SecurityCoach

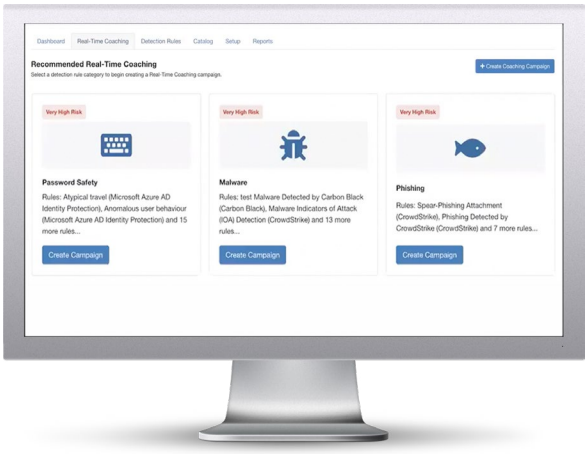
KnowBe4
Human error. Conquered.

Proposer un coaching en temps réel pour réagir à un comportement dangereux de l'utilisateur

Améliorer la culture de la sécurité dans son ensemble et réduire le risque

Les attaques par ingénierie sociale menacent constamment vos utilisateurs, qui sont visés par des personnes malveillantes employant tous les moyens possibles pour percer les défenses de cybersécurité de votre organisation. Le rapport Data Breach Investigations Report 2022 de Verizon indique que le facteur humain joue un rôle dans 82 % des cas. Vos équipes de sécurité sont submergées et stressées par leur quantité de travail ; elles ont besoin d'un peu de répit, sans être gênées par les alertes déclenchées par les comportements dangereux et répétés de vos employés.

Et s'il existait un moyen de récupérer les données d'événements utilisateur détectés par votre système de sécurité existant afin de fournir un coaching en temps réel à vos utilisateurs en réponse aux erreurs de sécurité tout en réduisant le nombre d'alertes que reçoit l'équipe de votre centre des opérations de sécurité (SOC) déclenchées par ces comportements dangereux et répétés ? **Avec SecurityCoach™, c'est désormais possible.**



Avantages clés

- Aider les utilisateurs à mieux comprendre et retenir la formation sur la sécurité ainsi que les politiques de sécurité en place grâce à un coaching en temps réel portant sur le comportement en situation réelle
- Tirer parti de votre système de sécurité existant pour fournir un coaching en temps réel à vos utilisateurs à risque et dégager plus de valeur de vos investissements existants
- Créer des campagnes personnalisées destinées aux utilisateurs ou rôles à risque élevé constituant des cibles de premier choix pour les cybercriminels, ou qui adoptent systématiquement un comportement à risque
- Évaluer et préparer des rapports sur l'amélioration des pratiques de sécurité à l'échelle de votre organisation et justifier un investissement continu
- Réduire la charge de travail de votre SOC et améliorer son efficacité en diminuant le nombre d'alertes déclenchées par des comportements à risque répétés

Qu'est-ce que SecurityCoach ?

SecurityCoach est le premier produit de coaching sur la sécurité en temps réel. Il a été conçu dans le but d'aider vos équipes informatiques et chargées des opérations de sécurité à mieux protéger la plus vaste surface d'attaque de votre organisation **: vos employés.**

SecurityCoach consolide votre culture de la sécurité en proposant un coaching en temps réel sur la sécurité à vos utilisateurs en réponse à leur comportement dangereux en matière de sécurité. Appuyez-vous sur votre système de sécurité existant pour configurer des campagnes de coaching en temps réel et fournir instantanément des SecurityTips en contexte qui complètent votre formation sur la sensibilisation à la sécurité et rappellent à vos utilisateurs vos politiques en la matière. Les utilisateurs retiennent davantage les informations transmises et comprennent mieux les risques associés à leurs comportements.

SecurityCoach s'intègre à la plateforme de formation sur la sensibilisation à la sécurité nouvelle génération de KnowBe4 ainsi qu'à votre système de sécurité existant pour fournir un coaching en temps réel pour répondre au comportement à risque de l'utilisateur final.

Pourquoi choisir SecurityCoach ?

Votre organisation fait face à un nombre croissant d'attaques par ingénierie sociale ciblant les utilisateurs. Pour vous défendre au mieux contre celles-ci, il est primordial de développer une forte culture de la sécurité à l'échelle de l'organisation, qui implique vos utilisateurs et rappelle l'importance de suivre les politiques de sécurité de l'organisation pour renforcer votre pare-feu humain.

