Automated Phishing Threat Analysis and Incident Remediation

CORTEX XSOAR BY PALO ALTO NETWORKS | COFENSE

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 are all sources of stress. 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 risk. 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 indicators of phishing and human-verified phishing intelligence in automated and/or manual playbooks for the incident response team to mitigate and eliminate the attack.

Run thousands of commands (including for Cofense alerts) interactively via a ChatOps interface while 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

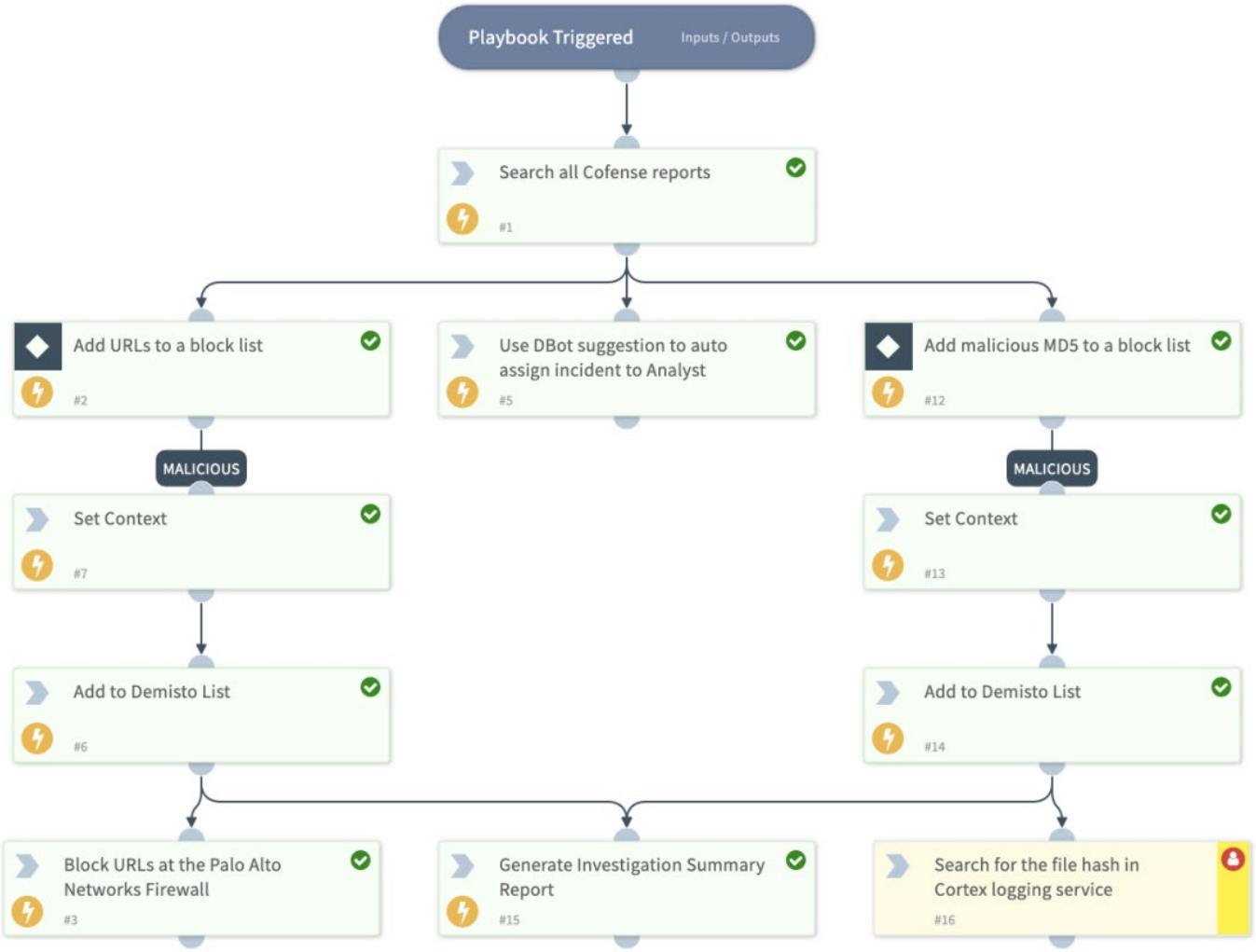
Products: Products: Cortex XSOAR, Cofense Triage™ and Cofense Intelligence™

