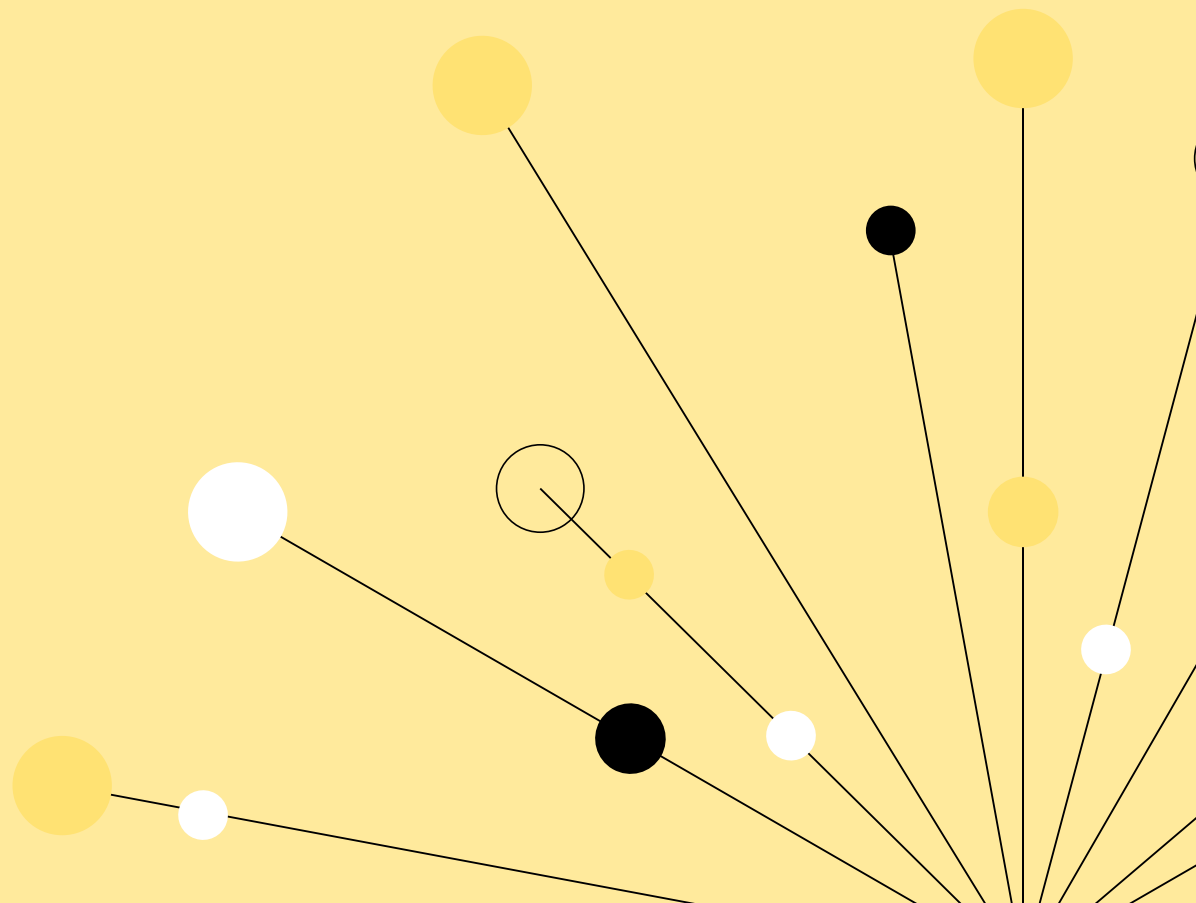# Cyber Security Engineer

Level 4 Apprenticeship

Programme Guide

QA.com

Why QA?

Endorsed by 4,000+ global clients, we are the leader in applied and cohort-based learning academies.

Today's biggest technological shifts are shaped by AI, cloud, and data.

In every technology revolution, there are winners and losers – and teams with applied skills make all the difference. We believe you can't change an organisation unless you change the capabilities of its people and ensure human and machine intelligence work together.

