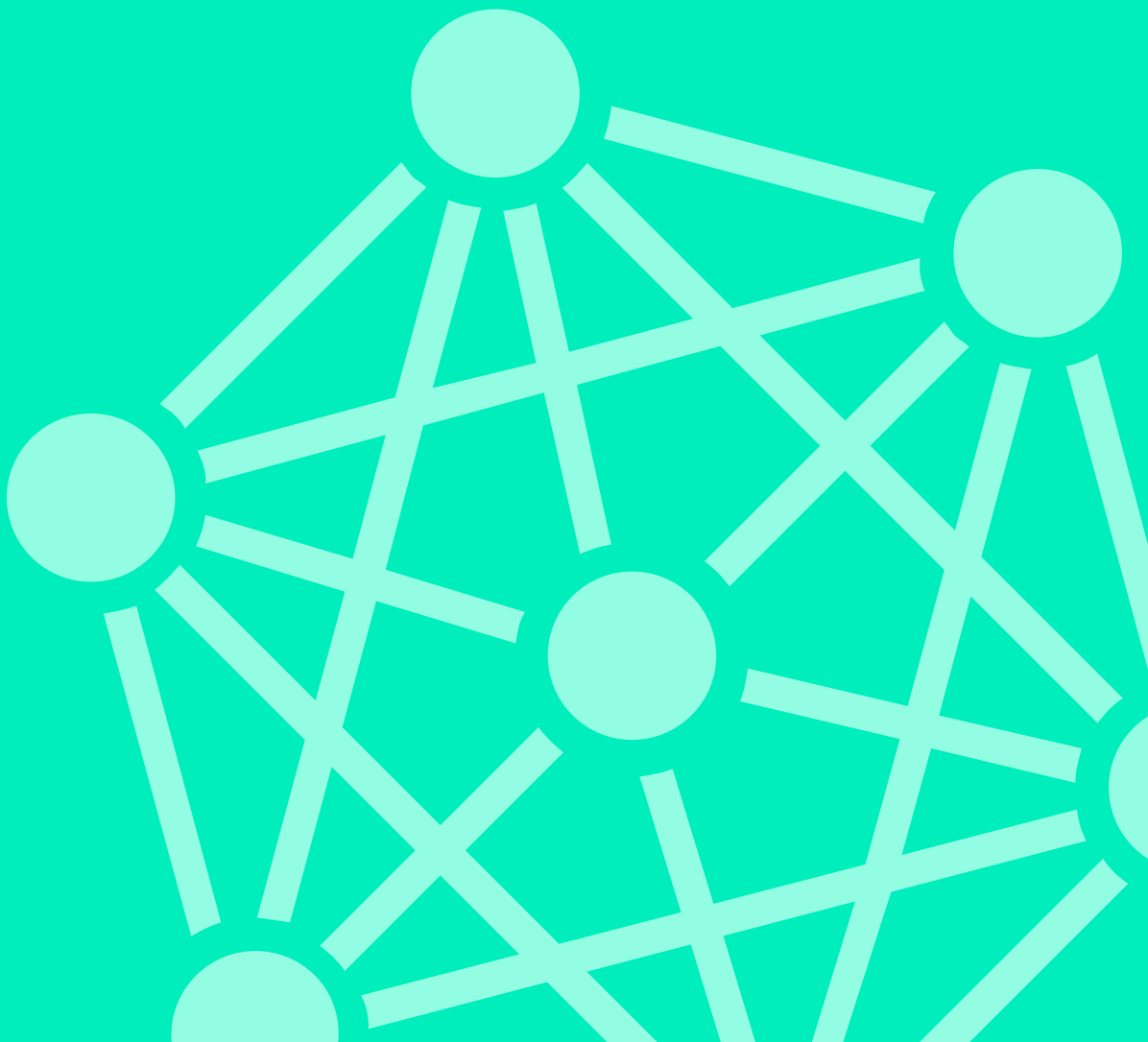
Logsign

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

Insider Threat Detection

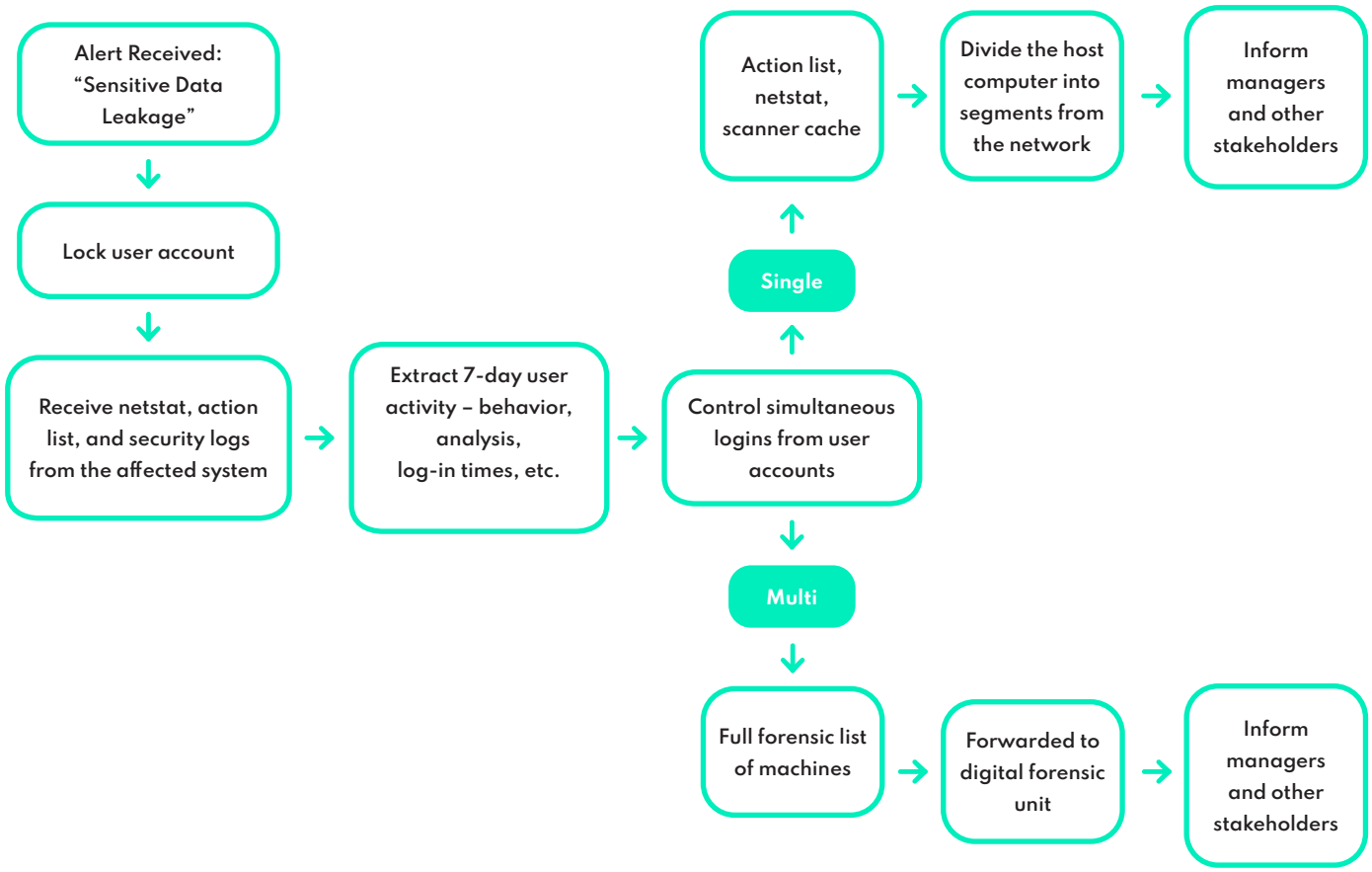


Insider Threat Detection

Customer Challenge

Negligence of employees, misusing employee credentials, and data theft by employees are leading causes of security incidents. With the help of manual tools, it becomes difficult for security teams to swiftly detect insider threats by collecting log data from multiple systems. In most of the cases, insider threat is similar to normal user behavior and may affect more than one system at once. Logsign SOAR acts as the single tool your SOC team needs to obtain a full picture of an incident. As a result, your mean time to detect (MTTD) and mean time to response (MTTR) decrease.

How to detect insider threats with Logsign SOAR



Business Process Analysis

It may take a security analyst up to 40 minutes to manually detect an instance of insider threat. With the help of automation, this time is cut down to 1-2 minutes.

Benefits

Logsign SOAR helps in the identification of threats that were unknown before. It partners with your SOC team in detecting and preventing insider threats before they cause a significant impact on your business operations. As automation is incorporated in your response and detection activities, your team's productivity increases, and they are not over exhausted.