# Work Force Development Roles along with Job Tasks and Skills

This is a summary of the job roles and skills required to perform each task. The job tasks are related to normal work activities performed by each role. Tasks that are performed as part of ICS4ICS and Cyber Incident are highlighted in light blue.

**Cybersecurity Roles**

| **Job Tasks** | **Cybersecurity Intelligence**  **Officer  (ICS4ICS)** | **Cybersecurity CIRT**  **(soc) Analyst** | **Cybersecurity Engineer** | **Cybersecurity Forensics**  **Analyst** | **Cybersecurity Threat Intel &**  **Vulnerability Analyst** |
| --- | --- | --- | --- | --- | --- |
| 1. AA/BA Education | Cyber/IT/Computer | AA Cyber/IT | Cyber/IT | Cyber/Computer | Cyber/Computer |
| 1. Certification | CISSP, GSEC, CompTIA SEC+ | CISSP, CISM,  GCIH, ECIH, CIH | CISSP, OSCP, GSEC, GCIA, CompTIA SEC+ | GCFA, CHFI, CCE  *MSWin*: GCFE, CCFE  *Digital*: CDFE  *Network*: GNFA  *Mal*: GREM, CREA | CISSP, CEH, OSCP,  GCTI, GCIA |
| 1. Obtain basic knowledge required to perform your role | Cyber Incident Response, Assets, Crypto, App Sec Mgmt, IAM, network, IDS/IPS, SIEM, EDR/XDR, HIDS, Web app Firewall,  ISA-62443 | Cyber Incident Response, Assets, Crypto, App Sec Mgmt, IAM, network, IDS/IPS, SIEM, EDR/XDR, HIDS, Web app Firewall | Assets, Crypto, App Sec Mgmt, IAM, network, IDS/IPS, SIEM, EDR/XDR, HIDS, Web app Firewall,  ISA-62443 | Assets, Crypto, App Sec Mgmt, IAM, network, IDS/IPS, SIEM, EDR/XDR, HIDS, Web app Firewall,  *Malware*: see list | Assets, Crypto, App Sec Mgmt, IAM, network, IDS/IPS, SIEM, EDR/XDR, HIDS, Web app Firewall, CSEC |
| 1. Obtain knowledge of IT/Cyber to provide background to perform your role | Security Ops, OS, Network firewall monitoring, Network scan, APT,  Ransomware,  Cyber crimes | Security Ops, OS, applications | Security Ops, OS, Network firewall monitoring, Network scan | APT,  Ransomware,  Cyber crimes | Security Ops, Network Packet Analysis |
| 1. Obtain knowledge of OT to provide background to perform your role | ISA Cybersecurity courses,  CISA / INL ICS training series | ISA Cybersecurity courses,  CISA / INL ICS training series | ISA Cybersecurity courses,  CISA / INL ICS training series | ISA Cybersecurity courses,  Forensics specific courses | ISA Cybersecurity courses,  Vulnerability specific courses |
| 1. Stay aware of the latest Knowledge required to perform your role | Maintain knowledge of technology, support and other processes, and best practices | | | | |
| 1. Use Industry Sector(s) Knowledge | Industry experience and expertise for critical infrastructure sector(s) and/or sub-sector(s) | | | | |
| 2. Business Requirements |  |  | Cyber solutions |  |  |
| 2. Design |  |  | Cyber solutions |  |  |
| 2. Design aligned with other technologies |  |  | Network design |  |  |
| 2. Evaluate technologies for Procurement |  |  | Cyber solutions |  |  |
| 3. Configuration |  |  | Cyber solutions, create processes /  Various tech. consult on config |  | Various tech. consult on config with Cyber Eng. |
| 3. Ensure Cybersecurity |  |  | Protect data |  |  |
| 3. Inventory |  |  | Cyber solutions |  |  |
| 3. Maintenance |  |  | Cyber solutions |  |  |
| 3. Manage Access |  |  | Select Access control solutions /  Various tech. consult on Access |  |  |
| 3. Release |  |  | Assess risks/CVE, Various tech. consult on risks / create process / upgrade specs |  |  |
| 3. Risk |  |  | Various Tech. assessments |  |  |
| 3. Testing |  |  | Cyber solutions |  |  |
| 4. Monitor |  |  | SIEM Config and create processes |  | Setup tools to detect vulnerabilities |
| 4. Vulnerability |  |  | Work with Vulnerability Analyst |  | Assess external vulnerable sources, org policies, vulnerable scans,  mitigate vulnerable / Establish vulnerable program |
| 5. Incident Response | Direct IR technical team efforts and provide reporting | Create IR plan with training, escalation, exercises /  Analyze events / define containment and remediation / create processes |  | Analyze and preserve data / recommend containment | Evaluate threats and recommend remediation |
| 5. Problem & Support |  |  | Support various technology team efforts |  |  |
| 5. Recovery (BCP/DR) |  | Engage BCP/DR experts to help various teams establish plans and work with them to invoke plans |  |  |  |
| 6. Documentation | Document installation, operational, and administration procedures, AND configuration and architectural, risk and vulnerability assessments, and incident reports | | | | |
| 6. People | Establish and maintain communication channels with stakeholders. | | | | |
| 6. Project |  |  | Contribute tech. expertise |  |  |
| 6. Train Staff |  |  | Train users and technical staff on work and support processes |  |  |
| 7. Cybersecurity Program |  |  | Define a program, policies, controls and standards / engage executives and auditors |  |  |
| 8. Programming |  | Automate common tasks | Automate common tasks |  | Automate common tasks |
| 9. Data Protection | Ensure data are protected under the applicable data classification and legal directives | | | | |

