Network Isolation and Segmentation

Each Purdue level has different requirements associated with the process and the organization. The following should be considered when assessing the security of each level:

- **Network Boundaries** – Start with corporate network and control network firewalls and DMZs between Levels 3 and 4. Lower-numbered levels will have less network restrictions due to process requirements.
- **Remote Access** – Test remote connectivity used by employees, vendors/integrators, and managed service providers. This access crosses the network boundaries and are the highest risk.
- **Virtual Local Area Networks (VLAN)** – Test process segmentation to understand the attack surfaces within the control network. Management servers at Level 3 should only communicate with specific assets and services at lower levels. Cross-process communications should be analyzed to understand these attack surfaces.
- **Wireless Networks** – Industrial control networks can deploy a variety of wireless technologies, including cellular, Wi-Fi, Bluetooth, Mesh networking, and other proprietary and ISM-related technologies.

Common Adversary Targets

Threat intelligence indicates adversaries are frequently targeting these ICS devices for harmful impacts.

- **Data Historian** – The database system storing industrial control system (ICS) process information. It is a trusted asset that may have trusted connections to both IT and ICS, and it could be abused to pivot from a compromise in IT to the control network.
- **Programmable Logic Controllers** – PLCs interface with physical hardware in the real world and monitor and change the state of operations. Controlling the PLCs or their communications impacts safety and availability.
- **Engineering Workstations** – Usually a laptop with the software to view, manage, and program network devices, PLCs, RTUs, and other field devices.
- **Network Shares** – Engineering documents with details about the control network, process, configurations, and other data necessary to understand the process and operations.

Access Control

Access control must be implemented to augment network boundaries. Most control networks cannot adhere to the credential policies defined for corporate environments. However, risk is significantly reduced by implementing a few basic access control concepts. Focus assessment efforts on:

- **Windows Active Directory** – Control network AD **cannot** have trusted relationships or trusted forests with the corporate AD. Additionally, user/administrative / service credentials should not be manually synchronized with the corporate environment.
- **Windows Group Policy Objects** – Review AD Group policy configurations to understand how the Windows security control mechanisms are implemented across Windows servers and workstations.
- **File Shares** – Review file shares to understand implementation and identify assets that can be accessed.
- **Application Access** – Review network services that permit access without authentication or using default credentials.

Vulnerability Detection

Information gathered from each phase should be reviewed to understand the attack surfaces within the control network. These attack surfaces should be reviewed for publicly documented vulnerabilities in the technology or service. Control asset deployments should be reviewed to determine vulnerabilities in implementation and configuration.

CRITICAL NOTE: Safety is more important than verification.

To evaluate and prioritize risk from vulnerabilities, use the MITRE ICS ATT&CK Matrix (https://collaborate.mitre.org/attackics/index.php/Main_Page) and the Industrial Control System Cyber Kill Chain (https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297). This information can be used to plan patching and remediation efforts. Many control networks cannot patch for long periods of time. This situation can be mitigated by monitoring for activity specific to identifying and exploiting known vulnerabilities.

Assessment Methodology Quick Start Guide v0.1

SANS ICS
ics.sans.org

By Dean Parsons & Don C. Weber
dparsons@sans.org | don@cutawaysecurity.com

This guide covers the basics for an industrial control sector assessment methodology. It is intended to be used to gauge the maturity of a security program implemented to protect control environments.

The guide concentrates on several primary areas to help gauge implementation of the current program and prioritize risk reduction.

How to Use This Sheet

This quick-start guide will cover the following areas to organize a security assessment of a control network:

- Data Gathering
- Physical Walk-Through
- Network Isolation and Segmentation
- Asset Inventory
- Access Control
- Vulnerability Identification
- Purdue Model Levels
- Assessment vs. Penetration Testing vs. Red Team
- Common Adversary Targets

Data Gathering

All assessments begin with gathering information about the organization, the process, and the project scope.

