Course Specification

Published Date:	26-Mar-2024
Produced By:	Multi Type Usr Record For All Personnel
Status:	Validated

Core Information

Awarding Body / Institution:	University of Wolverhampton		
School / Institute:	School of Engineering, Computing, and Mathematical Sciences		
Course Code(s):	CS027P01UV CS027P31UV	Full-time Part-time	1 Years 2 Years
UCAS Code:			
Course Title:	MSc Cyber Security		
Hierarchy of Awards:	Master of Science Cyber Security Postgraduate Diploma Cyber Security Postgraduate Certificate Cyber Security University Statement of Credit University Statement of Credit		
Language of Study:	English		
Date of DAG approval:	30/May/2018		
Last Review:	2017/8		
Course Specification valid from:	2017/8		
Course Specification valid to:	2023/4		

Academic Staff

Course Leader:	Oluwafemi Falobi
Head of Department:	Dr Consolee Mbarushimana

Course Information

Location of Delivery:	University of Wolverhampton
Category of Partnership:	Not delivered in partnership
Teaching Institution:	University of Wolverhampton
Open / Closed Course:	This course is open to all suitably qualified candidates.

Entry Requirements:

Entry requirements are subject to regular review. The entry requirements applicable to a particular academic year will be published on the University website (and externally as appropriate e.g. UCAS

A lower second honours degree in Computer Science or equivalent.

A Postgraduate Certificate in Computer Science or a related subject with a minimum of grade 50% in all modules.

Alternatively;

Evidence of industrial certifications in Information security such as CISSP, CEH, BCS will also be considered for suitable candidates with a minimum of 3 years working experience in related industries. An interview process will also be utilised to verify suitability for the course for candidates with non-standard academic backgrounds but with demonstrable industry experience in the field.

International Applicants

Your qualifications need to be deemed equivalent to the above entry requirements.

For further information relating to overseas qualification please use the following link https://www.wlv.ac.uk/international/our-locations/your-country/

Distinctive Features of the Course:

The exponential increase in mobile devices, converged applications and Cloud technologies, initiatives such as Bring your Own device (BYOD) / Choose Your Own Device (CYOD) and the advent of digital information technologies, has increased the proliferation of threats in our vibrant and active cyber-physical-natural environment diluting further its perimeter. Our cyberspace is constantly increasing its size almost linearly to its value recognising cyber security as a global response to the challenges posed by constantly evolving systems which are harder to secure. The MSc Cyber Security seeks to address the increasing demand in Cyber Security related domains in both academic vocational qualifications and projection for an increased shortage of Cyber Security professionals in the industry. The course has been designed by a team of leading experts, researchers and trainers in the field and gives the opportunity to the students to be exposed to cutting edge technologies, tools and techniques in cyber exploitation and defence.

Students also have full access to a dedicated Virtual Security Operations Centre (VSoC) established in close collaboration with the industry in a blended programme that amalgamates Governance, Risk and Compliance (GRC) and technical skills required by Cyber security Professionals. This is one of a few courses in the UK to internally host such a platform available to students as part of their course and personal development in the field of Information security.

Educational Aims of the Course:

The educational aims of this course are:

- To enhance critical understanding and synthesis skills with regards to security processes, techniques and methodologies around cyber security in a blended learning environment, with strong hands-on explication using cutting edge software and hardware. The course will cover cyber defence elements and state-of-the heart in exploitation techniques, threats and security risks in both targeted and multi-stage cyber-attacks in the cyberspace.
- To identify and mitigate security violations across the cyberspace with strong emphasis on Governance, Risk and Compliance (GRC) frameworks and standards; and the importance of automation and orchestration of security operations in highly volatile and sensitive environments in order to develop better and more efficient security controls.
- Be exposed to formalised network security principles and protocols' design and further expand your ability and capabilities in strong system administration and modelling of the threat landscape, underpinned by research informed delivery throughout the programme.
- Be exposed to a wide range of pedagogical approaches in network defence with the ability to design, develop and test innovative solutions to real-life issues governing the security status of systems, people and infrastructures in our modern cyberspace. This will allow students to gain a holistic education that balances technical, management and research skills to perfectly match the profile of Information security professionals.
- The course has been developed with reference to the requirements of Cyber Security Professional Bodies. It aims to produce graduates with subject-specific and transferable knowledge and skills suited to a career in the Cyber Security industry, or other related IT disciplines.

