Quarantine Phishing Threats with Cofense Vision and Splunk SOAR

Streamline phishing detection and response to maximize efficiency by using the Cofense Vision integration with Splunk SOAR

Quarantine Phishing Threats with Cofense Vision and Splunk SOAR
Relentless Attackers Create Phishing Emails Seeking to Wreak Havoc

THE CHALLENGE
Attacker's tactics evolve and find creative ways to bypass defenses to deliver malicious emails to a recipient's inbox. Conditioned employees will report suspicious emails to the SOC. But security teams face unique challenges in today's rapidly changing landscape and are responsible for investigation and response of several incidents besides phishing. Where is phishing investigation prioritized in the SOC? Once confirmed, phishing emails need to be quarantined from mailboxes. Cybersecurity and email administrators have competing priorities and are on disparate teams with different tools.

This adds additional layers of complexity to the day-to-day operations of security teams. SOC analysts can't wait around for the email team to search and quarantine the threat. Time is of the essence and response needs to happen in minutes, not hours or days. What's more, a similar phishing threat may reside in other mailboxes and the threats needs swift action to quarantine.

To overcome these challenges and enable security programs to scale, it is critical that organizations integrate, automate, and orchestrate to remove phishing threats lurking in the inbox

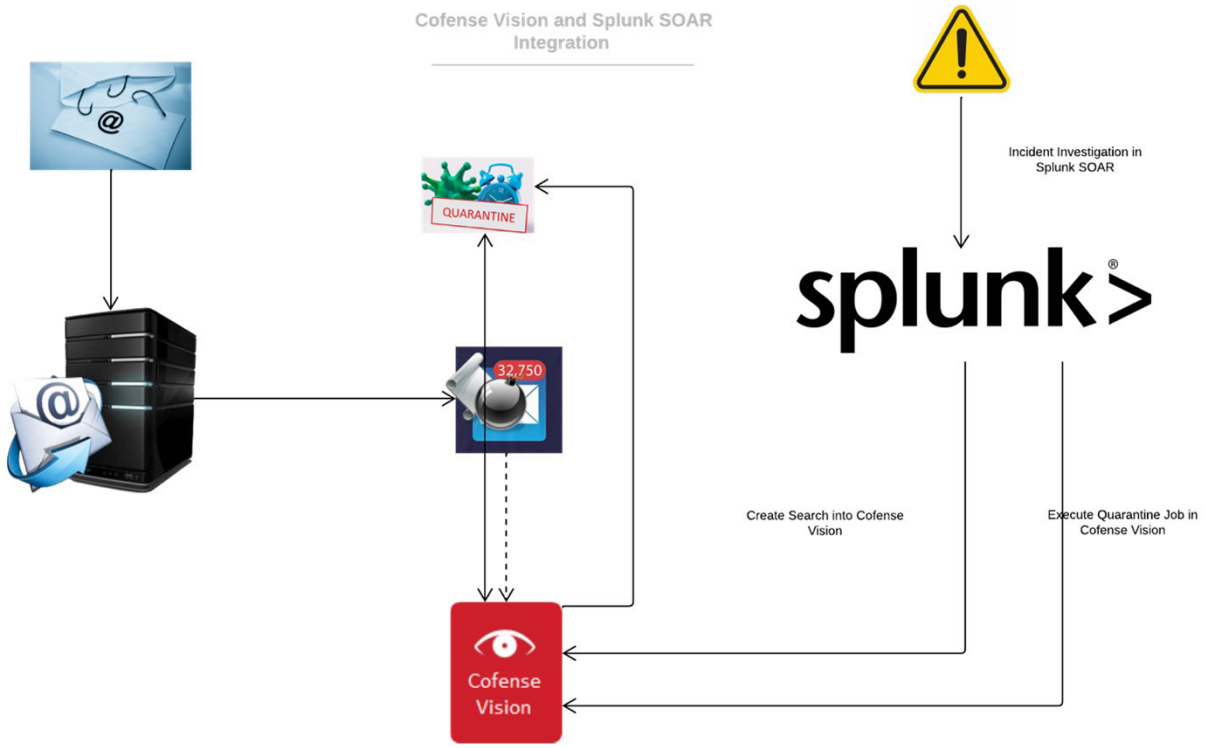
Quarantine Suspicious Email with Cofense Vision's Splunk SOAR Ap

The Cofense Vision app was created to allow Splunk SOAR's platform to fully-integrate with Cofense Vision and run playbooks to remove unwanted suspicious email in seconds. Leveraging Cofense Vision's API, Splunk SOAR can serve as the user interface for SOC analysts. Threat hunting teams can write indicators from Splunk SOAR into Cofense Vision, and setup quarantine jobs to remove emails matching content as soon as they're received. Cofense Vision's software instantly quarantines emails matching threats to the business and to protect your entire organization from compromise, and potentially a breach.