Success in numbers:

35+
Years of training experience

1,000+
AI, cloud & coding hands-on labs

40,000+
Careers launched & accelerated

£500M+
Levy spend invested

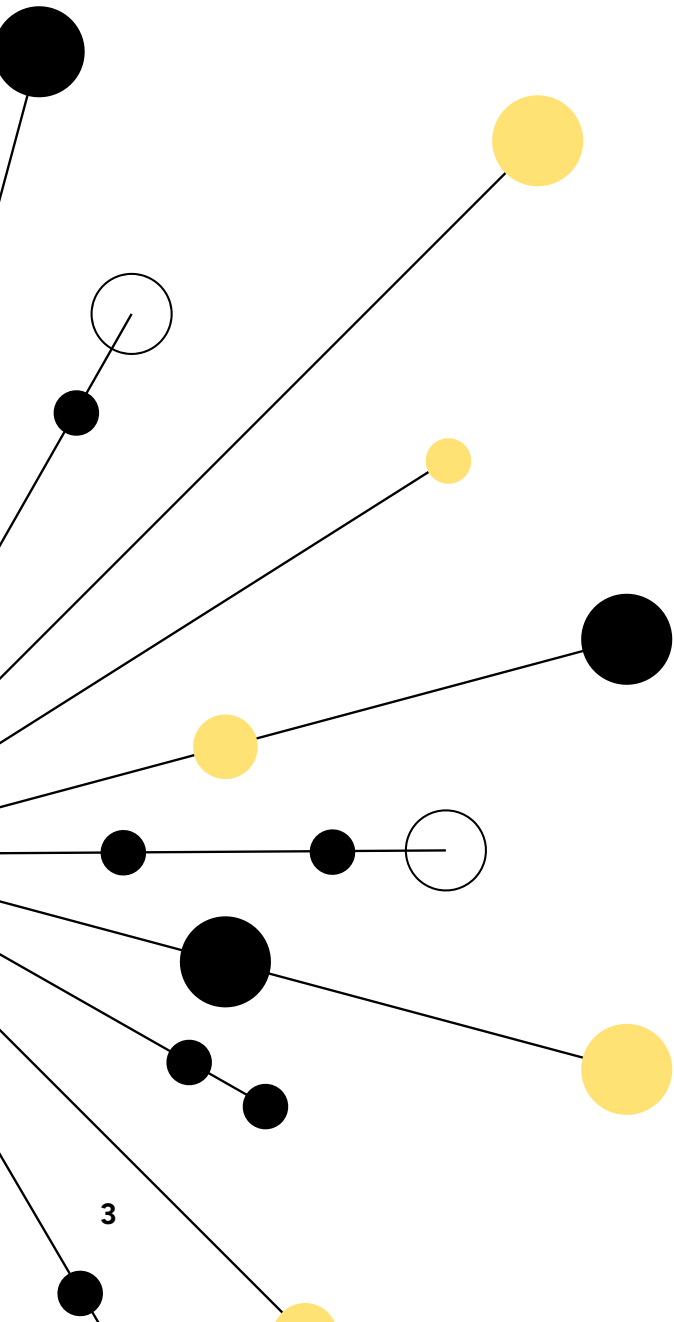**24 hours**
Feedback time for submissions

<1 minute
Response time to learner queries

**Ready to explore how QA can support you?**
Let's dive in!

Contents

Creating Change

Cybersecurity is the shield against digital threats.

This programme equips your organisation with core skills to design, implement, and secure networks, products, and systems to counter cyber threats and ensure robust controls.

Our apprenticeships drive business results by empowering organisations to apply skills consistently at speed and scale.
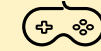
Project Ares®

Exclusive access to the award-winning, gamified platform by Circadence.

