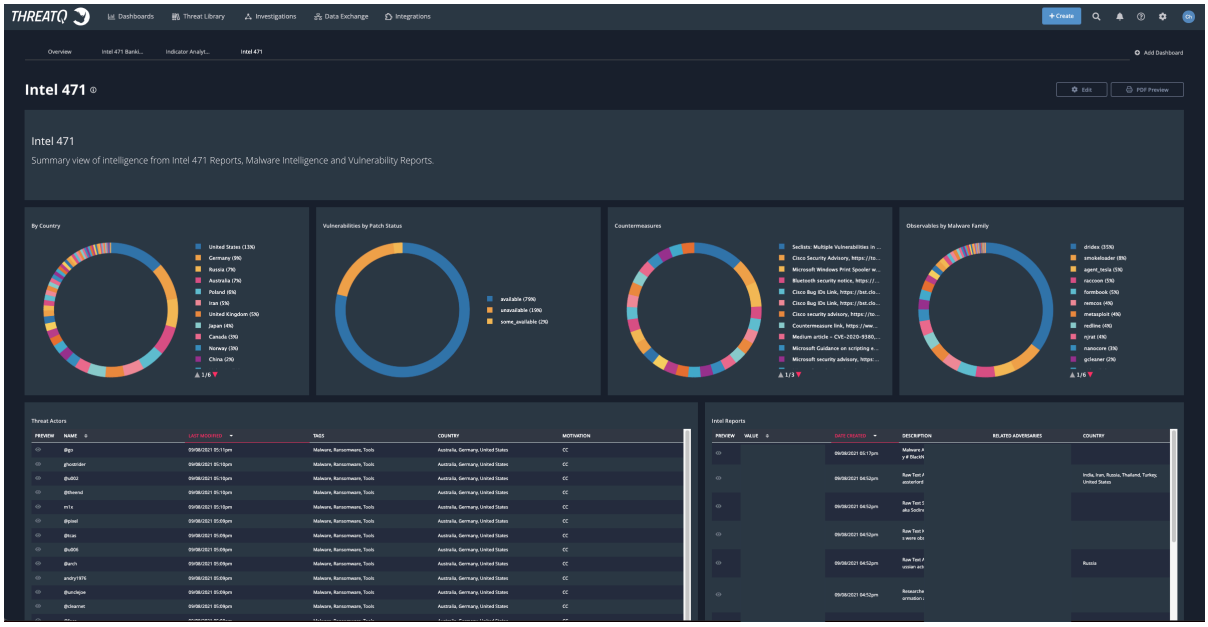
With ThreatQuotient's integration of Intel 471 Malware Intelligence, the ability to move beyond traditional correlation and pivoting of malware used by financially motivated cybercriminals is realized. Additional IOCs (file and network based) and associated tools used by the threat actors deploying the 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 ThreatQuotient 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 query data associated to 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, APAC and MENA.

For more information, visit www.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 cyberattacks. Our malware intelligence leverages our adversary intelligence and underground capabilities to provide timely data and context on malware and adversary infrastructure. Our pedigree is unmatched, built on experience from operating in the intelligence services, military, law-enforcement and private companies across the globe. We protect your organization, products, assets and people.

For more information: www.intel471.com.

THREATQUOTIENT™
11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQuotient.com
Sales@ThreatQuotient.com • +1 703 574-9885