




COFENSE TRIAGE & VISION INTEGRATIONS








Technical Alliance Partners

The Cofense Technology Alliance Program (TAP) fosters a collaborative and mutually beneficial ecosystem with our technical alliance partners. Together, we deliver a more robust solution to combat phishing attacks while effectively addressing our customers' needs. Cofense enables complementary IT solution providers to seamlessly integrate their security capabilities with Cofense products and services. By integrating security technologies, Cofense equips security analysts and incident responders with the tools they need to make smarter, more effective decisions about the threats targeting their organization. In addition, Cofense integrations enable customers to simplify deployment, improve efficiency, reduce costs, and optimize their overall IT security investments.




Triage SIEM Partners

Partner	How It Works
 a CISCO company	An add-on with Splunk is available in the "Splunkbase" that extracts data from Triage via API. Splunk can also receive Common Event Format events from triggers and categorizations. Triage admins can also send events based on manual trigger or report categorization, as well as when a YARA rule is matched.
	Enables bi-directional exchange of threat intelligence between Cofense Triage and Microsoft Sentinel. An app is available in the Azure Marketplace that pulls indicators from Cofense Triage and creates corresponding threat intelligence indicators in Sentinel. Likewise, it retrieves non-Cofense indicators from Sentinel and can create or update them in Cofense Triage, ensuring consistent threat intelligence across both platforms. This also ensures indicators of compromise (IOCs) from Cofense Triage can be shared with Defender for Endpoints within the Microsoft Suite.
	Enables the ingestion of Cofense Triage reports and uses them to create Google Security Operations alerts. These alerts can be used to perform orchestrations with playbooks or for manual analysis. The integration enables enrichment of the related entities and details about the Triage report so further downstream actions can be taken.


Triage Analysis Partners

Partner	How It Works
	The integration with Cofense Triage enables a range of actions, including testing connectivity to validate asset configurations, retrieving reports and individual report details, and downloading raw emails linked to specific report IDs. Admins can access categories, threat indicators, URLs, comments, rules, reports, and integration submissions, all with filtering options based on provided parameters.
	Cofense Triage can send to XSOAR phishing indicators that XSOAR can then process as part of a playbook. Triage can send IPs, domains, URLs, and hashes for XSOAR to receive and act on. Additionally, XSOAR can ingest IOCs from Triage through API endpoints. Categorized reports, along with indicator analysis tags, are capable of ingestion to use in playbooks.
	Cofense Triage sends phishing incident detail notifications to ServiceNow Security Operations. ServiceNow receives, parses, and creates tickets for security teams to process as part of their security incident response workflow. Triage provides phishing incident response process instructions for analyzing attachments, blocking network addresses, identifying recipients, and removing phishing emails.
	Cofense Triage can send phishing indicators to Swimlane that can then be processed as part of a playbook. Triage can send IPs, domains, URLs, and hashes for Swimlane to receive and act on. Additionally, Swimlane can ingest IOCs from Triage through API endpoints. Categorized reports, along with indicator analysis tags, are capable of ingestion to use in playbooks.
	ThreatQuotient can ingest malicious, suspicious, and benign indicators from Triage using its API. Analysts in Triage can tag hashes, domains, URLs, senders, and subjects that are malicious or suspicious and ThreatQuotient can ingest, cross-correlate in its threat library, and allow next-step actions based on intelligence.

Triage Threat Intelligence Partners



Partner	How It Works
 Cisco Umbrella	Triage can be configured to send data via the Cisco Umbrella Investigate API to query IP addresses and domains within Umbrella Investigate and receive indicator results if they are benign, suspicious, or malicious. Results back to Triage can then be used to help an analyst prioritize workload.
 Hatching™ A Recorded Future® Company	Cofense Triage allows you to submit report attachments to your organization's Hatching instance for analysis. This can be done automatically during email ingestion or manually by submitting any file from the Attachments tab of a Triage report that includes attachments. When Hatching completes the analysis, it returns the results to Triage. Triage users can manually submit a URL to Hatching for analysis also, although not automatically during ingestion.
 VIRUSTOTAL	If your organization has a valid VirusTotal subscription, Cofense Triage can send attachments, hashes of attachments, and URLs to VirusTotal for analysis. Beyond returning data about submitted items, VirusTotal also returns some threat-level analysis. Triage scores the threat level and visually represents it using icons and colors.

Triage Anti-Malware Partners

Partner	How It Works
 paloalto® NETWORKS	Analysts configure Triage to submit hashes of attachments or full files to Palo Alto WildFire. Triage admins can also manually submit any hash or supported attachment type from Triage to WildFire using the API. WildFire will return the results to Triage, where the results are used for incident response workflow. Triage provides a full malware contextual report received back from WildFire via the API. Additionally, Cofense Triage integrates with MineMeld to obtain Triage threat indicators.

COFENSE VISION INTEGRATIONS

Triage Anti-Malware Partners

Partner	How It Works
 splunk> SOAR	This integration provides a comprehensive set of investigative and management actions to support email security operations orchestrated from Splunk SOAR. It enables quarantining and restoring emails, managing IOCs, searching messages, and downloading emails and attachments. Key capabilities include retrieving message metadata, fetching full message content and attachments, managing quarantine jobs (create, approve, restore, stop, or delete), and performing detailed message searches. The app also allows users to create, update, retrieve, list, or delete IOCs from the Vision repository, as well as download component logs for troubleshooting and auditing purposes.
 CORTEX™ XSOAR BY PALO ALTO NETWORKS	Provides commands to initiate advanced search jobs to hunt and quarantine suspected attack campaigns from Cortex XSOAR/XSIAM. Search and quarantine actions can take place based on IOCs and email attributes to remove the threat from mailboxes. The integration also provides commands to download messages and their attachments, as well as create quarantine jobs in Vision. Analysts can manage IOCs used to search and quarantine emails that are part of emerging threats.

Cofense is the only cybersecurity company leveraging expert-supervised AI for phishing detection and response—delivering human-vetted intelligence and real-world training to help enterprises stay ahead of modern threats. Built to augment existing email defenses, Cofense identifies attacks that bypass perimeter filters, remediates them in minutes, and continuously strengthens the human layer through simulations modeled on active phishing campaigns. Informed by insights from over 35 million trained users, Cofense enables faster containment of threats and measurable reductions in risk. Organizations like Visa, Santander, and Blue Cross Blue Shield rely on Cofense to reduce exposure, meet regulatory demands, and build lasting resilience against the most persistent cyber threat: phishing.

PHISHME
COFENSE

SMARTER PHISHING DEFENSE.
STRONGER HUMAN SECURITY.

