Logsign

Windows Auditing with Logsign Next-Gen SIEM

Logsign Next-Gen SIEM Provides One Of The Best Ways To Analyze Windows Event Logs.

Datasheet

Windows Auditing with Logsign Next-Gen SIEM

Logsign Next-Gen SIEM 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 Next-Gen SIEM 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.**

Get More Security And More Compliance With 4 Steps

Collect all Windows messages.

Drill down to all message details.

Normalize logs automatically.

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

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

Logsign Next-Gen SIEM'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 Next-Gen SIEM, 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

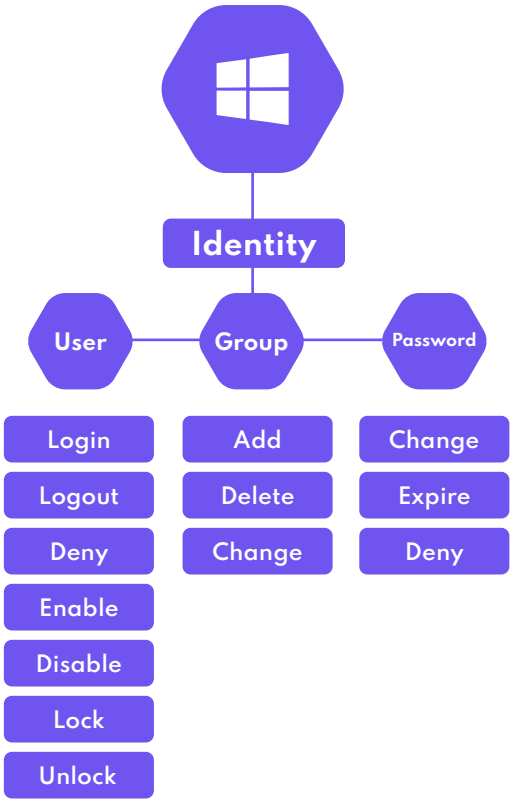
Logsign Next-Gen SIEM provides various predefined reports about Windows auditing, system and security.

Most of the Windows security audit events are normalized thoroughly by Logsign Next-Gen SIEM. 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

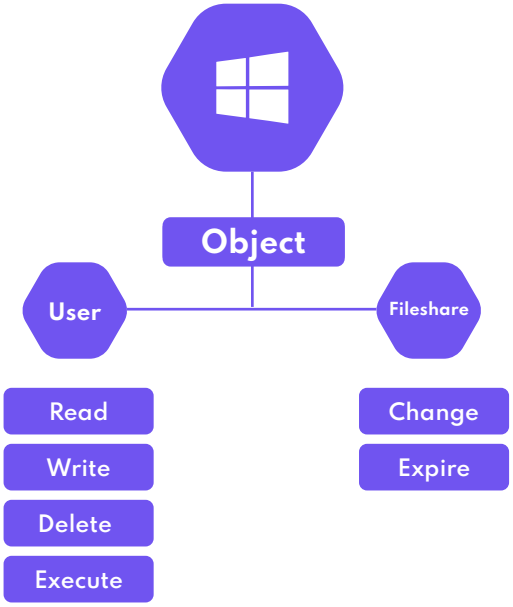
Logon & Logoff Activities reports contain on one side the transactions of successful logins, logouts, failed login attempts etc. and all the details belonging to theses events on the other. These details consist of user domain, username, date and time, message info, happened action, logon type etc. Access 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 Next-Gen SIEM 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 Next-Gen SIEM generates more than 20 reports in one report block capturing all Active Directory operational processes.



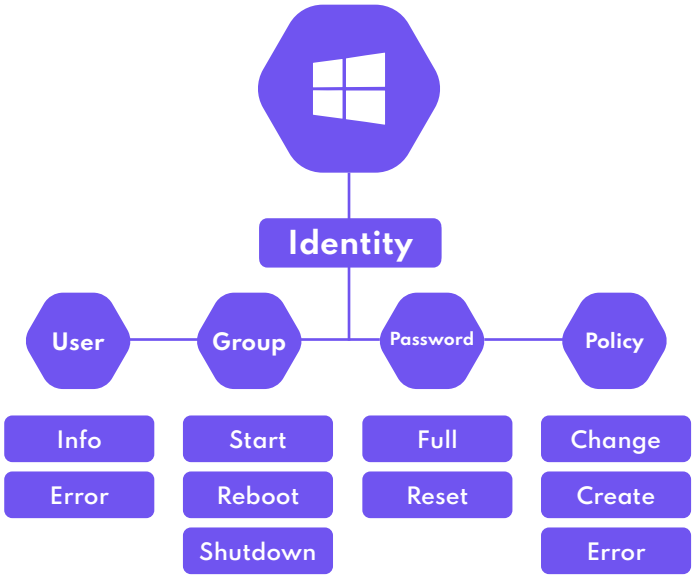
Windows File / Fileshare Events

The file and fileshare structure on Windows systems allows the analysis on file server auditing processes. Logsign Next-Gen SIEM 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 Next-Gen SIEM is just the tool you are looking for.

About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

0 850 660 0 850