Intakes:

September
January

Major Source of Funding:

Office for Students (OFS)

Tuition Fees:

Tuition fees are reviewed on an annual basis. The fees applicable to a particular academic year will be published on the University website.

Year	Status	Mode	Amount
2021/2	H	31	£3275.00
2022/3	H	Full Time	£7995.00
2022/3	Overseas	Full Time	£14450.00
2022/3	H	31	£3998.00
2023/4	H	Full Time	£8395.00
2023/4	Overseas	Full Time	£15450.00
2023/4	H	31	£4198.00
2024/5	H	Full Time	£8815.00
2024/5	Overseas	Full Time	£15950.00
2024/5	H	31	£4408.00

PSRB:

None

Course Structure:

January (Full-time)

Part time students study alongside full time students. However, they do not study more than 80 credits in each academic calendar year.

Module	Title	Credits	Period	Type
7CS024	Internet of Things Security	20	SEM2	Core
7CS023	Ethical Hacking	20	SEM2	Core
7CS022	Incident Management and Response	20	SEM2	Core
7CS020	MSc Project Cyber Security	60	SEM3	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS022	Incident Management and Response	20	SEM2	Core
7CS023	Ethical Hacking	20	SEM2	Core

January (Full-time)

Part time students study alongside full time students. However, they do not study more than 80 credits in each academic calendar year.

Module	Title	Credits	Period	Type
7CC009	Research Methods in Computing	20	SEM1	Core
7CS018	Information Assurance	20	SEM1	Core
7CS017	Proactive Network Defence	20	SEM1	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS018	Information Assurance	20	SEM1	Core
7CC009	Research Methods in Computing	20	SEM1	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS024	Internet of Things Security	20	SEM2	Core
7CS020	MSc Project Cyber Security	60	SEM3	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS017	Proactive Network Defence	20	SEM1	Core

September (Full-time)

Part time students study alongside full time students. However, they do not study more than 80 credits in each academic calendar year.

Module	Title	Credits	Period	Type
7CC009	Research Methods in Computing	20	SEM1	Core
7CS018	Information Assurance	20	SEM1	Core
7CS017	Proactive Network Defence	20	SEM1	Core
7CS024	Internet of Things Security	20	SEM2	Core
7CS023	Ethical Hacking	20	SEM2	Core
7CS022	Incident Management and Response	20	SEM2	Core
7CS020	MSc Project Cyber Security	60	SEM3	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CC009	Research Methods in Computing	20	SEM1	Core
7CS017	Proactive Network Defence	20	SEM1	Core
7CS022	Incident Management and Response	20	SEM2	Core
7CS023	Ethical Hacking	20	SEM2	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS018	Information Assurance	20	SEM1	Core
7CS024	Internet of Things Security	20	SEM2	Core
7CS020	MSc Project Cyber Security	60	SEM3	Core

Please note: Optional modules might not run every year, the course team will decide on an annual basis which options will be running, based on student demand and academic factors, to create the best learning experience.

Learning, Teaching and Assessment

Academic Regulations Exemption:

None.

Reference Points:

QAA Subject Benchmark Statement Computing, 2016

http://www.qaa.ac.uk/Publications/InformationAndGuidance/Documents/QAA386_Computing.pdf

QAA FHEQ level descriptors (M Level).

Institute of Information Security Professionals (IISP)

ISC2 Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK)

British Computing Society (BCS)

National Cyber Security Centre (NCSC)

Overview of Assessment:

As part of the course approval process, the course learning outcomes were mapped to each of the modules forming the diet of the programme of study. This process confirmed that all course learning outcomes can be met through successful completion of the modules. This mapping applies to the final award as well as to all of the intermediate awards.

