Cofense Integration Brief

Cofense and ArcSight Enterprise Security Manager (ESM)

Delivering Powerful Phishing Threat Defense & Response

Cofense PhishMe™ and Cofense Reporter™ turn employees into informants through active engagement by simulating real-world phishing attempts, providing on-the-spot education (when needed) and easing the reporting of suspicious emails to security teams.

Cofense Triage™ enables IT security teams to automate and optimize phishing incident response by allowing them to prioritize reported threats. Cofense Intelligence™ provides security teams with 100% human-verified phishing threat intelligence.

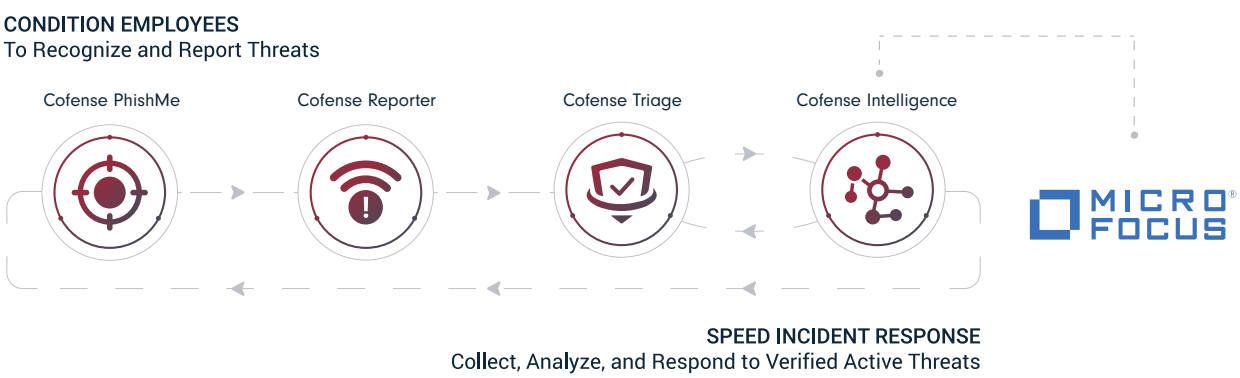
ArcSight, from Micro Focus®, is an Enterprise Security Manager (ESM) platform that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early. This defense-in-depth approach combines Cofense's focused phishing defense solutions and ArcSight's powerful incident response for better prevention and containment of threats.

Phishing Intelligence

- CEF-certified enables easy integration with ArcSight ESM
- Relevant, fresh, and contextual MRTI with no false positives
- High fidelity intelligence about phishing, malware, and botnet infrastructure
- Human-readable reports to understand attacker TTP's

Correlation and Actionable Decisions

- Consolidated data archiving and parsing of data, with analysis
- Real-time correlation across phishing intelligence and human-reported YARA rule matching
- Reliable alerts about phishing attacks
- Automatically route trouble tickets based on malware family



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. Employees conditioned to recognize and report suspicious email contribute valuable human intelligence that may otherwise go unnoticed for an extended period of time.

How it Works

The integration of Cofense Triage, Cofense Intelligence and ArcSight provides customers with the ability to ingest phishing-specific MRTI and syslog to map events in ArcSight. The intelligence and syslog data enable analysts to prioritize and decisively respond to high fidelity events. Cofense Intelligence and Cofense Triage both support ArcSight ESM's event data fields allowing analysts to recognize, report, and respond based on customizable criteria. Furthermore, Cofense Intelligence contains a link with one-click access to human-readable reports providing detailed insight into the attacker TTP's. Email message contents, malware artifacts with full threat detail, and executive summaries, convey to security teams and leaders the information they need to understand the threat to the business.

Cofense Intelligence maps to ArcSight ESM providing the following context for each 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

In addition, Cofense provides access to the Active Threat Report and full threat detail for the above correlated event.

Cofense Triage collects and prioritizes internally generated phishing attacks from Cofense Reporter and maps indicators within the event data fields to ArcSight:

- Recipe Match
- YARA Rule Match
- Recipe and Rule Category
- Email Subject
- Link to Incident
- Recipe and Rule Priority

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

About Micro Focus

Micro Focus is an American multinational information technology enterprise company, founded in November 2015 as part of the now-split Hewlett-Packard company. Micro Focus is a business-focused organization with four divisions: Enterprise Group, Services, Software, and Financial Services.

MICRO FOCUS

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