LOGPOINT

LOGPOINT FILE INTEGRITY MONITORING

Logpoint Converged SIEM enhances your security posture by enabling cross-correlation of incidents with other security alerts, helping to reduce false positives and to identify and prioritize real threats to your organization.

Why Is FIM Essential?

File Integrity Monitoring (FIM) is a key element in an effective cybersecurity solution. The importance of FIM lies in its ability to both being suitable for audit purposes, change monitoring, as well as to mitigate user-based threats.

- Identify attack sources more efficiently by obtaining information on what has been changed and when.
- Accelerate compliance and avoid hefty fines, notification costs, legal issues, and damaged reputation with a complete set of compliance reporting elements for regulatory domains.
- Reduce the workload of your analysts by using FIM data to enhance your UEBA output and reduce false positives.
- Combining FIM with standard audit records allows drill-back from the UEBA output, to validate results and confirm true positives.

How Does It Work?

Logpoint's FIM calculates the hash value of files, before and after changes could have been made. This way, it can detect any potential tempering of files by just comparing the current hash value against the original.

If the values do not match, the file has been modified. With the help of this process, security analysts can easily get alerted about any potential system compromise. Additionally, FIM also monitors any creation or deletion of the files and directories.

With Logpoint's native FIM features, you will always be in control of your sensitive assets and get alerted whenever a new directory or file is created, deleted, renamed or altered in its content. Logpoint allows you to pick and choose the most important activities and files so you only monitor where it really matters to you. This can be done through comparison to applicable threat indicator on the threat intelligence platform or lookup to tools such as virus total and thus reducing the alert noise.

By combining File Integrity Monitoring with Threat Intelligence, Logpoint provides you with a knowledge base of "known safe" files which can be leveraged to improve the accuracy and speed of change review.

Logpoint Converged SIEM enhances your security posture by enabling cross-correlation of incidents with other security alerts, helping to reduce false positives and to identify and prioritize real threats to your organization.

FIM: A Compliance Cornerstone

As regulatory requirements are increasing and grow more and more complex, the resources required to stay compliant are rapidly growing. Becoming compliant is often a lengthy and tedious process, but having an effective SIEM and a File Integrity Monitoring process in place can reduce the workload significantly.

Logpoint Converged SIEM with FIM supports;

- Compliance monitoring of critical parameters
- Automatic compliance alerts to your security team
- Out-of-the-box compliance reports
- Protection of sensitive data

Logpoint offer you immediate compliance assistance for a number of regulatory domains such as:

PCI-DSS

For organizations handling payment card transactions, complying with the Payment Card Industry–Data Security Standard (PCI-DSS) is essential to stay in business. To stay compliant, PCIDSS specifically requires FIM in a number of areas, such as tracking access to network resources and cardholder data, securing audit trails and regularly testing security systems and processes

ISO27001 And ISO27002

The ISO/IEC 27000 family of standards helps organizations keep information assets secure and manage the security of financial information, intellectual property, employee details or information entrusted by third parties. Multiple sections in ISO2700X series requires the use of FIM for data integrity protection in areas such as Communications and Operations Management, Information System Acquisition, Development, and Maintenance.

HIPAA

Health Insurance Portability and Accountability Act (HIPAA) is an internationally recognized US standard, created to protect sensitive patient data. It requires organization handling healthcare data to implement a number of measures that rely on FILM, including the ability to Protect Audit Trails, identify Unauthorized access and changes a corroborate the Authenticity of Data

Simple Installation And Deployment

The File Integrity Monitor is a part of AgentX, a lightweight application that transports logs and telemetry from endpoints to the SIEM and performs automated real-time investigation and remediation to threats with SOAR, greatly improving observability, investigation and response. In combination with SIEM and SOAR, it brings EDR capabilities to Logpoint Converged SIEM.

AgentX monitors the file system, identifying changes in content, permissions, ownership, and attributes of files that you need to keep an eye on. In addition, it natively identifies users and applications used to create or modify files. File integrity monitoring capabilities can be used in combination with threat intelligence to identify threats or compromised hosts. In addition, AgentX enriches event data with relevant compliance information so you can effortlessly identify PCI violations by querying them in the query interface runs constant policy checks based on CIS CSC v8. This way, compliance specialists can instantly detect when devices enter a non-compliant state.

AgentX is free to all Logpoint users and can be downloaded from the Logpoint Help Center and installed with few clicks.

“The File Integrity Monitor (FIM) is a part of AgentX, a lightweight application that enables you to collect logs and telemetry from endpoints and send them to the Converged SIEM platform for full endpoint observability, audit purposes, change monitoring, and to detect and remediate incidents in endpoints.”