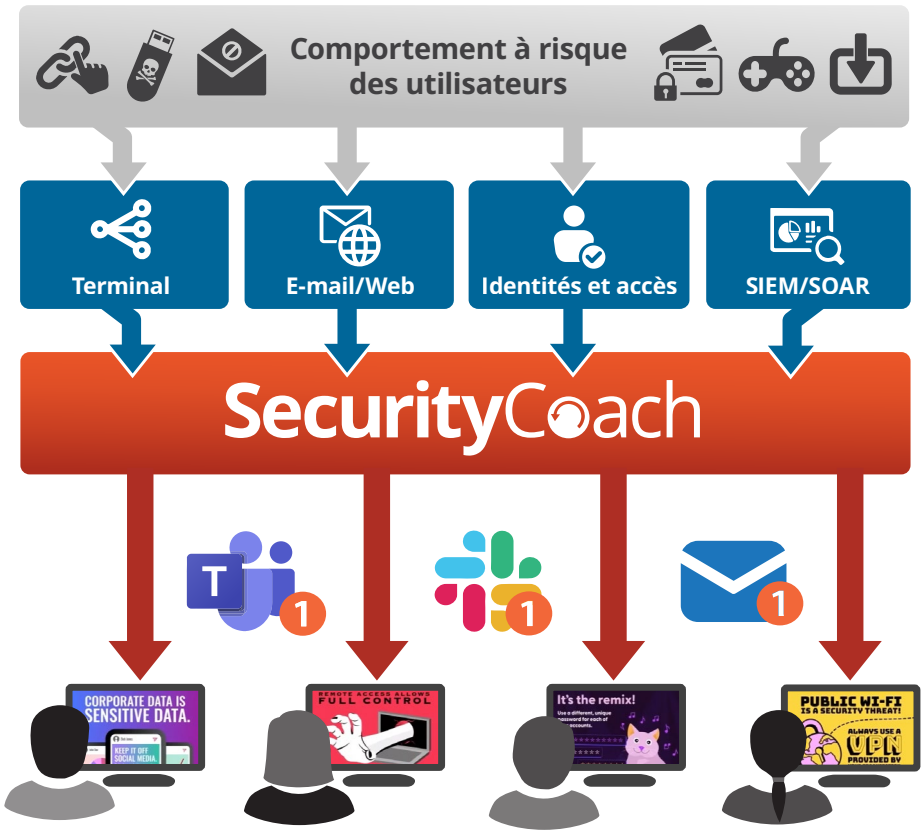
SecurityCoach constitue un gain de temps considérable pour votre équipe SOC très occupée en réduisant le nombre d'alertes déclenchées par des comportements dangereux et répétés. L'équipe SOC peut ainsi se concentrer sur les menaces les plus graves.

Comment fonctionne SecurityCoach ?

SecurityCoach se base sur des API standard pour s'intégrer rapidement et facilement à vos produits de sécurité existants Microsoft, CrowdStrike, Cisco, et bien d'autres encore. Les alertes générées par votre système de sécurité sont analysées par SecurityCoach pour identifier les événements liés à un comportement de vos utilisateurs menaçant la sécurité.

Par exemple, si un utilisateur ouvre une pièce jointe infectée susceptible de transmettre un rançongiciel sur votre réseau ou tente d'accéder à un site Web au contenu interdit depuis son ordinateur professionnel, vos produits de sécurité détectent la manipulation et créent une alerte d'événement. SecurityCoach identifie l'événement en question, puis envoie un SecurityTip en temps réel à l'utilisateur concerné sur Microsoft Teams, Slack ou par e-mail qui lui signale que ce qu'il est en train de faire représente un risque de sécurité et lui explique pourquoi. Vous pouvez définir des campagnes de coaching afin de cibler les utilisateurs à risque sur la base de ces événements depuis votre réseau, vos identités, votre sécurité Web et d'autres fournisseurs au sein de votre système de sécurité. Ces campagnes vous permettent d'informer vos utilisateurs dès qu'ils adoptent un comportement à risque en le commentant en temps réel et en rappelant les campagnes de formation sur la sensibilisation à la sécurité que vous avez mises en place. Appuyez-vous sur vos propres politiques de sécurité et aidez-vous des paramètres d'automatisation de SecurityCoach pour configurer facilement des campagnes de coaching en temps réel.

SecurityCoach insiste sur la nécessité de suivre les politiques de sécurité de votre organisation dans le but d'améliorer les comportements des utilisateurs et de consolider votre culture de la sécurité dans sa globalité.



