Guía de compra de soluciones de gestión de amenazas internas

Esta guía de compra destaca las características más importantes de una solución de gestión de amenazas internas (ITM). Resume los conocimientos adquiridos por Proofpoint en el desarrollo de programas ITM eficaces para organizaciones de todos los tamaños en todo el mundo y en todos los sectores. Esta guía práctica le ayudará tanto si acaba de empezar su trayecto de gestión de amenazas internas como si desea modernizar su solución ITM existente.

Seguridad centrada en las personas

Para proteger los datos contra las amenazas internas, necesita una solución que admita un modelo de seguridad centrado en las personas, que ofrece una visibilidad completa de las interacciones de los usuarios con los datos sensibles y la supervisión de los comportamientos de riesgo. Esto le proporciona información contextual importante sobre sus intenciones cuando algo que hacen parece perjudicial para la organización, ya sea intencionadamente o no.

Con una solución que adopta un enfoque centrado en las personas, puede comprender rápidamente sus riesgos internos en base a los indicadores de comportamiento. Cuando se examinan estos indicadores de manera holística, a lo largo del tiempo y en el contexto de otra actividad, pueden indicar que un usuario podría provocar daño a una organización y justificar una investigación más profunda para determinar la respuesta más apropiada.

Elementos clave de una solución ITM

Si desea bloquear las amenazas internas, debe ser capaz de identificar, proteger, prevenir y neutralizar los incidentes de origen interno. Solo cuando se hace todo esto de forma coordinada con un enfoque proactivo se consiguen reducir los riesgos de amenazas internas.

Identificar

Necesita una solución que proporcione visibilidad del comportamiento de riesgo antes de que se produzca un incidente de origen interno. Es importante identificar patrones de comportamiento anómalos a partir de una base referencia. La solución debe permitir la supervisión de los usuarios de riesgo, como los usuarios con acceso con privilegios, los riesgos de dimisión, los empleados que abandonan la empresa, los contratistas, los ejecutivos y los usuarios sometidos a investigación. A la hora de identificar a los usuarios de riesgo, también pueden tenerse en cuenta factores de estrés, como un cambio en la situación laboral (por ejemplo, un despido o una dimisión), cambios en la empresa (por ejemplo, una fusión y adquisición o una reorganización) y comportamientos preocupantes (por ejemplo, actos de descontento o conflictos financieros).

Cada organización debería decidir los controles de prevención que mejor funcionan en su caso en función de los objetivos, la cultura y la velocidad de innovación de su empresa.

Proteger

Necesitará una solución que proteja los datos y sistemas críticos mediante controles de seguridad centrados en las personas. Las políticas y las reglas deben crearse con indicadores de comportamiento. para ayudar a proteger frente a comportamientos de riesgo.

Es importante impedir que un usuario vulnere, voluntariamente o no, la política de seguridad a través de la formación de los usuarios, los recordatorios en tiempo real y el bloqueo. No todas las actividades pueden o deben bloquearse; es recomendable encontrar un equilibrio entre prevención y productividad de los usuarios. Cada organización debe decidir qué controles de prevención le funcionan mejor en función de sus objetivos empresariales, su cultura y su velocidad de innovación.

Es importante que una solución ITM proporcione una forma flexible y fácil de administrar el acceso a los datos de usuario. La solución debe disponer controles de acceso para garantizar que los analistas de seguridad solo tengan visibilidad de los datos absolutamente necesarios.

Detectar

Una solución ITM debe proporcionar actividades y alertas en tiempo real del comportamiento de los usuarios. Las alertas de la actividades de riesgo de los usuarios pueden incluir:

- Ocultación de información
- Elevación de privilegios
- Omisión de controles de seguridad
- Filtración de datos
- Descarga de software no aprobado
- Sabotaje de tecnologías de la información
- Creación de una puerta trasera
- Acceso no autorizado
- Uso inaceptable

Cuando se infringe una norma, la solución debe capturar todos los pormenores (quién, qué, cuándo y dónde) de la actividad de un usuario para proporcionar un contexto detallado y una visión del comportamiento y las intenciones. La solución también debe capturar pantallas para proporcionar pruebas irrefutables como parte de las investigaciones. Es importante que una solución ITM tenga la flexibilidad necesaria para responder dinámicamente a comportamientos de riesgo y capturar pantallas solo después de que se genere una alerta, lo que ayuda a proteger la privacidad de los usuarios y permite a los analistas de seguridad trabajar con mayor eficacia.

