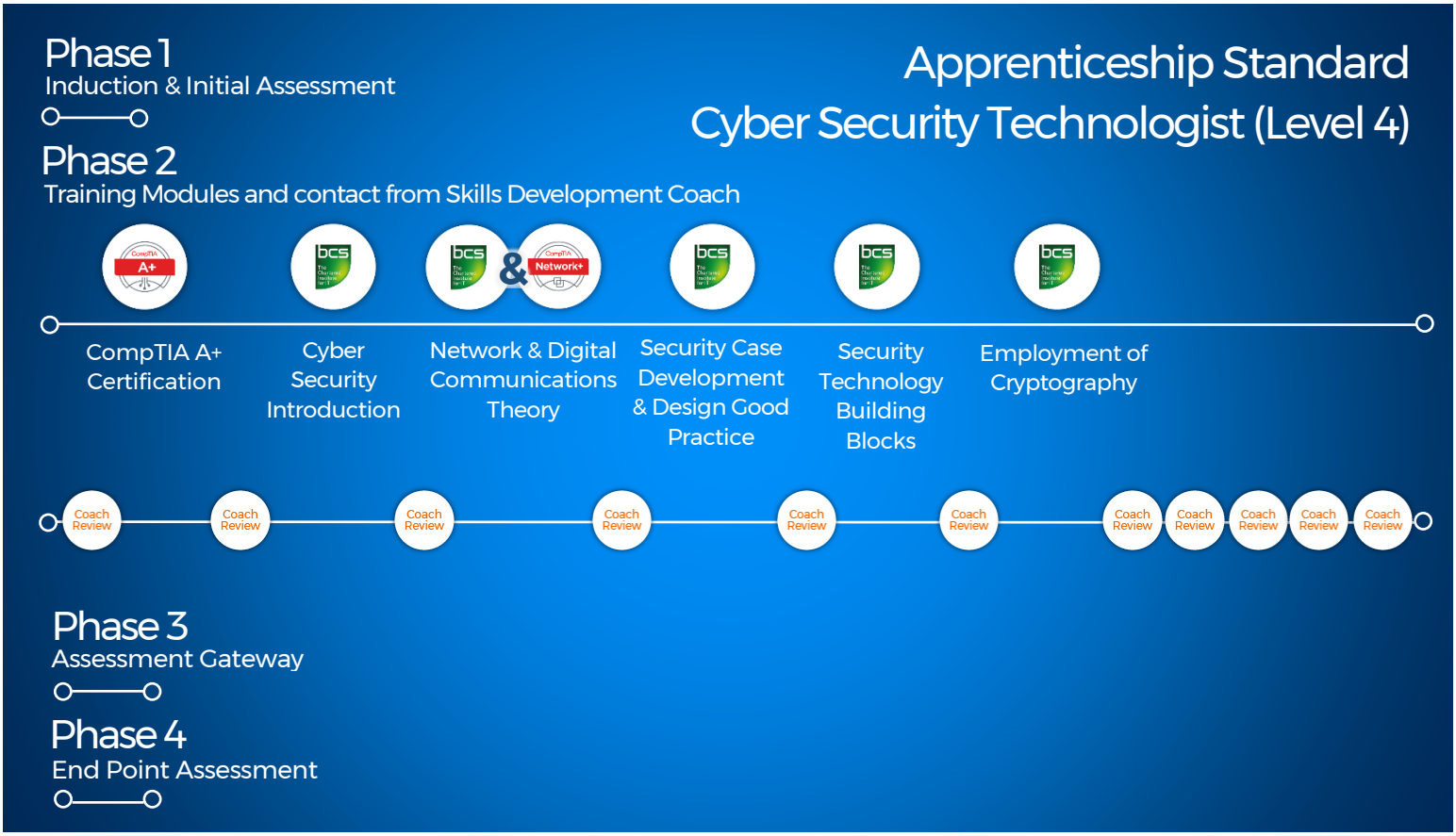
Cyber Security Technologist (Level 4)



