

Checklist for Assessment/Scanning of OT Devices and Applications

- Review all documentation consisting of operational and technical manuals, release notes, white papers and flow diagrams of the application and device. Provided by the manufacturer product/technical team.
- If the OT system is classified as level 4 system engage business owner to have vendor go through a security assessment provided by Harvard information security.
- Start creating inventory of the OT system.
- Validate Network requirements and integrations to other OT systems.
- Obtain test device from vendor if possible.
- Perform network packet captures before and after commissioning of the device, server, and on the Harvard or private control network level.
- Conduct vulnerability scans of the device and web interface if present.
 - User account with administrative /root access is required.
- Require copy of the firmware and software application or review legacy vulnerabilities.
- Validate interaction of the device or software application on the Harvard network.
- Engage for Integrator/vendor for follow-up questions from Assessment