# Level 4 Cyber Security Technologist.

This programme will provide your organisation with highly capable cyber security professionals equipped with the technical expertise and critical thinking skills essential in today's threat landscape. Learners will develop a deep understanding of cyber threats, attack methodologies, and the legal and regulatory frameworks that govern cyber security. The skills learners will develop on programme will allow you to strengthen your organisation's cyber resilience through effective risk assessment, cryptographic application, and incident response planning. With exposure to AI-driven threat intelligence and advanced firewall configurations, learners will be prepared to anticipate and counter emerging threats.

By the end of the programme, your organisation will benefit from professionals capable of aligning security strategies with business objectives, ensuring continuity, compliance, and confidence in your digital operations.

### Who's it for?

This occupation exists across virtually every industry that uses technology. You'll find it in sectors like digital, telecoms, tech, business services, defence, government, finance, healthcare, retail, transport, automotive, and even critical national infrastructure. It's also present in all kinds of organisations – whether it's a global corporation, a government agency, a university, a charity, or a small to medium-sized business (SME).

- **For employers:** this programme is suited to organisations seeking to strengthen their cyber security capabilities by developing in-house talent. It is particularly suited for businesses that handle sensitive data, operate within regulated industries, or are looking to proactively defend against evolving cyber threats.
- **For learners:** This programme is best suited to those who are currently working in roles related to IT, network administration, or information security. It's also suited to those who demonstrate analytical thinking, attention to detail, and a proactive approach to problem-solving – traits essential for identifying and mitigating cyber threats.

### Business impacts

**Stronger Defence Against Cyber Threats**
By training employees in real-world attack scenarios and AI-driven threat detection, businesses can proactively prevent cyberattacks, reducing the risk of data breaches, financial losses, and reputational damage.

**Workforce with Industry-Recognised Skills**
Employees trained will bring proven expertise, ensuring businesses comply with security regulations and maintain a skilled security team.

**Reduced Downtime and Compliance Risks**
A well-trained cyber security workforce minimises system vulnerabilities, ensures compliance with GDPR, ISO 27001, and other regulations, and reduces costly downtime caused by security incidents.

### Built for performance

- Programmes designed and delivered by industry experts
- Dedicated Performance Coach, qualified in both coaching and their specialist subject area
- Backup from a multidisciplinary performance team
- Market-leading online live learning experience
- 24/7 access to programme materials, enrichment resources, study support and specialist insight via our virtual learning platform
- Mentoring, networking and peer support through BPP Community, including our Student Ambassador Network
- Learning pathways built using a 'stretch and challenge' model by design, meaning each learner is pushed to their maximum abilities
- Progression pathways that can take you from entry level to specialist expert
- Dedicated Functional Skills support if required

estio
Part of the BPP Education Group

FIREBRAND
Part of the BPP Education Group

# Programme overview.

**Apprenticeship standard:** Cyber Security Technologist

**Cost:** £18,000

**Duration:** 18-24 months

**Entry requirements**

As a minimum learners will need to have:

- Five GCSEs at grades 9 to 4 (A* to C), and
- A level 3 qualification such as A-Levels (or equivalent)

For learners that do not have GCSE English and/or maths at grades 9 to 4 (A* to C):

- Learners aged 16-18 years must study and pass Functional Skills English and/or maths as part of the apprenticeship programme
- Learners aged 19 or above on the day they start the programme do not need to study or pass Functional Skills English and/or maths, unless required by their employer

## Prepare for the challenges of tomorrow

**Get ahead of evolving workforce skills needs**

Every BPP apprentice has access to our exclusive Emerging Skills programme.

Comprised of three bespoke courses, the programme combines expertise from BPP, Microsoft and xUnlocked to give learners essential knowledge and skills in the rapidly emerging areas of AI and sustainability.

- Available to all learners at no extra cost
- Accessible anytime, anywhere via our virtual learning platform
- Self-paced learning to fit into any busy schedule

xUnlocked

**Programme contents**

Generative AI Fundamentals (Four modules)

Developed by BPP's expert data scientists, this course offers an introduction to working with generative AI effectively, safely and ethically.

Introduction to Sustainability (Six modules)

Developed in partnership with sustainability experts, xUnlocked, this course builds fundamental knowledge on sustainability and sustainable working practices.

