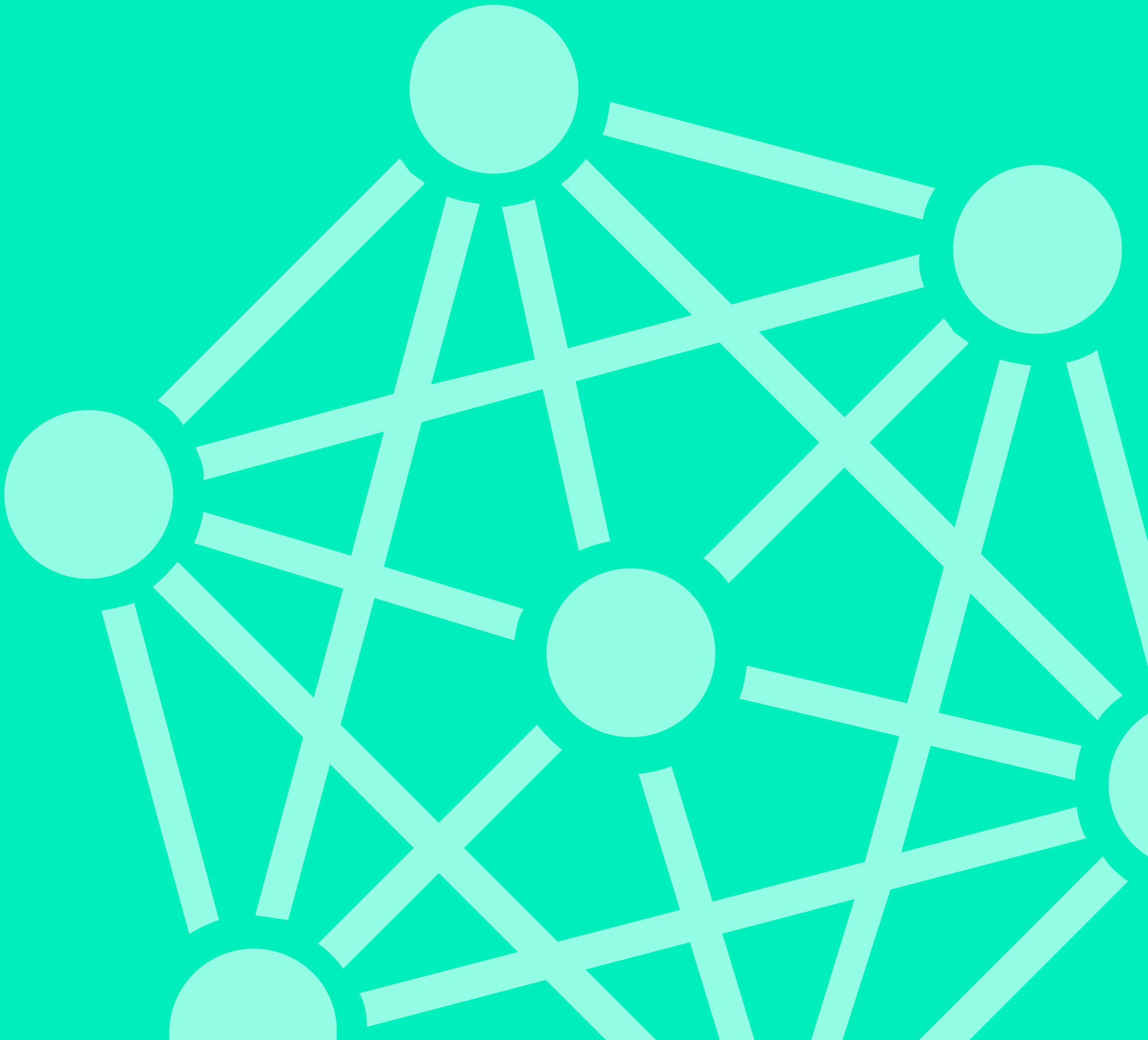
Logsign®

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

Identity Verification/ Enforcement

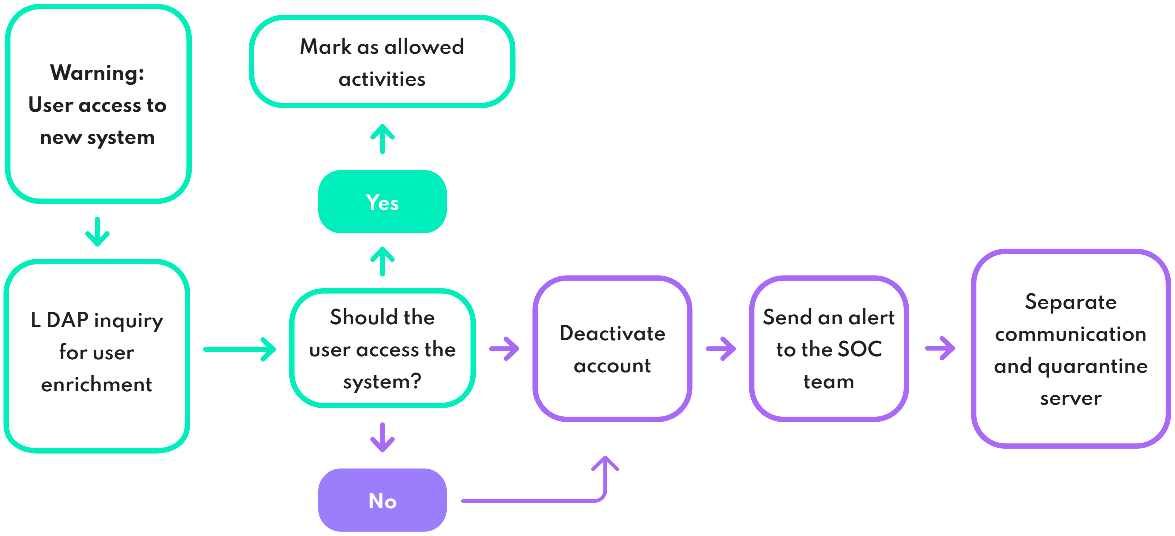


Identity Verification/Enforcement

Customer Challenge

Ideal organizations seek to grant minimal access level permissions to their employees for reducing the probability of insider's threat. While easy access for genuine users is desirable, Logsign SOAR helps in preventing unauthorized and inappropriate usage of identity information of individuals. In enterprise-level networks, a SOC team cannot spend their time in verifying every login request they get. If they do, the process would be prolonged and time-consuming. Security teams are expected to determine whether the new user's behavior is legitimate in a matter of few seconds.

How to verify/enforce identity with Logsign SOAR


Warning: User access to new system
L DAP inquiry for user enrichment
Should the user access the system?
Yes
Mark as allowed activities
No
Deactivate account
Send an alert to the SOC team
Separate communication and quarantine server

Business Process Analysis

It may take a security analyst up to 40 minutes to grant permission for accessing a system resource to a user. With the help of automation, this time is cut down to 1-2 minutes.

Benefits

To minimize the probability of insider's threat and data breaches, organizations have to adopt the principle of least privileges. Suppose Logsign SOAR detects that the user behavior is probably suspicious. In that case, one course of action it takes is to deactivate the user account and isolate the relevant endpoint to prevent any potential harm to the entire network.