GUÍA RÁPIDA

MONITOREAR EN TIEMPO REAL



ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

El **monitoreo es un control preventivo que disminuye la probabilidad de que ocurra un incidente** de ciberseguridad de impacto significativo. Además, permite identificar comportamientos sospechosos o maliciosos y detectar oportunamente una amenaza para actuar antes de que generen un impacto en la organización.

Sin embargo, ningún control preventivo es infalible. Por eso, es fundamental monitorear para identificar cuándo un control falla y **detectar posibles amenazas que logren superar las medidas de protección** existentes.

¿Qué significa monitorear?

El monitoreo es un **proceso compuesto por seis etapas** que permiten transformar los registros de nuestros sistemas en información útil para detectar y responder ante posibles amenazas.

1. **RECOLECTAR**
   Definir las fuentes de registros que se deben monitorear para obtener información relevante sobre la actividad de nuestros sistemas.

2. **PARSEAR**
   Recopilar, separar y ordenar la información de los registros de las distintas fuentes, con el fin de entenderla, analizarla y generar alertas en caso de ser necesario.

3 **CORRELACIONAR**

Relacionar eventos provenientes de distintas fuentes para identificar patrones sospechosos que podrían pasar inadvertidos al analizar cada evento por separado.

4 **ALERTAR**

En aquellos casos que exista evidencia suficiente para investigar una posible amenaza. Una alerta no confirma por sí sola la existencia de un incidente.

5 **ANALIZAR**

Las alertas, evaluar la evidencia disponible y determinar si existe una actividad sospechosa o un incidente de seguridad.

6 **RESPONDER**

Ejecutar las acciones necesarias para contener la amenaza, reducir su impacto y restablecer la operación segura de los sistemas afectados.

El objetivo de este proceso es identificar y priorizar las alertas que realmente importan, evitando que el exceso de notificaciones dificulte la detección de amenazas relevantes.

¿Qué monitorear?

Registros de identidad

Son una de las fuentes más importantes para detectar posibles compromisos de cuentas o usos indebidos de privilegios. Para ello, considera monitorear:

- Inicios de sesión exitosos y fallidos.
- Modificaciones en los métodos de autenticación multifactor (MFA).
- Cambios de privilegios y permisos.
- Creación, modificación y eliminación de cuentas.
- Accesos desde ubicaciones u horarios inusuales.

Endpoints y servidores

Los registros generados por antivirus y herramientas de detección y respuesta en endpoints (EDR) proporcionan información valiosa sobre posibles amenazas.

Es importante monitorear las detecciones de malware, las ejecuciones sospechosas, los cambios inusuales en los sistemas, entre otras actividades que puedan indicar un compromiso.

VPN y accesos remotos

Estos registros permiten identificar accesos sospechosos y posibles usos indebidos de las conexiones remotas, como:

- Autenticaciones exitosas y fallidas.
- Origen de las conexiones.
- Accesos remotos inusuales.
- Volumen de tráfico y patrones de conexión.
- Bloqueos y otros eventos de seguridad.

Correos electrónicos

El monitoreo del correo electrónico permite identificar comportamientos que podrían estar relacionados con el envío de spam, el compromiso de cuentas o la distribución de contenido malicioso.

Así también, es importante monitorear los accesos, los cambios en las reglas del correo y los inicios de sesión desde países o ubicaciones inusuales.

Aplicaciones críticas

Los registros de las aplicaciones críticas permiten identificar actividades sospechosas que podrían afectar la confidencialidad, integridad o disponibilidad de la información. Para ello, hay que considerar en el monitoreo:

- Accesos exitosos y fallidos.
- Errores y comportamientos anómalos.
- Acciones administrativas.
- Cambios en configuraciones y permisos.
- Transacciones inusuales.

El monitoreo en tiempo real es fundamental para transformar los registros en alertas útiles, detectar amenazas oportunamente y responder antes de que el impacto sea mayor.

Para optimizar las capacidades de monitoreo, considera:

- **Seleccionar los registros que aporten mayor valor** para detectar amenazas en los activos críticos. No todos los registros tienen la misma importancia. Es necesario priorizar.
- **Administrar la cantidad de información recolectada** y el tiempo en que se conserva.
- **Controlar el volumen de registros** para asegurar que los recursos disponibles sean suficientes.
- **Centralizar los registros** para facilitar el análisis y correlación.
- **Conservar información que permita reconstruir eventos,** identificar patrones y profundizar en el análisis de posibles incidentes.
- **Prioriza los activos críticos y las fuentes de registros relevantes,** para enfocar los esfuerzos de monitoreo en aquellos eventos que aportan mayor valor para detectar una amenaza.

