Loss of View, Technique T0829 - ICS

Archived: 2026-04-02 10:40:59 UTC

Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves. [1] [2] [3]

Sub-techniques: No sub-techniques

Last Modified: 15 April 2025

Procedure Examples

Mitigations

ID	Mitigation	Description
M0953	Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise. Maintain and exercise incident response plans [12], including the management of gold-copy back-up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.
M0810	Out-of-Band Communications Channel	Provide operators with redundant, out-of-band communication to support monitoring and control of the operational processes, especially when recovering from a network outage [13]. Out-of-band communication should utilize diverse systems and technologies to minimize common failure modes and vulnerabilities within the communications infrastructure. For example, wireless networks (e.g., 3G, 4G) can be used to provide diverse and redundant delivery of data.
M0811	Redundancy of Service	Hot-standbys in diverse locations can ensure continued operations if the primarily system are compromised or unavailable. At the network layer, protocols such as the Parallel Redundancy Protocol can be used to

ID	Mitigation	Description
		simultaneously use redundant and diverse communication over a local network. [14]

Detection Strategy

References

1. Corero Industrial Control System (ICS) Security Retrieved. 2019/11/04
2. Michael J. Assante and Robert M. Lee SANS Industrial Control System (ICS) Security; The Industrial Control System Cyber Kill Chain Retrieved 2024/11/25
3. Tyson Macaulay Michael J. Assante and Robert M. Lee Corero Industrial Control System (ICS) Security Retrieved. 2019/11/04 The Industrial Control System Cyber Kill Chain Retrieved. 2019/11/04 RIoT Control: Understanding and Managing Risks and the Internet of Things Retrieved. 2019/11/04
4. Mark Graham, Carolyn Ahlers, Kyle O'Meara; Dragos. (2024, July). Impact of FrostyGoop ICS Malware on Connected OT Systems. Retrieved November 20, 2024.
5. Team82. (2024, April 12). Unpacking the Blackjack Group's Fuxnet Malware. Retrieved September 11, 2024.
6. Anton Cherepanov, ESET 2017, June 12 Win32/Industroyer: A new threat for industrial control systems Retrieved. 2017/09/15
7. Booz Allen Hamilton. (2016). When The Lights Went Out. Retrieved December 18, 2024.
8. Kevin Beaumont How Lockergoga took down Hydro ransomware used in targeted attacks aimed at big business Retrieved. 2019/10/16
9. Hydro Kevin Beaumont How Lockergoga took down Hydro ransomware used in targeted attacks aimed at big business Retrieved. 2019/10/16 Retrieved. 2019/10/16
10. DHS/CISA. (2023, December 1). IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. Retrieved March 25, 2024.
11. Jamie Tarabay and Katrina Manson. (2023, December 22). Iranian-Linked Hacks Expose Failure to Safeguard US Water System. Retrieved March 25, 2024.
12. Department of Homeland Security 2009, October Developing an Industrial Control Systems Cybersecurity Incident Response Capability Retrieved. 2020/09/17
13. National Institute of Standards and Technology 2013, April Security and Privacy Controls for Federal Information Systems and Organizations Retrieved. 2020/09/17
14. M. Rentschler and H. Heine The Parallel Redundancy Protocol for industrial IP networks Retrieved. 2020/09/25