# PhishMe® Triage™ and Splunk® – Integration

## Phishing Intelligence

- Splunk Add-on (Splunk ES not required) automatically connects and structures PhishMe Intelligence for use by Splunk
- Splunk App provides context around IOCs to prioritize a response and initiate the best response workflow
- Relevant 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

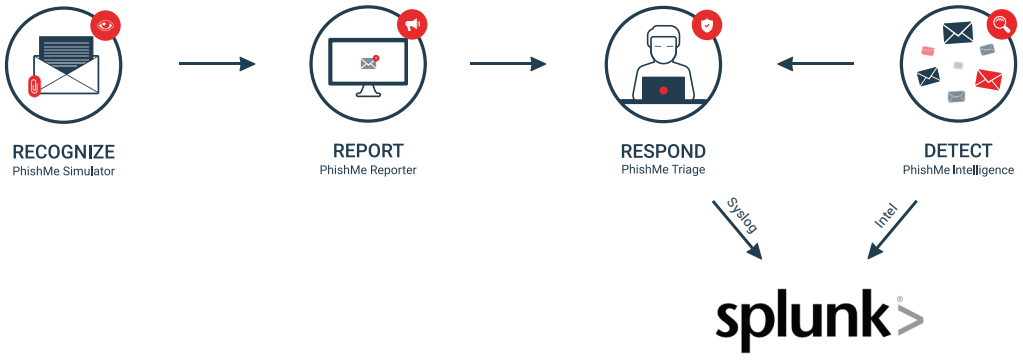
- Event data to enable analytic rules
- Correlation across phishing intelligence and human-reported YARA rule matching
- Automatically route trouble tickets based on malware family

## Delivering Powerful Phishing Threat Defense and Response

PhishMe and Splunk integrate for unmatched visibility into your biggest cybersecurity risk--spear phishing. Over 90% of data breaches are attributed to phishing attacks today. Organizations are searching for integrated approach to security that combines technology and human solutions to combat the constant phishing threats.

PhishMe delivers a comprehensive human phishing defense platform focused on fortifying employees – your last line of defense after a phish evades 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 immediate education, when needed, and simplifying the reporting of suspicious emails to security teams. PhishMe Triage™ enables IT security teams to automate and optimize phishing incident response by enabling them to priortize reported threats to speed incident response, while PhishMe Intelligence™ provides security teams with 100% human-verified phishing threat intelligence. This defense-in-depth approach combines PhishMe's focused phishing defense solutions and Splunk's advanced analytics-driven incident response for better prevention and containment of phishing threats.




**Splunk** is a leading enterprise security management solution that provides insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability and identity information. It enables security teams to quickly detect and respond to internal and external attacks to simplify threat management while minimizing risk and safeguarding your business. Splunk streamlines all aspects of security operations and is suitable for organizations of all sizes and expertise.

### 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. 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

PhishMe's Splunk-certified Add-on and App connect and optimize PhishMe Intelligence. The Splunk Add-on automatically converts PhishMe's machine-readable threat intelligence (MRTI) into risk-based threat lists enabling security teamsto quickly identify the latest phishing attacks bypassing their perimeter.

The Splunk App enables analysts to prioritize and decisively respond to high fidelity events. Using the App, incident responders can see the context of every alert and access human-readable Active Threat Reports when detailed insight into the attacker TTPs are required. These reports start with an executive overview and then describe the attack vector used to gain access to your employee's computer. PhishMe Intelligence provides Splunk with enriched IOC event data such as:

- IOC Type: URL, File Hash, IP Address, Domain
- Malware Family
- Impact Rating
- Threat Report Links
- Infrastructure Type: C2, Payload, Exfiltration
- Published Date
- Malware Description
- Threat ID

PhishMe's Triage syslog output allows Splunk administrators to leverage the native Splunk CEF app and prioritize reported event data. In turn, analysts can organize, analyze, and respond based on customizable criteria. PhishMe Triage collects and prioritizes internally-generated phishing attacks from PhishMe Reporter and maps indicators within the event data fields to Splunk:

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

With the powerful combination of internally-generated attack intelligence, 100% human-verified threat intelligence, and incident response event data fueling the power of Splunk, 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 Splunk**

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable. Join hundreds of thousands of passionate users by trying Splunk solutions for free: http://www.splunk.com/free-trials.

© Copyright 2016 PhishMe, Inc. All rights reserved.