Los usuarios negligentes representan la principal causa de pérdida de datos y amenazas internas. Pueden caracterizarse por tener buenas intenciones pero tomar malas decisiones. Sin embargo, sus errores tienen serias consecuencias.

Respuesta

Es importante poder investigar y responder a los incidentes con rapidez y eficacia. Cuanto más tiempo persista una amenaza interna, más daño puede hacer a su reputación y a su cuenta de resultados. Los flujos de trabajo de investigación son fundamentales para realizar un seguimiento del estado de un incidente, especialmente cuando es necesario remitirlo a departamentos ajenos a seguridad, como RR. HH., jurídico, privacidad y cumplimiento, que pueden tener que participar en una investigación. Una solución ITM sólida también debería integrarse con un sistema centralizado de gestión de eventos como un sistema SIEM en el que ya trabaje el equipo de analistas de seguridad.

3 principales casos de uso

Hay tres tipos básicos de amenazas internas. Todos son atribuibles a la intervención humana. Una solución centrada en las personas debe ser capaz de identificar:

- **Usuarios negligentes.** Son personas que no tienen cuidado y cometen errores.
- **Usuarios maliciosos.** Se trata de usuarios que quieren hacer daño a la empresa.
- **Usuarios comprometidos.** Se trata de personas cuyas credenciales han sido robadas por un ciberdelincuente externo.

1. Usuarios negligentes y errores comunes

Los usuarios negligentes fueron la causa principal de pérdida de datos y amenazas internas, según el informe Proofpoint Data Loss Landscape 2024. Se caracterizan por tener buenas intenciones pero tomar malas decisiones. Simplemente quieren hacer su trabajo de la forma más eficaz posible. Sin embargo, sus errores pueden tener graves consecuencias: interrupción de la actividad, daños a la reputación, debilitamiento de la posición competitiva, incumplimientos normativos y multas, acciones legales, etc.

Veamos algunos ejemplos de acciones de riesgo de los usuarios:

- Enviar mensajes de correo electrónico al destinatario equivocado, con o sin archivos adjuntos.
- Compartir datos sensibles en sitios de IA generativa
- Visitar sitios de phishing.
- Instalar software no autorizado.
- Compartir públicamente datos y archivos confidenciales.
- Enviar por correo electrónico datos de identificación personal (PII) a una cuenta de correo personal.
- Guardar datos corporativos sensibles en dispositivos personales.

Los usuarios maliciosos son peligrosos porque están en la mejor posición para robar datos confidenciales y provocar daños a la organización. Además, están motivados por el beneficio personal.

Protección frente a comportamientos negligentes

Una solución ITM eficaz detectará y prevendrá las actividades de riesgo. También ofrece a los usuarios negligentes apoyo para ayudarles a identificar y cambiar su comportamiento de riesgo.

Elementos indispensables:

- **Clasificación.** Compruebe que el mensaje, los datos y el contenido se supervisan continuamente, tanto manualmente como mediante inteligencia artificial (IA), para identificar y clasificar a los usuarios de riesgo. Cuando un usuario se considera de alto riesgo, el sistema le asigna una puntuación de riesgo para proteger los datos en consecuencia.
- **Supervisión.** La solución debe vigilar comportamientos y actividades de riesgo, como el uso no autorizado de aplicaciones y sitios web, el cambio de nombres y tipos de archivos en documentos confidenciales, el acceso a datos fuera del ámbito de su trabajo y la filtración de un gran volumen de documentos confidenciales. La supervisión de los grupos de alto riesgo puede identificar a los usuarios que necesitan un nivel de supervisión más profundo.
- **Prevención.** Hay que impedir que los usuarios filtren datos sensibles a través de los endpoints. Eso incluye mensajes de correo electrónico enviados al destinatario equivocado con o sin archivos adjuntos, memorias USB, cargas web, sincronización en la nube, impresión, etc. Si cometen un error, deben recibir al instante un mensaje de advertencia contextual que les permita corregirlo y evitar la pérdida de datos en tiempo real sin necesidad de que intervenga el administrador. En caso necesario, los usuarios pueden justificar el acceso a los datos. El equipo de seguridad podrá entonces autorizar o rechazar la solicitud.
- **Formación permanente.** Los usuarios negligentes no son conscientes de que su comportamiento es peligroso. Una solución ITM debe proporcionar formación y concienciación a los usuarios a través de notificaciones de comportamientos de riesgos y enlaces a las políticas de la empresa.

