

# **Module Synopses**

## **PDC 1 Certificate in Infocomm Security and Defences**

### **Module 1 - Infocomm Security and Network Essentials (45 hours)**

This module introduces students to the fundamental concepts of infocomm security such as identification, authentication, authorisation, integrity and confidentiality. Students will also learn security essentials like network protocols and basic operating system commands.

### **Module 2 - Cyber Defence and Range Exercises (90 hours)**

This module introduces students to tools to discover and exploit vulnerabilities in networks and operating systems. They will be taught the security issues found in software, especially web applications. Security components like firewalls and IDS (Intrusion Detection Systems) will also be introduced as countermeasures to defend against cyber-attacks. Students will have the opportunity to integrate the knowledge and technical skills learned by taking part in scenario-based exercises.

## **PDC2 Certificate in Security Incident Management**

### **Module 3 - Digital Forensics and Investigation (60 hours)**

This module equips students with the fundamental concepts and techniques of computer and mobile forensics. Students will learn to acquire, analyse and present computer and mobile data as evidence.

### **Module 4 - Security Policy and Incident Management (75 hours)**

This module equips students with the fundamental concepts and techniques of Security Information and Event Management (SIEM). Students will also learn the essentials of security policy development, risk assessments and security models.