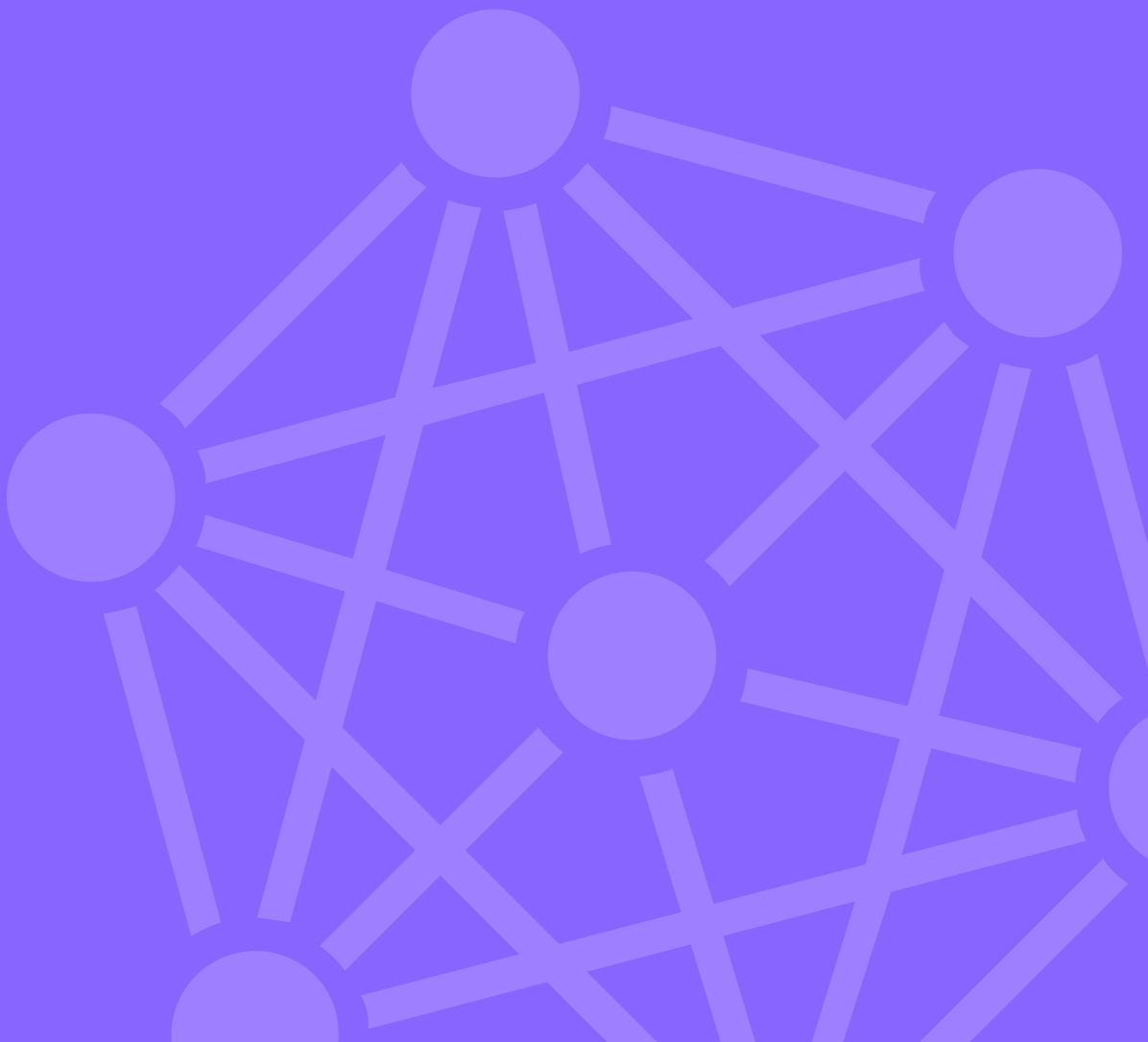
Logsign

Logsign Next-Gen SIEM Use Case:

Malware Detection



Malware Detection

Customer Challenge

It is well known that the signature-based antivirus technologies have lost their productivity as the primary weapon in the fight against malware. It is observed that the detection and cleaning rates have considerably lowered in the past few years. Malware targets monetary, personal, financial or commercial information. Credential theft, cyber warfare and espionage or service cuts aiming at specific companies can be counted as other targets.

Antivirus tools should be reinforced by means of network traffic analysis and system log analysis so as to detect the modern commercial malware. In addition, there are scenarios in which the antivirus technology detects but cannot delete the threat. In order to detect and emphasise such incidents, many corporations should considerably improve their abilities against cyber attacks.

How to detect and prevent malware

Detecting malware is difficult and complicated. Logsign SIEM analyzes the malware indicators and attack vectors by means of pre-defined correlation rules and feeds 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 Prevent Malware Threats:

1- Malware detecting process begins with Logsign SIEM correlation techniques by means of Cyber 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 malware 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.