CYBER ACADEMY BROCHURE

CONTENTS

Introduction 4

Experienced professionals 6

Certified cyber tech specialists 7

Assessment strategy 9

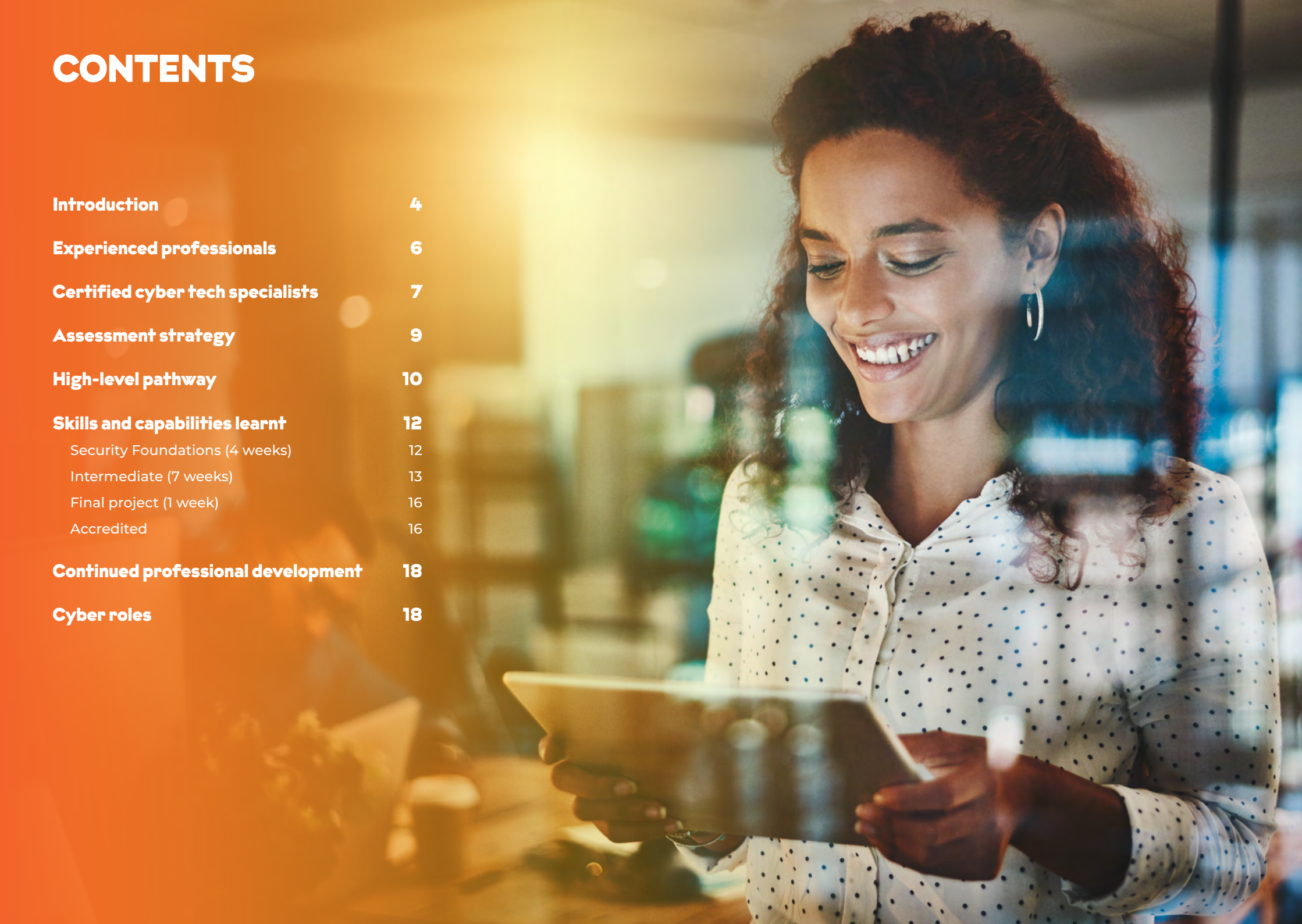
High-level pathway 10

Skills and capabilities learnt 12

- Security Foundations (4 weeks) 12
- Intermediate (7 weeks) 13
- Final project (1 week) 16
- Accredited 16

Continued professional development 18

Cyber roles 18



INTRODUCTION

The Cyber Security 12-week academy programme upskills experienced tech candidates through our academy to create cyber tech specialists ready to be deployed and hit the ground running at a client site.

The participants have a suite of exciting skills gained on their inaugural 12 week academy (Software Development/DevOps) programme. In-demand skills in software, cloud and agile in preparation for their next development journey, the QA cyber academy.

