Cofense Integration Brief

Cofense Intelligence™ and Intelligence ThreatQuotient

Operationalize Phishing Intelligence for Threat Defense & Response

Cofense delivers a comprehensive human phishing defense platform focused on fortifying employees – your last line of defense after a phish evades your other technology – and enabling incident response teams to better identify, verify and respond to targeted phishing attacks.

Cofense PhishMe® and Cofense Reporter™ turn employees intoinformants through active engagement by simulating real-world phishing attempts, providing on-the- spot education (when needed) and easing the reporting of suspicious emails to security teams. Cofense Triage™ enables IT security teams to automate and optimize phishing incident response by allowing them to prioritize reported threats. Cofense Intelligence™ provides security teams with 100% human-verified phishing threat intelligence.

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 a threat library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business.

Phishing Intelligence

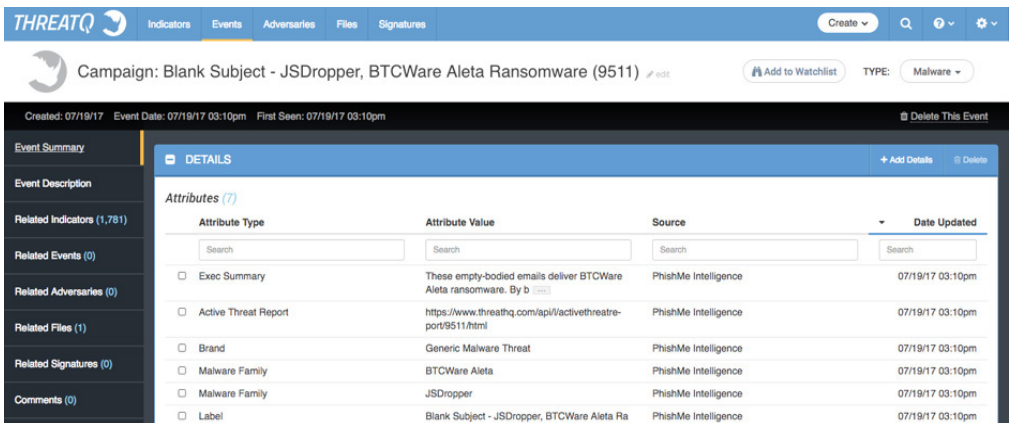
- Relevant, fresh and contextual MRTI with no false positives
- High fidelity intelligence about phishing, malware and botnet infrastructure
- Human-readable reports to understand attacker TTPs

Correlation and Actionable Decisions

- Aggregate multiple threat intelligence services to take action based on predefined policies
- Operationalize trustworthy phishing intelligence
- Ensure the most reliable and relevant data is assessed with ingested phishing indicators
- Gain real-time phishing threat visibility

With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure. Collectively with Cofense Intelligence and ThreatQ, security teams have an unobstructed view into credible phishing threats leading to higher confidence in the action taken based on the indicators.

(Ransomware IOCs from Cofense Intelligence ingested into ThreatQ platform)



IR Team Challenges

Attackers Evading Technical Controls

As technology evolves to defend against threats, attackers' creativity enables them to find ways into employees' inboxes hoping they will open the attachment or click the link. This can be thwarted through credible and trustworthy intelligence applied to network policies based on threat severity.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real-time correlation, prioritization, and automation of security events with the confidence to act is critical when seconds matter in mitigating threats.

Alert Fatigue

Too many threat intelligence feeds are full of false positives that distract security analysts. Excessive alerts only exasperate overwhelmed analysts with a finite amount of time.

How it Works

Cofense Intelligence and ThreatQ deliver the ability to aggregate, correlate, prioritize and operationalize phishing-specific machine-readable threat intelligence (MRTI). Using high fidelity phishing intelligence, analysts can decisively respond to alerts from intelligence consumed via Cofense's API. With ThreatQ, security teams can act based on Cofense Intelligence indicators through their existing infrastructure to alert or block ingress and egress traffic.

Cofense Intelligence uses easy-to-identify impact ratings of Major, Moderate, Minor, and None, for teams to create rules based on the level of impact. When ThreatQ receives these indicators security teams can define steps to operationalize threat intelligence.

Cofense Intelligence also provides rich contextual human-readable reports to security teams, allowing for in-depth insight into the criminal infrastructure. Analysts and security leaders gain visibility into email message contents, malware artifacts with full threat detail, and executive summaries, to easily understand the threat actor's TTP operation and risk to the business. These reports are automatically placed into the ThreatQ Library.

Cofense Intelligence ingested by ThreatQ provides rich insight for assertive action from the following types of indicators:

- Payload URLs and Exfiltration Sites
- Command and Control Servers
- Malicious IP Addresses
- Compromised Domains

In addition, Cofense provides access to the Active Threat Report and full threat detail for the correlated event.

With this formidable combination, security teams can respond quickly and with confidence to mitigate identified threats. High confidence threat intelligence is operationalized to make actionable decisions based on security policies for ingress and egress traffic.

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. To learn more, visit: www.threatquotient.com

THREATQ

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of close to 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175