Graylog Security

Empoderamos su ciberseguridad con tecnología SIEM avanzada

Graylog Security, disponible para usted a través de una experiencia autogestionada o SaaS, es una solución de ciberseguridad escalable que combina gestión de eventos e información de seguridad (SIEM), detección de amenazas y respuesta ante incidentes (TDIR), inteligencia de amenazas, investigación de incidentes y capacidades de detección de anomalías para ayudar a sus profesionales de seguridad a simplificar la identificación, la investigación y la respuesta a las amenazas cibernéticas.

SIEM impecable

Las organizaciones con recursos limitados necesitan detección de amenazas, análisis y respuesta a incidentes, e informes de cumplimiento proactivos y asequibles para fortalecer su postura de seguridad. Desarrollado sobre la plataforma Graylog, Graylog Security combina gestión de registros empresariales, detección de amenazas, pasos de corrección sugeridos e informes fáciles de implementar, gestionar y utilizar. Hemos diseñado nuestra plataforma de seguridad para brindarle la funcionalidad que necesita sin la complejidad y el costo de las soluciones SIEM tradicionales.

Graylog Security de un vistazo

UI centrada en la seguridad

Observe cómo aumenta su productividad y eficiencia con la exclusiva interfaz de usuario centrada en la seguridad de Graylog Security, diseñada para que los analistas accedan rápidamente a investigaciones, alertas y flujos de trabajo de informes.

Beneficios de Graylog Security

- Examine volúmenes de datos en segundos con capacidades de búsqueda ultrarrápidas
- Haga un seguimiento fácil de los activos e identifique rápidamente de dónde proviene un problema o registro
- Centre los esfuerzos de seguridad en lo más importante filtrando alertas falsas
- Aumente la productividad con una automatización en la que puede confiar para tareas repetitivas y que requieren mucha seguridad
- Aproveche un motor de aprendizaje automático de detección de anomalías que aprende continuamente sus comportamientos de seguridad con el tiempo

Puntuación basada en el riesgo

Céntrese en el riesgo "ahora mismo" con una puntuación automatizada basada en el riesgo. Graylog Security asigna una puntuación de riesgo a alertas individuales para que los analistas puedan priorizar los incidentes de seguridad fácilmente.

Búsqueda ultrarrápida para análisis forense y solución de problemas

Cada segundo cuenta cuando se trata de mantener su entorno seguro y protegido de las ciberamenazas. Graylog Security está diseñado para analizar terabytes de datos en segundos, lo que le permite encontrar datos de registro importantes en tiempo real. Acceda rápidamente al historial de consultas anterior en un menú desplegable fácil de usar.

Detección sensata de anomalías

Mantenha-se um passo à frente, mantendo as pessoas mal-intencionadas afastadas. Os recursos de detecção de anomalias do Graylog Security são projetados com um poderoso mecanismo de detecção de anomalias com aprendizagem de máquina (AM) que pode compreender automaticamente seu ambiente e alertá-lo sobre comportamentos anormais, para seus usuários e entidades (UEBA).

Identifique eventos de segurança prioritários em um mar de alertas

Manténgase a la vanguardia alejando a los actores de amenazas. Las capacidades de detección de anomalías de Graylog Security están diseñadas con un potente motor de detección de anomalías de aprendizaje automático (ML) que puede comprender automáticamente su entorno y alertarle sobre lo que no es un comportamiento normal para sus usuarios y entidades (UEBA).

Espacio de trabajo dedicado para investigaciones de incidentes

Gestione fácilmente las investigaciones de incidentes de principio a fin en Graylog Security con un espacio de trabajo todo en uno para recopilar y organizar conjuntos de datos, informes, pruebas y otros contextos mientras investiga un incidente o problema potencial, colabore entre equipos durante todo el proceso de investigación e identifique rápidamente tendencias utilizando datos guardados de investigaciones anteriores.

Encuentre rápidamente activos que supongan amenazas

El módulo de activos de Graylog Security le permite rastrear diferentes tipos de activos en todo el entorno y enriquecer los mensajes de registro con su información. La información sobre sus activos se puede añadir fácilmente a través de la UI de Graylog o sincronizarse a través de LDAP o AD.

Cobertura de amenazas seleccionada

Graylog Security lo ayuda a detectar amenazas en su entorno aprovechando técnicas cibernéticas avanzadas como detección de anomalías, reglas Sigma, inteligencia de amenazas y el marco MITRE ATT&CK®.

¿Qué tan bien está mitigando el riesgo?

