Cofense™ Integration Brief

COFENSE INTELLIGENCE AND DEMISTO ENTERPRISE

Delivering Powerful Phishing Threat Defense & Response

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 Intelligence™, organizations can leverage 100% human- verified phishing threat intelligence capable of complementing automation and orchestration platforms.

Demisto Enterprise helps analysts with incident management, security orchestration, and interactive investigation. Demisto Enterprise delivers a complete solution to help Tier-1 through Tier-3 analysts and SOC managers to optimize the entire incident lifecycle while auto-documenting and journaling the evidence. As a result, security teams improve response times, reduce risk exposure, and maintain process consistency across the enterprise security program. Demisto Enterprise unifies disparate technologies and incident handling processes into a single console to deliver real-time guided responses. With dedicated processes in place, Demisto Enterprise is the catalyst to the investigation and incident response workflow in the security operation.

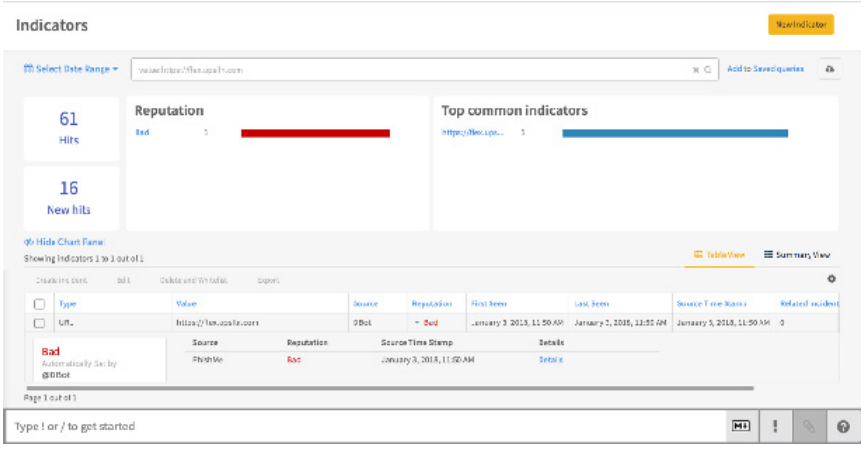
Phishing Intelligence

- ✓ Human-verified timely and contextual phishing (machine-readable threat intelligence) MRTI with no false positives
- ✓ High fidelity intelligence about phishing, malware, and botnet infrastructure
- ✓ Human-readable reports with context behind threat actor infrastructure to understand attacker tactics

Phishing Automation and Orchestration

- ✓ Automation driven from verified phishing threats with impact ratings for actionable decisions
- ✓ Investigation of phishing threats empower analysts and work more efficiently
- ✓ Ingest or query phishing indicators ensures the most reliable and relevant data is assessed
- ✓ Playbook execution determined by phishing indicator impact ratings makes for easier decisions

Demisto Enterprise speeds phishing investigation and incident response and removes a lot of the routine and mundane tasks conducted by security teams. Through the platform versatility and the integration with Cofense Intelligence, analysts conclude results that allow security teams to close gaps and disrupt attackers. With Cofense Intelligence and Demisto Enterprise, security leaders can confirm that routine, repetitive phishing investigation and response tasks are achieved consistently and efficiently freeing up valuable analyst time that can be devoted to more complex and advanced responsibilities.



(Cofense Intelligence URL in Demisto Enterprise)

With Cofense Intelligence security teams harness the power to leverage credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API and Demisto Enterprise enables analysts to validate incidents and their potential impact to the business. Analysts have unobstructed views into credible phishing threats leading to higher confidence in the action taken based on the indicator results and verdict mapping returned to the platform.

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 Intelligence and Demisto Enterprise deliver the ability to investigate, validate, and automate actions based on indicator impact ratings from phishing-specific MRTI. Using high fidelity phishing intelligence means that analysts can prioritize and decisively respond to alerts from intelligence consumed via Cofense's API. With Demisto Enterprise, security teams can operationalize Cofense Intelligence indicators through War Room search actions for URLs, IPs, domains, and files.

Cofense Intelligence human-readable reports are linked from within Cb Response to provide analysts with IOC context. This context is the additional insight for security teams to understand the criminal infrastructure and support remediation decisions. Analysts and security leaders will have visibility into email message contents, malware artifacts with full threat detail, and executive summaries to easily understand the threat actor's operation and the risk to the business.

The combination of Cofense Intelligence and Demisto Enterprise provides rich insight for assertive action from the following types of indicators:

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

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 that are automated and orchestrated across the infrastructure.

About Demisto Enterprise

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com

DEMISTO

Cofense is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today's top attack vector — spear phishing. Cofense's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that Cofense integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process. Cofense's customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

COFENSE

W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175