



THREATQ™ AND PHISHME® INTELLIGENCE™

PhishMe takes a fundamentally different approach in identifying threats as they emerge to provide security teams with indicators and context on the latest phishing threats targeting networks.

The joint solution of ThreatQ™ and PhishMe® enables you to normalize, relate, enrich and track phishing threats in the Threat Library; and automatically deploy prioritized and relevant data to your sensor grid for detection and blocking.

PHISHME INTELLIGENCE™

PhishMe Intelligence is the leading cyber security service designed to help enterprises stop dangerous malware and phishing attacks. PhishMe uses proprietary methods to automatically identify top phishing threats and provide companies with timely actionable intelligence, tools and guidance to address attacks that would otherwise go undetected.

Phishing remains the primary mechanism to infect an endpoint, steal credentials or hold data for ransom. Attackers can bypass security defenses and deliver malicious attachments or links with intent to gain a foothold into the business. What's more, attackers don't need to rely on malware to be effective and are able to repurpose non-malicious files that can still have similar damaging effects.

Many security vendors wait until a threat is seen on the network before they analyze it and declare it as malicious. This may involve waiting until a certain number of customers report a suspicious file or endpoint systems pass information back up to the vendor. Consequently, there is a delay between when an attack is launched and when your enterprise finally has reliable information about it. Since each threat is investigated in isolation, all threats are reported as equals without any context about the attack or related attacks. As a result of this approach, security experts do not have the threat intelligence to disrupt the attack or prioritize threat response.

PhishMe takes a fundamentally different approach in identifying threats as they emerge to provide security teams with indicators and context on the latest phishing threats targeting networks.

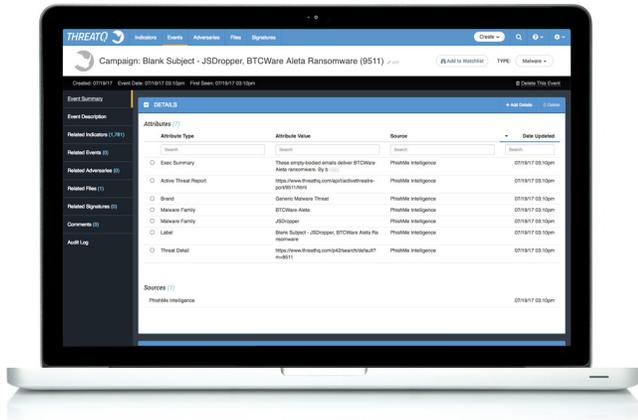
INTEGRATION HIGHLIGHTS

PhishMe delivers high-fidelity phishing indicators and contextual information highlighting attacker tactics across their global criminal operation

Security teams can easily operationalize PhishMe indicators in the ThreatQ platform

Indicators of phishing, such as attack vectors and malware families, help analysts in their phishing defense

Automatically deploy prioritized and relevant data to your sensor grid for detection and blocking.



THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, prioritization 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 a 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.

INTEGRATION USE CASES

Ingest indicators of phishing, including payload URLs, command and control servers, malicious files, IP addresses and more.

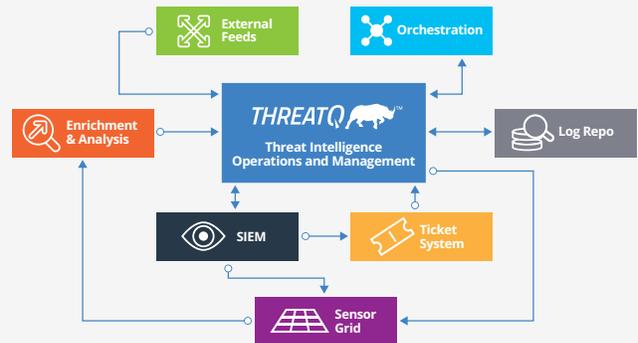
Extract indicators related to campaigns.

Import PhishMe human-readable reports, allowing to easily link indicators with context.

Extract and store phishing campaigns, malware families and malware artifacts in the Threat Library.

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.



ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

Copyright © 2017, ThreatQuotient, Inc. All Rights Reserved.

ABOUT PHISHME

PhishMe is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today's top attack vector — spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report and mitigate spear phishing, malware and drive-by threats.

Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process.

Find out more at phishme.com.

TQ_ThreatQ-PhishMe-Solution-Overview_Rev1