**OT/ICS Roles**

| **Job Tasks** | **OT Analyst** | **OT Engineer** | **OT Technician** | **OT Cybersecurity Analyst** | **OT Network Analyst** |
| --- | --- | --- | --- | --- | --- |
| 1. AA/BA Education | Computer, Electric  Automate, Telecom | Computer, Electric  Automate, Telecom  Software, Instrumentation | Computer, Eng, Cybersecurity | Computer, Electric, Cybersecurity | Computer, MIS |
| 1. Certification | CCNA, CompTIA Network+ | GICSP, CCNA, CND, CompTIA Network+ and SEC+,  ISA CAP,  PE License for Engineers | VMWare,  CCNA, CCT | GSEC,  CompTIA SEC+,  Network+, CCNA | CISSP, CCNA, CND, CompTIA Network+ |
| 1. Obtain basic knowledge required to perform your role | ISA Cybersecurity, SCADA, DCS, PLC,  Field devices and other equipment, IOT Security | ISA Cybersecurity, SCADA, DCS, HMI  PLC, RTU, IED, instrumentation,  Data historians,  Safety (SIS), IOT Security, ACM,  control systems protocols | ISA Cybersecurity, Industrial instruments,  Analyzers, Pumps, Motors, Controllers | ISA Cybersecurity, SCADA, DCS, PLC,  Field devices and other equipment, Knowledge of ICS Cyber Kill Chain and Purdue Model,  APTs, IoT security | Network (various) |
| 1. Obtain knowledge of IT/Cyber to provide background to perform your role | Network and capture tools, Security, and communication protocols | Unix, Windows, Oracle, SQL, Networking,  Telecom | Network and capture tools, Security, and communication protocols | Network and capture tools, Security tools (endpoint, IDS, SIEM, vuln mgmt), communication protocols,  Unix, Windows, Knowledge of basic attack classes, Basic incident triage/SOC analysis | Unix, Windows, Oracle, SQL, Networking,  Telecom |
| 1. Obtain the latest Knowledge required to perform your role | Maintain knowledge of technology, support and other processes, and best practices | | | | |
| 1. Use Industry Sector(s) Knowledge | Obtain Industry Sector specific knowledge and use in your job | | | | |
| 2. Business Requirements |  | Work with technical and business staff (Interface between OT team and IT Teams) | | | |
| 2. Design | Develop architectures of system components consistent with technical specifications | | | | |
| 2. Design aligned with other technologies | Identify gaps in OT network architecture | | | | |
| 2. Evaluate technologies for Procurement | Develop system procurement specifications | | | | |
| 3. Configuration | Configure your technologies in your field align with other technologists | | | | |
| 3. Configuration with controls | Oversee implementation of system controls | | | | |
| 3. Ensure Cybersecurity | Ensure Cybersecurity, Privacy, Compliance, and data protection requirements can be met in the solution | | | | |
| 3. Inventory | Perform asset management/inventory of technology (IT, OT, and other) resources | | | | |
| 3. Maintenance | Coordinate maintenance efforts for hardware, software, firmware, and other components | | | | |
| 3. Manage Access | Manage access controls for all systems and components within your scope of responsibility | | | | |
| 3. Release | Assess security/product patches to be applied, develop a patch schedule  Develop change management policies and procedures  Develop system upgrade specifications | | | | |
| 3. Release Permit | Follow safety rules, instructions and procedures of the Plant and issue work permit for the appropriate jobs | | | | |
| 3. Risk |  | Risk Audits;  PHA |  |  |  |
| 3. Testing | Lead system and component testing of technologies in field and integrated technologies | | | | |
| 3. Factory/Site Acceptance Test |  | Create plan/Lead |  | Participate |  |
| 4. Monitor | Monitor ICS environment/components to ensure health, identify security vulnerability, and abnormalities | | | | |
| 4. Performance | Monitoring performance of OT systems AND implement preventive measures to enhance OT reliability | | | | |
| 4. Vulnerability | Work with Cybersecurity to review OT, network, etc. for security threats and prepare action to protect them | | | | |
| 5. Incident Response | Respond to cyber incident to provide support for the OT environment | | | | |
| 5. Problem & Support | Provide technical support including problem resolution for users and technical teams | | | | |
| 5. Recovery (BCP/DR) | Identify and recover essential system functions or sub-systems for continuity and availability | | | | |
| 6. Documentation | Produce documentation and specs: installation, operational, and administration procedures, configuration and architectural documents, risk and vulnerability assessments, and incident reports | | | | |
| 6. People | Establish and maintain communication channels with stakeholders. | | | | |
| 6. Project | Participate in projects and contribute technical expertise | | | | |
| 6. Train Staff | Train users and technical staff on work and support processes and use of systems/applications | | | | |
| 8. Data | Produce reports as needed based on requests from management, business and OT staff, and others | | | | |
| 8. Improve | Drive consistency and best practices in work processes including automating work processes | | | | |
| 8. Programming |  | For advanced control strategies |  | Compare large datasets from APIs, CSV, XML |  |

