Cyber Security BSc (Hons) module details

Year one

Block 1: Foundation of Computing and Cyber Security

This module introduces you to the professional context of computer science, software engineering, cyber security, and digital forensics. It introduces mathematical structures that provide a basis for computer science and cyber security to prepare students with the necessary skills in this domain. Students gain skills to learn the concepts of computer science cyber security. In this module the students will learn the mathematical foundation of computing such as logic and boolean algebra, set theory, probability and statistics, relations, functions, and modular arithmetic.

Lecture: 24 hours
Seminar: 48 hours
Self-directed study: 156 hours
Consolidation: 40 hours
Revision: 30 hours
Assessment: 2 hours
Total: 300 hours

Block 2: Endpoint Security

Designed to provide a foundation in computer ethics, computer architecture and operating systems with a specific emphasis on their security. It will introduce the ethical theories affecting information systems, information security, software engineering, computer science and digital forensics. It requires students to develop critical analytical skills in applying ethical theories to technological outcomes regarding information systems, information security, software engineering, computer science and digital forensics.

Learning and teaching activity hours for the module:
Lecture: 36 hours
Practical: 48 hours
Workshop: 10 hours
Self-directed study: 100 hours
Consolidation: 36 hours
Revision: 30 hours
Assessment: 40 hours
Total: 300 hours

DE MONTFORT UNIVERSITY DUBAI

Block 3: Secure Coding

This module covers introduction to secure and object-oriented programming using C++. The programming concepts covered in this module are fundamental in almost any other programming language. Students initially learn about the fundamental problem-solving skills using algorithms and basic programming concepts that enable them to create, edit, compile, execute and test computer programs, then about applying key syntax rules for variables, expressions, statements, arrays, and functions in C++.

This module also covers developing/building trusted and reliable software to meet user's requirements including, e.g., naming conventions, initialisation of variables, variable scope and lifetime, validation of input, bound checking, string manipulation and reliability. Students learn about the latest security standards to understand the best practises for writing a software.

Practical: 48 hours
Lecture / Large Group: 24 hours
Reading - suggested reading is part of seminar work: 50 hours
Reflection: 50 hours
Revision: 40 hours
Consolidation: 88 hours
Total: 300 hours

Block 4: Business Infrastructure and Security

This module covers the theory and practice underpinning the foundations of modern networked information systems. Awareness of these principles and concepts is essential for individuals working in Cyber Security, to allow them to secure the systems that organisations depend upon. Topics introduced allow consideration for the opportunities to secure these systems, and the role these systems play in a wider context.

Learning and teaching activity hours for the module:
Lecture: 24 hours
Seminar: 48 hours
Self-directed study: 156 hours
Consolidation: 40 hours
Revision: 30 hours
Assessment: 2 hours

DE MONTFORT UNIVERSITY DUBAI

Year two

Block 1: Secure Scripting and Business Applications

This module covers the fundamentals of database design and implementation as well as the ethical and legal responsibilities associated with storing data. The module also considers how secure scripting techniques can address unauthorised access to stored data through poor business application design and implementation.

Practical: 60 hours
Lecture / Large Group: 40 hours
Self-directed Study (including coursework report): 99 hours
Reflection: 60 hours
Revision: 40 hours
Assessment: 1 hour
Total: 300 hours

Block 2: Incident Response and Cyber Threat Intelligence

This module covers incident response and cyber threat intelligence principles, industry standards as well as frameworks, tools and techniques. The students will learn about the essential preparations before an incident occurs, incident response life cycle stages, and appropriate approaches to incident handling. Organisational departments dealing with incidents, their structure and functions will be considered. The students will also be able to understand modern security operations.

Student hours per module:
Practical: 56 hours
Lecture / Large Group: 44 hours
Reading: 100 hours
Reflection: 60 hours
Revision: 40 hours

DE MONTFORT UNIVERSITY DUBAI

Block 3: Penetration Testing

This module shows students how to think like a hacker, how to probe systems for exploitable vulnerabilities and to report findings for implementing mitigation strategies. From social engineering and physical attacks to client-side and server-side attacks, students will replicate the same Tactics, Techniques, and Procedures (TTPs) that a malicious hacker would use, whilst being compliant with current ethics, law and regulations. In this module students will learn how to perform reconnaissance on a target, how to identify possible victims and how to enumerate their services, how to gain access, how to escalate an individual's privileges and how to create a final penetration test report.

