

Consideraciones fundamentales al evaluar proveedores de capacitación en concientización sobre seguridad



Consideraciones fundamentales al evaluar proveedores de capacitación en concientización sobre seguridad

Índice

Introducción	2
Evaluación de las plataformas de capacitación en concientización sobre seguridad	2
Siete componentes fundamentales que debe proporcionar un proveedor de SAT	3
#1 Contenido variado y atractivo	3
#2 Localización	4
#3 Estructura y automatización	4
#4 Pruebas	4
#5 Métricas e informes	5
#6 Encuestas y evaluaciones	6
#7 Más allá de la SAT	6
Lista de comprobación de proveedores de SAT	7
Conclusión	7

INTRODUCCIÓN

El panorama de proveedores de capacitación en concientización sobre seguridad (Security Awareness Training, SAT) es tan diverso como innovador. Este mercado ha cambiado significativamente en los últimos años, ya que los directores de seguridad de la información (Chief Information Security Officer, CISO) y los líderes de seguridad ahora buscan asegurarse de que cualquier programa de SAT esté cambiando el comportamiento de los usuarios y capacitando a su empresa para comprender, reducir y supervisar el riesgo cibernético de los empleados.

Un proveedor de SAT debe proporcionar una plataforma para lograr esto al:

- Ayudarlo a desarrollar una mentalidad más amplia en torno a la cultura de la seguridad y la gestión del riesgo humano.
- Proporcionar las herramientas necesarias para impulsar y medir el cambio de comportamiento.
- Asegurarse de que sus usuarios se conviertan en el firewall humano de su organización y en la última línea de defensa contra los ciberataques y las violaciones de seguridad de datos.

Este documento técnico proporciona una descripción general de lo que debe saber antes de evaluar las plataformas de SAT y, lo que es más importante, siete capacidades fundamentales que cualquier proveedor de SAT debe proporcionar para ayudar a su organización a lograr sus objetivos.

EVALUACIÓN DE LAS PLATAFORMAS DE CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE SEGURIDAD

Muchos programas de SAT de la vieja escuela no tienen en cuenta lo que se denomina “la brecha conocimiento-intención-comportamiento”. En pocas palabras, el mero hecho de proporcionar a un usuario información y datos relativos a la concientización sobre seguridad no significa que vaya a aprender de ellos o a interesarse por ellos.

La información por sí sola no cambia las acciones. En definitiva, las personas tienden a optar por el camino más fácil o lo que están acostumbradas a hacer. Asegúrese de que las principales partes interesadas de su organización comprendan estas tres realidades antes de evaluar a un proveedor de SAT.

- **El mero hecho de concientizar a alguien no significa que le vaya a importar**
Proporcionar a los empleados mucha información, datos y procedimientos no hará que se preocupen por la concientización sobre seguridad. Cuando reciben una recomendación de seguridad, la mayoría de los empleados “la tienen en cuenta” y la sopesan frente a otras prioridades.
- **Si intenta trabajar en contra de la naturaleza humana, fracasará**
Si existe un desfase entre las expectativas de su política y las realidades de comportamiento mencionadas anteriormente, es probable que su programa de SAT no cumpla las expectativas. En última instancia, se trata de capacitar y establecer expectativas con seres humanos, no de programar datos en una computadora.
- **Lo que hacen sus empleados es mucho más importante que lo que saben**
Los conocimientos por sí solos nunca han evitado que una organización sufra una violación de seguridad. Es un comportamiento lo que reforzará la postura de seguridad de una organización o dará lugar a una violación de seguridad. Céntrese en el comportamiento y no simplemente en proporcionar información y políticas.

SIETE COMPONENTES FUNDAMENTALES QUE DEBE PROPORCIONAR UN PROVEEDOR DE CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE SEGURIDAD

Al evaluar a los proveedores de SAT, asegúrese de que proporcionen los siguientes siete componentes. Esto lo ayudará a garantizar el éxito de su programa de SAT a corto plazo y, al mismo tiempo, lo preparará para el éxito al mostrarle las posibilidades que tiene de cara al futuro.

