PhishMe® and HPE ArcSight Integration

Phishing Intelligence

- CEF-certified enables easy integration with ArcSight
- 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

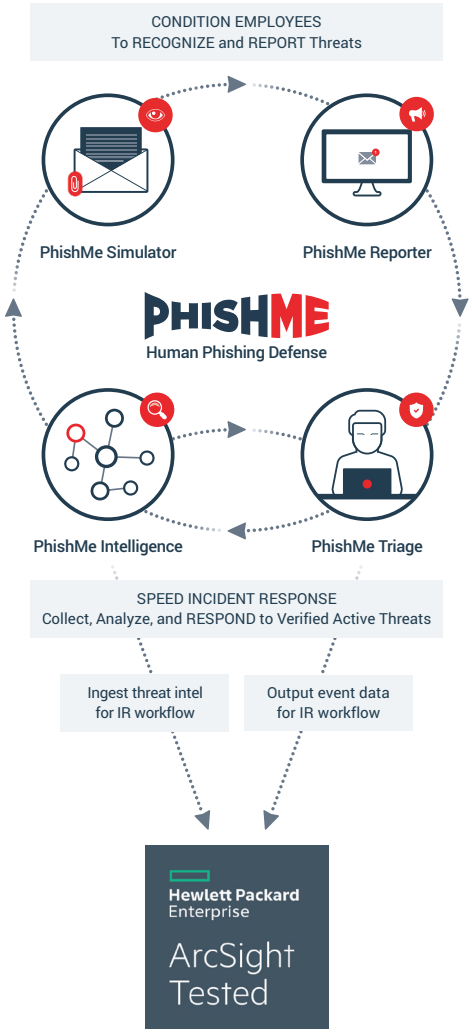
- Consolidated data archiving and parsing of data, with analysis
- Real-time correlation across phishing intelligence and human-reported YARA rule matching
- Reliable alerts about phishing attacks
- Automatically route trouble tickets based on malware family

Hewlett Packard Enterprise
ArcSight Tested

Delivering Powerful Phishing Threat Defense and Response

PhishMe delivers a comprehensive human phishing defense platform focused on fortifying employees — your last line of defense after a phish bypasses your other technology — and enabling incident response teams to better identify, verify, and respond to targeted phishing attacks.

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



HPE ArcSight is an Enterprise security management 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 PhishMe's focused phishing defense solutions and HPE ArcSight's powerful incident response for better prevention and containment of threats.

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 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, 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 PhishMe Triage, PhishMe Intelligence and HPE 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. PhishMe Intelligence and PhishMe Triage both support HPE's event data fields allowing analysts to recognize, report, and respond based on customizable criteria. Furthermore, PhishMe 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.

PhishMe Intelligence maps to ArcSight 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, we also provide links to the Active Threat Report and full threat detail for the correlated event.

PhishMe Triage collects and prioritizes internally generated phishing attacks from PhishMe 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 HPE ArcSight, security teams can respond quickly and with confidence to mitigate identified threats.

PHISHME

1608 Village Market Blvd.
Suite #200
Leesburg, VA 20175
Tel: 703.652.0717
WWW.PHISHME.COM

About PhishMe

PhishMe® is the leading provider of threat management for organizations concerned about human susceptibility to advanced targeted attacks. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process. PhishMe's customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security — Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.