whitepaper

The Benefits of Integrating File Integrity Monitoring with SIEM

solarwinds

Security Information and Event Management (SIEM) is designed to provide continuous IT monitoring, actionable intelligence, incident response, and regulatory compliance support. It identifies suspicious and malicious behavior by compiling logs from all security and security-relevant devices as well as systems and applications. Still, as attacks are becoming more difficult to detect, logs alone cannot provide the level of intelligence required to ensure data and network security. In addition, compliance audits are moving toward a risk-based format.

A SIEM is only as intelligent as the data it absorbs. Therefore, SIEM presents only part of the security picture. Many of the most damaging attacks are detected only by understanding file activity, which is difficult to log meaningfully. Intelligent monitoring of file activity and integrity helps complete the picture by providing critical information that helps detect stealthy attacks and zero-day malware. It also provides insight into insider activity.

Security threats are on the rise. Therefore, you need to regularly monitor your corporate data (intellectual property assets, software programs and codes, financial and earnings data, and customer account information) and maintain its integrity by restricting access to only authorized users. Enter file integrity monitoring.

File Integrity Monitoring (FIM) is the process of monitoring access and changes to system files. This enables organizations to better protect sensitive information from theft, loss, and malware attacks by closely watching who accesses and modifies files. In many industries, including FIM as an IT security component is required for meeting regulatory compliance standards such as PCI DSS, HIPAA, and SOX. The scope of FIM is not limited to only the content contained in files and folders, but also the integrity of system directories, registry keys, and values on the operating system.

By monitoring changes to files in real-time, you gain additional insight into many security threats, which helps prevent breaches.

Security Benefits of File Integrity Monitoring

- Protects sensitive data and files from unauthorized access and changes.
- Provides visibility into what file changed, when it was changed, and who changed it.
- Tracks file and directory access, movement, and shares.
- Detects zero-day malware, which can change key system files and executables, or create/install a malicious process or driver.
- Identifies insider abuse and protects sensitive data from being misused by employees.
- Gives insight into advanced persistent threats (APT), which are generally hard to detect. When you identify an unwarranted file change, it might be due to an APT attack.

It's not always malicious intent, malware, or a cyber-attack that causes changes to file content. File integrity breaches also occur within the scope of the file management lifecycle which includes transmission errors, software bugs, storage errors, write errors, and incorrect change-management procedures. By proactively monitoring changes and access to files, you can detect these errors and prevent your files from further impact.

Scope of File Integrity Monitoring

The scope of File Integrity Monitoring is broad. The more attributes you can monitor, the better data security you have. Typically, you should be able to monitor:

- When a file was accessed/created/modified/moved/deleted
- Login name of the user who accessed/modified a file
- Changes to attributes such as Read-Only, Hidden, etc.
- Changes to security access permissions
- Changes to directories and registry keys
- Changes to a file's group ownership

To ensure the integrity of all secure files, you need your file monitoring to include key content/data files, database files, Web files, audio/video files, system binaries, configuration files, and system registries.

Compliance Standards Require File Integrity Monitoring

Ensuring file integrity and detecting malicious attacks on secure data is a requirement of many popular compliance guidelines (listed below).

Compliance Standard	Section Addressing File Integrity Monitoring
Payment Card Industry Data Security Standard (PCI DSS)	Requirement 10.5.5 & 11.5
Sarbanes-Oxley Act (SOX)	Section 404
NERC Standard CIP	System Security (R15-R19)
Department of Defense Information Assurance Implementation (DIACAP)	DODI 8500.2
Federal Information Security Management Act (FISMA)	NIST SP800-53 Rev3
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	NIST Publication 800-66
SANS Critical Security Controls	Control 3

Challenges with File Integrity Monitoring

There are typically two approaches to file integrity monitoring.

1. Hash-based File Integrity Checking:

Scans critical files on systems on a regular schedule and alerts admins about detected changes by comparing the hash to the previous version. The alternative to this is you need to schedule this task to run according to a specified time interval. However, this way you miss out on all the times the checking is in progress. Also, this method is best suited for actual file changes—not file access and reads.

