Programme Specification

CSDF-CertHE-2022: Cyber Security

LU Certificate of Higher Education awarded by Lancaster University (FHEQ Level 4)

Programme Status: Approved | Version: 1

Introduction

This programme specification provides a summary of the main features of the Cyber Security programme and includes the learning outcomes that you as a student are expected to have achieved on successful completion of the programme.

Further detailed information related to this programme and the College can be found in the following resources:

- Programme Handbook
- B&FC Admissions Policy
- Work based and placement learning handbook (for foundation degrees)
- Student guide to assessment and feedback

When undertaken as part of a Degree Apprenticeship additional information is available in the following resources:

- The Programme Delivery Plan
- The End Point Assessment Guide
- B&FC Mentor Guide
- B&FC Apprenticeship Strategy

Key Programme Information

Programme Code	CSDF-CertHE-2022
Programme Title	Cyber Security
Teaching Institution	Blackpool and The Fylde College
Professional, Statutory and Regulatory Body (PSRB) Accreditation	None
UCAS Code	TBC
Language of Study	English
Version	1
Approval Status	Approved
Approval Date	06 June 2023
JACS Code	
Programme Leader	Keith Whitehead

Programme Awards

Award	**Award Type**	**Level**	**Awarding Body**
LU Certificate of Higher Education	Level 4 Target Award (120 credits)	Level 4	Lancaster University

Programme Overview

Qualified cyber security professionals are currently in high demand by business, government and law enforcement agencies across the globe. Graduating students from this programme will have gained the fundamental skills and knowledge necessary to quickly adopt the emerging technologies and concepts in this fast changing field, alongside the professional and business skills, techniques and ways of thinking needed to be able to align technical security requirements with business needs.

The Certificate of Higher Education in Cyber Security has been developed in line with recognied industry standards to provide a specific opportunity for you to gain a qualifcation in an increasingly vital subject area. The programme is for those wishing to develop a career as a cyber security professional, or to develop new skill sets that may enable them to consider alternative employment roles within IT services.

The Certificate of Higher Education in Cyber Security programme will provide you with a fundamental understanding of how to protect organisations, networks, IT systems and individuals against cyber-attacks and cyber threats. It will prepare you for the possibility of taking professional qualifications in career pathway, such as Cisco CCNA; Cisco CCNA Security; and CompTIA Security+.

Admission Criteria

Entry Requirements

- Level 3 qualification in a Computing or Digital related discipline
- A levels or relevant Access award (96 UCAS points)
- T levels in Digital related subject – Pass
- English Language and Mathematics GCSEs at grade C/grade 4 or above (or equivalent e.g. Functional Skills at Level 2
- Applicants who can demonstrate a significant amount of work experience in the sector and hold a level 2 vocational qualification in cyber security will be considered on an individual basis

Career Options and Progression Opportunities

A cybersecurity graduate has many career options available in both the public and private sectors. Here are some of the most common career paths for cybersecurity graduates:

1. Security Analyst: This is one of the most common entry-level roles in cyber security. Security analysts monitor computer systems and networks for security breaches, analyze data to identify potential threats, and develop strategies to prevent or mitigate attacks.

2. Security Tester: Security testers look to carry out remote testing of a client's network or on-site testing of infrastructure to expose weaknesses in security. This involves planning, implementation of attacks, and report writing with recommendations.

3. Incident Responder: Incident responders are responsible for responding to security incidents, investigating and analyzing breaches, and developing plans to prevent similar incidents from occurring in the future.

4. Network Security Engineer: Network security engineers design and implement security solutions to protect computer systems, networks, and data. This involves designing security systems, conducting security audits, and developing and testing security protocols.

5. Penetration Tester: Penetration testers are responsible for evaluating the security of computer systems, networks, and applications by attempting to exploit vulnerabilities. This involves conducting simulated attacks to identify weaknesses and recommending solutions to address them.

These are just a few of the many career options available to cyber security graduates. The learning you will complete through this platform will allow you to build further knowledge either in the industry or for further learning and could lead to further opportunities and possibilities including career paths such as network security specialist, cybercrime investigator, security auditor, and more. Ultimately, the right career path for you will depend on your individual skills, interests, and career goals.

Progression

Whilst the Certificate of HE is a standalone qualification students who successfully achieve the targeted Certificate of Higher Education would be able to continue onto the new Computer Science (Cyber Security) foundation degree (subject to validation).

