Programme Specification 2025-26

1.	**Programme title**	MSc Cyber Security and Emerging Threats
2.	**Awarding institution**	Middlesex University
3a	**Teaching institution**	Middlesex University London
3b	**Language of study**	English

4a	**Valid intake dates and mode of study**

Mode of Study	Cohort	Delivery Location	Duration
Full-time (FT)	Semester 1	1 Hendon, 3 Mauritius	1 Years
Part-time (PT)	Semester 1	1 Hendon, 3 Mauritius	2 Years
Full-time (FT)	Semester 1	Hendon	15 Months
Full-time (FT)	Semester 1	Hendon	24 Months

4c	**Delivery method**	On Campus/Blended Learning

5. Professional/Statutory/Regulatory body (if applicable)
N/A

6.	**Apprenticeship Standard** (if applicable)	N/A

7. Final qualification(s) available
Target Award Title(s)
MSc Cyber Security and Emerging Threats
MSc MSc Cyber Security and Emerging Threats with Professional Placement (15 months)
MSc MSc Cyber Security and Emerging Threats with Professional Placement (24 months)
Exit Award Title(s)
PGCert Cyber Security and Emerging Threats
PGDip Cyber Security and Emerging Threats

8. Academic year effective from	2025-26

9. Criteria for admission to the programme

Applicants for the programme should normally have one of the following:
•A second class or higher honours degree in Cybersecurity, Computer Science, or a closely related discipline awarded by a UK university or a qualification deemed equivalent by the University.
•A second class or higher honours degree in Engineering (e.g. Electrical Engineering), Mathematics, or another technical discipline, with relevant work experience in cybersecurity, penetration testing, threat intelligence, or a related field. Usually, applicants will be invited to an interview by the Programme Leader to assess the suitability to join the programme
Recognition of Prior Learning (RPL)
Applicants with significant industry experience or relevant professional certifications may be considered for admission under the Recognition of Prior Learning (RPL) framework. This may also enable exemptions from specific modules upon enrolment.
English Language Requirements
International students whose first language is not English, or who have not been taught in English throughout their academic career, must achieve an IELTS score of 6.5, with a minimum of 6.0 in each component. Equivalent English language qualifications may also be considered.
By implementing these criteria, the programme ensures inclusivity while maintaining the highest academic standards, preparing students for the evolving challenges of cybersecurity.

The University aims to ensure that its admissions processes are fair, open and transparent and aims to admit students who, regardless of their background, demonstrate potential to successfully complete their chosen programme of study where a suitable place exists and where entry criteria are met. The University values diversity and is committed to equality in education and students are selected on the basis of their individual merits, abilities and aptitudes. The University ensures that the operation of admissions processes and application of entry criteria are undertaken in compliance with the Equality Act.

We take a personalised and fair approach to how we make offers. We feel it's important that our applicants continue to aspire to achieving great results and make offers which take into account pieces of information provided to us on the application form.

This includes recognition of prior learning and experience. If you have been working, or you have other learning experience that is relevant to your programme, then we can count this towards your entry requirements and even certain modules once you start studying.

10. Aims of the programme

This programme aims to:
•Develop advanced knowledge of cybersecurity principles, practices, and regulations.
•Equip students with hands-on expertise in penetration testing, secure system design, and risk management, ensuring they are industry ready.
•Explore and apply cutting-edge technologies such as AI, machine learning, and quantum computing to address modern cybersecurity threats such as AI-powered cyber-attacks.
•Prepare students for impactful careers by integrating real-world challenges, ensuring graduates can respond effectively to emerging cyber threats.
Why Choose This Programme?
•Industry-Relevant Curriculum: Designed in collaboration with cybersecurity professionals, ensuring that graduates acquire the skills employers seek.

•Hands-On Learning: Access to specialist labs, simulated cyber-attack scenarios, and penetration testing exercises using industry-grade tools.
•Expert Faculty: Learn from experienced academics and industry practitioners actively engaged in cybersecurity research and consultancy.
•Exclusive Career Opportunities: Benefit from our strong industry links, networking events, and potential employment pathways with leading cybersecurity firms.
•Flexible Learning Pathways: Options for placements, research projects, and professional certifications to enhance employability.
•Emerging Tech Focus: Gain expertise in the latest developments in AI-driven security, quantum computing, and autonomous systems security.
By choosing this programme, students will not only gain world-class knowledge but also have the opportunity to apply it in real-world settings, ensuring they are fully equipped to lead in the cybersecurity industry.