Learning Outcomes	Modules
MA01 Demonstrate in-depth understanding and the ability to use modern technologies, techniques and methods in Cyber Exploitation and defence to develop both technical and management controls and solutions against Information security threats.	
MA02 Acquire and establish a systematic technical expertise and knowledge in risk assessment methodologies and frameworks and regulatory and legal requirements and compliance within a given organisational context in Cyber Security.	
MA03 Undertake a technical analysis of complex scientific evidence and argumentation independently of current knowledge in the subject matter and apply this in a range of relevant contexts in the cyber-physical space with regards to security and safety.	
MA04 Flexibly and autonomously apply knowledge in order to undertake a series of activities related to core aspects of security so as to provide innovative and cost-effective solutions adhering to ethical dimensions codes or practice and existing standards.	
MA05 Demonstrate your transferable skills to analyse self and other actions in enabling a wide range of vocational outputs within an organisational context and adhere to legal, social and ethical frameworks in the area of practice.	
MA06 Undertake a substantial independent piece of research work that tackles a complex problem in the area of Cyber Security, using incomplete information and demonstrating your ability to analyse, critically evaluate the scenario and utilize this to develop an appropriate solution.	

Learning Outcomes	Modules
PGCERT01 Demonstrate a systematic understanding of knowledge, and a critical awareness of current problems and/or new insights, much of which is at, or informed by, the forefront of your academic discipline, field of study or area of professional practice with a conceptual understanding that enables the student: (a) to evaluate critically current research and advanced scholarship in the discipline (b) to evaluate methodologies and develop critiques of them and, where appropriate, to propose new hypotheses (c) Flexibly and autonomously apply knowledge as a reflective practitioner using semi-structured approaches.	
PGCERT02 Demonstrate a comprehensive understanding of techniques applicable to your own research or advanced scholarship and ability to continue to advance your knowledge and understanding, and to develop new skills to a high level.	
PGCERT03 Demonstrate originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry are used to create and interpret knowledge in the discipline.	
PGCERT04 Ability to deal with complex issues both systematically and creatively, make sound judgements in the absence of complete data, and communicate your conclusions clearly to specialist and non-specialist audiences.	
PGCERT05 Demonstrate self-direction and originality in tackling and solving problems, and act autonomously in planning and implementing tasks at a professional or equivalent level.	
PGCERT06 Demonstrate the qualities and transferable skills necessary for employment requiring: (a) the exercise of initiative and personal responsibility (b) decision-making in complex and unpredictable situations (c) the independent learning ability required for continuing professional development.	
PGDIP01 Demonstrate a systematic understanding of knowledge, and a critical awareness of current problems and/or new insights, much of which is at, or informed by, the forefront of your academic discipline, field of study or area of professional practice with a conceptual understanding that enables the student: (a) to evaluate critically current research and advanced scholarship in the discipline (b) to evaluate methodologies and develop critiques of them and, where appropriate, to propose new hypotheses.	
PGDIP02 Demonstrate a comprehensive understanding of techniques applicable to your own research or advanced scholarship and ability to continue to advance your knowledge and understanding, and to develop new skills to a high level.	
PGDIP03 Demonstrate originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry are used to create and interpret knowledge in the discipline.	
PGDIP04 Ability to deal with complex issues both systematically and creatively, make sound judgements in the absence of complete data, and communicate your conclusions clearly to specialist and non-specialist audiences.	
PGDIP05 Demonstrate self-direction and originality in tackling and solving problems, and act autonomously in planning and implementing tasks at a professional or equivalent level.	

Learning Outcomes	Modules
PGDIP06 Demonstrate the qualities and transferable skills necessary for employment requiring: (a) the exercise of initiative and personal responsibility (b) decision-making in complex and unpredictable situations (c) the independent learning ability required for continuing professional development.	

Teaching, Learning and Assessment:

You will undertake a wide range of learning activities including;

- Computer based learning
- Supported learning using the University VLE (CANVAS) as a learning tool, for
- information and interactive communications
- Lectures
- Tutorials (smaller group / one-to-one)
- Workshops
- Case studies
- Structured laboratory exercises
- Individual structured assignment-based learning
- Directed study
- Individual or group exercises
- Research project investigations.

Assessment methods will include:

- Written reports
- Essays
- Literature reviews
- Exams
- Presentations.

Students will also have the opportunity to engage into formative assessment throughout the course, especially during exercises in the practical sessions where feedback on progress and performance will be given by their tutors for each of the tasks allocated. The assessment strategy for this course is designed around a holistic evaluation on knowledge and skills acquired with strong emphasis on the requirements for this mode of delivery and diverse skills, background and expectations of the target audience. All assessments used in the course are in perfect alignment with University requirements, regulations and policies. Coursework assignments typically incorporate formative feedback so that students can gain an insight into whether their work is meeting the necessary thresholds and focus on meaningful remarks to improve both their performance and understanding in the subject matter. The assessment strategy has been designed with strong influence by the requirements and needs of the audience in FT/PT mode of delivery for this course.

