elatt
The Learning Community

Cyber Security

Programme Outline for Apprenticeships at Level 4

2018

Who we are

ELATT is one of the top Tech apprenticeship providers in Greater London, bringing the best quality training into existing teams and helping companies bring new people into their workforce to help them grow. Established in 1986, ELATT has a long track record of delivering high quality online, and onsite work-based training – helping students to achieve outstanding results.

Recognised by Ofsted as Grade 1 (Outstanding) in all examined areas, ELATT won the prestigious Times Educational Supplement award of 'Best Training Provider and Further Education College in the UK'.

Introduction to the Cyber Security Apprenticeship Standards

Many companies outsource their Cyber Security to a Managed Security Service Provider (MSSP) or to a Virtual SOC (Security as a Service) web based platform. With the ongoing threat of Cyber attacks and the introduction of the GDPR regulation that every company must undertake to keep data safe, many companies are choosing to bring the Cyber Security function in-house.

IT teams are usually already undertaking cyber protection functions such as managing firewalls etc, and so are well set up to take on full control of this function. By doing this, there is no longer any risk of passing your security on to a third party, you can contact your own cyber security teams immediately and easily and members of staff who carry out this increasingly important element of your company's output, are people who work within the culture of your company and understand its aims.

There's a lot to be said about not outsourcing Cyber Security. However, most importantly, you need to be sure that you have the right skills in-house for now and in the future. This is where these two Cyber Security Apprenticeships Standards at Level 4 can help you. Companies can either recruit a new apprentice or use the apprenticeship training programme to upskill existing staff members.

ELATT are well set up to help you promote and recruit new talent in to your company and as part of the programme are happy to undertake much of the recruitment process at no extra cost in order to draw up a shortlist for interview.

As a Nationally recognised qualification, apprenticeships are part funded by the Government and if your company is a levy paying company, can be paid out of your Levy 'pot' that you have accumulated.

For further information about Apprenticeships in general or the Levy, download our Apprenticeships Guide on: www.elatt.org.uk/apprenticeships

Why choose ELATT?

Flexible delivery to suit your company's needs.
ELATT work with you, the employer to explore the best way that learning can be delivered i.e. a blend of learning in the workplace, learning in the classroom and online learning to our virtual learning environment.

Support in Recruiting new apprentices in to your workforce. If you are thinking of employing a new apprentice, ELATT can help you promote the recruitment opportunity, ensuring you gain maximum exposure on the National Apprenticeship site and in the local and recruitment media. We can organise the recruitment process, drawing up a shortlist for interview – thus saving on expensive recruitment costs.

NB Recruitment of apprenticeships are a great way to help you diversify your workforce and to get a better gender balance, particularly within IT departments.

Top quality training that fits your company's skill gaps.
All ELATT tutors are professional and qualified teachers with a specialisation in their field. Part of the reason ELATT achieved its Ofsted Outstanding status is because of the great results we achieve with students. Tutors work with you, the employer to design a curriculum that fits exactly the needs of your company, adding any further vendor qualifications linked to your business needs.

Expert business advice.
We know that for some employers who have not engaged with apprenticeships before, the process can be confusing and difficult to navigate. ELATT help you convert your Levy pot or apprenticeship budget in to high quality training programmes in Digital Skills and Business Skills – for both existing staff teams and new apprenticeship recruits. Our tutors listen to you, learn where your skills gaps are – or are likely to be in the future – and work with you to put the best training solutions for your company, achieving the best value for money from your apprenticeship levy 'pot'.

Cyber Security Technologists - Level 4

Job roles covered:

- Cyber Operations Manager
- Security Architect
- Penetration Tester
- Security Analyst
- Risk Analyst
- Intelligence Researcher
- Security Sales Engineer
- Cyber Security Specialist
- Information Security Analyst
- Governance & Compliance Analyst
- Information Security Assurance & Threat Analyst
- Forensics & Incident Response Analyst
- Security Engineer
- Information Security Auditor
- Security Administrator
- Information Security Officer

Introduction:

This standard is for employers looking to recruit and train people who are then able to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people. It therefore includes:

- Those focused on the technical side of work on areas such as security design & architecture, security testing, investigations & response: and
- Those focused on the risk analysis side on areas such as operations, risk, governance and compliance.

