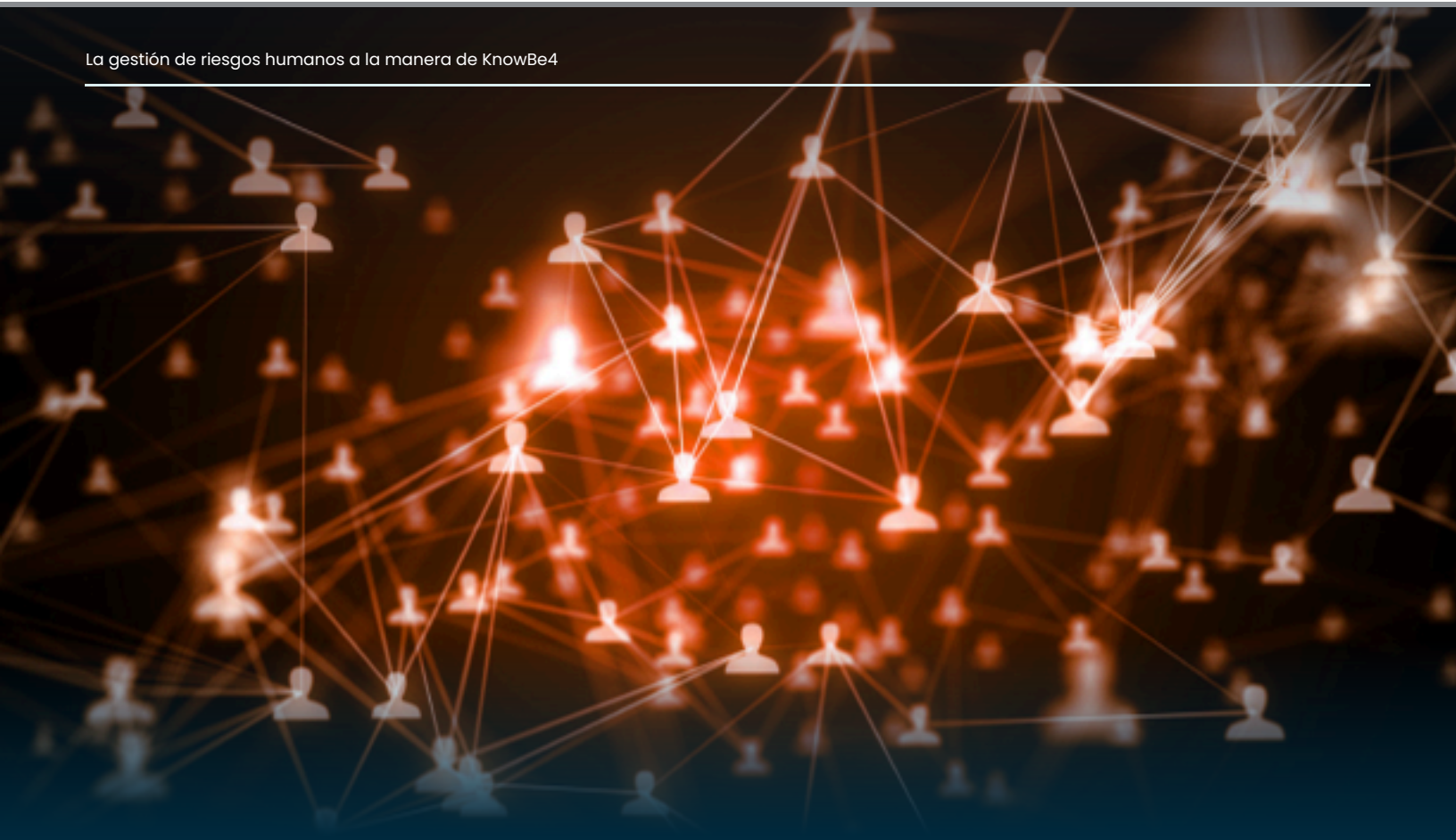
knowbe4

SEGURIDADAMÉRICA.com
Fortaleciendo Internet

La gestión de riesgos humanos a la manera de KnowBe4

Le presentamos AIDA: Artificial Intelligence Defense Agents



Introducción

El aumento de los ciberataques impulsados con IA está captando la atención de todos los profesionales de seguridad de la información.