2. Usuarios maliciosos

Los usuarios maliciosos son peligrosos porque están en la mejor posición para robar datos confidenciales y provocar daños a la organización. Además, les mueve el beneficio personal. Los empleados que abandonan la empresa son el tipo de usuarios internos de mayor riesgo, pero los hay de varios tipos.

Los principales tipos de las amenazas internas maliciosas son:

- **Fraude.** Se trata de engaños que causan trastornos en las empresas.
- **Sabotaje.** Esto incluye daños en un sistema o destrucción de datos.
- **Robo.** Se trata del robo de información privada que sea valiosa para una organización.
- **Espionaje.** Se trata de la venta de datos valiosos, secretos comerciales, etc. a un competidor o adversario.

Un sistema centrado en las personas supervisa a algunos usuarios más de cerca que a otros, aplica controles de acceso más estrictos a los usuarios de mayor riesgo

Lo que convierte a los usuarios internos maliciosos en una amenaza es que se encuentran en una posición de confianza. Como tal, pueden aprovechar su acceso privilegiado para hacerse con datos valiosos y explotar vulnerabilidades de seguridad. Es más, las empresas a menudo crean vulnerabilidades al permitir que sus empleados consulten y almacenen datos en sus dispositivos personales, lo que facilita el robo de datos sensibles y la posibilidad de provocar daños.

Protección frente a usuarios maliciosos

Un sistema centrado en las personas supervisa a algunos usuarios más de cerca que a otros, aplica controles de acceso más estrictos a los usuarios de mayor riesgo y bloquea proactivamente la actividad maliciosa basándose en factores de riesgo como la dimisión o el despido.

Elementos indispensables:

- **Visibilidad.** La visibilidad de la actividad de los datos y el comportamiento proporciona una visión holística e información contextualizada sobre la actividad de un usuario. Telemetría sobre sus interacciones con datos y sistemas, como cuando cambian el nombre de un archivo confidencial o lo suben a un sitio web no autorizado o a una carpeta de sincronización en la nube. Si un usuario descarga aplicaciones no autorizadas, manipula los controles de seguridad o instala un navegador TOR, estas actividades de riesgo también deben vigilarse. Una cronología contextualizada de los acontecimientos ayudará a comprender los pormenores (quién, qué, cuándo, dónde) de la actividad del usuario y proporcionará información sobre lo que un usuario estaba haciendo antes y después de una alerta.
- **Biblioteca de amenazas.** Necesita una biblioteca de amenazas completa para los casos de amenazas internas más comunes (fraude horario, filtración de datos, elusión de controles de seguridad). Esto le permitirá ponerse en marcha rápidamente, con reglas para los indicadores de comportamiento más habituales.
- **Investigaciones.** Necesita una solución que proporcione metadatos y capturas de pantalla precisas de las actividades de los usuarios, que ofrezcan pruebas digitales en las investigaciones. Los flujos de trabajo colaborativos son importantes para gestionar los incidentes internos. Dado que la investigación de información sobre amenazas internas implica a partes interesadas ajenas a la seguridad, como los departamentos de RR. HH., jurídico, privacidad y cumplimiento, tendrá que compartir los informes de riesgos asociados a los usuarios en formatos consumibles y fáciles de leer, como informes en PDF.
- **Controles de la privacidad.** Una solución ITM robusta incluye funciones como los controles de acceso basados en atributos, el enmascaramiento y la anonimización de datos y la compatibilidad con centros de datos multirregionales, a fin de cumplir los requisitos de privacidad y residencia de datos, y eliminar el sesgo en las investigaciones. Desea cambiar de forma dinámica y flexible la política de supervisión de un usuario en tiempo real si un usuario activa una alerta, garantizando así la privacidad del usuario mediante la captura de pantallas solo cuando sea necesario.

3. Usuarios comprometidos

Los usuarios comprometidos pueden ser víctimas del uso ilícito o la usurpación de sus cuentas por parte de los ciberdelincuentes. Una vez que sus cuentas se ven comprometidas, los atacantes tienen acceso a nivel interno a sus datos y sistemas. Lo que hace que los usuarios comprometidos sean un reto es que los ciberdelincuentes pueden estar al acecho en los sistemas internos durante meses hasta que son descubiertos.

