PHISHME

DATA SHEET

PhishMe Triage™

Phishing Incident Response Management

Humans. Employees. Users. They are every organization's greatest asset while also their greatest risk since they are the primary targets for phishing and spear phishing attacks.

Industry reports illustrate the risk of phishing and potential impacts to organizations:

- Over 90% of breaches begin with a phishing email.
- It takes more than 200 days for an organization to realize it has been breached
- 69% of organizations learn about their breach from external sources

There is No Silver Bullet

The rise in attacks and breaches over the last several years, promoted organizations to adopt a layered approach to security —using multiple point solutions to address any potential gaps or vulnerabilities. It's a sound approach but resulted in an overwhelming number of alerts for the security team to investigate.

WHY TRIAGE?

- **Unique and comprehensive phishing-specific incident response solution**
- **Full integration with PhishMe Reporter allows threat prioritization based on user reputation, attributes, and threat intelligence**
- **Allows you to cluster threats based on rules that triggered them**
- **Integrates with security technologies such as sandboxes, URL analysis solutions, and SIEM solutions for enhanced detection capabilities**
- **Allows Incident responders to share results with upstream security teams to prevent future attacks**

Unfortunately, attackers change tactics quickly and often. Phishing attempts continue and some will get past your technology and into the hands of those targeted—your employees. Do they know what to do with it? Do you have a way to assess and prioritize all the suspicious emails and potential threats forwarded and shared? Do you have a way to capture all that critical, internally-generated attack intelligence?

PhishMe Triage—Phishing Incident Response Management

PhishMe Triage is the first phishing-specific incident response platform that allows security operations and incident responders to automate the identification, remediation, and sharing of phishing threats.

PhishMe Triage gives incident responders the analytics and visibility into email-based attacks occurring against their organizations in near real-time. Triage is the only offering that operationalizes the collection and prioritization of employee-reported threats and seamlessly integrates with PhishMe Reporter™.

Triage is currently available as a hardware or virtual appliance.

3rd Party Integrations

Triage integrates with your existing SIEM, malware and domain analysis, and threat intelligence solutions. PhishMe is continuously developing new partnerships and integrations to improve functionality and accommodate market needs. The most current list of available integrations are available online.

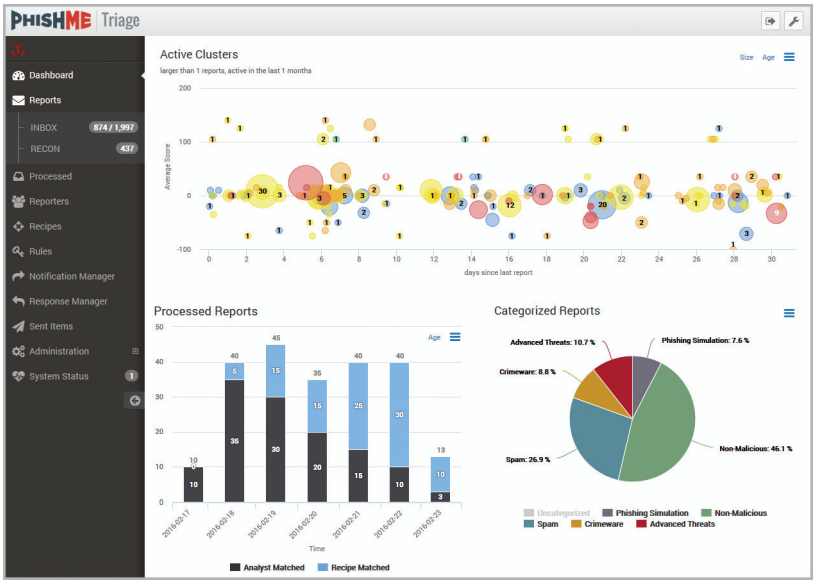
Key Features

Dashboard and reporting – Gain insight into the volume and types of emails being reported by your users and understand attack trends impacting your organization.

Smart Clustering – Triage can identify key commonalities among multiple reports. As these commonalities are discovered, Triage will create a cluster of reports. A cluster of reports can identify a campaign against your organization. Triage or operators can process all reports in a cluster as a single unit rather than having to process each report individually. By enabling clustering, Triage dramatically reduces the volume of individual reports that you must process and helps you identify and track campaigns.

Reporter Reputation – Reporter reputation is the equivalent of a trusted source. Reporters with higher reputation scores do a better job of distinguishing and reporting real threats. Reporters with lower, or negative, reputation scores may have previously submitted reports that Triage determined to be non-malicious or spam.

User Feedback – Triage allows administrators to customize and automate feedback responses to Reporters—based on the type of email they have reported via Response Manager.



Functional Triage Dashboard

YARA – Triage provides a powerful rules editor that enables you to write and edit strong YARA rules. The rules editor enables you to test a rule immediately to validate that it works against one or more reports. In addition, PhishMe shares a substantial library of tested YARA rules that you can use as-is or modify to your specific needs. PhishMe uses YARA to develop rules to identify and respond to user reports, while using YARA logic to develop Indicators of Phishing (IoP).

Escalations – Share valuable and actionable threat intelligence with upstream security teams to better protect against future threats via Notification manager. These one-time messages allow for teams to perform additional actions on the message or elements of the message.

About PhishMe

PhishMe® is the leading provider of Human Phishing Defense solutions for organizations concerned about their susceptibility to today's top attack vector—spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defense while operationalizing attack intelligence and phishing incident response for the security team. 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.

PHISHME

1608 Village Market Blvd. Suite #200 | Leesburg, VA 20175 | 703.652.0717

WWW.PHISHME.COM