LEVEL 3 CYBER SECURITY TECHNICIAN

There is nothing standard about the new apprenticeship Standards!

Following the 2019 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 fantastic entry point in to the world of Cyber Security! An ideal apprenticeship for broad purpose first line Cyber Security support.

The primary purpose of the Cyber Security Technician is help ensure, secure and uninterrupted IT operations.

Security is maintained through a vigilant culture, keeping abreast of industry information and threat trends, implementing, evolving and maintaining preventative measures as well as maintaining robust systems, mechanisms, controls and procedures for monitoring and responding to any kind of Cyber-attack.

This apprenticeship is the ideal platform to then progress to undertake the Level 4 Cyber Security Engineer programme.

Who is it for?

Job titles for this apprenticeship are likely to include:

- Cyber Security Administrator
- Access Control Administrator
- Incident Response Technician
- Junior Security Operations Centre (SOC) Analyst
- Junior Information Security Analyst
- Junior Threat and Risk Analyst
- Junior Penetration Tester
- Junior Security Analyst

Entry Requirements:

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

Here is a general overview of each eligibility criteria:

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 apprenticeship Standard 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.

Each apprenticeship requires a portfolio of evidence this will showcase the apprentice's work and will be reviewed by the apprenticeship assessment organisation to determine how well new knowledge has been successfully utilised vocationally. If a job role is close to the eligibility criteria we will consult with employers to see if adjustments can be made to ensure criteria is met.

Initial assessment of knowledge and skills:

A prospective apprentice must stand to gain significant knowledge and skills from an apprenticeship. If the apprenticeship is too advanced for them or if they already know much of the knowledge and skills the apprenticeship would provide then they may not be eligible for the funding.

The ATP 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 very straightforward, however in some instances funding can be specially authorised for reduction in order to fund the parts of an apprenticeship that would be relevant. The ATP will provide the assessment for these possibilities.

The Level 3 Cyber Security Technician is highly technical, so whilst employers can select their own entry criteria, they should include a minimum of a Level 2 qualification or equivalent in IT and/or 5 GCSEs including English and Maths.

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. The ATP will provide both functional and advanced English and maths diagnostics and teaching to ensure each apprentice is fully supported in these areas.

Programme Duration:

This apprenticeship is delivered over 18 months for full- time employees. For part-time employees the term is adjusted depending on contracted hours.

Standard Delivery Model:

Apprenticeship training is delivered through a blend of weekly live virtual classrooms sessions and regular face-to-face mentoring sessions that are held on a one-to-one basis in the workplace.

These live classrooms are held through Microsoft Teams. This software provides the full suite of educational tools including everything you would find in a conventional classroom and more e.g. live open interactions, private breakout rooms, note and question queues and interactive illustration boards. We can also use movie green screen technology for lesson illustrations.

A full timetable for the training and mentoring, exams and assessments are provided at the outset. Progress is reviewed at 12 week intervals in a meeting between the mentor, apprentice and employer (typically the Apprentice's line manager).

Employers and apprentices have full visibility of progress in real-time by accessing the e-portfolio system, alternatively regular updates can be provided by other means if preferred.

End Point Assessment (EPA):

Aside from qualifications that can be obtained by doing an apprenticeship, the most important and valuable goal is what has been achieved during the programme.

Successful apprentices will obtain a Pass or Distinction in their apprenticeship. A Pass or Distinction is determined is at a stage called End Point Assessment which takes place once all the leaning has been completed. Like 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. Then the apprentice will undergo their End Point Assessment.

EPA for this programme consists of:

1. Portfolio of Evidence demonstrating work on 6-8 projects covering all the standard criteria
2. Two Scenario Demonstrations with supplementing questions from the Assessor
3. A structured interview with the Assessor discussing the Portfolio of Evidence

Programme Structure:

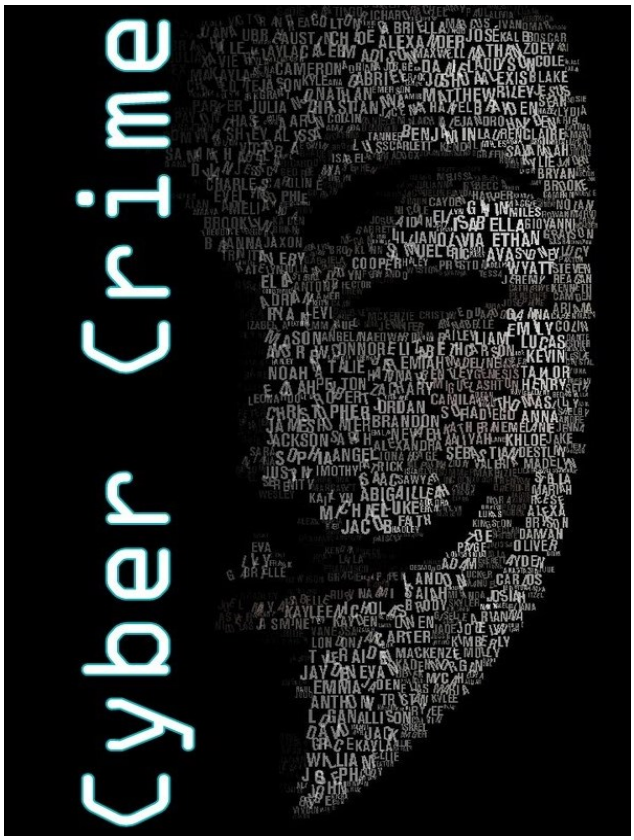
Technical Competencies:

