SUPERVISORY CONTROL AND DATA ACQUISITION SERVER SPECIALIST

RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Personnel
OVERALL FUNCTION	The Supervisory Control and Data Acquisition (SCADA) Server Specialist is responsible for the controller-side hardware, firmware, and software
COMPOSITION AND ORDERING SPECIFICATIONS	1. This position can be ordered as a single resource. 2. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment 3. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	SINGLE TYPE	NOTES
DESCRIPTION	The SCADA Server Specialist position is responsible for the controller-side hardware, firmware, and software and: 1. Responds to crisis or urgent situations for SCADA front-end systems and associated server-side infrastructure to manage controllers and their associated software and hardware systems 2. Is responsible for Incident Command System (ICS)/SCADA workstations and servers 3. Executes various approaches aimed at mitigating, preparing, responding, and recovering servers from shutdown 4. Is an adjunct to the National Incident Management System (NIMS) Type 1 SCADA Controller Specialist	Not Specified
EDUCATION	Not Specified	Not Specified
TRAINING	Completion of the following: 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Incident Command System for Single Resources and Initial Action Incidents 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction	Not Specified

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	Agency Having Jurisdiction (AHJ)-documented and validated knowledge, skills, and abilities demonstrated in the following areas: 1. Desktop, server, and mainframe operating systems including Windows, Unix, Linux, and Mac OS 2. Human Machine Interfaces (HMIs) 3. Remote controlled equipment and front-end-servers 4. Common two and three wire hardware control buses 5. Physical and server security, firewalls and intrusion detection systems 6. Data backup, types of backups, and recovery concepts and tools 7. Host/network access controls and defense-in-depth concepts and controls 8. Log analytics and the use of the corresponding industry tools 9. Applying host access controls and network access controls including firewalls and screening routers 10. Intrusion detection and prevention (IDS/IPS) systems 11. Performing backup and recovery functions 12. Diagnosing and troubleshooting SCADA issues AHJ-documented and validated experience demonstrated in the following areas: 1. Administering and operating SCADA servers, archive servers, and front-end servers 2. Server-side controller software operation, installation and troubleshooting 3. Master/central control terminal units and systems 4. Vendor patch management 5. Coordinating with and providing expert technical support to enterprise-wide computer network defense (CND) specialists to resolve CND incidents	Not Specified
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Specified
CURRENCY	1. Participates in exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 3. Active security clearance	Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	Not Specified	Not Specified

NOTES

Nationally typed resources represent the minimum criteria for the associated category.

REFERENCES

Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014