SecurityCoach
Informe de integración

KnowBe4
Human error. Conquered.

CROWDSTRIKE

La integración de SecurityCoach de KnowBe4 con Falcon Insight de Crowdstrike le permite aprovechar las alertas de seguridad de Falcon en relación con malware, ransomware, robo de credenciales y mucho más para enviar SecurityTips en tiempo real a los usuarios finales que se ponen en riesgo.

El problema

- Los ciberdelincuentes utilizan cada vez más técnicas de ingeniería social como el phishing (suplantación de identidad), el spear phishing (suplantación de identidad específica) y la suplantación de identidad para manipular a sus empleados, lo que da lugar a tiempos de inactividad y a violaciones de seguridad.
- De acuerdo con el Informe de investigaciones sobre la violación de seguridad de datos de Verizon de 2022, el factor humano forma parte del 82 % de las violaciones de seguridad.
- El equipo del Centro de Operaciones de Seguridad (Security Operations Center, SOC) recibe un promedio de 11 000 alertas al día, lo que genera el desgaste y el agotamiento de los analistas.
- Los usuarios olvidan el 50 % de la información que adquieren en un día y el 90 % en una semana si no reciben un refuerzo interesante y frecuente de su capacitación.

Cómo gestionar el problema

- SecurityCoach utiliza las API de CrowdStrike para analizar alertas e identificar comportamientos de seguridad riesgosos por parte de los usuarios finales.
- Puede configurar fácilmente campañas de asesoramiento en tiempo real utilizando sus propias políticas de seguridad y las diferentes categorías de comportamientos riesgosos.
- SecurityCoach ofrece los SecurityTips contextuales y en tiempo real que usted seleccione a partir de la biblioteca de plantillas gráficas ya preparadas y de las notificaciones personalizadas opcionales.

Ejemplos de casos de uso

- Prevención de malware: cuando CrowdStrike detecta malware, SecurityCoach puede asignarlo a un usuario determinado y enviarle un SecurityTip específico para evitar el malware.
- Seguridad de credenciales: cuando CrowdStrike detecta el robo de contraseñas, SecurityCoach puede instruir a los usuarios afectados sobre la seguridad de las contraseñas y la autenticación multifactor.

Beneficios y resultados

- Reducción mensurable del riesgo y fortalecimiento general de la cultura de la seguridad.
- Mejor comprensión y retención de su capacitación en concientización sobre seguridad, prácticas recomendadas y políticas de seguridad implementadas.
- Valor adicional considerable de sus inversiones actuales en KnowBe4 y CrowdStrike.
- Ahorro de tiempo para los analistas del SOC y mejora de la eficacia mediante la automatización y la reducción del ruido de alerta ocasionado por usuarios que repiten comportamientos de seguridad riesgosos.

Acerca de SecurityCoach de Knowbe4

SecurityCoach ofrece asesoramiento sobre seguridad en tiempo real a los usuarios en respuesta a comportamientos riesgosos para la seguridad. Según las reglas de su pila de software de seguridad actual, puede configurar su campaña de asesoramiento en tiempo real para determinar la frecuencia y el tipo de SecurityTip que se enviará a los usuarios en el momento en que se detecte un comportamiento riesgoso.

Acerca de CrowdStrike

CrowdStrike Inc., líder mundial en ciberseguridad, revoluciona el concepto de seguridad para la era de la nube con una plataforma de protección de terminales diseñada desde cero para detener las violaciones de seguridad. La arquitectura de agente único y ligero de la plataforma Falcon de CrowdStrike aprovecha la inteligencia artificial a escala de la nube, y ofrece protección y visibilidad en tiempo real en toda la empresa, lo que previene ataques en terminales dentro y fuera de la red. Con la tecnología patentada de CrowdStrike Threat Graph, Falcon de CrowdStrike correlaciona más de dos billones de eventos relacionados con terminales a la semana en tiempo real procedentes de todo el mundo, lo que impulsa una de las plataformas de seguridad más avanzadas del mundo.