11. Programme learning outcomes

Programme - Knowledge and Understanding

On completion of this programme the successful student will have a knowledge and understanding of:

1. Core concepts of network security principles, operating systems, and programming for modern computing environments.

2. Cybersecurity threats, vulnerabilities, and risk mitigation strategies across various domains.

3. Legal, regulatory, and compliance frameworks relevant to cybersecurity practices.

4. Emerging technologies such as AI/ML and quantum security to solve complex cybersecurity challenges.

Programme - Skills

On completion of this programme the successful student will be able to:

5. Design and implement secure network architectures and systems using modern programming techniques.

6. Select and apply appropriate penetration testing strategies, tools, and techniques to identify vulnerabilities.

7. Critically evaluate and justify their chosen approach, communicate findings through detailed reports, assess associated risks, and recommend mitigation strategies.

8. Develop and synthesize innovative cybersecurity solutions for emerging technologies, including autonomous systems.

9. Critically evaluate and defend cybersecurity policies and incident response strategies based on established frameworks.

12. Teaching/learning methods

• Delivery Approach: , Workshops, hands-on lab sessions, group projects, and online sessions as well as key concept videos
• Inclusive Learning: Research-informed teaching, accessibility considerations, and diverse learning resources are embedded throughout the program.

Approx. number of timetabled hours per week (at each level of study, as appropriate), including on-campus and online hours. FT 12hours, PT 6 hours.

Approx. number of hours of independent study per week (at each level of study, as appropriate). FT 28 hours, PT 14 hours.

Approx. number of hours on placement (including placement, work-based learning or year abroad, as appropriate). FT 3 months (15 months programme) or minimum of 36 weeks (24 months programme), PT N/A.

13. Employability

13a Development of graduate competencies

13b Employability development

Development of graduate competencies

The MSc Cyber Security and Emerging Threats programme is designed to develop advanced competencies that align with Middlesex University's Graduate Competencies at the Postgraduate Level, ensuring graduates are equipped to navigate and lead in the rapidly evolving cybersecurity landscape. Competencies are integrated through theoretical instruction, practical applications, interdisciplinary research, and industry collaborations.

Leadership and Influence
•Competency: Graduates will proactively lead cybersecurity teams, research initiatives, and professional projects, influencing decision-making and policy development.
•How Achieved: Leadership in group projects, engagement in research-led learning, and industry-based challenges in modules such as the Research methods & PG Individual Project and CST4565 (Cybersecurity for Emerging Technologies).

Entrepreneurship (Mindset)
•Competency: Students will develop an entrepreneurial mindset, identifying and addressing complex cybersecurity challenges using interdisciplinary approaches.
•How Achieved: Real-world problem-solving in cybersecurity, integrating insights from AI, quantum computing, and ethical hacking within modules such as CST4552 (Pen Testing) and CST4592 (Cybersecurity Governance and Secure Development).

Curiosity and Learning
•Competency: Graduates will demonstrate intellectual curiosity by exploring emerging cybersecurity threats and solutions, contributing original insights to the field.
•How Achieved: Independent research assignments, self-directed study opportunities, and participation in cybersecurity research initiatives within CST4565 and CST4622 (Operating Systems for Secure Environments).

Communication, Empathy, and Inclusion
•Competency: Students will be able to articulate complex cybersecurity concepts to technical and non-technical stakeholders while fostering an inclusive cybersecurity culture.
•How Achieved: Presentations, technical report writing, and teamwork-based assessments in modules such as CST4552 (Pen testing) and CST4592 (Cybersecurity Governance and Secure

Development).

Collaborative Innovation
•Competency: Graduates will lead and contribute effectively to cybersecurity research and problem-solving teams, ensuring knowledge exchange and critical evaluation.
•How Achieved: Group-based research projects, cybersecurity hackathons, and team-oriented coursework in CST4592.

Resilience and Adaptability
•Competency: Graduates will demonstrate resilience in addressing evolving cyber threats, adapting to new regulations and technological shifts.
•How Achieved: Exposure to real-world cybersecurity case studies, adaptive problem-solving assignments, and industry projects in CST4562 (Network Security Principles and Mechanisms).

Problem Solving and Delivery
•Competency: Students will solve real-world cybersecurity challenges through advanced methodologies and data-driven decision-making.
•How Achieved: Application of AI and quantum technologies in cybersecurity, complex threat modeling exercises, and penetration testing simulations within CST4552 and CST4565.

Technological Agility
•Competency: Graduates will be proficient in the use of cutting-edge cybersecurity tools, AI-driven security analysis, and next-gen digital forensic techniques.
•How Achieved: Hands-on training with cybersecurity platforms, AI integration in security frameworks, and exposure to quantum security methodologies within CST4565 and CST4622.

