SecurityCoach

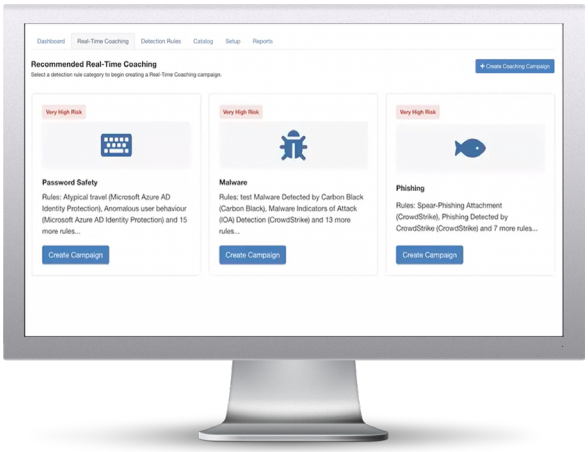
KnowBe4
Human error. Conquered.

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 Nutzer:innen auszutricksen und die Cybersicherheitsmaßnahmen Ihrer Organisation zu umgehen. Laut dem Verizon Data Breach Investigations Report 2022 ist der Faktor Mensch an 82 % aller Datenpannen beteiligt. Entlasten Sie Ihr gestresstes Sicherheitsteam, indem Sie die Anzahl der Warnmeldungen aufgrund von wiederholt riskantem Verhalten Ihrer Mitarbeiter:innen senken.

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



Wesentliche Vorteile

- Besseres Verständnis und Festigung der Kenntnisse der Nutzer:innen in Bezug auf Security Awareness Training und der geltenden Sicherheitsrichtlinien durch Echtzeit-Coaching zum tatsächlichen Verhalten
- Nutzung des vorhandenen Security Stack für das Echtzeit-Coaching von Nutzer:innen mit Risiko und optimale Nutzung getätigter Investitionen
- Benutzerdefinierte Kampagnen für Nutzer:innen 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

Was ist SecurityCoach?

SecurityCoach ist das erste Echtzeit-Sicherheitscoaching, das IT- und Sicherheitsteams dabei unterstützt, die größte Angriffsfläche Ihrer Organisation zu schützen **– Ihre Mitarbeiter:innen.**

SecurityCoach stärkt Ihre Sicherheitskultur, indem Ihre Nutzer:innen bei riskantem Verhalten ein Echtzeit-Sicherheitscoaching erhalten. Sie können Echtzeit-Coaching-Kampagnen basierend auf Ihrem Security Stack konfigurieren, mit denen Ihren Nutzer:innen kontextbezogene SecurityTips mit Informationen aus Ihrem Security Awareness Training und Ihren Sicherheitsrichtlinien angezeigt werden. Dadurch werden die erworbenen Kenntnisse gefestigt und die Nutzer:innen können zudem die mit ihrem Verhalten verbundenen Risiken besser nachvollziehen.

SecurityCoach lässt sich in die New-School Security Awareness Training Platform von KnowBe4 und in Ihren Security Stack integrieren, um Echtzeit-Coaching als Reaktion auf riskantes sicherheitsrelevantes Verhalten von Nutzer:innen bereitzustellen.

Gründe für SecurityCoach

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

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. Ihr Security Stack generiert Warnungen, die dann von SecurityCoach analysiert werden, um jene Ereignisse zu identifizieren, die auf das riskante sicherheitsrelevante Verhalten Ihrer Nutzer:innen zurückgehen.

Wenn ein:e Nutzer:in beispielsweise einen infizierten E-Mail-Anhang öffnet, der möglicherweise Ransomware enthält, die sich in Ihrem Netzwerk verbreiten könnte, oder wenn ein:e Nutzer:in versucht, eine Website mit unzulässigem Inhalt auf seinem:ihrem Arbeitscomputer aufzurufen, erkennen Ihre Sicherheitsprodukte diese Aktivitäten und generieren eine Ereigniswarnung. SecurityCoach ermittelt das Ereignis und sendet über Microsoft Teams, Slack oder per E-Mail einen Echtzeit-SecurityTip an diese:n Nutzer:in, in dem das Sicherheitsrisiko benannt und erläutert wird. Sie können Coaching-Kampagnen für Nutzer:innen mit Risiko basierend auf jenen Ereignissen einrichten, die Ihre Netzwerk-, Identitäts-, Internetsicherheits- oder sonstigen Anbieter Ihres Security Stack erfassen. Mithilfe dieser Kampagnen können Sie Ihre Nutzer:innen in dem Moment coachen, in dem sie sich riskant verhalten, und so in Echtzeit Feedback geben. Die in Ihrem Security Awareness Training vermittelten Kenntnisse werden gefestigt. Echtzeit-Coaching-Kampagnen können dabei basierend auf Ihren eigenen Sicherheitsrichtlinien und mithilfe der Automatisierungseinstellungen von SecurityCoach ganz einfach konfiguriert werden.

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

SecurityCoach-Workflow

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

Wichtige Funktionen

Echtzeit-Coaching
Mithilfe von Echtzeit-Coaching-Kampagnen können Sie Ihre Nutzer:innen in Echtzeit über ein riskantes Verhalten informieren. Wenn eine riskante Aktivität erkannt wird, erhalten Ihre Nutzer:innen 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 Nutzer:innen über Microsoft Teams, Slack 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 Security-Stack-Anbietern lassen sich über die jeweiligen Anbieter-APIs schnell und einfach integrieren. Unser Technologiepartner-Ökosystem wächst schnell, da wir möglichst viele Kunden unterstützen und die Human Firewall stärken 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.

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

Einfache Nutzerzuordnung
Nutzerdaten von Ihrem Identitätsanbieter oder 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 Nutzer:innen einfach.

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

Regelbasierte Automatisierung
Basierend auf den Regeln Ihres Security Stack und den definierten Nutzer:innen mit hohem Risiko können Sie für Ihre Echtzeit-Coaching-Kampagne die Häufigkeit und die Art der SecurityTips festlegen, die Nutzer:innen mit Risiko erhalten.

Starker SecurityTip-Katalog
Sie können anhand unseres umfangreichen und ständig wachsenden Katalogs Kampagnen erstellen. Bisher stehen 200 SecurityTips zu 60 verschiedenen Themen zur Verfügung, viele davon in 34 Sprachen.

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 möglichst viele Kunden unterstützen und die Human Firewall 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.

Informationen über das Zusammenspiel zwischen Anbieterintegrationen und SecurityCoach finden Sie unter www.knowbe4.com/integrations.