Assessment Methods:

At the University of Wolverhampton, a variety of modes of assessment will be used to support and test your learning and progress and to help you develop capabilities that are valued beyond your University studies and into your working life. Your course may include a variety of assessment activities:

Written examinations (including online examinations, open and closed book examinations and quizzes)
Coursework (for example, essays, reports, portfolios, project proposals and briefs, CVs, poster presentation)
Practical (for example, oral and video presentations, laboratory work, performances, practical skills assessment)

In the final year of your undergraduate degree, and at the end of your postgraduate degree, you are likely to be expected to write an extended piece of work or research, such as a dissertation or a practice-based piece of research.

Student Support:

General University Support:

University Libraries are the key source of academic information for students. Libraries provide physical library resources (books, journal, DVDs, etc.) and offer a range of study areas to allow students to study in the environment that suit them best: Social areas, quiet and silent areas.

Libraries also provide access to wide range of on-line information sources, including eBooks, eJournals and subject databases.

Libraries also provide students with academic skills support via the Skills for Learning programme. Students on campus can attend workshops or ask for one-to-one help on a range of skills such as academic writing and referencing. Students can access a range of online skills material at: www.wlv.ac.uk/lib/skills

The University Student Support website offers advice on a variety of matters (careers, counselling, Student Union advice, etc.). Students can also access these services by booking appointment with the SU, careers, counselling services, etc.

Course Specific Support:

Students will have access to both departmental and university-wide support during their studies. Students will have access to a personal tutor and may book appointments at any point during the academic year. Newly enrolled students on the course will receive a comprehensive induction in the week prior to the commencement of the academic year. In addition to this, the course co-ordinator or his/her representative will meet you to explain the course structure and other issues relating to your experience at the university. These introductions will give you outlines of your course and units, a description of the ways you will be encouraged to develop your knowledge and skills, and signpost resources and materials to assist the process of your learning and success. You will be allocated a personal tutor when you join the course. This academic will be responsible of monitoring your academic progress throughout the course and will help you with any academic or personal issues that might come up. The personal tutor is your consistent point of contact for support and guidance but will on occasion refer you to other university staff for specific issues.

Employability in the Curriculum:

The course modules have been designed with reference to industry accreditation requirements and will be periodically evaluated against these.

The delivery of the course is strongly underpinned by research informed teaching and access to industry level software and hardware. The course utilises a dedicated VSoC environment for the simulation and emulation of large scale attacks. It is fully integrated with modern tools used for cyber exploitation and security automation processes and exposes students in modern security operations through the development of capabilities in a fully integrated and controlled environment. Students will develop scenarios and exercises linked to the real-life security issues that companies and organisations face at all strategic, tactical and operational levels.

The diverse skillset around management of security as delivered in the course will equip you with a meaningful GRC knowledge and relevant experience to excel your career prospects. This is quite prominent due to the problem recruiters have to get hold of security managers with these skills. Interactive sessions in the form of demos will also be delivered by the teaching staff and guest speakers to further leverage understanding and stimulate attention towards relevant and pragmatic issues in the area.

The unit ‘Research Methodologies and Project Management’ in particular requires you to work in a team so as to apply a current project management methodology that embraces all of these knowledge areas in an integrated way while going through the stages of planning, execution and project control; you will work as

part of a team, take responsibility and make autonomous decisions that impact on the project team performance.

In addition, and somewhat complementary the final project fosters independent and autonomous study: typically derived from your own ideas, in collaboration with a dedicated member of the teaching staff as project supervisor. That gives the ability to initiate discussion and project ideas that enrich the academic context in your studies and provide the foundations for a solid, relevant and strong project delivered at the end of your course.

The course has been designed in close consultation with Information Security industry experts and utilises unique tools and platforms to deliver its core elements, skills and capabilities required in the field.

After the completion of this course graduates are more likely to progress in the following areas:

1. Information Security analysts
2. Penetration Testers
3. Information Systems managers
4. Security architects
5. Intrusion analysts
6. Lead security auditors.