Integrated Learning Approach
•Practical learning through labs, workshops, and scenario-based cybersecurity assessments.
•Research-informed teaching delivered by academics with industry experience.
•Real-world engagement through guest lectures, cybersecurity industry talks, and applied projects.

This comprehensive development of competencies ensures graduates are career-ready, adaptable, and equipped to lead in the rapidly evolving field of cybersecurity.

Employability development
The programme is designed to ensure career readiness through a combination of practical learning and exposure to real-world challenges. Modules are developed and delivered by academics with significant experience in both industry and research, providing students with insights into current trends and best practices in cybersecurity. The Programme Leader (PL) and Module Leaders (ML) will actively invite guest speakers from industry to run workshops and deliver talks, offering students valuable opportunities to learn from and network with professionals. Hands-on learning is further emphasized through lab-based activities, case studies, and scenario-based assessments, enabling students to develop practical skills directly applicable to professional environments. Additionally, support and embedded workshops on a range of career topics are available from the University's Employability Service.

13c Placement and work experience opportunities (if applicable)

For MSc Cyber Security and Emerging Threats with Professional Placement (15 months) and MSc Cyber Security and Emerging Threats with Professional Placement (24 months) only

As well as the normal programme structure, a programme with a placement is available (via application) for full-time students. Students can choose to apply for either a 3-month or minimum 36 weeks placement duration. Students are responsible for securing their placement through independent applications, with support available from the university's employability service. Suitable placements will typically be an appropriate role in the commercial sector relating to computer science or information systems, such as developer, IT support, or software quality assurance.

13d Future careers / progression

Successful students will be well placed for a range of roles in the professional computing sector, such as pen testing. Graduates will be equipped to pursue roles such as Cybersecurity Analyst, Penetration Tester, Threat Intelligence Specialist, Security Consultant, and roles in AI and quantum security.
The strong research underpinning of the programme provides a platform for further research activity, for example the potential to secure a role in an industry-based research setting or progress to further PhD study.

14. Assessment methods

Students' knowledge, understanding and skills are assessed by:

•Group and individual coursework
•Laboratory tests
•In-class activities
•Final Project
•Viva

15. Programme Structure (level of study, modules, credits and progression requirements)

Structure is indicative for Part-time routes.

Students must take all of the compulsory modules and choose following programme requirements from the optional modules.

Non-compensatable modules are noted below.

Available Pathways

Not Applicable

Year 1

Year 1 Level 7 FT and PT

Part-time students can select any one 30 credits modules and two 15 credits in one academic year followed by one more module (30 credits) and two 15 credits in the next academic year. Below is a suggested model of study.

Code	Type	Module Title	Credits at FHEQ Level
CST4552	Compulsory	Pen Testing 2025-26	30 at Level 7
CST4545	Compulsory	Programming, Systems, and Networks for Modern Computing 2025-26	15 at Level 7
CST4562	Compulsory	Network Security Principles and Mechanisms 2025-26	15 at Level 7
CST4565	Compulsory	Cybersecurity for Emerging Technologies 2025-26	30 at Level 7
CST4592	Compulsory	Cybersecurity Governance and Secure Development 2025-26	15 at Level 7
CST4533	Compulsory	Operating Systems for Secure Environments 2025-26	15 at Level 7
CST4990	Compulsory	Research Methods and Postgraduate Project 2025-26	60 at Level 7
CST4930	Compulsory	Preparing for the Professional Placement 2025-26	0 at Level 7

Year 2

Year 2 Level 7 Hendon FT students with placement option

Year 2 Level 7 Hendon FT students with placement option Placement Module

Code	Type	Module Title	Credits at FHEQ Level

CST4940	Optional	Postgraduate Work Placement 2026-27	0 at Level 7
CST4950	Optional	Postgraduate Work Placement (extended) 2026-27	0 at Level 7

Year 2 Level 7 PT

Part-time students can select any one 30 credits modules and two 15 credits in one academic year followed by one more module (30 credits) and two 15 credits in the next academic year. Below is a suggested model of study.

Code	Type	Module Title	Credits at FHEQ Level
CST4552	Compulsory	Pen Testing 2026-27	30 at Level 7
CST4565	Compulsory	Cybersecurity for Emerging Technologies 2026-27	30 at Level 7
CST4990	Compulsory	Research Methods and Postgraduate Project 2026-27	60 at Level 7

*Please refer to your programme page on the website re availability of option modules

16. Programme-specific support for learning

For more information, please visit:
https://mymdx.mdx.ac.uk/campusm/home#menu
The Department of Computer Science teaching and learning approach aligns with the University's goal to promote learner autonomy and resource-based learning. To enhance the experience of Computer Science students:
Specialist Laboratories and Software:
Students have access to state-of-the-art labs equipped with industry-standard software and hardware. These facilities support areas such as data analysis, machine learning, and data visualisation. Labs are available for both structured teaching sessions and self-directed projects.

