Detection of Program Upload, Detection Strategy DET0761

Archived: 2026-04-05 13:15:51 UTC

Analytics

- ICS

AN1893

Program uploads may be observable in ICS management protocols or file transfer protocols. Note when protocol functions related to program uploads occur. In cases where the ICS protocols is not well understood, one option is to examine network traffic for the program files themselves using signature-based tools.
Monitor device communication patterns to identify irregular bulk transfers of data between the embedded ICS asset and other nodes within the network. Note these indicators are dependent on the profile of normal operations and the capabilities of the industrial automation protocols involved (e.g., partial program uploads).
Monitor for device alarms produced when program uploads occur, although not all devices will produce such alarms.

Log Sources
