Industrial Automation and control System Network Characterization Operational technology

Company:

Statuses:

Pass, Fail, N/A, TBD

|  |  |  |
| --- | --- | --- |
| # | Cyber Security Questionnaire | Status |
| Secure network and system architecture principles | | |
|  | Is the Purdue reference model being used correctly, with all components placed on their designated network segments? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Component Overview | | |
|  | What hardware and software components are used in the OT environment? |  |
|  |  |
|  | Who are the key vendors for the OT systems and devices? |  |
|  |  |
|  | What communication protocols are in use (e.g., Modbus, OPC)? |  |
|  |  |
|  | Are there any third-party integrations or cloud services involved? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Risk Management | | |
|  | Has the organization addressed specific factory/plant/site OT-oriented cybersecurity risks? |  |
|  |  |
|  | Do risk owners exist and has the risk been communicated to the relevant stakeholders? |  |
|  |  |
|  | Are risk assessments performed in a timely manner to identify associated OT risks? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Supply Chain | | |
|  | Are all vendors accounted for? Is personnel for sensitive systems vetted prior to providing access? Are SLAs set for major outages with vendors? Is there an agreed upon software/hardware update policy with vendors? |  |
|  |  |
|  | What are the remote access capabilities for vendors and do they adhere to best practices without breaking the Purdue model? What is the on-premises support policy for vendors? |  |
|  |  |
|  | What are the onboarding and offboarding procedures for vendors? Do they align with best practices? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Identity and Access Management | | |
|  | Is there remote access to the ICS environment? |  |
|  |  |
|  | Are remote connections done via DMZs (IT to OT)? |  |
|  |  |
|  | Is unauthorized remote access prevented from the ICS site (e.g. cellular modems, dial-up, unauthorized ISP connections, direct vendor network connections)? |  |
|  |  |
|  | Are only named accounts used, with no shared accounts? |  |
|  |  |
|  | Are accounts locked after multiple failed authentication attempts? |  |
|  |  |
|  | What is the password policy? |  |
|  |  |
|  | How is multi-factor authentication implemented for users? |  |
|  |  |
|  | How are default accounts for systems handled? |  |
|  |  |
|  | Is session timeout properly configured? |  |
|  |  |
|  | Is the dedicated ICS domain logically segregated from the corporate Active Directory? If connected, how? |  |
|  |  |
|  | Are Domain Controllers and other AD servers placed on a dedicated Level 3 subnet based on the Purdue model? |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Secure Architecture | | |
|  | Does the Layer 2 separation (VLANs, port assignments, etc.) accommodate the Purdue model and restrict physical access appropriately? |  |
|  |  |
|  | Does the Layer 3 separation (ACLs, routing, etc.) accommodate the Purdue model and restrict network access appropriately? |  |
|  |  |
|  | Which IT/OT segmentation concepts are used - airgap, firewall, data diode? |  |
|  |  |
|  | If using an airgap, is the solution truly air-gapped on both the IT and OT sides? |  |
|  |  |
|  | If using a data diode, is it the only path for data between IT and OT? Does it limit transfer to specific file types? |  |
|  |  |  |
|  | Do firewall rules accommodate appropriate risk classifications between zones? |  |
|  |  |
|  | Do security controls block all communication by default except what is specifically required? |  |
|  |  |
|  | Is the firewall the only path for data between IT and OT? |  |
|  |  |
|  | Does the firewall limit lateral movement between IT and OT? |  |
|  |  |
|  | Does the firewall allow OT telemetry from the OT side? |  |
|  |  |
|  | Does the firewall prevent users in the Industrial zone from accessing arbitrary destinations in the Enterprise zone? |  |
|  |  |
|  | Is Internet access restricted to only zones 4 and 5? |  |
|  |  |
|  | Is Internet traffic filtered using a securely deployed proxy? |  |
|  |  |
|  | Do users on zones 4-5 use separate computers for internal vs external access? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Ransomware Protection | | |
|  | What are the potential scenarios and methods for ransomware to move laterally? |  |
|  |  |
|  | What would be the immediate impact and crown jewel assets at risk from ransomware? |  |

|  |  |  |
| --- | --- | --- |
| Security Program | | |
|  | Is there a well-documented procedure for network access requests that includes business justification, approvals, implementation dates, etc? |  |
|  |  |
|  | Does the OT network access request procedure require management approval? |  |
|  |  |
|  | For admin/jump servers, is access role-based using OT domain groups? |  |
|  |  |
|  | Are jump servers only able to communicate with devices managed by the assigned role? |  |
|  |  |
|  | Are jump servers hardened based on Microsoft hardening methodology? |  |
|  |  |
|  | Is information on jump servers scanned using file transfer services? |  |
|  |  |
|  | For file transfers, are all files into OT scanned using a transfer mechanism like CDR? |  |
|  |  |
|  | Is there a one-way mechanism enforcing remote file transfers in/out of OT? |  |
|  |  |
|  | Are there any direct external connections to the OT network? If so, what is the justification and approval? |  |
|  |  |
|  | Is a NAC solution in place? |  |
|  |  |
|  | Do Windows/Linux end-user systems have EDR, device control, host IPS/firewall, disk encryption, and application whitelisting? |  |
|  |  |
|  | Are there dedicated OT infrastructure systems for anti-virus, patching, etc. separate from the business network? |  |
|  |  |
|  | What is the process for transferring system updates to OT systems? What are the policies for standard vs proprietary systems? |  |
|  |  |
|  | What is the patch management strategy and governance capability? |  |
|  |  |
|  | What is the update procedure and status for security tools on OT end-user systems? |  |

|  |  |  |
| --- | --- | --- |
| Detection Capabilities | | |
|  | What is the process for identifying security alarms in OT? |  |
|  |  |
|  | Are OT-side security alarms from the firewall visible on the IT side? |  |
|  |  |
|  | Is there an audit process to regularly review firewall logs for misuse of IT-OT connections? |  |
|  |  |
|  | Is there a SIEM/SOC solution? Are personnel familiar with the OT environment for effective triage/response? |  |
|  |  |
|  | Is all communication in/out of the control network monitored and logged? |  |
|  |  |
|  | Is NetFlow utilized on the OT network? |  |
|  |  |
|  | What is the retention period for network monitoring logs? |  |
|  |  |
|  | Are security events from OT endpoints transferred and monitored in near real-time? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Incident Response | | |
|  | Is there a dedicated incident response plan for OT or does the organizational IRP address OT incidents? |  |
|  |  |
|  | Are OT containment capabilities and procedures documented and implemented? Who owns that process? |  |
|  |  |
|  | Have incident response drills and tabletop exercises been conducted for OT scenarios? |  |
|  |  |
|  | Are critical vendors part of the incident response plan/team? |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Data Protection | | |
|  | Are security measures in place to protect OT backups from cyber threats like ransomware? |  |
|  |  |
|  | What are the recovery procedures for OT systems and data? Have they been tested? |  |
|  |  |