Cofense Integration Brief

Cofense Intelligence™ and MISP

Operationalize Phishing Intelligence for Threat Defense & Response

Cofense delivers a comprehensive human phishing defense platform focused on fortifying employees – your last line of defense after a phish evades your other technology – and enabling incident response teams to better identify, verify and respond to targeted phishing attacks.

Cofense PhishMe™ and Cofense Reporter™ turn employees into informants through active engagement by simulating real-world phishing attempts, providing on-the- spot education (when needed) and easing the reporting of suspicious emails to security teams. Cofense Triage™ enables IT security teams to automate and optimize phishing incident response by allowing them to prioritize reported threats. Cofense Intelligence™ provides security teams with 100% human-verified phishing threat intelligence.

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. It combines a searchable repository with a multidirectional information sharing mechanism. Where possible, MISP also provides automation mechanisms that enable the automatic import and export of data and the interfacing with other systems. The aim is to speed up the detection of incidents and the production of defense countermeasures, especially for malware that is not blocked by anti-virus protection, or that is part of sophisticated targeted intrusion attempts.

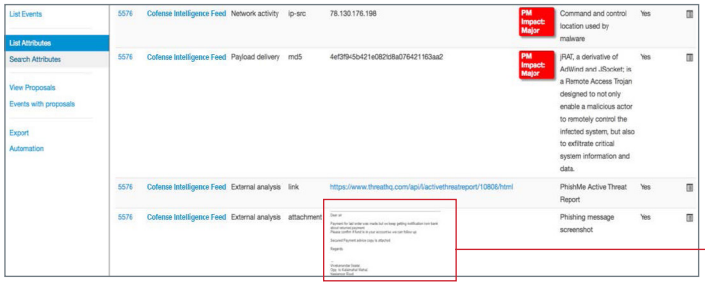
The Cofense Intelligence MISP feed provides a way to ingest file and network phishing indicators. Analysts are then able to correlate Cofense Intelligence with other intelligence feeds as well as understand the malware tactics from the indicators received.

Phishing Intelligence

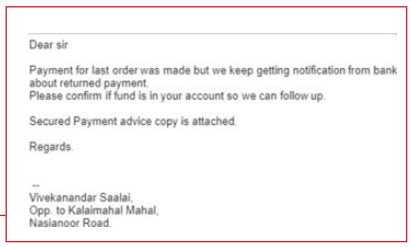
- Human-vetted phishing intelligence delivered as MRTI
- High fidelity intelligence about phishing, malware, and botnet infrastructure
- Human-readable reports to understand attacker TTPs

Correlation and Actionable Decisions

- Aggregate multiple threat intelligence services to take action based on pre-defined policies
- Operationalize trustworthy phishing intelligence
- Ensure the most reliable and relevantdata is assessed with ingested phishing indicators
- Gain real-time phishing threat visibility



(Cofense Intelligence Network and File Indicators Ingested into MISP Platform)



(Phishing Message Screenshot)

IR Team Challenges

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.

Actionable Intelligence

Security teams are hesitant to trust their sources of intelligence for fear of disrupting the business. Real-time correlation and prioritization of security events and the critical when seconds matter in blocking the threat.

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 intelligence applied to network policies based on threat severity.

Working Together

Cofense Intelligence into the MISP platform deliverthe ability to aggregate, correlate, prioritize and operationalize phishing-specific machine-readable threat intelligence (MRTI). Using high fidelity phishing intelligence, analysts can decisively respond to alerts from intelligence consumed via Cofense's API. With MISP, security teams can act based on Cofense Intelligence indicators through their existing infrastructure to alert or block ingress and egress traffic.

Cofense Intelligence uses easy-to-identify impact ratings of Major, Moderate, Minor, and None, for teams to create rules based on the level of impact. When MISP receives these indicators security teams can define steps to operationalize threat intelligence.

Cofense Intelligence also provides rich contextual humanreadable reports to security teams, allowing for in-depth insight into the criminal infrastructure. Analysts and security leaders gain visibility into email message contents, malware artifacts with full threat detail, and executive summaries, to easily understand the threat actor's TTP operation and risk to the business. These reports are available from Cofense's threat portal.

Cofense Intelligence ingested by MISP provides rich insight for assertive action from the following types of indicators:

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

In addition, Cofense provides access to the Active Threat Report and full threat detail for the above correlated event.

With this formidable combination, security teams can respond quickly and with confidence to mitigate identified threats. Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions based on security policies for ingress and egress traffic.

About MISP-Project

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

MISP Threat Sharing

COFENSE

W: cofense.com/contact **T:** 703.652.0717

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