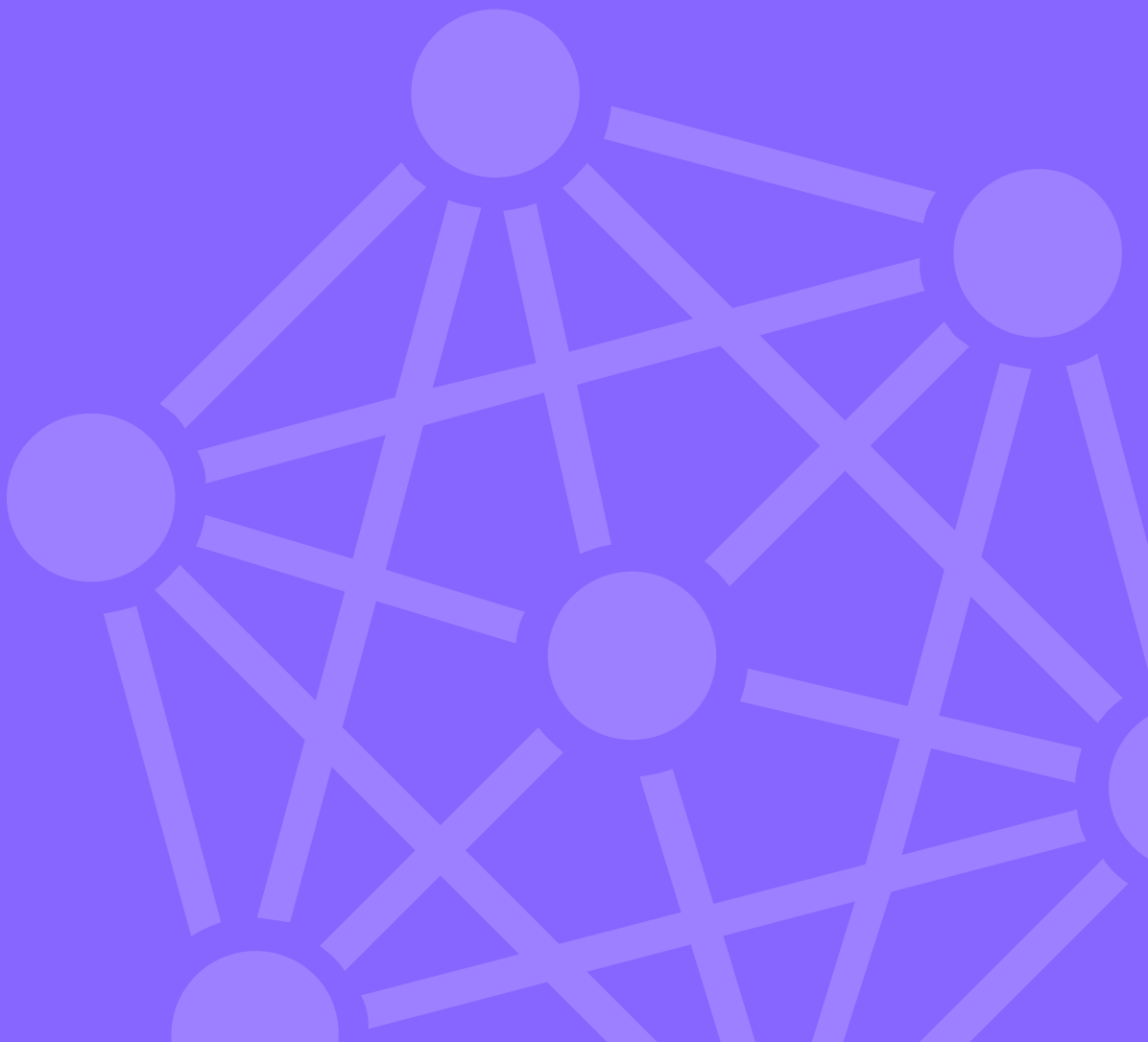
Logsign

Logsign Next-Gen SIEM Use Case:

# Monitoring and Managing the Highly Privileged User Account



# Monitoring and Managing the Highly Privileged User Account

## Customer Challenge

In order to access the organizational resources and sensitive information, the attackers' primary target is to obtain the privileged user credentials. Privileged user accounts are the accounts of users with managerial rights or root privileges and the accounts with upgraded privileges. Efficient privileged user monitoring plays an important role for the organizations in protecting their critical assets. In addition, it assists in meeting the compliance requirements, and decreasing the number of both insider and external threats.

### How to monitor and manage the privileged user accounts

Configuring the data coming from credential servers or from index servers such as Active Directory (AD) or LDAP should be set as the primary target. Incidents such as the daily upgrade of user credentials and user rights or creating new users should be monitored. Account names, account categories, departments of relevant users and other relevant information should be listed along with credential data.

Privileged access rights should be reviewed within appropriate time periods (at least once a month) and the privileged license allocation should be reviewed regularly. All privileged user accesses to the files and databases (including the local system access) should be monitored. The alert mechanisms of critical privileged user changes should be momentarily shared with relevant IT managers via e-mail and SMS.

## 7 Ways Logsign SIEM Assists Monitoring And Managing Of The Privileged User Account:

**1-** By means of correlation processes and Behavior Analysis, the user can be tagged as Attacker, Victim, and Suspicious.

**2-** Total number of incidents formed on privileged user accounts within time are shown on dashboards. This report indicates the normal privileged account usage method and defines the extraordinary or unexpected activities.

**3-** How many times the privileged accounts used on the dashboard within a certain period were used to log in is seen.

**4-** Momentary images of users are provided on the dashboard. On this dashboard, there are credential data panels that include the account names, account categories, departments, and other relevant information.

**5-** In order to obtain more information on the activities of privileged users, correlation definitions can be formed with the aim of detecting the critical actions. For instance; if a user tries to verify the credentials on an application from more than one host computers at the same time, a correlation search reporting the access can be created.

**6-** You can monitor a privileged user uploading a large file on a domain with "x.xxx". Correlation searches can be created by using the access and credential information.

**7-** The results are shared with relevant IT managers, and e-mail & SMS alert mechanisms are formed.