Más del 95 % de profesionales de ciberseguridad afirma que el phishing generado por IA es más difícil de detectar, y Microsoft informa que los correos electrónicos de phishing generados por IA tienen 4,5 veces más éxito que aquellos creados de manera manual.

El problema no es estar al tanto de la amenaza. El problema es que, en la realidad, los programas tradicionales en concientización sobre seguridad no pueden adaptarse con la suficiente rapidez para seguir el ritmo.

Este avance tecnológico en manos de malhechores generó un nuevo tipo de ataques de ingeniería social muy convincentes que son difíciles de combatir con capacitación en concientización sobre seguridad (SAT, por sus siglas en inglés) de carácter genérico.

Es hora de combatir la IA con IA. Para eso, llega KnowBe4 AIDA: Artificial Intelligence Defense Agents. AIDA es un paquete de agentes impulsados con IA que optimiza su enfoque a la gestión de riesgos humanos (HRM, por sus siglas en inglés) mediante varias tecnologías de IA a fin de preparar capacitaciones para usuarios personalizadas, adaptables y muy eficaces que cambien de verdad los comportamientos.

En este informe técnico, veremos la manera en que los agentes de AIDA pueden ayudar a optimizar su estrategia de HRM, y exploraremos casos de uso.

Qué abarca este informe

Hablemos de AIDA

AIDA es un paquete de agentes siempre activos que optimiza su enfoque hacia la gestión de riesgos relacionados con el factor humano (HRM, por sus siglas en inglés). Logra esto mediante varias tecnologías de IA a fin de preparar capacitaciones personalizadas, adaptables y muy eficaces para todos los usuarios con el objetivo de cambiar de verdad los comportamientos.

Al automatizar la generación de plantillas, la capacitación, las simulaciones de phishing y la generación de informes, AIDA reduce la carga administrativa de sus equipos de seguridad para que puedan concentrarse en proteger su red.

Un agente para gobernarlos a todos

Gracias a Orquestación con AIDA, esta automatización se extiende a la gestión completa del programa: evalúa continuamente el riesgo de cada usuario y proporciona de manera automática las pruebas y la capacitación adecuadas en el momento oportuno. Este paquete de agentes nativos de IA otorga la capacidad a los usuarios de convertirse en detectores activos de amenazas y fortalece así la defensa de su organización.

AIDA continuamente aprende y se adapta a las necesidades particulares de su organización para garantizar el máximo impacto y retorno de la inversión de sus iniciativas de concientización sobre seguridad. Por ejemplo, al reducir de un promedio de siete días a apenas unos segundos el tiempo que le lleva a la administración crear contenido de capacitación, AIDA le ahorra una cantidad considerable de tiempo a su equipo de seguridad.

A continuación, le presentamos un resumen de los agentes que componen el paquete de AIDA (más adelante en este informe técnico se exponen más detalles y casos de uso):

Agente de orquestación

AIDA automatiza la administración de programas mediante un enfoque que siempre está activo, y analiza de manera continua el riesgo de los usuarios para crear y programar automáticamente pruebas de seguridad contra el phishing (PST), capacitaciones sobre medidas correctivas y campañas continuas de capacitación.

- **Agente de capacitación sobre medidas correctivas:** Asigna automáticamente el contenido más relevante e interesante cuando sus usuarios no aprueban una prueba de phishing simulado.
- **Agente de capacitación continua:** Aborda de manera continua las brechas de conocimiento en la organización y asigna automáticamente contenido de capacitación personalizado a cada estudiante.
- **Agente de phishing:** Elimina la carga manual de las pruebas de seguridad, ya que crea, personaliza e implementa de forma autónoma ataques de phishing simulado sofisticados y adaptados a la función, el perfil de riesgo y las interacciones pasadas de sus usuarios.

Agente de generación de plantillas

AIDA aprovecha la IA generativa para crear plantillas de phishing muy realistas que pueden reflejar los vectores de ataque actuales. Los indicadores de ingeniería social (SEI, por sus siglas en inglés), o señales de alarma, se basan en el marco Phish Scale del Instituto Estadounidense de Estándares y Tecnología (NIST, por sus siglas en inglés).

