LearnTech

★★★★ Excellent Employer reviews ★★★★ Excellent Apprentice reviews

97.9% Pass Rate

Official ESFA reviews & pass rates data from the Gov.uk service.

Level 4 - 21 months + EPA

Cyber Security Engineer

There is nothing standard about the new apprenticeship Standards!

Following the 2019 - 2021 digital skills review, modern apprenticeships have once again taken a leap forward to provide better vocational training for apprentices and greater benefit to employers. The perfect solution for new career starts, professional upskilling or changes in career direction.

Programme Overview:

A Cyber Security Engineer is a highly technology focused role. They will typically design, build and test secure networks, security products or systems with a particular focus on the security aspects embedded in the design.

Who is it for?

Typical job titles include:

- Cyber Security Engineer
- Cyber Security Consultant
- Cyber Security Architect
- Cyber Security Analyst
- Cyber Security Specialist
- IT Security Technician

Job role eligibility (known as Competency Role Map):

The job role must contain opportunity for an apprentice to practice the content set out in the Level Cyber Security Technologist apprenticeship Standard (Engineer pathway), in order to achieve vocational competency.

Apprentices must have the opportunity to practice the knowledge taught in training sessions in order to convert new knowledge in to sustainable skills applied in the workplace. Where required, we can work with employers to ensure the job role meets the essential criteria.

Entry Requirements:

Entry requirements exist for all funded Further Education programmes. These ensure the value, gain and success of the programme. LearnTech will conduct the processes with employers and prospective apprentices to determine correct funding eligibility.

Initial Assessment of existing knowledge and skills:

A candidate must stand to gain significant knowledge and skills from the programme. If the apprenticeship is too advanced, or if they already know a significant amount of the knowledge and skills the apprenticeship would provide, then they may not be eligible for the funding.

LearnTech will review existing qualifications, knowledge and skills to determine if the prospective apprentice will benefit from the proposed apprenticeship such that it meets the funding criteria. In most instances this is straightforward, however in some instances funding is adjusted in order to fund only the parts of an apprenticeship that would be relevant. LearnTech provides the assessment for these scenarios.

The Level 4 Cyber Security programme is highly technical, so whilst employers can select their own entry criteria, they should include; at least 5 GCSEs at grade 4 or above, including English and maths. English and maths can be included in the apprenticeship, if required.

In many cases, this type of apprenticeship can demand a higher capability of English and maths than is taught at GCSE or A-Level. For example, advanced report writing, budgeting, complex structured explanations and/or advanced formulae and statistics. LearnTech will provide both functional and advanced English and maths diagnostics and teaching to ensure each apprentice is fully supported in these areas.

If you have any questions about this apprenticeship Standard or would like to book an information session, please contact our team: info@learn-tech.co.uk or +44(0)330 380 0249

Level 4 - 21 months + EPA

Cyber Security Engineer

LearnTech

Live virtual Delivery Model:

Our employer-designed delivery model has been developed over time using extensive employer feedback. The core aims are highly effective training for apprentices and as much flexibility as possible for employers.

The only weekly fixed element of training is a 1.5-2 hour training session, with the remaining learning being agreed between the employer and apprentice around workload and responsibilities.

The live classrooms are held via Microsoft Teams. This software provides a full suite of educational tools, including everything you would find in a conventional classroom and more e.g. live open interactions, private breakout rooms, notes, questions, and interactive illustration boards. These sessions are supported with practical labs, together with numerous other tools, selected specifically for their effectiveness in the virtual environment.

Whilst maximum flexibility is offered, if an employer prefers a day-release arrangement, it can be agreed that an entire day is set aside for the training.

All other requirements, including monthly one-to-one mentoring sessions, are arranged between the apprentice and their dedicated skills mentor. Quarterly progress reviews are arranged conveniently between the apprentice, their manager and their mentor.

Programme Structure:

Apprentices are taught principles, techniques and technologies. The education incorporates knowledge, skills and behaviours, as well as self-management and an objective led approach.

