



# Cofense Integration Brief

## Cofense Triage™ and 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

Action	List Type	Name	Entry Count	Use Contexts	Auto Import	Import Options	Import Filename
<input type="checkbox"/>	General Value	Cofense : CredentialPhish : ActionURLs	295665	URL	<input checked="" type="checkbox"/>	Append	cofense_action_phish_urls.txt
<input type="checkbox"/>	General Value	Cofense : CredentialPhish : ReportedURLs	378457	URL	<input checked="" type="checkbox"/>	Append	cofense_reported_phish_urls.txt
<input type="checkbox"/>	General Value	Cofense : Domain : Major	459	HostName	<input checked="" type="checkbox"/>	Append	cofense_domain_major_90.txt
<input type="checkbox"/>	General Value	Cofense : Domain : Moderate	2033	HostName	<input checked="" type="checkbox"/>	Append	cofense_domain_moderate_90.txt
<input type="checkbox"/>	General Value	Cofense : md5	38	Object	<input checked="" type="checkbox"/>	Append	cofense_md5_90.txt
<input type="checkbox"/>	General Value	Cofense : URL : Major	5792	URL	<input checked="" type="checkbox"/>	Append	cofense_url_major_90.txt
<input type="checkbox"/>	General Value	Cofense : URL : Moderate	3	URL	<input checked="" type="checkbox"/>	Append	cofense_url_moderate_90.txt
<input type="checkbox"/>	General Value	Cofense Reported Phish Domains	189362	DomainImpacted, HostName, URL	<input checked="" type="checkbox"/>	Append	cofense_reported_phish_hosts.txt
<input type="checkbox"/>	General Value	Phish action hosts	135176	DomainImpacted, HostName, URL	<input checked="" type="checkbox"/>	Append	cofense_action_phish_hosts.txt

# 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.

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 Exfiltrations Sites
- Malicious IP Addresses
- Compromised Domains
- C2 Servers

## Working Together

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.

### About LogRhythm

LogRhythm helps busy and lean security operations teams save the day — day after day. There's a lot riding on the shoulders of security professionals — the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources — the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps. Together, LogRhythm is ready to defend. Learn more at [logrhythm.com](http://logrhythm.com).



### About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of more than 35+ million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit [www.cofense.com](http://www.cofense.com) or connect with us on [Twitter](#) and [LinkedIn](#).



W: [cofense.com/contact](http://cofense.com/contact) T: 703.652.0717

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