Agente de generación de plantillas de devolución dellamada

Hace uso de la IA para crear plantillas de phishing que le permiten evaluar qué tan probable es que los usuarios caigan ante estafas de phishing de devolución de llamada, las cuales incluyen una combinación de técnicas de phishing y vishing.

Agente de páginas de destino recomendadas

Sugiere de manera automática páginas de destino contextualmente adecuadas para acompañar sus plantillas de phishing generadas por AIDA, a fin de garantizar una experiencia de prueba completa y educativa que refuerce los objetivos de aprendizaje.

Agente de actualización de conocimientos

AIDA proporciona actualizaciones de conocimientos breves en intervalos óptimos y garantiza que sus usuarios realmente apliquen los conceptos de seguridad críticos.

Agentedecuestionariossobrepolíticas

AIDA genera cuestionarios inteligentes basados en las políticas de seguridad y cumplimiento específicas de su organización. Esto garantiza que sus usuarios no solo reconozcan, sino que verdaderamente comprendan las pautas que se espera que sigan.

Agente de contenido de capacitación sobre deepfake

Genera contenido de capacitación sobre deepfake personalizado que incluye a una persona de alto rango de su organización. Este contenido generado por IA demuestra lo convincente que se ha vuelto la ingeniería social basada en IA, y brinda una guía clara y práctica para detectar estos ataques.

Agente de SAPA personalizada

El agente de Evaluación personalizada de la competencia en concientización sobre seguridad (SAPA) crea evaluaciones personalizadas del riesgo utilizando la documentación y las políticas específicas de su organización para evaluar a los usuarios, en lugar de generar una concientización genérica. Utiliza la IA para seleccionar preguntas relevantes a partir de una gran base de datos a fin de crear una evaluación específica para la organización en función de su entorno.

La conexión con la gestión de riesgos humanos

LaHRMahoraes la maneraprincipalde atenderla necesidad permanentede sólidas culturas de seguridad en las organizaciones de todos los tamaños. El concepto no se enfoca solo en ofrecer SAT con una frecuencia determinada. La meta es crear una cultura de la seguridad positiva a través de tres tácticas principales:

1. Cuantificar el riesgo humano mediante la detección y la medición del comportamiento humano
2. Utilizar esas mediciones para implementar contenido de capacitación pertinente y personalizado
3. Definir actualizaciones de conocimientos recurrentes para garantizar que los usuarios sepan cómo protegerse de los riesgos cibernéticos de mayor prevalencia e impacto

La SAT tradicional ya no es eficaz en su complejo entorno de trabajo. Un evento de capacitación por año no es suficiente. Además, los usuarios tienen agendas cada vez más cargadas, por lo cual, en las capacitaciones, debe aprovecharse bien el tiempo.

Una estrategia de HRM le permite ofrecer contenido pertinente y atractivo que cambie el comportamiento del usuario y tenga eco en diferentes roles, departamentos e incluso idiomas. AIDA es el pilar de esta iniciativa.

Siga leyendo para conocer más sobre cada agente.

Los agentes de AIDA

Antes de hablar de estos agentes, exploremos un recurso de KnowBe4 clave para todos ellos: **SmartRisk Agent™ de KnowBe4**. Esta función ofrece información y parámetros procesables, llamados **puntaje de riesgo**, para que pueda comprender las fortalezas y las debilidades de la seguridad de su organización.

SmartRisk Agent utiliza los datos de comportamiento de los usuarios finales de todos los productos de KnowBe4 para medir el riesgo cibernético de los seres humanos. Los puntajes de riesgo multidimensionales de este agente están diseñados para simplificarle la detección de posibles problemas en los niveles del usuario, el grupo y la organización. Cuantos más productos KnowBe4 use, obtendrá mejor información.

Veamos en detalle las capacidades de cada agente y algunos casos de uso.

Agente de orquestación

Lo que hace

Orquestación con AIDA es un sistema siempre activo e impulsado por IA que gestiona y personaliza automáticamente las SAT y las pruebas de seguridad contra el phishing (PST) de KnowBe4 para reducir el riesgo de los usuarios. AIDA utiliza IA para generar de manera inteligente plantillas de phishing y las envía automáticamente a los usuarios.