**IT Roles**

| **Job Tasks** | **IT Cloud Analyst** | **IT Desktop Analyst** | **IT Network Analyst** | **IT Server and**  **Host Analyst** | **IT SysAdmin** |
| --- | --- | --- | --- | --- | --- |
| 1. AA/BA Education | IT/Computer | IT/Computer | Computer/MIS | Computer | IT/Engineering |
| 1. Certification | See  AWS, Azure. Others | LPIC-1, ACSP, Network+, CompTIA A+ | CISSP, CCNA, CND, CompTIA Network+ | LPIC-1, IAT, RHCSA, VCP-DCV, CASE | LPIC-1, RHCSA, VCP-DCV, CASE, ISP, CCT |
| 1. Obtain basic knowledge required to perform your role | Cloud practitioner fundamentals, architecture, developer, security, Admin | Windows, AD, VMWare, SCCM, CITRIX, Linux, Mac, Network, Cisco VPN, PC hardware,  HDI-SCA | Network (various) | Server OS, storage solutions, services (Exch, file, print), server hardware, SQL | Windows, AD, VMWare, SCCM, Linux, Mac, Network, Cisco VPN, PC hardware |
| 1. Obtain the latest Knowledge required to perform your role | Stay aware of the latest Knowledge required to perform your role | | | | |
| 1. Use Industry Sector(s) Knowledge | Obtain Industry Sector specific knowledge and use in your job | | | | |
| 2. Business Requirements | Work with other groups technical and the business to define requirements | | | | |
| 2. Design | Develop architectures of system components including technical specifications. | | | | |
| 2. Design aligned with other technologies | Identify gaps in OT network architecture |  | Identify gaps in OT network architecture |  |  |
| 2. Evaluate technologies for Procurement | Develop system procurement specifications | | | | |
| 3. Configuration | Configure technologies including working with other technologists on integration | | | | |
| 3. Configuration (network) | Assist others to maintain network security, config. routers, firewalls, network solutions |  | Assist others to maintain network security, config. routers, firewalls, network solutions |  |  |
| 3. Ensure Cybersecurity | Ensure Cybersecurity, Privacy, Compliance, and data protection requirements can be met | | | | |
| 3. Inventory | Perform asset management/inventory of technology (IT, OT, and other) resources | | | | |
| 3. Maintenance | Coordinate maintenance efforts for hardware, software, firmware, and other components | | | | |
| 3. Manage Access | Manage access controls for all systems and components within your scope of responsibility | | | | |
| 3. Release | Assess security/product patches to be applied, develop a patch schedule  Develop change management policies and procedures  Develop system upgrade specifications | | | |  |
| 3. Risk | Assess and monitor cyber security risks and deploy solutions to manage risks | | | |  |
| 3. Testing | Lead system and component testing of technologies in field and integrated technologies | | | | |
| 4. Monitor | Monitor IT systems, such as network, software and hardware and resolve identified risks, errors, and/or issues | | Monitor networks - identify security breaches | Monitor IT systems, such as network, software and hardware and resolve identified risks, errors, and/or issues | |
| 4. Performance | Monitor system and data utilization to ensure app and systems function | Monitor performance for desktop services | Monitor network to ensure availability and performance for all system users | Monitor and maintain the Server infrastructure availability | Monitor system performance |
| 5. Problem & Support | Provide technical support including problem resolution for users and technical teams | | | | |
| 5. Recovery (BCP/DR) | Identify and recover essential system functions or sub-systems for continuity and availability | | | | |
| 6. Documentation | Produce documentation and specs: installation, operational, and administration procedures, configuration and architectural documents, risk and vulnerability assessments, and incident reports | | | | |
| 6. People | Establish and maintain communication channels with stakeholders | | | | |
| 6. Project | Participate in projects and contribute technical expertise | | | | |
| 6. Train Staff | Train users and technical staff on work and support processes and use of systems/applications | | | | |
| 8. Data | Custom reporting and analysis | Monthly metrics |  | Data extraction requests / design | Database integration and reporting |
| 8. Improve | Identify areas for improvement including automating processes | | | | |
| 8. SDLC | Support system and application development and maintenance efforts | | | | |
| 9. Data Protection | Ensure data are protected under the applicable data classification and legal directives | | | | |

