PhishMe™ Integration Brief

PhishMe Intelligence and EclecticIQ

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.

The EclecticIQ threat intelligence platform, makes sense of all of the threat data that security teams have to sort through to find the needle(s) in the haystack that can threaten your business, customers, intellectual property, and reputation.

EclecticIQ is analyst-centric, allowing teams to configure intelligence feeds, automatically enrich data, and integrate with IT security controls. The platform produces structured cyber intelligence and is easily shared and among staff to remove complex processes that may exist. With duplicate detection and automated prioritization, EclecticIQ can also integrated with exiting solutions to protect previous investments.

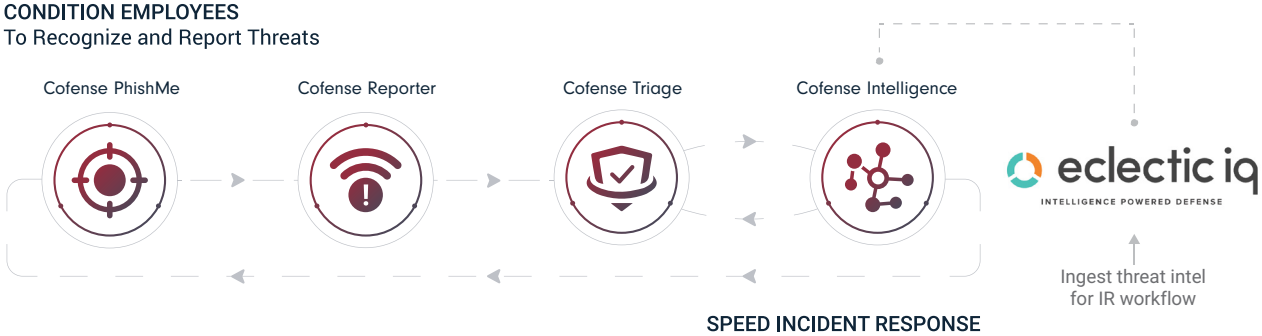
Phishing Intelligence

- 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 pre-defined 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 EclecticIQ, 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 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 EclecticIQ 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 EclecticIQ, 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 EclecticIQ, 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 EclecticIQ provides rich insight for assertive action from the following types of indicators:

- Payload URLs and Exfiltrations 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 EclecticIQ

EclecticIQ helps organizations to turn cyber threat intelligence into business value through products built for cyber security professionals in threat intelligence, threat hunting, SOC, and Incident Response. EclecticIQ Platform is the analyst-centric threat intelligence platform based on STIX/TAXII that meet the full spectrum of intelligence needs. EclecticIQ Fusion Center enables the acquisition of thematic bundles of cyber threat intelligence from leading suppliers with a single contract. The company won Deloitte's Technology FAST50 Rising Star Award for "Most Disruptive Innovator". EclecticIQ is headquartered in Amsterdam, The Netherlands. https://www.EclecticIQ.com.

eclectic iq
INTELLIGENCE POWERED DEFENSE

COFENSE

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175