Detection of Alarm Suppression, Detection Strategy DET0728

Archived: 2026-04-02 10:42:30 UTC

AN1861

Monitor for loss of network traffic which could indicate alarms are being suppressed. A loss of expected communications associated with network protocols used to communicate alarm events or process data could indicate this technique is being used. This will not directly detect the technique’s execution, but instead may provide additional evidence that the technique has been used and may complement other detections.
Monitor for loss of operational process data which could indicate alarms are being suppressed. This will not directly detect the technique’s execution, but instead may provide additional evidence that the technique has been used and may complement other detections.
Monitor for loss of expected device alarms which could indicate alarms are being suppressed. As noted in the technique description, there may be multiple sources of alarms in an ICS environment. Discrepancies between alarms may indicate the adversary is suppressing some but not all the alarms in the environment. This will not directly detect the technique’s execution, but instead may provide additional evidence that the technique has been used and may complement other detections.
Monitor for loss of expected operational process alarms which could indicate alarms are being suppressed. As noted in the technique description, there may be multiple sources of alarms in an ICS environment. Discrepancies between alarms may indicate the adversary is suppressing some but not all the alarms in the environment. This will not directly detect the technique’s execution, but instead may provide additional evidence that the technique has been used and may complement other detections.

Log Sources
