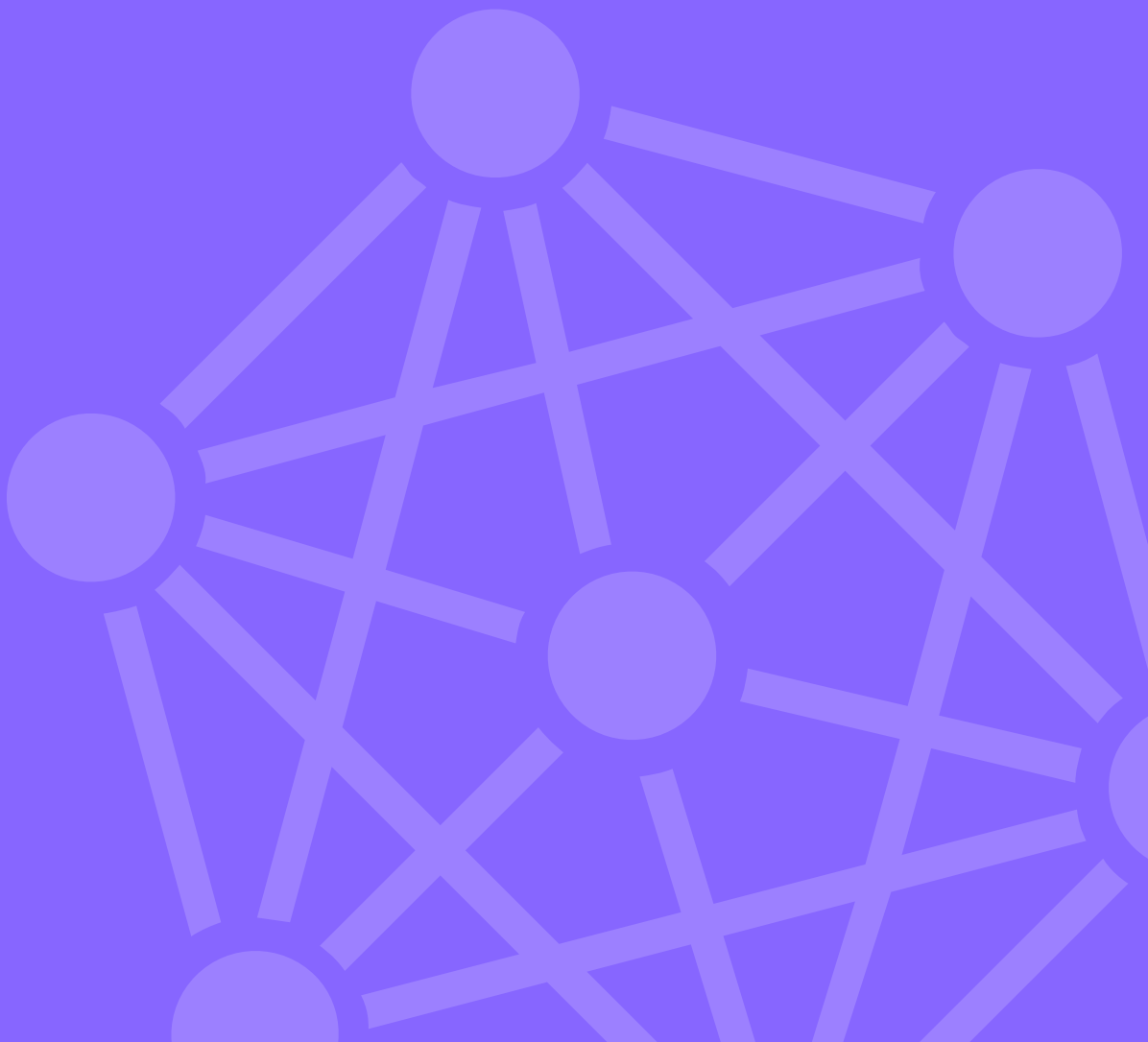
Logsign

Logsign Next-Gen SIEM Use Case:

GDPR: How to Detect Unauthorized Access to Personal Data



GDPR: How to Detect Unauthorized Access to Personal Data

Customer Challenge

GDPR states that the institutions must obtain explicit consent from individuals before collecting their personal data and keep these data strictly confidential. It makes institutions obligated to take technical precautions for the reasons below:

- Examining data access and flow on the network infrastructure
- Detecting data violations within 72 hours after they occur
- Conducting appropriate post-violation activities such as creating incident report or automatically eliminating a violation

How to detect unauthorized access to personal data with Logsign SIEM

Logsign SIEM groups parameters such as the number of log-in attempts, username, and user IP address to collect unsuccessful log-in attempts and creates incidents after a certain limit is passed. Logsign SIEM warns IT managers via SMS / E-mail if an unauthorized user access is detected.

Detecting Unauthorized Access to Personal Data in 4 Steps:

1. Detection process of unauthorized access begins with Logsign SIEM correlation techniques by using authentication source logs.

2. The user is labeled as Attacker after a behavioral analysis is conducted with correlation.

3. After the attacker begins the unauthorized access activity, logs are enriched by conducting behavioral analysis with the logs received from sources. Attacker's activities are correlated and shown on relevant dashboard panels.

4. Activities and relevant alerts are sent to IT managers via SMS / E-mail to warn them.