"Athena"

Interactive missions and realistic attack simulations, guided by the in-game advisor.
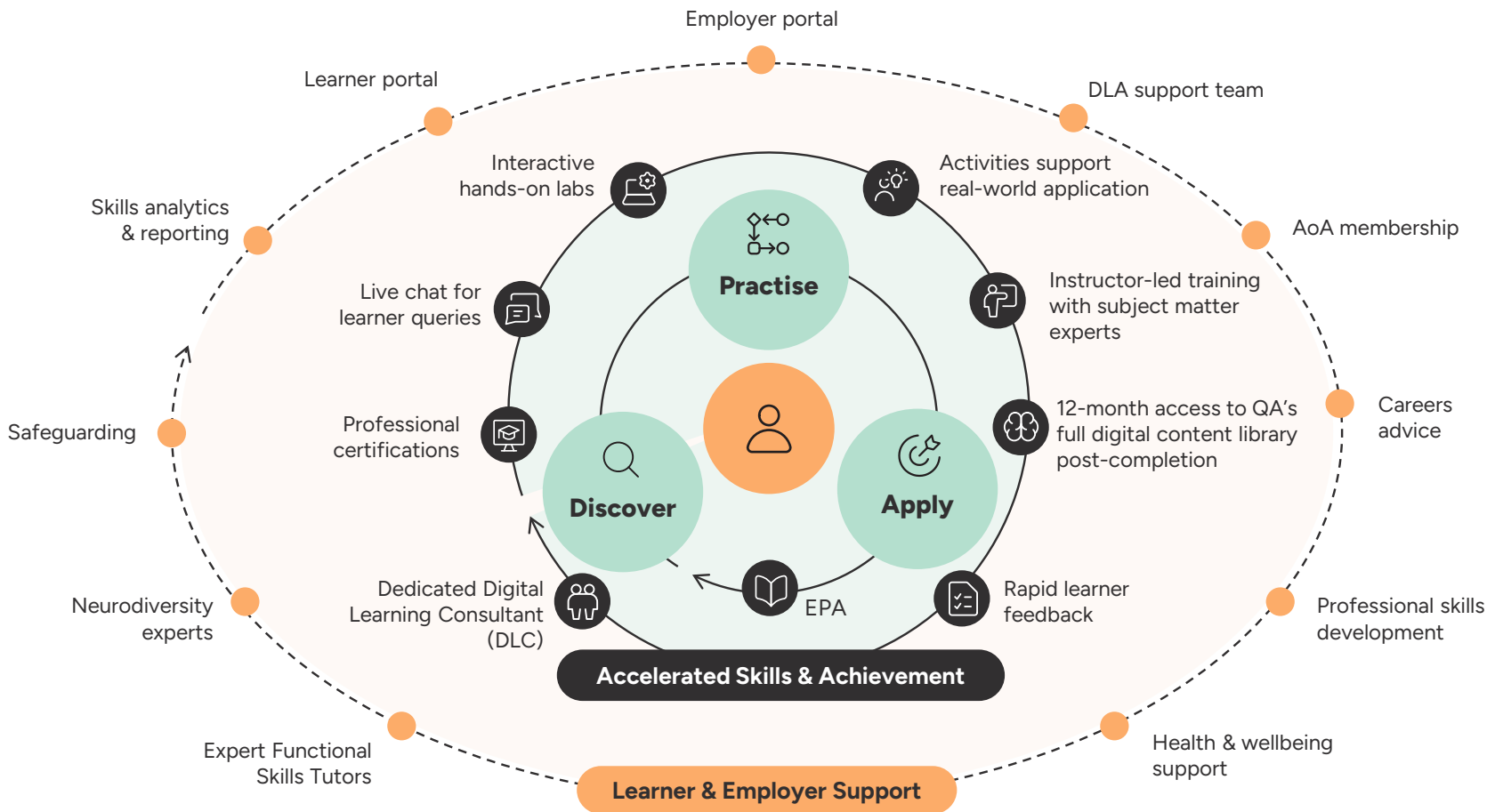
Skill Retention

Level-up cybersecurity teams and stay ahead of evolving threats.

Digital by Design

Our market-leading approach accelerates skill development and achievement through our **Discover**, **Practise**, **Apply** methodology, ensuring that both learners and employers are fully supported throughout their programme.

