knowbe4

Echtzeit-Coaching als Reaktion auf riskantes Nutzerverhalten

Ihre Sicherheitskultur verbessern, Ihre Risiken reduzieren

Social-Engineering-Angriffe sind und bleiben ein großes Problem. Cyberkriminelle versuchen, Ihre Nutzerinnen und Nutzer auszutricksen und die Cybersicherheitsmaßnahmen Ihrer Organisation zu umgehen. Laut dem Verizon Data Breach Investigations Report 2025 ist der Faktor Mensch an 60 % aller Datenpannen beteiligt. Entlasten Sie Ihr gestresstes Sicherheitsteam, indem Sie die Anzahl der Warnmeldungen aufgrund von wiederholt riskantem Verhalten Ihrer Mitarbeitenden senken.

Stellen Sie sich vor, Sie könnten Ihre Nutzerinnen und Nutzer mithilfe der von Ihrer Sicherheitsinfrastruktur erfassten Nutzerereignisdaten schulen, indem Sie mit Echtzeit-Coaching auf riskantes sicherheitsrelevantes Verhalten Ihrer Nutzerinnen und Nutzer reagieren und zugleich Ihr SOC-Team entlasten, indem Sie die Menge an Warnmeldungen aufgrund von wiederholt riskantem Verhalten reduzieren. Das ist ab sofort möglich – mit SecurityCoach™.

Was ist SecurityCoach?

SecurityCoach ist das erste Echtzeit-Sicherheitscoaching, das IT- und SOC-Teams dabei unterstützt, die größte Angriffsfläche Ihrer Organisation zu schützen – Ihre Mitarbeitenden.

SecurityCoach stärkt Ihre Sicherheitskultur, indem Ihre Nutzerinnen und Nutzer bei riskantem Verhalten ein Echtzeit-Sicherheitscoaching erhalten. Sie können Echtzeit-Coaching-Kampagnen über Ihre vorhandene Sicherheitsinfrastruktur konfigurieren, um Ihren Nutzerinnen und Nutzern kontextbezogene SecurityTips mit Informationen aus Ihrem Security Awareness Training und Ihren Sicherheitsrichtlinien anzuzeigen. Dadurch werden die erworbenen Kenntnisse gefestigt und die Nutzerinnen und Nutzer können zudem die mit ihrem Verhalten verbundenen Risiken besser nachvollziehen.

SecurityCoach lässt sich in das Security Awareness Training von KnowBe4 und in Ihre vorhandene Sicherheitsinfrastruktur integrieren, um Echtzeit-Coaching als Reaktion auf riskantes sicherheitsrelevantes Verhalten von Nutzerinnen und Nutzern bereitzustellen.

SecurityCoach

Wesentliche Vorteile

- Besseres Verständnis und Festigung der Kenntnisse der Nutzerinnen und Nutzer in Bezug auf Security Awareness Training und die geltenden Sicherheitsrichtlinien durch Echtzeit-Coaching zum tatsächlichen Verhalten
- Nutzung der vorhandenen Sicherheitsinfrastruktur für das Echtzeit-Coaching von Nutzerinnen und Nutzern mit Risiko und optimale Nutzung getätigter Investitionen
- Individuelle Kampagnen für Nutzerinnen und Nutzer mit hohem Risiko, die ein lohnendes Ziel für Cyberkriminelle darstellen oder die sich wiederholt riskant verhalten
- Daten und Reports über Verbesserungen beim Sicherheitsverhalten in Ihrer gesamten Organisation, mit denen sich eine fortgesetzte Investition rechtfertigen lässt
- Weniger Belastung für Ihr SOC und höhere Effizienz, da weniger Warnmeldungen aufgrund von wiederholt riskantem Verhalten eingehen

Gründe für SecurityCoach

Die Menge der Social-Engineering-Angriffe auf Ihre Nutzerinnen und Nutzer nimmt zu. Sie können Ihre Organisation am besten schützen, indem Sie eine starke Sicherheitskultur aufbauen, die Ihre Nutzerinnen und Nutzer einbindet und ihnen vor Augen führt, wie wichtig die Einhaltung der Sicherheitsrichtlinien Ihrer Organisation ist.

SecurityCoach nimmt Ihrem überlasteten SOC-Team einige Arbeit ab, da die Menge der durch wiederholt riskantes Verhalten verursachten Warnmeldungen reduziert wird. Ihr SOC-Team kann sich so auf Bedrohungen mit hoher Priorität konzentrieren.