All Cyber Specialists have previous experience on client site as fully trained Software Developers and DevOps Engineers.

The cyber academy programme provides candidates with the knowledge and skills to become a trusted member of your team with vital in-demand cyber capabilities. Blended with tech labs, instructor led workshops and gamified learning experiences to ensure the acquisition and application of knowledge and hands-on skills.

Gamified learning keeps the participant engaged and excited about continuous training, helping them see the true value of their capabilities. Hands-on training and active-learning models increase retention rates by 75 percent, so our cyber tech specialists can prepare for real-world challenges.

Furthermore, the programme is aimed to provide delegates with the personal and soft skills to maintain strong and impactful working relationships with stakeholders and colleagues.

The 12-week course takes a modular approach:

- **Foundation Security Skills**
- **Intermediate Applied Security Skills**
- **Gamified Security Simulations**

EXPERIENCED PROFESSIONALS

All Cyber Tech Specialists have previously been through the QA academy on either a 12-week Software Developer programme or 12-week DevOps programme and are therefore equipped with vital business and technical skills and knowledge, including but not limited to:

Existing skills

- Business Analysis skills and tools
- Understanding the full application stack
- Ability to code
- Understanding of Cloud Native
- Cloud Architecture
- Agile ways of working
- Working collaboratively

Soft skills

In addition to the skills learnt, the delegates have all been previously deployed at client sites and have experience of reporting, analysing and presenting, with many having undertaken national security vetting via their first deployment. Their experience, in addition to the new skills learnt on the 12-week Cyber Academy to upskill their capabilities, the Cyber Tech Specialists will have the impact you need to make a difference in your organisation.

CERTIFIED CYBER TECH SPECIALISTS

Throughout the programme, we teach the necessary skills through a series of learning interventions and cyber workshops. The candidates will leave the programme having earned the following cyber security certifications.

We recognise that traditional certifications need to be complemented with practical immersive experiential learning. That's why we blend hands-on gamified learning experiences throughout the programme to underpin a broad set of critical cyber skills and assured capability.

Certifications earned throughout the programme include:

- CompTIA – Security+
- NCSC Certified Training – Certified in the Art of Hacking
- NCSC Certified Training – Practitioner Certificate in Cloud Security
- NCSC Certified Training – Certificate in Digital Forensic Fundamentals
- Certified Threat Intelligence Analyst
- NCSC Certified Training – NIST Cyber Security Professional (NCSP©).
- Certified Security Risk Manager

ASSESSMENT STRATEGY

There is a clear progression through the structured pathways of cyber topics and validation though knowledge checks and independent exams.

Imbedded within the programme are real world progressive technical ‘in-game’ assessments which take place within the Project Ares platform from Circadence. This gamified learn-by-doing solution allows for on-going assessments and achievements to be recorded and measured throughout the programme.

Communication skills are imperative within the technical landscape. Our candidates are already experienced business analysis, we enhance this skill and develop technical communication techniques. Delegates will be assessed throughout the programmes with project activities after each module, including assessing their capability to research, analyse, report and present their findings in an unambiguous manner. Whilst also being able to disseminate salient facts to a non-technical audience.

HIGH-LEVEL PATHWAY

Cyber Tech Specialists have already completed a 12 week academy programme in:

DevOps academy
Or
Software Developer academy

and had a minimum of 12 months' experience on client site, before progressing to the Cyber programme.

Key:

- Cyber Tech Specialist
- Self-Paced Labs
- Facilitated Workshops
- Soft Skills Workshop
- NCSC Certified Training

Certified Training
in association with National Cyber Security Centre

Week 1 — **Fast Track Foundation Pathway**

- Networking & Operating System Fundamentals
- CompTIA Security
- Certified in the Art of Hacking
- Consolidation Exam / Certification

Week 4

Prerequisite to move to intermediate path

Week 5 — **Intermediate Pathway**

- AppSec and Encryption
- Practitioner Certificate in Cloud Security
- Certified Threat Intelligence Analyst

Week 8

- Certificate in Digital Forensics Fundamentals

Week 9

- Defensive Security Techniques
- NIST Cyber Security Professional
- Certified Security Risk Manager

Week 12

- Project ARES and Presentation

Security Project

SKILLS AND CAPABILITIES LEARNT

SECURITY FOUNDATIONS (4 WEEKS)

During the foundation weeks of the programme our cyber tech specialists learn a host of cyber skills, they learn how to;

- Install, configure, and deploy network components while assessing and troubleshooting issues to support organisational security.
- Implement secure network architecture concepts and systems design.
- Install and configure identity and access services, as well as management controls.
- Implement and summarise risk management best practices and the business impact.
- Install and configure wireless security settings and implement public key infrastructure.
- Detect various types of compromise.
- Discover fingerprint systems and services.
- Understand Windows and Linux operating systems through a variety of well-known vulnerabilities.
- Conduct password brute force attacks to compromise services and gain access to a host.
- Discover the techniques for hacking application servers and content management systems to gain access to customer data.
- Conduct client-side attacks and execute code on a victim's machine.
- Identify common web application vulnerabilities and introduce security within their software development life cycle in a practical manner.
- Utilise Wireshark for packet capture analysis.
- Discover Identity and Access Management best practice
- Understand fundamental cryptography concepts and public key infrastructure.
- Understand incident response tools, techniques and procedures.