#1 Contenido variado y atractivo

El contenido es clave. Es el componente informativo de cualquier programa de SAT. Tampoco es un modelo único. Los usuarios se inclinan hacia diferentes estilos de contenido que se ajustan a sus preferencias de aprendizaje individuales. Téngalo en cuenta al evaluar las plataformas de SAT. Para cambiar los comportamientos y crear una cultura de la seguridad sólida en su organización, es fundamental disponer de una serie de contenidos que resuenen en los distintos grupos de empleados. Busque una plataforma de SAT que disponga de una amplia biblioteca de contenidos multilingües y continuamente actualizados, incluidos módulos interactivos, videos, juegos, afiches, boletines informativos, evaluaciones, etc.

Asegúrese de que cualquier proveedor de SAT admita el aprendizaje móvil para que los usuarios puedan asimilar el contenido y completar ejercicios sobre la marcha.

Además, considere la capacitación basada en roles o en preferencias. Lo que se enseña a las personas en un centro de llamadas será probablemente diferente de lo que se enseña a alguien en TI. El contenido debe apoyar estas diferencias. Desde el punto de vista demográfico, los usuarios tendrán diferentes estilos de aprendizaje dentro de su organización: algunas personas asimilarán mejor videos divertidos de tres a cinco minutos de duración, mientras que un equipo ejecutivo puede sentirse menospreciado por este enfoque. La capacidad de tener flexibilidad en torno a sus temas principales de capacitación para garantizar que todos obtengan el contenido que necesitan es una consideración fundamental al evaluar las plataformas de SAT.

Por último, implementar contenido de capacitación para los usuarios es casi tan importante como el contenido en sí. Asegúrese de que cualquier proveedor de SAT admita el aprendizaje móvil para que los usuarios puedan asimilar el contenido y completar ejercicios sobre la marcha. Además, es fundamental disponer de una interfaz administrativa fácil de usar que permita asignar, seguir, medir y notificar los esfuerzos de capacitación, de modo que se puedan extraer conclusiones útiles y significativas sobre los aumentos/disminuciones del riesgo y las zonas de la organización en las que es necesaria una mayor intervención. Además, busque plataformas de SAT flexibles que le permitan incorporar contenidos personalizados de terceros.



#2 Localización

La localización es el proceso crucial de traducir contenidos, además de proporcionar ejemplos, imágenes y elementos interactivos específicos de cada región para los usuarios. Se trata de un proceso en profundidad que va mucho más allá de la mera traducción de contenidos y es fundamental para las organizaciones con presencia mundial y con una base de empleados multilingües.

Asociarse con un proveedor de SAT que permita a sus usuarios seleccionar el idioma/región en el que se encuentran, o con el que se sientan más cómodos, es un factor crucial para garantizar que puedan absorber y aplicar el material de capacitación. Asegúrese de que el proveedor de SAT proporcione localizaciones de alta calidad y utilice expertos locales en la materia para garantizar que el contenido y los ejemplos sean relevantes.

#3 Estructura y automatización

La SAT no se trata de un evento aislado. Crear una cultura de la seguridad requiere capacitación y pruebas continuas seguidas de refuerzo. Además, cuando cree un programa de SAT, recuerde que el aprendizaje se produce en tres etapas diferentes, por lo que es fundamental buscar plataformas que tengan el contenido y las herramientas necesarias para dirigirse a cada etapa de aprendizaje y ofrecer resultados en cada una de ellas.