Wie funktioniert SecurityCoach?

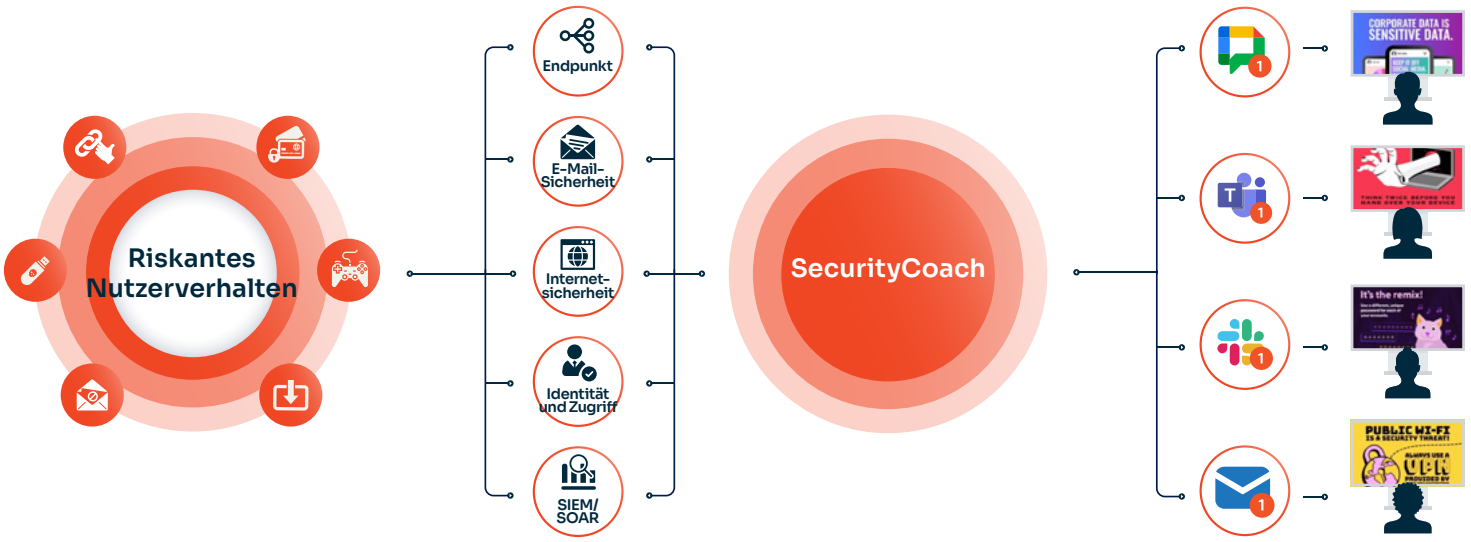
SecurityCoach lässt sich mithilfe von Standard-APIs schnell und einfach in Ihre vorhandenen Sicherheitsprodukte von Microsoft, CrowdStrike, Cisco und anderen Anbietern integrieren. Ihre Sicherheitsinfrastruktur generiert Warnungen, die dann von SecurityCoach analysiert werden, um jene Ereignisse zu identifizieren, die auf das riskante sicherheitsrelevante Verhalten Ihrer Nutzerinnen und Nutzer zurückgehen.

Wenn ein Nutzer beispielsweise einen infizierten E-Mail-Anhang öffnet, der möglicherweise Ransomware enthält, die sich in Ihrem Netzwerk verbreiten könnte, oder wenn eine Nutzerin versucht, eine Website mit unzulässigem Inhalt auf ihrem Arbeitscomputer aufzurufen, erkennen Ihre Sicherheitsprodukte diese Aktivitäten und erstellen eine Ereigniswarnung. SecurityCoach ermittelt das Ereignis und sendet über Microsoft Teams, Slack, Google Chat oder per E-Mail einen Echtzeit-SecurityTip an diese Nutzerinnen und Nutzer, in dem das Sicherheitsrisiko benannt und erläutert wird. Sie können Coaching-Kampagnen für Nutzerinnen und Nutzer mit Risiko basierend auf jenen Ereignissen einrichten, die Ihre Netzwerk-, Identitäts-, Internetsicherheits- oder sonstigen Anbieter aus Ihrer Sicherheitsinfrastruktur erfassen.

