Palo Alto Networks WildFire and Cofense Triage

Efficiently Analyze and Respond to Suspicious Emails

Benefits of the Integration

Together, Cofense and Palo Alto Networks WildFire:

- Analyze employee-reported email attachments with standalone WildFire API to discover malicious files.
- Prioritize within Cofense Triage, email security incidents, and alert SOC teams to take action.
- Extract phishing threat indicators to be used by research and intelligence teams to learn attacker's tactics.
- Efficiently automate file analysis to keep SOC and IR teams productive.
- Provides thorough file scanning and report verdicts to inform analyst's decision making.

The Challenge

Attackers continue to use phishing as a tactic to compromise credentials or deliver malware with malicious attachments. Email gateways are not completely effective at blocking, as attackers find new and creative ways to avoid detection and quarantine. Security teams are often unaware when malicious campaigns are successful at reaching an employee's inbox. Unsuspecting employees may have their credentials stolen or their systems infected by opening a malicious payload. Ransomware is just one example where one wrong action can lead to widespread damage and hamper business operations.

The Solution

Phishing email attachments can be analyzed to determine if the payload is malicious. Once a suspicious email is reported by an employee, attachment hashes are queried to determine if the file is benign or malicious. Or the entire file can be submitted for analysis. The result is that the files analyzed help determine if there is a malicious payload. The results of the analysis produce a report for security analysts to gain more context.

Attributes from the attachments can then be used to provide security teams with insight into the attacker's tactics. When combined, the integration leverages automation to submit at ingestion, return results, and prioritize the analyst's phishing analysis response.

Cofense Triage

Cofense Triage prioritizes and remediates phishing threats quickly. Triage assists SOC teams by prioritizing suspicious emails reported by employees. When a suspicious email is reported, thousands of intelligence-driven rules automatically assess the report, cluster with other reports containing similar payloads, and identify the highest-priority threats for immediate action. Cofense Triage includes powerful tools for a precise view of phishing emails: attachments, URLs, and headers.

Palo Alto Networks WildFire

Palo Alto Networks Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. Central to this architecture is WildFire malware prevention service, which turns every Palo Alto Networks deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and impact the network.

Palo Alto Networks and Cofense

Palo Alto Networks standalone WildFire API subscription integrates with Cofense Triage to analyze suspicious and employee-reported phishing emails. Security teams can identify threat indicators from reported emails and respond to an attack before it leads to a breach.

Cofense Triage at ingestion queries the standalone WildFire API subscription for known malicious hash values indicators or full

file submission and generates reports containing payload information. The integration configuration takes only minutes to enable in Cofense Triage and helps maximize existing security investments through a purpose-built integration. Once files are analyzed, security teams will quickly determine which reported emails are malicious or benign. Analysts now know where to prioritize their time, which reported emails need an immediate response, and which are not a threat to the business.

Use Case 1: Automatically Analyze Suspicious Emails

Challenge

Every employee is at risk of receiving suspicious emails—some of which may be phishing. Security teams need to ensure employees are empowered to easily report suspicious emails for analysis. However, security teams are tasked with many other events, some of which may be benign, which wastes time. Yet, they need to know which reported emails are malicious so that they can respond quickly.

Solution

Employees are conditioned to report suspicious emails to the security team. Cofense Triage ingests and automatically analyzes email attachments by leveraging the standalone WildFire API subscription. In tandem, Triage and WildFire examine files and return results to security analysts. The results help analysts determine which emails are malicious and which are benign.

Use Case 2: Prevent Access to Malicious Phishing Indicators

Challenge

Security teams need accurate phishing indicators to avoid mistakes with false positives. Phishing-specific results with detailed analysis help analysts know where to focus their time. Too many solutions only have data when security teams need intelligence highlighting threat severity. This is especially true with email, where a trusted sender domain may contain malicious URLs used by a phisher who compromised the credentials of a trusted entity.

Solution

With Triage and WildFire, indicator results make it easy for analysts to have confidence in their actions. In addition, the indicators can be exported and integrated into the security stack to help protect against the same or similar tactics that may evolve.

Figure 1: Cofense Triage and standalone WildFire API integration

Palo Alto Networks and Cofense Integrations

Palo Alto Networks Cortex XSOAR and Cofense have other integrations in the Marketplace. Cortex XSOAR integrates with Cofense Triage, Cofense Vision, and Cofense Intelligence.

About Cofense

Cofense is the leading provider of protection, detection and response email security solutions, and the only company to combine a global network of over 35 million people reporting phish with advanced AI-based automation to stop phishing attacks. For more information, visit www.cofense.com.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com