THE SOLUTION

When cybersecurity teams search and remove suspicious emails from employee's mailboxes without the need to involve email administrators, they can quarantine suspicious emails before employees open them. Furthermore, cybersecurity analysts can auto-quarantine emails matching credible phishing indicators. As soon as the email is received, the suspicious message will be quarantined in near real time, removing the risk employees will open and engage. Leveraging the integration between Cofense Vision and Splunk SOAR your security team can quarantine credential theft, emails with nefarious links to malicious websites, and malware-based attachments from the mailbox. The combination of credible phishing intelligence from millions of Reporters world-wide along with employee-reported threats, arm the SOC with actionable intelligence to hunt and quarantine.

INTEGRATION BENEFITS Together, Cofense Vision and Splunk SOAR enable customers to search and quarantine suspicious emails that have bypassed secure email gateways.		
Contribute actionable intelligence: Benefit from Cofense's phishing intelligence to identify and quickly quarantine suspicious emails lurking in the inbox.	**Search and quarantine:** Create precise or broad indicator queries to identify and quarantine suspicious emails before employees have a chance to open messages.	**Auto-quarantine email:** Auto-quarantine or escalate for approval, emails which may need to be removed from mailboxes without waiting for email administrators.
Extract phishing indicators: Download entire emails and attachments to enrich other incident response actions, forensic, and playbooks.		



The Cofense Vision app for Splunk SOAR will enable the SOC to automate search and quarantine of highly actionable intelligence. Leveraging both technologies, the security team will be able to hunt for, and quarantine suspicious email with Cofense Vision. Maximize your security investments and reduce analysts' investigation time to remove threats before damage is done. Ransomware, credential theft, and business email compromise, are all threats facing business regardless of size and industry. Your team can use this powerful integration to:

- Contribute additional sources of intelligence for use in queries
- Search for all messages precisely, or broadly mapping to indicators
- Execute playbooks to quarantine emails
- Extract malicious email attributes to enrich incident data
- Threat hunt for presence of indicators elsewhere gleaned from quarantined emails
- Reduce MTTR and MTTD

Use Case 1: Automated Phishing Search and Quarantine

Challenge: When a security incident occurs involving phishing, it can lead to any number of downstream effects. Credential compromise, ransomware, and attackers gaining a foothold into infrastructure to move laterally and exfiltrate data, are too common. It's crucial for employees to recognize and report suspicious email. In addition, it is imperative SOCs can search and quarantine emails that pose a threat and remove them before employees have a chance to open.

Solution: Cofense Vision is purpose-built to allow SOCs to search and quarantine emails without the need to involve the messaging team who have other priorities. Cybersecurity teams know time is critical and Cofense Vision provide a conduit to journaled email for SOCs to detect and respond to custom threat criteria. Using Cofense Vision's app for Splunk SOAR, your team is ready to automate discovery, incident handling, and response for suspicious email discovered by Cofense Vision. This integration also provides precision and broad search capabilities to identify and quarantine what other defenses missed. Cofense Vision's API grants access to Splunk SOAR to centralize phishing incident and response.

Benefit: Automate the search and quarantine of phishing threats with Splunk SOAR and Cofense Vision to scale your organization's security posture and resiliency toward timely removal of suspicious emails residing in mailboxes. Centralized management through purpose-built commands and playbooks allow SOCs to identify and respond in seconds.

Use Case 2: Bi-directional Phishing Intelligence for Detection and Response

Challenge: Threat intelligence is often too broad and not specific to phishing. Security teams can get distracted with indicators that are less credible. Skillful attackers shift tactics to evade the SOCs' ability to detect and respond to threats.

Solution: Cofense Vision leverages credible phishing intelligence from Cofense's research and intelligence teams and from the Phishing Detection Center, which receives thousands of malicious emails every day from millions of Reporters world-wide. In addition to the intelligence Cofense produces, Cofense Vision can ingest indicators. URLs, domains, hash values, email senders, and more, can be written into Cofense Vision and used in search queries. Once matched, either with Cofense Intelligence or others, Cofense Vision can identify and quarantine emails matching indicators. Furthermore, Splunk SOAR can glean emails that match threats and extract to be used in additional incident response actions.

Benefit: Automate the search and quarantine of phishing threats with Splunk SOAR and Cofense Vision matching phishing threat indicators. Automate publishing of phishing threat indicators for email quarantine before employees open.

About Splunk

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative. Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received over 1,020 patents to date and availability in 21 regions around the world — and offers an open, extensible data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process. Build a strong data foundation with Splunk.

For more information, visit http://www.splunk.com/

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, Cofense is the only comprehensive email security solution powered by a global network of 35+ million reporters which utilizes a combination of unique intelligence sources to identify, protect, detect and respond to all email security threats. Powered by the Cofense Phishing Detection and Response (PDR) platform, organizations that deploy the full suite of Cofense solutions 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: cofense.com/contact T: 703.652.0717

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