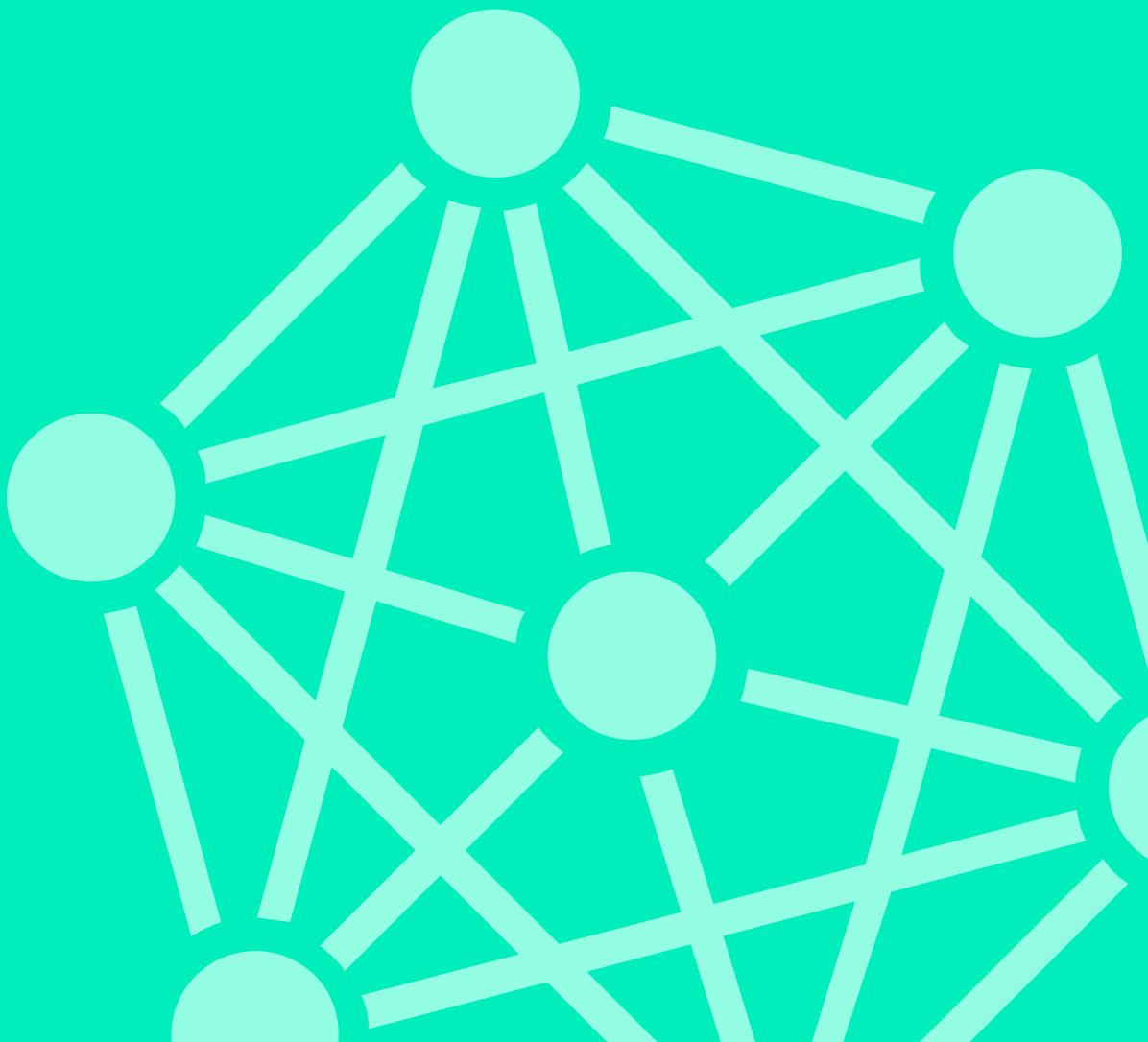
Logsign

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

Endpoint Protection



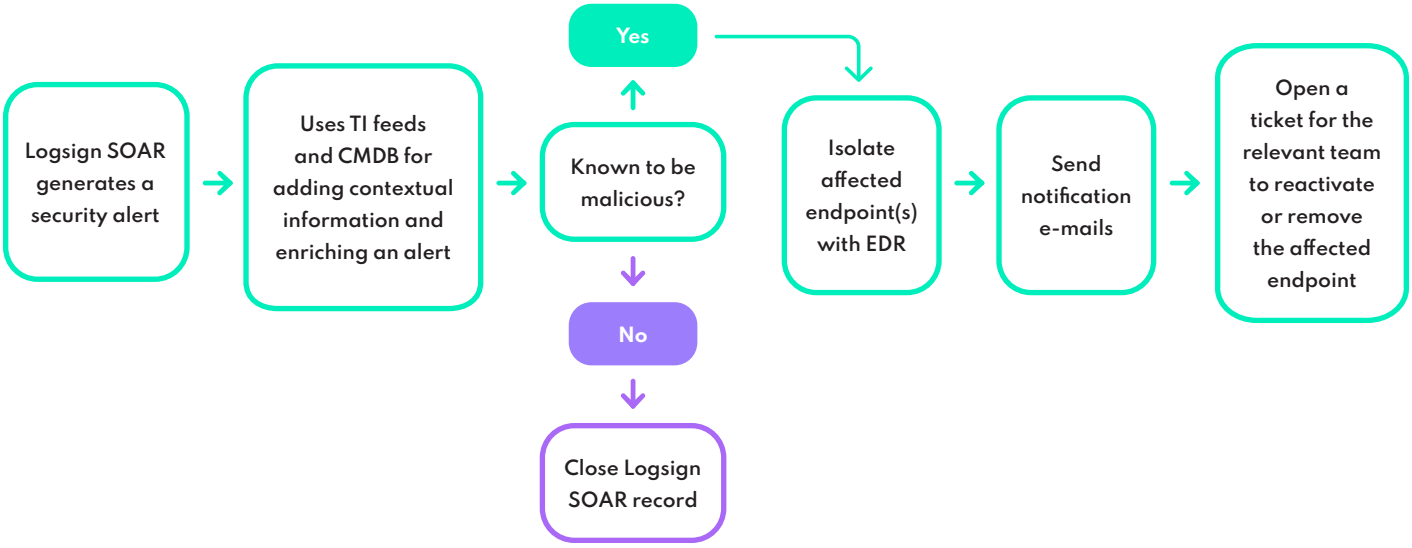
Endpoint Protection

Customer Challenge

Modern-day enterprises own hundreds or thousands of endpoints. These endpoints generate a plethora of log data that can unnecessarily occupy your SOC team. Security alerts from these endpoints are often repetitive and mundane. Manually responding to each alert takes a significant amount of time for your SOC team and decreases their efficiency as well as productivity. As a result, they may not be able to focus on high-risk alerts that can substantially impact your business operations.

How to protect endpoints with Logsign SOAR

Logsign SOAR automatically prioritizes alerts due to endpoint devices and helps your SOC team in automating appropriate mitigation measures.



Business Process Analysis

It may take a security analyst up to 40 minutes to deal with a security alert. With the help of automation, this time is cut down to 1-2 minutes.

Benefits

Logsign SOAR enriches security alerts by utilizing threat intelligence feeds, CMDB, and EDR. As soon as it detects an affected endpoint, it notifies your security team and proceeds forward with automated mitigation measures. Further, it isolates the affected endpoint and helps your SOC team in ensuring that a security alert does not become a security incident.