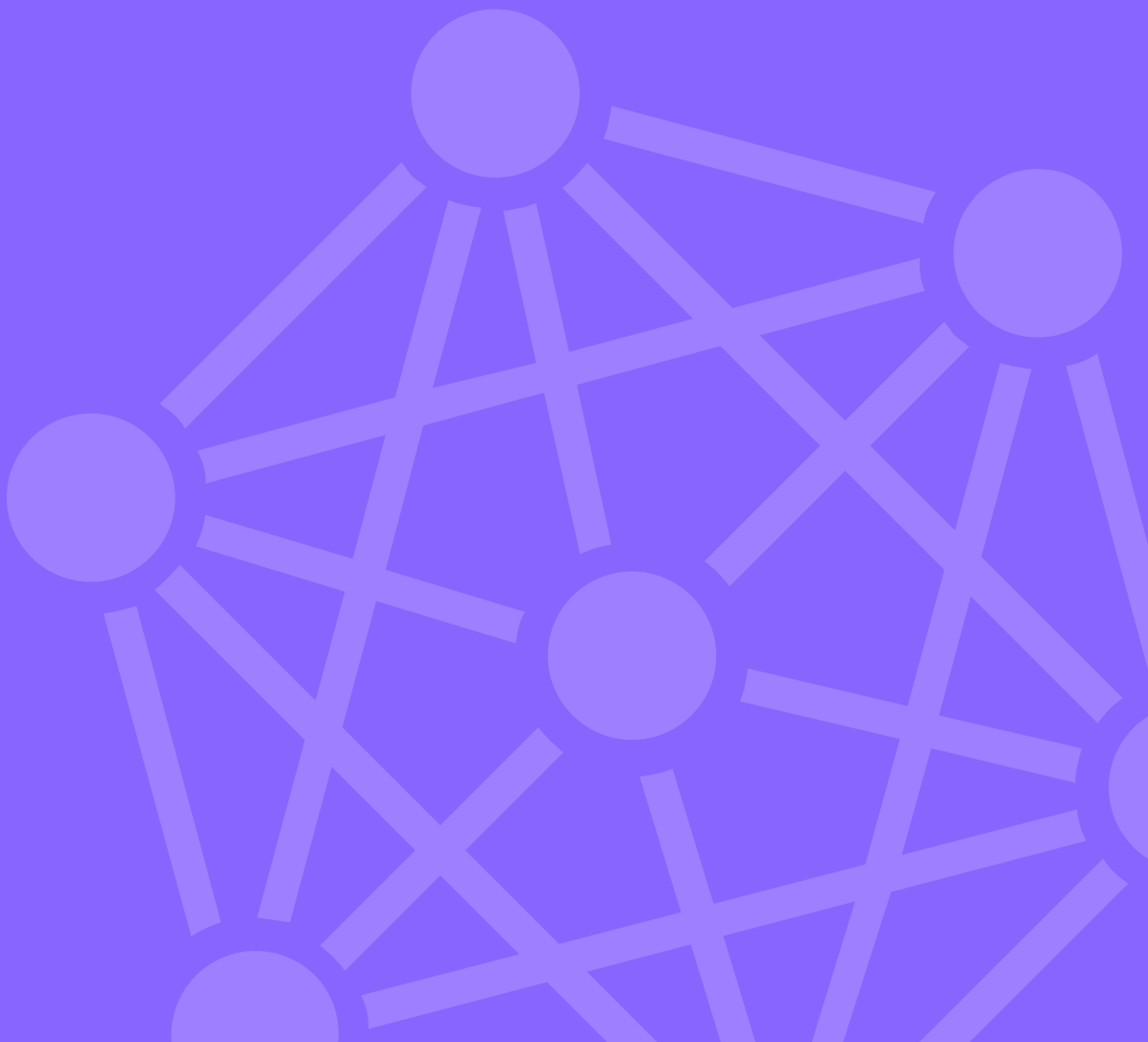
Logsign

Logsign Next-Gen SIEM Use Case:

Detecting and Preventing Data Exfiltration



Detecting and Preventing Data Exfiltration

Customer Challenge

Data exfiltration is the unauthorized transferring of data from corporate system by means of flash drive, user computer, IT servers, and mobile devices. Unauthorized transfers can be manually or automatically conducted through a network, with the help of malicious programs.

Data exfiltration is a security violation which occurs when a person copies, transfers or obtains the data of the company from a computer or server without permission. While data can be exfiltrated by means of various techniques, it is mostly exfiltrated by cyber criminals over the Internet or a network. In general, the aim and primary target of these attacks are to access a network or machine in order to reach and copy specific data.

How to detect and prevent data exfiltration

A proactive measure to be taken by the companies is to prevent the users from downloading unknown or suspicious applications. Malwares installed to the user computer should be able to externally communicate with a C&C server in order to deliver their messages or take out the data. This unauthorized communication should be detected and prevented.

Dataflow of a company includes the transferring or moving of the data within its internal network and from the external network to the inside. One of the methods used in detecting data exfiltration should be the monitoring of the e-mails, DNS inquiries, file access demands, and illegal port connections. Detection is made easier when monitoring panels and alerts are formed.

7 Ways Logsign SIEM Helps to Detect And Prevent Data Exfiltration:

1. Detecting compromised user credentials

Logsign SIEM detects the abnormal behavior of the user by means of a correlation motor. For instance; Logsign SIEM creates an alert to warn relevant IT managers in case a user accesses extraordinary data or systems at unusual hours.

2. Suspicious Privilege Escalation

Privileged user account is the primary target for access. Logsign SIEM can detect users with escalated authority for critical systems.

3. Command and Control Communication

Logsign SIEM associates the network traffic with Threat Intelligence service in order to discover the malware which communicates with external attackers. This indicates a compromised user account.

4. Data Exfiltration

You can use Logsign SIEM correlation skills and Thereat Intelligence service in order to analyse incidents that may seem irrelevant with one another – such as USB disc driver insertion and process information, personal e-mail services, cloud storage services or the formation of high data traffic through the Internet and local network.

5. Rapid Encryption

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

6. Lateral Movement

According to the Mitre Att&ck matrix, lateral movements can be detected within the framework of the alert rules written based on the techniques listed under the Lateral Threat Detection headline.

7. Prevention

Logsign SIEM automatically takes action in order to prevent the detected data exfiltration from spreading.