Whether focused on the technical or risk analysis side, this standard is for employers in all parts of the economy, who are looking to recruit and train people who will work to achieve required security outcomes in a legal and regulatory context and who will be able to develop and apply practical knowledge of information security to deliver solutions that fulfill an organisation's requirements.

Entry Requirements:

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

Technical Competencies:

By the end of the apprenticeship, the learner will be able to:

Threats, hazards, risks and intelligence

- Discover (through a mix of research and practical exploration) vulnerabilities in a system
- Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate use of relevant external sources of threat intelligence or advice (e.g. CERT UK). Combine different sources to create an enriched view.
- Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP)
- Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.

Developing and using a security case

- Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.
- Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).

Organisational context

- Identify and follow organisational policies and standards for information and cyber security.
- Operate according to service level agreements or employer defined performance targets.

Future Trends

- investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for your business, with supporting reasoning.

Technical Knowledge and Understanding:

By the end of the apprenticeship standard, the learner will understand:

- Why cyber security matters – the importance to business and society
- Basic theory – concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard. Also how these relate to each other and lead to risk and harm
- Security assurance – concepts (can explain what assurance is for in security, and 'trustworthy' versus 'trusted') and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance; and extrinsic assurance methods)
- How to build a security case – deriving security objectives with reasoned justification in a representative business scenario
- Cyber security concepts applied to ICT infrastructure – can describe the fundamental building blocks and typical architectures and identify some common vulnerabilities in networks and systems.
- Attack techniques and sources of threat – can describe the main types of common attack techniques; also the role of human behaviour.
- Explain how attack techniques combine with motive and opportunity to become a threat.
- Cyber defence – describe ways to defend against attack techniques
- Relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant features of UK and international law
- The existing threat landscape – can describe and know how to apply relevant techniques for horizon scanning including use of recognised sources of threat intelligence
- Threat trends – can describe the significance of identified trends in cyber security and understand the value and risk of this analysis

Specialisms: In addition to the core knowledge module described above, all apprentices will do ONE of the following Options:

Option 1 (Technologist):

- Knowledge Module 2: Network and Digital Communications Theory
- Knowledge Module 3: Security Case Development and Design Good Practice
- Knowledge Module 4: Security Technology Building Blocks
- Knowledge Module 5: Employment of Cryptography

OR

Option 2 (Risk Analyst):

- Knowledge Module 6: Risk Assessment
- Knowledge Module 7: Governance, Organisation, Law, Regulation & Standards

Underpinning Skills, Attitudes and Behaviours:

By the end of the apprenticeship standard, the learner must demonstrate:

- Logical and creative thinking skills
- Analytical and problem solving skills
- Ability to work independently and to take responsibility
- Ability to 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
- Ability to maintain productive, professional and secure working environment

Qualifications:

There are no vendor or professional qualifications identified that would exempt the above knowledge modules.

English and Maths:

Level 2 English and Maths will need to be passed, if not already, prior to taking the end point assessment.

Duration:

24 months.

Cyber Intrusion Analysts - Level 4

Job roles covered:

- Secure Operations Centre (SOC) Analysts
- Intrusion Analysts
- Network Intrusion Analysts
- Incident Response Centre (IRC) Analysts
- Network Operations Centre (NOC) Security Analysts

Introduction:

This standard is for employers looking to recruit and train people 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, will integrate and correlate information from a variety of sources and in different forms, and where necessary will 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.

Professional Recognition:

This apprenticeship is recognised for entry onto the register of IT technicians confirming SFIA level 3 professional competence and those completing the apprenticeship are eligible to apply for registration.

