Cofense Intelligence Integrations

TECHNICAL ALLIANCE PARTNERS

Cofense Intelligence™ provides unparalleled phishing threat intelligence collected and vetted by security experts to ensure the greatest accuracy and response effectiveness. Cofense provides the context that security analysts and incident responders need to make decisions on the phishing threats facing their company. Cofense integrations enable customers to simplify deployment, improve efficiency, reduce costs, and optimize their overall IT security investments. The Cofense Technology Alliance Program (TAP) cultivates a strong and mutually profitable ecosystem with our technical alliance partners to provide a more comprehensive solution to fight phishing attacks, and best meet our customers' requirements.

Threat Intelligence Partners

Partner	How It Works
ANOMALI	Cofense Machine-Readable Threat Intelligence (MRTI) can be ingested into the Anomali ThreatStream ThreatIntelligence Platform (TIP) using Cofense's API. Cofense has an app in the Anomali app store. ThreatStreamingests Cofense Intelligence indicators and provides links to contextual reports.
eclectic iq	Cofense Intelligence and EclecticIQ Platform deliver the ability to acquire, aggregate and take action from phishing- specific MRTI. EclecticIQ Platform ingests phishing IOCs via Cofense's API. With EclecticIQ Platform, security teams are able to take action based on Cofense Intelligence indicators through their existing infrastructure to alert or block ingress or egress traffic.
KING UNION	Cofense Intelligence and King & Union Avalon deliver the ability to acquire, aggregate and take action from phishing-specific MRTI. The Avalon Platform ingests phishing IOCs via Cofense's API. With Avalon security teams are able to take action based on Cofense Intelligence indicators through their existing infrastructure to alert or block ingress or egress traffic.
MISP Threat Sharing	The Cofense Intelligence MISP feed provides a way to ingest file and network phishing indicators. Analysts are then able to correlate Cofense Intelligence with other intelligence feeds as well as understand the malware tactics from the indicators received. Additionally, phishing message screenshots and links to Active Threat Reports provide for context.
paloalto NETWORKS	Cofense Intelligence can be ingested into Palo Alto Networks MineMeld application. Customers are required to create an open source MineMeld server which formats Cofense Intelligence so that it can be applied to Palo Alto Networks next-generation firewalls. The firewalls use external dynamic lists that pull in the indictors from MineMeld and are then applied to firewall security policies. MineMeld pulls in Cofense indicators and formats them which can then be applied to security policies.
PATERVA A new train of thought	Cofense Intelligence and Paterva's Maltego application integrate so that analysts can gather, interrogate and visualize data in order to find relationships. Cofense has developed transforms for Maltego to visualize relationships between observables within a specific attack and explicitly pinpoint how attackers are delivering their malicious payloads.
Recorded Future	Recorded Future has an extension available within their platform that leverages Cofense's API for phishing intelligence. Analysts in Recorded Future can seamlessly pivot to Cofense and get indicator validation on IPs, domains, and files.
ThreatConnect	Cofense provides an app in ThreatConnect to ingest MRTI into the platform. Cofense's API is leveraged to pull in actionable phishing indicators. Analysts can then create process around indicator impact ratings.
THREATQ	Cofense MRTI can be ingested into the ThreatQuotient Threat Intelligence Platform (TIP) using Cofense's API. The customer will enable Cofense Intelligence from within ThreatQ platform and ingest Intelligence which will show threat IDs, malware families, URLs, IP addresses, etc.
TREND MICRO	Cofense Intelligence can be ingested into Trend Micro TippingPoint and then actionable rules applied. An indicator can have a block rule placed within TippingPoint against IPs, domains, or URLs. This allows analysts to block and monitor based on indicators from Cofense Intelligence.