Blended Learning breakdown

		Training Centre	Remote
Phase 1	Induction & Initial Assessment	1 day	Training Centre only
Phase 2	CompTIA A+ (Recommended if no L3 or equivalent skills)	2 weeks	40 hours self-study 8 remote training sessions
	Cyber Security Introduction	1 week	20 hours self-study 4 remote training sessions
	Network & Digital Communications Theory (CompTIA Network+ optional exam, BCS mandatory exam)	2 weeks	Training Centre only
	Security Case Development & Design Good Practice	1 week	20 hours self-study 4 remote training sessions
	Security Technology Building Blocks	1 week	20 hours self-study 4 remote training sessions
	Employment of Cryptography	1 week	20 hours self-study 4 remote training sessions
Phase 3	Assessment Gateway	Up to 1 week*	Training Centre only
Phase 4	End Point Assessment	3 – 5 days	Training Centre only

*To be arranged by your Skills Development Coach

estio

Course Details

Induction/Initial Assessment

1 day in the training centre

Functional Skills

If required, learners will sit a Maths and/or 3 English exams.
Allow 1 – 2 days per exam.

CompTIA A+ Certification

(Recommended only if learner is not of equivalent level of knowledge)

- Understanding hardware
- Networking & mobile devices
- Hardware & network
- Troubleshooting
- Windows operating systems
- Other operating systems (Linux/Mac)
- Security
- Software troubleshooting
- Operational procedures

Security Case Development and Design Good Practice

- Describe what good practice in design is and how this may contribute to security
- Describe common security architectures that incorporate security hardware and software components
- Understand how to develop a 'security case', recognising that threats evolve and threats also respond to a security design

Cyber Security Introduction

- Explain why information and cyber security is important to business and society
- Explain basic concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, risk & hazard
- Explain how the concepts of threat, hazard and vulnerability relate to each other and lead to risk
- Explain what penetration testing ('ethical hacking') is and how it contributes to assurance
- Applying basic security concepts to develop security requirements
- Describe some common vulnerabilities in computer networks and systems (for example, non-secure coding and unprotected networks)
- Describe the main different types of common attack techniques (for example: phishing, social engineering, malware, network interception, blended techniques e.g. 'advanced persistent threat', denial of service, theft)
- Describe Legal, standards, regulations and ethical standards relevant to cyber security

Network & Digital Communications Theory

- Explain what is meant by data and protocol and how they relate to each other
- Describe an example data format and a simple protocol in current use (using protocol diagrams). Describe example failure modes in protocols
- Describe at least one approach to error control in a network
- Describe the main features of network protocols in widespread use on the Internet, their purpose and relationship to each other in a layered model
- Describe the main routing protocols in current use in computer networks and explain the differences between static and dynamic routing protocols and the pros and cons of each in different circumstances.
- Explain some of main factors that affect network performance and propose ways to improve performance

Security Technology Building Blocks

- Describe common types of security hardware and software which are used to protect systems
- (e.g. firewalls, encryption for data at rest, encryption for communication, IDS, IPS, IDAM tools, AV, web proxy, application firewalls, cross domain components, HSM, TPM, UTM)
- Explain how each may be used to deliver risk mitigation or implement a security case
- Understanding the benefits/limitations, and taking into account the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component, describing any residual risks

Employment of Cryptography

- Describe the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc) and explain how they are applied and to what end and their limitations
- Explain the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy
- Describe the role of cryptographic techniques in a range of different systems and the practical issues introducing such into service and updating them
- Appreciate that there are legal issues relevant to cryptography in particular when crossing national borders
- Awareness of UK, EU and US export control of cryptography

Assessment Gateway, Assessment Preparation & Administration Week

(Up to 1 week in the training centre)
Preparation week to understand the four elements of the assessment gateway

Assessment Phase

Summative Portfolio

Synoptic Project

Technical Interview with SME

Employer Reference

Achievement of Apprenticeship

BCS
Cyber Security Technologist (Level 4)

For further information please contact the Estio Client Engagement Team on 01133 500 333
www.estio.co.uk