- **Aprendizaje formal estructurado (10 %):** se refiere a cuestiones como la capacitación presencial, el aprendizaje en línea implementado a través de un sistema de gestión de aprendizaje (Learning Management System, LMS), días de capacitación, etc.
- **Aprendizaje informal (20 %):** significa pedir consejo a otros miembros del equipo, colaborar, ver videos o leer.
- **Aprendizaje experimental (70 %):** se trata principalmente de oportunidades de aprendizaje del día a día, como en el trabajo, la interacción social, cuando se trabaja dentro de los flujos de trabajo comerciales o dentro de la cultura corporativa y departamental.

El 90 % del aprendizaje de una persona tiene lugar fuera de entornos estructurados formales.

Como puede ver, el 90 % del aprendizaje de una persona tiene lugar fuera de entornos estructurados formales. Muchos programas de SAT fracasan porque se centran únicamente en este primer 10 %. Asegúrese de que su programa de SAT aborde las tres etapas y que cualquier plataforma que esté evaluando tenga las herramientas para enfocarse en las tres etapas de aprendizaje. Un ejemplo perfecto: poner un breve video sobre contraseñas en la página de cambio de contraseñas de su organización, para que esté fácilmente disponible en el momento en que se necesite.

Por último, la automatización también es fundamental. Cualquier proveedor de SAT debería incorporar elementos de automatización en su programa para facilitar el aprovisionamiento de usuarios, de modo que las campañas de capacitación puedan programarse con semanas de antelación sin necesidad de una acción directa por parte de los administradores del programa. Esta automatización también debería mejorar la facilidad de uso y el retorno de la inversión al racionalizar el tiempo de gestión de los programas y ofrecer con mayor eficacia contenidos a los usuarios adecuados en el momento oportuno. Por último, también se debe aprovechar la automatización para proporcionar eventos reactivos/correctivos para la “capacitación justo a tiempo” y para proporcionar informes programados para la gerencia y los ejecutivos.

#4 Pruebas

Si bien la capacitación es la piedra angular fundamental de cualquier programa de SAT, probar a los usuarios para ver cómo responderán a las simulaciones de phishing es como determinar si está cambiando el comportamiento de seguridad y mitigando el riesgo humano. ¿El usuario hará clic en el correo electrónico, lo reportará o no hará nada?

Además, los usuarios necesitan una forma simplificada de reportar los correos electrónicos de phishing para ayudar a su organización a desarrollar la resiliencia. Este mecanismo le permite a su equipo de TI obtener más información sobre posibles ataques dirigidos a su organización, así como alertar a todos los demás.

Si bien la mayoría de las plataformas de SAT brindan varios tipos de simulaciones y plantillas de phishing, además de herramientas de usuario final que respaldan los informes de phishing, el problema está en los detalles. Asegúrese de asociarse con un proveedor de SAT que se mantenga a la vanguardia del panorama de amenazas y, como resultado, proporcione plantillas de correo electrónico de phishing basadas en amenazas del mundo real.

Además, si un empleado no pasa una prueba de phishing simulada, una plataforma de SAT debe brindar capacitación “justo a tiempo” para establecer un momento de aprendizaje sobre ese incidente específico mientras aún está fresco en la mente del usuario.

Al igual que la entrega de contenidos y el desarrollo de programas, los programas de simulación de phishing también se beneficiarán de la automatización y el aprendizaje automático. La plataforma de simulación de phishing de un proveedor debe aprovechar el aprendizaje automático para recomendar y ofrecer plantillas de phishing informadas y personalizadas basadas en la capacitación y el historial de phishing del usuario, y ser capaz de reconocer correos electrónicos de phishing legítimos y convertirlos en pruebas simuladas.



#5 Métricas e informes

La medición y la elaboración de informes es otra forma de determinar la eficacia de su programa de SAT para cambiar el comportamiento y reducir el riesgo humano. También es fundamental para cuantificar el éxito de su programa en concientización sobre seguridad ante los ejecutivos.

