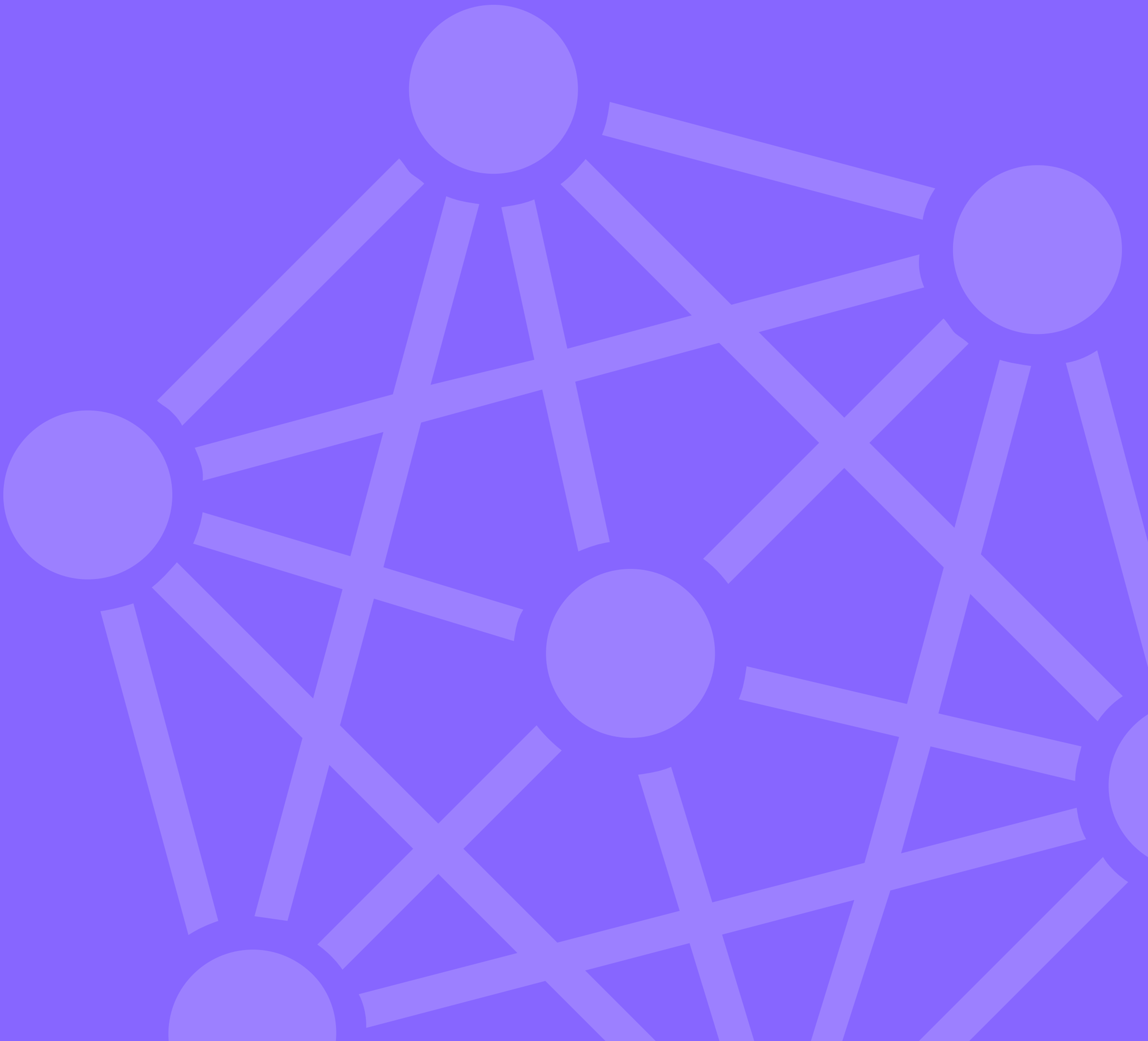
Logsign®

Logsign Next-Gen SIEM Use Case:

Identifying and Detecting Zero-Day Attacks



Identifying and Detecting Zero-Day Attacks

Customer Challenge

A zero-day exploit is the attack that benefits from the security gaps of a program or an application. There is a natural problem in all threat detection models that depend on statistics and signatures. Although these methods are appropriate for the recognised security threats, they have been known to perform inadequately when it comes to zero-day attacks.

As the traditional methods depend on the databases of the recognised threats, it was proven that they have had very limited abilities when it comes to the struggle against the changes within the attack methodologies. With zero-day attacks, the attackers can detect the weakness on the source code of the program or application software and develop malicious codes for a cyber attack by benefiting from the security gap.

How to detect and prevent zero-day attacks

Detecting the zero-day attacks is difficult and complicated. Logsign SIEM analyzes the zero-day attack indicators and attack vectors by means of pre-defined correlation rules and cyber TI, and shares with the IT managers the obtained data by creating dashboards, alerts, and reports.

5 Steps Used By Logsign SIEM To Detect And Stop The Zero-Day Attacks:

1- Detecting process of the Zero-Day attacks begins with Logsign SIEM correlation techniques by means of TI, Web Proxy, AD Auth, DNS server, IPS, Process events, and Endpoint protection platform (EPP) source logs.

2- By means of correlation processes and Behavior Analysis, the user is tagged as Attacker, Victim, and Suspicious.

3- Following the first activity started by the attacker on the side of the user, the logs are enriched by means of a behavior analysis conducted with the logs coming from the sources. The log activities formed during the activities of the attacker, which are both from the insider to the external and vice versa, are shown on the relevant dashboard panels by being subjected to correlation.

4- The results are shared with relevant IT managers, and alert mechanisms as e-mail & SMS are formed.

5- In order to prevent the zero-day attacks from logging in the C&C serves on the Internet and the exploit process, Logsign SIEM writes the relevant deny rules by means of an API sharing on Palo Alto, Fortigate and Checkpoint firewall.