Employer portal

Learner portal

DLA support team

Interactive hands-on labs

Activities support real-world application

Practise

AoA membership

Skills analytics & reporting

Instructor-led training with subject matter experts

Live chat for learner queries

12-month access to QA's full digital content library post-completion

Careers advice

Professional certifications

Discover

Apply

Safeguarding

Rapid learner feedback

Dedicated Digital Learning Consultant (DLC)

EPA

Professional skills development

Neurodiversity experts

Accelerated Skills & Achievement

Expert Functional Skills Tutors

Health & wellbeing support

Learner & Employer Support

Discover

Leveraging QA's learning platform, learners follow a development path focused on their job role.

Practise

Learners come together for instructor-led training sessions, practising their skills through hands-on labs and sandboxes in a safe environment while collaborating with peers.

Apply

These practiced learnings are applied on the job through work-based activities at key and sequenced stages, fully supported and reviewed by the specialist DLC team.

5

Programme Overview

Details of standard: Cyber Security Technologist

Total cost: £18,000

Programme duration: 20 months

Live instructor sessions: 23 days

Delivered in collaboration with our strategic vendor partners:

PROJECT ARES®

DVMS Institute
NIST CYBERSECURITY FRAMEWORK
FOUNDATION
APMG International

Experience QA's self-paced learning platform with interactive labs and configurable learning.

| Cyber Security | Network Fundamentals | Operating Systems | Security Management | Defence and Cloud Security | Threat Analysis |

Learner Journey

The Cyber Security Engineer programme integrates live and online workshops with self-paced learning, employing a guided discovery approach for individual learner contexts.

Learners are assigned a Digital Learning Consultant (DLC) for personalised coaching and support. These specialists ensure their successful progress, wellbeing, and readiness for assessments.

Modules – 16 months

Module 1: Introduction to Cyber Security (6 weeks)

Module 2: Networking Fundamentals (6 weeks)

Module 3: Operating Systems with Programming and Scripting (5 weeks)

Module 4: Security Foundations (6 weeks)

Module 5: Security Management (6 weeks)

Module 6: Active Defence (5 weeks)

Module 7: Cloud Security (6 weeks)

Module 8: Threat Analysis (6 weeks)

Work-Based Project

EPA – 4 months

Professional Discussion

Scenario Demonstrations with Questioning

Work-Based Project with Report

Knowledge Test

Optional Certification

NIST Cyber Security Framework Foundation

IfATE CTS4 Qualification Award

Modules

Following each module, learners apply their newly acquired knowledge and skills to ongoing work projects.

01

Module 1:
Introduction to Cyber Security

Offers a foundational overview of cyber security and IT, with an emphasis on service management concepts.

It provides insight into the critical role of cybersecurity in today's digital landscape, the common technologies involved, and its increasing significance across industries.

Topics:

- Service Management Concepts
- Service Value Stream
- Guiding Principles
- Computing & Network Fundamentals

- Cyber Security Fundamentals
- Governance & Risk
- Security Considerations

Live Instructor Sessions: 0 Days

02

Module 2:
Networking Fundamentals

Provides discovery of networking, covering both on-premise and cloud networking infrastructures.

Topics:

- Network Operations
- Network Security
- Virtualisation & Cloud
- Network Structure & Protocols
- IP Addressing & Internet Working
- Applications & Security Management

Live Instructor Sessions: 5 Days

03

Module 3:
Operating Systems with Programming and Scripting

Explores Windows, MacOS and Linux operating systems – focusing on administration and its importance in maintaining a strong cyber security posture.

Topics:

- System Architecture
- Package Management
- Command Line Basics
- Partitions & File Systems
- Shells, Scripting & Databases
- Linux Administration
- System Services
- Networking & Security

Live Instructor Sessions: 0 Days

04

Module 4:
Security Foundations

Develops foundational cyber security skills, knowledge, and familiarity with essential tools.

Topics:

- UK Laws & Regulations
- Cryptography Basics
- Critical Security Control
- Modern Network Architecture
- Risk Management Principles
- Operation System & Application Security
- Applied Cryptography Techniques

Live Instructor Sessions: 5 Days

05

Module 5:
Security Management

Explores cybersecurity from a business perspective, from Agile fundamentals and advancing to key industry security frameworks like ISO and NIST.

