OT Asset Discovery

Building and Maintaining an Industrial Asset Inventory

OT Security Learning Series

Document 510 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Asset discovery and inventory management is the foundation of any OT security program. You cannot protect assets you don't know exist, and you cannot assess risk without understanding what systems are in your environment.

Information

Industry reports from SANS ICS and Dragos indicate that organizations commonly underestimate their OT asset count by 30–50%. Unknown assets represent unmanaged risk and potential attack vectors.

1.1 Why Asset Inventory Matters

- **Vulnerability management:** Know what needs patching
- **Risk assessment:** Understand exposure and criticality
- **Incident response:** Identify affected systems quickly
- **Compliance:** Required by IEC 62443, NERC CIP, etc.
- **Change management:** Baseline for detecting unauthorized changes

2 Discovery Methods

2.1 Passive Discovery

Key Point

Passive methods are preferred for OT environments:

- Network traffic analysis (SPAN/TAP)
- Protocol fingerprinting from observed communications
- DHCP and DNS log analysis
- Switch CAM table queries (low risk)

2.2 Active Discovery

Warning

Active scanning risks in OT:

- May crash legacy PLCs and controllers
- Can trigger safety system responses
- May disrupt real-time communications
- Should only be performed during maintenance windows

If active discovery is necessary:

- Use OT-aware scanning tools with rate limiting
- Test in lab environment first
- Schedule during planned downtime
- Have rollback procedures ready

2.3 Manual Methods

- **Physical walkdowns:** Visually inspect and document equipment
- **Documentation review:** Network diagrams, as-built drawings
- **Vendor records:** Maintenance contracts, support agreements
- **Interviews:** Operations and maintenance staff knowledge

3 Asset Attributes

3.1 Essential Information

Attribute	Description
Device Name/ID	Unique identifier for the asset
IP/MAC Address	Network identifiers
Device Type	PLC, HMI, Switch, Server, etc.
Vendor/Model	Manufacturer and model number
Firmware/OS Version	Software version for vulnerability matching
Location	Physical and logical (Purdue level, zone)
Function	Role in the process (criticality)
Owner	Responsible person or department

3.2 Security-Relevant Attributes

- **Network connectivity:** What can it communicate with?
- **Protocols used:** Modbus, OPC, Ethernet/IP, etc.
- **Authentication:** Does it support/require authentication?
- **Patch status:** Last update, available patches
- **End-of-life status:** Vendor support availability
- **Backup status:** Configuration backup available?

4 Inventory Management

4.1 Initial Baseline

1. Deploy passive monitoring on key network segments

2. Conduct physical walkdowns of critical areas
3. Review existing documentation and diagrams
4. Merge and deduplicate discovered assets
5. Validate with operations and engineering staff

4.2 Ongoing Maintenance

Keeping Inventory Current

- **Continuous monitoring:** Detect new devices automatically
- **Change management integration:** Update on approved changes
- **Periodic reviews:** Quarterly validation with stakeholders
- **Reconciliation:** Compare discovered vs documented assets

4.3 Common Challenges

- **Shadow OT:** Unauthorized devices connected by staff
- **Transient devices:** Vendor laptops, temporary equipment
- **Legacy systems:** Undocumented, forgotten equipment
- **Serial devices:** Not visible on IP networks
- **Air-gapped systems:** Require manual discovery

5 Criticality Assessment

5.1 Classification Criteria

Assess each asset's criticality based on:

- **Safety impact:** Could failure cause injury?
- **Process impact:** Effect on production if unavailable
- **Recovery time:** How long to restore or replace?
- **Data sensitivity:** Confidential process information?
- **Connectivity:** Exposure to other networks

5.2 Criticality Levels

Level	Description
CRITICAL	Safety systems, emergency shutdown, life safety
HIGH	Core process control, production-critical systems
MEDIUM	Supporting systems, historians, non-critical HMIs
LOW	Monitoring only, easily replaceable

6 Integration

6.1 Connected Systems

Asset inventory should integrate with:

- **Vulnerability management:** Match assets to CVEs
- **SIEM/SOC:** Provide context for security alerts
- **CMDB:** Enterprise configuration management
- **Backup systems:** Ensure critical configs are backed up
- **Incident response:** Rapid asset lookup during incidents

7 Further Reading

Standards

- **IEC 62443-2-1** – Security Management System Requirements
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Asset Identification Resources
  https://www.cisa.gov/resources-tools/resources
- **SANS ICS** – State of ICS/OT Cybersecurity Survey
  https://www.sans.org/white-papers/
- **Dragos** – Year in Review Reports
  https://www.dragos.com/year-in-review/

Part of the OT Security Learning Series