AgentX is free to all Logpoint users.

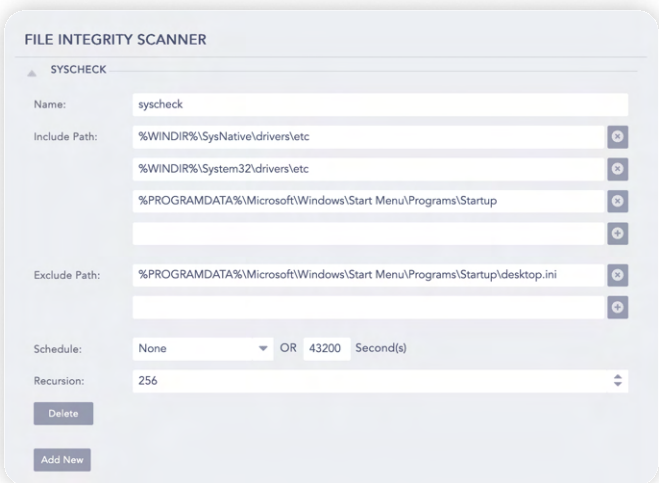
Download Logpoint

FIM use cases

Use Case 1:

Challenge:
Mitigate user-based threats to privileged files

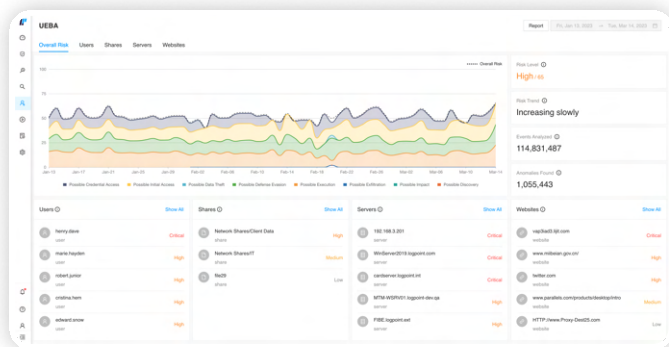
Solution:
Logpoint's FIM application monitors any kind of access attempts to privileged file share systems and provides information on the type of access and the actions performed in the file. Additionally, the original and the altered checksums can also be compared to understand access behavior better.



Use Case 2:

Challenge:
Enhance the accuracy of the UEBA output

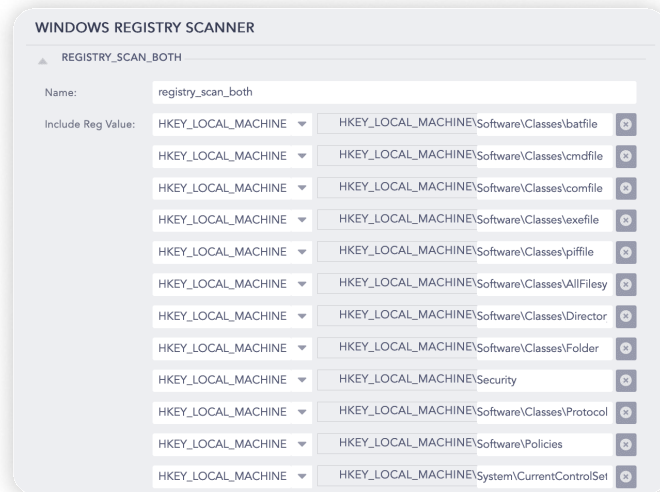
Solution:
UEBA is by nature an excellent tool to automate investigation processes by generating outputs based on comparison with the baseline models. By enriching UEBA with FIM data, you can further enhance the output from the UEBA by narrowing down the chance of false-positives. Artifacts with contextual data surrounding the UEBA-results enable a higher degree of certainty thus contributing to better incident management.



Use Case 3:

Challenge:
Make the workload of audits less intensive

Solution:
The native log-retention Logpoint SIEM makes it possible for alert- and event information to be stored for later forensics analysis of incidents or suspicious activity. This meets compliance objectives for change audit and log retention in a number of standards, such as PCI-DSS.



