SOLUTION BRIEF

Cofense Triage Integration Brief

Cofense Triage™ and Trellix Helix

Operationalize Phishing Threat Reports and Indicators for Investigation, Response, and Resiliency

Cofense® and Trellix integrate for visibility into one of the biggest cyber security risks — phishing. With many of today's data breaches starting with phishing, security teams require insight into adversary tactics that can be operationalized to alert and respond to phishing threats.

Cofense Triage™ gives incident responders the ability to act on phishing alerts quickly by automating threat investigation and response. SOC teams can focus on interpreting results and responding to phishing threats effectively. With Cofense Triage's 2nd version API, dozens of endpoints retrieve valuable phishing data to provide security teams with the ability to correlate other data points and view the risk to the company.

Cofense Triage

Mutual customers of Cofense and Trellix Helix can integrate in minutes. By utilizing Trellix Helix connect, customers can choose the Cofense tile and start ingesting data from multiple endpoints.

Quickly index and view attributes from phishing threats reported by employees.

Phishing attributes from Cofense Triage's reports mailbox locations along with threat indicators.

Trellix Helix

Gain greater visibility into alerts and events coming in from Cofense and other Trellix products and other 3rd party data in one single console.

Integrate your existing security tools and connect with over 450 Trellix solutions and third-party products in one location.

Identify threats and prioritize critical alerts with contextual intelligence.

Take control of incidents from detection to response.

High fidelity intelligence about phishing, malware, and targeted employees generated from Cofense and quickly displayed.

Solution

Security teams condition employees to recognize and report suspicious emails bypassing secure email gateway (SEG) technology. Employees report emails that are suspect using Cofense Reporter™, with one-click ease of use reporting. Cofense Triage is a purpose-built phishing analysis and response solution that ingests reported emails, analyzes, and highlights which emails are a threat and which are benign – saving time.

Cofense Triage is enriched with Cofense's lab and research team intelligence which is uncovering advanced global phishing threats. Security analysts gain insight into phishing URLs, IPs, domains, files, command and control (C2), payload, and exfiltration sites. Security teams are much more confident in the action they take based on thorough indicator report analysis. Lastly, responding to reporters about the reported email, completes the feedback loop to encourage future reporting about suspicious emails. Security teams can defend the enterprise against the number one threat vector facing companies today – phishing.

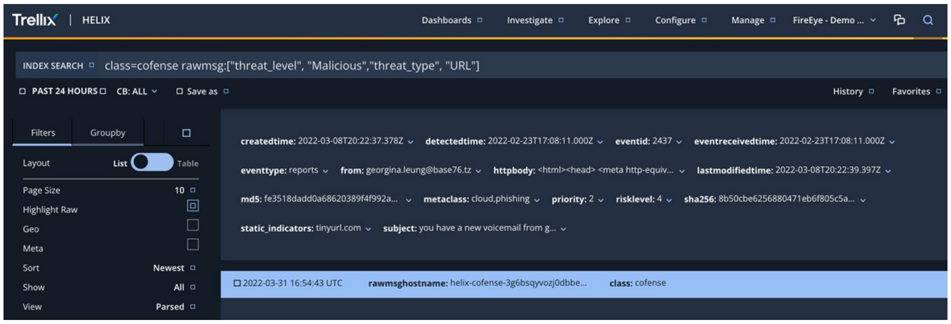
How it Works

Cofense's application in Trellix Helix enables a seamless integration connecting from Helix into Cofense Triage to get phishing reports and threat indicators. Once configured, Helix will poll Cofense Triage and ingest useful phishing data that can then be used in detection and response as well as providing threat hunting teams with useful reports and indicators to piece together events. Phishing data from Cofense is a valuable asset within Helix when it comes to correlating global events which may have started with phishing. Data ingested includes:

Senders	Report body
Subjects	Risk level
Threat indicators	Attachments
URLs	Rule priority
Threat level	Threat type

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at https://trellix.com.



INDEX SEARCH class=cofense rawmsg:["threat_level", "Malicious","threat_type", "URL"]

□ PAST 24 HOURS □ CB: ALL □ Save as

Layout List Table
Page Size 10
Highlight Raw ☑
Geo □
Meta □
Sort Newest
Show All
View Parsed

createdtime: 2022-03-08T20:22:37.378Z detectedtime: 2022-02-23T17:08:11.000Z eventid: 2437 eventreceivedtime: 2022-02-23T17:08:11.000Z
eventtype: reports from: georgina.leung@base76.tz httpbody: <html><head> <meta http-equiv... lastmodifiedtime: 2022-03-08T20:22:39.397Z
md5: fe3518dadd0a68620389f4f992a... metaclass: cloud,phishing priority: 2 risklevel: 4 sha256: 8b50cbe6256880471eb6f805c5a...
static_indicators: tinyurl.com subject: you have a new voicemail from g...

□ 2022-03-31 16:54:43 UTC rawmsghostname: helix-cofense-3g6bsqyvozj0dbbe... class: cofense

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.