Topics:

- Agile Fundamentals
- ISO 27001 & ISO 27002
- NIST Cybersecurity Framework
- GDPR & Digital Economy
- Core Functions, Categories & Subcategories
- Cyber Risks & Impact Analysis
- Security Controls & Case Studies
- Cybersecurity Improvement
- Risk & Impact

Live Instructor Sessions: 3 Days

06

Module 6:
Active Defence

Methods for identifying and countering potential attacks, including attack vectors, system vulnerabilities, and defence strategies.

Topics:

- Introduction to Attack & Defence
- OWASP Top 10
- Penetration Testing
- Encryption & Forensics
- Burp Suite Overview
- Reporting & Presentation

Live Instructor Sessions: 0 Days

07

Module 7:
Cloud Security

Examines cloud technologies and associated security implications – focusing on monitoring, data protection, and compliance.

Topics:

- Cloud Computing Fundamentals
- Web Basics
- SIEM Tools & Usage
- Cloud Concepts & Virtualisation
- Cloud Security Frameworks & Certifications
- Security Technologies: Azure, AWS, GCP
- Assurance, Data Protection & Compliance

Live Instructor Sessions: 5 Days
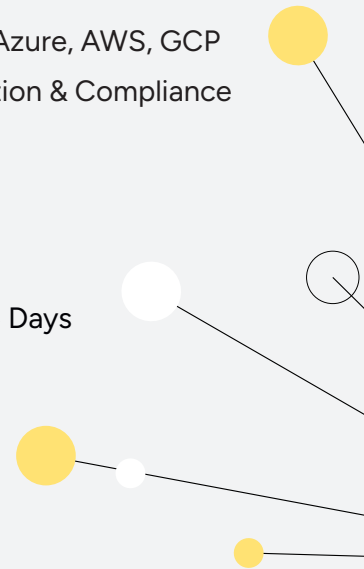
08

Module 8:
Threat Analysis

Examines threat intelligence and malware – covering advanced detection and eradication techniques.

Topics:

- Understanding Threats
- Risk Management
- Detection & Response
- Cyber Law
- Information Gathering & Analysis
- Threat Types & Futureproofing
- Horizon Scanning & Case Building

Live Instructor Sessions: 5 Days

Tools and Technologies

Network Simulation and Security Tools

- Packet Tracer
- Kali Linux
- PowerShell
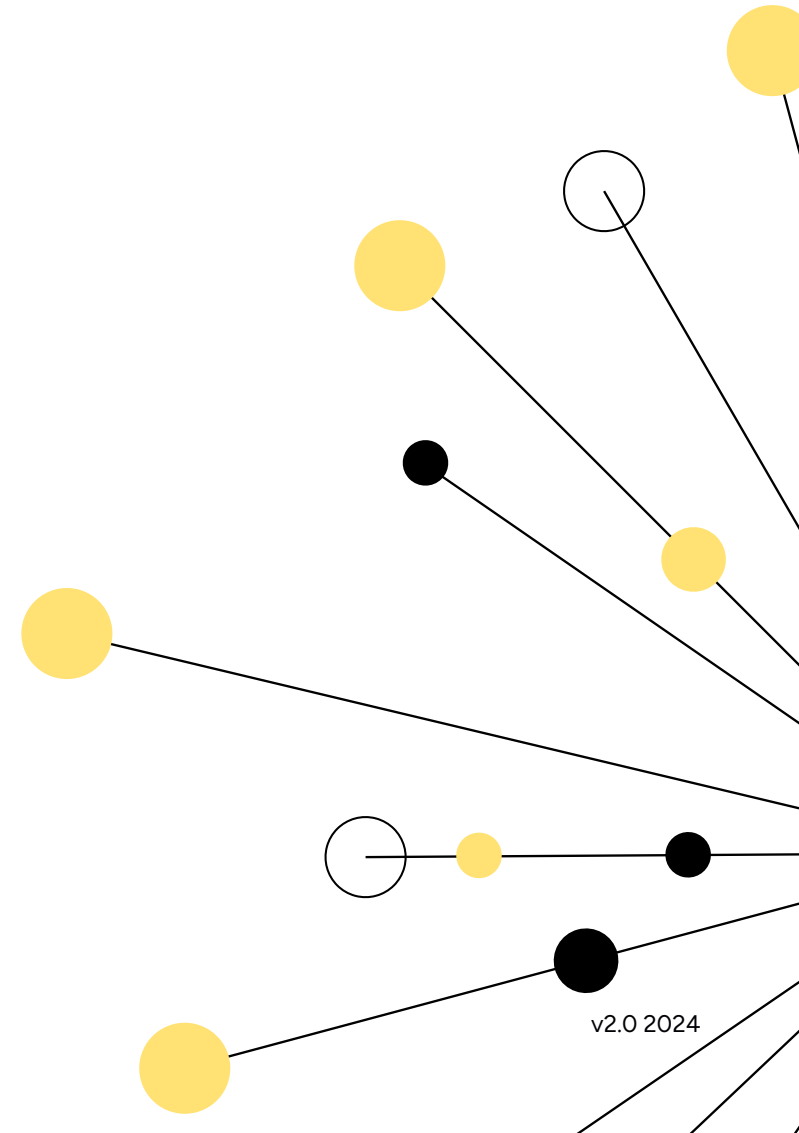
Security Information and Event Management Tools

