REGISTER YOUR INTEREST FOR MORE INFORMATION.
VISIT OUR WEBSITE OR CONTACT OUR TEAM.

BIT TRAINING
Powered by the BIT GROUP

W thinkbittraining.co.uk T 01752 724000 E sales@thinkbittraining.co.uk

TRAINING

LEVEL 4 APPRENTICESHIP

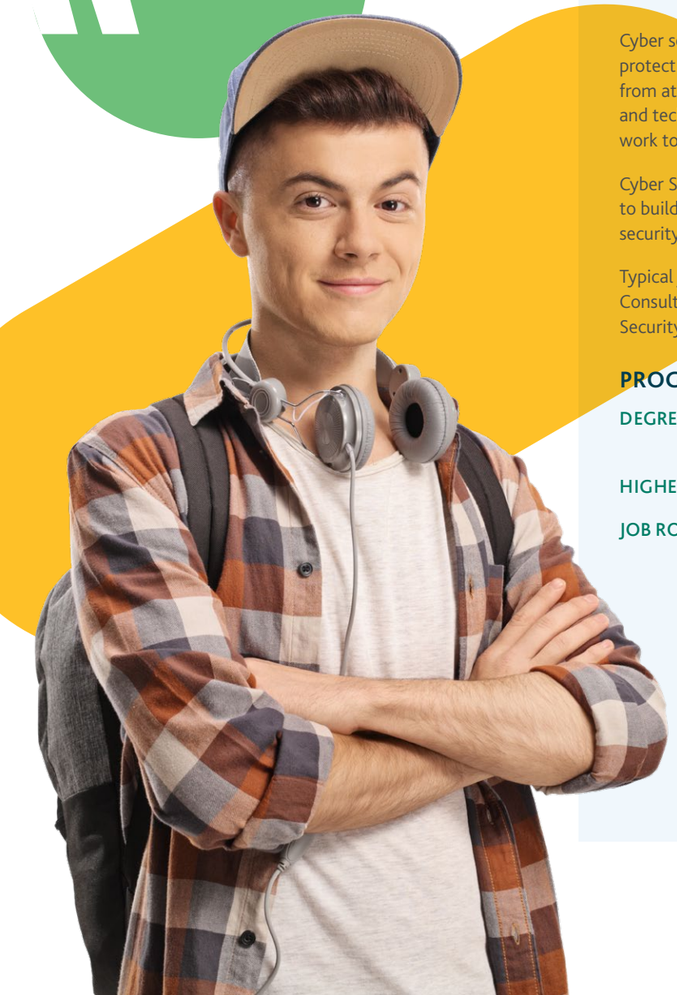
BIT Training – CompTIA Cyber Engineer

STANDARD: CYBER SECURITY TECHNOLOGIST LEVEL 4 (CYBER ENGINEER PATHWAY)

BIT Training – CompTIA Cyber Engineer

STANDARD: CYBER SECURITY TECHNOLOGIST LEVEL 4 (CYBER ENGINEER PATHWAY)

CYBER SECURITY TECHNOLOGISTS PROTECT ORGANISATIONS, SYSTEMS, INFORMATION, PERSONAL DATA AND PEOPLE FROM ATTACKS AND UNAUTHORISED ACCESS.



LENGTH OF PROGRAMME: 24 Months in Learning + 4 Months EPA (28 Months Total)

PROGRAMME COST: £18,000*

DELIVERY METHOD: Remote/Hybrid Delivery

Cyber security Technologists apply an understanding of cyber security to protect organisations, systems, information, personal data and people from attacks and unauthorised access. They understand security concepts and technology and how to mitigates risks arising from threats. They work to achieve cyber security outcomes in a legal and regulatory context.

Cyber Security Engineers are technology focused. Their primary focus is to build and test secure networks or security products with a focus on the security aspects of the design.

Typical job roles include: Cyber Security Engineer, Cyber Security Consultant, Cyber Security Architect, Cyber Security Analyst, Cyber Security Specialist, IT Security Technician, Embedded Engineer.