SIEM Partners

Partner	How It Works
IBM	IBM QRadar ingests Cofense MRTI by using Cofense's app within IBM App Exchange. The intelligenceingested can then be used in a SOC to monitor and alert on activity matching indicators.
LogRhythm	Cofense MRTI can be ingested into LogRhythm using Cofense's API. The ingestion of intelligence can then be used in a SOC to monitor/alert on activity when a domain, URL, or IP address matches what Cofense has provided to the customer.
McAfee	Cofense MRTI can be ingested into McAfee ESM using Cofense's API via a standalone Python script. This CEF ingestion can then be used in a SOC to monitor/alert on activity when a domain or IP address matches what Cofense has provided to the customer.
MICRO FOCUS	Cofense MRTI can be ingested into ArcSight using Cofense's API via a standalone python script. This CEF ingestion can then be used in a SOC to monitor/alert on activity when an indicator matches what Cofense has provided to the customer.
RSA READY	Cofense MRTI imported into RSA NetWitness in STIX format. The ingestion of indicators can be used in a SOC to monitor/alert activity when an indicator matches what Cofense has provided to the customer.
splunk>	Cofense Intelligence can be ingested into Splunk using Cofense's API and the Splunk App which is available within the Splunkbase library. This ingestion can then be used in a SOC to monitor/alert on activity when an indicator matches what Cofense has provided to the customer.

Analysis Partners

Partner	How It Works
CENTRIPETAL NETWORKS	Cofense MRTI indicators are ingested into the Centripetal Networks QuickThreat Gateway using Cofense's API. Custom rules in Centripetal Networks allow analysts to block or alert based on impact rating of IPs, domains, and URLs.
CORTEX	Cofense Intelligence serves to validate phishing incident impact so that analysts can make efficient use of their time. XSOAR playbooks leverage Cofense Intelligence indicator IPs, domains, URLs, and files. Analysts can use the results and context for additional actions and playbooks. Also, Cofense Intelligence is supported in XSOAR – threat intelligence management module.
CYWARE	Cyware CTIX (Cyware Threat Intelligence Exchange) can ingest Cofense Intelligence phishing indicators in JSON format. Each indicator ingested can be used in playbooks and threat lookups from CTIX to use the threat impact rating of each Cofense Intelligence indicator.
sumo logic	Cofense Intelligence serves to validate phishing incident impact so that analysts can make efficient use of their time. Sumo Logic's (formerly, DFLabs) platform can leverage Cofense Intelligence indicator IPs, domains, URLs, and files. Analysts can use the results and context for additional actions and playbooks.
splunk>	Cofense Intelligence is capable of validating incident impact to allow analysts efficient use of their time. Splunk SOAR (formerly, Phantom) actions include hunt URL, hunt IP, hunt file, and hunt domain, to name a few. Analysts can then use Cofense's results in additional actions and playbooks.
servicenow	ServiceNow Security Operations Polls the Cofense Intelligence API in a search-based integration to validate incidents that may be related to phishing. Security Operations makes use of Cofense Intelligence indicator IPs, domains, URLs, and files. Analysts can use the results and context for additional actions and orchestration.

SWIMLANE	Cofense Intelligence is a value-added data source integrated with Swimlane's orchestration platform. As threats are identified, Swimlane automation and orchestration customers can use Cofense Intelligence to verify if a threat is real. Swimlane takes in multiple threat intelligence sources, such as Cofense's, and correlates them against IP addresses, hashes, domains and URLs to prioritize and remediate events.
Trellix	Cofense Intelligence and FireEye Security Orchestrator deliver the ability to investigate, validate, and orchestrate based on indicator impact ratings from phishing-specific MRTI. Ingestion of phishing IOCs allow analysts to use commands such as ipSearch, urlSearch, domainSearch, and hashSearch.
vmware®	VMware's Carbon Black endpoint solution ingests Cofense Intelligence IOCs to be used for analysis, event correlation, and enrichment. Endpoint activity can assess activity with IOCs and provide insight into the threat severity and additional context with human readable Active Threat Reports.

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

COFENSE