AIDA escala de forma automática la dificultad de cada prueba en función del desempeño de los usuarios. El sistema utiliza contenido personalizado y cambios realistas en el logotipo para lograr que las simulaciones sigan siendo relevantes y adecuadamente desafiantes.

Incluso teniendo habilitado este sistema, usted conserva el control completo para ajustar en detalle el comportamiento del sistema y supervisar toda la actividad.

Cómo usarlo

Con el agente de orquestación, lo que usted hace es definir “planes” a fin de limitar la frecuencia de pruebas y capacitaciones para grupos de usuarios, mientras que AIDA decide de manera independiente a quién poner a prueba, qué vectores de ataque utilizar y cuál es el momento óptimo para reducir con eficacia el riesgo de la organización.

El agente de orquestación gestiona estos tres agentes para desarrollar los siguientes planes:

- **Agente de capacitación sobre medidas correctivas:** garantiza que cada uno de sus usuarios, independientemente de su cargo o ubicación, reciba capacitación personalizada según sus riesgos, necesidades y estilo de aprendizaje específicos. Este recurso permite optimizar la retención y la aplicación real de sus prácticas recomendadas de seguridad.
- **Agente de capacitación continua:** asigna automáticamente capacitaciones periódicas a los usuarios a partir de sus perfiles únicos de riesgo.
- **Agente de phishing:** proporciona ejercicios de phishing específicos para cada persona y función.

Casos de uso

- **Fortalecimiento de puntos débiles en cuanto al phishing**: a partir de las respuestas de los usuarios o los malos resultados de pruebas de phishing simulado específicas, asigne automáticamente capacitaciones que les enseñen a los usuarios las estrategias y las tácticas de phishing específicas antes de que las vean en la vida real.
- **Incorporación de nuevos miembros del personal**
  Evalúe el puntaje de riesgo de los nuevos miembros del personal y sugiera una SAT personalizada para la base de conocimientos que ya poseen mediante grupos inteligentes dirigidos.

Agente de generación de plantillas

Lo que hace

Elagentedegeneración de plantillas produce correos electrónicos de phishing muy convincentes y personalizados para las necesidades y el perfil de riesgo específicos de su organización mediante el poder de la IA generativa integrada. El agente puede diseñar diversos escenarios de phishing en varios idiomas y con diferentes niveles de dificultad, tonos y vectores de ataque a fin de garantizar que sus usuarios estén preparados para todo el abanico de amenazas que podrían encontrar en la vida real.

Cómo usarlo

Usted puede configurar fácilmente diferentes variables, como el idioma, el lugar y el vector de ataque. Configure la dificultad de los correos electrónicos de phishing simulado seleccionando indicadores de ingeniería social (SEI) específicos o eligiendo un nivel de dificultad predefinido. Las plantillas, una vez generadas, se pueden consultar, editar y guardar para el futuro, lo cual le ahorra tiempo valioso a la hora de crear y gestionar un buen programa de simulación de phishing.

Casos de uso

- **Pruebas de phishing en varios idiomas**
  Prepare e implemente rápidamente correos electrónicos de phishing en varios idiomas para una fuerza de trabajo global. El generador de plantillas hasta puede adaptar el texto de los correos electrónicos a una región específica con las expresiones, los matices y los estilos culturales locales.

- **Respuesta rápida ante las amenazas emergentes**
  ¿Halló un ataque totalmente nuevo en la vida real? Solo necesita unos minutos con el generador de plantillas para diseñar un ataque de phishing simulado similar que prepare a su fuerza de trabajo para lo que se viene.

Agente de generación de plantillas de devolución de llamada

Lo que hace

El agente de generación de plantillas de devolución de llamada crea ataques de phishing simulados de devolución de llamada, en los cuales la meta principal es lograr que el usuario llame a un número de teléfono específico, en lugar de hacer clic en un enlace. El agente AIDA genera audios de saludos y respuestas (que se oyen luego de que el usuario responde al saludo), así como traducciones para ambos, además del texto del cuerpo del correo electrónico.

