Automate Phishing Response with Cofense and Cortex XSOAR

Automated Phishing Threat Analysis, Intelligence, and Incident Remediation Management

Benefits of the Integration

Together, Cofense Triage, Cofense Intelligence, and Cortex XSOAR enable you to:

- **Identify threats in your system:** Analyze and accurately respond to emerging phishing threats, like credential theft, ransomware, and targeted malware.
- **Enrich phishing threat indicators:** Use Cofense Triage and Cofense Intelligence phishing data to automatically enrich suspicious alerts and events with Cortex XSOAR and instantly disrupt phishing attacks in progress.
- **Manage employee-reported emails effectively:** Improve SOC efficiency with automated prioritization of employee submitted phishing reports by leveraging Cofense Triage and Intelligence within your Cortex XSOAR workflows.
- **Leverage insights:** Enrich and coordinate your Cofense phishing response workflows with Cortex XSOAR's selection of 780+ third-party product integrations.

Automate Phishing Analysis and Intelligence to Increase SOC Productivity

Of the hundreds of tactics available to threat actors, phishing is one of the most successful and harmful to organizations. Attackers use techniques like credential theft, ransomware, and targeted malware payloads. Delivered through trusted parties, services, and applications, the latest evolution of phishing emails is sent to millions of employees every day. Entry-level phishing protection is not enough to secure the SOC from phishing threats that bypass secure email gateways (SEGs) and other defenses. To minimize the chance of phishing emails reaching employees, security teams need a solution that accelerates identification and mitigation.

Cortex XSOAR Marketplace is a digital storefront for discovering turnkey security orchestration content packs centrally within Cortex XSOAR.

Content packs are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security orchestration use cases.

The Cofense Triage and Intelligence packs allow the SOC to automatically respond to phishing threats, leveraging Cofense's phishing expertise to speed accurate responses to phishing attacks.

Cofense Triage includes:

- **2** automations
- **2** classifiers
- **17** incident fields
- **1** incident type
- **3** integrations
- **1** layout
- **3** playbooks

Cofense Intelligence includes:

- **1** integration
- **1** threat intelligence module feed
- **6** search and reputation commands

Cofense content packs for Cortex XSOAR are easily deployed with a single click from the in-product Marketplace, providing the prebuilt content you need to streamline your response workflows. Together with Cortex XSOAR, Cofense Triage and Cofense Intelligence can save your SOC hundreds of hours per week with automated phishing incident response and threat intelligence playbooks.

Bridge gaps and advance the maturity of your security program by tapping into the fastest-growing community of security experts. To discover new SOAR content, visit paloaltonetworks.com/cortex/xsoar/marketplace.

