MANAGED SECURITY SOLUTIONS

File Integrity Monitoring (FIM)

The Last Line of Defense Against Threats That Evade Your Firewall

Undetected cyber threats often remain undetected on target networks for weeks or even months. Our host-based intrusion detection system is your last line of defense against threats that evade your firewall, NIDS, and antivirus.

File Integrity Monitoring (FIM) tracks file modifications on a host, regardless of whether these changes were made by a user or a service. Quite often, this is the only way to validate whether or not an attack has been successful. In addition to being an essential component of any security program, FIM is also a core requirement of many industry compliance frameworks including PCI DSS.

Key Benefits

Host-based file integrity monitoring is often the only way to validate whether a threat has caused any genuine harm. Our file integrity monitoring (FIM) experts use proprietary technologies and processes to ensure the integrity of critical system files and detect unauthorized changes in real-time.

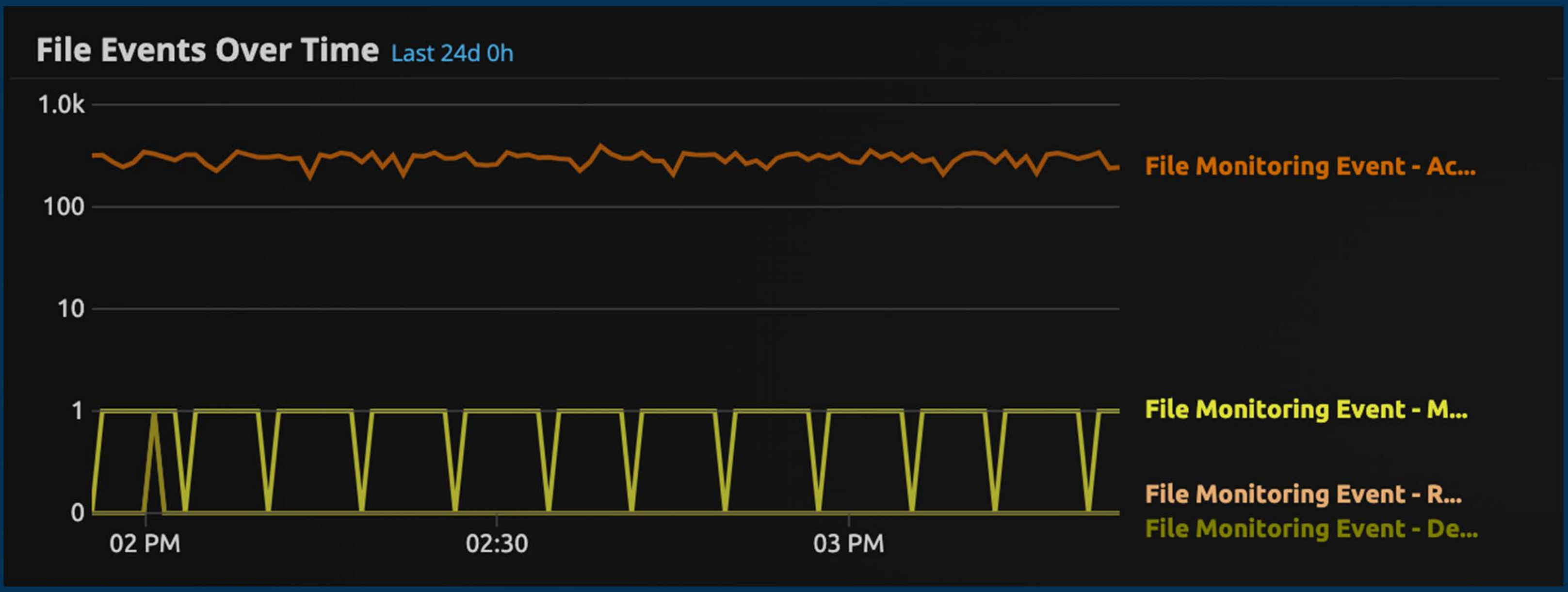
Protect Critical Files From Unauthorized Changes

Suitable For All Compliance Frameworks

Last Line Of Defense Against Sophisticated Threats

File Access Activity

Monitoring file access activity provides valuable contextual data when investigating security incidents. When compared against a baseline this can help highlight suspicious or irregular activity, sometimes exposing insider threats. It's also helpful when analyzing malware and exploit activity as it can help quickly identify what files have been dropped or modified. File integrity monitoring is a critical component of most compliance strategies.


File Events Over Time
Last 24d 0h
1.0k
02 PM
02:30
03 PM
File Monitoring Event - Ac...
File Monitoring Event - M...
File Monitoring Event - R...
File Monitoring Event - De...