Cómo usarlo

Lasplantillas de devolución de llamada se crean al igual que las plantillas de phishing basadas en correo electrónico. Elija "Creación rápida" para una generación de forma ágil, o ajuste el tono, la dificultad, la personalización y los idiomas. Una vez generados, los guiones de saludo y respuesta se pueden editar por completo para maximizar la personalización.

Casos de uso

- **Atraso de facturas urgentes**
  Envíe a usuarios específicos un correo electrónico donde se reclame un pago vencido o donde se afirme que una suscripción está a punto de renovarse automáticamente. El objetivo es lograr que el usuario llame al número provisto para discutir el monto o cancelar el servicio. AIDA crea un correo electrónico que ejerce mucha presión junto con un audio de saludo simulado del servicio al cliente para cuando el usuario realiza la llamada.

- **Fraude del director ejecutivo (CEO)** (suplantación de identidad ejecutiva)
  El usuario recibe un mensaje que aparenta provenir de la persona responsable de la dirección ejecutiva o de los altos mandos ejecutivos donde se solicita la atención inmediata del usuario sobre un asunto urgente. La meta es convencer al usuario de llamar a un número para "verificar" los detalles o recibir instrucciones de manera oral. AIDA redacta un correo electrónico con el tono adecuado (p. ej., serio pero amable) y genera una respuesta de voz que imita durante la llamada a un miembro ejecutivo o a su asistente.

Agente de páginas de destino recomendadas

Lo que hace

Elagente de páginas de destino recomendadas funciona junto con el agente de generación de plantillas para sugerir páginas web relevantes y creíbles vinculadas a partir de correos electrónicos de phishing simulados. Juntos, estos agentes realizan la generación y optimización de plantillas en cuestión de segundos, en lugar de horas, lo cual respalda una experiencia de aprendizaje coherente para el usuario, con menos carga para usted.

Cómo usarlo

Cuandose usael agente de generación de plantillas para crear una plantilla de phishing con un vector de ataque de enlace o código QR, el agente de páginas de destino recomendadas selecciona automáticamente una página de destino para esa plantilla. Puede ver la página seleccionada o elegir una diferente de manera manual durante el proceso de edición.

Casos de uso

- **Phishing para restablecer contraseñas**
  Use un correo electrónico de phishing simulado que aparenta ser una solicitud de restablecimiento de contraseña en combinación con una página de destino que solicite a los usuarios que ingresen información delicada en un formulario.

- **Confiar sin dejar de verificar**
  Use una prueba de phishing que se haga pasar por un correo electrónico interno con un enlace hacia una política nueva u otra información de la empresa en combinación con una página de destino que les pida a los usuarios que distingan entre los correos electrónicos internos de la organización y los correos electrónicos de phishing que hayan recibido. Estas son todas páginas de destino personalizadas con la marca que se pueden ajustar para mostrar cómo se ven los correos electrónicos internos de su organización.

Agente de actualización de conocimientos

Lo que hace

El agente deactualización de conocimientos ayuda a los usuarios a perfeccionar sus habilidades de ciberseguridad y ganar insignias con cuestionarios breves generados por IA y basados en escenarios: una forma rápida y divertida de repasar los puntos clave de su capacitación reciente.

Cómo usarlo

Ustedpuededefinir parámetros para las actualizaciones de conocimientos, como el plazo entre la finalización de una capacitación y la disponibilidad de la actualización de conocimientos. Una vez activado el recurso, los usuarios pueden acceder a sus actualizaciones de conocimientos en su Experiencia de aprendizaje, lo que simplifica la interacción con este elemento continuo de su proceso de aprendizaje.

Casos de uso

- **Refuerzo de laconcientización sobre phishing**
  Las actualizaciones de conocimientos generadas por IA y basadas en escenarios se pueden usar en una capacitación sobre medidas correctivas ofrecida luego de que el usuario haya hecho clic en un correo electrónico de phishing simulado, a fin de complementar la capacitación inicial. Este refuerzo sostenido ayuda a mantenerse alerta a las cambiantes tácticas de phishing.

