COFENSE INTELLIGENCE INTEGRATIONS

PHISHME COFENSE

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.

SIEM Partners

Partner	How It Works
splunk> a cisco company	Cofense Intelligence can be integrated into Splunk Enterprise through Cofense's API and the Splunk app, available in the Splunkbase library. Once ingested, this data can be used in a SOC to monitor and generate alerts whenever an indicator matches intelligence provided by Cofense.
Microsoft Sentinel	This integration enables seamless threat intelligence sharing between Cofense Intelligence and Microsoft Sentinel. It retrieves Cofense indicators through the Threat Feed API, generates corresponding threat intelligence indicators in Microsoft Sentinel, and stores malware data in a custom log analytics table for visualization in Sentinel workbooks and raw data access. Additionally, the integration pulls all Microsoft Threat Intelligence indicators from Sentinel and updates or creates related Cofense threat indicators in Microsoft Defender for Endpoint, ensuring consistent and actionable intelligence across platforms.

Analysis Partners

Partner	How It Works
Phantom®	Cofense Intelligence is capable of validating incident impact to allow analysts efficient use of their time. 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.
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.

Threat Intelligence Partners

Partner	How It Works
ANOMALI	Cofense Machine-Readable Threat Intelligence (MRTI) can be ingested into the Anomali ThreatStream Threat Intelligence Platform (TIP) using Cofense's API. Cofense has an app in the Anomali app store. ThreatStream ingests Cofense Intelligence indicators and provides links to contextual reports.
Hatching™ A Recorded Future® Company	Hatching has an extension available within their platform that leverages Cofense's API for phishing intelligence. Analysts in Hatching can seamlessly pivot to Cofense and get indicator validation on IPs, domains, and files.
paloalto® NETWORKS	Cofense Intelligence can be ingested into the Palo Alto 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's next-generation firewalls. The firewalls use external dynamic lists that pull in the indictors from MineMeld and are then applied to firewall security policies.
THREATQUOTIENT™ A SECURONIX COMPANY	Cofense MRTI can be ingested into the ThreatQuotient Threat Intelligence Platform (TIP) using Cofense's API. The customer will enable Cofense Intelligence from within the ThreatQ platform and ingest intelligence, which will show threat IDs, malware families, URLs, IP addresses, etc.

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.