ANOMALI

COFENSE

Phishing Threats Evolve and Your SOC Needs Visibility Into Phishing IOCs Evading Layers of Defense

Detect and respond to phishing threats reported by employees, with Anomali and Cofense Triage™.

ANOMALI AND COFENSE® JOINT SOLUTION FEATURES:

- Phishing IOCs: URLs, hostnames, email senders, email subjects, and malware file hash values, designated with severity ratings, ingested into ThreatStream.
- Analyst-vetted phishing indicator designations correlating to high-actionable phishing threat intelligence.
- Severity and confidence score mapping and tags of Cofense IOCs.
- Operationalize phishing IOCs across technology stack to disrupt active phishing attacks.

IMMEDIATE TIME TO VALUE

- Detect and respond to phishing threats from IOCs obtained through analyst vetting.
- Integrates with customer-managed or Cofense-managed Phishing Defense Center (PDC).
- Actionable phishing intelligence and visibility into threats evading email gateways.
- Enable integration within a few minutes.

STOP ACTIVE PHISHING ATTACKS WITH EMPLOYEE-REPORTED, ANALYST-VETTED PHISHING INTELLIGENCE

Attackers use a variety of tactics to evade secure email gateways and other security defenses. Credential phishing is the predominate favorite of attackers to gain access and move throughout systems, while conversation-style emails, Business Email Compromise (BEC), relentlessly target recipients which may lead to a loss of funds or disclosure of sensitive documents. However, conditioned employees are an asset, not a liability, when they recognize suspicious emails that have evaded defenses, and report them to the SOC for analysis.

Credible Phishing Indicators

Analyst vetting means confidence in quality and no false positives.

Targeted Phishing Campaigns

IOCs specific to the customer and not a generic feed.

Strengthen Defenses

Operationalize with IOCs to stop current, and similar attacks.

PHISHING IOCS IN DISPARATE SYSTEMS

CHALLENGE

A healthcare customer using Cofense's Phishing Defense Center (PDC) receives escalation tickets from Cofense when phishing threats are reported and found in employee email accounts. The escalation tickets consist of phishing indicators existing in the email as well as secondary indicators, such as redirects, payload sites, and command and control infrastructure. The customer wanted an automated way to ingest indicators into ThreatStream and remove the manual process.

SOLUTION

ThreatStream queries Cofense Triage's phishing threat indicators endpoint to ingest URLs, hostnames, email sender, email subject, and hash values associated with credible phishing campaigns. Each indicator contains a malicious or suspicious severity rating along with confidence scoring.

CUSTOMER BENEFIT

Customers automate the ingestion of credible phishing indicators for action in disrupting an active phishing attack before it leads to a breach.

OPERATIONALIZE PHISHING INDICATORS

CHALLENGE

A global company in the energy sector was unable to automate phishing indicators into their technology stack. The tier 1 SOC was able to identify and designate phishing threats, but it required another manual process before being able to bolster defenses in other systems. Email and web gateways, firewalls, and endpoints were not being updated with credible phishing indicators.

SOLUTION

Using the API integration with Cofense Triage, the customer ingests indicators and automates with ThreatStream across the technology stack. Network and endpoint solutions consume phishing indicators identified by Cofense Triage and automated with Anomali ThreatStream.

CUSTOMER BENEFIT

Customers devote time to other tasks and eliminate manual processes and potential for human error while updating other security solutions.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI