RESUMEN DEL PRODUCTO

Monitorización de Integridad de Archivos

El uso de la monitorización permanente para garantizar la integridad de los archivos confidenciales es mucho más que una simple práctica recomendada. Para muchas organizaciones, se trata también de una obligación legal. Al combinar la Monitorización de Integridad de Archivos con SIEM totalmente integrado, la Administración de Bitácoras, el Análisis Automatizado y el Análisis Forense de Equipos Anfitriones y Redes, LogRhythm permite a los clientes simplificar y reforzar su postura de seguridad, auditoría y cumplimiento normativo con una única solución plenamente integrada.

Monitorización de Integridad de Archivos con visibilidad de usuarios

El método holístico de LogRhythm permite notificar al personal de seguridad cuando se crean archivos o se visualizan, eliminan o modifican archivos clave y cuando se producen cambios en la propiedad colectiva de los archivos. Para la monitorización selectiva, LogRhythm ofrece controles y filtros granulares capaces de detectar archivos concretos y realizar análisis con los intervalos deseados u operar en el modo en tiempo real para una protección continua. A continuación, el comportamiento en el nivel de archivo puede correlacionarse con actividades de seguridad y auditoría adicionales para crear una visión completa de cualquier actividad de red potencialmente dañina.

Exigencias de la PCI DSS 11.5:

Implementar una monitorización de integridad de archivos para alertar al personal de cualquier modificación no autorizada de los archivos críticos de sistema o de contenidos, realizando asimismo comparaciones de archivos al menos semanalmente o con más frecuencia si se puede automatizar el proceso.

"El cumplimiento de la PCI es coser y cantar. Suponer que estás protegido porque tomas medidas preventivas solo te hace más débil: tienes que pasar a la acción para estar un paso por delante de quienes siempre quieren sacar partido a cualquier punto débil de tu red".

Bernie Rominski
Responsable de seguridad de TI
Regis Corporation

Con la incorporación de la Monitorización de Integridad de Archivos, LogRhythm puede usarse para monitorizar y alertar sobre toda una variedad de comportamientos maliciosos, desde el acceso inadecuado de los usuarios a archivos confidenciales hasta intrusiones de botnet y transmisión de datos confidenciales. La solución combinada permite a las organizaciones satisfacer requisitos de cumplimiento normativo específicos, tales como las normas PCI DSS (Payment Card Industry Data Security Standard) 11.5 y 12.9, sin necesidad de adquirir un producto separado.

Totalmente integrado con la administración de bitácoras y eventos y la monitorización y el control de terminales

- Satisface 80 diferentes requisitos de control de la norma PCI DSS.
- Envía alertas contextualizadas cada vez que se visualizan, modifican o eliminan datos confidenciales.
- Proporciona un conjunto completo de datos forenses para una identificación rápida de la causa original de las intrusiones de seguridad.
- Configuración y administración centralizadas y basadas en políticas.

Monitoriza todos los tipos de archivos

- Incluidos los ejecutables, archivos de configuración, archivos de contenidos, archivos de bitácora y auditoría, archivos de web y mucho más.
- Sus controles granulares garantizan que cada archivo monitorizado se analice con la frecuencia deseada.
- El FIM en tiempo real ofrece detalles específicos acerca de qué usuario visualizó, modificó o eliminó qué archivos.

Incorpora políticas llave en mano para las aplicaciones más comunes.

La Monitorización de Integridad de Archivos de LogRhythm es compatible con los sistemas Windows, Unix y Linux.