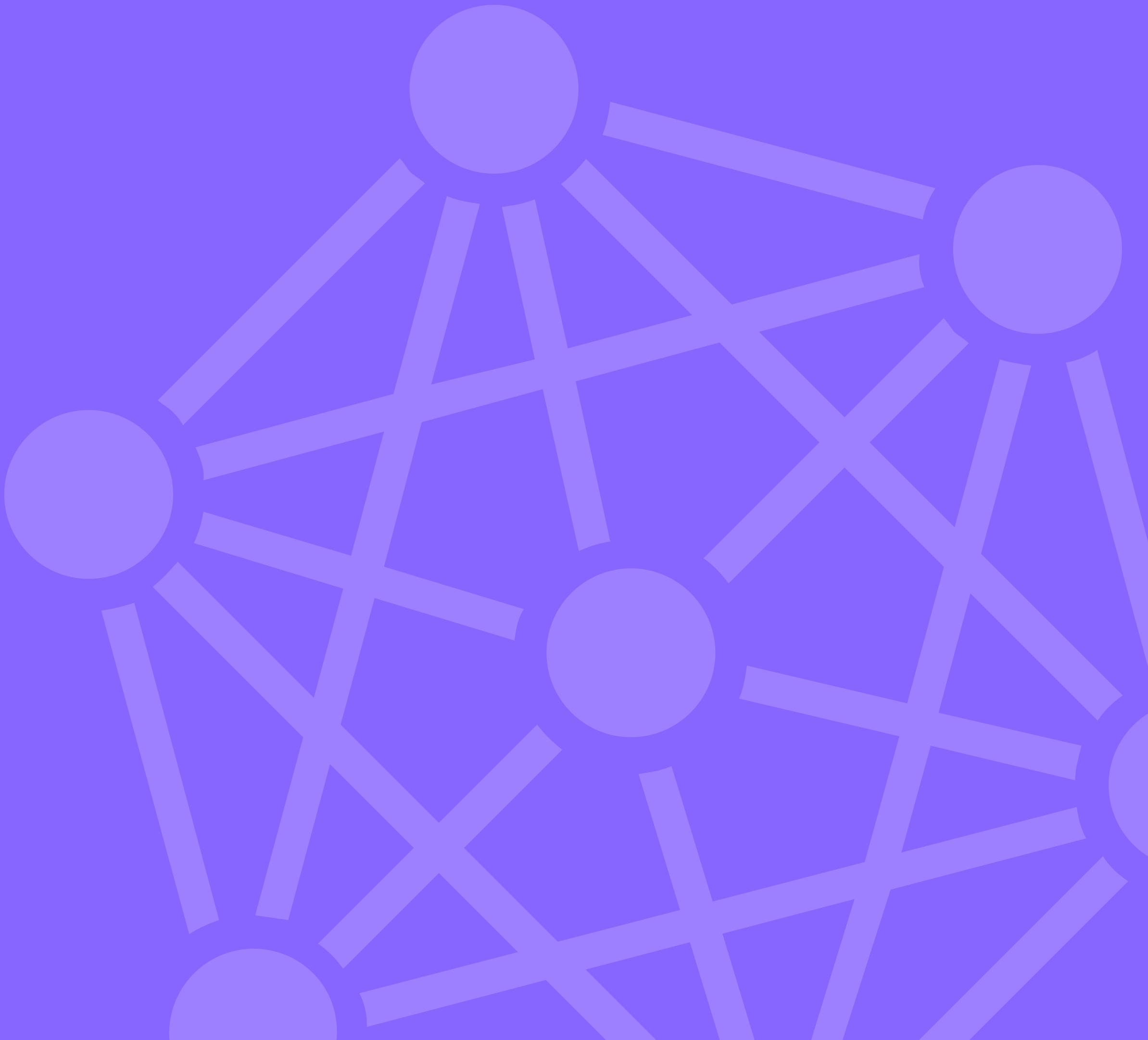
Logsign

Logsign Next-Gen SIEM Use Case:

Identifying Insider Threats



Identifying Insider Threats

Customer Challenge

According to the insider threat statistics provided by the Verizon Data Breach Investigations Report, three of the first five reasons of security incidents are related to an insider threat. Therefore, in addition to the measures taken within the framework of external threats, measures need to be taken for the insider threats as well.

Many organizations focus on the protection against external threats. However, adequate measures may not be taken against the threats originating from the current and former employees, service contractors or business partners that have daily access to their internal networks.

How can I identify and prevent the internal threats?

Identifying the insider threats is difficult and complicated. Logsign SIEM analyzes the insider threat indicators and attack vectors by means of pre-defined correlation rules and cyber threat intelligence, and shares with the IT managers the obtained data by creating dashboards, alarms, and reports.

Logsign SIEM Helps to Prevent Insider Threats in 6 Ways:

1. Detecting Compromised User Credentials

Logsign SIEM detects the abnormal behavior of the users with the help of the correlation motor. For instance, Logsign SIEM produces an alarm to warn the IT managers in case of an access to unusual data or systems on unusual hours.

2. Suspicious Privilege Escalation

Privileged user account is a target with access priority. Logsign SIEM can detect the users that increase their authority for critical systems.

3. Command and Control (C&C) Communication

Logsign SIEM can associate the network traffic with the Threat Intelligence Service in order to discover the malware that communicates with the external attackers. This points out a jeopardized user account.

4. Data Exfiltration

You can use the Logsign Correlation and Threat Intelligence Service in order to analyse the incidents that may seem irrelevant with one another – such as USB disc driver adding and process information, personal e-mail services, cloud storage services or creating high data traffic via the Internet or local network.

5. Rapid Encryption

It can detect the encryption of the data in the user systems. These abnormal incidents on the user data may be a ransomware attack.

6. Lateral Movement

According to the Mitre Att&ck matrix, lateral threats can be identified within the framework of the alarm rules prepared according to the technics under the Lateral Threat Detection headline.