Cofense Triage & Intelligence Integration Brief

Cofense Triage™, Cofense Intelligence™ and Splunk® SOAR

Operationalize Phishing Threat Indicators for Investigation, Response, and Resiliency

Cofense® and Splunk® integrate for visibility into one of the biggest cyber security risks — phishing. With many of today's data breaches attributed to phishing, security teams require insight into adversary criminal infrastructure that can be operationalized to alert and respond to phishing threats.

Cofense Triage™ and Splunk SOAR support incident responders with their need to act on all alerts quickly by automating threat qualification and investigation. SOC teams can focus on interpreting results and responding to phishing threats effectively. With Cofense Triage's 2nd version API, dozens of endpoints retrieve valuable phishing data to provide security teams with the ability to correlate with other data points and view the risk to the company.

Cofense Intelligence™ is 100% human-verified machine-readable threat intelligence (MRTI). Customers receive a fully vetted source of intelligence verified by Cofense researchers. Cofense also provides security teams with context around the criminal infrastructure to extend beyond a list of Indicators of Compromise (IOCs), and enable teams to see their adversary's full operation as opposed to one-offs that change rapidly. Splunk SOAR playbooks leverage Cofense-provided phishing intelligence into the platform and analysts can then operationalize their workflow based on phishing indicators and their impact.

Cofense Triage

Splunk SOAR ingests employee-reported phishing incidents using multiple endpoints from Cofense Triage

Phishing attributes from Cofense Triage's Inbox, reconnaissance, and processed mailbox locations along with threat indicators and second-stage IOCs

Create incidents and enrich phishing data from multiple integrated actions available from Cofense Triage

Cofense Intelligence

Playbooks conduct threat lookups and enrichment using Cofense Intelligence phishing indicators

Relevant and contextual MRTI with no false positives enhance the security incident response process to rid false positives to focus on real phishing threats

High fidelity intelligence about phishing, malware, and botnet infrastructure

The Solution

Cofense Triage and Cofense Intelligence indicators provide security teams with visibility into phishing criminal infrastructure. Analysts gain insight into phishing URLs, IPs, domains, files, command

and control (C2), payload, and exfiltration sites. Additionally, Cofense Intelligence human-readable contextual executive and technical reports are available to provide further insight into the phishing infrastructure uncovered by Cofense. Security teams are much more confident in the action they take based on thorough indicator report analysis.

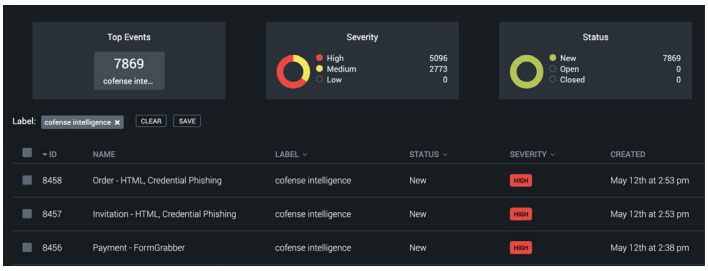
Cofense Intelligence reports not only identify what is a security risk, but explicitly state why indicators are malicious so that analysts don't have to do additional research. Cofense Triage indicators are amassed from Cofense research and intelligence and from employees who report suspicious emails that bypass defenses. Armed with human-verified intelligence indicators and verbose reports, security teams can defend the enterprise against the number one threat vector facing companies today – phishing.

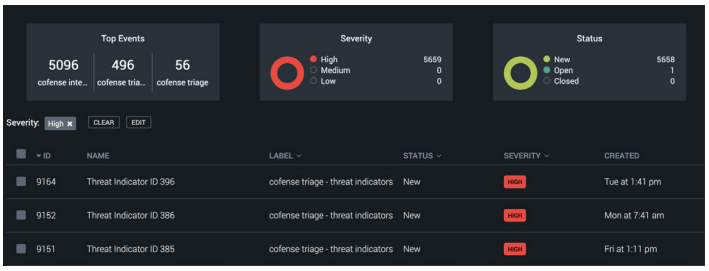
How it Works

Cofense's integrations for Splunk SOAR connect, ingest, and enrich for phishing analysis and response. The Cofense Triage app allows security teams to ingest employee-reported threats and run 20+ actions for enrichment and incident decision making. With Cofense Intelligence, Splunk SOAR conducts threat lookups and enrichment actions against Cofense's human-verified phishing intelligence. Analysts rely on Cofense's data to quickly identify the latest phishing attacks bypassing their perimeter.

Cofense's integrations enable analysts to prioritize and decisively respond to high fidelity events using command actions and to make educated decisions in their responses from:

URL, File Hash, IP Address, Domain	Malware Family
Threat Rating	2nd Stage Indicator
Malware Family	Reporter





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 close to 30 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 or connect with us on Twitter and LinkedIn.

W: cofense.com/contact **T:** 703.652.0717

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