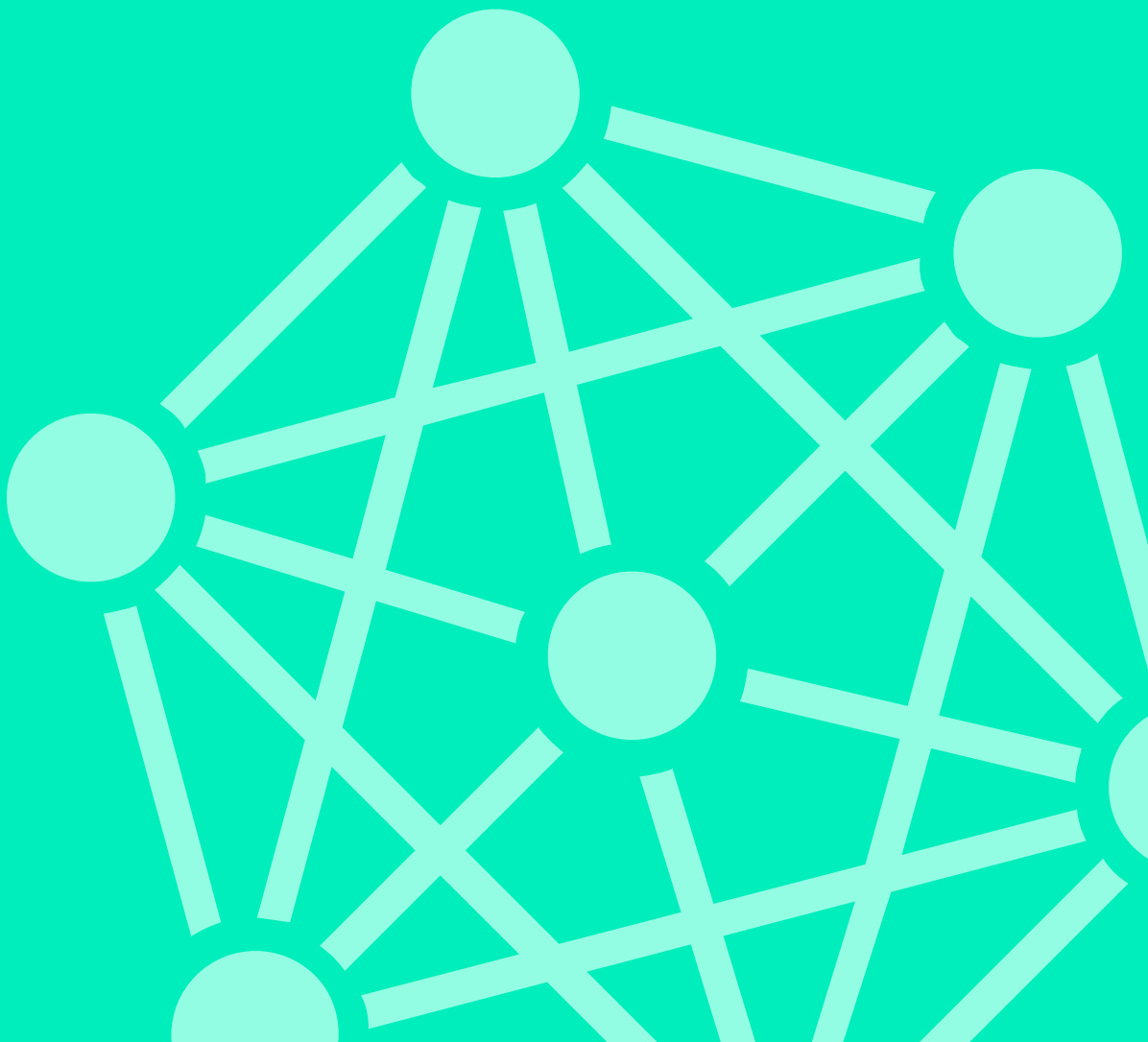
Logsign

Logsign Security Orchestration, Automation and Response (SOAR) Use Case:

Malicious Network Traffic



Malicious Network Traffic

Customer Challenge

Malicious traffic can be a result of incoming requests or a suspicious file's attempt to connect to an untrusted resource. If malicious traffic goes undetected, it can directly impact an organization's security posture. Suspicious files often attempt to communicate through HTTP requests to their command and control (C&C) servers which are operated by the attackers. The attacker can provide various instructions through the C&C server for uploading/downloading available files, data exfiltration, unauthorized access, botnet activities, and privilege escalation.

How to analyze malicious network traffic?

With the help of Logsign SOAR, you can utilize the machine power to detect malicious network traffic automatically.

1. As soon as the SOAR platform detects an instance of malicious network traffic, it generates an alert.
2. It adds contextual information and searches for more details on the relevant threat.
3. It prevents any further connections from the traffic source.
4. The platform sends an alert to your SOC team members.

Business Process Analysis

It may take a security analyst up to 50 minutes to deal with an instance of malicious network traffic. With the help of automation, this time is cut down to 1-2 minutes.

Benefits

Manually, security analysts rely on threat intelligence feeds, asset inventories, and tools like nslookup and whois to gather information about suspicious traffic. This process consumes a substantial amount of time. With the help of automation, Logsign SOAR cuts down the time consumed and provides your SOC team with contextual information to decide whether suspicious traffic is malicious. When new instances of malicious traffic are detected, Logsign SOAR continues to update its database and improvise its detection capabilities.