THREATQUOTIENT™

ThreatQ™ for Healthcare

Healthcare organizations are attractive targets for today's hackers due to reams of personal and health information providers process and store on behalf of consumers. Electronic Health Records (EHR), which include valuable data, such as a person's full name, birth date, SSN and billing information, are like digital gold to adversaries given the lucrative opportunities associated with selling personal information on the black market.

Ransomware attacks account for 72% of malware incidents in the healthcare industry. These campaigns often involve credential theft and infect multiple machines before detection, wreaking havoc on health system operations. Attacks like WannaCry in May 2017, which impacted more than 100 countries, serve as a warning for healthcare providers and emphasize the urgent need for better cybersecurity defenses in health systems worldwide.

KEY CHALLENGES

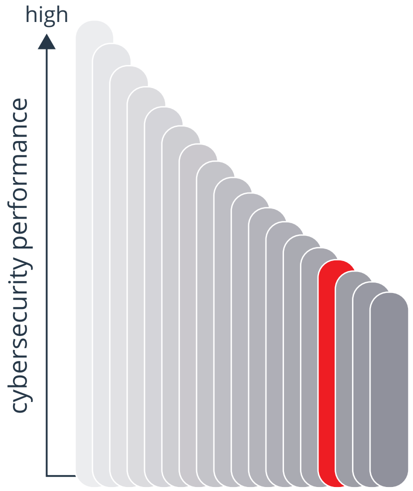
DATA AVAILABILITY

Instant and reliable access to accurate patient data saves lives. Clinicians need to see patient records on demand. An unwavering focus on patient well-being and health outcomes nearly always outweighs data protection. Hence the ongoing reliance on some insecure information-sharing processes and outdated communications technologies. But vigilance is mandatory. Confidential medical data is particularly vulnerable to malware and ransomware attacks, and therefore mandates stringent security controls. Threat intelligence can provide valuable details on attackers' motives and their tactics, techniques and procedures (TTPs) that can be used to determine how to most effectively strengthen defenses.

LEGACY SYSTEMS

Medical facilities and clinicians typically rely on outdated systems and devices, often running older versions of software and security tools that are highly vulnerable to compromise. Needing anytime anywhere access to patient information, healthcare workers and administrators are often reluctant to upgrade devices given potential interruptions in care delivery. However, a single outdated or compromised system can result in a major breach.

In order to effectively prioritize remediation efforts aimed at protecting both old and new assets, a health system must correlate threat intelligence data



The healthcare industry ranks 15th in cybersecurity performance when compared to 17 other major U.S. industries.[1]

8-10X

A healthcare record sells for 8 to 10 times the price of a credit card on the black markets[2]

$380 Cost per stolen healthcare record[3]

$2.2M The average cost of a data breach to healthcare organizations over the last two years[4] with potential security weaknesses in its environment. This enables a provider with limited security resources to focus on addressing critical infrastructure vulnerabilities that pose the greatest risk to the organization.

MODERN ASSETS

Modern technologies, like Internet of Things (IoT) medical devices and EHR applications, are delivering unprecedented accessibility, connectivity and scalability to improve efficiency and enhance patient care. But at the same time, they are expanding the attack surface and sensitive data is repeatedly being exposed to threats involving theft and misuse. Striking the optimal balance between advanced digitization and enforced security policies to protect assets across the growing attack surface remains difficult. Automatically recalculating and re-evaluating priorities and threat assessments based on the latest threat intelligence and a changing internal environment, helps to ensure ongoing focus on the most relevant risk mitigation strategies.

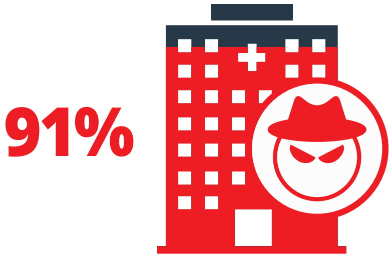
BRINGING ORDER TO HEALTHCARE SECURITY OPERATIONS

A robust threat intelligence platform gives healthcare providers the context, customization and prioritization they need to make better decisions, accelerate detection and response and advance team collaboration. 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., NH-ISAC) 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 the health system environment
- **INTEGRATE** only relevant indicators into your HIPAA-related security policies
- **PROACTIVELY HUNT** for malicious activity which may cause significant harm to patient records and healthcare organizations
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status
- **ACCELERATE ANALYSIS** and response to attacks against multiple targets including network-connected medical devices
- **AUTOMATICALLY** push threat intelligence to detection and response tools

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



Healthcare organizations reporting one or more data breaches in the last two years[2]

Compromised healthcare accounts grew from 26.4M to 33.7M in 2017[5]

The number of known healthcare hacking incidents increased 2.6 times, in the last two years[6]

[1] SecurityScorecard, 2018 Healthcare Cybersecurity Report

[2] Cisco Cybersecurity Strategies for Healthcare

[3] Ponemon Institute LLC Ponemon Institute Research Report. 2017 Cost of Data Breach Study

[4] Ponemon Institute LLC Ponemon Institute Research Report. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, 2016

[5] Gemalto, 2017 Breach Level Index

[6] HIPAA Journal, Largest Healthcare Data Breaches of 2017

ABOUT THREATQUOTIENT™

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system.

For additional information, please visit threatq.com.