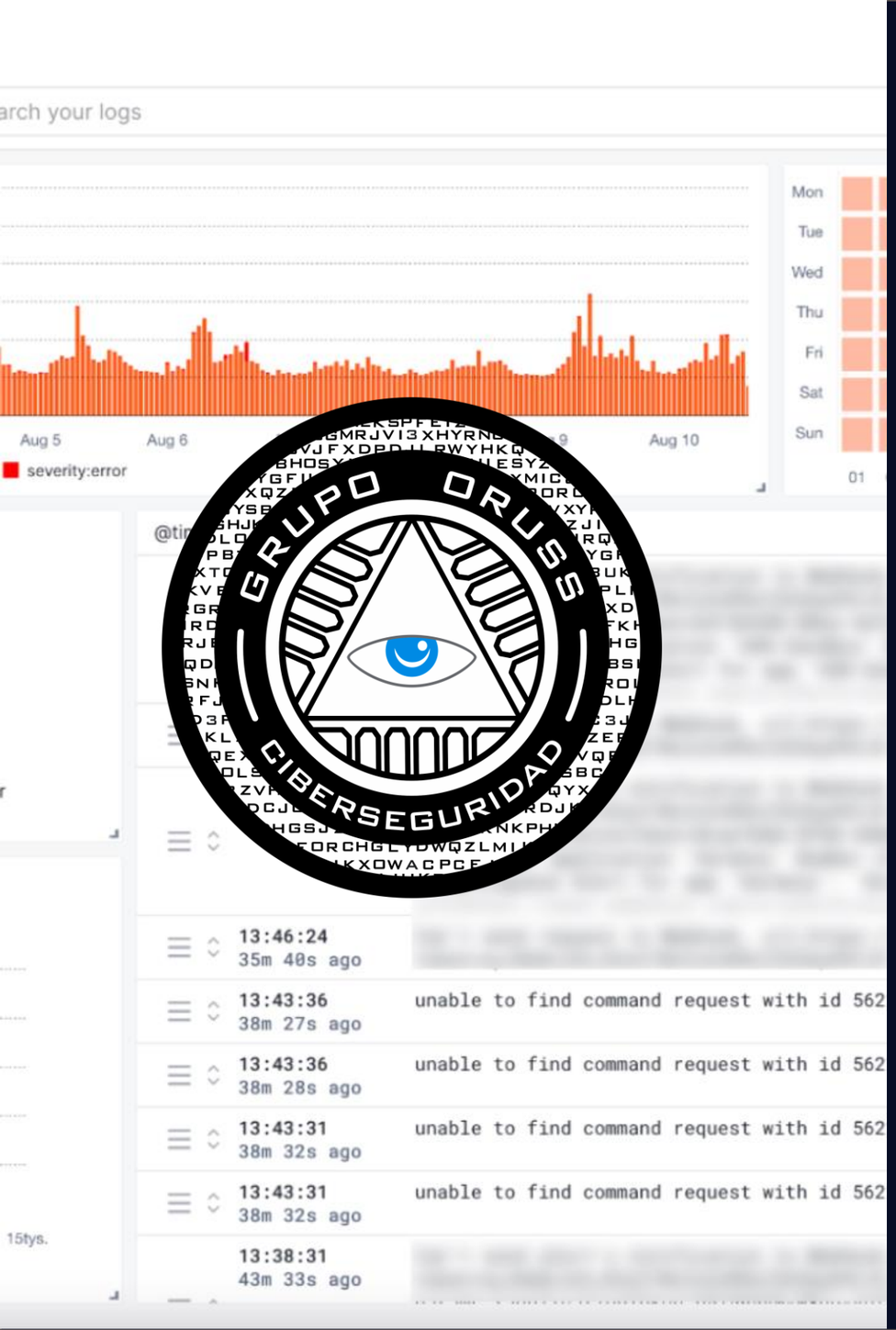


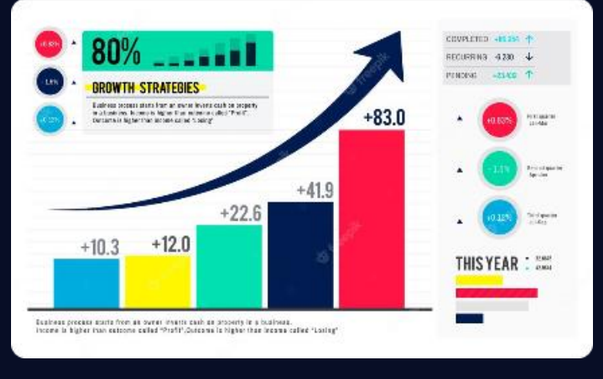

# Logs y Monitorización: Detectando ataques en tiempo real.

Los ataques cibernéticos son cada vez más sofisticados. La monitorización de monitorización de logs se ha vuelto esencial para detectar amenazas de de seguridad. En esta presentación te mostraremos cómo hacerlo en tiempo tiempo real.