Technical Competencies:

By the end of the apprenticeship, the learner will be able to:

- Accurately, impartially and concisely record and report the appropriate information, including the ability to write reports (within a structure or template provided).
- Integrate and correlate information from various sources (including log files from different sources, network monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a network security breach.
- Recognise anomalies in observed network data structures (including by inspection of network packet data structures) and network behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.
- Recognise and identify all the main normal features of log files generated by typical network appliances, including servers and virtual servers, firewalls, routers.
- Recognise and identify all the main features of a normally operating network layer (including TCP/IP, transport and session control or ISO OSI layers 2-5), including data structures and protocol behaviour, as presented by network analysis and visualisation tools.
- Use basic configuration of the required automated tools, including network monitoring and analysis tools, SIEM tools, correlation tools, threat & vulnerability databases.
- Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.
- Interpret and follow alerts and advisories supplied by sources of threat and vulnerability (including OWASP, CISP, open source) and relate these to normal and observed network behaviour.
- Undertake own research to find information on threat and vulnerability (including using the internet).
- Manage local response to non-major incidents in accordance with a defined procedure.
- Interact and communicate effectively with the incident response team/process and/or customer incident response team/process for incidents.
- Operate according to service level agreements or employer defined performance targets.

Technical Knowledge and Understanding:

By the end of the apprenticeship standard, the learner will understand:

- 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
- and be able to utilise at least three Operating System (OS) security functions and associated features.
- and be able to 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 explain how the concepts relate to each other and the significance of risk to a business.
- and be able to propose appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- and be able to propose how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.
- and be able to advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.
- 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.
- and be able to adhere to and be able to advise on the ethical responsibilities of a cyber security professional.

English and Maths:

Level 2 English and Maths will need to be passed, if not already, prior to taking the end point assessment.

Underpinning Skills, Attitudes and Behaviours:

By the end of the apprenticeship standard, the learner must demonstrate:

- Logical and creative thinking skills
- Analytical and problem solving skills
- Ability to work independently and to take responsibility
- Ability to 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
- Ability to 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

Qualifications:

Apprentices must achieve each of the Ofqual-regulated Knowledge Modules, as summarised below. There are no vendor or professional qualifications identified that would exempt the above knowledge modules.

1. Networks (for level 4 Cyber Intrusion Analyst Apprenticeship)
2. Operating Systems (for level 4 Cyber Intrusion Analyst Apprenticeship)
3. Information and Cyber Security Foundations (for level 4 Cyber Intrusion Analyst Apprenticeship)
4. Business Processes (for level 4 Cyber Intrusion Analyst Apprenticeship)
5. Law, Regulation and Ethics (for level 4 Cyber Intrusion Analyst Apprenticeship)

Duration:

24 months.

Ofsted Highlights

On achievement...

Success rates for information and communication technology (ICT) courses are outstanding.

Virtually all learners gain their planned qualification at the end of their ICT courses. Alongside the main qualification, a good proportion of learners also complete manufacturers' awards such as one or more specialist vendor certifications.

On teaching...

Teachers are well qualified and all have an academic qualification in the subject which they teach. Several also have, or are working towards, higher degrees or doctorates. A significant minority also has industrial or commercial experience.

The quality of teaching, learning and assessment is outstanding. Lively, but professional, classroom sessions and support outside the classroom have been key factors in ensuring that a very high proportion of learners gain their intended qualification. But, almost as importantly, learners gain confidence in themselves and their abilities.

On student support...

All teachers are very supportive of their learners and this helps learners develop beyond the formal requirements of the course; as one passionate teacher rightly said, 'We help them unlock their potential.

A sensitive style of individual teaching ensures that learners are comfortable about asking for assistance. As a result, teachers are often the first point of contact for a range of concerns, including sensitive personal issues.

Speak to our experts today

If you are interested in any of the apprenticeships that ELATT offer, a quick chat with our apprenticeship expert advisor, will help you navigate the system, inform you of the facts that relate to you and help you plan you're the best value for money apprenticeship programme for your company.

employers@elatt.org.uk

www.elatt.org.uk/apprenticeships

0800 0420 184