MONICA NGSIEM

El mejor aliado de los analistas de seguridad

Mónica NGSIEM

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

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. **Mónica 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. **Mónica NGSIEM triplica la productividad** de un equipo de ciberseguridad y permite alcanzar un retorno de la inversión completo en solo cuatro meses.

Toma decisiones más contextualizadas y rápidas

Mónica NGSIEM consume cantidades masivas de datos que proceden de fuentes técnicas, investigaciones, fuentes abiertas, fuentes ocultas, redes sociales, fuentes internas y de terceros. Una vez recogida toda esta información, la agrega, analiza y contextualiza en un único lugar.

Ayudado por el aprendizaje automático y la automatización, **Mónica NGSIEM** consigue analizar más de 100.000 eventos por segundo, frente a los 4.800 eventos que una persona es capaz de procesar en un día. 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 **Mónica 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.

Obtén una imagen más completa y real del riesgo

La gestión de la seguridad de **Mónica 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**.

Aprovecha la visibilidad completa de tu infraestructura tecnológica

Mónica NGSIEM permite la monitorización de eventos de cualquier dispositivo, sistema o aplicación. Entre los agentes intranet, se pueden encontrar dispositivos de seguridad lógica, de electrónica de red, servidores web, sistemas gestores de bases de datos, sistemas operativos y de seguridad de Host o aplicaciones propietarias. Por otro lado, los portales web de clientes y proveedores, aplicaciones cloud-store y aplicaciones no corporativas, se encuentran entre los agentes extranet, mientras que los agentes ambiente incluyen redes sociales, páginas web y blogs, sistemas de información no TIC y dispositivos de seguridad física.

Descubre amenazas empleando las técnicas de detección más avanzadas

La recopilación, análisis y entrega automatizada de datos proporcionan inteligencia en tiempo real a escala. **Mónica 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. **Mónica 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 más fácil que nunca

La consola de operación y administración de **Mónica NGSIEM** está basada en HTML5, lo que permite acceder desde cualquier navegador con protocolo HTTP seguro. Además, cuenta con tecnología responsive capaz de adaptarse a cualquier dispositivo de usuario (PC, Tablet, Smartphone). Los cuadros de mando favorecen la visualización personalizada de la información y la función drill down por vínculos entre pantallas de operación te permite analizar los datos con un mayor nivel de detalle. El editor de informes integrado y el planificador asociado permiten también personalizar y automatizar la generación y notificación de incidentes, amenazas e indicadores.

El único SIEM nacional y europeo incluido en CPSTIC

Funcionalidades de seguridad han sido certificadas por la principal institución española en materia de ciberseguridad, el Centro Criptológico Nacional (CCN). Este organismo dependiente del Centro Nacional de Inteligencia (CNI) ha incluido nuestro NGSIEM en su Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC). La larga trayectoria de **Mónica**, nacido hace más de 15 años, sigue demostrando sus grandes capacidades y alta calidad.

Mónica es un producto certificado en sus funcionalidades de seguridad, clasificado 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.

Integración con otras soluciones CCN-CERT

</carmen> </lucía> </pilar> </claudia> </sat-inet>

</mónica>

monica@ccn-cert.cni.es

www.ccn-cert.cni.es

Common Criteria

PRODUCTO SEGURIDAD TIC CCN Centro Criptológico Nacional CUALIFICADO

CCN-CERT centro criptológico nacional