PhishMe® Integration Brief

PhishMe Intelligence and ThreatConnect®

PHISHME

Delivering Powerful Phishing Threat Defense & Response

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 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.

ThreatConnect® customers use the platform to unite people, processes, and technologies behind a cohesive, intelligence-driven defense against threats to their business. Using the ThreatConnect threat intelligence platform, you can simultaneously work across your cybersecurity teams and functions with your trusted communities. Whether you have a mature program or are just getting started, you are ready to start using ThreatConnect to make faster, data-driven security decisions.

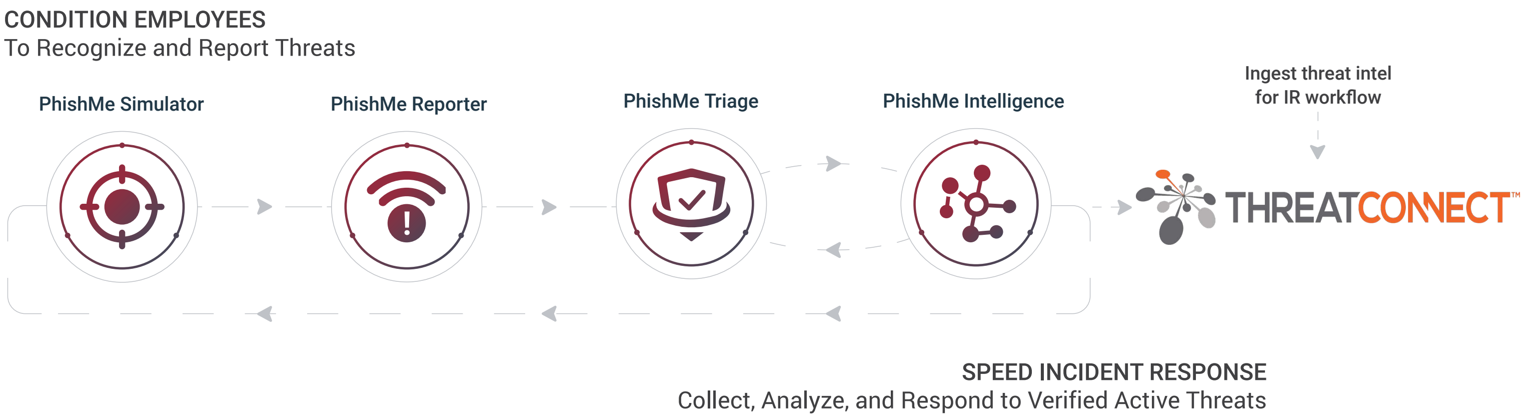
Phishing Intelligence

- ✓ Relevant, fresh, 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

- ✓ Aggregate multiple threat intelligence services to take action based on predefined policies
- ✓ Operationalize trustworthy phishing intelligence
- ✓ Ingested phishing indicators ensures the most reliable and relevant data is assessed
- ✓ Real-time phishing threat visibility

Collectively with PhishMe Intelligence and ThreatConnect, security teams have unobstructed views into credible phishing threats leading to higher confidence in the action take based on the indicators.



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. This can be thwarted through credible and trustworthy intelligence applied to network policies based on threat severity.

How It Works

PhishMe Intelligence and ThreatConnect deliver the ability to acquire, aggregate and take action from phishing-specific machine-readable threat intelligence (MRTI). Using high fidelity phishing intelligence means that analysts can prioritize and decisively respond to alerts from intelligence consumed via PhishMe's API. With ThreatConnect, security teams are able to take action based on PhishMe Intelligence indicators through their existing infrastructure to alert or block ingress or egress traffic.

PhishMe Intelligence uses easy-to-identify impact ratings of major, moderate, minor, and none, for teams to create rules based on the level of impact. When these indicators are received by ThreatConnect, steps can be defined to operationalize threat intelligence.

.

Furthermore, PhishMe Intelligence provides rich contextual human-readable reports to security teams, allowing for in-depth insight into the criminal infrastructure. Analysts and security leaders will have visibility into email message contents, malware artifacts with full threat detail, and executive summaries, to easily understand the threat actor's TTP operation and risk to the business.

PhishMe Intelligence ingested by ThreatConnect provides rich insight for assertive action from the following types of indicators:

- Payload URLs and Exfiltration Sites
- Command and Control Servers
- Malicious file and IP Addresses
- Compromised Domains

In addition, PhishMe provides access to the Active Threat Report and full threat detail for the above correlated event.

With this formidable combination, security teams can respond quickly and with confidence to mitigate identified threats. Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions based on security policies for ingress and egress traffic.

About ThreatConnect

ThreatConnect unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Built for security teams at all maturity levels, the ThreatConnect platform enables organizations to benefit from their collective knowledge and talents; develop security processes; and leverage their existing technologies to identify, protect and respond to threats in a measurable way. More than 1,200 companies and agencies worldwide use ThreatConnect to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence. To register for a free ThreatConnect account or learn more, visit: www.threatconnect.com.

THREATCONNECT™

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.

PHISHME

For more information contact:

W: phishme.com/contact T: 703.652.0717
A: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175