- SEIM Tools

Cloud Platforms

- Azure
- AWS
- GCP

Remote Labs and Learning Platforms

- Project Ares
- GoToMyPC
- Learning on Demand

End-Point-Assessment

We ensure all learners are fully prepared for their End-Point-Assessment (EPA) through our internal gateway process, maximising their success rates.

Assessment criteria:

01

Knowledge
Ability to convey knowledge effectively.
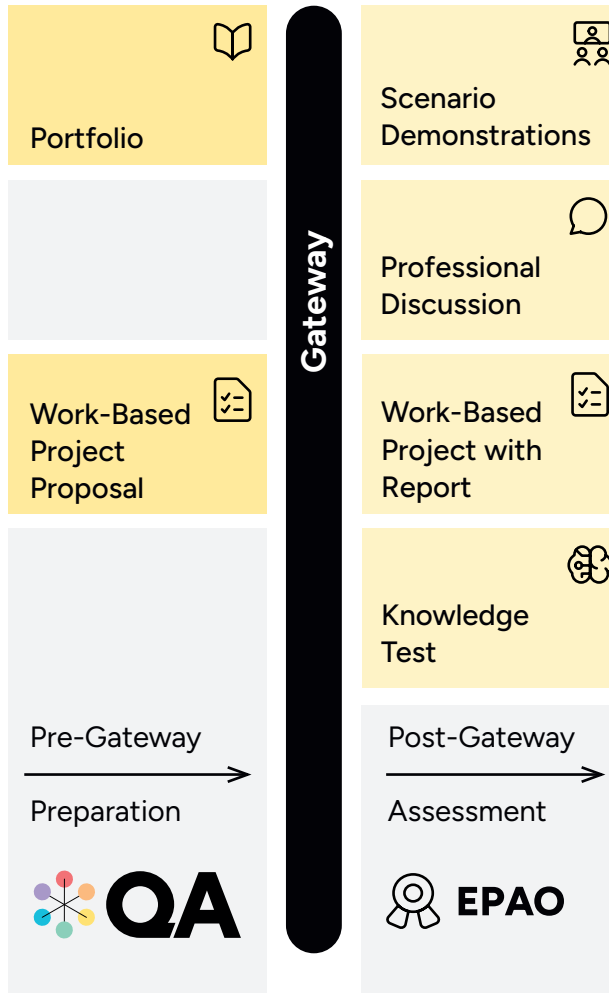
02

Skills
Demonstrate practical skills with confidence.

03

Behaviour
Exhibit professional workplace behaviour.

