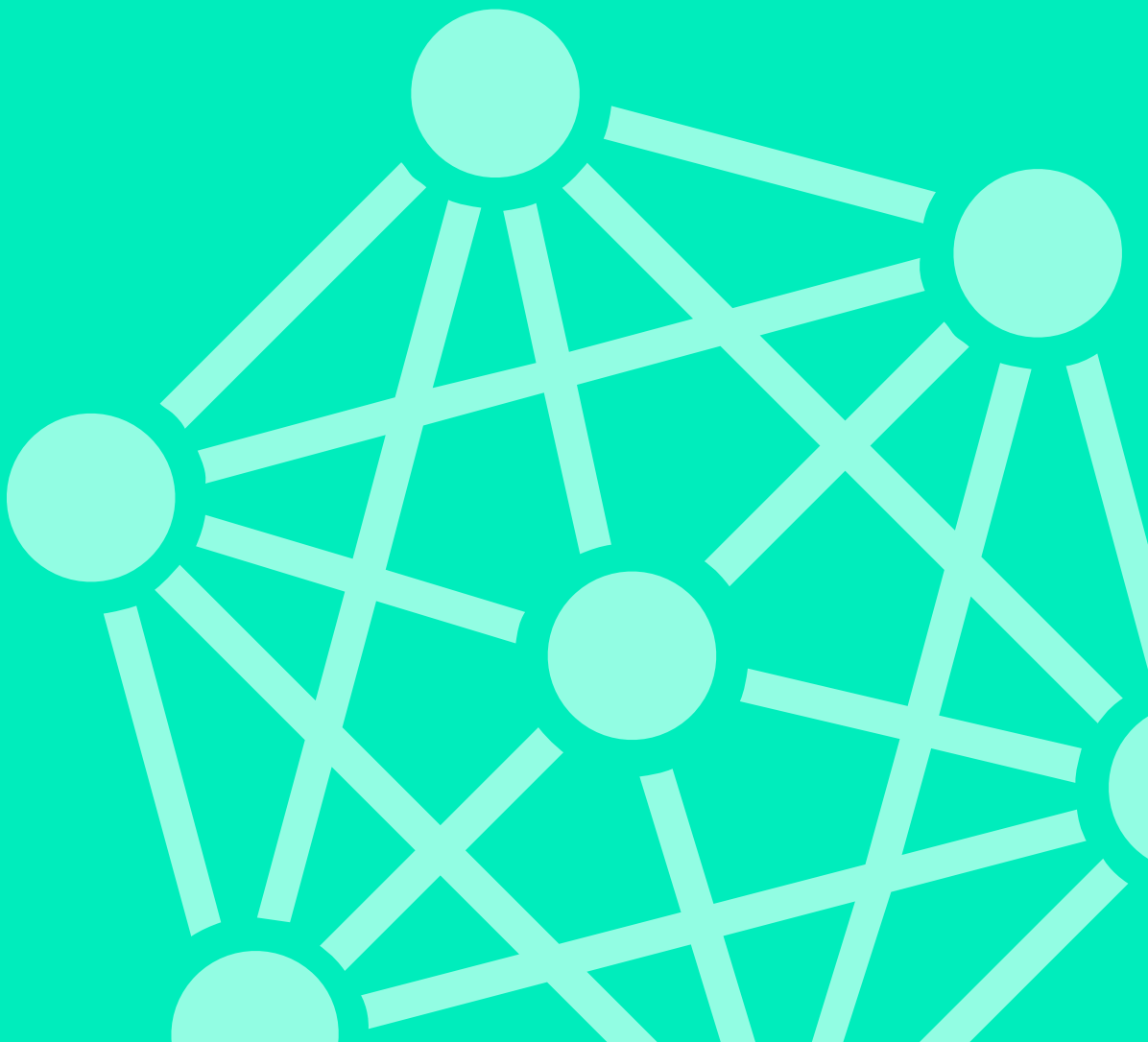
Logsign

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

Threat Hunting

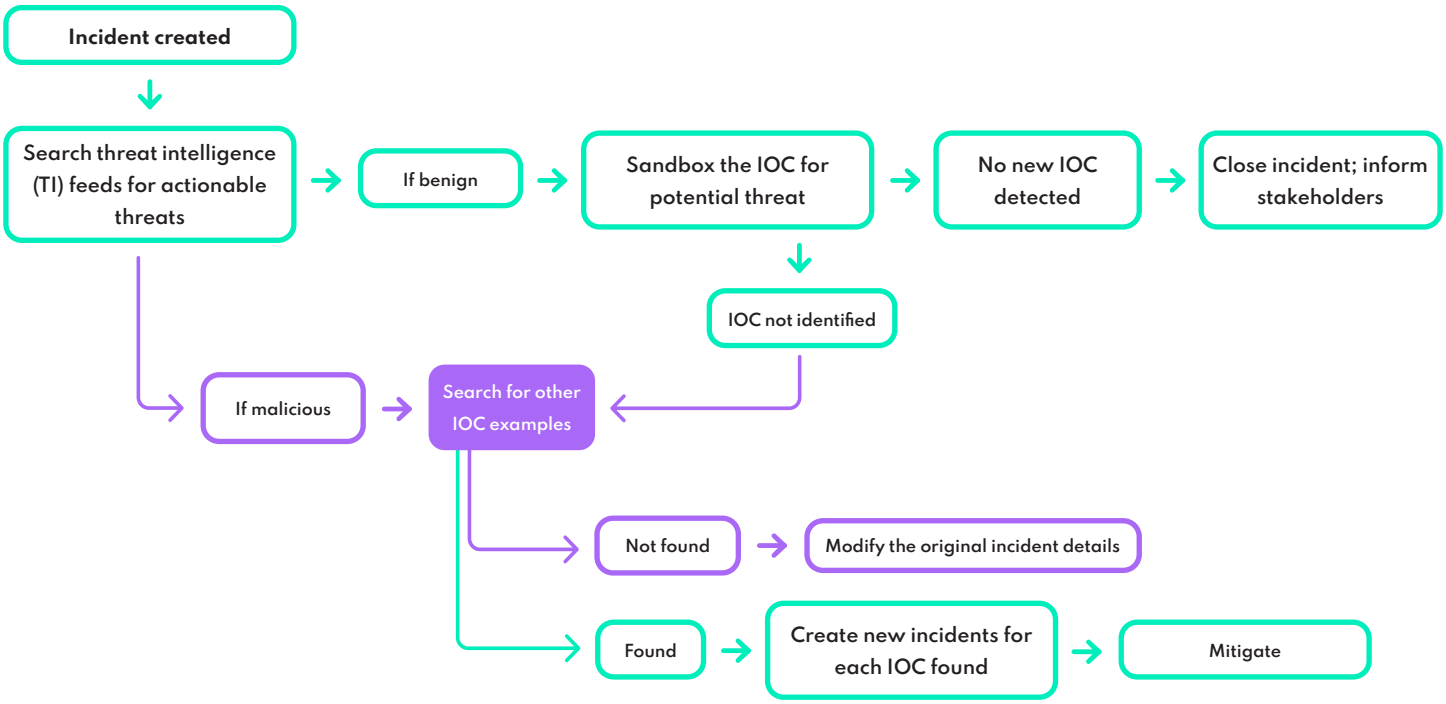


Threat Hunting

Customer Challenge

In the ever-evolving threat landscape, an organization cannot sit back and wait for an attack to happen. An ideal security program involves passive as well as active security measures. One such measure that shows proactiveness on an organization's part is continuous threat hunting. Threat hunting involves searching for, detecting, and isolating threats that can potentially impact the security of an organization's IT infrastructure.

How to hunt threats with Logsign SOAR



Business Process Analysis

An automated process for identifying IOCs will conclude in a few minutes.

Benefits

Threat hunting is a luxury skillset, and it requires time and patience. According to a SANS Institute survey, only 31% of organizations have dedicated staff member(s) for threat hunting. However, with a proactive SOC team, your organization is in a better place to detect and mitigate advanced persistent threats (APTs). With Logsign SOAR, you can automate the identification of possible IOCs, their impact, and other contextual information so that you can find and fix a potential security incident even before it occurs.