ISA/IEC 62443 Cybersecurity Risk Assessment Specialist Training

COURSE CONTENT

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The ISA/IEC 62443 Cybersecurity Risk Assessment Specialist Training by Multisoft Systems is designed to equip professionals with the skills and knowledge necessary to assess and manage cybersecurity risks within industrial automation and control systems (IACS). Based on the globally recognized ISA/IEC 62443 standards, this training focuses on identifying vulnerabilities, evaluating risks, and implementing effective mitigation strategies to protect critical infrastructures.

Module 1: Preparing for an Assessment

- ✓ Security lifecycle
- ✓ Scope
- ✓ System architecture diagrams
- ✓ Network diagrams
- ✓ Asset inventory
- ✓ Cyber criticality assessment

Module 2: Cybersecurity Vulnerability Assessment

- ✓ Risk
- ✓ Types of cybersecurity vulnerability assessments
- ✓ High-level assessments
- ✓ Passive and active assessments
- ✓ Penetration testing
- ✓ Conducting high-level assessments
- ✓ Assessment tools
- ✓ Cyber Security Evaluation Tool (CSET)

Module 3: Conducting Vulnerability Assessments

- ✓ Vulnerability process
- ✓ Pre-assessment
- ✓ Standards
- ✓ Research
- ✓ Kick off and walk thru
- ✓ Passive data collection
- ✓ Active data collection
- ✓ Penetration testing

Module 4: Cyber Risk Assessments

- ✓ Understanding risk
- ✓ Risk identification, classification, and assessment
- ✓ ISA/IEC 62443-2-1
- ✓ System under Consideration (SuC)
- ✓ Conduct high-level risk assessment
- ✓ Consequence scale
- ✓ Establish zones and conduits
- ✓ Zone and conduit drawings and documentation
- ✓ Document cybersecurity requirements

Module 5: Conducting Cyber Risk Assessments

- ✓ Detailed cyber risk assessment process
- ✓ Threats
- ✓ Vulnerabilities
- ✓ Consequences
- ✓ Likelihood
- ✓ Calculate risk
- ✓ Security levels
- ✓ Countermeasures
- ✓ Residual risk
- ✓ Documentation

Module 6: Critiquing System Architecture Diagrams

- ✓ Asset inventory
- ✓ Gap assessment
- ✓ Windows vulnerability assessment
- ✓ Capturing ethernet traffic
- ✓ Port scanning

- ✓ Using vulnerability scanning tools
- ✓ Perform a high-level risk assessment
- ✓ Creating a zone and conduit diagram
- ✓ Perform a detailed cyber risk assessment
- ✓ Critiquing a cybersecurity requirements specification

Module 7: Documentation and Reporting

- ✓ Document to maintain
- ✓ Required reports
- ✓ Zone and conduit diagrams
- ✓ Cybersecurity Requirements Specification (CRS)