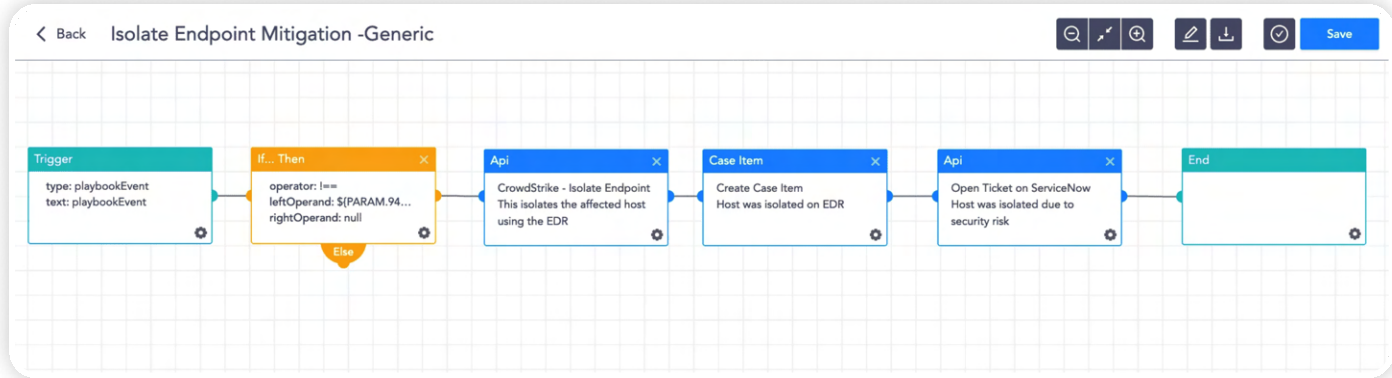
FIM use cases

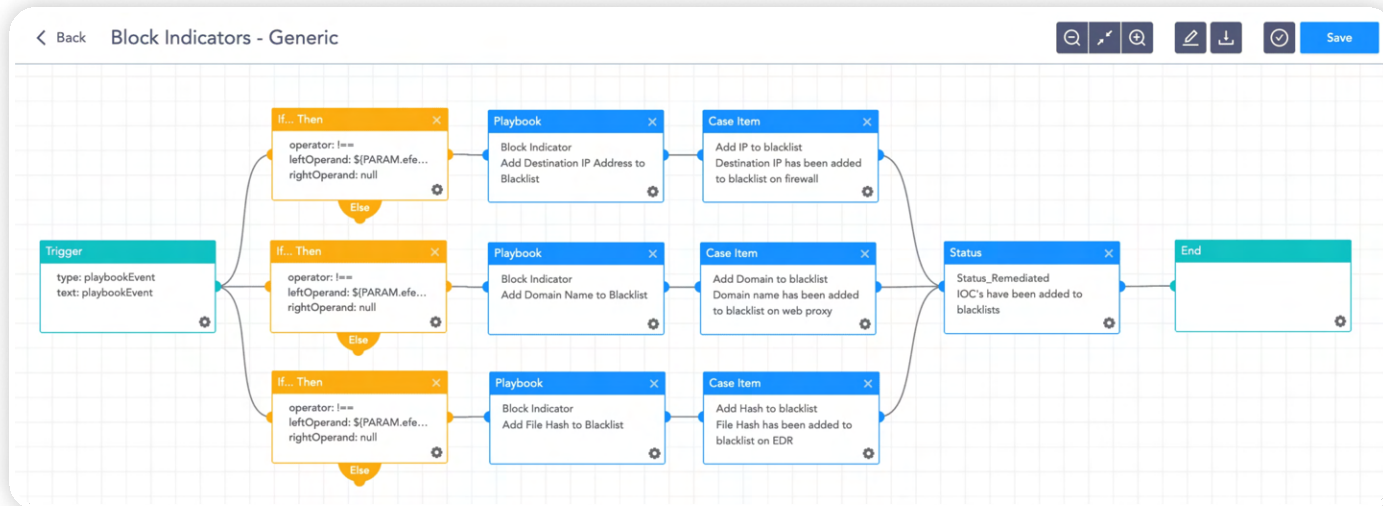
Use Case 4:

Challenge:
Identifying threat indicators associated with an executed malware payload

Solution:
Logpoint's FIM is an effective tool to monitor the creation of new files or change in file's extension indicating malware payload execution. The hash value given by the Integrity Monitor can be compared to the Virus total database, hence identifying the associated threat.

Powered by SOAR, AgentX performs automated investigation and remediation of threats. In this case, the native endpoint agent will trigger a playbook to identify the infected host and isolate it; then contain and quarantine it before the malware spreads to other machines, and finally remove it.





About Logpoint

Logpoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Our Converged SIEM platform combining SIEM, SOAR, UEBA, BCS and EDR capabilities, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses. We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions. Our offices are located throughout Europe, Asia and in North America. Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence. With more than 100 certified partners, we are committed to ensuring our deployments exceed expectations.


LOGPOINT