Microsoft AI and Security Essentials (Seven modules)

This official Microsoft learning pathway is comprised of a core pathway on AI Essentials, followed by either an AI Fundamentals pathway or Security pathway. Dedicated Microsoft experts guide learners to gain Microsoft digital badges as they progress, with the option to gain a recognised Microsoft Certification on completion.

estio Part of the BPP Education Group | FIREBRAND Part of the BPP Education Group

# AI skills, *for all.*

Embedded AI training modules for every data and tech programme. Empowering every learner to drive AI-centric transformations within their business.

- Available to all learners at no extra cost
- Bespoke to BPP, developed by our expert data scientists
- Self-guided online learning to fit into any busy schedule
- Accessible anytime, anywhere via our virtual learning platform

Generative AI Foundations → Advanced Prompt Engineering → AI Strategy and Business Implementation → AI Tools, Platforms and Customisation

**Knowledge and skills gained**

Focusing on practical application of technical and non-technical AI skills, the modules explore AI's capacity to optimise structured interactions, align governance frameworks, and deploy scalable solutions, with a significant focus on ethical considerations and operational efficiency.

- Ability to design and implement complex prompts for diverse use cases
- Understanding and application of HITL techniques and fact-checking principles
- Ability to conduct prompt A/B testing
- Understanding of AI governance frameworks and compliance requirements
- Ability to adapt AI messaging for different stakeholders
- Ability to assess AI ecosystems
- Understanding of API-driven generative AI (GenAI) benefits

**Tools**

Large language models (LLMs)
(for example Copilot or Google Gemini)

No-code AI automation platforms
(no prior coding knowledge required)

**Optional masterclasses**

Live online sessions available every month

Example topics include:

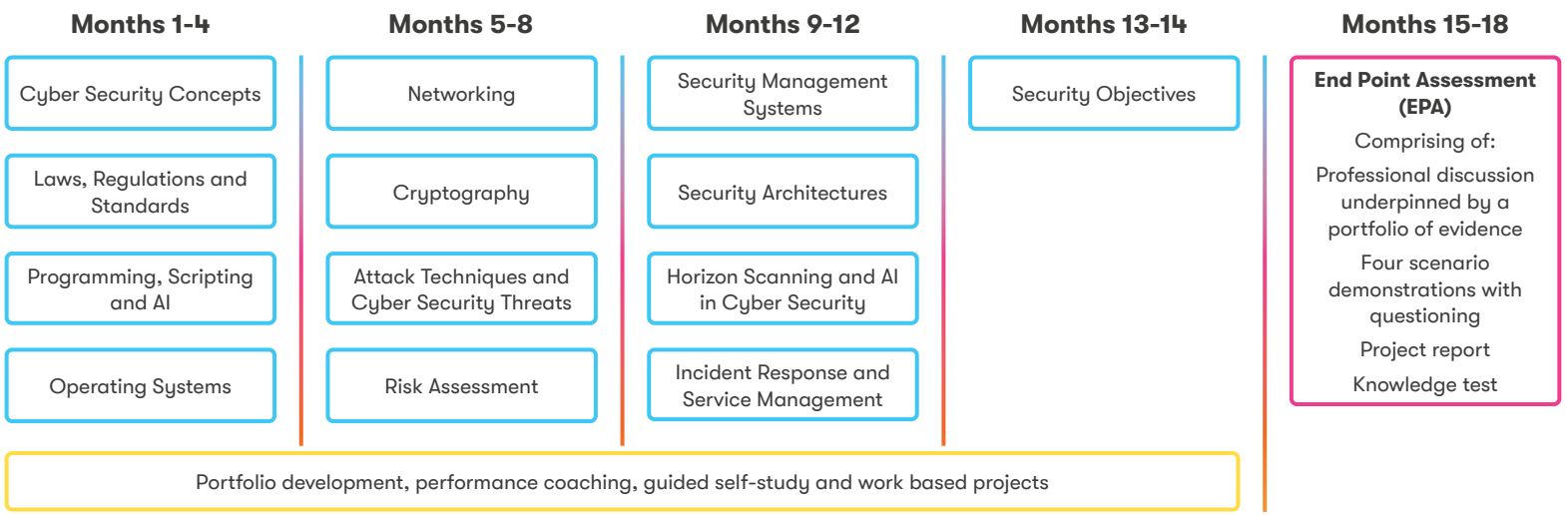
- Data Leadership
- Ethical Hacking and Cyber Security
- Discovering and Analysing Market Trends
- Sustainable Technology and Green Computing
- Responsible AI
- Setting AI Strategy
- Emerging Landscapes – AI
- Quantum Computing Fundamentals

estio Part of the BPP Education Group | FIREBRAND Part of the BPP Education Group

# **Delivery option one:** Online Monthly (Block Release).

Structured to focus learning, with online live lectures and seminars delivered over monthly full-day blocks.