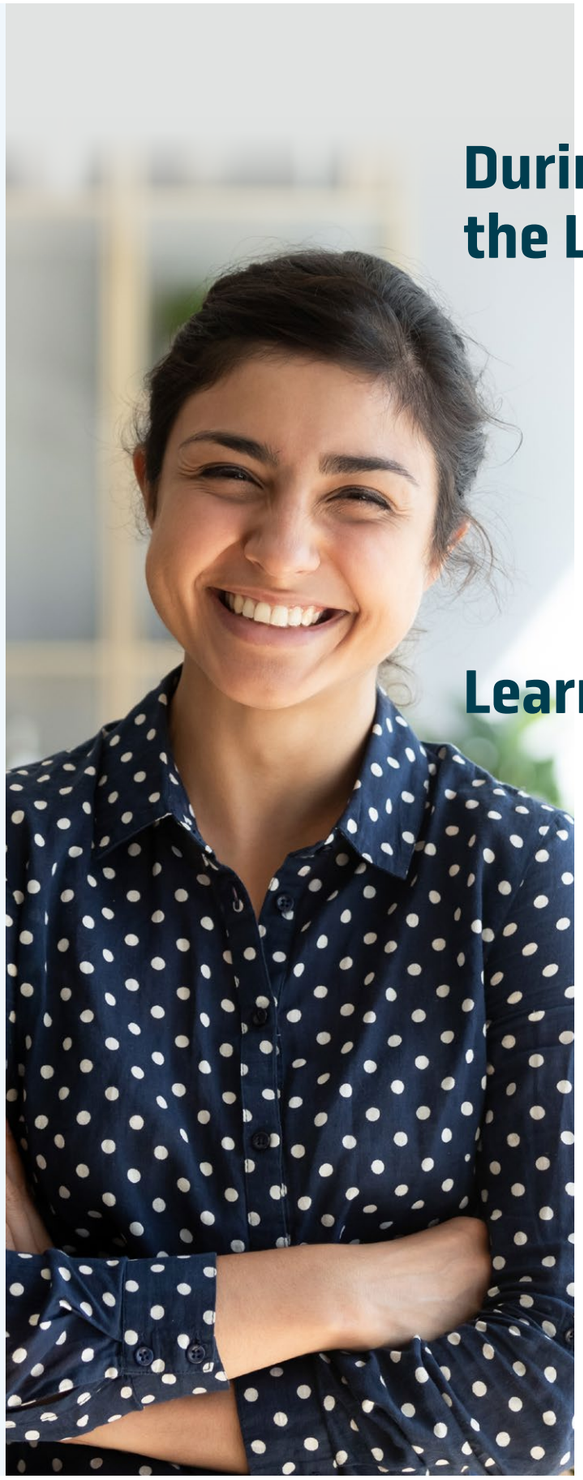
PROGRESSION ROUTES

DEGREE APPRENTICESHIPS: L6 Cyber Security Technical Professional (with integrated degree)

HIGHER EDUCATION: University

JOB ROLES: Cyber Risk Manager; Cyber Risk Analyst; Cyber Research Analyst; Cyber Incident Manager; Cyber Security Engineer; Cyber Security Design Engineer

*Programme costs are 95-100% government funded



During the Programme, the Learner will Complete

TECHNICAL DELIVERY

- CertNexus Cybersec First Responder (CFR)
- CompTIA CySA+
- ITIL® 4 Foundation
- CompTIA CASP+
- 2-day Wargames Activity
- Try Hack Me Academy (BIT Training Cyber Engineer L4 Pathway)
- A comprehensive portfolio of evidence showing their knowledge, skills and competency as a Cyber Security Engineer

Learning Commitment

LEARNER PORTFOLIO

- 1 half day training at the start of each module plus monthly support sessions from their tutor
- 1-2 days self-study each month planning, completing and evidencing portfolio evidence projects

INDUSTRY CERTIFICATIONS

- 2 Training days per month
- Self-study through CompTIA's CertMaster Learn platform
- Free Exam Voucher for all CompTIA Exams

FUNCTIONAL SKILLS

- Maths Level 2*
- English Level 2*

*Proof of GCSE grade C/4 or above or equivalent qualifications will proxy apprentices from sitting functional skills.

Core Duties

Our learning modules holistically allow apprentices to demonstrate competency across the following core duties.

DUTY 1 Identify cyber vulnerabilities in a system to ensure security is maintained.

DUTY 2 Identify security threats and hazards to a system, service or processes to inform risk assessments and design of security features.

DUTY 3 Research and investigate attack techniques and recommend ways to defend against them.

DUTY 4 Support cyber security risk assessments, cyber security audits and cyber security incident management.

DUTY 5 Develop security designs with design justification to meet the defined cyber security parameters.

DUTY 6 Configure, deploy and use computer, digital network and cyber security technology.

DUTY 7 Develop program code or scripts for a computer or other digital technology for example an industrial control system.

DUTY 8 Write reports, give verbal reports and presentations in the context of the cyber security role.

DUTY 9 Manage cyber security operations processes in accordance with organisational policies and standards and business requirements.

DUTY 10 Participate in cyber war gaming and simulations (technical & non-technical) for example to better understand cyber-attack and defence, rehearse responses, test and evaluate cyber security techniques.

DUTY 11 Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.

DUTY 12 Work from a given design requirement to design, build and test digital networks.

DUTY 13 Analyse security requirements and develop a security case taking account of all applicable laws and regulations.

DUTY 14 Implement structured and reasoned security controls in a digital system in accordance with a security case.

DUTY 15 Prevent security breaches using a variety of tools techniques and processes.

