With the powerful combination of Visa Threat Intelligence data and the ThreatQ™ threat intelligence platform, organizations can better detect and protect against cyber attacks targeting payment data.

**THREATQ™ AND VISA THREAT INTELLIGENCE**

Visa Threat Intelligence delivers exclusive Indicators of Compromise derived from Visa investigations and forensic reports on breaches in the global payments ecosystem to provide highly accurate context with low false positives.

**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 the Threat Library™, Adaptive Workbench™ and 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.

**VISA THREAT INTELLIGENCE**

Visa Threat Intelligence is an exclusive source of verified merchant breach intelligence delivered to subscribers via the Visa Developer Center API. Visa Threat Intelligence Indicators of Compromise (IOCs) help organizations determine if they have been the victim of a financially motivated breach and can be instrumental in fortifying cyber defenses to prevent future breaches in a broader effort to prevent card fraud. Visa Threat Intelligence provides cybersecurity teams IOCs and related intelligence that can help identify breaches in advance of actual payment data theft or fraud.

Visa Threat Intelligence is focused on attacks against payment data and is sourced from Visa’s extensive visibility into the global payments ecosystem. Visa works with merchants, cybersecurity experts and their investigative
teams to collect and analyze evidence left by the hackers and cybercrime organizations:

- Malware used to penetrate networks and steal payment card data
- Network indicators observed over the duration of an attack
- TTPs (Tactics, Techniques & Procedures) used throughout the attack lifecycle
- Threat actor-specific indicators
- Other artifacts that are critical to cybersecurity threat hunters