Mithilfe dieser Kampagnen können Sie Ihre Nutzerinnen und Nutzer in dem Moment schulen, in dem das riskante Verhalten auftritt. Sie können Echtzeit-Feedback anbieten und an die Inhalte aus aktuellen Security-Awareness-Trainingskampagnen erinnern. Sie können Echtzeit-Coaching-Kampagnen konfigurieren, die auf Ihren eigenen Sicherheitsrichtlinien beruhen, und diese Kampagnen mithilfe von SecurityCoach automatisieren.

SecurityCoach unterstreicht die Notwendigkeit, die Sicherheitsrichtlinien Ihrer Organisation zu befolgen, verbessert das Nutzerverhalten und stärkt Ihre Sicherheitskultur.

SecurityCoach-Workflow



1. Die Sicherheitsanbieter, die Sie in Ihre KnowBe4-Konsole integrieren, überwachen riskante Aktivitäten auf den Geräten Ihrer Nutzerinnen und Nutzer.
2. Die Warnmeldungen werden an SecurityCoach übermittelt. SecurityCoach analysiert die erkannten Ereignisse und legt fest, welche Bedrohungen sich am besten für das Echtzeit-Coaching Ihrer Nutzerinnen und Nutzer eignen.
3. Wenn ein riskantes Nutzerverhalten erkannt wird, erhalten die jeweiligen Nutzerinnen und Nutzer über Microsoft Teams, Slack, Google Chat oder per E-Mail automatisch einen Echtzeit-SecurityTip von SecurityCoach.

Gründe für SecurityCoach

Echtzeit-Coaching

Mithilfe von Echtzeit-Coaching-Kampagnen können Sie Ihre Nutzerinnen und Nutzer in Echtzeit über ein riskantes Verhalten informieren. Wenn eine riskante Aktivität erkannt wird, erhalten Ihre Nutzerinnen und Nutzer eine Coaching Notification mit einem SecurityTip zur Aktivität und wie sie in Zukunft vermieden werden kann.

SecurityTip-Benachrichtigungen

In dem Moment, in dem riskantes Nutzerverhalten erkannt wird, erhalten die entsprechenden Nutzerinnen und Nutzer über Microsoft Teams, Slack, Google Chat oder per E-Mail einen Echtzeit-SecurityTip von SecurityCoach. Diese Sofortbenachrichtigungen sind eine wirkungsvolle Erweiterung zu jedem Security Awareness Program.

API-Integrationen

Sicherheitslösungen von Microsoft, Cisco, Netskope, Zscaler und anderen Sicherheitsanbietern lassen sich über die jeweiligen Anbieter-APIs schnell und einfach integrieren. Unser Technologiepartner-Ökosystem wächst schnell, da wir unsere Kunden umfassender unterstützen und durch den Faktor Mensch verursachte Risiken reduzieren möchten.

Integrierte Erkennungsregeln

Über Erkennungsregeln wird festgelegt, welche riskanten Aktivitäten Sie anhand der von Ihren integrierten Sicherheitsanbietern bereitgestellten Daten verfolgen möchten. SecurityCoach empfiehlt Erkennungsregeln basierend auf den häufigsten Sicherheitsthemen in der Reihenfolge der Priorität, wobei Regeln mit sehr hohem und hohem Risiko zuerst angezeigt werden.

Dashboard und detaillierte Reports

Das integrierte Dashboard bietet eine Übersicht über Coaching-Kampagnen, Erkennungsregeln und erkannte Sicherheitsereignisse. Detaillierte Reports liefern Erkenntnisse über die Sicherheitsrisiken Ihrer Organisation und helfen dabei, Trends bei den riskanten Aktivitäten Ihrer Nutzerinnen und Nutzer im Laufe der Zeit zu beobachten.

SecurityCoach ist auch mit dem Risk Score verknüpft. Daher erhalten Sie von SmartRisk Agent™ aussagekräftigen Daten und Kennzahlen.

Einfache Nutzerzuordnung

Nutzerdaten von Ihrem Identitätsanbieter oder aus einem Verzeichnis werden mit Ihren Sicherheitsereignisprotokollen kombiniert, um Nutzerzuordnungsregeln zu erstellen. Dank zahlreicher integrierter Nutzerzuordnungsregeln und der Möglichkeit, benutzerdefinierte Regeln zu erstellen, ist die Konfiguration zur automatischen Zuordnung von Nutzerinnen und Nutzern einfach.

Empfehlungen zu Kampagnen

SecurityCoach empfiehlt Echtzeit-Coaching-Kampagnen, die optimal zu Ihren Erkennungsregeln passen. Sie können SecurityTips aus unterschiedlichen Kategorien von riskantem Verhalten auswählen.

