Proofpoint Threat Response y el RGPD

Cumplimiento con automatización de la seguridad y mejores prácticas de privacidad de datos

VENTAJAS PRINCIPALES

Adopción de las mejores prácticas de seguridad

- Solución de las amenazas dirigidas con más rapidez y eficiencia
- Disminución de la carga del equipo de TI, gracias a la respuesta a incidentes automática
- Reducción del exceso de alertas
- Recopilación y priorización de datos de distintos dispositivos de seguridad
- Visibilidad de todas las amenazas, con información de contexto

Cumplimiento del RGPD

- Prevención de uso compartido de datos personales con terceros
- Integración con sistemas de control internos
- Incorporación a los registros internos de tratamiento de datos
- Prueba de cumplimiento con el aval de Proofpoint

La mayoría de las organizaciones de éxito actuales utilizan tecnología de automatización para gestionar los incidentes de seguridad. ¿En qué consiste esta tendencia? ¿Y qué debe tener en cuenta cuando adopte la automatización de la seguridad para cumplir las normativas, seguir las mejores prácticas y conseguir ventajas para la empresa a largo plazo?

EL CAMINO A LA AUTOMATIZACIÓN DE INCIDENTES

El panorama de las amenazas actual requiere una respuesta rápida. Pero los equipos de seguridad se enfrentan a numerosos retos que les impiden responder a las amenazas dirigidas de forma rápida y eficaz. Entre ellos figuran:

- **Escasez de personal:** la respuesta a incidentes puede ser un proceso lento que requiere mucho trabajo. Algunas tareas llevan mucho tiempo y crean dificultades, y repetir las mismas tareas para cada incidente puede desbordar a un equipo de seguridad ya de por sí sobrecargado.
- **Exceso de alertas:** cuantos más dispositivos de seguridad utilice, mayor será el número de alertas. Su equipo de seguridad deberá filtrar estas alertas de forma manual. ¿Qué problema plantea esto? Está a merced de un error humano. Y con frecuencia los incidentes reales se pasan por alto.
- **Dispositivos de seguridad y datos dispares:** la investigación para la respuesta a incidentes requiere información de varias fuentes inconexas. Cada punto de datos es como una pieza de un rompecabezas. Como muchas organizaciones, cada vez se enfrenta a más amenazas dirigidas y es fundamental responder en cuestión de minutos. La necesidad de analizar demasiada información inconexa puede ralentizar la respuesta a los incidentes.

Las soluciones de organización, automatización y respuesta (SOAR, por sus siglas en inglés) pueden ayudarle a resolver estos problemas. Estas soluciones recogen alertas de distintas fuentes y crean flujos de trabajo para automatizar la respuesta a incidentes. El uso de una solución SOAR le permite ahorrar tiempo. Mediante la automatización de la respuesta a incidentes, también se limita o reduce el número de empleados a jornada completa que se necesitan para resolver los incidentes de seguridad. Así disminuye el tiempo medio para responder, contener y solucionar las amenazas.

Proofpoint Threat Response es una solución SOAR que elimina el trabajo manual y las conjeturas de la respuesta a incidentes. De esta forma, ayuda a su equipo de seguridad a corregir las amenazas más rápidamente y con más eficacia. Threat Response recoge alertas de varias fuentes y las agrupa y completa con contexto esencial de la inteligencia sobre amenazas de Proofpoint, en cuestión de segundos. Ofrece información sobre "quién, qué y dónde" en relación con los ataques, asignación de IP de usuarios e inteligencia de amenazas externa, como fuentes STIX y TAXII. Sus analistas pueden filtrar rápidamente los incidentes de seguridad. Basándose en el contexto y los datos forenses recopilados y analizados, Threat Response presenta una vista de la amenaza con contexto detallado. Sus analistas pueden realizar acciones automatizadas, como:

- Retirar mensajes entregados en buzones de correo de los usuarios.
- Añadir usuarios a grupos con pocos permisos.
- Actualizar listas de bloqueo de firewalls y filtros web.
- Contener la amenaza bloqueando o poniendo en cuarentena amenazas en Microsoft Exchange, firewalls, sistemas de detección y respuesta de endpoints (EDR), gateways web, Microsoft Active Directory, herramientas de control de acceso a la red (NAC) y otras soluciones.