Lecture: 20 hours
Practical: 60 hours
Self-directed reflection: 20 hours
Self-directed reading: 20 hours
Self-directed online learning: 80 hours
Self-directed revision: 40 hours
Assessment: 60 hours

Block 4: Industrial Cryptography

Cryptography constitutes today a fundamental and ingrained part of the security of all modern communication. Everything from web browsing, email, and telephony, to messaging apps, data storage and video conferencing, is today secured by cryptographic techniques.
This module will introduce the central principles, methods, and definitions of cryptography, as well as presenting some of the most important applications and implementations. Modern cryptography is concerned with an enormous variety of scenarios where the involved parties do not fully trust each other such as internet banking, electronic voting, integrity of data, security of computer networks, and many more.

Learning and teaching activity hours for the module:
Lecture: 24 hours
Seminar: 48 hours
Self-directed study: 137 hours
Consolidation: 40 hours
Revision: 30 hours
Assessment: 21 hours

DE MONTFORT UNIVERSITY DUBAI

Year three

Block 1: Malware and Attacker Techniques

This module provides students with practical skills of investigating malware in accordance with best practice, using industry standard tools and techniques whilst adhering to professional code of ethics and legal requirements. Students learn the fundamentals of assembly language and apply it to malware reverse engineering and malware de-armouring. They will also gain an in-depth understanding of malware behaviour and evasive techniques as well as malware strategies employed by Advanced Persistent Threat (APT) actors.

Learning and teaching activity hours for the module:
Lecture: 28 hours
Practical labs: 42 hours
Self-directed study: 140 hours
Consolidation: 35 hours
Revision: 20 hours
Assessment: 35 hours

Block 2: Cyber Physical Systems Security

Cyber Physical Systems are ubiquitous to the modern way of life, controlling or impacting all Critical National Infrastructure sectors identified by the UK government, such as Water, Power and Telecommunications. Cyber Physical Systems (CPS) integrate physical processes, computing, and communication to monitor and control mission-critical applications.

This module will be delivered in seven-week block mode with the following estimated teaching and learning activity hours:

Lecture: 24 hours
Practical/Lab: 48 hours
Self-directed study: 141 hours
Consolidation: 45 hours
Assessment: 42 hours

Block 3 / 4: Final Project

The project provides students with the opportunity to carry out a significant piece of work that reflects the aims and outcomes of their specific programme. It provides students with the opportunity to demonstrate practical and analytical skills present in their programme of study; to work innovatively and creatively; to synthesise information, ideas, and practices to provide a quality solution, together with an evaluation of that solution. The project should meet some real need in a wider context.

Lecture: 6
Supervisor meetings: 5
Self-study: 289
Optional Modules (choose one):

Block 3 / 4: Cyber Security and Social Responsibility

Cyber Security professionals are often tasked with ensuring an organisation meets legal and regulatory standards when handling data. This module allows for consideration of, and brings awareness to moral and ethical aspects that may be encountered when building computing systems or processing data.

Note that the expected methods of delivery below assumes delivery over two blocks while students take on another module at the same time, such as the final year project.

Lecture: 30 hours
Reading: 45 hours
Self-directed study: 100 hours
Review: 22 hours
Consolidation: 50 hours
Collaborative activity: 50 hours
Assessment: 3 hours

Block 3 / 4: Artificial Intelligence for Cyber Security\

The application of AI algorithms to the domain of cyber security has gained a lot of momentum in the last few years, especially with the proliferation of Deep Neural Network architectures and applications. In this module, the application of AI to cyber security will be examined in detail. Students will be trained on how to collect, pre-process, and analyse cyber security datasets. Students will gain fundamental knowledge about AI algorithms, including statistical machine learning algorithms and deep neural networks, and how such algorithms are applied to cyber security applications. State-of-the-art tools and software libraries will be used to apply taught concepts to train and evaluate different AI models to develop cyber security solutions.
Lecture: 24 hours

Practical/Lab: 56 hours
Assessment: 60 hours
Reading: 100 hours
Reflection: 60 hours

Block 3 / 4: Digital Forensics and Cyber Crime Investigation

This module will guide students through the Digital Forensics Incident Response (DFIR) life cycle in traditional and/or enterprise crime scenes involving digital devices such as computers/laptops/mobile devices/networks and the associated legal and ethical considerations and requirements.
Students will use a combination of proprietary and open-source forensic tools to collect and analyse digital evidence in a forensically sound manner whilst completing the appropriate and necessary paperwork, prior to presenting their findings for a given audience.

Lectures: 24 hours
Staffed Labs: 48 hours
Unstaffed Labs: 24 hours
Self-directed study: 140 hours
Collaboration: 24 hours
Assessment: 40 hours