



# Cofense Integration Brief

## Cofense Intelligence™ and Anomali ThreatStream

### 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.

ThreatStream, the Anomali threat intelligence platform, makes sense of all of the threat data that security teams have to sort through to find the needle(s) in the haystack that can threaten your business, customers, intellectual property, and reputation.

ThreatStream also enables users to more easily share threat intelligence by supporting trusted community creation, collaboration and analysis. With the press of a button, ThreatStream users can share threat intelligence in real-time with trusted peers or within any circles of trust they've created. With the collaboration capabilities of ThreatStream, users are essentially taking advantage of an 'early warning system' that enables them to anticipate and protect themselves from attack.



### Phishing Intelligence

- Relevant, fresh, and contextual MRTI with no false positives
- 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
- Ingested phishing indicators ensures the most reliable and relevant data is assessed
- Real-time phishing threat visibility

Collectively with Cofense Intelligence and Anomali, 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



## 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.

### How it Works

Cofense Intelligence and Anomali ThreatStream 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 Anomali, 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 Anomali, 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 ThreatStream 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 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 Anomali

Anomali™ is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations.

[www.anomali.com](http://www.anomali.com)

ANOMALI™

### 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 32 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](http://www.cofense.com) or connect with us on [Twitter](#) and [LinkedIn](#).



W: [cofense.com/contact](http://cofense.com/contact) T: 703.652.0717

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