Su red puede estar segura un minuto e insegura al siguiente. Las configuraciones incorrectas del firewall , los conflictos de políticas, las nuevas intrusiones u otros cambios siempre surgen y, a menudo, pasan desapercibidos. El monitoreo continuo proporciona una forma para que las empresas estén constantemente al tanto de su estado de seguridad, para que puedan actuar sin demora para priorizar y ejecutar respuestas.

¿Qué es el monitoreo continuo?

Es un conocimiento continuo del estado de seguridad de la red, incluidas las vulnerabilidades y amenazas.

Específicamente, el monitoreo continuo ayuda a las organizaciones a administrar el riesgo al:

- Supervisar continuamente los cambios en los puntos de aplicación de la seguridad que podrían provocar una exposición innecesaria, una configuración incorrecta, un cambio no autorizado y un riesgo inaceptable.
- Ayudando a detectar y mitigar las vulnerabilidades de seguridad.
- Mantener el cumplimiento continuo de los estándares de la industria.
- Identificación de amenazas y agujeros de seguridad en las políticas de seguridad.
- Generación de informes detallados para todas las evaluaciones periódicas.
- Capturar documentación valiosa de políticas para cumplir con los requisitos de evaluación de cumplimiento.
- Asegurar que los cambios de política se adhieran a los requisitos existentes.
- Recertificación de todas las reglas y configuraciones de firewall obligatorias.
- Proporcionar inteligencia procesable para orientación de remediación.

Cómo funciona el monitoreo continuo

La supervisión continua examina los conjuntos de reglas y compara los cambios propuestos con un conjunto de comprobaciones. Estos controles se asignan a las políticas de seguridad internas, los requisitos reglamentarios o cualquier otro requisito relacionado con los controles de acceso de seguridad de la red.

¿Quién necesita un seguimiento continuo y por qué? El monitoreo continuo es particularmente importante para las empresas cubiertas por un estándar regulatorio . Todos los estándares regulatorios requieren un cumplimiento constante; no hay ningún requisito que diga: "Cumplir entre 9-5, MF" o "Cumplir la

mayor parte del día anterior". El cumplimiento se supone que es siempre activa, por lo que organizaciones como minoristas, organizaciones de salud, empresas de servicios públicos y de energía, y las agencias federales y contratistas que deben cumplir con PCI DSS, HIPAA, NERC, NIST, FedRAMP, GDPR , etc., se basan en monitoreo continuo para prevenir filtraciones de datos, sanciones, posibles litigios y pérdida de reputación.

La supervisión continua también es muy recomendable para cualquier empresa que ejecute un entorno híbrido. Los entornos híbridos son muy dinámicos , con dispositivos y terminales que se unen y se desconectan a lo largo del día. A medida que ocurren estos cambios, se pueden crear vulnerabilidades y las defensas y el cumplimiento pueden verse comprometidos. La única forma de prevenir estos riesgos es mantener la visibilidad de los cambios en la red.

Sin embargo, incluso las organizaciones que no se preocupan por el cumplimiento y no utilizan redes híbridas se benefician del monitoreo continuo. Todas las empresas necesitan una comprensión ininterrumpida de lo que está sucediendo en sus redes. De lo contrario, no tienen forma de saber si sus datos y propiedad intelectual están seguros, sus medidas de seguridad son adecuadas y sus políticas funcionan según lo previsto.

6 mejores prácticas para el monitoreo continuo

Hay varias formas de planificar una estrategia de monitoreo continuo, pero la mayoría de las organizaciones adoptan un enfoque basado en el riesgo, como el definido en NIST SP 800-137 . El Marco de gestión de riesgos del NIST describe un proceso de 6 etapas para gestionar el seguimiento continuo.

1. **Categorice la criticidad subyacente y el valor de los activos de datos y sistemas de TI específicos.** Defina y asigne valor a los activos mediante el análisis de los datos capturados en escáneres de vulnerabilidades. La revisión de estos datos le permite cuantificar y priorizar el riesgo asociado con la vulnerabilidad de los activos de la red.
2. **Seleccione controles de seguridad básicos y aplique políticas de dispositivos directamente relacionadas con el riesgo general Las** redes empresariales son más grandes y complejas que nunca con centros de datos virtuales, computación en la nube y movilidad. Cada componente adicional genera más controles de seguridad que se deben implementar y rastrear. Utilice una política de seguridad de red y una solución de gestión de riesgos que mejore su postura de seguridad al proporcionar un análisis de configuración potente y reducir el riesgo de forma proactiva.