Certifications achieved in Foundation phase:

- CompTIA Security+
- Certified in the Art of Hacking*

INTERMEDIATE (7 WEEKS)

During the intermediate weeks of the programme our cyber tech specialists learn a range of key cyber skills, including;

Cloud Security and how to;

- Use cloud security principles, patterns and architectural frameworks to protect cloud services and cloud security architectures.
- Understand data protection and compliance for cloud-based applications.
- Discover the range of technical security controls available using Cloud Service Provider and partner technologies.
- Understand best practice cloud security assurance, audit and security testing techniques for cloud-based services.
- Review the implications and benefits of containers and serverless architectures.
- Implement secure cloud configurations on AWS and Microsoft platforms.
- Use cloud technologies and technical security controls in labs based on services from cloud service providers AWS and Microsoft.

Application Security and how to;

- Use a secure development lifecycle to embed best practice security processes in a development lifecycle.
- Exploit each of the OWASP top ten vulnerabilities.
- Secure web application security vulnerabilities to defend against common security weaknesses.
- Understand the financial and wider repercussions of different vulnerabilities.

Cyber Threat Intelligence and how to;

- Use threat intelligence in risk management, SIEM, and incident response.
- Understand the various steps involved in planning a threat intelligence program.
- Discover the types of data feeds, sources, and data collection methods.
- Utilise threat intelligence data collection and acquisition through cyber intelligence courses and malware analysis.
- Complete threat analysis process, including threat modelling, fine-tuning, evaluation, runbook, & knowledge base creation.
- Understand threat intelligence dissemination and sharing protocol including dissemination preferences, intelligence collaboration, sharing rules and models, TI exchange types and architectures, participating in sharing relationships, standards, and formats for sharing threat intelligence.
- Practice the effective creation of threat intelligence reports.

Digital Forensics and how to;

- Understand the purpose, benefits, and key terms of digital forensics.
- Describe and adhere to the principles of the forensic framework.
- Understand the importance of the chain of custody.
- Demonstrate a basic knowledge of key locations in different operating systems.
- Identify how different file systems represent files and how they deal with deletion.
- Understand where timestamps and other meta data comes from.
- Have knowledge of the legal framework in which they operate, and the expected level of ethical behaviour.

Security Frameworks and how to;

- Utilise the Mitre Att&ck framework to understand adversary tactics and techniques based on real-world observations.
- Acknowledge the correlation between Information Security risk management and security controls.
- Understand the concepts, approaches, methods and techniques that enable an effective security risk management process according to ISO 27005.
- Interpret the requirements of ISO 27001 in Information Security Risk Management.
- Acquire the competence to effectively advise organisations in Information Security Risk Management best practices.
- Use the NIST Cyber Security framework, discover how to improve an organisations ability to prevent, detect, and respond to cyber-attacks.
- Use business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organisation's risk management processes.

Certifications achieved;

- Practitioner Certificate in Cloud Security*
- Certificate in Digital Forensic Fundamentals*
- Certified Threat Intelligence Analyst
- Certified Security Risk Manager,
- NIST Cyber Security Professional (NCSP©)*.

FINAL PROJECT (1 WEEK)

Our week-long final challenge provides a gamified learning experience for our cyber tech specialists. Using the state of the art Circadence Project Ares platform in a totally immerse experience. The platform uses automated features to support skills adoption with an in-game advisor 'Athena' who advises our players through the scenario-based challenges. With automated adversaries responding to players for added challenge.

Within this extended practice environment, we provide a safe place to apply all of the acquired skills throughout the programme, with added scoring of players and opponent actions with replay for objective assessment. Ultimately actions culminate to inform models on best tactics for scenarios with instructor orchestration and observation.

ACCREDITED

Our cyber tech specialists are accredited with best practice and leading industry cyber security certifications. Many of the individual training modules and certification exams are accredited under the National Cyber Security Centre (NCSC) Certified Training* scheme.

