Cofense Integration Brief

COFENSE INTELLIGENCE™ AND PHANTOM™

Delivering Powerful Phishing Threat Defense & Response

Cofense delivers comprehensive human phishing defense solutions focused on fortifying employees – your last line of defense after a phishing attack evades your other technology. Cofense enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks. Armed with Cofense Intelligence™ organizations leverage 100% human- verified phishing threat intelligence capable of complimenting automation and orchestration platforms.

Phantom enables analysts to respond automatically to known threats. With dedicated processes in place, these known threats become part of the workflow and add powerful automation to security operations. Phantom provides analysts with additional functionality to investigate more comprehensive incidents that require human analysis. This is where analysts gather incident details and thoroughly research for crucial decisions. Armed with the proper course of action, the Phantom platform can instantly orchestrate actions across the infrastructure.

Phishing Intelligence

- ✓ Human-verified timely and contextual phishing Machine-Readable Threat Intelligence (MRTI) with no false positives
- ✓ High fidelity intelligence about phishing, malware, and botnet infrastructure
- ✓ Human-readable reports with context behind threat actor infrastructure to understand attacker tactics

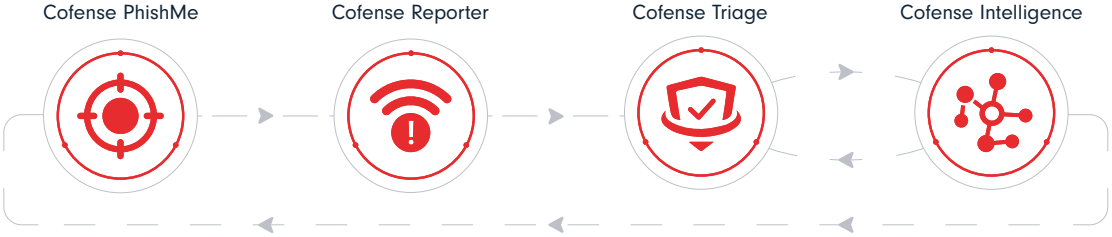
Phishing Automation and Orchestration

- ✓ Automation driven from verified phishing threats with impact ratings to for actionable decisions
- ✓ App-enabled investigation of phishing threats empower analysts and work more efficiently
- ✓ Ingest or query phishing indicators ensures the most reliable and relevant data is assessed
- ✓ Playbook execution determined by phishing indicator impact ratings makes for easier decisions

Phantom integrates seamlessly with existing technology through supported apps and playbooks to automate and orchestrate actions that typically take hours to achieve. With Phantom, security leaders can ensure that routine, repetitive tasks are achieved consistently and efficiently freeing up valuable analyst time that can be devoted to more complex and advanced responsibilities.

With Cofense Intelligence and Phantom, security teams harness the power to validate credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API and a Phantom-certified app that enables analysts to validate incidents and their potential impact to the business. Analysts have unobstructed views into credible phishing threats leading to higher confidence in the action taken based on the indicator results returned to the platform.

CONDITION EMPLOYEES
To Recognize and Report Threats



SPEED INCIDENT RESPONSE
Collect, Analyze, and Respond to Verified Active Threats

IR Team Challenges

Attackers Evading Technical Controls.

As technology evolves to defend against threats, the attackers' creativity enables them to find ways into the employees' inbox hoping they will open the attachment or click the link. This can be thwarted through credible and trustworthy phishing 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 Phantom deliver the ability to investigate, validate, and automate actions based on indicator impact ratings from phishing-specific MRTI. Using high fidelity phishing intelligence means that analysts can prioritize and decisively respond to alerts from intelligence consumed via Cofense's API. With Phantom, security teams can operationalize Cofense Intelligence indicators through actions such as:

- **Hunt URL**
- **Hunt IP**
- **Get Report**
- **Hunt File**
- **Hunt Domain**
- **On Poll (ingest threats)**

Previously mentioned, Cofense Intelligence provides rich contextual human-readable reports to security teams, allowing for in-depth insight into the criminal infrastructure. Analysts and security leaders will have visibility into email message contents, malware artifacts with full threat detail, and executive summaries to easily understand the threat actor's TTP operation and the risk to the business.

The combination of Cofense Intelligence and Phantom provides rich insight for assertive action from the following types of indicators:

- **Payload URLs and Exfiltration Sites**
- **Command and Control Servers**
- **Malicious file and IP Addresses**
- **Comprimised Domains**

Security teams can respond quickly and with confidence to mitigate identified threats. Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions that are automated and orchestrated across the infrastructure.

About Phantom

Phantom is the first community-powered security automation and orchestration platform. It integrates your existing security technologies, providing a layer of connective tissue between them. You can work smarter, respond faster and strengthen the defenses of your entire security infrastructure by automating repetitive tasks associated with detection, investigation, and response. Learn more at: https://phantom.us/

Phantom™

COFENSE

W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175