Alarm Suppression, Technique T0878 - ICS

Archived: 2026-04-05 17:11:59 UTC

Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. Alarm messages may be a part of an overall reporting system and of particular interest for adversaries. Disruption of the alarm system does not imply the disruption of the reporting system as a whole.

A Secura presentation on targeting OT notes a dual fold goal for adversaries attempting alarm suppression: prevent outgoing alarms from being raised and prevent incoming alarms from being responded to. [1] The method of suppression may greatly depend on the type of alarm in question:

- An alarm raised by a protocol message
- An alarm signaled with I/O
- An alarm bit set in a flag (and read)

In ICS environments, the adversary may have to suppress or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring. [1] Methods of suppression may involve tampering or altering device displays and logs, modifying in memory code to fixed values, or even tampering with assembly level instruction code.

Source: https://attack.mitre.org/techniques/T0878