



Cofense Integration Brief

Cofense Triage and Hatching

Analyze and Automate Phishing Threat Defense & Response

Cofense delivers comprehensive human phishing – your last line of defense after a phishing attack evades your other technology. With Cofense Triage, SOC teams have the solution to analyze and automate employee-reported phishing emails that bypass secure email gateways (SEGs). Cofense enables incident response and SOC teams to better identify, verify, and respond to targeted phishing attacks.

Hatching™ offers a malware sandbox solution, Hatching Triage, capable of analyzing upwards of 500,000 submissions per day. Over 100 file types are capable of being analyzed to help security teams in their decision making and response to suspicious files. Upon analysis, Hatching produces relevant and timely report information that provides analysts with deep visibility into suspicious files and URLs.

Integration Results

<https://www.cf-dem0-2022.com/demo.html>

Hatching • Created Today Mar 3, 2022 at 15:33:04 EST

Triage Info

```
"https://priv[redacted].ge/2203[redacted];qvmw"
```

Cofense Triage Integration Results

Phishing Detection and Response

- Benefit from employees detecting phishing threats and arming SOC and IR teams with phishing indicators
- Ingest and analyze of suspicious emails bypassing secure email gateways (SEGs)
- Review in-depth malware and malicious site tactics after analysis.
- Prioritize email threats, removing benign emails from distracting SOC teams

With Cofense Triage and Hatching, security teams can detect and respond to phish based on analysis of reported attachments and URLs. Analysts use the indicators to respond to the attack before a breach occurs. Malware and malicious site tactics are highlighted and can be used for additional threat hunting across the organization. Security teams will view phishing tactics reported by employees and respond to the reporter to encourage future behavior and leveraging the power of people.

Hatching Configuration

Enabled	<input checked="" type="checkbox"/>
Host	example.com
API Port	443
API Key	0123456789abcde987654321
Use SSL	<input checked="" type="checkbox"/>
Verify SSL	<input checked="" type="checkbox"/>
Max Number of Concurrent Submissions	
Enable Data Expiration	<input checked="" type="checkbox"/>
Data expiration	30 Days
Enable Risk Scoring	<input checked="" type="checkbox"/>

Cofense Triage - Configuration for Hatching

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](#).



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

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