OT Security Course

Course Duration: 24 Hrs. **Course Code: OT-SEC-101**

Course Overview

The **OT Security** course is designed for professionals responsible for protecting Operational Technology (OT) environments, including industrial control systems (ICS), SCADA systems, and critical infrastructure. The course focuses on identifying OT-specific threats, implementing security controls, and integrating OT security with IT security frameworks. Participants will gain hands-on experience securing industrial networks while understanding compliance, risk management, and incident response in OT environments.

What You'll Learn?

By completing this course, you will be able to:

- Understand the fundamentals of OT environments and systems
- Identify common OT threats and vulnerabilities
- Implement OT network segmentation and access controls
- Secure ICS, SCADA, and industrial devices
- Monitor OT networks for security incidents
- Develop incident response plans for OT environments
- Apply industry best practices and compliance standards (e.g., NIST, IEC 62443)

Target Audience

This course is ideal for:

- OT and ICS Security Engineers
- Industrial Control System Operators

- Network and Security Engineers managing critical infrastructure
- SOC Analysts focusing on OT security
- IT/OT convergence teams

Pre-Requisites

Participants should have:

- Basic understanding of networking and cybersecurity fundamentals
- Familiarity with IT security concepts
- Knowledge of industrial processes and OT systems is recommended

Course Content

Module 1: Introduction to OT Security

- Overview of OT systems, ICS, and SCADA
- Differences between IT and OT networks
- OT security landscape and challenges

Module 2: OT Threats and Vulnerabilities

- Common OT attacks and threat actors
- Vulnerability assessment in industrial networks
- Case studies of OT security incidents

Module 3: Network Segmentation and Access Control

- OT network architecture and zoning
- Role-based access control and network segmentation
- Secure remote access for OT systems

Module 4: Device and Endpoint Security

- Securing PLCs, RTUs, and industrial devices
- Patch management and firmware security
- Endpoint monitoring and anomaly detection

Module 5: Monitoring, Detection, and Response

- OT network monitoring tools and techniques
- Incident detection and response strategies
- Threat intelligence for OT environments

Module 6: Compliance, Risk Management, and Best Practices

- OT security standards and frameworks (NIST, IEC 62443)
- Risk assessment and mitigation strategies
- Operational best practices for OT security