## 18-month programme (inc. EPA)




Core modules  End Point Assessment

### Apprenticeship standard

Cyber Security Technologist

### Delivered by

Estio

### Time commitment*

- **14 months** on programme
- **39 days** *(six hours per day)* in online live training sessions
- **10-12 hours** guided self-study, per module, via our virtual learning platform
- **1 hour** performance coaching session, every month
- **1 hour** progress review, every eight weeks
- **6 hours** per week in off-the-job learning, during working hours
- **1 hour** EPA preparation session
- **4 months** in End Point Assessment

estio
Part of the **BPP** Education Group



*On average.

# **Delivery option one:** Programme modules.

**Cyber Security Concepts**

The aim of this module is to equip apprentices with a solid understanding of key cyber security concepts, including common threats, attack techniques, and the motivations behind them. Apprentices will also learn how to apply industry-recognised best practices to protect systems and data, helping them to develop a proactive and informed approach to cyber defence.

**Laws, Regulations, and Standards and Professional Bodies**

The apprentice will explore how to identify and apply key laws, regulations, and standards that govern cyber security in the UK. They will learn how these legal frameworks influence cyber security practices and how to ensure compliance when designing and implementing security measures.

**Programming, Scripting, and AI**

The apprentice will develop programming skills to create programs that will allow them to analyse aspects of the operating systems or network systems. The basic concepts of AI to assist in cyber exploits, program writing and analysis will be explored.

**Operating Systems and Digital System Concepts**

The aim of this unit is to provide apprentices with the skills and knowledge to navigate three different types of operating system. The apprentice will investigate the function and features of significant digital system components and analyse typical architectures.

**Networking**

The aim of this module is to provide students with knowledge of computer networking essentials, how they operate, protocols, standards, security considerations and a range of networking technologies.

It gives the students the knowledge and skills that they need for the planning, designing, implementation and management of computer networks and understanding of the network infrastructure capabilities and limitations.

**Cryptography**

In this module, the apprentice will gain knowledge of the basic terminology and concepts of cryptography and common cryptography techniques in use. The apprentice will understand the importance of effective cryptography key management and the main techniques used. The apprentice will gain knowledge of legal, regulatory and export issues specific to use of cryptography.

**Attack Techniques and Cyber Security Threats**

This module will allow the apprentice to identify the main types of common attack techniques. The apprentice will gain an understanding of the role of human behaviour, including the significance of the 'insider threat'.

The apprentice will be able to identify trends in the cyber security threat landscape. They will further their knowledge by learning how to deal with threats. They will gain knowledge of emerging attack techniques by applying frameworks such as Mitre Att&ck and understand the hazards and risks posed by such attacks.

estio

Part of the **BPP** Education Group

# **Delivery option one:** Programme modules.

**Risk Assessment**

In this module the apprentice will gain knowledge of risk assessment and audit methodologies and approaches to risk treatment.

The apprentice will analyse and develop approaches to identifying the vulnerabilities in organisations and security management systems.

Apprentices will understand the threat intelligence life cycle.

**Security Management Systems**

In this module the apprentice will investigate and analyse the principles of security management systems.

They will gain knowledge about governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.

**Security Architectures**

In this module the apprentice will investigate and analyse the principles of security management systems.

They will gain knowledge of governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.

**Horizon Scanning and AI in Cyber Security**

In this module the apprentice will gain knowledge of horizon scanning, including use of recognised sources of threat intelligence and vulnerabilities.

**Incident Response and Service Management**

This module will teach the apprentice how to understand and follow the incident management process, apply it effectively, and learn how to gather and protect evidence during an incident investigation.

Apprentices will also gain knowledge of foundational life cycle and service management process as used in most IT business, with a focus on ITIL.

