# Cofense Integration Brief

## Cofense Intelligence™ and ThreatConnect

### Delivering Powerful Phishing 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.

ThreatConnect® customers use the platform to unite people, processes, and technologies behind a cohesive, intelligence-driven defense against threats to their business. Using the ThreatConnect threat intelligence platform, you can simultaneously work across your cybersecurity teams and functions with your trusted communities. Whether you have a mature program or are just getting started, you are ready to start using ThreatConnect to make faster, data-driven security decisions.

### Phishing Intelligence

- Relevant, fresh, and contextual MRTI with no false positives
- botnet infrastructure
- Human-readable reports to understand attacker TTPs

### Correlation and Actionable Decisions

- Aggregate multiple threat intelligence services to take action based on pr policies
- Operationalize trustworthy phishing intelligence
- Ingested phishing indicators ensures the most reliable and relevant data is assessed
- Real-time phishing threat visibility

Collectively with Cofense Intelligence and ThreatConnect, security teams have unobstructed views into credible phishing threats leading to higher confidence in the action take based on the indicators.

**CONDITION EMPLOYEES**
To Recognize and Report Threats


**SPEED INCIDENT RESPONSE**
Collect, Analyze, and Respond to Verified Active Threats

# 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 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 and prioritization of security events and the critical when seconds matter in blocking the threat.

### 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 ThreatConnect deliver the ability to acquire, aggregate and take action from phishing-specific machine-readable threat intelligence (MRTI). Using high fidelity phishing intelligence means that analysts can prioritize and decisively respond to alerts from intelligence consumed via Cofense's API. With ThreatConnect, security teams are able to take action based on Cofense Intelligence indicators through their existing infrastructure to alert or block ingress or 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 these indicators are received by ThreatConnect, steps can be defined to operationalize threat intelligence.

Furthermore, 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 detail, and executive summaries, to easily understand the threat actor's TTP operation and risk to the business.

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

- Payload URLs and Exfiltrations Sites
- Command and Control Servers
- Malicious file and 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 threats. Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisons based on security policies for ingress and egress traffic.

### About ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com.

ThreatConnect™

### 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