THREATQUOTIENT™

COFENSE

THREATQ™ AND COFENSE TRIAGE™

Cofense Triage™ takes a collaborative approach to analyzing employee-reported phishing emails that bypass email gateways and other defenses to quickly filter through reports and provide analysts with phishing indicators to stop phishing attacks in their tracks.

The joint solution integration of ThreatQ™ and Cofense Triage enables security teams to receive, analyze and respond to phishing threats that have evaded technical systems. ThreatQ ingests phishing indicators from Triage via an API to normalize, relate, enrich and track phishing threats in the Threat Library™; automatically deploying prioritized and relevant data to your sensor grid for detection and blocking.

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.

COFENSE TRIAGE

Cofense Triage accelerates phishing qualification, investigation and response. Instead of slowing your efforts with time-consuming manual processes, Cofense Triage automates analysis, so you can focus on making decisions to remediate faster. Cofense Triage's continuously updated library of rules gives analysts indicators and insights around threat actor tactics—quickly, to isolate high-risk messages and significantly improve response time. Our library is curated by our threat intelligence and research teams who identify emerging campaigns and develop rules to cut through noise faster. You can choose to share rules you create based on threats in your environment, allowing all customers to benefit.

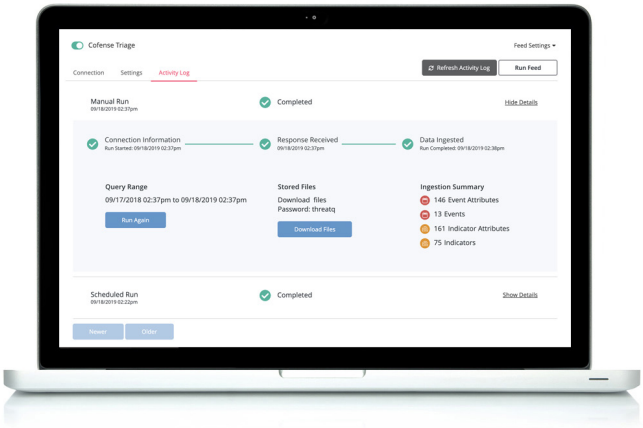
Organizations invest heavily in perimeter defenses designed to quarantine suspected phish from reaching the inbox of employees. Properly conditioned employees are able to recognize and report suspicious emails to the SOC for analysis. Cofense Triage automates the analysis of employee-reported emails

INTEGRATION HIGHLIGHTS

Cofense Triage quickly analyzes reported emails and allows human analysts to tag high-fidelity actionable phishing indicators for next step actions within the ThreatQ platform.

Security teams can designate threat indicators based on severity for ingestion into ThreatQ for additional automation.

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



to uncover real phish and take action in advance to prevent a breach. Triage gets rid of the benign reported emails through built-in noise reduction. Next, Triage automatically analyzes and can process suspicious emails to uncover indicators such as domains, URLs, hashes, filenames, senders and many more. Additionally, SOC analysts are able to determine first-hand and validate enterprise phishing threats. ThreatQ is able to ingest phishing threat indicators via the Triage API and automate next step actions and populate the Threat Library.

Cofense Triage harnesses the power of suspicious employee-reported emails and reduces the SOC analyst burden of manual analysis. The end result is that security teams are able to respond and disrupt phishing attacks in their tracks!

INTEGRATION USE CASES

The integration supports a variety of use cases such as:

Human-vetted indicators of phishing, including domains, URLs, senders, hashes, filenames and more, ingested in ThreatQ for additional automation and orchestration.

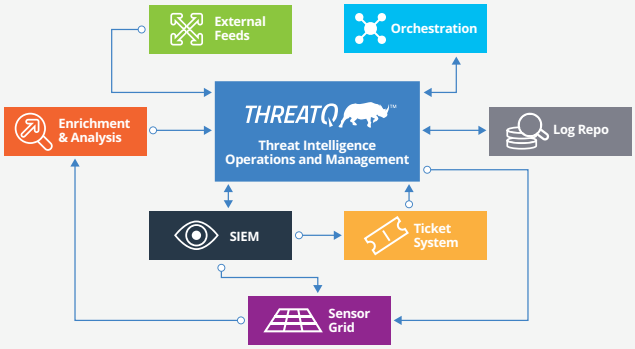
Quickly respond to and thwart phishing threats that have bypassed email gateways and other inline defenses

In tandem with Cofense Intelligence, leverage employee-reported phish to take action before a breach occurs.

Extract and automate additional threat response workflow across enterprise solutions from 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 '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 additional information, please visit threatquotient.com.

ABOUT COFENSE

Cofense, formerly known as PhishMe®, is the leading provider of human-focused phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Our 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 Cofense products integrate easily into our customers' existing security technology, demonstrating measurable results to help inform an organization's security decision-making process.

For additional information, please visit www.cofense.com.

TQ_ThreatQ-Cofense-Solution-Overview_Rev1