Cofense Integration Brief

Cofense Intelligence™ and McAfee®

Rapidly respond to phishing delivering powerful phishing threat defense and response

Cofense Intelligence and Cofense Triage both support McAfee® event data fields, allowing analysts to recognize, report, and respond to phishing events based on customizable criteria. Cofense Intelligence data in McAfee Enterprise Security Manager has one-click access to humanreadable 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 Cofense Triage allows for analysts to link back into Cofense 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.

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.

McAfee Compatible Solutions

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

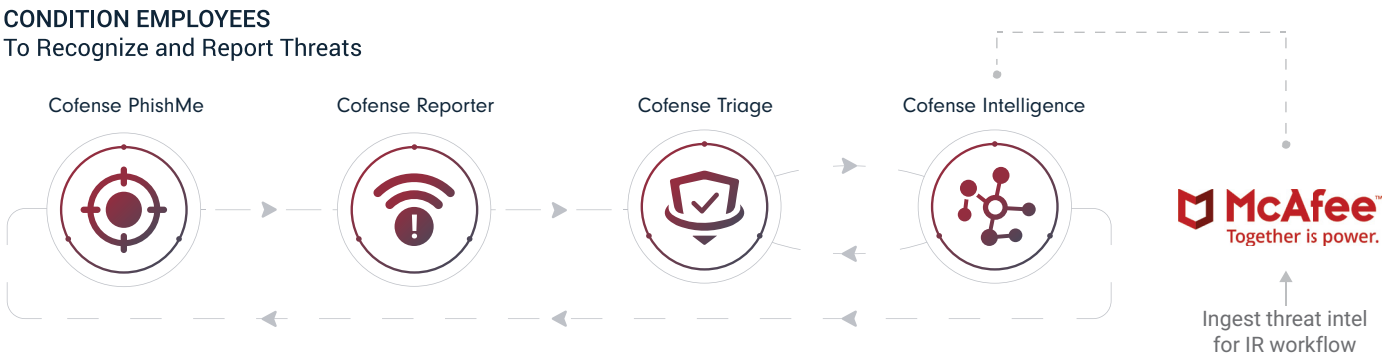

Figure 1. Cofense components that work with McAfee Enterprise Security.

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, 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.

Working Together

Cofense 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

Cofense 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.

Cofense Triage collects and prioritizes internally generated phishing attacks from Cofense 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

Cofense 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.

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.

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 more than 35+ 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