Detection of Point & Tag Identification, Detection Strategy DET0788

Archived: 2026-04-05 13:00:46 UTC

AN1920

Monitor ICS automation protocols for anomalies related to reading point or tag data, such as new assets using these functions, changes in volume or timing, or unusual information being queried. Many protocols provide multiple ways to achieve the same result (e.g., functions with/without an acknowledgment or functions that operate on a single point vs. multiple points). Monitor for changes in the functions used.
Monitor asset application logs which may provide information about requests for points or tags. Look for anomalies related to reading point or tag data, such as new assets using these functions, changes in volume or timing, or unusual information being queried. Many devices provide multiple ways to achieve the same result (e.g., functions with/without an acknowledgment or functions that operate on a single point vs. multiple points). Monitor for changes in the functions used.

Log Sources

Source: https://attack.mitre.org/detectionstrategies/DET0788