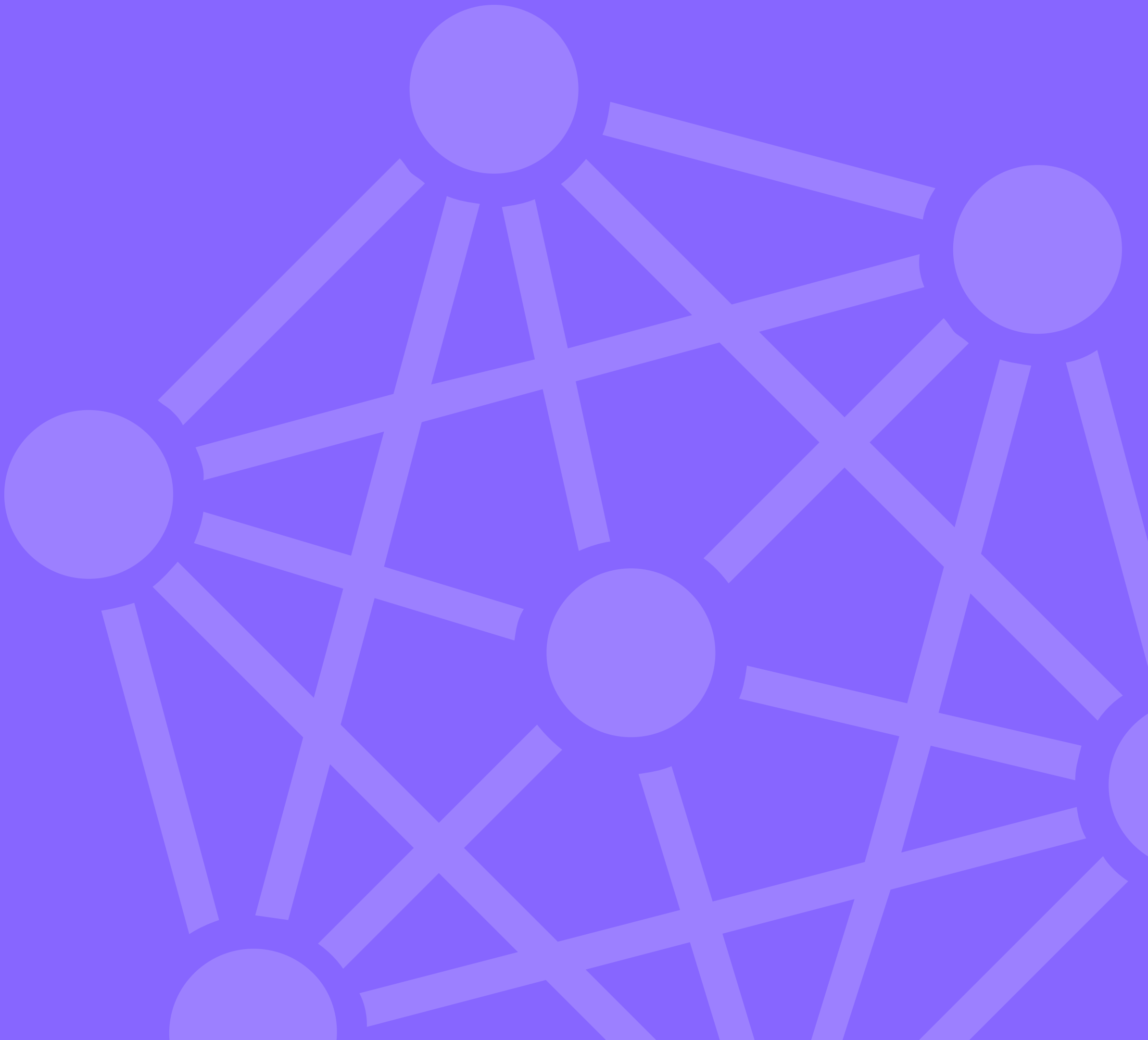
Logsign

Logsign Next-Gen SIEM Use Case:

Detecting Lateral Movements



How to Detect Lateral Movements

Customer Challenge

Network attacks are getting more complicated in today's security environment. To obtain basic access information, attackers use various methods such as Phishing attack or Malware infection.

After they enter the relevant IT system, they disguise as the user with wide access authorization while trying to increase their privileges. Many institutions do not have the staff, tools or bandwidth that will detect any extraordinary activities. After the attacker leaks into the network, it may take them days or weeks to discover the weaknesses in the systems. It is necessary for the lateral movements in this time period to be detected. Lateral movement refers to the gradual movements of cyber attackers, and the techniques they use to search for important targeted data and assets.

How to detect lateral movements with Logsign SIEM?

Lateral movement activities can be analyzed and detected by Logsign SIEM via pre-defined correlations and Cyber Threat Intelligence (TI) service. Audit logs, process formation logs, Firewall, IDS/IPS, and EDR logs are used during the detection process.

Lateral movements that can be detected as pre-defined by Logsign SIEM:

- Unsuccessful log-in attempts on disabled accounts,
- Extraordinary activities based on the time of day or day of week,
- Extraordinary accesses to servers, file shares, applications, or other sources,
- Too much extraordinary access to some sources,
- Abnormal application use and abnormal access to data storage.

Six Ways Logsign SIEM Can Help Stop Lateral Movements:

1. Detecting Compromised User
Logsign SIEM identifies abnormal behavior of users by means of correlation. For instance, Logsign SIEM creates alerts to warn relevant IT managers in case of access to extraordinary data or systems at extraordinary hours.

2. Detecting Suspicious Privileged Authorization Increase
Main target is to detect privileged user account accesses. Logsign SIEM immediately identifies users that increase authorization for critical systems.

3. Command and Control (C&C) Communication
Logsign SIEM may associate the network traffic with Cyber Intelligence Module to discover malware that communicates with external attackers. This refers to a compromised user account.

4. Detecting Data Leakage
You can use Logsign Correlation and Cyber Threat Intelligence (TI) service to analyse incidents that may seem irrelevant – such as USB disc driver adding and process information, personal e-mail services, cloud storage services or creating high data traffic through local network.

5. Rapid Ciphering
It can detect the ciphering of the data on user systems. These abnormal movements on user data may be a ransomware attack.

6. Detecting Lateral Movements
Lateral Movements can be detected via alert rules created based on the Mitre Attack framework.