Cofense™ Integration Brief

Cofense Intelligence™ and SentinelOne

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 capable of supporting endpoint security platforms.

SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects and responds to attacks across all major vectors. The Endpoint Protection Platform (EPP) unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

Designed for extreme ease of use, the SentinelOne platform saves customers time by applying AI to automatically eliminate threats in real time for both on-premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint.

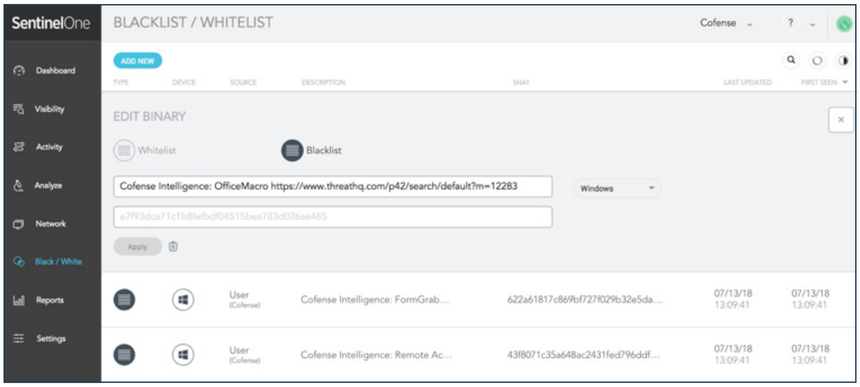
Phishing Intelligence

- ✓ Human-verified, timely and contextual phishing intelligence delivered as machine-readable threat intelligence (MRTI)
- ✓ High fidelity intelligence about phishing, malware, and botnet infrastructure
- ✓ Human-readable reports with context behind threat actor infrastructure to understand attacker tactics

Phishing Detection and Response

- ✓ Real-time response and historical analysis driven from verified phishing threats associated with malicious files
- ✓ Hash file indicators used in phishing campaigns
- ✓ Blacklisted files based on malicious phishing tactics
- ✓ Pinpoint hosts coming in contact with phishing files to take additional incident response action

With Cofense Intelligence and SentinelOne, security teams can detect and respond based on credible, human-verified phishing intelligence. Cofense Intelligence offers a RESTful API that SentinelOne polls for file hash indicators and cross-correlates in the platform. The constant polling of credible human-verified phishing intelligence associated with malicious files provides security teams with visibility into the latest global phishing threats. An endpoint communicating with phishing file hashes provided from Cofense can quickly be identified and investigated. Analysts have a view into credible phishing threats leading to higher confidence in the action taken based on the indicator results returned to the platform.



EDIT BINARY

○ Whitelist ● Blacklist

Cofense Intelligence: OfficeMacro https://www.threathq.com/p42/search/default?m=12283

Windows

e7f93dca71c1b8fefbdf04515bea783d026ae485

TYPE	DEVICE	SOURCE	DESCRIPTION	SHA1	LAST UPDATED	FIRST SEEN
●	⊞	User (Cofense)	Cofense Intelligence: FormGrab...	622a61817c869bf727f029b32e5da...	07/13/18 13:09:41	07/13/18 13:09:41
●	⊞	User (Cofense)	Cofense Intelligence: Remote Ac...	43f8071c35a648ac2431fed796ddf...	07/13/18 13:09:41	07/13/18 13:09:41

(Cofense Intelligence Office Macro indicator detected communicating by SentinelOne blacklist)

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 endpoint policies.

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 confidence to deny the communication is absolutely 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

SentinelOne, working with Cofense Intelligence, provides analysts with the ability to investigate, validate, and remediate based on indicator impact 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. With SentinelOne, security teams can operationalize Cofense Intelligence phishing artifacts and indicators.

Cofense Intelligence human-readable reports are linked from within SentinelOne to provide analysts Indicators of Compromise (IOC) with context. This provides the additional insight so security teams can understand the criminal infrastructure and support remediation decisions.

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 operation and the risk to the business.

The combination of Cofense Intelligence and SentinelOne provides clear insight for assertive action from malicious file artifacts.

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 that are detected and responded to across endpoints.

About SentinelOne

SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects and responds to attacks across all major vectors. Designed for extreme ease of use, the SentinelOne platform saves customers time by applying AI to automatically eliminate threats in real time for both on-premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint.

SentinelOne™

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