COST: **$$$**$ IMPACT: **HIGH** COMPLEXITY: **HIGH**

2.F: Does the WWS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?

Recommendation: Require connections between the OT and IT networks to pass through an intermediary, such as a firewall, bastion host, jump box, or demilitarized zone, which is monitored and logged.

Why is this control important?

This control is important because a WWS can limit the ability of an attacker to access OT control systems after compromising the IT network.

OT systems were not originally designed with the same level of security as IT networks. As the Internet became popular, organizations typically kept OT networks separate from IT systems, leaving what is called an "airgap" between OT and IT networks. Over time, however, organizations realized they could find operational efficiencies and cost savings by connecting OT and IT systems and sharing data between them.

While the concept of an airgap is still a popular response to OT/IT connectivity security concerns, it is virtually impossible to maintain one even in the most secure facilities (e.g., Stuxnet, 2010). Therefore, most cyberattacks that target OT networks begin as attacks on a WWS's IT network.

Segmentation is a security practice that digitally divides a WWS's OT and IT computer networks with the goal of improving network performance and cybersecurity.

Implementation Tips

Only allow connections to the OT network from the IT network via approved assets and other approved means.

The most common tool that a WWS can use for network segmentation is to install a firewall at the boundary of the OT and IT networks, which can deny all connections between OT and IT systems by default. With a firewall, a WWS can

Additional Guidance

- ✓ A useful framework for understanding where to segment the network is the Purdue Enterprise Reference Architecture (PERA), or Purdue Model for short. This model separates OT and IT networks into layers, helping to differentiate the types of assets at each level of a control system network. Levels 0 through 3 consist of OT assets, and Levels 4 and 5 refer to the IT enterprise network. Network segmentation primarily occurs between the OT and IT networks at Levels 3 and 4, where a WWS can establish a "demilitarized zone" as a buffer between OT and IT networks using hardware and software tools to monitor, log, and filter traffic.
- ✓ By default, deny all connections to the OT network from the IT network unless explicitly allowed (by IP address and port) for specific system functionality.

control information flow between subnetworks or systems by traffic type, source, destination, and other options.

To fortify cybersecurity measures across operational environments, it is recommended that the OT network be segmented based on specific operational areas, such as individual pumping stations, to effectively localize and mitigate the spread of potential cyber incidents. Additionally, access from the IT network to the OT network should be set to read-only mode to prevent unauthorized actions, except when accessing an RDS (Remote Desktop Service), where users must re-authenticate to ensure secure and controlled access. This approach not only strengthens security posture but also ensures adherence to established best practices, enhancing protection across networks.

Resources

NIST 800-82 (Revision 3) Guide to Operational Technology (OT) Security: See sections 5 & 6 and Appendix E for more information on "Network Segmentation and Segregation." *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-4 (page 28) and SC-7 (page 297) for more information on "Information Flow Enforcement" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NSA "Stop Malicious Cyber Activity Against Connected OT" Advisory: This advisory lists steps that a WWS can take to evaluate risks against its OT system via IT system connection and implement changes with current resources to realistically monitor and detect malicious activity. *https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF*

MITRE ATT&CK - Stuxnet: See "Replication Through Removable Media" for more information on Stuxnet's spread. *https://attack.mitre.org/software/S0603/*

SANS Institute – The Purdue Model and Best Practices for Secure ICS Architectures: See this resource for more information on the Purdue Model and where Network Segmentation occurs in an OT network. *https://www.sans.org/blog/introduction-to-ics-security-part-2/*

DHS CISA – Understanding Firewalls for Home and Small Office Use: See this resource for more information on selecting and configuring a firewall. *https://www.cisa.gov/tips/st04-004*