Module Synopses

PDC 1 Certificate in Industrial Control Systems and Cybersecurity Operations

Module 1 - Industrial Control Systems (60 hours)

The module covers various components and technologies in Advanced Manufacturing (Industry 4.0). Topic includes networking of Automation equipment using open communication standards to provide connectivity between machines and connectivity to Information Technology services. It includes configuring and programming of PLC system for automation tasks with web based and mobile apps information services. Concepts of secured coding, and condition monitoring with wireless sensors network will also be covered.

Module 2 - Cyber Security Operations (60 hours)

The aim of this module is to introduce the core security concepts and skills needed to monitor, detect, analyse and respond to cybercrime, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes on the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems. The module prepares candidates for Cisco CCNA Cyber Security Operations certification.

PDC 2 Certificate in Industrial Control Systems (ICS) Ethical Hacking and Incident Response

Module 3 - ICS Cyber-Range Essentials (60 hours)

This module aims to teach tools to discover and exploit vulnerabilities in simulated ICS Cyber Range Environment. It will also cover security issues and weaknesses of ICS protocols, different attack surfaces and types of exploits targeted at PLCs. Participants will learn what the best practices for securing ICS are, how to deploy countermeasures to defend against cyber-attacks. Participants will work in groups such as Pentesting and System Hardening, to protect and defend against simulated cyberattacks using tools, techniques learned in this module.

Module 4 - ICS Incident Response and Assessment (60 hours)

This module covers concepts and techniques of performing incident response against identified threats and actors to ensure the safety and reliability of operations in ICS environment. Participants will also learn the essentials of security policy development, risk assessments and security model relevant to an ICS environment. Participants will also work on assigned group projects, such as Breach and Simulated Attacks of OT systems, to come up with incident response plan covering technical and non-technical aspects based on case studies.