Flux de travail de SecurityCoach

1. Les fournisseurs de systèmes de sécurité que vous intégrez à votre console KnowBe4 surveillent l'apparition d'activités à risque sur les appareils de vos utilisateurs.
2. Les données des alertes sont ensuite transmises à SecurityCoach, qui les analyse et détermine quelles menaces constituent les meilleures opportunités de coaching en temps réel pour vos utilisateurs.
3. Lorsqu'un comportement à risque est détecté chez un utilisateur, SecurityCoach lui envoie automatiquement une notification SecurityTip en temps réel sur Microsoft Teams, Slack ou par e-mail.

Fonctionnalités clés

Coaching en temps réel
Les campagnes de coaching en temps réel vous permettent d'informer vos utilisateurs sur leurs comportements à risque en temps réel. Lorsqu'une activité à risque est détectée, vos utilisateurs reçoivent une notification d'entraînement sous forme de SecurityTip portant sur l'activité en question et expliquant comment éviter de la reproduire.

Notifications SecurityTip
Dès qu'un comportement à risque est détecté chez un utilisateur, SecurityCoach lui envoie directement une notification SecurityTip en temps réel sur Microsoft Teams, Slack ou par e-mail. Ces notifications instantanées renforcent considérablement votre programme de sensibilisation à la sécurité.

Intégrations basées sur les API
Servez-vous des API des fournisseurs pour une intégration simple et rapide à vos fournisseurs de système de sécurité existants, comme Microsoft, Cisco, Netskope, Zscaler, et plus encore. Notre écosystème de partenariats technologiques se développe de jour en jour pour accompagner nos clients et renforcer le pare-feu humain.

Règles de détection intégrées
Les règles de détection précisent quelles sont les activités à risque que vous souhaitez surveiller à l'aide des données transmises par vos fournisseurs de sécurité intégrés. SecurityCoach recommande des règles de détection portant sur les thèmes de sécurité les plus courants en fonction de leur priorité, les règles à Risque très élevé et Risque élevé étant proposées en premier.

Recommandations de campagnes
SecurityCoach recommande les campagnes de coaching en temps réel les mieux adaptées à vos règles de détection. Vous pouvez sélectionner des SecurityTips portant sur différents types de comportements à risque.

Faciliter le mappage utilisateur
Les données d'utilisateurs provenant de votre fournisseur d'identité ou de votre annuaire sont associées à vos journaux d'événements de sécurité pour élaborer des règles de mappage utilisateur. Grâce à une grande diversité de règles de mappage utilisateur intégrées et la possibilité de créer des règles personnalisées, vous pouvez facilement configurer ces règles afin de mapper automatiquement les utilisateurs.

Tableau de bord et rapports détaillés
Le tableau de bord intégré récapitule l'ensemble des campagnes de coaching, des règles de détection et des événements de sécurité détectés. Les rapports détaillés fournissent des informations sur les risques de sécurité qu'encourt votre organisation et vous aident à suivre les tendances de vos utilisateurs en termes d'activités à risque au fil du temps.

Automatisation basée sur les règles
En vous appuyant sur les règles de votre système de sécurité et vos utilisateurs ou rôles considérés à risque élevé, vous êtes en mesure de configurer votre campagne de coaching en temps réel afin de déterminer la fréquence et le type des SecurityTips reçus par les utilisateurs à risque.

Vaste catalogue de SecurityTips
Vous avez la possibilité de créer des campagnes à l'aide de notre catalogue complet regroupant 200 SecurityTips sur 60 thèmes différents, pour la plupart disponibles dans 34 langues. Nous y rajoutons régulièrement de nouvelles entrées pour couvrir davantage de sujets.

Intégrations de sécurité performantes

SecurityCoach s'appuie sur des API standard pour s'intégrer rapidement et facilement à vos produits de sécurité existants CrowdStrike, Microsoft, Cisco, Netskope, Zscaler et bien d'autres encore. Notre écosystème de partenariats technologiques se développe de jour en jour pour accompagner nos clients et renforcer le pare-feu humain.

Vous devrez configurer une intégration dans votre console KnowBe4 afin de permettre à SecurityCoach d'accéder à vos plateformes de sécurité. Grâce à ces intégrations, SecurityCoach est capable de réaliser un suivi lorsque certaines actions sont détectées. Configurer une intégration est un processus simple et rapide, et nous vous proposons des guides d'intégration consacrés à chacun des fournisseurs présents dans notre base de connaissances. Une fois l'intégration terminée, les événements et les autres données provenant de vos plateformes de sécurité apparaîtront sur votre tableau de bord SecurityCoach.

Pour en savoir plus sur le fonctionnement de ces intégrations du fournisseur à SecurityCoach, rendez-vous sur www.knowbe4.com/integrations.