- **Retención de las capacitaciones sobre cumplimiento**
  Las actualizaciones periódicas y enfocadas en temas clave del cumplimiento permiten que las organizaciones sometidas a requisitos regulatorios específicos demuestren la diligencia debida continua para mantener una cultura de cumplimiento, y potencialmente reducir los riesgos y mejorar los resultados de las auditorías.

Agente de cuestionarios sobre políticas

Lo que hace

Este agentede cuestionarios sobre políticas impulsado con IA genera automáticamente cuestionarios basados en las políticas específicas de su organización, lo que garantiza que los empleados no solo lean, sino también comprendan y retengan la información clave.

Cómo usarlo

En suconsola de KnowBe4, puede agregar la política de su organización en formato PDF. Tras agregar la política, puede editar y administrar preguntas de cuestionarios relacionadas con la política y, luego, crear una campaña de capacitación para asignar la política a sus usuarios. Una vez que haya asignado la política a una campaña, puede realizar un seguimiento del progreso y los reconocimientos de sus usuarios.

Casos de uso

- **Incorporaciónde personal nuevo**
  A través de cuestionarios sobre políticas personalizados, puede asegurarse de que el personal nuevo no solo consulte las políticas, sino que también demuestre haberlas entendido. Esto puede proporcionar un punto de referencia mensurable de la eficacia de la capacitación inicial sobre cumplimiento y reducir el riesgo de incumplimiento de las políticas debido a interpretaciones erróneas.

- **Revisión anual de las políticas**
  Optimice su proceso anual de revisión de las políticas usando el agente de cuestionarios sobre políticas para generar rápidamente cuestionarios actualizados que reflejen los cambios en las pautas y las reglas de la empresa. Las campañas de capacitación basadas en políticas ayudan a garantizar la retención de los conocimientos y ofrecen a los administradores métricas claras del nivel de comprensión de las políticas en toda la empresa, lo que permite identificar áreas donde se necesita más capacitación o aclaraciones.

Agente de contenido de capacitación sobre deepfake

Lo que hace

La función de capacitación sobre deepfake le permite crear videos deepfake simulados para personalizar todavía más la SAT. Al crear un deepfake de un miembro conocido del liderazgo o equipo ejecutivo de su organización, puede demostrar a los usuarios lo fácil que se puede suplantar la identidad de alguien. Estos videos están restringidos y vinculados a guiones pregrabados, lo cual garantiza que el contenido se utilice estrictamente para fines educativos.

Cómo usarlo

Se guía alos usuarios de la plataforma KnowBe4 durante el proceso de creación de cinco pasos. Para garantizar que los deepfakes se utilicen solo para fines educativos, KnowBe4 brinda una variedad de guiones grabados previamente que imitan el sentido de urgencia que suelen emplear las personas atacantes. Con el uso de un video enviado del sujeto del deepfake, el agente procesa el audio para clonar la voz. El audio se puede volver a generar de ser necesario.

Casos de uso

Elagente de contenido de capacitación sobre deepfake genera un activo de capacitación sobre deepfake seguro y controlado que logra lo siguiente:

- Demuestra lo convincentes que pueden ser las personas atacantes al hacerse pasar por alguien de confianza.
- Enseña al personal cómo evaluar las pistas de audio y video.
- Brinda orientación sobre qué hacer cuando algo parece extraño.

Agente de SAPA personalizada

Lo que hace

Elagentede SAPA personalizada es una evolución inteligente impulsada por AIDA de la Evaluación de la competencia en concientización sobre seguridad (SAPA) de KnowBe4. Mientras que las evaluaciones tradicionales brindan una referencia de confianza, el agente de SAPA personalizada conduce a las organizaciones hacia mediciones conscientes del entorno. Gracias a que primero comprende las políticas internas y el conjunto de seguridad específico de una organización, ofrece una evaluación personalizada que identifica las brechas específicas de conocimiento que afectan el perfil del riesgo único de la organización.

Cómo usarlo

El agentedeSAPA personalizada se utiliza para evaluar la concientización sobre seguridad, no para capacitar directamente a los usuarios. La administración debe completar una breve encuesta sobre el entorno para que el agente pueda comprender sus políticas, herramientas y flujos de trabajo, y luego analizar y ejecutar la evaluación. Los resultados ofrecen una clara visibilidad de las fortalezas, debilidades y tendencias de riesgo, lo cual ayuda a los equipos a planificar programas en concientización sobre seguridad más específicos y a medir el progreso con el paso del tiempo.

