OT Cybersecurity for DCS & SCADA: Security, Governance & Risk Management

Course Description

This course provides a comprehensive exploration of OT (Operational Technology) cybersecurity in the context of Industrial Control Systems (ICS), SCADA (Supervisory Control and Data Acquisition), and Distributed Control Systems (DCS). Participants gain knowledge of SCADA fundamentals, DCS configuration, ICS/SCADA security models, governance frameworks, vulnerability management, and risk mitigation strategies. The program emphasizes both foundational and advanced security principles, aligned with international standards, to ensure protection of critical infrastructure and industrial operations.

Audience Profile

This course is designed for:

- IT Security Professionals and Analysts
- ICS/SCADA and DCS Engineers
- Cybersecurity Consultants in OT/ICS domains
- Network Security Administrators
- Process Control, Automation & Instrumentation Engineers
- Incident Responders and Forensic Analysts
- Risk Management and Compliance Officers
- Industrial Network Specialists and System Integrators
- Government and Defense Personnel focused on critical infrastructure
- Plant Managers and Operations Managers in manufacturing or utilities
- R&D and Technical Consultants in industrial cybersecurity

Prerequisite

Participants should have a fundamental understanding of:

- Process control principles
- Industrial control systems (ICS), PLCs, and sensors
- Basic networking and IT security concepts

Course Objectives

By the end of this course, participants will be able to:

- Understand and apply ICS/SCADA and DCS security models
- Identify vulnerabilities and apply risk management techniques
- Configure, operate, and secure SCADA/DCS systems against cyber threats
- Apply international standards such as ISO 27001, IEC 62443, NERC CIP, and NIST SP 800-82
- Implement governance, risk, and compliance frameworks in OT environments
- Detect, respond to, and mitigate security incidents in SCADA/DCS infrastructures
- Leverage modern OT security strategies including IDS/IPS, bridging the air gap, and IoT/cloud integration

---

Table of Contents (TOC)

Day 1: Fundamentals of SCADA & DCS

- Introduction to SCADA Systems
- SCADA Architecture & Functions
- Data Acquisition, Communication & Visualization
- Comparison of PLC, SCADA, and DCS
- Applications of SCADA and DCS

Day 2: ICS/SCADA Security Models & Networking

- IT Security Model vs ICS/SCADA Security Model
- TCP/IP Fundamentals & ICS Protocols (Modbus, Profibus, Fieldbus)

- DCS Networking & Communication Standards
- Redundancy Concepts in DCS
- Human-Machine Interface (HMI) Security

Day 3: Threat Landscape & Vulnerability Management

- Hacking Methodologies in ICS/SCADA Environments
- Intelligence Gathering, Footprinting, Scanning & Exploitation
- Vulnerability Assessment Challenges in OT
- Zero-Day Vulnerabilities & Exploit Lifecycle
- ICS/SCADA Vulnerability Databases & CVEs
- Risk Management & Case Studies

Day 4: Governance, Standards & Compliance

- ISO 27001 & ICS/SCADA Frameworks
- ISA99 / IEC 62443 (Industrial Automation & Control Security)
- NERC CIP (North American Electric Reliability Corporation)
- NIST SP 800-82 (Guide to ICS Security)
- CFATS (Chemical Facility Anti-Terrorism Standards)
- Governance Models for ICS & DCS Security
- Security Policies, Roles & Responsibilities
- Risk Mitigation for Legacy Systems

Day 5: Defense in Depth & Security Operations

- Bridging the Air Gap: Options & Challenges
- Security Guards, Data Diodes & Next-Gen Firewalls
- IDS/IPS in ICS Environments (NIDS, HIDS, NNIDS)
- Incident Detection & Response
- Alarm Management & Logging for Security Monitoring
- Advanced Control Methods in DCS (Feedforward, Cascade, SPC)

- Latest Trends: IoT & Cloud Integration for OT Security
- Case-based Hands-on Exercises & Final Review