- **Goals of assessment** – The OT, IT, and InfoSec teams should all agree on the scope and purpose of the assessment. The OT team should determine when the assessment occurs in order to reduce the impact on the process.
- **Identify Key Personnel** – Understanding the process comes from interviews with many individuals: leadership, process engineers, operators, system/network administrators, vendors and integrators, and managed service providers.
- **Company OSINT** – Online information provides a lot of information about an organization. Google, Shodan, LinkedIn, and other websites will augment understanding of the control network.
- **Policies and Procedures** – Control network policies and procedures, relevant to the scope of the assessment, provide details about the expectations of security controls and technology implementations.
- **Regulations and Requirements** – Security controls and assessment scope can be driven by specific regulatory requirements.
- **Process Description and Purpose** – Understanding the process and its requirements helps with threat modeling, attack surface identification, and testing priorities.
- **Network and Traffic Flow Diagrams** – These documents provide details about what technologies were intended to be implemented and can be used to compare the current implementation.
- **Asset Inventories** – These documents will provide details about hardware and software implemented on the control network. This information should be used to identify known attack surfaces and vulnerabilities.

Physical Walk-Through

The security assessment team needs to understand the actual process that is being tested.

- **Safety Training** – Access to process environments typically requires safety training and personal protective equipment (PPE). This may involve a simple form to review and sign, or it could involve an hour or two of training and testing.
- **Meeting with Leadership and Team** – Review scope and intent with key personnel to ensure agreement and reduce apprehension.
- **Process Walk-Through** – Walk through key areas of the process to gain an understanding of the actual process.
- **Control Cabinets** – Physically inspect control and network cabinets to understand how technologies are deployed, wired, and maintained.
- **Physical Security** – Gain an understanding of the physical security controls and physical security team's responsibilities.
- **Operators and Engineer Interviews** – Interact with process operators to understand their normal tasks and their major concerns for the safety of personnel and the resilience of the process.

Assessment vs. Penetration Test vs. Red Team

- **Security Assessment** – An evaluation of a system or systems to understand the attack surface and reduce risk to the control network. Minimal impact and modifications to assets to gather information.
- **Penetration Test** – Testing exploits and weaknesses of a secured environment to demonstrate risks inherited from known and discovered vulnerabilities in deployed assets and services. May negatively impact process.
- **Red Team Assessment** – An evaluation of an organization to determine how skilled adversaries and threat actors will target and attack the control network. Actions are similar to penetration test but are more advanced in actions on target.

Asset Inventory

Organizing logging and monitoring within the control network is most effective when prioritized to address network events, then system events, and finally the consolidation, correlation, and evaluation of these events. The following are several starting points for this discussion.

- **Passive Network Monitoring** – Gather system, field device, and protocol communication information by monitoring the network using network taps or SPAN ports. Low risk but may induce changes to network device configurations and increase CPU utilization. Monitor carefully and plan rollback.
- **Active Scanning** – Gather inventory data by conducting light and safe network scans to identify devices on the network. Scanning when connected to different network segments will most likely be required. There is a medium to high risk to the process, and the work should be monitored carefully and in communication with the operational technology (OT) team.
- **Service Enumeration** – Interactions with network services are necessary to understand the attack surface. These interactions should be limited to tools that understand the protocols and normal functionality of the service. There is a high risk to the process, and this work should be performed on small target sets and in communication with the OT team. Limit to development/lab equipment when possible.
- **Inventory Correlation** – Review discovered assets and services with inventory tracking.

Purdue Model Levels

Control networks are typically implemented following the Purdue Enterprise Reference Architecture Model, typically referred to as the Purdue Model. The following details how this model organizes assets within the control network:

- **Level 5** - Internet, Cloud Services
- **Level 4** - Enterprise IT Business Systems
- **Level 3** - ICS Plant Site, SCADA Controls
- **Level 2** - HMI, Engineering Workstations
- **Level 1** - Process Control, Field Devices
- **Level 0** - Sensors, Hardware Actuators