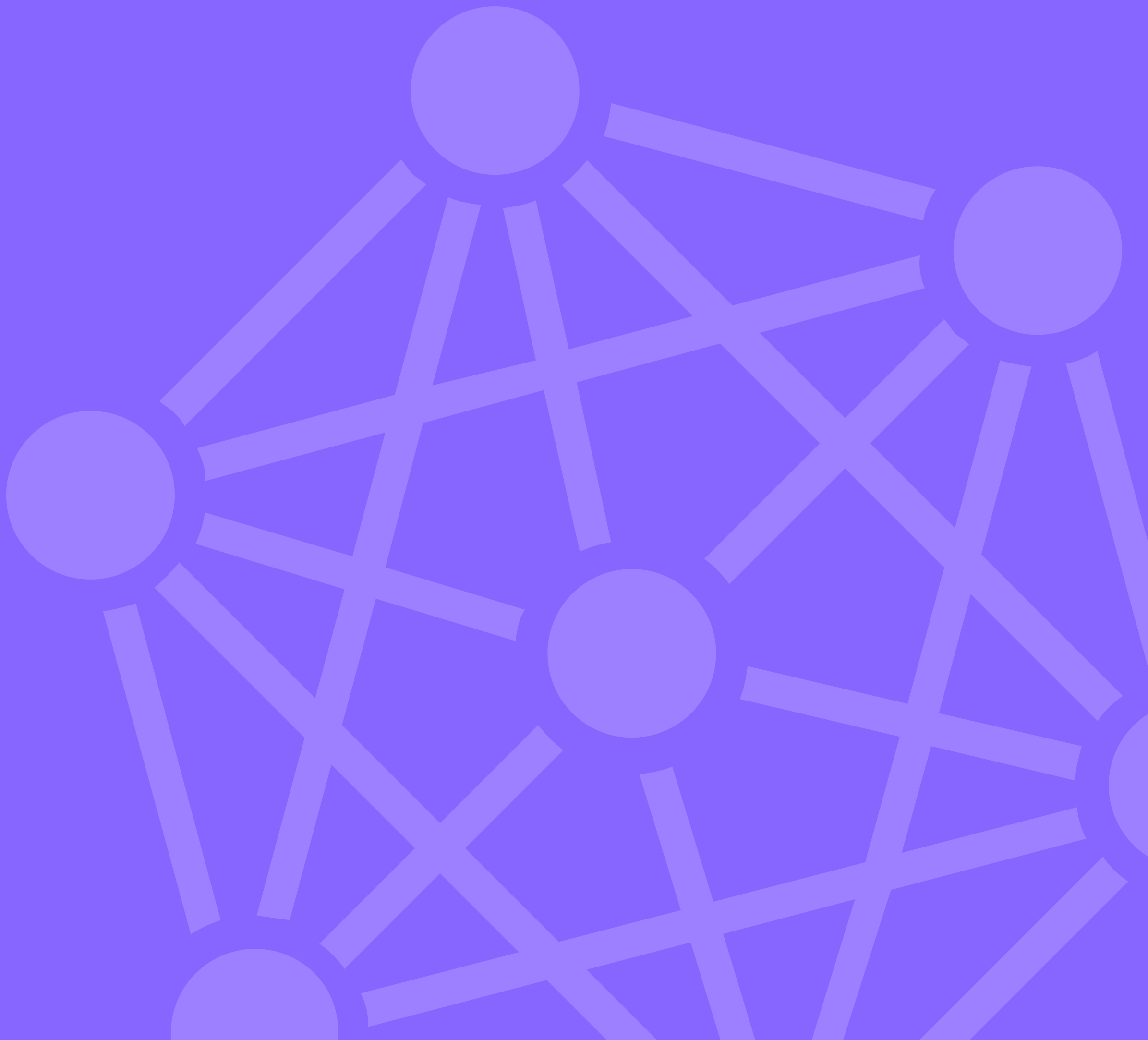
Logsign

Logsign Next-Gen SIEM Use Case:

Detecting Brute Force Attacks



Detecting Brute Force Attacks

Customer Challenge

Nowadays, Brute Force attacks come to the forefront as a widespread attack due to the developing of more rapid and effective password cracking tools. Before the Brute Force attack, businesses should configure the identity authentication system for security incidents such as suspicious log-in attempts or any changes to be made on the system files, therefore, be able to detect beforehand any malicious event.

During the Brute Force attack, cyber pirates generally use an automatic (via target-oriented cyber pirate software) trial-and-error method in order to leak into their targeted user accounts and obtain the information within them. This method makes possible the breaking of passwords that bear various security elements with complicated combinations.

How to detect Brute Force attacks

The fact that the tools used in Brute Force attacks are easy-to-use and enable more rapid results puts this method forward in using it during system penetration attempts. Logsign SIEM collects failed log-in attempts by grouping parameters such as the frequency of log-in attempts, username and user IP address, and creates incident after a certain threshold value is exceeded. Logsign SIEM sends an SMS & E-mail to IT managers as soon as the Brute Force attack is detected.

4 Steps Used by Logsign SIEM in Detecting Brute Force Attacks:

1. By using authentication source logs, detection process of Brute Force attacks is started with Logsign SIEM correlation techniques.
2. User is labelled as Attacker after behavioral analysis is conducted with correlation operations.
3. After the Attacker starts the Brute Force activity, the logs are enriched by conducting behavioral analysis with the logs received from the sources. Activities by the attacker are correlated and displayed in the relevant dashboard panels.
4. Incidents about the activities are shared with IT managers and alert mechanisms in e-mail & SMS are created.