grupo ica
Sistemas y Seguridad

LogICA NGSIEM

El mejor aliado de los analistas de seguridad

Reúne toda la información de seguridad relevante

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas. La falta de visibilidad de la red, los análisis manuales que consumen mucho tiempo y la falta de contexto, afectan negativamente a la eficiencia de los equipos. LogICA NGSIEM es un sistema automatizado de gestión de información y eventos de seguridad que recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que sucedan.

Toma decisiones contextualizadas y rápidas

LogICA NGSIEM consume cantidades masivas de datos que proceden de valiosas fuentes externas, internas y de terceros. Una vez recogida toda esta información, la agrega, analiza y contextualiza en un único lugar.

LogICA NGSIEM consigue analizar más de 100.000 eventos por segundo. Sus capacidades SOAR facilitan la orquestación entre múltiples fuentes, reducen los falsos positivos, permiten establecer un triaje y una priorización de incidentes y facilitan la respuesta automática ante amenazas conocidas.

Con LogICA NGSIEM, la eficiencia de los equipos de seguridad aumenta en un 32% y son capaces de identificar un 22% más de amenazas antes de lleguen a causar graves consecuencias.

LogICA NGSIEM

- Detecta y resuelve amenazas en tiempo real.
- Prioriza e investiga incidentes relevantes.
- Punto único de control y almacenamiento centralizado.
- Responde de forma automática -SOAR-.
- Analiza el comportamiento del usuario -UEBA-.
- Ciberinteligencia de Amenazas.
- Tecnología española alineada con la Estrategia Nacional de Ciberseguridad.

info@grupoica.com

www.grupoica.com

Obtén una imagen completa y real del riesgo

LogICA NGSIEM permite la monitorización de eventos de cualquier dispositivo, sistema o aplicación. La gestión de la seguridad de LogICA NGSIEM tiene en cuenta tres estadíos temporales: el histórico de eventos, la acción en tiempo real y la acción preventiva. El primero recoge y salvaguarda en un sistema protegido cualquier registro de información, posibilitando realizar búsquedas avanzadas de eventos y desarrollo de análisis avanzados.
La ingestión de eventos en modo streaming permite el análisis y la alerta en tiempo real. El tratamiento de datos históricos a través del análisis estadístico y el uso de algoritmos complejos facilitan el reconocimiento de bandas de normalidad, tendencias y puntos débiles, anticipándose a las amenazas.

Descubre amenazas empleando las técnicas de detección más avanzadas

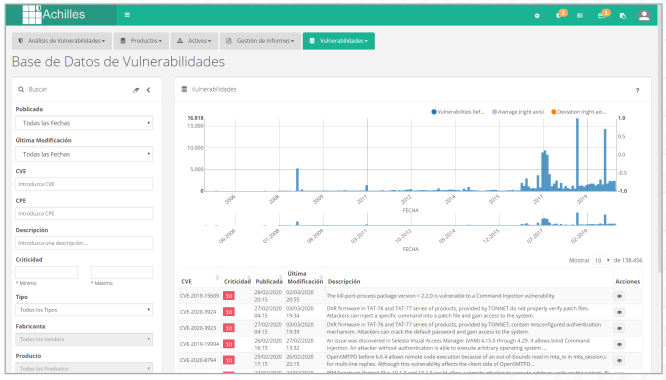
LogICA NGSIEM emplea las técnicas más avanzadas de recopilación y análisis de datos, como el aprendizaje automático, la ciberinteligencia de amenazas y el análisis del comportamiento del usuario (UEBA). De esta manera, los equipos de seguridad pueden centrarse en lo que realmente importa y añadir otros insights con un nivel de personalización que es complicado replicar con máquinas. LogICA NGSIEM permite a los analistas identificar amenazas a una velocidad 10 veces mayor, ayudando a resolver incidentes de seguridad un 63% más rápido.

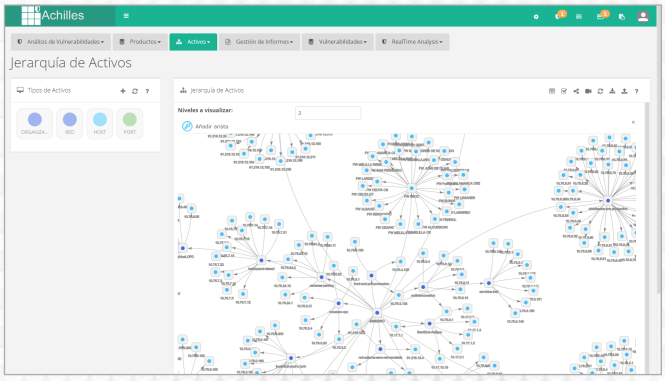
Monitoriza y gestiona incidentes de forma sencilla

La consola de operación y administración de LogICA NGSIEM está basada en HTML5, lo que permite acceder desde cualquier navegador con protocolo HTTP seguro. Además, cuenta con tecnología responsive para PC, Tablet, Smartphone. Los cuadros de mando favorecen la visualización personalizada de la información y la función drill down permite analizar los datos con un mayor nivel de detalle. El editor de informes permite personalizar y automatizar la generación y notificación de incidentes, amenazas e indicadores.

El único SIEM nacional y europeo incluido en CPSTIC

Las funcionalidades de seguridad de LogICA NGSIEM están certificadas por el Centro Criptológico Nacional (CCN). LogICA NGSIEM, está incluido en su Catálogo de Productor (CPSTIC) y posee la clasificación Esquema Nacional de Seguridad (ENS) Alta que lo habilita para ser empleado en sistemas afectados por el ENS en cualquiera de sus categorías: Alta, Media y Básica.





grupo ica
Sistemas y Seguridad

info@grupoica.com

www.grupoica.com