Casos de uso

- **Referencia con consciencia del entorno**
  En lugar de medir los conocimientos generales, la evaluación se alinea con sus políticas y tecnología internas para brindar al liderazgo un panorama más claro de dónde hay riesgos. Se recomienda asignar la primera SAPA luego de la prueba inicial de phishing, pero antes de la primera campaña de capacitación. Así se establece una referencia para medir el progreso a futuro.

- **Planificación impulsada por los datos**
  Utilice los datos de la evaluación para priorizar las correcciones y dar forma a las campañas de capacitación. Dado que los resultados se vinculan con la realidad de la organización, los equipos de seguridad pueden justificar con confianza las decisiones del programa y comunicar con precisión los riesgos al liderazgo.

Conclusión: ¿por qué elegir AIDA?

AIDAofrece unpaquete deagentes nativosdeIAquetransformanla manera deocuparsedela HRM.AIDAcapacitaasu organización para que se mantenga a la vanguardia usando la IA para vencer a las amenazas de la IA.

Esto es lo que AIDA les aporta a usted y su organización:

Ahorro de tiempo

Al reducir a unos pocos segundos el tiempo que le lleva al personal de administración crear capacitaciones de phishing y una SAT personalizada y continua para cada persona, AIDA le ahorra una cantidad considerable de tiempo a su equipo de seguridad.

Alineación con las normas de la industria

La alineación de AIDA con el marco Phish Scale del NIST garantiza que su SAT sea coherente con las iniciativas de seguridad más amplias de su organización.

Unificación de los equipos de seguridad

Mejore las relaciones, genere confianza y reduzca la fricción entre su equipo de seguridad y otros departamentos al garantizar que los usuarios estén alineados con los objetivos de seguridad.

Eficiencia convertida en ahorros presupuestarios

Al gestionar el riesgo relacionado con el factor humano de manera activa y eficiente, tendrá flexibilidad en su presupuesto de seguridad para invertir en otras iniciativas clave.

KnowBe4 le brinda a su organización la capacidad para ponerse por delante del phishing, vishing y deepfakes, y la gama completa de ingeniería social. En un entorno donde los humanos y los agentes de IA colaboran en tiempo real, sus defensas deben ser tan rápidas y adaptables como las amenazas a las que se enfrenta.

Prueba de seguridad contra el phishing (PST) gratuita

Descubraqué porcentajede sus empleados tienen predisposición para ser víctimas de phishing (phish-prone) con la prueba de seguridad contra el phishing (PST) gratuita.

Automated Security Awareness Program gratuito

Creeunprogramaenconcientizaciónsobre seguridad personalizado para su organización.

Phish Alert Button gratuito

Ahorasus empleados tienenunaforma segura de denunciar los ataques de phishing con un solo clic.

Comprobación de exposición del correo electrónico gratuita

Descubraantes quelos malhechores cuál delas direcciones de correo electrónico de sus usuarios está expuesta.

Domain Spoof Test gratuita

Descubra sihackerspueden falsificaruna dirección de correo electrónico de su propio dominio.

Acerca de KnowBe4

KnowBe4 capacitaa lafuerza laboral actual para que pueda tomar decisiones de seguridad más acertadas todos los días. Con la confianza de más de 70 000 organizaciones en todo el mundo, KnowBe4 es pionero en seguridad digital para la fuerza laboral, protegiendo tanto a agentes de IA como a personas. La Plataforma KnowBe4 ofrece simulación de ataques y capacitación, seguridad de la colaboración y seguridad de los agentes impulsada por AIDA (Artificial Intelligence Defense Agents), además de un puntaje de riesgo propio. La plataforma aprovecha 15 años de datos de comportamiento para combatir amenazas avanzadas, como ingeniería social, inyección de ***prompts*** e IA oculta. Al proteger a personas y agentes, KnowBe4 lidera la industria en confianza y defensa de la fuerza laboral.

knowbe4

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet