COFENSE | PARTNER

CORTEX™ XSOAR BY PALO ALTO NETWORKS

Automate Phishing Threat Analysis and Incident Remediation

Phishing emails are one of the most frequent, easily executed, and harmful security attacks that organizations – regardless of size – face today. Many data breaches begin with a malware-based or credential- stealing phishing email capable of inflicting financial and reputation damage. Security analysts face numerous challenges while responding to phishing attacks. A barrage of attacks, multiple screens to coordinate response, manual and repetitive tasks, non-standardized processes and reporting metrics are all sources of stress.

Cofense has several content packs available on the Cortex XSOAR Marketplace. Cofense Triage and Cofense Intelligence combine automated phishing analysis and human-verified indicators of phishing. Cofense Triage ingests, clusters, and analyzes reported phishing emails to prioritize threats. Cofense Intelligence enriches Cortex XSOAR playbooks with rich contextual data for automated incident response actions and analyst investigation.

Integration Features

Cortex XSOAR playbooks leverage the combination of Cofense Triage indicators and reports of phishing and Cofense Intelligence's phishing intelligence, to be used in playbooks for the incident response team to remediate.

Automate report ingestion and execute playbook commands in addition to collaborating with other analysts and Cortex XSOAR's chatbot.

Benefits

Prioritize risk quickly with automated email analysis and extraction of phishing indicators.

Shorten decision-making cycle and response by automating phishing response.

Gain insights for future threat hunting from cross-correlation of phishing indicators.

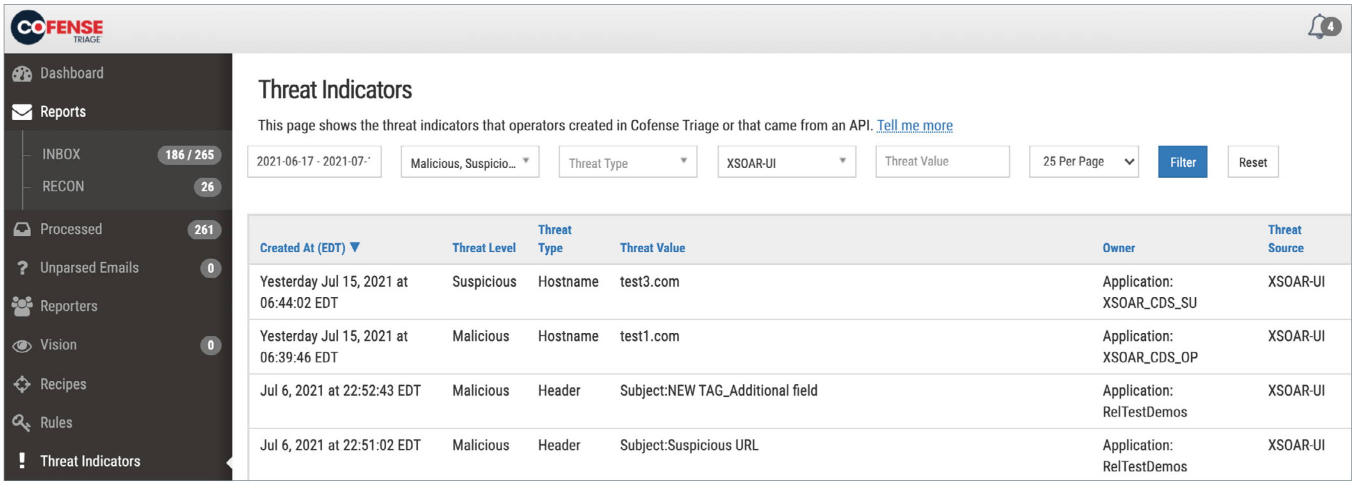
Compatibility

Products: Cortex XSOAR, Cofense Triage™ and Cofense Intelligence™

1 Use Case #1

Remediate Phish Evading SEGs with Cofense Triage v2 API

Challenge: Attackers continueto successfully evade secure email gateways (SEGs) designedto defend the business against phishing threats. Employees,the last line of defense after technologies have been bypassed, report suspicious emails to thesecurity team to investigate, which adds to their workload.



Threat Indicators

This page shows the threat indicators that operators created in Cofense Triage or that came from an API. Tell me more

Created At (EDT) ▼	Threat Level	Threat Type	Threat Value	Owner	Threat Source
Yesterday Jul 15, 2021 at 06:44:02 EDT	Suspicious	Hostname	test3.com	Application: XSOAR_CDS_SU	XSOAR-UI
Yesterday Jul 15, 2021 at 06:39:46 EDT	Malicious	Hostname	test1.com	Application: XSOAR_CDS_OP	XSOAR-UI
Jul 6, 2021 at 22:52:43 EDT	Malicious	Header	Subject:NEW TAG_Additional field	Application: RelTestDemos	XSOAR-UI
Jul 6, 2021 at 22:51:02 EDT	Malicious	Header	Subject:Suspicious URL	Application: RelTestDemos	XSOAR-UI

Solution: While responding to a phishing attack, analysts can query Cofense Triage from within Cortex XSOAR for details about phishing rules matched, reporter reputation, and categorized phishing threats such as crimeware and advanced threats with optional tags. These indicators can be used for next step actions, such as remediation at the endpoint or network level based on the severity and attack payload method. Cofense Triage analyzes and highlights which emails require remediation, transferring information to Cortex XSOAR, which contains automated playbooks to find threats elsewhere in the enterprise.

