PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Implementación de Árboles Binarios de Búsqueda en un Sistema SIEM para Optimización de Consultas de Seguridad

ESTUDIO DE CASO 1: Implementación de Árboles Binarios de Búsqueda en un Sistema SIEM para Optimización de Consultas de Seguridad

Contexto

Una institución financiera internacional implementa un sistema SIEM (Security Information and Event Management) que recibe aproximadamente 3 millones de eventos diarios provenientes de firewalls, IDS/IPS, servidores y aplicaciones críticas.

Cada evento contiene:

- Timestamp
- Dirección IP origen
- Nivel de severidad
- Tipo de incidente

Inicialmente, los eventos se almacenaban en una lista enlazada. Las búsquedas de registros históricos (por timestamp o IP) requerían recorridos completos, generando tiempos de respuesta elevados.

Problema

Durante un intento de ataque coordinado, el equipo de seguridad necesitaba:

- Identificar eventos entre dos rangos de tiempo específicos.
- Consultar rápidamente registros asociados a una IP sospechosa.
- Analizar patrones históricos en tiempo real.

El tiempo promedio de consulta era de 6 a 8 segundos, lo que retrasaba la respuesta ante amenazas activas.

Solución Propuesta

Se implementó un Árbol Binario de Búsqueda (BST) para indexar los eventos por timestamp.

Estrategia:

- Cada nodo almacenaba un evento.
- El árbol se organizó según el timestamp.
- Se aplicaron recorridos Inorden para recuperar registros cronológicamente.
- Se implementaron búsquedas por rango.

Implementación

1. Insertar cada evento según su timestamp.
2. Usar búsqueda logarítmica para localizar eventos específicos.
3. Aplicar recorrido Inorden para obtener historial ordenado.
4. Implementar filtros adicionales por IP y severidad.

Resultados

Métrica	Antes (Lista)	Después (BST)
Tiempo promedio de búsqueda	6–8 s	0.9 s
Consulta por rango	7 s	1.2 s
Uso de CPU	85%	55%

Se logró una reducción del 80% en tiempo de consulta.

Impacto en Ciberseguridad

- Respuesta más rápida ante incidentes.
- Mejor correlación de eventos.
- Mayor eficiencia en análisis forense.
- Escalabilidad ante crecimiento de datos.

Reflexión Técnica

La elección adecuada de estructuras de datos impacta directamente en la capacidad operativa de un SOC. Un BST permite mantener orden dinámico y realizar búsquedas eficientes; sin embargo, si el volumen crece significativamente o los datos llegan ordenados, puede ser necesario migrar a un árbol balanceado (AVL o Red-Black) para garantizar estabilidad en el peor caso.

En ciberseguridad, la optimización algorítmica no es opcional: es un componente estratégico para la resiliencia del sistema.