Los ciberdelincuentes externos aprovechan las vulnerabilidades humanas. La ingeniería social, y en particular, el phishing, es una de las formas más habituales que utilizan los ciberdelincuentes para engañar a los usuarios. No sorprende si tenemos en cuenta su enorme éxito. El 71 % de las organización han sufrido un ataque de phishing.

Las técnicas de phishing más habituales son las siguientes:

- Envío de enlaces o adjuntos maliciosos y solicitudes de datos.
- Smishing (phishing mediante mensajes SMS)
- Phishing en redes sociales
- Ataques teléfono o TOAD
- Estafas Business Email Compromise (BEC)
- Elusión de la autenticación multifactor (MFA)

El objetivo último es el mismo: los ciberdelincuentes externos desean acceder a los datos y sistemas de valor para intentar conseguir un beneficio personal y financiero.

Protección frente a usuarios comprometidos

Una solución ITM eficaz debe ofrecer visibilidad y contexto que ayuden a comprender si el comportamiento de un usuario es inusual. Si un usuario es propenso a hacer clic en enlaces de phishing, por ejemplo, puede supervisar a ese usuario de riesgo para detectar comportamientos inusuales. También puede proteger los datos asegurándose de que solo pueden verlos aquellos que realmente lo necesitan.

Elementos indispensables:

- **Supervisión de proactiva.** Mediante la creación y el registro de exploraciones personalizadas, sus equipos pueden realizar un seguimiento regular de la filtración de datos y actividades de riesgo. Las personas muy atacadas o VAP (Very Attacked People), que tienen tendencia a hacer clic en enlaces o adjuntos maliciosos o a interactuar con aplicaciones vulnerables, pueden ser supervisadas para detectar comportamientos inusuales que pudieran indicar un compromiso de usuario. El mismo enfoque puede utilizarse para otros grupos de alto riesgo, como los empleados que abandonan la empresa o los usuarios con acceso con privilegios. Como es imposible identificar de antemano todos los usuarios internos de riesgo, la solución ITM debe ser capaz de cambiar de manera dinámica y flexible la política de supervisión de un usuario en tiempo real si el usuario activa una alerta.
- **Controles de acceso adaptables.** Puede aplicar reglas de acceso condicional a los datos, como la inclusión en listas seguras y/o en listas de bloqueo de países, redes o direcciones IP de alto riesgo. También pueden limitar el acceso a datos sensibles a determinados usuarios y grupos con privilegios y permitir cargas y descargas solo en dispositivos gestionados. Los requisitos de privacidad pueden cumplirse mediante el control de acceso basado en atributos.
- **Integraciones.** Una solución ITM eficaz complementará su sistema de seguridad, aportando contexto por la facilidad con la que puede integrarse en una serie de herramientas:
  - Organización, automatización y respuesta a incidentes de seguridad (SOAR)
  - Sistemas de administración de información y eventos de seguridad (SIEM)
  - Respuesta a incidentes
  - Gestión de incidentes
- **Arquitectura moderna.** Una plataforma nativa para la nube puede ampliarse para cientos de miles de usuarios. Una solución ITM debe recopilar telemetría a través de un agente ligero de endpoints que no afecte a la productividad de los usuarios ni entre en conflicto con otras soluciones.

Conclusión

La protección de la organización frente a los riesgos internos, ya sea de manera intencionada o no, requiere una solución de gestión de amenazas internas (ITM) que permita un enfoque proactivo. Una solución ITM debería tener visibilidad de los comportamientos de riesgo y la capacidad de responder de manera automática y dinámica. Dada la colaboración transversal necesaria para apoyar las iniciativas contra los riesgos internos, una solución ITM debe permitir los flujos de trabajo de investigación y recopilar pruebas irrefutables, como capturas de pantalla, para acelerar las investigaciones. Por último, una solución ITM debe poder adaptarse al crecimiento de su empresa, aprovechar sus inversiones existentes y proporcionar acceso flexible y controles de la privacidad para garantizar el cumplimiento. El uso de una solución ITM con estas funciones principales garantizará la protección de su empresa frente a los riesgos internos, al tiempo que facilitará el trabajo de su equipo de seguridad.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.