Benefit: By leveraging Cofense Triage v2 API, analysts will receive common indicators and context across phishing attacks in a campaign, allowing them to link incoming incidents accordingly for a faster, more efficient, and scalable response. These associations exist in posterity, building acknowledge repository so that analysts can learn from and respond better to future attacks. Furthermore, Cortex XSOAR and Cofense Triage have bidirectional communication, allowing for XSOAR identified indicators to appear directly in Cofense Triage, matching and responding to the evolving threat landscape.

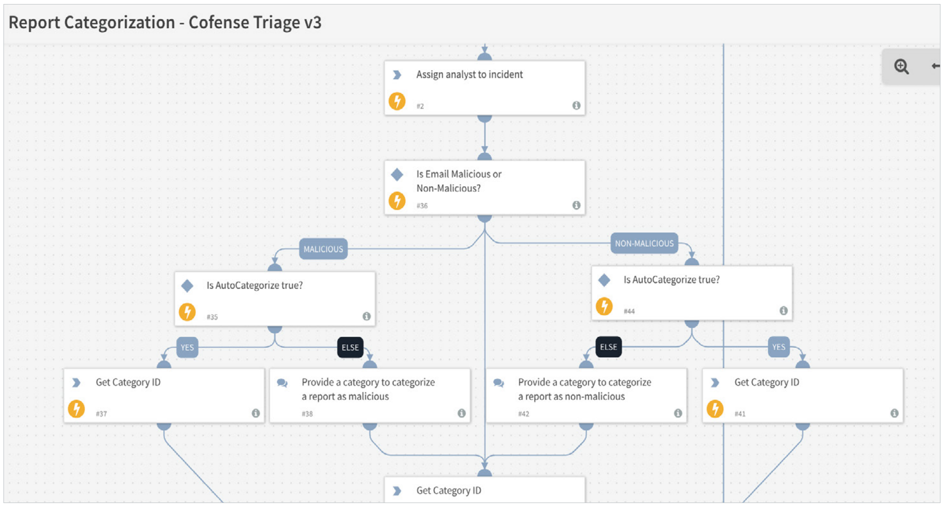
2 Use Case #2

Bidirectional Phishing Analysis, Enrichment, and Responsel

Challenge: Employees have been conditioned to report suspicious emails. This can generate many emails that your security team needs to manually analyze and respond to. Reported emails left unprocessed and waiting for analyst review can delay necessary action needed to respond to real phishing threats. Time is critical to thwart an attack.

Solution: Cofense Triage v2 API allows for bidirectional communication between platforms. Configure Cortex XSOAR to ingest from Cofense Triage's inbox, reconnaissance, and processed locations. Additional criteria can be compiled to better identify incidents that match specific phishing attack conditions. Incidents created in Cortex XSOAR run playbooks calling dozens of commands and arguments to automatically analyze, enrich, and respond. Extracted indicators can be written back into Cofense Triage and employee provided phishing reports can be categorized for easier investigation.

Benefit: Reported emails are processed and playbooks can take additional action within both Cofense Triage and Cortex XSOAR. Cofense Triage and Cortex XSOAR use bidirectional APIs ensuring emails are analyzed timely and phishing attributes are for analysts to act and fill holes where other technologies have failed and employees helped make a difference.

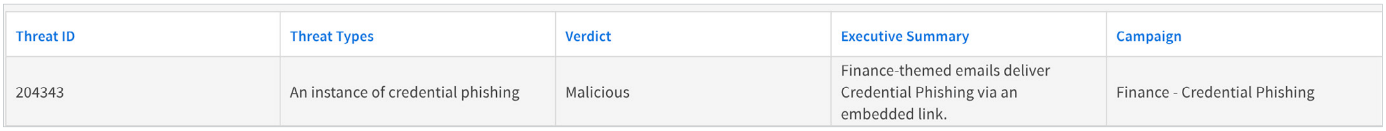

Report Categorization - Cofense Triage v3
Assign analyst to incident
#2
Is Email Malicious or Non-Malicious?
#36
MALICIOUS
NON-MALICIOUS
Is AutoCategorize true?
#35
Is AutoCategorize true?
#44
YES
ELSE
ELSE
YES
Get Category ID
#37
Provide a category to categorize a report as malicious
#38
Provide a category to categorize a report as non-malicious
#42
Get Category ID
#41
Get Category ID

3 Use Case #3

Actionable Phishing Intelligence Incident Response

Challenge: There is often a mismatch between the high-volume nature of phishing attacks and analyst agility in responding to them. For analysts, phishing attack identification, triage, reputation checks, and response usually involves switching between multiple screens and repeated manual tasks.

Solution: Analysts can map phishing attack categories from Cofense Intelligence to specific Cortex XSOAR playbooks that automate repeatable tasks such as indicator collection, reputation checks, and mail communication with affected parties. The phishing response playbook will trigger and execute automatically on receipt of a phishing attack investigation.



Threat ID	Threat Types	Verdict	Executive Summary	Campaign
204343	An instance of credential phishing	Malicious	Finance-themed emails deliver Credential Phishing via an embedded link.	Finance - Credential Phishing

Challenge: Playbooks can provide standardized response procedures and post-response documentation, helping analysts bypass repeatable manual steps and giving them access to scalable, comprehensive reports based on a rich pool of indicators and investigation actions that are common across incidents.

About Cortex XSOAR

Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the inciden lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https:// www.paloaltonetworks.com/cortex/xsoar.

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 32 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