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

**2.T:** Does the WWS collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?

**Recommendation:** Collect and store logs and/or network traffic data to aid in detecting cyberattacks and investigating suspicious activity.

### Why is this control important?

Logging is recording data about events that take place in your OT or IT systems. When responding to a cyberattack, having detailed logs will help your utility and investigators determine how and when an attacker was able to break into the systems, what areas they accessed, and if they breached any sensitive data. Regular reviews of these logs may also allow your WWS to detect an attacker before they are able to impact systems.

### Implementation Tips

Check logs regularly for both completeness and to ensure that all necessary information can be found in case of a cyberattack.

If a log source (e.g., Windows Event Logging) is not active, notify the System Administrator or individual responsible for system security.

If logs are not available for certain OT assets, collect information about network traffic and communications to and from these assets.

See the next page for Additional Guidance on this control.

### Resources

**NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations:** See control AU-2 (page 66) for more information on “Event Logging." *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

**NIST Policy Template Guide:** See Security Logging (4.1a/b) Initial Log Generation. SOP for collecting and maintaining logs. *https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Logging-Standard.docx*

**WaterISAC’s 15 Cybersecurity Fundamentals:** See page 31 for more information on “Logging and Auditing.” *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

**Microsoft Learn – Windows Event Collector:** See this resource for more information on setting up Windows Event Collector. *https://learn.microsoft.com/en-us/windows/win32/wec/windows-event-collector*

`

### Additional Guidance

- ✓ Log sources include but are not limited to network logins and logs from servers, end-user assets (e.g., desktops and laptops), networking equipment (e.g., routers and switches), applications/programs, Intrusion Detection System/Intrusion Protection Systems (IDS/IPS), firewalls, anti-virus software, Data Loss Prevention (DLP) tools, and Virtual Private Networks (VPNs).
- ✓ If possible, WWSs should capture, review, and securely store logs from all these sources for future reference in the event of a cyberattack. At a minimum, WWSs should enable logging for critical servers, firewalls, and remote access tools such as VPNs. A review of the configuration manuals for any firewalls or remote access tools should provide instruction on how to configure and enable logging for these specific assets.
- ✓ For Windows-based systems, the Windows "Event Viewer" application gives the WWS the ability to manually review security logs on an individual asset. To see an example security log in Windows, open the "Event Viewer" app. In the console tree, expand "Windows Logs", and then click "Security". The results pane lists individual security events. To see more details about a specific event, click the event in the results plane. The WWS can collect Windows Events from both servers and endpoints (e.g., desktops and laptops) on a central server for more efficient manual analysis using the Windows Event Collector. While this method is an improvement over fully manual log review, it will not include logs from non-Windows assets and applications – providing an incomplete picture of WWS operations.
- ✓ To overcome this issue, the WWS can use log aggregation software and Security Information Event Management (SIEM) systems to centrally collect logs from practically all sources, simplify reviewing logs, and target events of interest. In addition to having all logs in one place, these tools can also automate many steps of log analysis, making the WWS security team more effective and saving time in the process.