# La importancia de la monitorización de logs

## Seguridad del sistema

Los logs son una ventana al sistema y monitorearlos permite permite detectar problemas de de seguridad en tiempo real.




## Entendiendo tu sistema

Análisis de logs puede ayudar a entender el comportamiento del sistema y optimizar su rendimiento.

## Colaboración de equipos

Compartir información en tiempo tiempo real permite que los equipos de seguridad trabajen trabajen juntos de manera eficiente y efectiva.

# Qué son los logs

1

## Registro de Eventos

Los logs son registros de eventos que se generan en un sistema o aplicación. Registran todo lo que sucede.

2

## Importancia de la Estructura

Para que sean útiles, deben tener una una estructura clara y organizada que que permita buscar y filtrar información. información.

3

## No Son Solo para Análisis

Además de la monitorización y el análisis, análisis, los logs también son importantes importantes para la investigación de incidentes.

# Cómo realizar la monitorización en tiempo real

## Configura tus Reglas

Identifica patrones de actividad para crear reglas reglas que te ayuden a detectar amenazas o problemas de seguridad.

## Automatiza Alertas

Crea alertas automáticas para que puedas actuar rápidamente ante cualquier amenaza o problema.

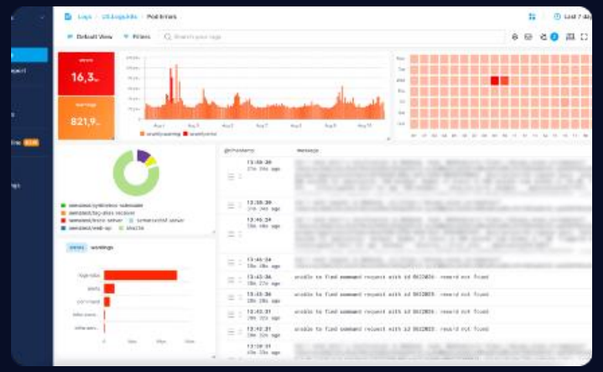
## Configura Métricas

Establece métricas que te permitan evaluar el rendimiento del sistema y detectar cambios o problemas.

## Usa Herramientas de Monitoreo

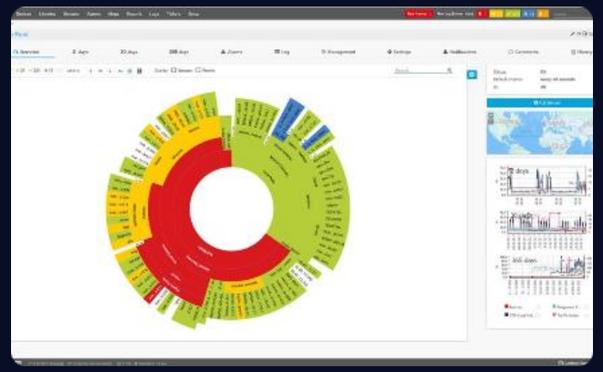
Las herramientas de monitoreo en tiempo real te real te permiten visualizar eventos y logs en una una interfaz fácil de usar.

# Herramientas para la detección de ataques



## Gestión de Logs

Hay herramientas de gestión de de logs que permiten recopilar y recopilar y almacenar logs de manera centralizada.



## Detección de Amenazas

Las herramientas de detección de detección de amenazas pueden pueden identificar patrones anómalos en los logs y alertar sobre ellos.


## Análisis de Tráfico de Red Red

Las herramientas de análisis de de tráfico de red pueden observar observar los logs del tráfico de red de red para detectar patrones anormales.

# Indicadores de ataques en los logs

1

## Horarios inusuales

Los ataques suelen ocurrir fuera de las horas de oficina.

2

## Direcciones IP sospechosas

Identifica direcciones IP sospechosas, sospechosas, especialmente aquellas que que tienen un historial de ataques.

3

## Acciones anómalas

Busca acciones inusuales, como múltiples múltiples intentos fallidos de inicio de de sesión o descargas masivas de archivos. archivos.

# Conclusiones y recomendaciones

1

## La monitorización de logs es crucial para la seguridad

Sin ella, los atacantes podrían pasar desapercibidos y comprometer tu sistema. sistema.

2

## Adoptar un enfoque proactivo

En lugar de esperar a ser ser atacado, procura detectar y prevenir ataques antes de que sucedan.

3

## Considera la automatización

La automatización puede puede ser útil para reducir reducir la carga de trabajo trabajo que implica la monitorización de logs.

**Apoya tu proceso de remediaciones con:**

# ALINA

ALINA es un innovador chatbot impulsado por Inteligencia Artificial que te ayudará a resolver las remediaciones propuestas en este informe.

https://grupooruss.com/alina


# ¡Gracias!

www.grupooruss.com