Induction and Diagnostic Assessments:
All new Computer Science students participate in an induction programme, which may include early diagnostic testing in numeracy, programming logic, and technical literacy. The University offers one-to-one tutorials and workshops for students needing additional support.
Digital and Networked Facilities:

Students are provided with a personal email account, secure networked storage, and remote access to essential software and systems, enabling effective study and collaboration.
Programme and Module Handbooks:
An electronic version of the programme handbook is posted on My Learning. distributed during enrolment. In addition, Module-specific handbooks and online learning resources covering foundational and advanced computer science topics are also provided.

Library and Support Services:
Extensive library resources, including access to technical books, academic journals, and digital archives, are available to support Computer Science learning. Students can also access personalised advice and guidance on academic and personal matters through the student support services.

Group Tutorials and Continuous Feedback:
Group tutorials are provided for each module, enabling interactive learning and in-depth discussions on all taught modules. Feedback is consistently provided on all formative assessments to facilitate continuous improvement.

Research and Collaboration Opportunities:
The department's research initiatives in fields such as artificial intelligence, machine learning, computational data science, and data visualisation inform teaching. Students may have the chance to collaborate on research projects with faculty members, gaining hands-on experience in cutting-edge developments.

Support for Students with Disabilities:
Middlesex University is committed to supporting students with disabilities. Some practical elements of the Computer Science programme, such as hands-on lab work, may require adaptations. Prospective students are encouraged to visit the campus to discuss their specific needs confidentially. For additional support, contact the Disability Support Service at disability@mdx.ac.uk

17. HECos code(s)	100376: Computer and Information Security

18. Relevant QAA subject benchmark(s)	Computing 2022

19. University Regulations
This programme will run in line with general University Regulations: Policies | Middlesex University This will run in line with the university regulation: https://www.mdx.ac.uk/about-us/policies/

20. Reference points
•Cyber Security Body of Knowledge (CyBOK): •QAA Subject Benchmark Statement Computing (2022) •QAA Master's Degree Characteristics Statement (2020)

•QAA Framework for Higher Education Qualifications (2024)
•Middlesex University Regulations
•Middlesex University Learning and Quality Enhancement Handbook (section 3)
•Middlesex University Graduate Competencies
•Middlesex University Learning Framework Principles for Postgraduate Programmes

21. Other information *(if applicable)*

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if they take full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

Curriculum map for MSc Cyber Security and Emerging Threats
Programme learning outcomes

Knowledge and understanding

A 1	Core concepts of network security principles, operating systems, and programming for modern computing environments.
A 2	Cybersecurity threats, vulnerabilities, and risk mitigation strategies across various domains.
A 3	Legal, regulatory, and compliance frameworks relevant to cybersecurity practices.
A 4	Emerging technologies such as AI/ML and quantum security to solve complex cybersecurity challenges.

Skills

B 1	Design and implement secure network architectures and systems using modern programming techniques.
B 2	Select and apply appropriate penetration testing strategies, tools, and techniques to identify vulnerabilities.
B 3	Critically evaluate and justify their chosen approach, communicate findings through detailed reports, assess associated risks, and recommend mitigation strategies..
B 4	Develop and synthesize innovative cybersecurity solutions for emerging technologies, including autonomous systems.
B 5	Critically evaluate and defend cybersecurity policies and incident response strategies based on established frameworks.

Programme learning outcomes – Highest level achieved by graduates

A1	A2	A3	A4	B1	B2	B3	B4	B5
7	7	7	7	7	7	7	7	7

Mapping by level of study and module

Module Title	**Module Code by Level of study**	A 1	A 2	A 3	A 4	B 1	B 2	B 3	B 4	B 5
Level 7										
Programming, Systems, and Networks for Modern Computing	CST4545	□	□	□		□	□		□	
Network Security Principles and Mechanisms	CST4562		□	□	□	□		□		
Pen Testing	CST4552	□				□		□	□	□
Cybersecurity for Emerging Technologies	CST4565	□	□	□			□			
Cybersecurity Governance and Secure Development	CST4592	□	□		□			□		
Operating Systems for Secure Environments	CST4622		□	□	□		□	□	□	
Research Methods & Postgraduate Project	CST4990	□	□	□	□	□	□	□	□	□