Detection of Block Reporting Message, Detection Strategy DET0789

Archived: 2026-04-05 17:16:08 UTC

Analytics

- ICS

AN1921

Monitor asset alarms which may help identify a loss of communications. Consider correlating alarms with other data sources that indicate traffic has been blocked, such as network traffic. In cases where alternative methods of communicating with outstations exist alarms may still be visible even if reporting messages are blocked.
Monitor for the termination of processes or services associated with ICS automation protocols and application software which could help detect blocked communications.
Monitor application logs for changes to settings and other events associated with network protocols that may be used to block communications.
Monitor for a loss of network communications, which may indicate this technique is being used.
Monitor for lack of operational process data which may help identify a loss of communications. 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