Programme Aims

Aim 1 - To provide an alternative route into HE for those who wish to pursue education relevant to their level of study and ability, which serves as a foundation for further study of cyber security within the digital sector.

Aim 2 - To develop the skills, knowledge and personal/professional confidence that will enable students to identify, generate and access opportunities in the Cyber and Digital Security sector.

Aim 3 - Enable students to work towards developing professional standards in Cyber Security.

Aim 4 - To provide students with opportunities to acquire a number of practical and technical skills in Cyber security.

Programme Learning Outcomes

Level 4

Upon successful completion of this level, students will be able to:

1. Demonstrate knowledge of key cyber security concepts, mechanisms, services and protocols that are used as basic building blocks for engineering security solutions
2. Identify and evaluate trends in cyber-attacks, evolving security threats, the mechanisms for monitoring and detecting them, protection controls for mitigating their risks and approaches for holistic cyber defence.
3. Apply best practices for security management within an enterprise abiding by legal obligations, regulatory requirements, international standards, ethical considerations, good governance, incident response and business continuity plans.
4. Demonstrate knowledge and concepts of cyber security topics such as network security, digital forensics, information assurance, security testing, threat modelling and secure software development.
5. Systematically analyse security threats to information assets of an organisation, propose suitable countermeasures and justify choices using relevant quantitative and qualitative methods for evaluating associated business risk.
6. Present, identify and interpret digital forensic information from a variety of sources such as audit logs, hard disks, operating systems, file systems and web browsers in order to detect breaches of security policy, law or regulations.
7. Utilise network forensic tools for collecting, analysing, and processing electronic evidence through application of sound methodologies.
8. Apply and evaluate appropriate tools to manage threats against software or systems.
9. Demonstrate an ability to collaboratively generate ideas and solutions to problems in a time limited environment, and communicate these effectively through a differentiated approach.

Programme Structure

Module	Level	Credits	%	Category	Description	Length/Word Count	Grading Method
Stage 1							
CSDF 401: Cyber Security Architecture (Mandatory)	4	20	50%	Practical: Presentation	n/a	15	Letter Grade
			50%	Practical: Practical Skills Assessment	n/a	30	Letter Grade
CSDF 402: Threat Intelligence (Mandatory)	4	20	100%	Coursework: Portfolio / e-Portfolio	n/a	4000	Letter Grade
CSDF 403: Legislation (Mandatory)	4	20	70%	Coursework: Report	n/a	2500	Letter Grade
			30%	Written Exam: Formal Written Examination	n/a	90	Letter Grade
CSDF 404: Security by Design (Mandatory)	4	20	40%	Coursework: Essay	n/a	1500	Letter Grade
			60%	Practical: Practical Skills Assessment	n/a	40	Letter Grade
CSDF 405: Cyber Security Management (Mandatory)	4	20	40%	Coursework: Case Study	n/a	1500	Letter Grade
			60%	Practical: Group Presentation	n/a	30	Letter Grade
CSDF 406: Systems and Programming (Mandatory)	4	20	30%	Coursework: Comparative Study	n/a	1000	Letter Grade
			70%	Practical: Group Presentation	n/a	40	Letter Grade

Study Workload

Attendance at the institution is expcected for one day per week, this will enable you to carry out independent research alongside developing theoretical knowledge. For each module there will be a minimum requirement of 152 hours of independent study. This will consist of guided reading activities, online tutorials, seminars and workshops, supported through our online learnign paltform, Canvas, online resources that enable you to study in your own time.

The delivery of contact lectures, seminars, workshops and guest speakers from the Cyber Security sector will form the remaining hours of study. It is essential, in order to be successful, that you engage in additional and wider independent study outside of the designated course contact time in order to develop a broader understanding of Cyber Security and the wider cyber environment. As well as being available digitally through your VLE a calendar of all academic assessments will be provided in your handbook at the start of the year; these involve work based research projects, written reports, and consideration of theory and supporting you to develop your independent study skills.

Programme Delivery: Learning and Teaching

The programme will be delivered at the University campus and in your induction the programme team will highlight the extensive range of learning resources and additional support available to you whilst undertaking your course – these resources range from the cutting edge Cyber Labs, modern networking rooms and access to libraries and study areas to academic support, student wellbeing and support from learning mentors. During your time on the programme you will also get to use the brand new IGLOO immersive pod, which will allow you to learn in a 360 degree immersive digital space.

