Cofense Triage Integration Brief

COFENSE TRIAGE™ & COFENSE INTELLIGENCE WITH LOGRHYTHM®

Cofense delivers comprehensive human phishing defense solutions focused on fortifying employees – your last line of defense — after a phishing attack evades your other technology. Cofense enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks.

Armed with Cofense Triage ™ and Cofense Intelligence™, organizations leverage a combination of employee-reported phish bypassing secure email gateways and 100% human-verified phishing threat intelligence. Both sources enrich automation, orchestration and response.

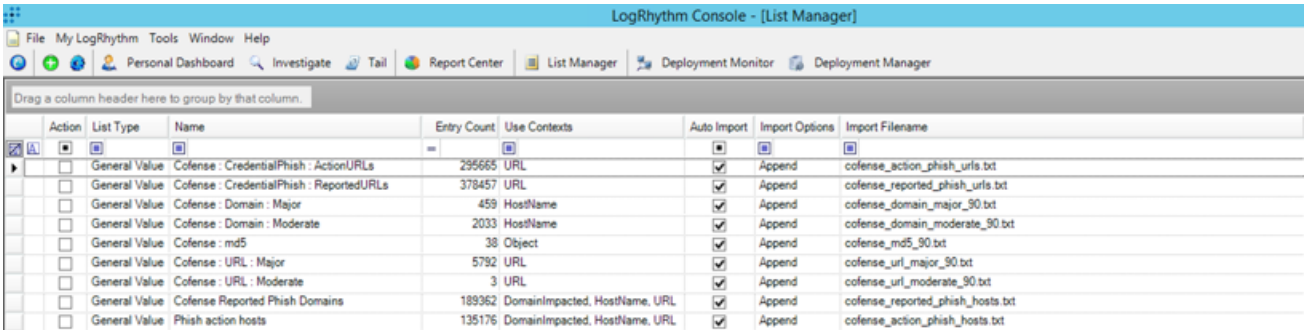
When it comes to stopping threats, seconds matter. That's why LogRhythm built its platform for speed. Analysts can quickly identify threats, automate and collaborate on investigations, and remediate threats with agility.

LogRhythm delivers solutions for next-generation SIEM, log management, endpoint/network monitoring and forensics, security analytic in a unified security intelligence platform.

Reduce phishing investigation and incident from minutes down to seconds with Cofense and LogRhythm. Analysts operationalize results that allow security teams to close gaps and disrupt attackers. Cofense and LogRhythm improve efficiency and standardize processes that can be automated.

Security leaders can ensure routine, repetitive tasks are achieved consistently and efficiently, freeing up valuable analyst time that can be devoted to more complex and advanced responsibilities.

- Employee-reported phishing analysis by Cofense Triage from emails bypassing secure email gateways
- High fidelity intelligence about phishing, malware, and botnet infrastructure collected by Cofense analysts
- Human-verified timely and contextual phishing machine-readable threat intelligence
- Incident response automation initiated by verified phishing threats accelerates resolution times
- Playbook-enabled investigation of phishing threats empower analysts to work more efficiently
- Automatically ingesting or querying phishing indicators enriches incident analysis and response
- Playbook execution determined by phishing indicator impact ratings facilitates decisions



Cofense Triage Integration Brief

COFENSE TRIAGE™ & COFENSE INTELLIGENCE WITH LOGRHYTHM®

When combined, Cofense Triage, Cofense Intelligence, and LogRhythm offer security teams the ability to harness the power of credible employee-reported and human-verified phishing intelligence. Cofense Triage ingests and analyzes employee-reported phishing emails bypassing secure email gateways.

Analysts using LogRhythm can receive phishing events from Cofense Triage to help focus in on threats that have evaded the email gateway and respond quickly. Cofense Intelligence human-verified indicators are a valuable source of intelligence that analysts can use in the LogRhythm NextGen SIEM Platform to investigate incidents and conduct threat hunting. Analysts have unobstructed views into credible phishing threats leading to confidence in the action taken based on the indicator results returned to the platform.

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 phishing intelligence applied to network policies based on threat severity.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real-time correlation, prioritization, and automation of security events with the confidence to act is critical when seconds matter in mitigating threats.

Alert Fatigue

Too many threat intelligence feeds are full of false positives that distract security analysts. Excessive alerts only exasperate overwhelmed analysts with limited time.

Cofense Triage automatically analyzes employee-reported phishing emails and LogRhythm can ingest phishing data via syslog for next step actions. Cofense Triage provides rules and intelligence from Cofense security researchers. When reported emails match Cofense or analyst-written rules, malicious emails are highlighted, while benign are eliminated. From here ingestible phishing events can be used in next step playbooks.

Cofense Intelligence provides contextual human-readable reports to security teams, allowing for 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 the risk to the business from the following types of indicators:

Payload URLs and exfiltration sites, malicious IP addresses, compromised domains, C2 servers