Cortex XSOAR and KnowBe4

Automated Reporting for Security Awareness Training Events and Suspicious Email Remediation Management Improves Security Culture and Increases SOC Productivity

Security teams face unique challenges in today's rapidly changing landscape of phishing, malware, and other social engineering and cybersecurity threats. Collaboration across disparate teams and siloed tools adds additional layers of complexity to security teams' day-to-day operations. When security teams use different systems for simulated phishing, security awareness training, incident response, and remediation, it is difficult to track and optimize the full lifecycle of an incident. To overcome these challenges and allow security programs to scale, organizations should integrate, automate, and orchestrate as many security tasks as possible across their primary teams, tools, and systems.

Leveraging the content packs and integrations between Cortex XSOAR and KnowBe4, your security team can automate and optimize complex workflows across the full stack of your information systems and security tools. Using the Cortex XSOAR and KnowBe4's Kevin Mitnick Security Awareness Training (KMSAT) content pack will provide the reporting and automation that your security team needs to analyze and improve your security awareness training program.

Using the Cortex XSOAR and KnowBe4 PhishER content pack will provide the automation that your security team needs to respond to potential email threats. With Cortex XSOAR, security teams can seamlessly integrate their existing automation and workflows with KMSAT and PhishER. Whether you want to assess compliance, use custom events to initiate specialized training, or investigate user-reported email threats, these integrations will allow your security awareness and SOC teams to standardize and scale the most effective workflow possible.

The KnowBe4 KMSAT Content Pack

The KnowBe4 KMSAT content pack was created for phishing, training, and custom user events related to your security awareness training program. The integration between Cortex XSOAR and KMSAT allows you to fully leverage the resources available to your security teams and help your organization build a strong human firewall. This integration allows you to analyze data and risk indicators and conduct response and remediation by using automation playbooks. Utilize the full potential of your security resources by integrating KMSAT with your top tools and automated orchestration playbooks within Cortex XSOAR.

Benefits of the Integration

Together, KMSAT and Cortex XSOAR enable you to:

- **Discover threats, noncompliance, and more.** Monitor events to quickly and accurately adapt your security program to maximize awareness.
- **Enrich security culture.** Use data to help target risky behaviors and enhance training.
- **Manage remediation.** Use custom events to improve your security team's efficiency by automating remedial training.
- **Leverage insights.** Pull data from KMSAT to coordinate security responses from 900+ Cortex XSOAR third-party product integrations.

The KnowBe4 PhishER Content Pack

The KnowBe4 PhishER content pack was created for analyzing user-reported email threats and enriching the process with threat intel from other systems. The pairing of Cortex XSOAR's powerful platform with PhishER leverages the full resources available to your security teams. Scale to cover your entire organization with alerts for user-reported threats and the ability to add data, comments, and resolution information from within the Cortex XSOAR platform. This enables Cortex XSOAR users to analyze data and risk and create a response via playbooks. Utilize the full potential of your security resources, including the siloed enrichment data that you already have, by integrating PhishER with your top tools and automated orchestration playbooks within Cortex XSOAR.

Benefits of the Integration

Together, PhishER and Cortex XSOAR enable you to:

- **Discover threats.** To quickly and accurately analyze your reported threats to maximize speed to resolution.
- **Enrich responses.** Use data to help identify real threats from benign spam.
- **Manage remediation.** Using Cortex XSOAR, improve your team's efficiency with playbooks to automate your security response.
- **Leverage insights.** Take information from PhishER to coordinate security responses from 900+ Cortex XSOAR third-party product integrations.

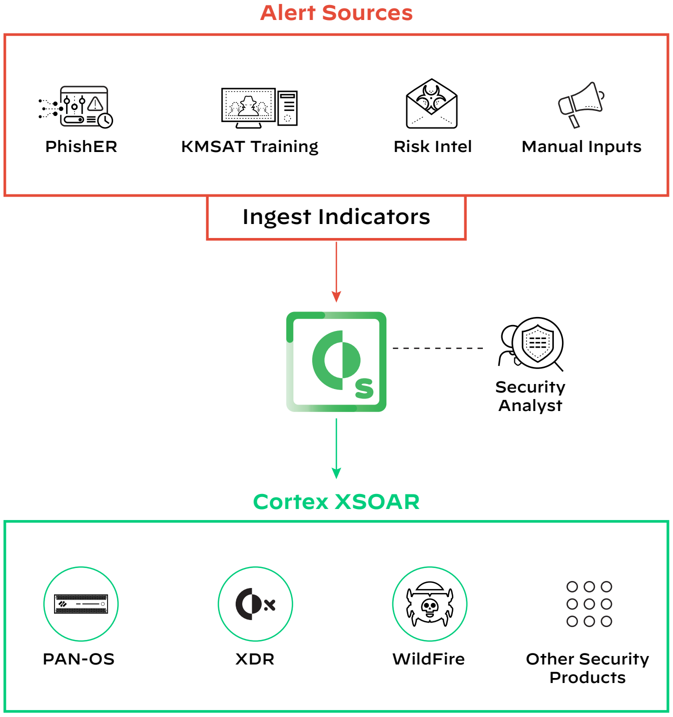

Figure 1: Dashboard or potential playbook

Use Case 1: KMSAT—Automated Noncompliance and Risk Indicators

Challenge

When a security team evaluates the success or compliance of its training efforts, it can be hard to manually address the collection of compliance data or the need for additional training. It's crucial for these professionals to continue improving the organization's security culture, but it can be time-consuming to address it in this way.

Solution

KMSAT provides reporting of training completions and simulated phishing tests to help you monitor compliance and discover risks in your organization. Using the KnowBe4 KMSAT content pack for Cortex XSOAR, your team can automate incident discovery and response for risks that KMSAT tracks. For example, you can use commands to send specific Risk Score or Phishing Security Test (PST) data. Then, you can use this data in automations, playbooks, and reports in Cortex XSOAR. This integration also allows you to create custom events that can initiate additional KMSAT training and phishing campaigns from Cortex XSOAR.

Benefit

Automate the collection of training completion evidence and simulated phishing data with Cortex XSOAR and KMSAT to scale your organization's security posture without adding new staff or expertise to your current security team.

Use Case 2: PhishER—Automated Incident Enrichment and Response

Challenge

When a security incident is identified involving user-reported emails, it can be extremely taxing for a SOC to manually address the potential security threats.

Solution

PhishER provides machine learning and user-submitted comments to discover email threats across your environment. Using the PhishER content pack for Cortex XSOAR, your team is enabled to automate discovery, incident handling, and response for all the threats discovered and provided by PhishER. This integration also provides context enrichment and commenting capabilities, e.g., when you send PhishER data to other connected platforms through Cortex XSOAR, automate manual functions, and send data back to PhishER to change attributes and add tags or comments.

Benefit

Automate the analysis of user-reported email threats and your response/resolution with Cortex XSOAR and PhishER to scale your organization's security posture without adding new staff or expertise to your current SOC team.

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 56,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist, and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense. For more information, visit www.knowbe4.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