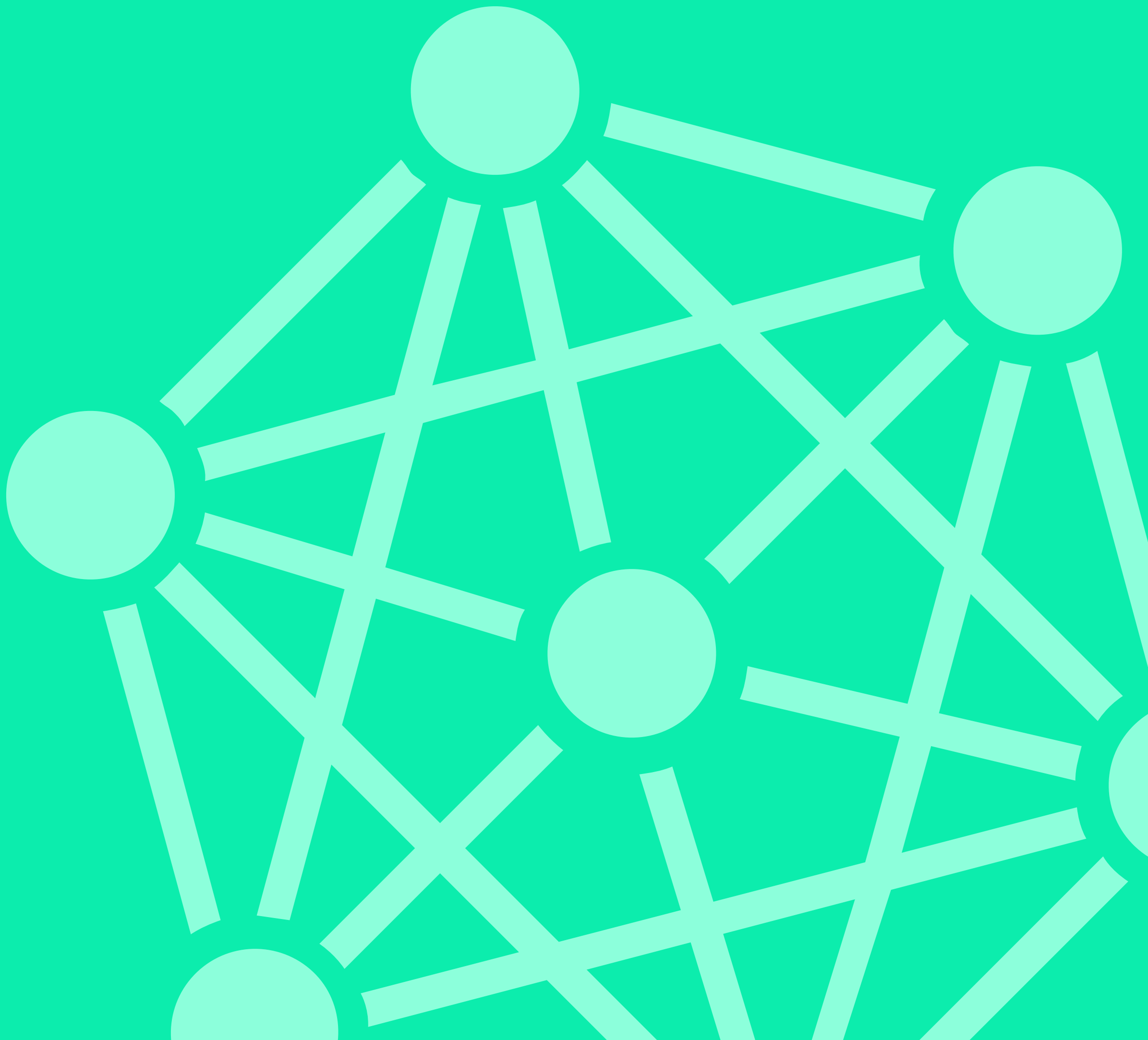
Logsign®

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

Forensic Investigation



Forensic Investigation

Customer Challenge

Various regulations and standards require organizations to collect forensic evidence after a security incident. At times, regulatory or court proceedings may require this evidence and an organization is reasonably expected to prove its authenticity. To ensure that best practices for evidence collection are adopted, the post-incident forensic investigation becomes a tedious and time-consuming task. Logsign SOAR solution automates forensic evidence collection from different sources and records the actions taken by itself as well as various members of your SOC team.

How to conduct an automated forensic investigation

- As soon as a security incident is detected, the SOC team initiates the incident response process.
- Logsign SOAR collects the requires information throughout the response process.
- This collected information becomes available for utilization by your SOC team from the centralized dashboard.

Business process analysis

It may take a security analyst minimum of 45 minutes to collect forensic evidence from an organizational network of a reasonable size. With the help of automation, this time is cut down to 1-2 minutes.

Benefits

Logsign SOAR automates the collection of forensic evidence by collecting log data from relevant sources. When the incident response team begins their mitigation process, this information is readily available on the centralized dashboard. Your SOC team has more time to analyze the collected data; instead of spending it on gathering log data from different sources.