Comprenda su resiliencia cibernética con Graylog Security midiendo los KPI de seguridad críticos que representan la eficacia con la que mitiga el riesgo para saber dónde centrar las iniciativas de mejora.

Reduzca el TCO al tiempo que fortalece su seguridad

Las capacidades nativas de la nube, la UI intuitiva y el contenido listo para usar de Graylog Security significan que puede comenzar a obtener datos valiosos de sus registros más rápido en comparación con los SIEM heredados. Reduzca sus costos de mano de obra con funciones diseñadas para reducir significativamente la fatiga de alertas, obtener respuestas rápidamente y empoderar a sus profesionales de seguridad. Aproveche un nivel "tibio" donde se pueden guardar los datos, lo que permite opciones de almacenamiento remoto o local menos costosas y, brindando al mismo tiempo la misma experiencia de búsqueda sólida y ultrarrápida.

Funciones potentes y ultrarrápidas

Detección de anomalías / UEBA
Capacidades que aprenden rápidamente el comportamiento "normal" e identifican automáticamente desviaciones para usuarios y entidades a escala, con ajustes y mejoras continuos con el tiempo.

Enriquecimiento de activos
Obtenga información sobre su entorno con la capacidad de hacer un seguimiento de diferentes activos y enriquecer los mensajes de registro con información adicional.

Informes de cumplimiento
Aproveche la funcionalidad del panel de control de Graylog para crear y configurar fácilmente informes programados.

Correlación y alertas
Reciba alertas por correo electrónico, mensajes de texto, Slack y más. Actualice los criterios de alerta en función de una lista dinámica en una tabla de búsqueda.

Normalización y enriquecimiento de datos
Realice una investigación más rápida añadiendo WHOIS, geolocalización de IP e inteligencia de amenazas u otros datos estructurados.

Registros de usuarios de Graylog
Haga un seguimiento de quién accedió a qué datos de registro y qué acciones tomó contra ellos para garantizar el cumplimiento y la seguridad.

Investigación de incidentes
Espacio de trabajo todo en uno para recopilar y organizar conjuntos de datos, informes, pruebas y otros contextos mientras se investiga un posible incidente.

Paneles de control prediseñados, alertas
Comience rápidamente con contenido prediseñado para casos de uso de seguridad: plantillas de búsqueda, paneles de control, alertas correlacionadas, tablas de búsqueda dinámicas y más.

Generador de consultas de búsqueda
Cree y combine múltiples búsquedas para cualquier tipo de análisis en una sola acción y exporte los resultados a un panel de control.

Paneles de control de análisis de seguridad
Combine widgets para crear visualizaciones de datos personalizadas y automatizar la entrega de informes en su bandeja de entrada.

Integraciones SOAR
Comparta datos fácilmente con otros sistemas críticos para el negocio para lograr total transparencia y colaboración.

Fuentes de inteligencia sobre amenazas
Añada contexto a los datos del registro de eventos con sus fuentes de inteligencia sobre amenazas existentes e identifique posibles problemas de seguridad.

graylog SECURITY

Consulte a nuestros expertos y vea Graylog Security en acción

Definitivamente ver es creer. En Graylog, queremos que obtenga respuestas a todas sus preguntas antes de comprar. Ofrecemos demostraciones de productos programadas que demuestran la funcionalidad del producto y dan tiempo para una sesión de preguntas y respuestas. **Programe su demostración de Graylog Security hoy mismo** y vea nuestra poderosa plataforma de ciberseguridad en acción.

Graylog Security le permite obtener información sobre las correlaciones de eventos en decenas de miles de componentes de red para detectar amenazas identificadas o actividades sospechosas.

Acerca de Graylog

Graylog es líder en gestión de registros y en gestión de eventos e información de seguridad (SIEM), haciendo que el mundo y sus datos sean más eficientes y seguros. Desarrollado por profesionales pensando en profesionales, Graylog desbloquea respuestas a partir de datos para miles de profesionales de TI y seguridad que resuelven problemas de seguridad, cumplimiento, operación y DevOps todos los días. Graylog, implementada en más de 50,000 instalaciones en todo el mundo, es una plataforma galardonada diseñada para ofrecer velocidad y escala en la captura, el almacenamiento y la habilitación de análisis en tiempo real de terabytes de datos de máquinas. Graylog elimina el ruido y ofrece una experiencia de usuario excepcional haciendo que el análisis de datos, la búsqueda de amenazas, la detección y la investigación de incidentes sean rápidos y eficientes utilizando una arquitectura más rentable y flexible.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog