El Logger AlienVault USM

Las organizaciones de seguridad deben de proteger su infraestructura frente al escenario rápidamente cambiante de amenazas y asegurar el cumplimiento normativo, además de ajustarse a requisitos de niveles de servicio exigentes.

Los logs son una parte muy importante en la seguridad; sin embargo, por sí solos sirven para poco más que para realizar informes forénsicos y de cumplimiento normativo. El Logger USM de AlienVault, junto con el Sensor USM y el Servidor USM, proporcionan una seguridad más exhaustiva y efectiva que los productos de logging independientes a la hora de satisfacer los requisitos cada vez más exigentes de seguridad y de cumplimiento normativo.

- **CONSOLA FORENSE PARA INVESTIGACIÓN DE INCIDENTES**
- **ALMACENAMIENTO A LARGO PLAZO LOGS FIRMADOS DIGITALMENTE PARA CUMPLIMIENTO DE NORMATIVAS**
- **ESCALABILIDAD DISTRIBUIDA HORIZONTALMENTE CON ACCESO DESDE UNA SOLA CONSOLA**

El Logger USM es el componente para archivar datos con seguridad de la plataforma Gestión de Seguridad Unificada (USM™, Unified Security Management). USM le permite configurar, gestionar y operar más fácil y eficientemente las cinco acciones esenciales de seguridad que no deberían faltar en ninguna empresa: descubrimiento de activos, análisis de vulnerabilidades, detección de intrusiones, monitorización de comportamientos e información de seguridad y gestión de eventos (SIEM). La unificación de estas características esenciales de seguridad en una sola plataforma simplifica la gestión y reduce la complejidad, permitiendo emplear más tiempo en asegurar la red y menos tiempo en aprender, implementar y configurar herramientas.

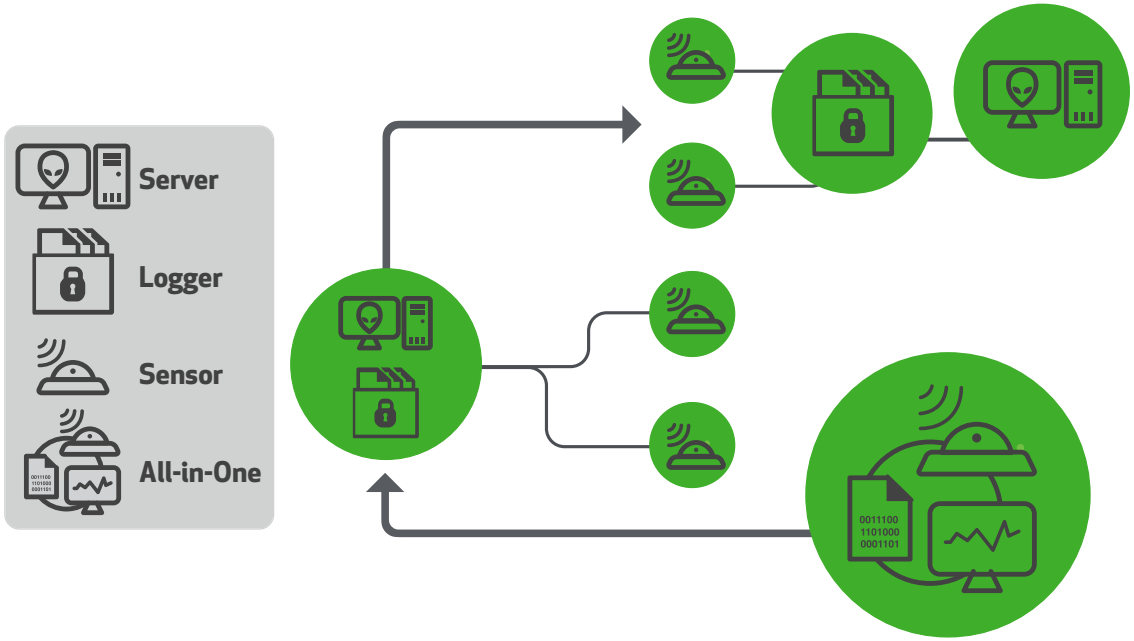
El Logger AlienVault ejecuta una tarea sencilla pero clave: almacena de forma forense todos los registros que produce su organización. Además de los numerosos requisitos de cumplimiento normativo relacionados con el mantenimiento de logs sin modificar, es importante tener una visibilidad completa del registro histórico con fines forenses. El Logger USM almacena información de acuerdo a las estrictas normas de seguridad del mercado. Recopila datos en su formato original, los firma digitalmente, les asigna un time-stamp, y los almacena con seguridad el formato sin modificar, preservando la integridad de los datos. De esta forma podrá explorar los datos con facilidad y aislar los datos que sean de su interés a través de la función integrada de búsqueda.

El Logger USM almacena grandes cantidades de datos, asegurando a la vez su admisibilidad como prueba forense en los juzgados. Puede aumentar aún más la seguridad del transporte de sus datos implementando túneles encriptados entre el Logger USM y la fuente del evento. El Logger de Datos USM es compatible con la mayoría de los sistemas de encriptado e incluye un cliente VPN para su uso en hosts de redes.

En ocasiones, los análisis forenses desencadenan la investigación de un evento relacionado o de cambios en las prácticas actuales de seguridad. El Logger USM permite el análisis forense y está completamente integrado en la plataforma USM de AlienVault, ofreciéndole un acceso ininterrumpido a los logs históricos desde la misma consola que la gestión de amenazas, descubrimiento de activos, la evaluación de vulnerabilidades, la detección de intrusiones, la monitorización conductual y la SIEM.

FUNCIÓN	BENEFICIO
REGISTRADOR	
Almacenamiento firmado digitalmente	Asegura la admisibilidad como prueba forense en los juzgados.
Compresión 5:1 [1]	Reduce los costes de almacenamiento.
Búsqueda integrada	Encuentra fácilmente los datos de interés.
Políticas de conservación centralizadas	Hace cumplir los requisitos normativos y corporativos de conservación de datos.

[1] El coeficiente de compresión medio experimentado por nuestros clientes es de 5:1. La compresión real puede ser mayor o menor, dependiendo del tipo de datos que se registren.



CONTÁCTENOS PARA SABER MÁS

WWW.ALIENVAULT.COM