Soluciones de Ciberseguridad

SIEM as a Service

Log Management, Security Event Management, Security Information Management y Security Event Correlation. Todo como servicio, en una cuota mensual y bajo SLA.

¿Se han mirado hoy los logs? Lo que desconoces *puede* perjudicarte

El problema en la gestión de logs en sistemas informáticos actuales se descompone de tres partes:

Cada día se manejan más y más datos de más y más sistemas, que a su vez generan más logs que nunca.

El aumento del volumen de datos combinado con la heterogeneidad de los mismos, ha hecho que la complejidad de gestión se dispare.

Y por último, la tercera parte del problema es el tiempo disponible del personal del departamento de TI. ¿Se han mirado hoy los logs?

¿Qué es un SIEM (Security information and event management)?

Un SIEM es una herramienta informática que nos permite garantizar la recogida de todos los logs de nuestros diferentes sistemas, pudiendo gestionar eventos o alertas relacionados con dichos logs, y creando, almacenando y distribuyendo informes generados a partir de toda la información gestionada. Esto nos permite generar correlaciones entre eventos: Si pasa esto aquí y allá sucede lo otro, entonces puede estar pasando esto, detectando de manera muy temprana las amenazas.

SIEM as a Service de Nologin

Usando IBM QRadar SIEM, se procesan los eventos (logs) y flujos de red en tiempo real de manera no intrusiva, sin afectar al rendimiento de la infraestructura productiva.

Gracias al conocimiento de Threat Intelligence compartido por IBM y otras fuentes, se pueden correlar los eventos y flujos, clasificarlos, valorarlos y responder a amenazas que se hayan reportado en cualquier lugar del mundo.

Se ofrece como servicio, en una cuota mensual y bajo SLA.

Gold Business Partner

Competency Threat Management

Authorized Systems and Storage Storage

Nuestro SIEM se integra con LUCÍA

Nuestro SIEM se integra con LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

Beneficios de las soluciones SIEM

- Aumento de eficiencia.
- Prevención de brechas de seguridad
- Identificación de ineficiencias operativas
- Reducción de impacto de incidentes o caídas de sistema
- Ahorro de costes
- Mejora de los sistemas de reporting
- Cumplimiento de normativa GDPR
- Control total de las constantes vitales de los sistemas informáticos.

"Lo más atractivo de un SIEM gestionado por un grupo especializado, es la economía de conocimiento que genera. Con nuestro equipo de expertos el despliegue es mucho más rápido y ante cualquier incidente que se produzca ya conocemos la solución. Eso, en un equipo interno, llevaría semanas resolverlo."

¿Por qué un SIEM como servicio?

- Reducción de la complejidad de la solución
- No es necesario operar sistemas complejos ni formar al equipo
- Se transforman costes CAPEX a OPEX
- Se reduce el pasivo laboral
- SLA garantizado bajo contrato:monitorización y SOC en 24x7
- Reducción del tiempo de resolución de incidencias
- Predicibilidad de costes
- Reducción de casi un 50% de coste a 5 años
- Evolución del sistema garantizada

Siempre en contacto

24x7

El sistema está gestionado en 24x7 por nuestros ingenieros.

Un sistema de tickets permite interactuar al equipo de IT del cliente con Nologin dando soporte para solucionar los incidentes de seguridad detectados.

SIEM as a Service de Nologin

Requisitos para la gestión de los servicios de seguridad

Nologin satélite

Todo el procesamiento de datos se hace en los sistemas de Nologin. Para ello, hay dos opciones:

A) La instalación de un colector de registros para centralizar los registros del activo y enviarlos al SIEM de Nologin.

B) O enviar los registros directamente al SIEM centralizado sin ningún satélite instalado.

Requisitos Globales

Acceso VPN a la infraestructura	Los servidores utilizados por Nologin para proporcionar el servicio se encuentran en nuestros dos centros de datos. Las VPNs de sitio a sitio deben establecerse desde estos dos sitios y los centros de los clientes, así que las comunicaciones serán seguras y aseguraremos la redundancia y los bajos tiempos de salida. Nos adaptaremos a las tecnologías VPN utilizadas por los clientes usando estándares VPN
Lista de contactos	El cliente proporcionará todos los contactos que tendrán acceso a las herramientas utilizadas por Nologin para la gestión del servicio.
Gestión de servicios	Todas las tareas relacionadas con la correcta gestión comercial y operativa quedan en el lado del cliente.

nologin

Nologin Consulting S.L.U. es una compañía dinámica con un alto grado de conocimiento en el entorno de las Tecnologías de la Información, que ofrece a sus clientes servicios y soluciones de calidad para definir, implantar y administrar sus Sistemas Informáticos y de Comunicaciones.

(+34) 976 512 433 | www.nologin.es.

Nologin ESPAÑA

Zaragoza Avda. de Ranillas 1D, Of.3G, 50018

Madrid Paseo de la Castellana 216, planta 8ª, Of. 811 , 28046

Si se encuentra fuera de España, puede encontrar información de la oficina más cercana en nuestro sitio web.