Regelbasierte Automatisierung

Basierend auf den Regeln Ihrer vorhandenen Sicherheitsinfrastruktur und den definierten Nutzerinnen und Nutzern mit hohem Risiko können Sie für Ihre Echtzeit-Coaching-Kampagne die Häufigkeit und die Art der SecurityTips festlegen, die Nutzerinnen und Nutzer mit Risiko erhalten.

Umfassender SecurityTip-Katalog

In unserem umfangreichen Katalog stehen zahlreiche Inhalte für Ihre Kampagnen bereit – darunter Hunderte SecurityTips, auch in Form von GIFs und Videos, zu über 60 verschiedenen Themen. Freuen Sie sich auf exklusives SecurityTip-Material von unserem „Inside Man“ AJ, der Ihre Nutzerinnen und Nutzer in Echtzeit coacht.

Social-Engineering-Indikatoren

Versenden Sie im Rahmen Ihrer Phishing-Kampagnen aus dem Security Awareness Training von KnowBe4 auch SecurityTips über SecurityCoach, in denen Nutzerinnen und Nutzer über Social-Engineering-Indikatoren (SEI) oder Warnsignale aufgeklärt werden, die ihnen eventuell entgangen sind.

Leistungsstarke Sicherheitsintegrationen

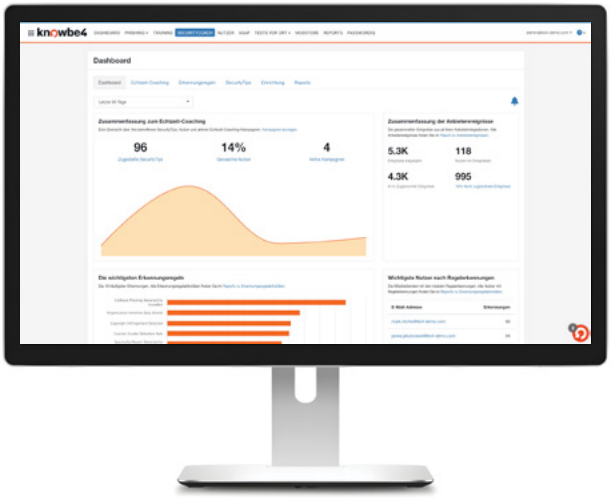
SecurityCoach lässt sich mithilfe von Standard-APIs schnell und einfach in Ihre vorhandenen Sicherheitsprodukte von CrowdStrike, Microsoft, Cisco, Netskope, Zscaler und anderen Anbietern integrieren. Unser Technologiepartner-Ökosystem wächst schnell, da wir unsere Kunden umfassender unterstützen und Ihre Sicherheitskultur stärken möchten.

Sie richten in Ihrer KnowBe4-Konsole eine Integration für Ihre Sicherheitsplattformen ein, damit Daten an SecurityCoach übermittelt werden können. Danach kann verfolgt werden, wenn bestimmte Aktionen entdeckt werden. Eine Integration ist schnell und einfach eingerichtet. In unserer Wissensdatenbank stehen Integrationsleitfäden für jeden Anbieter zur Verfügung. Nach der Integration werden Ereignisse und andere Daten von Ihren Sicherheitsplattformen auf Ihrem SecurityCoach-Dashboard angezeigt.

Endpunkt-sicherheit	Bitdefender, Carbon Black., CROWDSTRIKE, CYLANCE, paloalto NETWORKS, Microsoft, Malwarebytes, SentinelOne, SONICWALL, SOPHOS
Identitäts- und Zugriffsverwaltung	Google, okta
Kommunikation	slack, Microsoft Teams, Google Chat
E-Mail- und Internetsicherheit	cisco, CLOUDFLARE, FORTINET, Google, Microsoft, mimecast, netskope, proofpoint., splunk>, zscaler

Mit der **kostenlosen Testversion** von **SecurityCoach** können Sie Ihre Sicherheitsprodukte einbinden und erhalten einen Überblick über das Ausmaß riskanter Verhaltensweisen Ihrer Nutzerinnen und Nutzer.

Mehr erfahren



knowbe4

KnowBe4 Germany | Rheinstr. 45/46, 12161 Berlin – Deutschland | KnowBe4.de |
+49 30 34 64 64 60 | kontakt@knowbe4.com

Andere genannte Produkt- und Firmennamen sind eventuell Marken und/oder eingetragene Marken ihrer jeweiligen Unternehmen.

Copyright © 2025 KnowBe4. Alle Rechte vorbehalten.