**Security Objectives**

The apprentice will learn how to analyse employer or customer needs to define security objectives. They will then develop a security case – considering potential threats and the broader context – that outlines proposed security measures with clear, reasoned justification.

estio

Part of the **BPP** Education Group

# **Delivery option two:** Intensive (Block Release).

Highly focused and intensive training delivered either face-to-face at one of our residential centres, or online live.

## 24-month programme (inc. EPA)

| Months 1-4 | Months 4-8 | Months 9-12 | Months 13-20 | Months 21-24 |
|---|---|---|---|---|
| Cyber Introductions (3 days) | Python Fundamentals (4 days) | CompTIA Network+ (4 days) | EC-Council Certified Network Defender (5 days) | **End Point Assessment (EPA)** |
| E-Learning and Why Cyber Security Matters | Ethical Principles Code of Practice | CompTIA Security+ (4 days) | Operation of Security Management Systems and Incident Response | Comprising of: |
| Cyber Security Concepts and its Importance to Business | Laws and Regulations | Preventing Security Breaches and Continuous Improvement | | Professional discussion underpinned by a portfolio of evidence |
| Rationale for Security Objectives | | Following Organisations Policies and Procedures | | Four scenario demonstrations with questioning |
| | | | | Project report |
| | | | | Knowledge test |

Portfolio development, performance coaching, guided self-study and work based projects

Technical modules and certifications | Work based projects | End Point Assessment

### Apprenticeship standard

Cyber Security Technologist

### Delivered by

Firebrand

### Time commitment*

- **20 months** on programme
- **14 training sessions** either online live or face-to-face
- **228 hours** guided self-study, per module
  - Cyber Introduction – 36 hours
  - Python Fundamentals – 48 hours
  - CompTIA Network+ – 48 hours (via CertMaster)
  - CompTIA Security+ – 48 hours (via CertMaster)
  - EC-Council Certified Network Defender – 60 hours
- **6 hours** per week in off-the-job learning, during working hours
- **4 months** in End Point Assessment

### Optional Certification Exams

- The exams included in this programme are CompTIA Network+, CompTIA Security+, and EC-Council Certified Network Defender
- Learners have the option to sit certification exams as part of the programme, but this is not mandatory to successfully complete the apprenticeship
- The cost of one exam attempt for each certification is included in the programme, giving learners the opportunity to gain additional qualifications at no extra cost. Resit costs are funded by the employer
- Learners will only be encouraged to undertake certification exams once they can demonstrate competency by passing a mock test

FIREBRAND
Part of the BPP Education Group



*On average.

# **Delivery option two:** Programme modules.

**Cyber Introduction**

Understand the range of data analysis tools introduced in the course and recognise that direct access to these applications is not required for successful participation.

Recognise the availability of pre-configured virtual labs for practical application use during residential or OIL courses, eliminating the need for software installation on personal or workplace devices.

**Python Fundamentals**

Learn how to write basic Python code, declare variables, and work with console input and output. Learn how to create programmes and projects in Python. Work with strings, lists, loops, dictionaries, and functions. Learn language syntax but also patterns for how to structure apps.

This course will help the learner develop the foundations they need to work on any Python project.

**EC-Council Certified Network Defender**

The course provides a comprehensive foundation in network defence by covering threat reconnaissance, social engineering, and malware deployment tactics, along with methods for detecting and mitigating these attacks.

It emphasises incident detection and response, risk management, and securing critical assets. Learners explore threat intelligence, virtual security services, business continuity planning, IoT security risks, and web vulnerabilities aligned with the OWASP Top 10.

The course equips participants with the knowledge and skills necessary to protect organisational infrastructure and respond effectively to evolving cyber threats.

**CompTIA Network+**

The course equips IT professionals with the essential skills to design, implement, and maintain secure and efficient networks. It covers configuring and managing network devices, optimising traffic flow, and troubleshooting issues to ensure reliability. Learners gain expertise in network security, standards, and virtualisation, preparing them to tackle real-world challenges.

**CompTIA Security+**

This course provides a comprehensive foundation in cyber security, covering key concepts, threats, and mitigation strategies essential for securing modern environments. It delves into security architecture principles and explores best practices for managing operations, vulnerabilities, and data protection. It emphasises security governance, risk management, and effective communication skills for security professionals.

FIREBRAND
Part of the **BPP** Education Group