PhishMe™ Integration Brief

PhishMe™ Intelligence and FireEye®

Delivering Powerful Phishing Threat Defense & Response

PhishMe delivers comprehensive human phishing defense solutions focused on fortifying employees – your last line of defense after a phishing attack evades your other technology. PhishMe enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks. Armed with PhishMe 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 PhishMe 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.

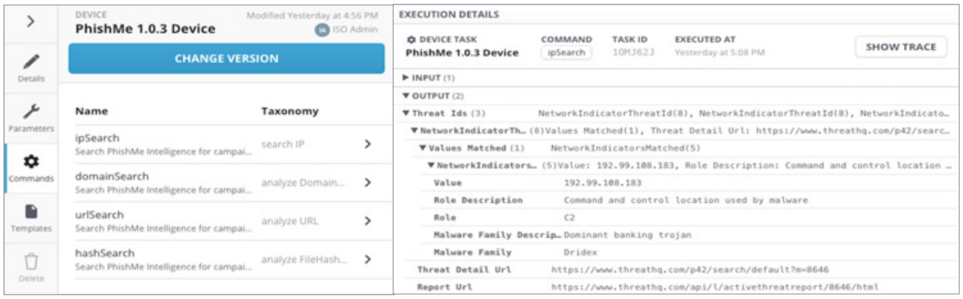
Phishing Intelligence

- 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 pre-defined policies
- Operationalize trustworthy phishing intelligence
- Ingested phishing indicators ensures the most reliable and relevant data is assessed
- Real-time phishing threat visibility

With PhishMe Intelligence and FSO, security teams harness the power of credible, human-verified phishing intelligence. PhishMe 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.



DEVICE
PhishMe 1.0.3 Device
Modified Yesterday at 4:56 PM
ISO Admin

Name	Taxonomy
ipSearch Search PhishMe Intelligence for campai...	search IP
domainSearch Search PhishMe Intelligence for campai...	analyze Domain...
urlSearch Search PhishMe Intelligence for campai...	analyze URL
hashSearch Search PhishMe Intelligence for campai...	analyze FileHash...

EXECUTION DETAILS

DEVICE TASK	COMMAND	TASK ID	EXECUTED AT
PhishMe 1.0.3 Device	ipSearch	10MJ62J	Yesterday at 5:08 PM

```
▶ INPUT (1)
▼ OUTPUT (2)
▼ Threat Ids (3)              NetworkIndicatorThreatId(8), NetworkIndicatorThreatId(8), NetworkIndicato…
  ▼ NetworkIndicatorTh… (8)Values Matched(1), Threat Detail Url: https://www.threathq.com/p42/searc…
    ▼ Values Matched (1)      NetworkIndicatorsMatched(5)
      ▼ NetworkIndicators… (5)Value: 192.99.108.183, Role Description: Command and control location …
        Value                   192.99.108.183
        Role Description        Command and control location used by malware
        Role                    C2
        Malware Family Descrip… Dominant banking trojan
        Malware Family          Dridex
    Threat Detail Url         https://www.threathq.com/p42/search/default?m=8646
    Report Url                https://www.threathq.com/api/l/activethreatreport/8646/html
```

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

IR Team Challenges

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.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real-time correlation and prioritization of security events and the critical when seconds matter in blocking the threat.

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 intelligence applied to network policies based on threat severity.

How it Works

PhishMe 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 PhishMe's API. With FSO, security teams can operationalize PhishMe Intelligence indicators through commands such as:

- ipSearch
- urlSearch
- domainSearch
- hashSearch

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

- Payload URLs and Exfiltrations Sites
- Command and Control Servers
- Malicious file and IP Addresses
- 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™

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 32 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