Specialist Diploma in Operational Technology Cybersecurity (Network and System Defence)

Module Synopsis

PDC 1 Certificate in Industrial Control Systems and Cybersecurity Operations

Industrial Control Systems

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.

Cybersecurity Operations Fundamentals

This module aims to introduce the core security concepts and skills needed to monitor and detect cybercrime, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure the security and operational readiness of secure networked systems. The module covers topics from the Cisco CCNA CyberOps Associate certification.

PDC 2 Certificate in Network and Operational Technology System Defence

Operational Technology System Defence

This module aims to develop an understanding of the importance of Operational Technology (OT) security, cyber threats, and solutions available for cybersecurity. The module covers OT architecture, OT systems and devices, and the Industrial Internet of Things (IIoT). With the convergence of Information Technology (IT) and OT, participants will be introduced to the NIST Cybersecurity Framework and Purdue model for implementing OT and IIoT security vulnerabilities and defence solutions, including testing and security monitoring.

Network Security Management and AI

The module will expose the participants to network security management solutions that provide a high level of visibility into network behaviour, automate device configuration, enforce global policies, view firewall traffic, generate reports, and provide a single management interface for physical and virtual systems to manage potential threats and risks to an organization’s network security. In addition, participants will also be introduced to Artificial Intelligence (AI) that can assist in mitigating cyber threats and bolster security infrastructure through pattern detection, real-time cybercrime mapping and thorough penetration testing.