Contribution ID: **269** Type: **not specified**

Tracking Files across the operating system using eBPF

Given the increasing concerns around user data and AI model theft, we prioritized developing robust mechanisms to monitor critical files throughout the file system. Leveraging eBPF, we implemented real-time detection for the creation of sensitive files and established comprehensive tracking of their lifecycle events, including renames, moves, deletions, compression, decompression, and uploads. This security enhancement enables us to maintain a detailed lineage of each file, facilitating the identification of unauthorized access or sharing attempts.

A key challenge was designing a reliable method to tag files for persistent tracking, ensuring that identifiers remain consistent even as files are renamed or transformed. Developing heuristics to detect uploads and downloads proved complex, since these actions can occur through various system calls and network behaviors.

Looking ahead, there are several technical directions for expanding this capability. One promising approach is to extend file tracking to cover transfers between systems within our visibility scope, allowing us to monitor file movements not just locally but also across multiple hosts. This would further strengthen our ability to detect and respond to potential data exfiltration or misuse at scale.

Primary author: EL KHOURY, Carl

Presenter: EL KHOURY, Carl

Session Classification: eBPF Track

Track Classification: eBPF Track