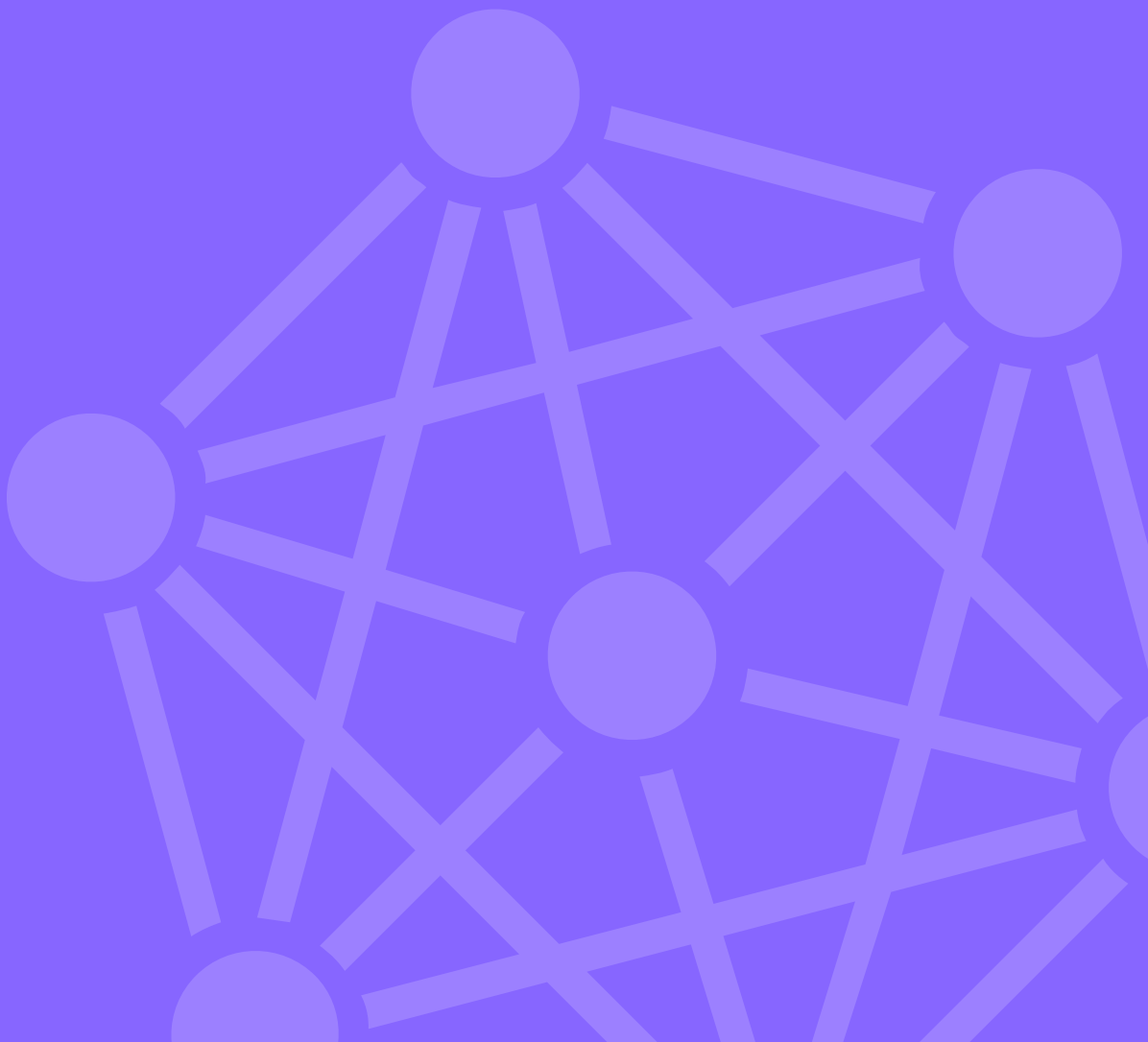
Logsign

Logsign Next-Gen SIEM Use Case:

How to Detect Superman VPN User



How to Detect Superman VPN User

Customer Challenge

Employees of corporate firms work in offices and on the field in geographically different places. It is very difficult for these locations and staff to connect to the headquarters from point to point due to costs and infrastructure problems. In these cases, the offices and staff need to securely connect to the headquarters. In order to meet this need, virtual private networks that cryptically carry the outgoing data towards the Internet were developed. VPN connections can be conducted between two locations or with the VPN software (VPN Client) installed on the staff computer. As a result of the increased managerial costs due to the VPN software installed on the computer, web-based VPN solutions (SSL VPN) were created. Illegally exploiting these accesses is possible by obtaining the user access information. Illegal VPN access uses point at the fact that the user broke the speed obstacle and was able to access sources in far away places in a very short time period.

How to detect Superman VPN user

Logsign SIEM tool can monitor all logs on the VPN condenser and detect the user behind each new connection request and their IP address. When the previous connection request from the same user is concerned, SIEM can check both the time and the IP address of this access. Later on, it can associate the IP addresses (Geo Location) with geographical location coordinates by using any prestigious third-party service.

4 Steps Used by Logsign SIEM in Detecting the Superman VPN User:

1. VPN access source logs of the users are collected, and VPN access detection process begins with Logsign SIEM correlation techniques.

2. Correlation processes and statistical behavior analysis are conducted in order to list the geographical locations where the user connected at specific times.

3. Following these steps, relevant rules are written on the side of the correlation.

4. The created activities and relevant correlations are shared with IT managers and e-mail & SMS notifications are sent.