THE CYBER SCHEME

IN PARTNERSHIP WITH

HACKTONICS

OPERATIONAL TECHNOLOGY SECURITY TRAINING

ACCREDITED BY THE CYBER SCHEME

THE CYBER SCHEME
ACCREDITED
TRAINING CENTRE

ACADEMIC EXCELLENCE. PRACTICAL CAPABILITY. PROFESSIONAL CONFIDENCE.

Operational Technology (OT) environments present security challenges that differ significantly from those encountered in traditional enterprise IT.

Industrial control systems support critical processes across sectors including energy, manufacturing, transport and utilities, creating a growing need for cyber security professionals who understand both technical vulnerabilities and operational impacts.

Protecting OT environments requires a different mindset from traditional IT security. Availability, safety and operational continuity are often the primary concerns, demanding specialist knowledge of industrial control systems, operational processes, legacy technologies and the evolving threat landscape facing critical infrastructure.

Hacktonics and The Cyber Scheme have partnered to deliver an accredited training pathway designed to build practical OT security capability. Combining academic expertise, specialist technical knowledge and independent professional assurance, the pathway provides a structured route from foundational understanding through to advanced technical assessment.

Whether you are new to operational technology, transitioning from an IT security background, or looking to deepen existing expertise, the pathway offers progressive development through hands-on practical exercises and realistic industrial environments. Participants develop the knowledge and skills needed to identify vulnerabilities, assess risk and help protect operational systems.

WHY THIS TRAINING IS DIFFERENT

Many cyber security courses explain operational technology concepts. Few provide the opportunity to work directly with specialist OT training environments and industrial systems.

Throughout the pathway, participants gain practical experience using Hacktonics' specialist OT training platforms, industrial control system environments and realistic attack scenarios. Learning is focused on real-world application, helping participants understand how threats emerge, how attacks can affect operational processes, and how effective security controls can be implemented in complex industrial environments.

The pathway has been designed to help participants understand not only how vulnerabilities arise, but also how they affect operational processes, system resilience, safety considerations and organisational risk. By combining theory with practical application, the training develops capabilities that can be transferred directly into operational roles.

Independent accreditation by The Cyber Scheme provides assurance that the training has been reviewed against recognised standards for course quality, delivery and relevance to professional practice, giving participants and employers confidence in the quality and practical value of the learning experience.

THE TRAINING PATHWAY

OT SECURITY TESTING – FOUNDATIONS

One-Day Course

Designed for cyber security professionals who understand IT security but are new to operational technology and industrial control systems.

Key learning outcomes include:

- Understanding operational technology and industrial control systems
- Recognising common OT assets and communication protocols
- Identifying common vulnerabilities and security challenges
- Using OT asset discovery techniques
- Understanding the operational impact of cyber attacks.

PENTESTING OPERATIONAL TECHNOLOGY SYSTEMS – PRACTITIONER

Two-Day Course

Designed for participants who have completed the Foundations course or possess equivalent knowledge and experience.

Key learning outcomes include:

- Understanding the structure of an OT penetration test
- Conducting OT asset discovery and vulnerability assessment
- Establishing and evaluating OT security baselines
- Investigating industrial protocol vulnerabilities
- Performing controlled PLC security testing exercises
- Applying mitigation strategies to improve security posture.

OPERATIONAL TECHNOLOGY SECURITY TESTING – ADVANCED

Three-Day Course

Designed for experienced OT security practitioners seeking deeper technical understanding of industrial systems, attack methodologies and security architecture.

Key learning outcomes include:

- Advanced analysis of industrial protocols
- PLC and HMI security assessment
- End-to-end OT attack scenarios
- Industrial system vulnerability analysis
- Security architecture review and risk management
- Application of security frameworks within operational environments.

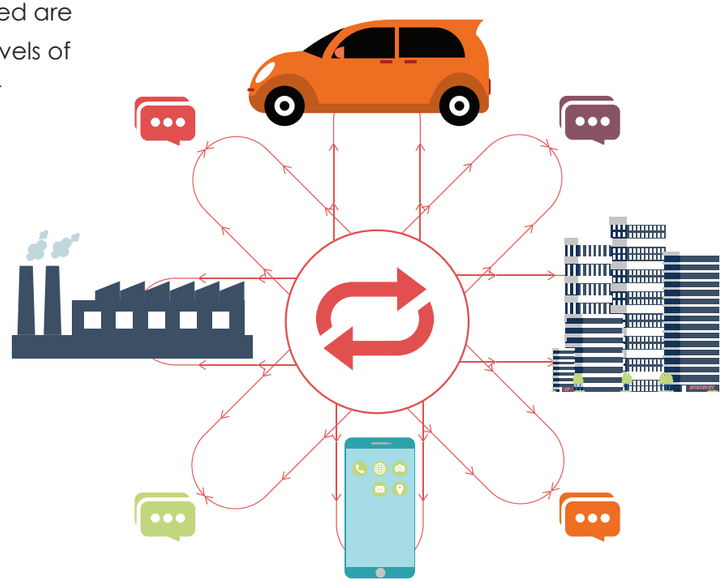
WHO SHOULD ATTEND?

