Cofense Integration Brief

Cofense Triage™ and ServiceNow – Security Incident Response®

Legacy email security technologies can't keep up with innovative, human-created phishing attacks. Phishing Detection and Response (PDR) is imperative to disrupt phishing attacks. When employees are conditioned to detect and report phish in their inbox, security operations center (SOC) analysts need to be able to quickly and precisely separate the threats from the noise and respond before an incident becomes a breach.

Cofense Triage™ leverages out-of-the-box phishing detection components to highlight suspected phish. With Cofense Triage bidirectional APIs, ServiceNow® Security Incident Response (SIR) can create tickets for analysts to work through to closure.

Integration Features

- Ingest employee-reported phishing emails from Cofense Triage™ into ServiceNow Security Incident Response based on severity, category, threat indicators, reporter, and more.
- Create security incidents in ServiceNow Security Incident Response (SIR) from events in Cofense Triage's cluster and reports from inbox, reconnaissance, and processed queues.
- Ingest phishing threat indicators from Cofense Triage into ServiceNow SIR to enrich and respond. URLs, domains, headers, comments, .eml files, and attachments.
- Run playbooks in Cofense Triage from ServiceNow to categorize reports and respond to reporters and security teams.
- Bidirectionally manage phishing threats between Cofense Triage and ServiceNow SIR.

Benefits

- Integrate ServiceNow SIR and Cofense Triage.
- Accelerate phishing email identification and mitigation.
- Bi-directional integration and enrichment between platforms.
- Improve analyst efficiency to investigate and respond without switching screens.
- Centralized visibility into security incident management and response.

Suspicious Emails Require Timely Investigation

Challenge: Every employee-reported email could be a phish evading technology defenses. Threats may not be prioritized and investigated timely, and analysts are inundated with false positives and other obligations. It's important to identify phishing threats and respond in minutes.

Solution: Security teams leveraging Cofense Triage quickly cluster similar reported emails and remove benign reports, leaving only the select few emails to respond to. Cofense Triage analyzes and highlights legitimate phishing threats from human-verified phishing indicators and tactics.

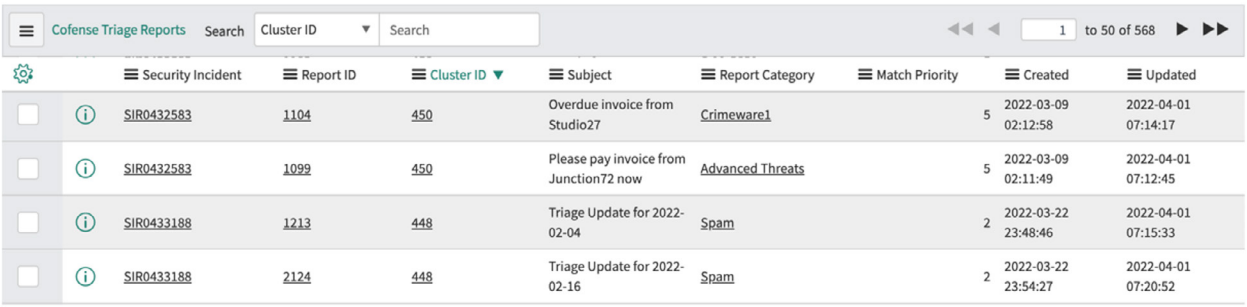
Benefit: Analysts process a manageable phishing workload. Phishing emails, their associated threat indicators and observables, and incident details are accessible within ServiceNow SIR. Phish are analyzed and incidents managed bidirectionally through playbooks.

Lack of Centralized Visibility into Phishing Incidents

Challenge: Solutions lacking integration leave analysts with the need to switch between screens. Integrations provide visibility into reported emails that may indicate a phishing attack and there is a need to ingest the indicators and observables into a centralized security incident platform.

Solution: Cofense Triage leverages rules and human-verified phishing intelligence from global phishing expertise. Reported benign emails are processed as non-malicious, leaving others processed as crimeware, advanced threats, or business email compromise. ServiceNow SIR ingests from Cofense Triage malicious processed reports along with indicators and observables.

Benefit: Analysts get the benefit of automated phishing workflows and centralized reporting in ServiceNow for threats uncovered by Cofense Triage. Additionally, ServiceNow SIR can read and write to Cofense Triage to ingest as well as post information bidirectionally.



Security Incident	Report ID	Cluster ID	Subject	Report Category	Match Priority	Created	Updated
SIR0432583	1104	450	Overdue invoice from Studio27	Crimeware1	5	2022-03-09 02:12:58	2022-04-01 07:14:17
SIR0432583	1099	450	Please pay invoice from Junction72 now	Advanced Threats	5	2022-03-09 02:11:49	2022-04-01 07:12:45
SIR0433188	1213	448	Triage Update for 2022-02-04	Spam	2	2022-03-22 23:48:46	2022-04-01 07:15:33
SIR0433188	2124	448	Triage Update for 2022-02-16	Spam	2	2022-03-22 23:54:27	2022-04-01 07:20:52

Automated Phishing Detection and Response to Prevent Security Breaches

Challenge: Knowing which reported emails require incident response as well as who else has received a malicious email, requires immediate action. Manual investigation does not scale and delays response to threats. Timely analysis is essential to protecting the business.

Solution: Cofense Triage offers customers rules and analytics to manage the platform themselves, or leverage Cofense's PDR managed service. Both solution options integrate with ServiceNow SIR.

Benefit: The solution combines the power of two solutions for quick identification of threats and decisive action to cut off an attack in progress and prevent a breach. Additionally, phishing indicators and observables are collected, updated when necessary, and referenceable against previous, current, or future phishing threats in Cofense Triage. Analysts can easily identify which threats have been managed and which are new and require immediate attention.

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