INTEGRATION SOLUTION BRIEF

PhishMe® and Lastline® Integration

Speed Phishing Incident Detection and Response

- Collect and prioritize internally-reported phishing events
- Analyze thoroughly with an algorhitmic engine designed for reducing excessive alerts
- Leverage global malware analysis sandbox with builtin threat intelligence
- Correlation across phishing intelligence and human-reported YARA rule matching
- Use rich, contextual reporting illustrating malware target and capabilities
- Mutually-supported SIEM integrations
- Automate phishing incident response workflow

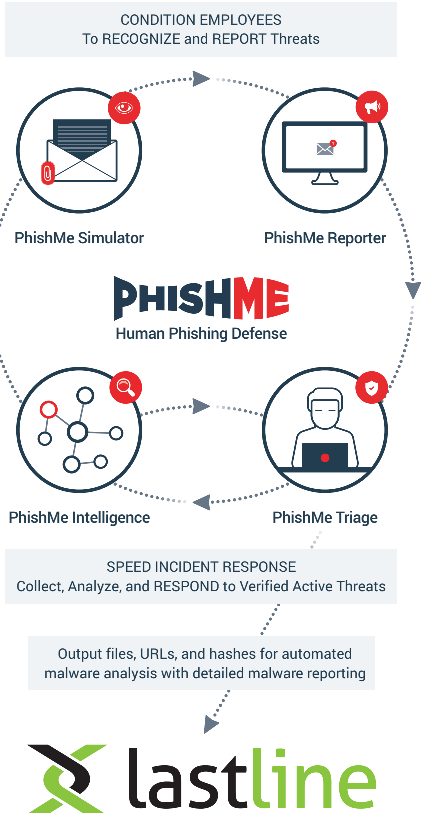
Elevating Phishing Incident Detection and Response

PhishMe Triage and Lastline Analyst integrate for advanced detection and response visibility into the greatest cybersecurity risk – spear phishing. With over 90% of data breaches attributed to phishing attacks, organizations need to adopt an integrated approach to security by layering both technology and human solutions to combat ever-evolving threats.

PhishMe delivers a comprehensive human phishing defense solution focused on engaging employees to be part of the defense after a malicious email bypasses your other technology, and enabling incident response teams to better identify, verify and respond to targeted phishing attacks.

PhishMe Simulator™ and PhishMe Reporter™ conditions employees to resist phishing attempts and empowers them to become part of the defense by reporting potentially malicious phishing attacks in real-time. PhishMe Triage™ enables IT security teams to automate and prioritize reported threats to speed incident response. PhishMe Intelligence™ provides security teams with 100% human-verified phishing threat intelligence. This integration now combines PhishMe's focused phishing defense solutions and Lastline's advanced analytics-driven incident response for better prevention and containment of phishing threats.

Lastline delivers real-time analysis of advanced malware and understanding the Internet's malicious infrastructure. Lastline leverages this threat intelligence to create advanced malware defenses for companies of all sizes.


CONDITION EMPLOYEES
To RECOGNIZE and REPORT Threats
PhishMe Simulator
PhishMe Reporter
PHISHME
Human Phishing Defense
PhishMe Intelligence
PhishMe Triage
SPEED INCIDENT RESPONSE
Collect, Analyze, and RESPOND to Verified Active Threats
Output files, URLs, and hashes for automated malware analysis with detailed malware reporting
lastline

By focusing on cloud-based automated systems and processes, Lastline analyzes advanced malware at an unprecedented speed and volume, enabling them to analyze binaries and web content in real-time as it enters the Enterprise network in addition to mapping the Malscape at a level of accuracy and relevance not previously available. Lastline's higher level of accuracy and attention to the everyday requirements of IT managers allows for the delivery of actionable threat intelligence to security teams and to companies that rely on managed security services for their protection.

IR Team Challenges

Attackers Evading Technical Controls. As technology evolves to defend against threats, creative attackers find new 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.

Point Solutions. Each technology solution has a role in solving a particular problem, but must interoperate with others for a formidable security posture. Integration is necessary for organizations to achieve maximum visibility into phishing attacks.

Alert Fatigue. Phishing remains a top cyber threat, but the volume of security alerts can be overwhelming. Identifying which files, URLs, and IPs are malicious cannot be guesswork. When time is of the essence, clear, actionable information is crucial.

How it Works

PhishMe Triage provides customers out-of-the-box capabilities to analyze suspicious email at ingestion. As emails are received by PhishMe Triage, they are automatically clustered together and prioritized. PhishMe Triage analyzes employee-reported email based on the attributes of the email through YARA rule matching, reputation of the employee reporting, threat intelligence, and combined malware analysis with Lastline Analyst, to name a few. With Lastline Analyst, mutual customers can choose to configure PhishMe Triage to send files hashes, URLs, and attachments, to Lastline (hosted or on-premise) for analysis. Lastline Analyst detects and correlates thorough inspection of the contents and then provides analysts with reports that specify if the email is benign, suspicious, or malicious. Quickly, customers can determine if the reported email was designed with malicious intent. Attributes of reported email can be streamlined and incorporated into the security team's workflow to alert and take decisive action.

The analysis results produced by Lastline Analyst are strengthened when PhishMeTriage collects and prioritizes internally-generated phishing attacks from PhishMe Reporter and maps indicators useful in the workflow such as:

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

The combination of empowered human defenders, PhishMe's purpose-built phishing incident response solution, and Lastline's global advanced malware analysis engine, results in security teams reducing phishing susceptibility. Security teams benefit by making the most of their security investments that enriches their solutions and maximizes their return on security investment.

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 human-focused 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 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 Lastline

Lastline® is innovating the way companies detect active breaches caused by advanced persistent threats, targeted attacks and evasive malware. Lastline's Deep Content Inspection™ goes beyond the legacy malware analysis used in most firewalls, UTM's, IPS systems, and antimalware software. Lastline's open architecture integrates advanced threat defenses and intelligence into existing operational workflows and security systems. Inspection of suspicious objects occurs at scale in real-time using a full-system emulation approach to sandboxing that is superior to virtual machine-based and OS emulation techniques. Lastline's technology correlates network and object analysis to achieve timely breach confirmation and incident response. Lastline was built by Anubis and Wepawet researchers and industry veterans with decades of experience focused specifically on advanced breach weaponry and tactics.