THE APPRENTICE and TRAINING PARTNERSHIP

LEVEL 4 APPRENTICESHIP FOR CYBER INTRUSION ANALYST

Programme Overview:

The primary role of a Cyber Intrusion Analyst is to detect breaches in network security for escalation to incident response or other determined function. An Intrusion Analyst will typically use a range of automated tools to monitor networks in real time, will understand and interpret the alerts that are automatically generated by those tools, including integrating and correlating information from a variety of sources and in different forms and where necessary seek additional information to inform the Analyst's judgement on whether or not the alert represents a security breach. When an Analyst has decided that a security breach has been detected, he or she will escalate to an incident response team, or other determined action, providing both notification of the breach and evidence with reasoning that supports the judgement that a breach has occurred. An Analyst will typically work as part of a team (or may lead a team) and will interact with external stakeholders, including customers and third party sources of threat and vulnerability intelligence and advice

Entry Requirements:

Individual employers will set the selection criteria, but this is likely to include A Levels, level 3 apprenticeship or other relevant qualification relevant experience and/or an aptitude test with a focus on functional maths.

Initial Assessments:

An initial assessment of Maths and English will be carried out for all apprentices using an approved diagnostic tool (BKSB, ForSkills); this will include Initial Assessment and full Diagnostic of knowledge in Maths and English to gauge the level at which the apprentice is working. This will enable us to support the apprentice and structure training provision.

Who is it for?

The Cyber Intrusion Analyst Level 4 Apprentice may have key responsibilities which can include:

- Secure Operations Centre (SOC) Analyst
- Intrusion Analyst
- Network Intrusion Analyst
- Incident Response Centre (IRC) Analyst
- Customer Services/Relationship Administrator
- Network Operations Centre (NOC) Security Analyst

Programme Duration:

The duration of this apprenticeship is typically 24 months

Delivery Model:

A minimum of 20% of the apprenticeship training takes place off-the-job and is flexibly delivered to suit your business with either classroom training and/or workshops in the workplace or block-training or day-release at our centre, with the remaining time being spent in the workplace.

A full timetable for training, ongoing assessment and End-Point Assessment will be issued to both you as the employer; and the apprentice, once the delivery model and training elements have been agreed.

On Programme Assessment will take the form of progress reviews with the trainer, employer and apprentice at least every 12 weeks. Feedback with ongoing development will include additional learning materials, resources and training delivered through the apprentice's e-portfolio OneFile; to which employers have access to view the progress and the development of each apprentice.

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk

End Point Assessment:

As the apprentice progresses through the apprenticeship, the employer and training provider will agree the apprentice has meet the Standard and be ready for End Point Assessment. This is called the 'Gateway' and will trigger End-Point Assessment.

This is carried out by a Qualified Independent Assessor by an Approved External Awarding Organisation and will test the knowledge and competencies of the apprentice using a range of methods, these can include; an interview, scenarios with questions, portfolio of evidence sampled, professional discussion, watching a presentation of the apprentice's evidence plus other methods.

The Independent Assessor will make the final judgement as to whether the apprentice has fully met the requirements of the Standard. Grading will also be awarded with a maximum mark of 100, this will be awarded by the Independent Assessor based on the apprentice's assessment. Grades awarded are distinction, merit, pass or fail. End-Point Assessment is normally carried out in the workplace.

Programme Structure:

The programme is broken down into areas to ensure that each apprentice has a rounded knowledge of principles, techniques and technologies. This involves an understanding of knowledge, skills and behaviour; as well as managing self and delivering results.

Technical Competencies

- Understands IT network features and functions, including virtual networking, principles and common practice in network security and the OSI and TCP/IP models, and the function and features of the main network appliances
- Understands and can utilise at least three Operating System (OS) security functions and associated features.
- Understands and can apply the foundations of information and cyber security including: explaining the importance of cyber security and basic concepts including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat' as well as explaining how the concepts relate to each other and the significance of risk to a business.
- Understands and can propose appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands and can propose how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.
- Understands and can advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.
- Understands the main features and applicability of law, regulations and standards (including Data Protection Act/Directive, Computer Misuse Act, ISO 27001) relevant to cyber network defence and follows these appropriately.
- Understands, can adhere to and can advise on the ethical responsibilities of a cyber security professional.

Technical Knowledge and Understanding

- Understands IT network features and functions, including virtual networking, principles and common practice in network security and the OSI and TCP/IP models, and the function and features of the main network appliances
- Understands and can utilise at least three Operating System (OS) security functions and associated features.
- Understands and can apply the foundations of information and cyber security including: explaining the importance of cyber security and basic concepts including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat' as well as explaining how the concepts relate to each other and the significance of risk to a business.
- Understands and can propose appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands and can propose how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.
- Understands and can advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.
- Understands the main features and applicability of law, regulations and standards (including Data Protection Act/Directive, Computer Misuse Act, ISO 27001) relevant to cyber network defence and follows these appropriately.
- Understands, can adhere to and can advise on the ethical responsibilities of a cyber security professional.

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk

Underpinning Skills, Attitudes and Behaviours

Learned through a blended mixture via on the job training and one to one training sessions, workshops and tutorials and applied according to business environment

- 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 productive, professional and secure working environment
- Ability to interpret written requirements and technical specification documents
- Effective telephone and e mail skills, including ability to communicate effectively with strangers under pressure, including reporting a security breach

The designated trainer 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.

Qualifications:

Apprentices must achieve each of the Ofqual-regulated Knowledge Modules, as summarised below:

- BCS KM1: Networks
- BCS KM2: Operating Systems
- BCS KM3: Information and Cyber Security Foundations
- BCS KM4: Business Processes
- BCS KM5: Law, Regulation and Ethics

Additional Professional Certifications that can be taken with The Apprentice and Training Partnership to complement these job roles on completion of the knowledge units are;

- MTA Network Fundamentals
- MTA Windows Operating Systems Fundamentals
- MTA Security Fundamentals
- CompTIA Security+
- CompTIA Network+

Progression:

This apprenticeship is recognised for entry to IISP 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:

In order to create an apprenticeship that best suits your business requirements, we will meet with you to discuss the delivery of the programme and how the apprenticeship will be funded. We will provide ongoing support including:

- Search and selection of the right apprentices to meet your business requirements.
- Specifying the training modules to optimise 'in job' performance.
- A tailored service in order to seamlessly integrate with your apprentice managers.
- Updates and information regarding apprenticeship costs and funding.
- Support and guidance for the apprentice and employer from start to finish with one main point of contact for you throughout the whole apprenticeship.
- Employer and apprentice access to a comprehensive range of resources and support material via OneFile.
- Time-efficient visits for training and assessment to work around you.
- Industry specialist qualified trainers and assessors.

Questions?

If you have any questions or concerns relating to supporting an Apprentice, your assigned tutor is always available to help, or, contact one of our advisors on **0330 380 0249.**

If you have any questions relating to this Apprenticeship Standard, please contact
Katie Fowler, Head of Operations and Quality **T.** 0330 380 0249 **E.** k.fowler@theatp.co.uk