



TRAINING

LEVEL 3 APPRENTICESHIP

BIT Training - CompTIA Cyber Security Technician

STANDARD: CYBER SECURITY TECHNICIAN LEVEL 3

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





BIT Training – CompTIA Cyber Security Technician

STANDARD: CYBER SECURITY TECHNICIAN LEVEL 3

CYBER SECURITY TECHNICIANS PROVIDE 1ST LINE CYBER SECURITY SUPPORT, MONITORING AND DETECTING POTENTIAL CYBER SECURITY THREATS.

LENGTH OF PROGRAMME: 18 Months in Learning + 3 months EPA (21 months total)
PROGRAMME COST: £11,000
DELIVERY METHOD: Remote/Hybrid Delivery

Typical job roles include: Access Control Administrator, Cyber Security Administrator, Incident Response Technician, Junior Information Security Analyst, Junior Penetration Tester, Junior Security Analyst, Junior Security Operations Centre (SOC) Analyst, Junior Threat and Risk Analyst.

Cyber Security Technicians provide 1st line cyber security support, monitoring and detecting potential cyber security threats and escalating them as necessary. Typically working in a SOC (or similar) environment you will conduct specific cyber security tasks under supervision including patching software, implementing access control, configuring firewalls, SIEM and protection tools. They will proactively support the organisation by deliver the security culture of an organisation, educating end users about Cyber threats.

PROGRESSION ROUTES

HIGHER APPRENTICESHIPS: L4 Cyber Security Technician Apprenticeship

HIGHER EDUCATION: L4 HTQ Qualifications, University

JOB ROLES: Cyber Operations Manager, Cyber Risk Analyst, Intelligence Researcher, Security Analyst, Security Architect

During the Programme, the Learner will Complete

TECHNICAL DELIVERY

- APMG – Information Security Analyst Foundation
- CompTIA Network+
- CompTIA Security+
- 2-day Wargames Activity
- Try Hack Me Academy (BIT Training CST L3 Pathway)
- A comprehensive portfolio of evidence showing their Knowledge, Skills and Competency as a Cyber Security Technician

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 Apply procedures and controls to maintain security and control of an organisation.

DUTY 2 Contribute to the production and development of security culture across an organisation including assisting with the promotion of cyber security awareness programmes, monitoring the effectiveness of cyber security awareness programmes, promoting an effective cyber security culture.

DUTY 3 Process cyber security helpdesk requests ensuring confidentiality, integrity and availability of digital information, meeting relevant legal and regulatory requirements for example access control requests.

DUTY 4 Conduct the installation and maintenance of technical security controls in accordance with relevant procedures and standards.

DUTY 5 Monitor, identify, report and escalate information security incidents and events in accordance with relevant procedures and standards.

DUTY 6 Administer cryptographic and certificate management activities in accordance with relevant procedures and standards.

DUTY 7 Conduct regular review of access rights to digital information assets in accordance with relevant procedures and standards.

DUTY 8 Maintain an asset register of controlled environments in accordance with relevant policies, procedures and standards.

DUTY 9 Assist with backup and recovery processes in accordance with relevant policies, procedures and standards.

DUTY 10 Contribute to documenting the scope and evaluating the results of vulnerability assessments in accordance with management requirements.

DUTY 11 Contribute to risk assessments and escalate where appropriate in accordance with relevant procedures and standards.

DUTY 12 Contribute to routine threat intelligence gathering tasks.

DUTY 13 Document incident and event information and incident, exception and management reports in accordance with relevant policies, procedures and standards.

DUTY 14 Contribute towards the production and review of cyber security policies, procedures, standards and guidelines drawing on their experience of applying policies for example - acceptable use, incident management, patching, anti-virus, bring your own device (BYOD), access control, social media, password, data handling and data classification, information technology asset disposal.

DUTY 15 Monitor cyber security compliance and provide relevant data to auditors if required by the auditor.

DUTY 16 Collaborate with people both internally and externally to support secure and uninterrupted business operations of an organisation.

DUTY 17 Practice continuous self-learning to keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.

DUTY 18 Monitor and detect potential security threats and escalate in accordance with relevant procedures and standards.



Modules in Detail

MODULE 1: Application of information security policies & procedures

Apprentices will demonstrate that they understand their organisations information security policies as well as cyber security policies, procedures and guidelines and will demonstrate how they apply these policies in their role. They will provide evidence of how they manage tasks in line with polices and escalate tasks where appropriate. Apprentices will demonstrate they can competently and effectively complete compliance checks and support cyber security audits. They will show understanding of the principles behind compliance and monitoring and be able to collate and report on the audit outcomes.

MODULE 2: Cyber security awareness and culture

Apprentices will show understanding of their organisations cyber security culture and be actively involved in monitoring cyber security awareness programmes including contributing to development and implementation of these programmes recommending improvements as appropriate.

MODULE 3: Maintaining professional knowledge of cyber security developments

Apprentices will show how they keep up to date with changes in the cyber security industry. They will review and evaluate their own development needs through SWOT skills scans, SWOT analysis and personal development plans as well as feedback from their employer. They will be able to show how changes or developments in the organisation impact on them and on their job role.

MODULE 4: Information security governance practice

Apprentices will demonstrate competence and understanding of their organisations Information Security Management System and understand the different components involved. They will demonstrate ability to report effectively on the compliance and resilience of the business based on its outputs. They will apply this knowledge alongside the principles of organisational governance to support and plan disaster prevention and recovery methods.



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

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:

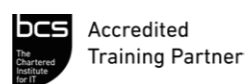
EPA KNOWLEDGE EXAM 40 question multiple choice exam (60 minutes duration).

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

- Implementing Cyber Controls
- Vulnerability Management
- Incident Management
- Risk Management

PROFESSIONAL DISCUSSION The apprentice will complete a professional discussion lasting 60 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



LEVEL 3 APPRENTICESHIP

BIT Training - CompTIA Cyber Security Technician Timeline

