Cofense Integration Brief

COFENSE INTELLIGENCE™ AND SWIMLANE

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 leverage 100% human-verified phishing threat intelligence that is capable of complementing automation and orchestration platforms.

Swimlane's automation and orchestration platform proactively gathers evidence and quickly remediates attacks from threat actors using automated software-defined security methods. It streamlines the incident response process by collecting alert data from existing security tools, centralizing all relevant event detail, and automatically executing the correct response via highly flexible workflows and playbooks. Swimlane also increases situational awareness for security analysts by collecting and aggregating related discoveries and threat intelligence to help analysts rapidly and logically triage and resolve assigned alerts.

Phishing investigation and incident response reduces from minutes down to seconds. Through the power of Swimlane and the integration with Cofense Intelligence, analysts operationalize results that allow security teams to close gaps and disrupt attackers. Swimlane and Cofense Intelligence improve efficiency and standardize processes that can be automated. Security leaders can ensure routine, repetitive tasks are achieved consistently and efficiently, freeing up valuable analyst time that can be devoted to more complex and advanced responsibilities.

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

- ✓ Incident Response automation initiated by verified phishing threats accelerates resolution times
- ✓ Playbook-enabled investigation of phishing threats empower analysts to work more efficiently
- ✓ Automatically ingesting or querying phishing indicators enriches cases with the most relevant and reliable data
- ✓ Playbook execution determined by phishing indicator impact ratings facilitates accurate and easy decisions

When combined, Cofense Intelligence and Swimlane enables security teams to harness the power of credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API leveraged by Swimlane which enables analysts to investigate 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 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 Swimlane deliver the ability to investigate, validate, and orchestrate 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.

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 the risk to the business.

The combination of Cofense Intelligence and Swimlane 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**

Threat intelligence that is operationalized with a high degree of confidence leads to actionable decisions that are automated and orchestrated across the infrastructure.

About Swimlane

Swimlane is a leader in security orchestration and automation. The company's incident response management platform empowers organizations to manage, respond to and neutralize cyber threats with the adaptability, efficiency and speed necessary to combat today's rapidly evolving cyber threats. By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real time dashboards and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations. Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe.

SWIMLANE

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.

COFENSE

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