Cofense Integration Brief

COFENSE TRIAGE™ AND LOGRHYTHM®

Over 90% of today's data breaches are attributed to phishing attacks. Thus, organizations need to adopt an integrated approach to security by layering both technology and human solutions to combat these ever-evolving threats. The Cofense and LogRhythm integration provides security teams with the ability to quickly respond to phishing attacks that have bypassed infrastructure security controls. By leveraging the power of human-reported phishing attacks, analysts can prioritize the most critical events and then take action with LogRhythm's Security Intelligence Platform.

Incident Response

- ✓ Cofense's algorithmic engine analyzes suspicious reported emails and prioritizes the most critical
- ✓ Workflow automation based on recipe, alert, and event categorization
- ✓ Analysts respond to high priority phishing events supporting better time management and quicker incident resolution

Integration

- ✓ Enterprise Security Intelligence Platform provides event visibility and correlation with other machine data for threat lifecycle management
- ✓ SmartResponse enables immediate and automated response actions to contain the attack

IR Team Challenges

Attackers Evading Technical Controls

As technology evolves to defend against threats, attackers are becoming more creative at infiltrating employees' inboxes, hoping they will open the attachment or click the link.

Employees conditioned to recognize and report suspicious email are a valuable source of human intelligence, contributing data that may otherwise go unnoticed for an extended period of time.

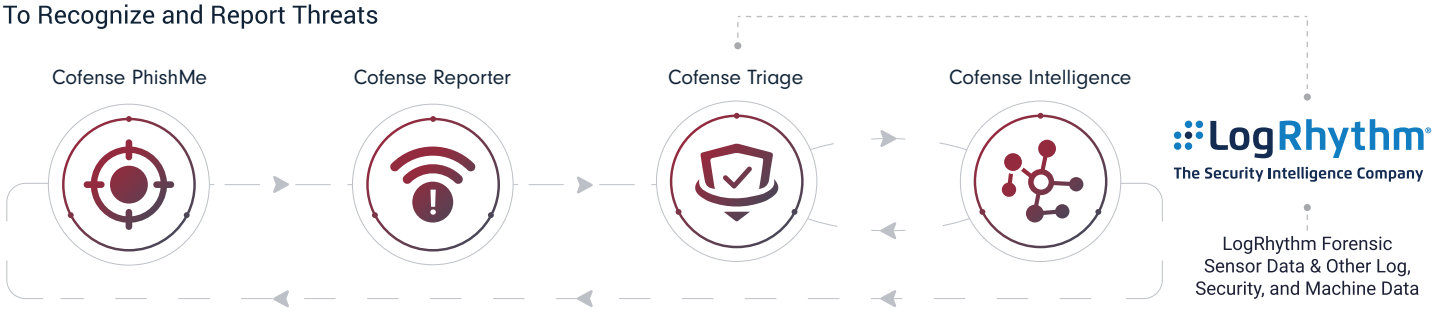
Threat Prioritization

Security teams can't take chances on which events require immediate action and which are benign. Identifying critical events helps disrupt the attacker's mission more efficiently.

Workflow Automation

Too many alerts to analyze and process lead to a delay in action. Automation is necessary to reduce the burden on security teams so they can focus more time on hunting and remediation.

CONDITION EMPLOYEES
To Recognize and Report Threats



SPEED INCIDENT RESPONSE
Collect, Analyze, and Respond to Verified Active Threats

How It Works

Cofense Triage and LogRhythm's Security Intelligence Platform provide security teams the ability to create a workflow that defends against phishing attacks. This workflow contains Indicators of Phishing (IoPs) to help highlight the most critical events requiring action.

Cofense Triage enables IT security teams to automate and prioritize reported threats to speed incident response. Triage ingests human-reported phishing emails and automatically prioritizes security events that are most critical based on phishing intelligence, anti-malware technologies, URL and IP address analysis, and YARA rules. Integration with Cofense Reporter allows threat prioritization based on user reputation, attributes, and threat intelligence. SOC and incident response analysts now have actionable intelligence to detect and contain security incidents.

Cofense Triage collects and prioritizes internally generated phishing attacks from Cofense Reporter and maps indicators within the event data fields to LogRhythm's Security Intelligence Platform:

- **Recipe Match**
- **YARA Rule Match**
- **Recipe and Rule Category**
- **Email Subject**
- **Link to Incident**
- **Recipe and Rule Priority**

LogRhythm's Security Intelligence Platform receives and correlates security events from Triage along with petabytes of other machine data, allowing for deep visibility and end-to-end threat detection and response workflows.

Security teams can leverage LogRhythm's extensive search and visualization capabilities to conduct further investigation, or based on predefined criteria, invoke automated remediation via SmartResponse™ to take real-time action on hosts at the endpoint or network.

This customizable workflow means that organizations can determine the level of response and automation they wish to take, reducing the time needed to perform common investigation and mitigation steps against phishing attacks.

The integration between Cofense Triage and LogRhythm's Security Intelligence Platform provides organizations with a strong understanding and control over the phishing incident response process. Organizations can confidently execute swift, decisive action on the most critical events and disrupt attackers before they can complete their mission.

About LogRhythm

LogRhythm® empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented SmartResponse™ automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface

LogRhythm
The Security Intelligence Company

COFENSE

W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175