OUR LEARNING MODULES HOLISTICALLY ALLOW APPRENTICES TO DEMONSTRATE COMPETENCY ACROSS A WIDE RANGE OF CORE DUTIES.

Modules in Detail

MODULE 1: Cyber security concepts & its importance to business and society

Apprentices will demonstrate they understand and can evaluate core cyber security and security assurance concepts and are able to apply them effectively in their organisation. They will also be able to critically evaluate these concepts to explain how they bring benefits exploring the interrelation of risk and harm.

MODULE 2: Rationale for security objectives

Apprentices will produce evidence to show how they have analysed simple security cases without supervision including the security objectives, threats, and for identified attack techniques identify mitigation or security controls that could include technical, implementation, policy, or process.

MODULE 3: Ethical principles, codes of practice, law & regulation

Apprentices will demonstrate they can competently explain the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. They will also demonstrate they understand the ethical principles and codes good practice of cyber security professional bodies and show how they have demonstrated the ethical responsibilities of a cyber security professional.

MODULE 4: Preventing security breaches & continuous improvement

The apprentice will show how they have reviewed the employers cyber security posture and made recommendations for improvement in relation to future trends in technology and threats reflecting on what the implications are for the organisation/ business. They will demonstrate how they have competently evaluated and used tools, techniques and processes to prevent a breach to digital system security.

MODULE 5: Following organisations policies & processes

Explains life cycle and service management practices with reference to an established standard at foundation level.

Apprentices will demonstrate they can Identify their organisations policies and standards for information and cyber security and are able to operate according to and follow their service level agreements or other defined performance targets.

MODULE 6: Operation of security management systems & incident response

The apprentice will produce evidence that shows how they advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.

They will also show they understand how a security management system works, including how governance, organisational structure, roles, policies, standards, guidelines combine effectively to achieve the intended security outcomes.

thinkbittraining.co.uk | 01752 724000

End Point Assessment (EPA)

EPA takes place over a period of four months once all learning is complete.

At the end of the learning period, the apprentice, employer and coach will meet to agree the apprentice is able to demonstrate all the duties, and to progress the apprentice through gateway to their EPA period.

EPA REQUIREMENTS:

EPA KNOWLEDGE EXAM 40 question multiple choice exam (60 minutes duration).

EPA PROJECT The apprentice will complete a 6-week, 2000 word, work based project with an agreed title designed to showcase their abilities as a Cyber Security Engineer. The project title will be agreed at the gateway point.

EPA SCENARIOS The apprentice will complete four practical scenarios in a controlled environment on the following topics:

- Attack & threat research
- Risk assessment
- Set up & configure a system with security features
- Computer programme & script writing

PROFESSIONAL DISCUSSION The apprentice will complete a professional discussion lasting 90 minutes during which the Endpoint Assessor will discuss the apprentices learning and work experiences on programme and allow them to showcase their competency across all the apprenticeship duties. The structure of the professional discussion will be based on the portfolio of evidence submitted by the apprentice at gateway.

DELIVERY PARTNERS

CERTNEXUS CompTIA bcs The Chartered Institute for IT Accredited Training Partner

LEVEL 4 APPRENTICESHIP

BIT Training – CompTIA Cyber Engineer Timeline

MONTH 1
Induction

MONTH 2-5
Module 1

CYBER SECURITY CONCEPTS & ITS IMPORTANCE TO BUSINESS AND SOCIETY
CertNexus Cybersec First Responder (CFR) | 10 Days

MONTH 6-8
Module 2 & 3

RATIONALE FOR SECURITY OBJECTIVES
CompTIA CySA+ | 5 Days

MONTH 9-12
Module 3

ETHICAL PRINCIPLES, CODES OF PRACTICE, LAW & REGULATION
CompTIA CySA+ | 5 Days

Midway Portfolio Review

MONTH 13-15
Module 4

PREVENTING SECURITY BREACHES & CONTINUOUS IMPROVEMENT
ITIL® 4 Foundation | 2 Days

MONTH 16-18
Module 5

FOLLOWING ORGANISATIONS POLICIES & PROCESSES
CompTIA CASP+ | 4 Days

MONTH 19-22
Module 6

OPERATION OF SECURITY MANAGEMENT SYSTEMS & INCIDENT RESPONSE
CompTIA CASP+ | 4 Days

MONTH 22
Portfolio Review

PORTFOLIO REVIEW
CompTIA CASP+ | 2 Days
CompTIA CASP+ Certification Achieved

MONTH 23
Project Preparation

WARGAMES ACTIVITY
(2 Day Workshop)

MONTH 24
Endpoint Preparation

EPA SCENARIO & PROFESSIONAL DISCUSSION PREPARATION
EPA Knowledge Exam Preparation
(4 Day Workshop)

Gateway

MONTH 25-28
Endpoint Assessment - EPA Knowledge Exam EPA Project | EPA Scenarios | EPA Professional Discussion based on Portfolio