SOPHOS

KnowBe4's SecurityCoach integration with Sophos Intercept X Endpoint allows you to leverage security alerts for viruses, malware, and other endpoint threats to send real-time SecurityTips to risky users.

The Problem

➜ Social engineering techniques like phishing, spear phishing, and impersonation are increasingly being used by cybercriminals to manipulate your employees, causing downtime and security breaches

➜ The human factor is involved in 82% of data breaches, according to the 2022 Verizon Data Breach Investigations Report

➜ The average SOC team receives an average of 11,000 alerts per day, resulting in alert fatigue and analyst burnout

➜ Users forget 50% of information they learn within one day and 90% within one week without engaging and frequent reinforcement of their training

Managing the Problem

➜ SecurityCoach uses Sophos APIs to analyze alerts and identify end user risky security behavior

➜ You easily configure real-time coaching campaigns using your own security policies and the different categories of risky behavior

➜ SecurityCoach delivers the contextual, real-time SecurityTips you choose, using the ready-made graphic template library and optional custom notifications

Use Case Examples

➜ **Malware Avoidance**—When Sophos detects Malware, SecurityCoach can map the malware to a specific user and send them a targeted SecurityTip on avoiding malware

➜ **Online Security**—When Sophos detects that a user visits a risky website, SecurityCoach can coach that user on reasons to avoid such websites

Benefits and Outcomes

➜ Measurable reduction in risk and a stronger security culture across your organization

➜ Improved comprehension and retention of your security awareness training, best practices, and established security policies

➜ Significant additional value from your existing investments in KnowBe4 and Sophos

➜ Time saved for SOC analysts and improved efficacy through automation and reducing alert noise caused by users repeating risky security behaviors

About KnowBe4 SecurityCoach

SecurityCoach enables real-time security coaching of your users in response to risky security behavior. Based on the rules in your existing security software stack, you can configure your real-time coaching campaign to determine the frequency and type of SecurityTip that is sent to users at the moment risky behavior is detected.

About Sophos

Powered by threat intelligence, AI and machine learning from SophosLabs and SophosAI, Sophos delivers a broad portfolio of advanced products and services to secure users, networks and endpoints against ransomware, malware, exploits, phishing and the wide range of other cyberattacks. Sophos provides a single integrated cloud-based management console, Sophos Central – the centerpiece of an adaptive cybersecurity ecosystem that features a centralized data lake that leverages a rich set of open APIs available to customers, partners, developers, and other cybersecurity vendors. Sophos sells its products and services through reseller partners and managed service providers (MSPs) worldwide.