Technical Competencies:

- Identify cyber vulnerabilities to ensure security is maintained
- Identify security threats and hazards, service or processes to inform risk assessments and design of security features
- Research and investigate attack techniques and recommend ways to defend against them
- Support cyber security risk assessments, audits and incident management
- Develop security designs with design justification to meet the defined cyber security parameters
- Configure, deploy and use computer, digital network and cyber security technology
- Develop program code or scripts for a computer or other digital technology for example an industrial control system
- Write reports, give verbal reports and presentations in the context of the cyber security role
- Manage cyber security operations processes in accordance with organisational policies, standards and business requirements
- 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
- Keep up-to-date with industry trends and developments to enhance relevant skills, taking responsibility for own professional development

Programme Duration:

This apprenticeship is delivered over 21 months for full-time employees. For part-time employees, the term is extended depending on contracted hours.

End Point Assessment (EPA):

An allowance of three months is required for the EPA process, which begins once all the training is completed.

Successful apprentices will obtain a Pass, Merit or Distinction grade. The grade is determined by the EPA process. Like almost all examinations, a mock will take place before the final assessment.

Once all components of the apprenticeship have been achieved, including the mock, a final review is conducted to ensure everything has been covered, this is called gateway. The apprentice will then undergo their EPA.

The EPA for this programme consists of:

1. **Portfolio of Evidence demonstrating work on 6-8 projects covering all the criteria**
2. **A project report**
3. **Knowledge test**
4. **Scenario demonstration with questioning**
5. **A structured interview with the assessors exploring the project, portfolio of evidence and employer reference**

If you have any questions about this apprenticeship Standard or would like to book an information session, please contact our team: info@learn-tech.co.uk or +44(0)330 380 0249

Level 4 - 21 months + EPA
Cyber Security Engineer

LearnTech

Work from a given design requirement to design, build and test digital networks:

- Networking: OSI and TCP/IP models, data, protocols and how they relate to each other. Main routing protocols; main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking
- Functions and features of at least three Operating Systems (OS) and their security functions and associated security features
- Functions and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security
- Programming or scripting languages

Analyse security requirements and develop a security case taking account of all applicable laws and regulations:

- Cyber security concepts. Why cyber security matters to business and society. Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods
- Applicability and how to apply the appropriate law, regulations and standards specifically relevant to cyber security. To include laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation), use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions
- Analysis of employer or customer requirements to derive security objectives and taking account of the threats and overall context, to develop security cases which set out proposed security measures with reasoned justification

Implement structured and reasoned security controls in a digital system in accordance with a security case:

- Common security architectures and methodologies, reputable security architectures that incorporate hardware and software components. Uses cyber security technology components in digital systems to provide security functionality including use of hardware and software to implement security controls
- Basic terminology and concepts of cryptography, common cryptography techniques, effective key management and the main techniques used for legal, regulatory and export issues specific to cryptography
- Security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes

Prevent security breaches using a variety of tools techniques and processes:

- Main types of common attack techniques, the role of human behaviour, including the significance of the 'insider threat'. How attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards
- The significance of trends in cyber security threats. Performing risk analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment
- Ethical principles and codes of good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional

If you have any questions about this apprenticeship Standard or would like to book an information session, please contact our team: info@learn-tech.co.uk or +44(0)330 380 0249

Level 4 - 21 months + EPA
Cyber Security Engineer

LearnTech

Behavioural development embedded:

- Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions
- Analytical - Working with data effectively to see patterns, trends and draw meaningful conclusions
- Works independently and takes responsibility. For example, works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges
- Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their remit
- Thorough & organised. For example, uses their time effectively to complete work to schedule and takes responsibility for managing their own workload and time
- Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy
- Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences
- Maintains a productive, professional and secure working environment
- Creative - Taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges
- Problem Solving - Identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence

The designated mentor will support the employer and apprentice throughout the programme as a single point of contact for questions and queries. This includes additional support for portfolio and project preparation, along with any advice and guidance needed.

Professional Membership:

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.

Next steps:

To configure an ideal apprenticeship we will meet with you virtually to discuss your requirements, present the options and collaborate to determine the best apprenticeships to meet your needs. We will provide ongoing support including:

- Recruitment of candidates
- Quality assured Information Advice and Guidance
- Updates and information on legislation and funding
- Support and guidance for apprentice and employer throughout the apprenticeship
- Access to a comprehensive suite of resources and support material via OneFile
- Industry specialist qualified trainers and mentors

If you have any questions about this apprenticeship Standard or would like to book an information session, please contact our team: info@learn-tech.co.uk or +44(0)330 380 0249