PRIVACIDAD DE DATOS Y OPERACIONES DE SEGURIDAD

El RGPD y "Licitud del tratamiento"

Según el Reglamento General de Protección de Datos (RGPD), el tratamiento de los datos personales es una función legítima de los responsables correspondientes. Esto se fundamenta en que los datos personales son necesarios para garantizar la seguridad de la red y la información. También es legítimo el tratamiento de datos personales para prevenir acciones maliciosas que puedan poner en riesgo la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales almacenados o transmitidos. Estos "intereses legítimos" se definen en el artículo 6 del RGPD, "Licitud del tratamiento". El interés legítimo puede determinarse por ley. Pero esto solo es posible si se puede justificar el tratamiento de los datos. Este debe cumplir los principios de proporcionalidad y subsidiariedad. Estas excepciones al uso de los datos personales por parte de seguridad de TI se definen en el artículo 6(1)f del RGPD y en el punto 49.

A la hora de cumplir el RGPD, ampliar y proteger su infraestructura con servicios de seguridad como Threat Response aporta una gran ventaja. Esta solución es una parte fundamental de una arquitectura de TI moderna. La configuración de Threat Response puede incluir el tratamiento de datos en arquitecturas de seguridad externas, como servicios de seguridad o de inteligencia de amenazas. Threat Response no proporciona ninguna información a personas externas. Solamente utiliza estos datos para los fines acordados, descritos en el contrato de servicio por escrito entre usted y Proofpoint. Threat Response solo está disponible localmente, sin transferencias de datos externas, de forma predeterminada.

Añada Threat Response a los registros de actividades de tratamiento de datos

Según el RGPD, para el cumplimiento es importante garantizar una configuración e integración correctas en otros sistemas. Puede añadir Threat Response a sus registros de tratamiento de datos internos, según exige el RGPD en el artículo 30 "Registro de las actividades de tratamiento".

Intercambio interno de datos de PII

El artículo 47 del RGPD, "Normas corporativas vinculantes", permite la transferencia internacional de información interna. Estas normas corporativas deben incluir todos los principios de privacidad de los datos esenciales, así como los derechos aplicables para garantizar las medidas de seguridad adecuadas para las transferencias o categorías de transferencias de datos personales.

Para garantizar el cumplimiento del RGPD, debe efectuar la implementación a través de un sistema de control interno (ICS). Esto implica que debe establecer dicho sistema de control. Un ICS compatible está formado por elementos del sistema de control interno y el sistema de supervisión. El sistema de control ofrece formas de controlar las actividades de su organización. De esta forma, garantiza el registro correcto de las transacciones comerciales y el cumplimiento de los principios del RGPD.

INTERCAMBIO DE DATOS CON TERCEROS[1]

Para conseguir un nivel adecuado de protección, el RGPD permite a las organizaciones contratar a expertos externos, o utilizar herramientas o servicios de otros proveedores, para complementar las medidas de seguridad internas. El RGPD incluye normativas muy estrictas para garantizar que otros proveedores (encargados del tratamiento) refuercen su nivel de protección de datos. Se definen en el artículo 28 "Encargado del tratamiento". El responsable solo debe usar encargados del tratamiento que ofrezcan suficientes garantías de la implementación de las medidas técnicas y organizativas tal y como se requiere para cumplir los requisitos del RGPD. Los encargados del tratamiento deben garantizar la protección de los derechos del interesado.

Para cumplir este estricto requisito, Proofpoint ofrece varios documentos para sus registros para todos los productos relacionados, con el fin de facilitarle el cumplimiento. Esto incluye los acuerdos de tratamiento de datos que necesita para su directorio de tratamiento.

Threat Response, que se basa en las mejores prácticas del sector y de cumplimiento de normativas, automatiza y agiliza la respuesta a incidentes. Además, ayuda a garantizar que utiliza los datos personales en un contexto de seguridad que cumple perfectamente el RGPD. Como ventaja añadida, Proofpoint proporciona documentación defendible para demostrar el cumplimiento.

1 Esto se aplica cuando se configura el intercambio de datos o servicios externos (ejemplo: Proofpoint Targeted Attack Protection).

MÁS INFORMACIÓN

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