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

3.A: Does the WWS keep a list of threats and attacker tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the WWS?

Recommendation: Receive CISA alerts, prioritize the Known Exploited Vulnerabilities (KEV) list, and maintain documentation of TTPs relevant to the WWS.

Why is this control important?

Attackers frequently employ common steps or methods during a cyberattack, known as TTPs. If a WWS is aware of common TTPs, then they can monitor for these TTPs on the WWS network and detect an attack before it disrupts or damages operations.

This control is important because it helps a WWS be aware of and detect threats to their OT and IT networks.

Implementation Tips

WWS should monitor both external and internal components as part of their OT and IT cybersecurity program. External monitoring observes events at the boundary of the network, and internal monitoring captures events within WWS systems.

Adopt measures and mitigations recommended in CISA Alerts, such as suspicious network traffic alerting or commercial prevention and detection systems to detect key threats where feasible. CISA's Known Exploited Vulnerabilities (KEV) catalog, included in their vulnerability alerts, helps organizations prioritize and address vulnerabilities that are actively being exploited by malicious actors. These alerts provide critical information on mitigation strategies and are essential for prioritizing security efforts to close the most dangerous gaps in cyber defenses quickly.

Additional Guidance

- ✓ Alerts and advisories provide timely information about current cybersecurity issues and TTPs, vulnerabilities, and exploits. Register to receive alerts and advisories via email from DHS CISA. Other helpful sources for understanding TTPs and actions an attacker may take to move across an OT or IT network are the MITRE ATT&CK and MITRE ATT&CK for ICS frameworks, respectively.
- ✓ There are many commercially available tools that a WWS can use to monitor for certain types of cyberattacks or intrusions into the WWS network. These tools include Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), firewall rules that filter out and alert on certain traffic, and ICS network monitoring tools.
- ✓ These tools can send alerts to a central monitoring system, often called a System Information and Event Monitoring (SIEM) tool. A SIEM tool pulls data from many sources (e.g., IDS/IPS, firewalls, network monitoring tools, Windows Events) into one dashboard and can alert the WWS to unusual or malicious network activity.

Follow your Incident Response plan (see Factsheet 2.S) for the containment, removal of, and recovery from any identified threats.

Resources

NIST 800-82 (Revision 3) Guide to Operational Technology (OT) Security: See Appendix F.7.18 (page 291) for more information on "System and Information Integrity". *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 SI-4 (page 336) for more information on "System Monitoring". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA's National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*

MITRE ATT&CK and MITRE ATT&CK for ICS: See these resources for more information on common TTPs in OT and IT systems, respectively. *https://attack.mitre.org/matrices/ics/*; *https://attack.mitre.org/matrices/enterprise/*