- Apply procedures and controls to maintain security and control of an organisation
- Contribute to the production and development of security culture across an organisation
- Conduct the installation and maintenance of technical security controls following relevant procedures and standards
- Monitor, identify, report and escalate information security incidents and events
- Administer cryptographic and certificate management activities
- Administer cryptographic and certificate management
- Conduct regular review of access rights to digital information assets
- Maintain an asset register of controlled environments
- Assist with backup and recovery processes
- Contribute to documenting the scope and evaluating the results of vulnerability assessments following management requirements
- Contribute to risk assessments and escalate where appropriate
- Document incident and event information, assist with exception and management reports
- Monitor cyber security compliance and provide relevant data to auditors as required
- Contribute to routine threat intelligence gathering
- Document incident and event information and incident, exception and management reports
- Contribute towards the production and review of Cyber Security policies, procedures, standards and guidelines

- Monitor Cyber Security compliance and provide relevant data to auditors as required
- Collaborate with people both internally and externally to support secure and uninterrupted business operations of an organisation
- 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
- Monitor and detect potential security threats and escalate following relevant procedures and standards

Technical Knowledge and Understanding:

- Principles and components of organisational information security and governance for hardware, operating systems, networks, software and cloud
- Cyber security policies and standards based on an Information Security Management System (ISMS)
- Types of physical, procedural and technical controls
- All relevant UK and international legislation, professional body codes of conduct and ethical use of information assets
- Cyber security components of an effective security culture, different organisational structures and cultures, importance of maintaining secure information and the impact of a poor security culture
- Cyber security compliance and monitoring techniques
- Core terminology of cyber security; CIA triad-confidentiality, integrity, availability. Assurance, authenticity, identification, authentication, authorisation, accountability, reliability non-repudiation and access control
- Common operational tasks e.g. patching, software updates, access control, configuring firewalls, security, incident and event management tools (SIEM) and protection tools (Anti-virus, Anti-malware, Anti-spam)
- Cryptography, certificates and certificate management
- Detecting, reporting, assessing, responding to and learning from information security events
- Identity and access management - authentication, authorisation and federation, relationship to privacy, access rights and control, and the types of access control, access control mechanisms and application control
- Digital information assets in a controlled environment, the need to maintain an inventory and the need for secure information asset disposal
- Disaster prevention and recovery methods, service planning, basic disaster prevention and recovery practices
- Vulnerability categorisation, common exposures, software misconfiguration, sensitive data exposure and injection vulnerability
- Using components with known vulnerabilities, insufficient logging and monitoring, broken access control authentication, security misconfiguration and incorrect cross-site validation
- Vulnerability assessment techniques, how to evaluate results of an assessment to determine best recommendations
- Strengths and weaknesses of common assessment tools
- Types of security events – brute force, malware, suspicious user, suspicious device, unauthorized changes
- Forensic principles – evidence gathering and anti-contamination and anti-compromise
- Standard event and incident reporting requirements and how to document information as part of a chain or evidence
- Common policies – acceptable use, incident management, patching, anti-virus, BYOD, access control, social media, password, data handling and data classification, IT asset disposal
- Cyber security audit procedures, plans, documents, evidence and appropriate format
- Wider impact of customer issues, problems, business value, brand awareness, cultural awareness, diversity, accessibility, internal/external audience
- Service desk delivery, request responses and escalation methods
- Risk assessment, management and business impact analysis principles
- How to use data ethically and the implications for wider society, with respect to data use



Underpinning skills, attitudes and behaviours:

- Exceptional diligence towards following technical procedures and in maintaining security controls
- Attention to detail
- Judgement in determining validity of security requests from a range of internal and external stakeholders
- Desire to extract detail where appropriate in order to determine information risk assessments
- Calculated initiative
- Communicate effectively with both technical and non-technical stakeholders
- Professional, diplomatic and good customer service
- Proactive in maintaining current industry knowledge across technical, legal, regulatory and professional subject matter
- Ability to communicates, co-operate and collaborate in a multi-functional, multi-disciplinary environment team
- Strong work ethic
- Operate with initiative and take ownership of work
- Structured organisation and prioritisation of tasks

The designated trainers and mentors will support the employer and apprentice throughout the programme dedicated points of contact for questions and queries. This includes additional support for portfolio and project preparation, along with any advice and guidance needed.

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 apprentices
- 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