Cofense Triage 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.

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.

Integration Features

- Ingest employee-reported phishing emails from Cofense Triage™ into ServiceNow Security Incident Response based on severity, category, threat indicators, and reporter reputation.
- Create security incidents in ServiceNow Security Incident Response (SIR) from events in Cofense Triage's inbox, reconnaissance, and processed queues.
- Ingest phishing threat indicators from Cofense Triage into ServiceNow SIR to enrich and respond.
- Update and process phishing emails in Cofense Triage from ServiceNow SIR.
- Bidirectionally manage phishing threats between Cofense Triage and ServiceNow SIR.

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.

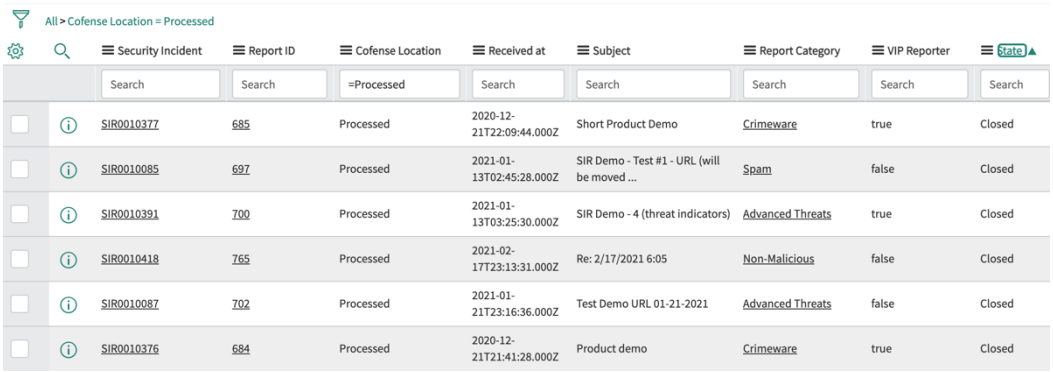
Benefit: Analysts process a manageable phishing workload. Phishing emails, their associated threat indicators and observables, and incident details are accessible within ServiceNow SIR. Phish are analyzed and incidents managed bidirectionally.

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.



All > Cofense Location = Processed

Security Incident	Report ID	Cofense Location	Received at	Subject	Report Category	VIP Reporter	State
Search	Search	=Processed	Search	Search	Search	Search	Search
SIR0010377	685	Processed	2020-12-21T22:09:44.000Z	Short Product Demo	Crimeware	true	Closed
SIR0010085	697	Processed	2021-01-13T02:45:28.000Z	SIR Demo - Test #1 - URL (will be moved ...	Spam	false	Closed
SIR0010391	700	Processed	2021-01-13T03:25:30.000Z	SIR Demo - 4 (threat indicators)	Advanced Threats	true	Closed
SIR0010418	765	Processed	2021-02-17T23:13:31.000Z	Re: 2/17/2021 6:05	Non-Malicious	false	Closed
SIR0010087	702	Processed	2021-01-21T23:16:36.000Z	Test Demo URL 01-21-2021	Advanced Threats	false	Closed
SIR0010376	684	Processed	2020-12-21T21:41:28.000Z	Product demo	Crimeware	true	Closed

Categorized Phishing Incidents

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.