PhishMe® Triage™ and OpenDNS Investigate™ – Integration

Incident Response

- Collect and prioritize internally-generated phishing threats.
- Analyze rich anti-malware data through an automated algorithmic engine designed to reduce excessive alerts.
- Create and automate phishing incident response processes.

Integration

- Leverage existing intelligence investments.
- Analyze email through an anti-malware engine in tandem with global threat intelligence from OpenDNS.

Boost spear phishing incident response with human intelligence and global threat visibility

PhishMe and OpenDNS, now a part of Cisco™, combine the power of human-reported phishing attacks with global insight into malicious domains and networks. The end result enables security analysts to make intelligent, actionable decisions using both internally-generated and global threat intelligence.

The Challenges

The Neglected Link. Attackers focus on infiltrating your defenses through your employees. What they don't realize is that humans can be your strongest defense and best source of attack intelligence.

Alert Fatigue. Phishing remains a top cyber threat, but the volume of security alerts is overwhelming. When time is of the essence, clear, actionable information is paramount.

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

How it Works

PhishMe Triage and OpenDNS Investigate work together through a RESTful API to quickly prioritize security events and streamline analysts' incident response process for security risk domains, IP addresses, and associated networks contained in malicious emails.

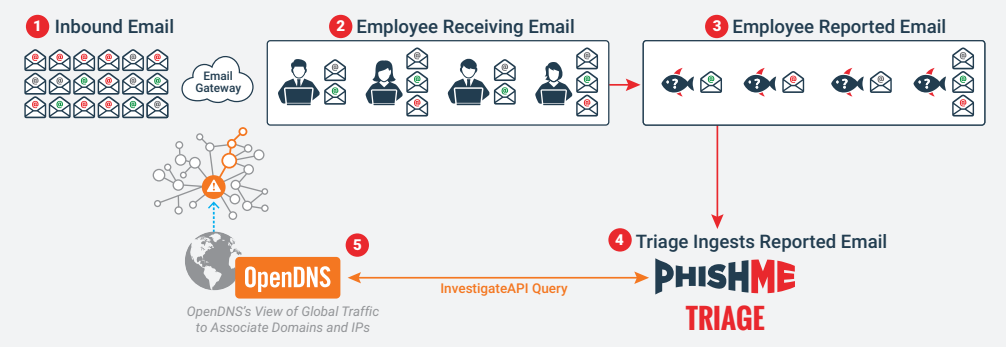
PhishMe Triage is designed to simplify phishing incident response events matching malicious content from email reported by employees that perimeter defenses missed. Triage determines contextual commonalities and indicators of phishing (IoPs) through URL and IP address analysis, anti-malware technologies, and phishing threat intelligence, as well as human intelligence reputation, volume, and severity. Collectively, Triage identifies, prioritizes, and remediates, providing SOC and incident response analysts with timely and actionable intelligence to disrupt and contain security incidents.

OpenDNS Investigate provides the most complete view of the relationships and evolution of Internet domains, IP addresses, and autonomous systems to pinpoint attackers' infrastructures and predict emergent threats. OpenDNS analyzes more than 80 billion Internet requests daily from over 65 million active users across 160+ countries with their DNS traffic pointed to OpenDNS. Plus, 500 peering partners exchange BGP route information with OpenDNS to show connections and relationships between different networks on the Internet.

OpenDNS is now part of Cisco.

When integrated with Triage, the analyst receives intelligence from Investigate that is contained within the appliance to rapidly highlight malicious, benign, or suspicious domains or IP addresses on the Internet. The analysis is automated at email ingestion to ease the analysts' research requirements and speed up their decision-making response time. Triage empowers the analyst to create custom procedures for similar or future events as well as escalate as part of the incident response workflow. Incident responders are armed with enriched information to prevent future events, or create specific detection criteria to glean more from the targeted attack tactics.

The ability for Triage to identify and rank threats based on its own analysis engine is complimented by Investigate to reaffirm the email contains attributes leading to credential or host compromise capabilities. The integration delivers enterprise security teams a significantly better return on security investment aimed at reducing the #1 threat facing security leaders today; spear phishing.



PhishMe's Human Phishing Defense

PhishMe Triage can accept input from other sources but is seamlessly integrated with PhishMe Reporter™ and PhishMe Simulator™ for a comprehensive program to condition employees to recognize phishing attacks and enable them to easily report attacks to security teams.

For more information on PhishMe solutions, please visit **www.phishme.com**. For more information on PhishMe Triage and OpenDNS Integration, please visit **www.phishme.com/OpenDNS**.

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 OpenDNS

OpenDNS, acquired by Cisco in August 2015, is a leading provider of DNS-layer network security and Internet threat intelligence, enabling the world to connect to the Internet with confidence on any device, anywhere, anytime. Its predictive intelligence uses statistical models to automate protection against emergent threats before they can reach customers. For more information, visit www.opendns.com.

PHISHME

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