Logsign
Your teammate in cyber security

SOLUTION BRIEF

WINDOWS AUDITING

LOGSIGN SIEM PROVIDES ONE OF THE BEST WAYS TO ANALYZE WINDOWS EVENT LOGS.

Logsign can be easily integrated with Windows auditing environment by using Windows Management Instrumentation (WMI) services, supplying you with a complete solution to collect all Windows events, their normalization and enrichment.

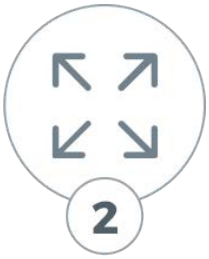
Thus, Logsign helps you analyze all Windows events in a clearer and less sophisticated way, compared to both native Windows systems and other solutions.

> **“Increase your data analytics capacity with comprehensive Windows integration.”**

Eventually Logsign not only increases your ability to monitor Windows events but meanwhile decreases IT managers'workload with enhanced easy to understand reports of all Windows events.

GET MORE SECURITY AND MORE COMPLIANCE WITH 4 STEPS

Collect all Windows messages.



Drill down to all message details.

Auto normalize with a security and compliance oriented focus.

Have an all-round view via predefined report and alert templates.

Logsign collects and normalizes over 400 eventsfrom windows ecosystem. This enables you to monitor even the most specific events and correlate them with other user behaviours.

Logsign's this vast Windows Audit capacity keeps growing non stop in comply with the evolution of Windows products and our customers' needs.

By the help of Logsign, you can enjoy quick, simple but meaningful insights.We not only allow the normalization of Windows events that consist of hundreds of columns, but also provide you a possibility to review all data in the same context categories via our smart, structured column architecture with events from non-MS solutions.

Predefined Alert & Report Templates

Logsign provides various predefined reports about Windows auditing, system and security.

Most of the Windows security audit events are normalized thoroughly by Logsign. Flexible report architecture allows an easy, simple and functional review on all user session logs, file and fileshare actions, account management activities and more Windows events. Predefined reports on all categories of Windows simplifies your work. All these reports can be customized and improved if needed.

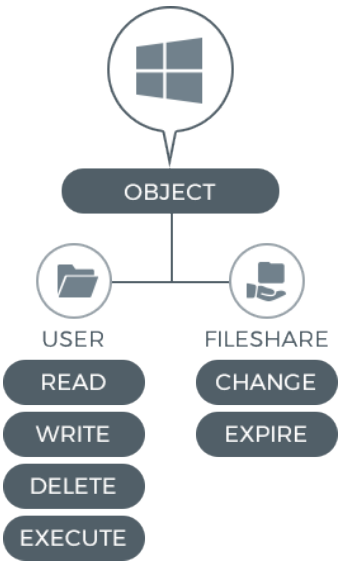
Windows Logon & Logoff Activities

Logon & Logoff Activities reports contain on one side the transactions of successful logins, logouts, failed login attempts etc. and all the details belonging to theses events on the other. These details consist of user domain, username, date and time, message info, happened action, logon type etc. Access this information by just one click, and analyze them in detail by using related filters.

All user activities can be analyzed with more than one report. Also terminal server events and the Remote Desktop Protocol (RDP) or VPN sessions can be analyzed in separate reports.

Windows Account Management

All user operations are included in the Windows Account Management audit category. Logsign provides reliable and strong reporting support about all the processes such as creating and deleting user, password activities, user enable/disable attempts, group changes, lock/unlock transactions and more. Logsign generates more than 20 reports in one report block capturing all Active Directory operational processes.



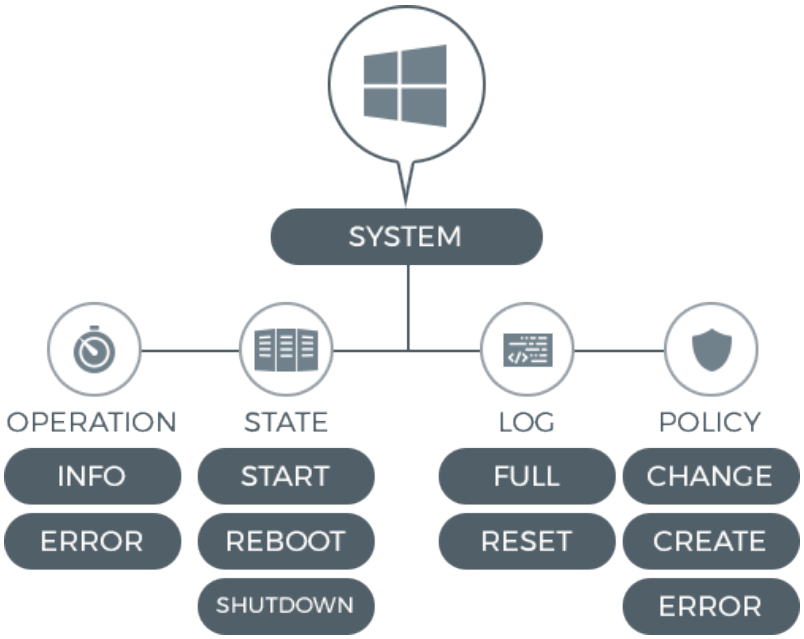
Windows File / Fileshare Events

The file and fileshare structure on Windows systems allows the analysis on file server auditing processes. Logsign normalizes all the user, time and object based actions; and provides the reports about read files, deleted folders, modified files etc.

All these events such as file, fileshare and detailed fileshare can be analyzed in much more detailed and efficient way than on Windows systems.

System Events

It is always important to obtain information about who, when and by which style a Windows server is rebooted or powered off. All these actions are normalized and presented with all its details in reports.



Directory Services

It is possible to analyze the operational changes on the side of organizational units. Analyze the events about the objects that are added or deleted on Group Policy Management as well as the created or deleted OU events.

In short if you are in a Windows dominated environment and want to see very detailed user/file activities with easy to design reports, Logsign is just the tool you are looking for.

Logsign is a Security Information and Event Management (SIEM) solution which provides security analyses and compliance to regulations in one platform. Founded in 2010, Logsign believes that cyber security is a teamwork and that security products have to be much smarter. With this conviction, it focused its endeavors on Security Intelligence and SOC solutions. It actively provides services for more than 500 medium and large scale firms and governmental agencies. It is working to be an irreplaceable team-mate for all of its stakeholders in the field of cyber security, to raise its customers' security awareness to the maximum and to reinforce their position concerning security. It also proved its competence in the field of technology as a cyber security software producer, landing among Deloitte Technology EMEA Fast 500 in 2016.

For more information visit www.logsign.com

Help Center support.logsign.net / 0 850 660 0 850

Please contact us at info@logsign.com

İstanbul HQ ● Ankara ● San Francisco