



Caso de estudio

ESTUDIO DE CASO 1: Métodos Avanzados de Ordenamiento en un Sistema SIEM

Contexto

Una organización financiera implementa un SIEM (Security Information and Event Management) que recibe más de 2 millones de eventos diarios provenientes de firewalls, IDS, servidores y endpoints.

Los eventos llegan desordenados y deben clasificarse por:

- Fecha y hora
- Nivel de severidad
- Dirección IP

El sistema inicialmente utilizaba ordenamiento básico (Bubble Sort), generando retrasos significativos.

Problema

El tiempo de procesamiento superaba los 40 segundos por lote de 100.000 registros, afectando la capacidad de respuesta ante incidentes críticos.

Solución Propuesta

Se evaluaron tres algoritmos avanzados:

Merge Sort

- Garantiza $O(n \log n)$
- Estable (útil para mantener orden por timestamp)
- Requiere memoria adicional

Quick Sort

- Muy rápido en promedio
- Bajo consumo de memoria
- Riesgo de peor caso $O(n^2)$

Heap Sort

- Garantiza $O(n \log n)$
- Espacio $O(1)$
- Ideal para priorización

Implementación y Resultados

Después de pruebas controladas:

Algoritmo	Tiempo promedio (100k eventos)
Bubble Sort	40 s



Caso de estudio

Algoritmo	Tiempo promedio (100k eventos)
Merge Sort	2.1 s
Quick Sort	1.8 s
Heap Sort	2.3 s

Quick Sort mostró mejor rendimiento promedio. Sin embargo:

- Merge Sort fue elegido para ordenamiento por timestamp (estabilidad).
- Heap fue utilizado para priorización de alertas críticas.

Resultados

- Reducción del tiempo de procesamiento en 95%.
- Mejora en detección temprana de incidentes.
- Mayor escalabilidad ante crecimiento de datos.

Reflexión

Los métodos avanzados de ordenamiento no solo mejoran eficiencia, sino que impactan directamente la capacidad de respuesta en ciberseguridad. La elección del algoritmo depende del contexto: estabilidad, memoria disponible y comportamiento del peor caso.