Cofense Integration Brief

COFENSE INTELLIGENCE™ AND FIREEYE®

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.

FireEye Security Orchestrator (FSO) helps analysts improve response times, reduce risk exposure, and maintain process consistency across the enterprise security program. FSO unifies disparate technologies and incident handling processes into a single console to deliver real-time responses. With dedicated processes in place, FSO is the catalyst to the investigation and incident response workflow in the security operation.

FSO speeds phishing investigation and incident response from minutes down to seconds. Through the power of FSO and the integration with Cofense Intelligence, analysts operationalize results that allow security teams to close gaps and disrupt attackers. FSO integrates seamlessly with FireEye solutions that orchestrate across the enterprise. With FSO, 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.

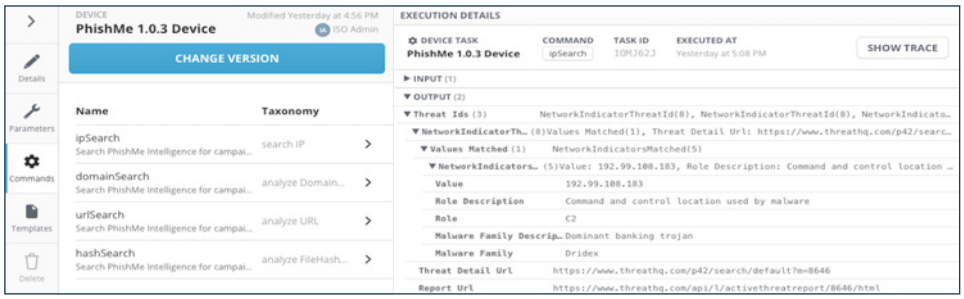
Phishing Intelligence

- ✓ 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 for actionable decisions
- ✓ Playbook-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

With Cofense Intelligence and FSO, security teams harness the power of credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API leveraged by FSO which enables analysts to investigate 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.



(Cofense Intelligence – ipSearch command from within FireEye Security Orchestrator platform)

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 FireEye Security Orchestrator deliver the ability to investigate, validate, and orchestrate 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 FSO, security teams can operationalize Cofense Intelligence indicators through commands such as:

- **ipSearch**
- **domainSearch**
- **urlSearch**
- **hashSearch**

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 FSO provides rich insight for assertive action from the following types of indicators:

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

Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions that are automated and orchestrated across the infrastructure.

About FireEye

FireEye® is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber-attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye™

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

COFENSE

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