Identify and respond to phishing threats faster with Cofense Triage, Intelligence, and ServiceNow

The Challenge
One of the most common and effective ways to breach an organization is to send unsuspecting employees phishing emails that look legitimate. These messages attempt to trick an employee to click a link to a hostile website, or open a malicious attachment, providing an opening for malware, or possibly giving away authentication credentials.

Organizations can empower employees to recognize and report phishing threats, making them a vital part of phishing defense. These employee-reported emails need quick analysis to determine malicious versus benign reports. Furthermore, the analysis cannot consume a security analyst’s already extremely limited time.

Cofense Triage™, the first phishing-specific security orchestration, automation, and response (SOAR) platform, helps stop active phishing attacks in progress. By leveraging real-time, internally reported attack intelligence from conditioned users, Cofense Triage makes it easy to stop phishing attacks in progress by eliminating the noise of the abuse mailbox, automating standard responses, and orchestrating across other security systems to quickly respond to and eliminate phishing threats.

Cofense Intelligence™ delivers human-verified, phishing-specific threat intelligence as both long-form reports and machine-readable threat intelligence. It aids security analysts by delivering timely phishing intelligence indicators and contextual reports to make critical decisions based on threat severity. Cofense Intelligence is designed for analysts to consume and make accurate decisions.

Cofense™ has partnered with ServiceNow to respond to phishing-based security threats faster. Once a threat has been identified, an analyst can produce actionable intelligence with context and send the alert to ServiceNow® Security Operations. A new security incident is created within Security Operations, where workflows can automatically gather additional threat intelligence and assign the incident for remediation. Moreover, with phishing intelligence, analysts can conduct threat lookups to help with incident response and threat mitigation.

Cofense Triage use case example
Here’s how the phishing incident workflow can be automated using Cofense Triage and ServiceNow Security Operations. Cofense Triage receives and clusters together similar reported emails and highlights phishing indicators and severity.

Cofense Triage key benefits:
• Automate and accelerate phishing incident response through an integrated workflow
• Reduce routine, manual workload so analysts can spend time on other priorities
• Streamline threat analysis and security response through integrated platforms

Cofense Intelligence key benefits:
• Human-verified phishing intelligence provides accurate incident context
• Prioritize security incidents with phishing threat lookup indicator severity ratings
• Make better security decisions with contextual reports of phishing campaign tactics and associated IoCs
Figure 1–Cofense Triage automatically clusters reported phishing emails and provides the analyst with a summary view for actionable response.

Next, Triage will automatically analyze the emails and identify indicators of phishing, including reporter reputation, YARA rule matching, and intelligence plus integration analysis. The phishing indicators are then included in the notification template and sent to Security Operations to create a security incident. Triage analysts can control which of these indicators are included in the new security incident to assist the next responder.

Figure 2–Cofense Triage notification template populated with indicators of phishing to create a security incident in ServiceNow Security Operations.
Once the security incident has been created containing Indicators of Compromise (IoCs) identified by Cofense Triage, Security Operations can then use workflows to prioritize and assign the incident, providing the responder all the information needed to quickly remediate. Once the incident is closed, a post-incident review is automatically generated that contains a time-stamped record of response activities.

Cofense Triage includes customizable templates for use with Security Operations to analyze attachments, identify phishing recipients, and perform additional actions on phishing indicators.

**Cofense Intelligence use case example**

Cofense Intelligence can also be used with ServiceNow Security Operations. Cofense Intelligence is used as a phishing threat lookup service by Security Operations. As security incidents are created in Security Operations, analysts can investigate the incident and receive severity results to help prioritize work based on the calculated risk score. Not every indicator in an incident is malicious and Cofense Intelligence identifies which indicators are a threat and which are not. This is particularly helpful in prioritizing response and remediation. Additionally, analysts receive a short explanation of the threat with available hyperlinks to additional insight if needed.
Next, analysts can use the indicator results to assist in determining next steps. Cofense Intelligence returns the results analysts need to take-action on malicious files, URLs, domains, and IPs. Analysts and security leaders get visibility into email message content, malware artifacts with full threat detail, and executive summaries to easily understand the threat actor’s operation in addition to the risk to the business. The combination 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

With accurate intelligence from Cofense, security analysts can then use the workflow and orchestration capabilities of ServiceNow Security Operations to quickly contain and eradicate malicious emails.

![Image of Cofense Intelligence phishing report](https://www.threathq.com/p42/search/default?tm=9525)

**Figure 5**—Cofense Intelligence indicator summary in Security Operations.

<table>
<thead>
<tr>
<th>Observable</th>
<th>Integration vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>781f313154d6f29f1ccab48da6d39f</td>
<td>Cofense Threat Scanner</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Engine</th>
<th>Engine version</th>
<th>Retrieval date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cofense</td>
<td>1.0</td>
<td>2018-07-17 12:09:16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload URLs</td>
<td>Remote access trojan</td>
</tr>
<tr>
<td>Malware Artifacts</td>
<td>Remote access trojan</td>
</tr>
</tbody>
</table>

**Figure 6**—Cofense Intelligence phishing report ([www.threathq.com](https://www.threathq.com)) with additional indicators and context from hyperlink available in figure 5 example.
Summary
The collaboration between Cofense Triage, Cofense Intelligence, and ServiceNow Security Operations provides an effective end-to-end phishing incident response process. When employees are empowered to report suspicious email, security teams gain a valuable source of intelligence. Cofense Triage automates the analysis for security teams to determine the severity of the email risk. With Cofense Intelligence, security analysts are more efficient when using credible human-verified phishing intelligence. Not only can security analysts quickly determine what is a threat, but they also have access to contextual reports so that they can understand why an indicator is a threat along with the linkage between the attacker’s infrastructure. Through leveraging an established security response workflow process, security teams can automate and rapidly react to a phishing incident and disrupt attackers.

About Cofense
Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology, and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response, and reduce the risk of compromise.

About ServiceNow
ServiceNow is changing the way people work. We help the modern enterprise operate at lightspeed and be more scalable than ever before. Customers use our platform to define, structure, and automate the flow of work, removing dependencies on email, spreadsheets, and other manual processes to transform the delivery of service to the enterprise. With ServiceNow Security Operations, customers can bring incident data from their security tools into a structured enterprise security response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.