Whilst lectures, seminars and practical workshops feature strongly in this programme, there are a range of other opportunities available due to the advantages of being taught in small cohorts. This means that real time attack and defence games, penetration testing and wider Cyber Security knowledge can be developed as part of tutor- and student-led activities in the lectures, seminars and through role plays and tabletop scenarios. A regular trip to Lancashire Constabulary’s Hutton HQ (HYDRA room) as well as in person and virtual attendance at Cyber conferences will serve to give you a vocational and experience-based curriculum.

Over the course of the programme, you may get the chance to listen to visiting speakers from the Cyber Security sector as well as from other areas such as finance and e-commerce, law enforcement and community agencies. Our flexible and responsive approach to learning means these events and activities can be built-in to the programme in order enhance sessions where appropriate.

Programme Delivery: Assessment

All assessments on this programme have been designed to support you and are relevant to policing practice. Your assessments with consist of essays, simulations, reports, briefing papers, role plays, oral presentations, case studies, online assessments and open book and multiple choice examinations. Guidance on academic regulations around misconduct, research integrity and ethical research approval will be provided via your programme handbook and also provided on your VLE page. Blackpool & Fylde College current taught regulations can be found here

Programme Delivery: Work Based and Placement Learning

Whilst there is no specific work based placement in this Certificate of Higher Education, employer engagement within the programme is embedded throughout many of the modules. Employers and sector partners within the cyber security sector have supported the design of the curricuum ensuirng that the programem content aligns to the skills and competencies required for specific jobs in the cyber sector. Guest lectures and workshops hosted by sector specialists provide an insight into the skills and competencies required for cyber roles whilst employers may also collaborate with you on assessments, projects and coursework within the programme.

Programme Delivery: Graduate Skill Development

Graduate skills development refers to the process of acquiring and honing the skills, knowledge, and attributes that are necessary to succeed in the workplace and in one's personal life. These skills are typically developed during a degree level program and can include both technical skills related to the international cyber security sector as well as soft skills that are essential in the digital and wider professional sectors.

Graduates from this programme will have also develop a strong foundation in various areas of cybersecurity, including network security, information assurance, digital forensics, and risk management. Specific graduate skills developed by the course also include legal, ethical and regulatory frameworks surrounding cybersecurity and the ability to analyse cyber threats and identify vulnerabilities in systems and networks.

Throughout the programme you will develop a range of soft skills including strong communication and collaboration skills necessary to work effectively with other IT and business professionals to ensure security is integrated into all aspects of an organisation. In addition to these specific methods, soft skills development will also be integrated throughout the programme in various ways. For example, group projects can provide opportunities for students to develop teamwork and communication skills, whilst the creative assessments will help you improve your writing and critical thinking abilities.

Over the course of the programme students will be invited to take part in inter-professional events; providing you with the opportunity to collaborate with other practitioners on a range of applied degree programmes at Blackpool & the Fylde College and Lancaster University which may enhance your employability.

Study Costs: Equipment Requirements

Resources required to study on the programme are largely provided by the College. There may be small costs associated with printing of work and posters over the duration of the course. Students are encouraged to bring their own lap-top device to lectures, seminars and workshops, but access to computer facilities is provided by the college. A one-day conference trip to a venue in the region, including conference fee and transport, typically costs around £60/student, although this will be partially funded by the college and is also subject to discount rates offered by conference organisers for group visits.

Study Costs: Additional Costs

As part of the programme, you are strongly recommended to attend external events, aimed at developing your knowledge, understanding and appreciation of course material, develop practical skills and embed theoretical concepts. There may also be the opportunity to attend Cyber Security conferences involving law enforcement practitioners, policy-makers and academic researchers. Costs may be incurred to cover transport, accommodation and food. Travel for local trips is paid for by the college. Though most of the course material is available online, there may be additional costs to consider, such as printing and photocopying of course material, though students will be given a photocopying allowance to cover this.

You are encouraged to purchase an introductory textbook in Cyber Security in support of your studies.

Related Courses

Related courses delivered at B&FC:

- FdA/BSc(Hons) Network Engineering and Cyber Security
- FdA/BSc (Hons) Computer Science