Detection of Monitor Process State, Detection Strategy DET0727

Archived: 2026-04-05 13:58:26 UTC

AN1860

Monitor ICS automation network protocols for functions related to reading an operational process state (e.g., "Read" function codes in protocols like DNP3 or Modbus). In some cases, there may be multiple ways to monitor an operational process' state, one of which is typically used in the operational environment. Monitor for the operating mode being checked in unexpected ways.
Monitor applications logs for any access attempts to operational databases (e.g., historians) or other sources of operational data within the ICS environment. These devices should be monitored for adversary collection using techniques relevant to the underlying technologies (e.g., Windows, Linux).

Log Sources

Source: https://attack.mitre.org/detectionstrategies/DET0727#AN1860