Para mantener el apoyo de los ejecutivos, es fundamental conocer los resultados del programa en relación con los objetivos específicos y poder demostrar claramente las mejoras. Un buen proveedor proporcionará una sólida plataforma de informes y análisis que permitirá a su organización medir lo que más importa. Esto también debería incluir informes ejecutivos para permitir a los gerentes de programas de SAT crear fácilmente informes específicamente adaptados al liderazgo.

Además, identifique proveedores que midan el riesgo humano y las métricas de cultura de la seguridad. Las métricas del programa de SAT de la vieja escuela generalmente se centran en las tasas de finalización, el rendimiento de las pruebas, las métricas de participación, etc. Es fundamental poder medir el perfil de riesgo de las personas o los departamentos para poder tomar decisiones basadas en datos sobre los ajustes de la capacitación. Debe ser capaz de evaluar cómo cambia el riesgo de su organización con el tiempo y medir realmente el rendimiento de su programa de capacitación para comprender dónde hay que introducir mejoras para reforzar el firewall humano de su organización.

#6 Encuestas y evaluaciones

La presencia de capacitación formal y continua de concientización sobre seguridad puede parecer fuera de lugar para los empleados, ya que pueden percibir que la ciberseguridad es un trabajo de TI. Por lo tanto, es importante entender las actitudes dentro de su organización y cómo están cambiando con la presencia de la SAT. Esto lo ayudará a resaltar áreas en las que se está desempeñando bien o en las que necesita tomar medidas correctivas. También permite medir el progreso en términos de cultura de la seguridad y es diferente de las métricas mencionadas anteriormente porque se analizan las preferencias, la opinión y el estado de ánimo.

Las encuestas y evaluaciones deben incluir la medición no solo de sentimientos y actitudes, sino también de conocimientos y competencias. Cualquier plataforma de SAT debe proporcionar la capacidad de ejecutar evaluaciones basadas en habilidades y encuestas de cultura de la seguridad (Security Culture Surveys, SCS) para permitirle medir el conocimiento y la competencia en seguridad de sus usuarios y medir la postura general de la cultura de la seguridad de su organización. El objetivo es identificar a los usuarios más competentes a la hora de saber cómo responder a una determinada situación y qué significa hacer lo correcto. Además, cualquier plataforma debe brindar la capacidad de comparar su organización con sus pares dentro de su industria y estandarizar las evaluaciones con validez científica para medir con precisión el progreso que ha logrado su organización.

Esto también debería incluir la capacidad de medir el puntaje de riesgo humano de los empleados. Abordar la gestión del riesgo humano es el objetivo final. Una vez que conozca el perfil de riesgo de un individuo o departamento, podrá ajustar la capacitación y obtener información valiosa sobre dónde mejorar su programa de seguridad, lo que reforzará la postura de seguridad de su organización.

#7 Más allá de la SAT

El panorama de los proveedores de SAT ha experimentado un cambio fundamental en los últimos años. Los principales proveedores han pasado de proporcionar ofertas centradas únicamente en la capacitación de los usuarios a plataformas que ahora abordan cuestiones más amplias, como la creación de una cultura de la seguridad dentro de una organización y la gestión del riesgo humano.

Es fundamental asociarse con un proveedor de SAT que no solo alcance sus objetivos inmediatos, sino que también pueda mostrarle las posibilidades futuras. Tenga en cuenta estos puntos clave a la hora de evaluar a un proveedor de SAT:

- **Centrarse en la concientización, el comportamiento y la cultura de la seguridad**
En última instancia, reducir el riesgo humano debe ser su objetivo. Según Forrester Research, conviene asociarse con proveedores que ofrezcan una cuantificación del riesgo humano y un cálculo del riesgo en función del comportamiento del usuario.* La SAT se convierte entonces en la piedra angular para dar forma a su cultura de la seguridad.
- **¿El proveedor proporciona un conjunto de ofertas que le permitirán a su organización ir más allá de la SAT?**
Como ya se ha mencionado, la SAT es la piedra angular para crear una cultura de la seguridad en una organización, pero no es necesariamente el único componente. Otros componentes, como la detección y respuesta humanas, las plataformas SOAR, la respuesta ante incidentes y la inteligencia sobre amenazas, son otros componentes clave que podrían agregarse a su hoja de ruta de cultura de la seguridad en el futuro. Asegúrese de asociarse con un proveedor que satisfaga sus necesidades actuales y futuras.

