Detection of Rootkit, Detection Strategy DET0780

Archived: 2026-04-02 10:48:44 UTC

Technique Detected: Rootkit | T0851

ID: DET0780

Domains: ICS

Analytics: AN1912

Version: 1.0

Created: 21 October 2025

Last Modified: 21 October 2025

Version Permalink

Live Version

Analytics

- ICS

AN1912

Monitor for changes made to firmware for unexpected modifications to settings and/or data that may be used by rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Asset management systems should be consulted to understand known-good firmware versions and configurations.

Log Sources

Data Component	Name	Channel
Firmware Modification (DC0004)	Firmware	None