THREATQUOTIENT™

ThreatQ™ for Retail and Hospitality

When it comes to cybersecurity, breaches in the retail and hospitality industry might be the most high-profile and are happening at an alarming rate. According to a report by Thales, nearly 75 percent of U.S. retailers say they have been breached — up from 52 percent from the prior year.[1] Retailers and hospitality vendors are investing heavily in cybersecurity to protect payment card data and other personally identifiable information (PII). However, some of the most effective measures retailers can take to keep their brands out of the headlines are grounded in the adage, "Those who do not learn from history are doomed to repeat it." This is because cyber criminals reuse tactics, techniques and procedures (TTPs). In so doing, they leave a recognizable trail of breadcrumbs or indicators that provide insights into threats.

Subscribing to threat data feeds isn't enough. Organizations need a way to aggregate and de-duplicate all external and internal threat data, filter out the noise, assess and prioritize threat intelligence, and use that threat intelligence to act — decreasing time to detection and mitigation. The faster a team can streamline their ability to import, enrich, deploy and operationalize that information, the more pressure defenders are applying to the adversary, which leads the adversary to offensive mistakes and oversights. Operationalizing threat intelligence also allows teams to learn from industry peers and their own past experiences to discover adversarial TTPs and proactively reassess and strengthen defenses to mitigate future attacks.

US Retailer Breaches

A 2018 report by Thales finds that nearly 75 percent of U.S. retailers say they have been breached, up from 52 percent the year prior.[2]

Cyber Attacks by Industry

Retailers suffer three times more attacks than the financial industry.[3]

KEY CHALLENGES

PERSONALLY IDENTIFIABLE INFORMATION AND PAYMENT INFORMATION

PII and credit card data is the lifeblood of the retail industry. Every transaction involves the exchange of valuable information, and this massive amount of data makes retailers lucrative targets for threat actors. Secure payment technology helps strengthen defenses, but it is not a silver bullet. When attacks *do* happen, research by Visa shows that they result in higher-impact breaches. Also of note, while Europay, Mastercard and Visa (EMV) chip technology increases security of point-of-sale (POS) transactions, it does nothing to protect "card not present" transactions involved in e-commerce.

SPEAR PHISHING

Large US Retailer Cybercrime Attacks

The average cost of cybercrime attacks per large retailing organization in the United States is estimated at $12.69M.[4]

Many of the top threats to the retail and hospitality industry use spear phishing emails that are nearly impossible to discern from legitimate emails. Some campaigns engage in a rapid, wide-scale attack to target multiple merchants concurrently using a shotgun approach. Others target the merchant's POS vendor or integrator to gain access. Once inside the network, they take advantage of vulnerabilities for credential takeover and privilege escalation to steal payment card data or launch ransomware attacks.

VULNERABILITY PATCHING

Bad actors take advantage of the fact that IT and security teams struggle to keep up with patching of their POS systems, e-commerce payment applications and underlying internal infrastructure. As merchants strive to remain competitive, they invest in additional digital channels, applications and technologies that add complexity to the environment and further compound patching challenges. A lack of skilled cyber security professionals and organizational bureaucracy are often behind the inability to patch in a timely manner.

BRINGING ORDER TO RETAIL AND HOSPITALITY SECURITY OPERATIONS

A robust threat intelligence platform gives retailers and hospitality providers the context and prioritization they need to make better decisions, accelerate detection and response, and advance team collaboration and learning for continuous improvement. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external (e.g., R-CISC) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository.
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities.
- **PRIORITIZE** what matters most for your environment.
- **PROACTIVELY HUNT** for malicious activity which may signal payment card fraud, denial of service attacks and other harm to consumers and merchants.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture.
- **ACCELERATE ANALYSIS AND RESPONSE** to attacks against multiple targets, including POS systems, e-commerce applications, new digital channels and supporting infrastructure.
- **AUTOMATICALLY** push threat intelligence to detection and response tools.

Request a live demo of the ThreatQ platform and ThreatQ Investigations at threatq.com/demo.

[1] 2018 Thales Data Threat Report – Retail Edition (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[2] 2018 Thales Data Threat Report – Retail Edition (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[3] Cisco 2018 Security Capabilities Benchmark Study. (https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/retail-security-infographic.pdf)

[4] Symantec White Paper — Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust (https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf)

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

TQ_ThreatQ-for-Retail-and-Hospitality_Rev2

THREATQUOTIENT™

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