**NIMS/ICS Roles**

| **Job Tasks** | **Incident Commander** | **Operations Section Chief**  **(ICS4ICS)** | **Planning Section Chief** | **Logistics Section Chief** | **Finance Admin Section Chief** | **Public Information Officer** | **Safety Officer** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. AA/BA Education | Mgmt/Ops | Computer/MIS | Business/PM | SCM | Finance | Journalism | Safety/Health |
| 1. Certification | ICS4ICS Credentials by role (via FEMA NIMS/ICS Training) | | | | | | |
| 1. Obtain basic knowledge for role | ICS4ICS Job Aids and NIMS/ICS Forms for each role AND learn company NIMS/ICS plan | | | | | | |
| 1. Obtain knowledge of IT/Cyber |  | IT/Cyber |  |  |  |  |  |
| 1. Obtain knowledge of OT for role |  | OT |  |  |  |  |  |
| 1. Use Industry Sector(s) Knowledge | Obtain Industry Sector specific knowledge and use in your job | | | | | | |
| 6. People | Establish and maintain communication channels with stakeholders | | | | | | |
| 9. Data Protection | Protect confidential and Personal information based on laws and company policies | | | | | | |
| 9. Safety/Health of people | Recognize and mitigation hazardous situations | | | | | | |
| NIMS/ICS. Accessibility | Ensure accessibility for all staff | | | | | | |
| NIMS/ICS. IAP | Participate in the planning process including review, validate and modify plans | | | | | | |
| NIMS/ICS. Legal and Regulatory | Demonstrate knowledge of and apply relevant legal, regulatory, and fiscal constraints | | | | | | |
| NIMS/ICS. Meetings | Attend and participate in team meetings and develop and provide your team with priorities | | | | | | |
| NIMS/ICS. Org key personnel | Create org | Identify kind, type and number of resources required to achieve section objectives | | | | | |
| NIMS/ICS. Org |  | Evaluate staffing needs and org team in your section | | | | | |
| NIMS/ICS. Org | Perform roles on your team that have not yet been staffed | | | | | | |
| NIMS/ICS. Oversight | Ensure staff follows applicable org policies, contracts, standard operating procedures and agreements | | | | | | |
| NIMS/ICS. Prioritize | Disseminate priorities and expected completion timelines to staff | | | | | | |
| NIMS/ICS. Team health and safety | Evaluate mental and physical fatigue of assigned personnel | | | | | | |
| NIMS/ICS. Transition | Participate in transition or incident closeout and demobilization | | | | | | |
| NIMS/ICS. Turnover | IC Turnover | Receive briefing from Incident Commander (IC) or outgoing Section Chief or Officer | | | | | |
| NIMS/ICS. Work env | Create a positive work environment | | | | | | |
| NIMS/ICS. Role specific tasks | IC | Operations | Planning | Logistics | Finance | PIO | Safety |