* The Forrester Wave: Soluciones de capacitación y concientización sobre seguridad del primer trimestre de 2022

LISTA DE COMPROBACIÓN DE PROVEEDORES DE SAT

- ☐ Amplia y variada biblioteca de contenidos de aprendizaje
- ☐ Localización
- ☐ Plataforma de capacitación y phishing altamente automatizada
- ☐ ¿El proveedor brinda la posibilidad de cargar su propio contenido de capacitación o descargar contenido de su plataforma?
- ☐ Plataforma de implementación de capacitación con funciones de automatización
- ☐ Capacidad para cargar contenidos de terceros en la plataforma de capacitación/sistema de gestión del aprendizaje
- ☐ Plataforma flexible de phishing simulado con plantillas de phishing variadas, personalizables y localizadas
- ☐ Automatización, inteligencia artificial y aprendizaje automático integrados en las plataformas de capacitación y phishing
- ☐ Sólidas capacidades de prueba y evaluación de los usuarios para medir sus conocimientos y el impacto de la capacitación
- ☐ Métricas e informes intuitivos para mostrar el retorno de la inversión
- ☐ Funciones de informes ejecutivos

CONCLUSIÓN

En última instancia, estas capacidades sientan las bases para garantizar que el programa de SAT de su organización cambie el comportamiento de los usuarios y le permita a su empresa comprender, reducir y supervisar verdaderamente el riesgo cibernético. La SAT servirá de plataforma para desarrollar una comprensión más amplia de la cultura de la seguridad y la gestión del riesgo humano, y convertir a los usuarios en el firewall humano de su organización.

HAGA
CLIC AQUÍ

Obtenga más información sobre
la capacitación en concientización sobre seguridad
de Kevin Mitnick de KnowBe4

Recursos adicionales



Prueba de seguridad contra el phishing (PST) gratuita

Descubra qué porcentaje de sus empleados tienen predisposición para ser víctimas de phishing con la prueba de seguridad contra el phishing (PST) gratuita.



Automated Security Awareness Program gratuito

Cree un programa en concientización sobre seguridad personalizado para su organización.



Phish Alert Button gratuito

Ahora sus empleados tienen una forma segura de informar los ataques de phishing con un solo clic.



Comprobación de exposición del correo electrónico gratuita

Descubra antes que los malhechores cuál de las direcciones de correo electrónico de sus usuarios está expuesta.



Domain Spoof Test gratuita

Descubra si los hackers pueden falsificar una dirección de correo electrónico de su propio dominio.



Acerca de KnowBe4

KnowBe4 es la plataforma integrada de capacitación en concientización sobre seguridad y phishing (suplantación de identidad) simulado más grande del mundo. Al constatar que se estaba descuidando seriamente el elemento humano en la seguridad, se creó KnowBe4 para ayudar a que las organizaciones manejen el problema de la ingeniería social con una metodología integral de capacitación sobre concientización de la nueva escuela.

Este método integra pruebas iniciales con simulacros de ataques del mundo real, capacitación interactiva y atractiva, y evaluación continua a través de informes simulados sobre la fortaleza empresarial para crear una organización con mayor capacidad de adaptación y que considere la seguridad como principal prioridad.

Decenas de miles de organizaciones en todo el mundo utilizan la plataforma de KnowBe4 en todas las industrias, incluidos los campos estrictamente regulados como las finanzas, la salud, la energía, el gobierno y los seguros, para movilizar a sus usuarios finales como última línea de defensa y permitirles tomar mejores decisiones de seguridad.

Para obtener más información, visite www.KnowBe4.com