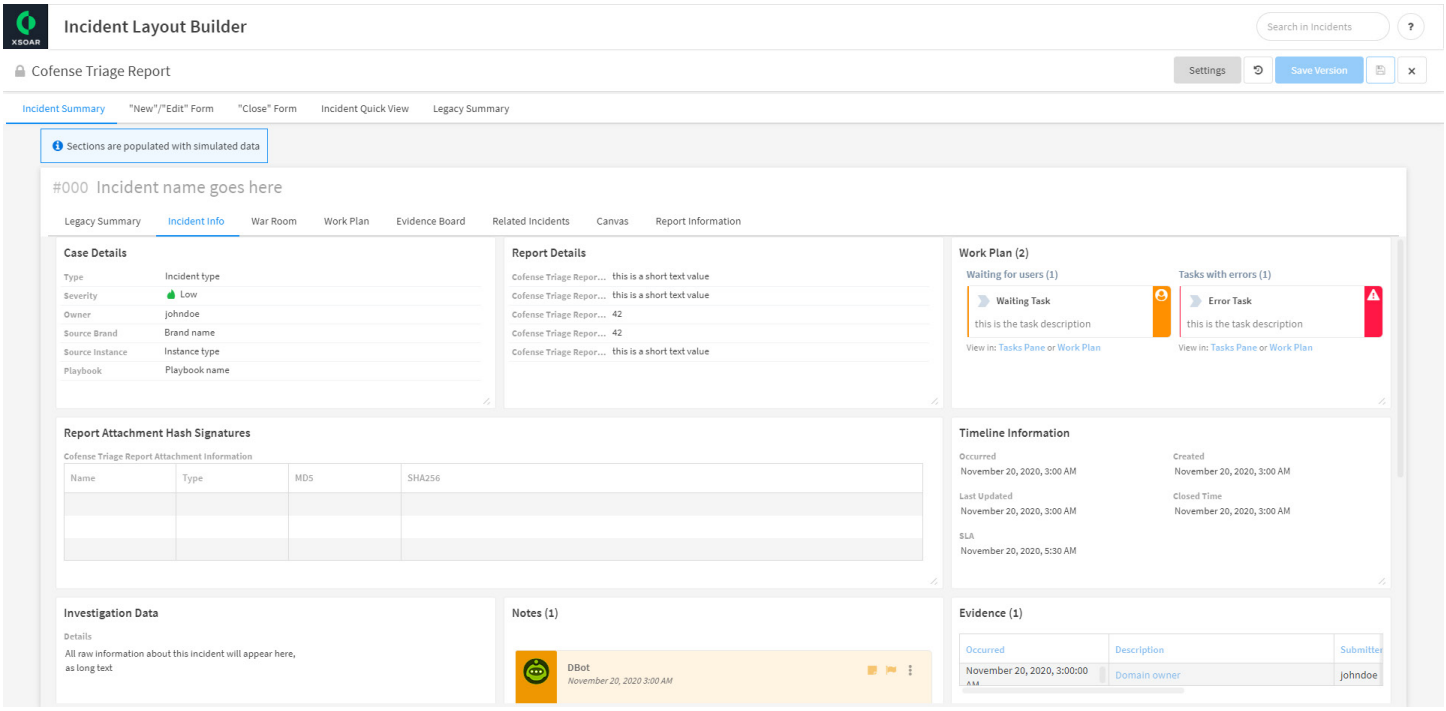

Figure 1: Cofense Triage Incident Layout in Cortex XSOAR

To meet the need for advanced phishing detection, Cofense has partnered with Cortex® XSOAR to release integrated content packs for Cofense Triage and Cofense Intelligence, available in the Cortex XSOAR Marketplace. With the click of a button, your security team can install these prebuilt packs and immediately start to automate and optimize complex phishing analysis and response workflows across different information systems and security tools. Whether you want to consume attributes from unresolved or processed phishing reports or ingest phishing threat indicators, this integration will significantly reduce the time it takes to analyze and respond to phishing attacks and enable your SOC to standardize and scale the most effective phishing defense possible.

Cofense Triage and Cofense Intelligence

The Cofense Triage content pack specializes in reducing noise while identifying phishing threats so that your security team can address them without disrupting the day-to-day operations of your employees. Cofense Intelligence provides SOCs with the ability to ingest human-verified phishing indicators and contextual reports that are vigorously vetted by Cofense Labs so that your automated and manual workflows are always enriched with verified threat indicators. Access to verified indicators and easy-to-understand context makes it easier for the SOC to act fast and contain threats before they can operationalize.

The Cofense Triage content pack for Cortex XSOAR provides full coverage of the phishing analysis, detection, and response capabilities of the platform, enabling your SOC to easily consume employee-submitted phishing reports. The Cofense Intelligence content pack contains timely, credible, and human-verified phishing indicators for SOCs to ingest for actionable decisions. Leveraging both technologies, your security team will be able to detect, analyze, prioritize, and respond to phishing threats. Your team can use this powerful integration to:

- Automatically determine priority and assign phishing incidents to your security team.
- Inform fast decision making with verified threat intel from Cofense in Cortex XSOAR.
- Threat hunt for phishing indicators of compromise and contextualize your findings.
- Extract phishing indicators to help inform decisions in the future.

Use Case 1: Detection of an Active Phishing Attack

Challenge

When a security incident occurs involving phishing, time is of the essence to analyze the threat and its severity. The SOC needs to resolve the incident quickly and understand the breadth of the attack. It is critical for SOCs to answer questions like, "How many employees have been impacted?" and "What are the phishing attributes and indicators that evaded detection by the secure email gateway?"

Solution

Cofense Triage provides native phishing intelligence rules from the Cofense Labs research and intelligence team who discover global phishing threats and equip SOCs with the critical intelligence and report context they need. The Cofense content pack provides full integration of this context and enables SOC teams to automatically understand the entirety of the attack within Cortex XSOAR.

Benefit

The speed and ease of automating your phishing workflows allow your security team to quickly adjust protocols, inform stakeholders, and protect employees moments after a phish has been detected or reported. The result is a stronger security program for a safer organization and more time for your SOC to focus on other key initiatives.

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations 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.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. 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