Cyber Security Technologist Apprenticeship

The primary role of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people.

Level: 4

Duration: 24 months

Campus: Aireville Campus

Overview

This involves working to achieve the required security outcomes, in a legal and regulatory context, in all parts of the economy. Individuals will develop and apply practical knowledge of information security to deliver solutions that fulfil an organisation’s requirements.

This Apprenticeship is recognised for entry to both IISP and BCS Associate Membership and for entry onto the Register of IT Technicians confirming SFIA Level 3 professional competence. Those completing the Apprenticeship are eligible to apply for registration.

Training Delivered	Duration	Method Of Delivery
Qufaro CyberEPQ	E-Learning – 5 Days	37.5 hours
CompTIA Network+	Face to Face – 5 Days	37.5 hours
CompTIA Security+	Face to Face – 5 Days	37.5 hours

Python Programming – 2 Days 15 hours

CompTIA Cyber Security Analyst – 5 Days 37.5 hours

CompTIA Cybersecurity Advanced Practitioner+ – 5 Days 37.5 hours

Modules

TECHNICAL COMPETENCIES

Threats, hazards, risks and intelligence

- Discover (through a mix of research and practical exploration) vulnerabilities in a system

- Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate use of relevant external sources of threat intelligence or advice (e.g. CERT UK). Combine different sources to create an enriched view.

- Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP)

- Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.

Developing and using a security case

- Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.

- Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).

Organisational context

- Identify and follow organisational policies and standards for information and cyber security.

- Operate according to service level agreements or employer defined performance targets. Future Trends

- Investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for your business, with supporting reasoning.

SKILLS, ATTITUDES & BEHAVIOURS

- Logical and creative thinking skills

- Analytical and problem-solving skills

- Ability to work independently and to take responsibility

- Can use own initiative

- A thorough and organised approach

- Ability to work with a range of internal and external people

- Ability to communicate effectively in a variety of situations

- Maintain a productive, professional and secure working environment

KNOWLEDGE & UNDERSTANDING

- Why cybersecurity matters – the importance of business and society

- -Basic theory – concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard. Also how these relate to each other and lead to risk and harm

- Security assurance – concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods)

- How to build a security case – deriving security objectives with reasoned justification in a representative business scenario

- Cybersecurity concepts applied to ICT infrastructure – can describe the fundamental building blocks and typical architectures and identify some common vulnerabilities in networks and systems.

- Attack techniques and sources of threat – can describe the main types of common attack techniques; also the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat.

- Cyber defence – describe ways to defend against attack techniques

- Relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant features of UK and international law

- The existing threat landscape – can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence

- Threat trends – can describe the significance of identified trends in cybersecurity and understand the value and risk of this analysis

MODULES ON THE COURSE

- Cyber Security Introduction

- Network and Digital Communications Theory

- Security Case Development and Design Good Practice

- Security Technology Building Blocks

- Employment of Cryptography

Entry Requirements

Individual employers will set the selection criteria, but this is likely to include

- A Levels, relevant Level 3 Apprenticeship, or other relevant qualifications

- relevant experience and/or an aptitude test with a focus on functional Maths.

English and Maths Level 2 will need to be achieved, if not already, prior to taking the end-point assessment.

Career Progression

Typical job roles could include: Cyber Operations Manager, Security Architect, Security Analyst, Risk Analyst, Intelligence Researcher, Security Sales Engineer, Cyber Security Specialist, Information Security Analyst, Governance & Compliance Analyst, Information Security Assurance & Threat Analyst, Forensics & Incident Response Analyst, Security Engineer, Information Security Auditor, Security Administrator, Information Security Officer

Equipment Info

Struggling to find an employer – don't worry!

Join our Apprenticeship Access Academy and join a full-time course until you find one. We'll even give you the heads up when a suitable vacancy comes up. Plus, we will support you to improve your employability skills.

Want to know more? Speak to the Apprenticeship Team now on 01756 693 681 and we will do our best to get you started in your dream job.