2. Real-time File Integrity Checking:

The actual file auditing process that captures real-time file access and changes within file audit events. By analyzing these events in real-time, you are able to get information on not just file changes, but also all the file read, write, and create events. The setback with this approach is dealing with a large volume of events to pinpoint the violation you are looking for.

In Windows® systems, FIM can be performed by gathering file audit events from a specific file, folder, or an entire system and analyzing the event logs to see file-change attributes. This is easier said than done.

One challenge with enabling native Windows file auditing and using Windows Event Viewer to detect file changes is you end up receiving numerous events (mostly false-positives) and sifting through all of them to find the exact event that reveals a breach. Another challenge is knowing the exact event ID to pinpoint a violation. You need to spend more time and effort searching for these event IDs and find a way to eliminate all the noise and extraneous events generated in the file auditing process.

The Best File Integrity Monitoring Approach: Integration with SIEM

The insight gained through File Integrity Monitoring is best used when it is fed into the broader event stream from log data collected from various parts of your network (workstations, servers, domain controllers, file servers, antivirus software, IDS/IPS systems, etc.). This data can be correlated to produce situational awareness between diverse events.

SIEM systems already collect log data from across your IT infrastructure for correlation and analytics. When you combine FIM events with SIEM, you can achieve a more robust security system that offers defense in depth threat intelligence to detect advanced and sophisticated threats.

Some applications of combining FIM with SIEM include:

User-aware File Integrity Monitoring:

System, Active Directory® (AD), and file audit events are correlated to obtain information on which user was responsible for accessing and changing a file. You can also identify other activities of the user before and after the file change for complete user activity monitoring.

Data Loss Prevention:

Correlating file audit events with other log data gathered by SIEM provides advanced threat intelligence, which is useful for pinpointing breach attempts. With the remediation capability of SIEM, you can automate responsive actions (shut down systems, detach USB devices, disconnect systems from the network, log off users, disable user accounts, etc.) to safeguard data and prevent breaches.

Zero-day malware detection:

Malware is one of the primary threat vectors on file integrity and safety. Therefore, having SIEM detect zero-day malware via AV and IDS/IPS logs and correlating them with file audit events, you can stop the malware in its tracks before it harms your secure files. You can use SIEM's incident response actions to kill the malicious process or quarantine the systems for complete endpoint protection.

Continuous compliance support:

Where FIM is a key requirement for many compliance regulations, SIEM systems offer out-of-the-box templates that help with compliance audits. Including FIM results in your compliance reports shows auditors your complete network security information.

Another benefit of combining FIM with SIEM is that SIEM systems help reduce the noise of unnecessary events. You can customize alerts to receive them only when predefined correlation conditions are met. This eliminates the complexity of manually going through a barrage of file audit events.

How SolarWinds Can Help

SolarWinds® Log & Event Manager (LEM) is an affordable, full-functioned SIEM virtual appliance that you can deploy in any-sized, resource-constrained IT security department. SolarWinds LEM provides built-in FIM functionality for detecting file changes in real-time and correlating that information with other system and network events to achieve full awareness of threats and violations. LEM includes many FIM templates to help support PCI, HIPAA, SOX, and other compliance requirements. Immediate benefits of LEM include:

- **Cost Efficiency:** SolarWinds LEM is designed and priced specifically for small security departments. FIM is included with LEM at no extra cost. This further reduces your costs for license and maintenance of intelligent security monitoring and regulatory compliance.
- **Operational Efficiency:** You manage both FIM and SIEM through the same agents and console, which reduces operational and resource overhead.
- **Greater Intelligence:** All SIEM functions, including visual dashboards, correlation, Active Response, and nDepth are available to FIM.
- **Active Response:** With FIM embedded into LEM, security pros don't just see threats, they can effectively stop them. By leveraging LEM's Active Response capability, suspicious processes and activities can automatically be stopped.

With the help of out-of-the-box response actions to remediate threats and troubleshoot issues, SolarWinds LEM can become your cost-effective information security solution to protect secure data. **Visit www.solarwinds.com/lem** to learn more!