3. **Implemente y valide controles efectivos que ejecuten adecuadamente las políticas de seguridad** Elija una solución de monitoreo continuo que admita firewalls líderes de Check Point, Cisco, Juniper, McAfee y Palo Alto. También debe integrarse a la perfección con los escáneres de vulnerabilidades, como Qualys, Rapid7, McAfee, nCircle y Nessus, para que pueda evaluar y definir la vulnerabilidad de los activos subyacentes.
4. **Evalúe continuamente todos los controles para asegurarse de que funcionan al unísono para mantener la protección de la infraestructura cruzada** Realice **un** seguimiento y registre los cambios de configuración en un registro de auditoría. La mayoría de las soluciones de monitoreo continuo ofrecen una biblioteca integrada de controles que permiten evaluaciones personalizadas de políticas de seguridad, seguimiento de mitigaciones de auditorías anteriores y análisis de riesgos específicos del entorno.
5. **Autorice solicitudes para modificar el acceso a la red y registre todos los cambios y sus parámetros específicos.** Realice un seguimiento de los cambios de configuración y fallas comunes por dispositivo y busque tendencias a más largo plazo. Obtenga una vista previa del impacto potencial de todos los cambios antes de que se implementen en la red de producción para garantizar que los cambios cumplan con los estándares de cumplimiento de la red. Una vez que se implementa un cambio, documente los cambios en la red con informes detallados e identifique qué dispositivos se cambiaron, qué se cambió y quién realizó los cambios.
6. **Supervise todos los controles de seguridad necesarios en todo momento para mantener el cumplimiento de la política general.** Utilice alertas de cambio de configuración en tiempo real para identificar violaciones de la política de seguridad. Evalúe automáticamente el cumplimiento de las nuevas configuraciones de dispositivos. Informe de inmediato las configuraciones que se salen de la norma, idealmente a través de notificaciones automáticas a los teléfonos móviles del equipo de seguridad y las bandejas de entrada de correo electrónico.

Capacidades imprescindibles en una solución de monitorización continua

Hay muchas soluciones que incluyen algún nivel de monitoreo continuo, pero varían mucho en la variedad y el alcance. Estas son las características que son críticas para brindar visibilidad, permitir flexibilidad y fortalecer la seguridad:

- ✓ El monitoreo en tiempo real utiliza datos de toda la red para alimentar una transmisión en vivo de registros, configuraciones, cambios, políticas, vulnerabilidades, etc. Esto proporciona una imagen completa de lo que está sucediendo en el entorno en un momento dado.
- ✓ El análisis de seguridad en tiempo real mide la eficacia de las políticas de firewall existentes, incluida la puntuación comparativa, para comprender la aplicación actual del acceso.
- ✓ Una sólida capacidad de búsqueda de políticas puede buscar rápidamente en todos los dispositivos dentro del dominio empresarial desde un solo lugar en la aplicación.
- ✓ Utilice el análisis de flujo de tráfico para comprender el comportamiento del tráfico de la red al rastrear el origen y el destino de cada regla en cada una de las políticas de firewall existentes.
- ✓ Modele y pruebe el impacto de los cambios antes de la implementación para asegurarse de que no creen riesgos de TI adicionales. Esto reduce el tiempo y aumenta la eficiencia al tiempo que proporciona una documentación completa de todos los cambios con fines de cumplimiento.
- ✓ La ingesta de datos a escala se flexiona con sobrecargas, cambios y mutaciones de red, cambios de plataforma y tráfico. Esto evita ralentizaciones y bloqueos que anularían los beneficios del monitoreo en tiempo real.
- ✓ Los informes personalizables brindan flexibilidad para mezclar y combinar controles según el contexto, qué se está monitoreando, qué acciones son necesarias, etc.

No más misterios en la red

En las complejas infraestructuras actuales, las brechas de seguridad pueden pasar desapercibidas. Los datos puntuales en los que confían la mayoría de las organizaciones son buenos para comprender un evento pasado o demostrar el cumplimiento, pero no les ayudan a hacer que sus redes sean más seguras en el momento.

La única forma de obtener inteligencia procesable en un entorno complejo es a través de datos históricos y continuos a una escala que analiza millones de vulnerabilidades en segundos. Armadas con esta información, las organizaciones pueden proteger de manera proactiva sus activos y tomar mejores decisiones sobre las respuestas de seguridad y las inversiones.