Detection of Program Download, Detection Strategy DET0752

Archived: 2026-04-05 15:00:07 UTC

Analytics

- ICS

AN1884

Monitor device alarms for program downloads, although not all devices produce such alarms.
Monitor for protocol functions related to program download or modification. Program downloads may be observable in ICS automation protocols and remote management protocols.
Consult asset management systems to understand expected program versions.
Monitor devices configuration logs which may contain alerts that indicate whether a program download has occurred. Devices may maintain application logs that indicate whether a full program download, online edit, or program append function has occurred.

Log Sources
