SOLUTION BRIEF

Rapidly Respond to Phishing

Delivering powerful phishing threat defense and response

PhishMe Intelligence and PhishMe Triage both support McAfee® event data fields, allowing analysts to recognize, report, and respond to phishing events based on customizable criteria. PhishMe Intelligence data in McAfee Enterprise Security Manager has one-click access to human-readable reports providing detailed insight into the attacker tactics, techniques, and procedures (TTPs); email message content; malware artifacts with full threat detail; and executive summaries. Additionally, the syslog output of PhishMe Triage allows for analysts to link back into PhishMe Triage to view email message elements that are useful in the incident response process. Security leaders and their teams are armed with the information they need to understand the phishing threats to the business.

McAfee Compatible Solution

- PhishMe Triage 1.5 or above
- PhishMe Intelligence
- McAfee Enterprise Security Manager 9.5.1 or above

McAfee COMPATIBLE

Incident Response Team Challenges

Some of the key challenges faced by security teams with respect to phishing event investigation include:

- **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 confidence to deny the communication is absolutely critical when seconds matter in blocking the threat.
- **Attackers evading technical controls:** As technology evolves to defend against threats, attackers' creativity enables them to find ways into employees' inbox, hoping they will open the attachment or click the link. Employees conditioned to recognize and report suspicious email contribute valuable human intelligence that may otherwise go unnoticed for an extended period of time.

PhishMe Intelligence maps to McAfee Enterprise Security Manager, providing the following context for each indicator of compromise (IoC) within event data fields:

- IoC type: URL, file, IP address, domain
- Severity
- Malware family
- Malware file hash
- Infrastructure type: C2, payload, exfiltration
- Published date
- Malware file name
- Threat ID

PhishMe Intelligence machine-readable threat intelligence (MRTI) is Common Event Format (CEF)-supported, allowing for easy integration into McAfee Enterprise Security Manager. Analysts receive human-readable Active Threat Reports about attacker TTPs and their underlying botnet and command and control infrastructure.

PhishMe Triage collects and prioritizes internally generated phishing attacks from PhishMe Reporter and maps indicators within the event data fields to McAfee Enterprise Security Manager:

- Recipe match
- YARA rule match
- Recipe and rule category
- Email subject
- Link to incident
- Recipe and rule priority

PhishMe Triage provides security analysts with insight into the reported phishing incidents that require attention immediately. As part of the McAfee Enterprise Security Manager incident response workflow, analysts can automatically route tickets based on indicators of phishing.

With this formidable combination of internally generated attack intelligence, 100% human-verified threat intelligence, and incident response event data fueling the power of McAfee Enterprise Security Manager, security teams can respond quickly and with confidence to mitigate identified threats.

About PhishMe Intelligence

PhishMe Intelligence provides accurate and timely alerts so that IT teams can take fast action when under attack. PhishMe analysts and researchers work to analyze and verify phishing threats delivering ransomware, key loggers, Remote Access Trojans (RATs), and other types of crimeware. This high-fidelity data is delivered in multiple forms to effectively prepare and respond to attacks. PhishMe Intelligence is available via a restful application programming interface (API) to access machine-readable threat intelligence (MRTI) in Structured Threat Information eXpression (STIX), JavaScript Object Notation (JSON), and CEF formats. In addition to this human-readable threat intelligence, reports provide deep-dive analysis of your biggest threats

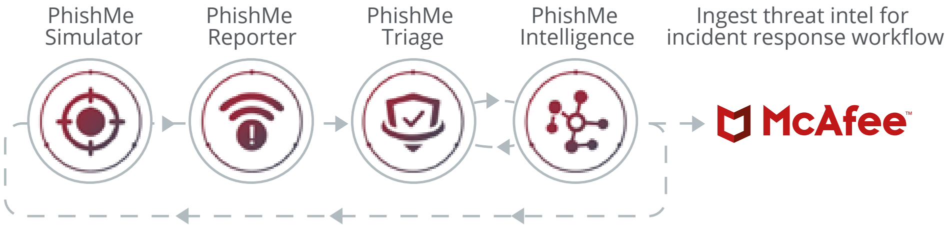

Figure 1. PhishMe components that work with McAfee Enterprise Security.

About PhishMe Triage

PhishMe Triage is the first phishing-specific incident response platform that allows security operation (SOC) and incident responders to automate the prioritization, analysis, and response to phishing threats that bypass your email security technologies. It gives you the visibility and analytics you need to speed processing and response to employee-reported phishing threats and decrease your risk of breach.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com