This pathway is designed for cyber security professionals seeking to develop specialist capability in Operational Technology and Industrial Control Systems security. It is particularly relevant to penetration testers, security consultants, security assessors, security operations personnel, critical infrastructure teams, OT professionals and ICS specialists.

Participants should select the course level that reflects their existing knowledge and experience. Foundations is suitable for professionals familiar with IT security who are new to OT. Practitioner and Advanced are intended for those with increasing levels of OT security knowledge or equivalent experience.

THIS PATHWAY MAY BE SUITABLE FOR:

- Penetration testers
- Security consultants
- Security assessors
- Cyber security practitioners
- Security operations personnel
- Critical infrastructure organisations
- Operational technology professionals
- Industrial control systems specialists.



PRACTICAL LEARNING ENVIRONMENT

Practical capability sits at the heart of every course. Participants work with specialist OT training environments designed to replicate the technologies, protocols and devices commonly encountered within operational environments.

TRAIN IN A REALISTIC INDUSTRIAL ENVIRONMENT

Delegates gain hands-on experience using Hacktonics' specialist Lab-in-a-Box Industrial Control System training equipment and the LINICS operational technology security platform.

The training environment includes Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), industrial protocols and specialist OT security tools. Practical exercises enable delegates to explore asset discovery, vulnerability assessment, protocol analysis and attack impact within realistic industrial environments.

WHAT IS LINICS?

LINICS® is a Linux-based platform developed specifically for Industrial Control Systems security professionals. It combines specialist OT security tools alongside selected general-purpose cyber security tools in a single operational technology testing environment.

The platform enables delegates to investigate industrial assets, analyse protocols, assess vulnerabilities and better understand the relationship between technical compromise and operational impact.

Practical exercises may include:

- Asset discovery
- Vulnerability identification
- Industrial protocol analysis
- Security baseline assessment
- PLC security testing
- OT attack investigation
- Security architecture review

The focus is on helping participants understand the relationship between technical vulnerabilities, operational processes and organisational risk.

PRACTICAL INFORMATION

Do I need prior OT experience?

No. The Foundations course is designed for cyber security professionals who are new to Operational Technology. Practitioner and Advanced courses assume increasing levels of OT knowledge or equivalent experience.

Do I need to complete the previous course before attending the next level?

Not necessarily. Delegates may enter at Practitioner or Advanced level if they can demonstrate equivalent knowledge and experience.

What equipment do I need to bring?

No specialist equipment is required. Laptops and software are provided.

Can my organisation book multiple places?

Yes. Organisations interested in multiple delegate places or team bookings should contact The Cyber Scheme to discuss options.

Are accessibility adjustments available?

Yes. Please contact The Cyber Scheme before attending so that any access requirements or reasonable adjustments can be discussed.

READY TO BUILD OT SECURITY CAPABILITY?

The Hacktonics accredited training pathway provides a structured route from foundational understanding through to advanced operational technology security assessment.

Combining specialist instruction, practical learning and independent accreditation, the pathway is designed to support the development of real-world capability in one of cyber security's fastest-growing disciplines.

THE CYBER SCHEME
ACCREDITED TRAINER

ABOUT HACKTONICS

Hacktonics specialises in Operational Technology security training and the development of realistic industrial cyber security learning environments. Combining academic expertise, specialist technical knowledge and hands-on delivery, Hacktonics helps cyber security professionals develop practical capability within industrial and operational environments.

Winner of the CYBERUK 2026 Cyber Den Innovation Competition, Hacktonics has been recognised by the NCSC as one of the UK's leading cyber security innovators, reflecting its commitment to advancing OT security through research-led innovation and industry-focused training.

HACKTONICS

INSTRUCTOR PROFILES

Professor Awais Rashid

Head of the Bristol Cyber Security Group and Editor-in-Chief of CyBOK. Internationally recognised for more than 25 years of cyber security research, education and professional development.

Dr Joe Gardiner FHEA

Industrial Control Systems security specialist with extensive experience developing OT security testbeds, learning environments and practical ICS training programmes.

> "The cyber skills shortage is acute when it comes to Operational Technology (OT)"

Professor Awais Rashid
Director

THE CYBER SCHEME

ACCREDITED BY THE CYBER SCHEME

The Cyber Scheme's Training Accreditation framework supports high-quality cyber security training that is relevant to professional practice and workforce development.

Accreditation provides independent review of course structure, delivery approach, learning outcomes and overall quality, giving learners and employers confidence that training has been assessed against recognised professional expectations.

Licensed Body

UK CYBER SECURITY COUNCIL

Assured Service Provider

in association with National Cyber Security Centre

Training Course

Delivery Partner

in association with National Cyber Security Centre

Cyber Advisor Assessment Provider