Explore the detailed assessment criteria within the **Cyber Security Technologist standard**.

EPA process:

Gateway

Portfolio

Work-Based Project Proposal

Pre-Gateway

Preparation

QA

Scenario Demonstrations

Professional Discussion

Work-Based Project with Report

Knowledge Test

Post-Gateway

Assessment

EPAO

Scenario Demonstrations with Questioning: Complete four scenarios, supplemented by Q&As to explain reasoning.

Professional Discussion: Engage in a formal two-way conversation to showcase knowledge, skills, and behaviours.

Work-Based Project with Report: Develop project addressing a cyber security issue with business application, supported by a report.
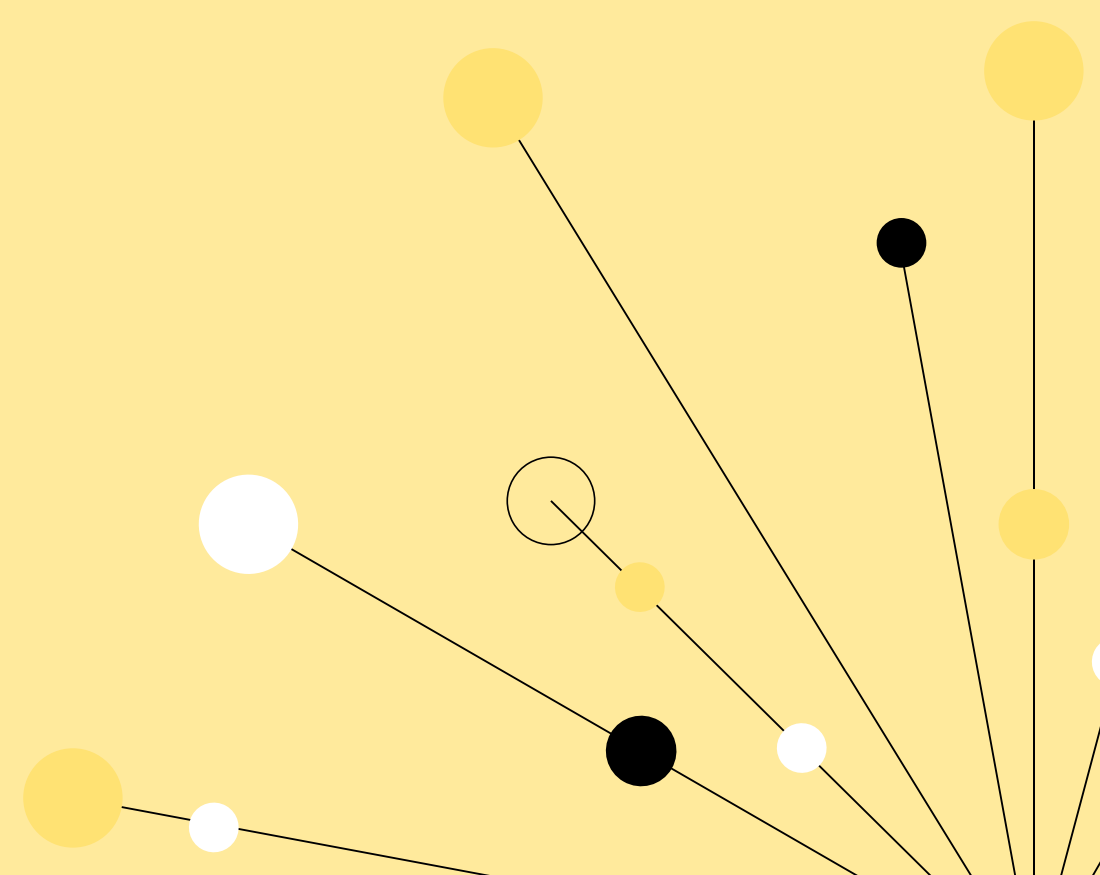
Knowledge Test: Answer multiple-choice questions aligned with key knowledge statements.

Ready to partner with us?

Let's talk:

📱 0113 220 7150

💻 qa.com/contact