Certified Training

in association with
National Cyber Security Centre

CONTINUED PROFESSIONAL DEVELOPMENT

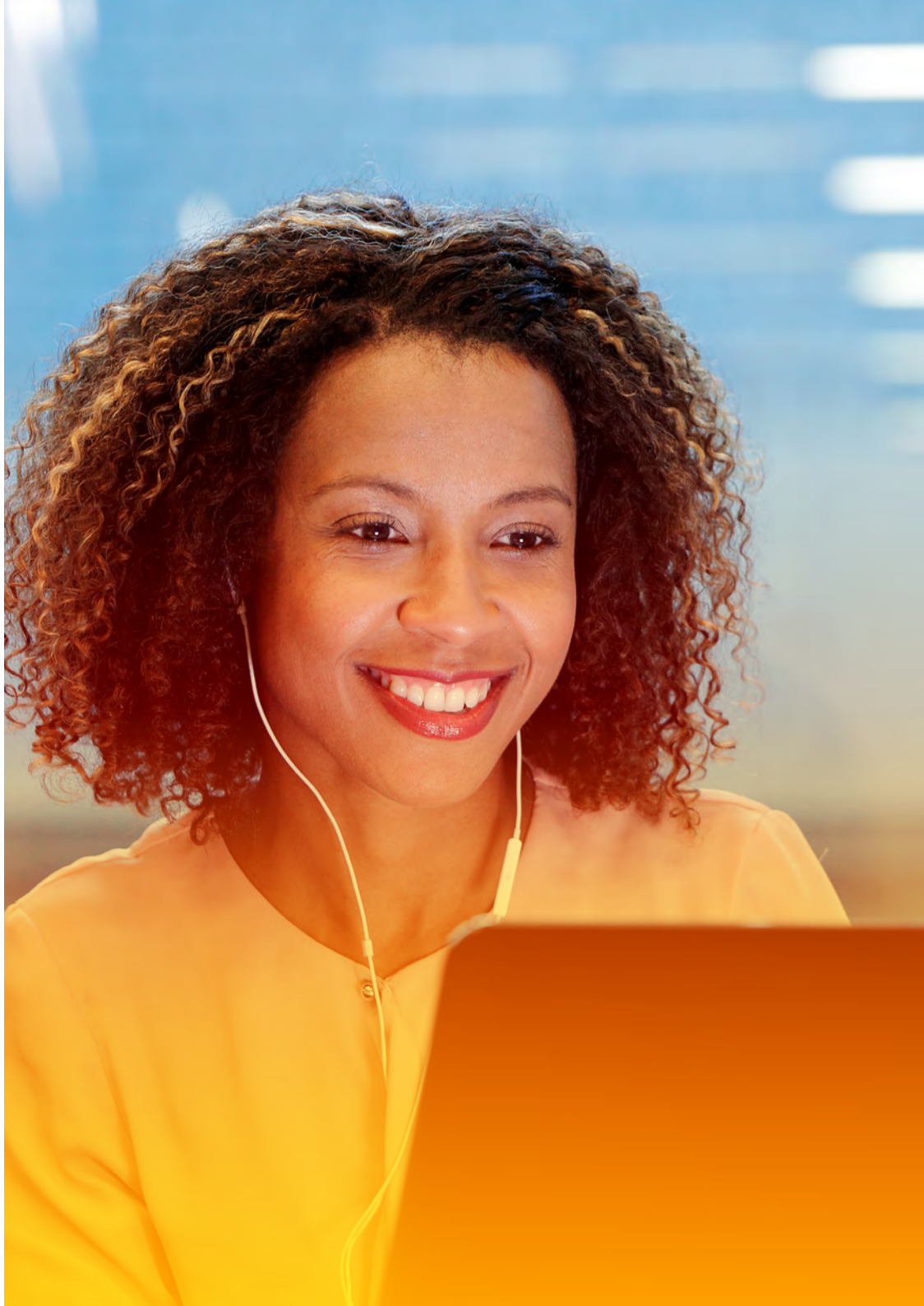
Once deployed we support our Cyber Specialists with a pathway of ongoing personal development, including QA's unique Cloud Academy, offering over 1,500 courses and certifications to continue their development.

We provide access to complementary training and certifications in Security, Cloud, DevOps, Project Management and much more through videos, quizzes, exams, hands-on labs and sandbox environments to enable them to learn and practice skills in a safe, secure environment.

CYBER ROLES

Cyber Tech Specialists are able to hit the ground running in roles including:

- Cyber Security Engineer
- Cyber Security Analyst
- Cyber Security Specialist
- Information Security Risk Analyst
- Junior Cyber Security Consultant
- SOC Analyst
- Cyber Threat Analyst
- Junior Risk Assessor
- Vulnerability Analyst
- Cyber Security Technician
- Junior Cyber Researcher
- Application Security Specialist



Contact us today to find out more

0345 074 7995

qa.com/contact