Sofia Moreno Lopez A1028251
(en equipo con Nicole Davila)

La detección de infecciones en una red representa un desafío crítico en el ámbito de la ciberseguridad, ya que puede determinar si se produce la filtración de información confidencial de usuarios, permisos de administrador o incluso provocar la caída completa de la red. Para abordar este tipo de problemas, una solución eficiente podría ser la implementación de árboles de búsqueda binaria como una estructura de datos clave en la gestión y búsqueda de información relevante para la detección de amenazas cibernéticas.

La elección de un árbol de búsqueda binaria se justifica por su complejidad promedio de O(log n), lo que representa un algoritmo altamente rápido y crucial cuando se trata de buscar información específica sobre comportamientos sospechosos en la red. Esto implica la búsqueda de registros de tráfico de la red en momentos específicos, patrones de comportamiento, recuento de accesos por dirección IP, entre otros.

La simplicidad en la identificación de patrones en los datos es otro beneficio significativo de los árboles de búsqueda binaria. Al almacenar firmas de malware o patrones conocidos como comportamientos maliciosos, el sistema puede realizar búsquedas rápidas para verificar la existencia de coincidencias en el tráfico de la red. Esta capacidad agiliza el proceso de identificación y respuesta ante posibles amenazas.

Además, los árboles de búsqueda binaria permiten realizar inserciones y eliminaciones de manera eficiente, lo cual es vital para mantener actualizadas las bases de datos de amenazas en un entorno donde la evolución rápida de las mismas es la norma. La capacidad de adaptarse rápidamente a nuevos patrones y amenazas contribuye significativamente a la efectividad del sistema de detección y protección cibernética en general.