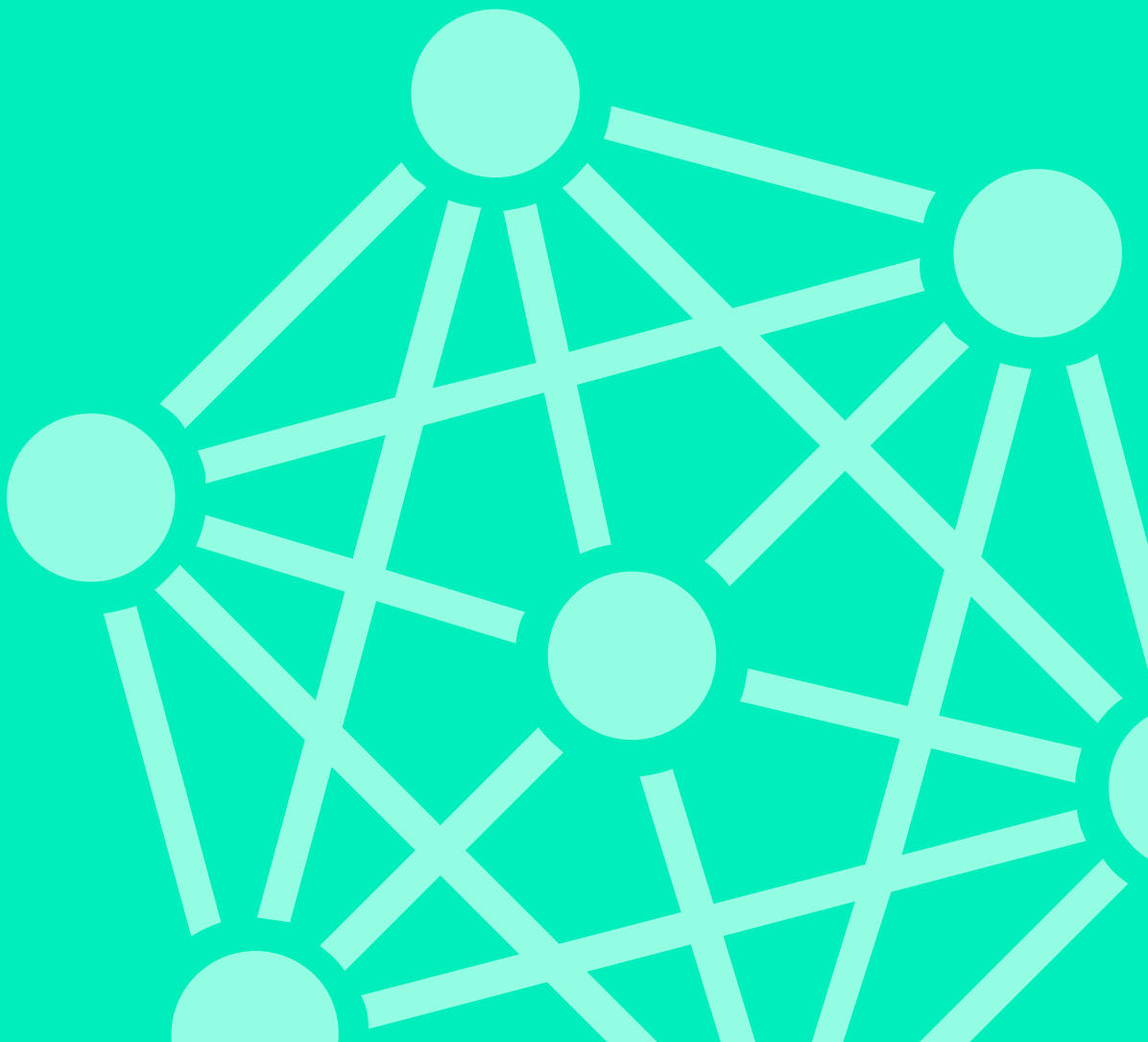
Logsign

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

SIEM Incident Triage

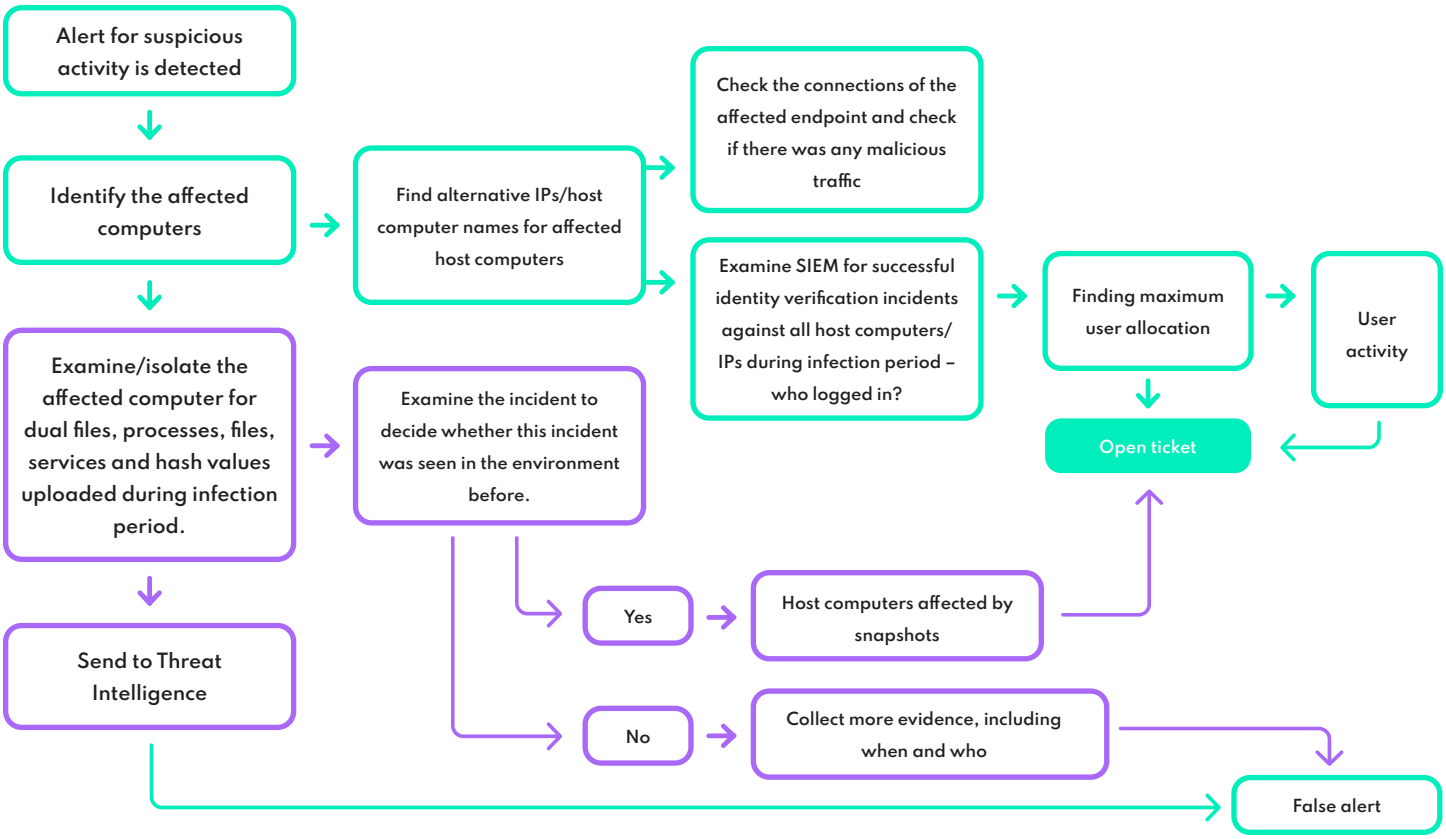


SIEM Incident Triage

Customer Challenge

Manually, it is not feasible for your SOC team to review every alert that might be a potential threat. If your organization uses a legacy SIEM solution, it may not provide the necessary incident context and require your team to gather additional information. As your SOC team can only deal with a limited number of security alerts, this increases the chances of exhaustion and missing genuine alerts.

SIEM Incident Triage with Logsign SOAR



Business Process Analysis

It may take a security analyst up to 45 minutes for manually responding. However, with the help of automation, Logsign SOAR cuts down this time to 1-2 minutes.

Benefits

Logsign SOAR allows security teams to handle a high volume of security alerts and incidents with the help of automation. In cases where the platform requires a security analyst to take the final decision, it showcases the relevant contextual information for the analyst to decide. In other words, SOAR facilitates your organization in responding to security alerts with a clearly defined workflow and consistency.