Use Case #1
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: Using rule-sets, 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.

paloalto NETWORKS

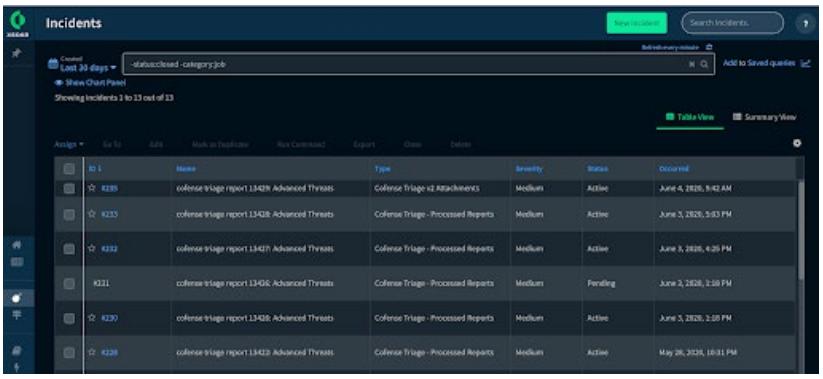


Benefit: Playbooks can provide standardized response procedures and post-response documentation, helping analysts bypass repeatable manual steps and giving them access to scalable, comprehensive reports based on a rich pool of indicators and investigation actions that are common across incidents.

Use Case #2
Remediate Phish Evading Secure Email Gateways

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

Solution: While responding to a particular phishing attack, analysts can query Cofense Triage and Intelligence from within Cortex XSOAR for details about categorized phishing threats such as crimeware and advanced threats. These indicators can be used for next step actions, such as remediating at the endpoint or network level based on the severity and attack payload method. Cofense Triage analyzes and highlights which emails require remediation and Cortex XSOAR can run through a series of steps to find threats elsewhere in the enterprise.



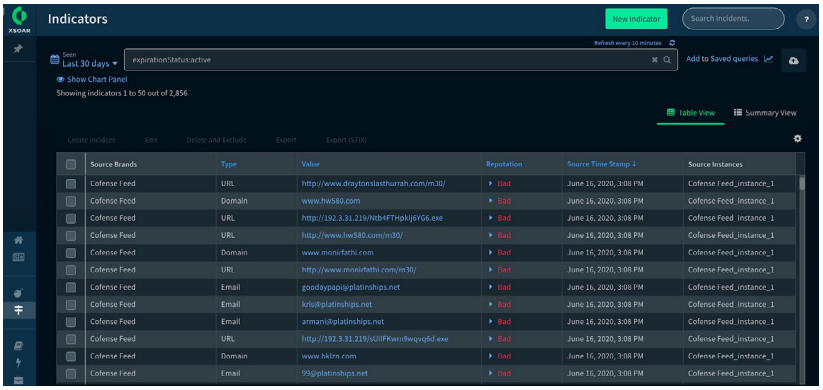
Benefit: By leveraging common indicators and context across phishing attacks in a campaign, analysts can link incoming incidents accordingly for a more efficient, speedy, and scalable response. These linkages exist in posterity, building a knowledge repository for analysts to learn from and respond better to future attacks.

Use Case #3

Reputable, Timely, And Actionable Threat Intelligence

Challenge: Organizations have multiple sources of threat intelligence that vary in reputation, timeliness, accuracy, and actionability. Too many sources of intelligence lack the context to help analysts make faster phishing incident response decisions.

Solution: Cofense Intelligence is timely, relevant, actionable and reliable. Cofense Intelligence is human-verified and integrates into Cortex XSOAR threat intel management. Analysts ingest highly reputable intelligence and prioritize workflow based on the content and context associated with indicators.



Benefit: The indicators have threat severity level designations on URLs, domains, files, and IPs so that security teams can conduct threat lookups or run them through playbooks to add to network and endpoint technologies. Human-vetted phishing intelligence removes the guesswork and lack of credibility often associated with sources of threat intelligence. Security analysts now have confidence in decisions they make and can do it quickly and through automation.

About Cofense

Cofense®, the leading provider of intelligent phishing defense solutions worldwide, is uniting humanity against phishing. The Cofense suite of products combines timely attack intelligence on phishing threats that have evaded perimeter controls and were reported by employees, with best-in-class security operations technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com

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 incident 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.