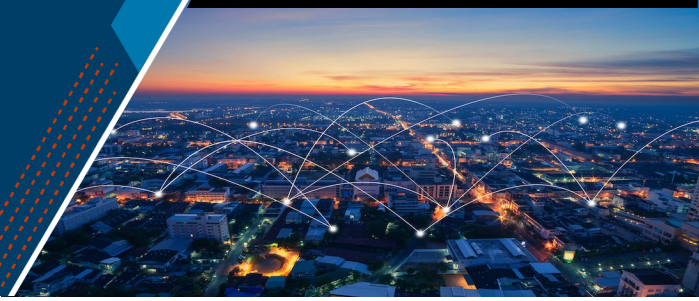
PREGUNTAS FRECUENTES SOBRE LOGGING MADE EASY



¿QUÉ ES LOGGING MADE EASY?

La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés) lanzó Logging Made Easy (LME) en octubre de 2023. LME es una solución gratuita de gestión de registros diseñada para organizaciones pequeñas y medianas con recursos limitados, que de otro modo tendrían poca o ninguna capacidad para detectar ataques. LME ofrece un sistema centralizado de registro para los sistemas operativos Linux, macOS y Windows, lo que permite la detección proactiva de amenazas y mejora la seguridad, dado que las organizaciones pueden monitorear sus redes, identificar usuarios y analizar activamente los datos de Sysmon para detectar rápidamente posibles actividades maliciosas.

Para proporcionar una funcionalidad mejorada y mantenerse al día con el entorno tecnológico en constante evolución, CISA lanzó LME 2.0 en noviembre de 2024. LME 2.0 es una solución de gestión de registros y detección de amenazas que utiliza las herramientas de código abierto Elastic y Wazuh. LME 2.0 introduce mejoras y nuevas funciones respecto a versiones anteriores, manteniendo su naturaleza gratuita y de código abierto. LME 2.0 facilita su adopción al tiempo que incrementa la seguridad y mejora las capacidades de registro, detección y alerta.

¿QUÉ HACE QUE LME SEA ÚNICO?

LME permite una gestión de registros fluida, priorizando la transparencia, la seguridad y la colaboración para ofrecer un valor incomparable. Lo que hace que LME sea único son sus paneles personalizables que muestran registros del sistema en tiempo real.

¿QUÉ BENEFICIOS OBTENGO?

LME simplifica la gestión de registros con una implementación sencilla, monitoreo centralizado y una interfaz fácil de usar. Al utilizar LME, los usuarios obtienen visibilidad de amenazas en tiempo real, lo que permite detectar eventos de seguridad y responder a ellos de manera proactiva. El compromiso de LME con la transparencia y la colaboración comunitaria genera confianza, lo cual se ve reflejado en las reseñas positivas. Elegir LME brinda acceso a una solución de gestión de registros sólida, accesible y colaborativa que se adapta a los objetivos de las organizaciones para lograr un futuro digital seguro.

¿CÓMO DESCARGAR LME?

No es necesario registrarse ni realizar un largo proceso de incorporación. Simplemente visite la página de GitHub de LME de CISA para obtener instrucciones paso a paso sobre cómo descargarlo e instalarlo. GitHub facilita el desarrollo de software de código abierto dado que proporciona una plataforma colaborativa para alojar, compartir y administrar repositorios de código, además de habilitar el control de versiones, las contribuciones de la comunidad y el seguimiento de problemas.

¿QUÉ SOFTWARE UTILIZA LME?

LME 2.0 utiliza Elastic Stack (para la gestión de registros, búsqueda y visualización), Wazuh (para la detección y respuesta de puntos finales) y Podman (para la contenedorización). Esta pila de software de código abierto garantiza

transparencia, flexibilidad y escalabilidad, al tiempo que proporciona una mejor detección de amenazas y paneles personalizables.

¿QUÉ SISTEMAS OPERATIVOS PUEDEN UTILIZAR LME?

LME 2.0 es compatible con los sistemas operativos Windows, Linux y macOS. Los agentes de Elastic y Wazuh permiten la compatibilidad en estas plataformas, lo que garantiza una amplia cobertura para el monitoreo y el registro. Aunque los agentes de Wazuh también son compatibles con los sistemas operativos Solaris, AIX y HP-UX, CISA no ha probado LME en puntos finales que ejecuten estos sistemas operativos.

¿QUIÉN PUEDE USAR LME?

Aunque está diseñado para organizaciones pequeñas y medianas con recursos limitados, cualquier persona puede descargar LME 2.0. Consulte la documentación de requisitos previos de LME 2.0 para obtener más detalles sobre la infraestructura y el hardware necesarios, incluidos los requisitos de CPU, memoria y almacenamiento.

¿LME PUEDE FUNCIONAR EN LA NUBE?

LME 2.0 admite implementaciones tanto locales como en la nube, lo que permite a las organizaciones alojar LME en su infraestructura local o en la de un proveedor de servicios en la nube.

¿LME 2.0 ES UNA REINSTALACIÓN COMPLETA O UNA ACTUALIZACIÓN?

Tanto los usuarios nuevos como los existentes deben realizar una instalación completa de LME 2.0 desde la página de GitHub de LME. Aunque los usuarios actuales necesitarán reinstalar la herramienta, este proceso garantiza que utilicen la versión más reciente con todas las funciones actualizadas. Las instrucciones de instalación están disponibles en la página de GitHub de LME.

¿LAS VERSIONES ANTERIORES DE LME DEJARÁN DE FUNCIONAR?

Si bien CISA recomienda actualizar a LME 2.0, los usuarios pueden seguir utilizando versiones anteriores de LME. Sin embargo, CISA no brindará asistencia para versiones anteriores.

¿CÓMO PUEDEN LOS USUARIOS ACTUALES DE LME MIGRAR A LME 2.0 Y CONSERVAR EL HISTORIAL DE REGISTROS?

Los usuarios actuales de LME deben hacer clic aquí para acceder a instrucciones sencillas sobre cómo transferir el historial de registros desde versiones anteriores. LME reintegrará automáticamente el historial de registros y los datos.

¿HAY NUEVOS REQUISITOS DEL SISTEMA ACTUALIZADOS PARA LME 2.0?

Los requisitos del sistema de LME 2.0 siguen siendo prácticamente los mismos. Los usuarios pueden encontrar documentación detallada en la página de GitHub de LME. Aquellos que no estén seguros de cumplir con los requisitos previos de instalación deben revisar la documentación de requisitos previos para obtener orientación.

¿DÓNDE PUEDEN LOS USUARIOS DE LME RECIBIR ASISTENCIA ADICIONAL?

Para recibir asistencia adicional con LME 2.0, los usuarios pueden explorar las siguientes opciones:

- Informar problemas de LME a través de la pestaña “Issues” (Problemas) en la parte superior de la página de GitHub o hacer clic en GitHub Issues (Problemas de GitHub).
- Visitar “Discussions” (Discusiones) para verificar si su problema ya se ha abordado o para iniciar un nuevo hilo de discusión.
- Enviar un correo electrónico directamente a CyberSharedServices@cisa.dhs.gov para consultas o comentarios

adicionales.

¿DÓNDE PUEDEN LOS USUARIOS ENCONTRAR RECURSOS ADICIONALES?

Visite el sitio web de LME de CISA para acceder a recursos adicionales.