Cofense Integration Brief

Cofense Triage™ Intelligence™ and Cyware CTIX and CSOL

Cofense delivers comprehensive human phishing defense solutions focused on fortifying employees – your last line of defense -- after a phishing attack evades your other technology. Cofense enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks. Armed with Cofense Triage ™ and Cofense Intelligence™, organizations leverage a combination of employee-reported phish bypassing secure email gateways and 100% human-verified phishing threat intelligence. Both sources of intelligence enrich automation, orchestration and response.

Cyware solutions enable organizations to develop proactive cyber defense capabilities, effectively exchange strategic, tactical, and operational threat intelligence, and quickly respond to and manage security threats in real-time. Cyware combines separate but integrated solutions including CTIX, an advanced threat intelligence platform (TIP) and CSOL, a vendor-agnostic security automation (SOAR) platform..

Cyware solutions leverage advanced automation capabilities to speed up the threat intelligence lifecycle and orchestrate response actions to help security teams stay ahead of threats..

Phishing investigation and incident response is reduced from minutes down to seconds with Cofense and Cyware. Analysts operationalize results that allow security teams to close gaps and disrupt attackers. Cofense and Cyware improve efficiency and standardize processes that can be automated. Security leaders can ensure routine, repetitive tasks are achieved consistently and efficiently, freeing up valuable analyst time that can be devoted to more complex and advanced responsibilities.

When combined, Cofense Triage, Cofense Intelligence and Cyware offer security teams the ability to harness the power of credible employee-reported and human-verified phishing intelligence. Cofense Triage ingests and analyzes employee-reported phishing emails bypassing secure email gateways. Analysts using the Cyware Security Orchestration Layer (CSOL) can directly ingest phishing indicators using Cofense Triage's API. Cofense Intelligence human-verified indicators are a valuable source of intelligence that analysts can use in the Cyware Threat Intelligence eXchange (CTIX) platform to investigate incidents and conduct threat hunting. Analysts have unobstructed views into credible phishing threats leading to higher confidence in the action taken based on the indicator results returned to the platform.

Cofense Triage and Cofense Intelligence

- Employee-reported phishing analysis by Cofense Triage from emails bypassing secure email gateways
- High fidelity intelligence about phishing, malware, and botnet infrastructure collected by Cofense analysts
- Human-verified timely and contextual phishing machine-readable threat intelligence

Phishing Automation and Orchestration

- Incident Response automation initiated by verified phishing threats accelerates resolution times
- Playbook-enabled investigation of phishing threats empower analysts to work more efficiently
- Automatically ingesting or querying phishing indicators enriches incident analysis and response
- Playbook execution determined by phishing indicator impact ratings facilitates decisions

IR Team Challenges

Attackers Evading Technical Controls

As technology evolves to defend against threats, the attackers' creativity enables them to find ways into the employees' inbox hoping they will open the attachment or click the link. This can be thwarted through credible and trustworthy phishing intelligence applied to network policies based on threat severity.

Actionable Intelligence

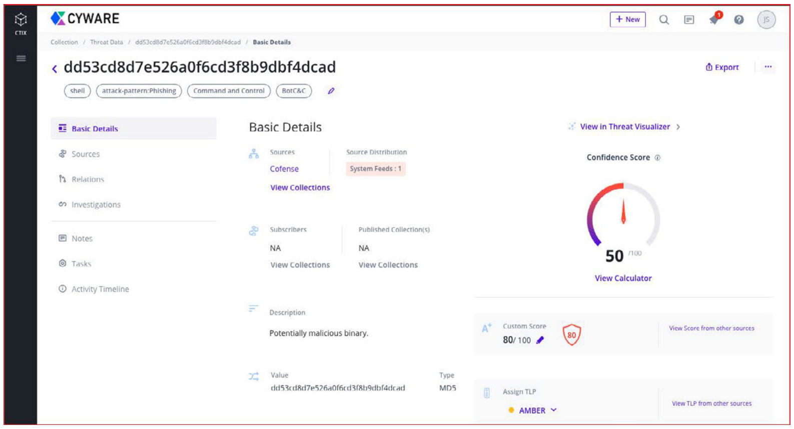
Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real- time correlation, prioritization, and automation of security events with the confidence to act is critical when seconds matter in mitigating threats.

Alert Fatigue

Too many threat intelligence feeds are full of false positives that distract security analysts. Excessive alerts only exasperate overwhelmed analysts with a finite amount of time.

How it Works

Cofense Triage automatically analyzes employee- reported phishing emails and Cyware CSOL can ingest IOCs via JSON for next step actions. Cofense Intelligence provides analysts with high fidelity phishing indicators in the Cyware CTIX platform that they can investigate, validate, and orchestrate impact ratings from phishing specific formatted, MRTI. Analysts can prioritize and decisively respond to indicators retrieved from Cofense and Cyware solutions.



Collection / Threat Data / dd53cd8d7e526a0f6cd3f8b9dbf4dcad / Basic Details

dd53cd8d7e526a0f6cd3f8b9dbf4dcad

shell | attack-pattern:Phishing | Command and Control | BotC&C

Basic Details

Sources: Cofense
Source Distribution: System Feeds : 1

Subscribers: NA
Published Collection(s): NA

Confidence Score: 50 /100

Description: Potentially malicious binary.

Custom Score: 80/ 100

Value: dd53cd8d7e526a0f6cd3f8b9dbf4dcad
Type: MD5

Assign TLP: AMBER

Cofense Triage provides rules and intelligence from Cofense security researchers. When reported emails match Cofense or analyst-written rules, malicious emails are highlighted, while benign are eliminated. With available APIs, Cofense Triage provides Cyware CSOL with ingestible phishing indicators for use in next step playbooks.

Cofense Intelligence provides rich contextual human- readable reports to security teams, allowing for in-depth insight into the criminal infrastructure. Analysts and security leaders will have visibility into email message contents, malware artifacts with full threat detai l, and executive summaries to easily understand the threat actor's TTP operation and the risk to the business from the following types of indicators:

- Payload URLs and Exfiltration Sites
- Command and Control Servers
- Malicious IP Addresses
- Compromised Domains

About Cyware

Cyware offers the technology organizations need to build a virtual cyber fusion center. With separate but integrated solutions including an advanced threat intel platform (TIP), vendor-agnostic security automation (SOAR), and security case management, organizations are able to increase speed and accuracy while reducing costs and analyst burn out. Cyware's virtual cyber fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies of all sizes and needs. To learn more about Cyware, visit cyware.com.

CYWARE

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 30 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.

COFENSE

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175