



SIKER

ICS Cyber Security Training Prospectus



BELIEVE
LEARN
ACHIEVE



CONTENTS

- 1 - Cyber Security Training at Siker
- 2 - Cyber Training Portfolio at a Glance**
- 3 - What is Industrial Control Systems (ICS)
- 4 - ICS Courses**
- 5 - ICS Courses cont.
- 6 - ICS training in development**
- 7 - ICS training in development Overviews
- 8 - Contact Us**

“Siker are recognised as subject-matter experts in ICS security by the National Cyber Security Centre of the United Kingdom. Our ICS cyber security training programmes are nationally and internationally recognised.”



STEVE SHEPHERD MBE
Managing Director & Head of
Academy

CYBER SECURITY TRAINING AT SIKER

Our ICS cyber training courses have been designed by industry experts and academics. Our aim is to safeguard organisations that provide Critical National Infrastructure (CNI) from ever-growing cyber threats.

SIKER PASSPORTS

Training passports offer discounted rates across all our cyber disciplines, including OT. Simply purchase a set number of training days at the discounted rate (e.g. 160 or 240 hours) and save on the cost of booking courses individually.

TRAINING DELIVERY METHOD

Siker offers three delivery methods:

- Virtual on demand
- Virtual face-to-face
- Classroom-based (various venues)

ON-SITE TRAINING

For groups of 8 or more, we can deliver exclusive on-site (or remote) training from our existing suite of courses.

BESPOKE TRAINING

We can create bespoke training for organisations that require specific content.



ABOUT SIKER

Siker's roots began with the development of cyber training programmes for industry. Siker specialises in OT cyber security training and business development for industrial organisations, as well as in developing cyber security capability and training programmes for clients in the UK and abroad.

HOW TO BOOK YOUR PLACE ON A SIKER COURSE

Know which course you want to attend? Please press the Buy Now button on our website <https://sikercyber.com> or contact us online by emailing education@sikercyber.com. You will receive a booking form via email, which will be valid for 7 days.

OUR ICS CYBER TRAINING PORTFOLIO AT A GLANCE

Awareness

ICS110
Security Fundamentals for
OT Leaders

ICS150
ISA/IEC62443 Series of
Standards Fundamentals

Fundamentals

ICS202
ICS Security Incident
Response Fundamentals

ICS203
ICS Practitioners Security

ICS211
Leading an OT/ICS
Cyber Incident

Intermediate

Advanced

ICS405
Securing ICS: Becoming an
Industrial Cyber Security
Professional



PENETRATION TEST ENGAGEMENT

SCOPE

- External Network
- Internal Network
- Web Applications
- Wireless

OBJECTIVES

- Identify Vulnerabilities
- Gain Initial Access
- Escalate Privileges
- Maintain Access
- Achieve Domain Admin

WHAT IS INDUSTRIAL CONTROL SYSTEMS (ICS)

Industrial Control Systems (ICS) are integrated hardware and software systems that monitor, control, and automate industrial processes and critical infrastructure, including power generation, water treatment, manufacturing, oil and gas, and transport.

In today's interconnected world, the cyber risks to Industrial Control Systems (ICS) include targeted cyberattacks that can disrupt operations, damage equipment, compromise safety, and interrupt critical services. Transform your cyber defence strategy with our high-impact, nationally accredited OT courses, designed to safeguard critical national infrastructure.

PEN TEST NOTES

- ☒ RECONNAISSANCE
- ☒ SCANNING
- ☒ ENUMERATION
- ☒ EXPLOITATION
- ☒ PRIV ESC
- ☒ LATERAL MOVEMENT
- ☒ EXFILTRATION

ICS COURSES

SECURITY FUNDAMENTALS FOR OT LEADERS (ICS110)

This one-day course prepares leaders in OT or with OT accountabilities to understand the basics of OT cyber security risk and to take proactive measures to reduce that risk in their OT environments. By attending this course, you will gain fundamental knowledge that will help you lead teams to identify and, where possible, reduce cyber security risk in your OT environments, thereby supporting the continuity of operations in a safe and reliable way.



ISA/IEC62443 SERIES OF STANDARDS FUNDAMENTALS (ICS150)

This one-day course has been designed to provide those in management and engineering with an understanding of ISA/IEC 62443. ISA/IEC 62443 is an international series of standards that address cyber security for Operational Technology (OT) in automation and control systems. The standard is divided into sections and describes both technical and process-related aspects of cyber security for automation and control systems. This knowledge is vital when protecting Critical National Infrastructure (CNI).



ICS SECURITY INCIDENT RESPONSE FUNDAMENTALS (ICS202)

This two-day NCSC Assured Training course has been designed to provide practitioners with an understanding of the cyber security challenges facing their environments. This knowledge is vital when managing the day-to-day running of all aspects of security risk for those environments. The course will show how to protect Industrial Control environments and best identify and support their organisations' cyber security and risk mitigation/reduction strategies for their ICS environments.



ICS COURSES CONT.

ICS PRACTITIONERS SECURITY (ICS203)

This NCSC Assured Training, two day course has been designed to provide practitioners with an understanding of the cyber security challenges facing their environments. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments.

The course will show how to protect Industrial Control environments and best identify and support their organisations' cyber security and risk mitigation/reduction strategies for their ICS environments.



LEADING AN OT/ICS CYBER INCIDENT (ICS211)

One of the first steps in an OT/ICS cyber risk approach is to understand when an incident occurs and whether you are prepared for what could manifest. Do your teams understand who will do what, and, most importantly, who will lead the incident response effort and what they need? This course will focus on some of the challenges you may face, including understanding the difference between leading and managing the incident. Whilst the majority of the skills will be non-technical, you need to properly prepare for leading a technical team.



SECURING ICS: BECOMING AN INDUSTRIAL CYBER SECURITY PROFESSIONAL (ICS405)

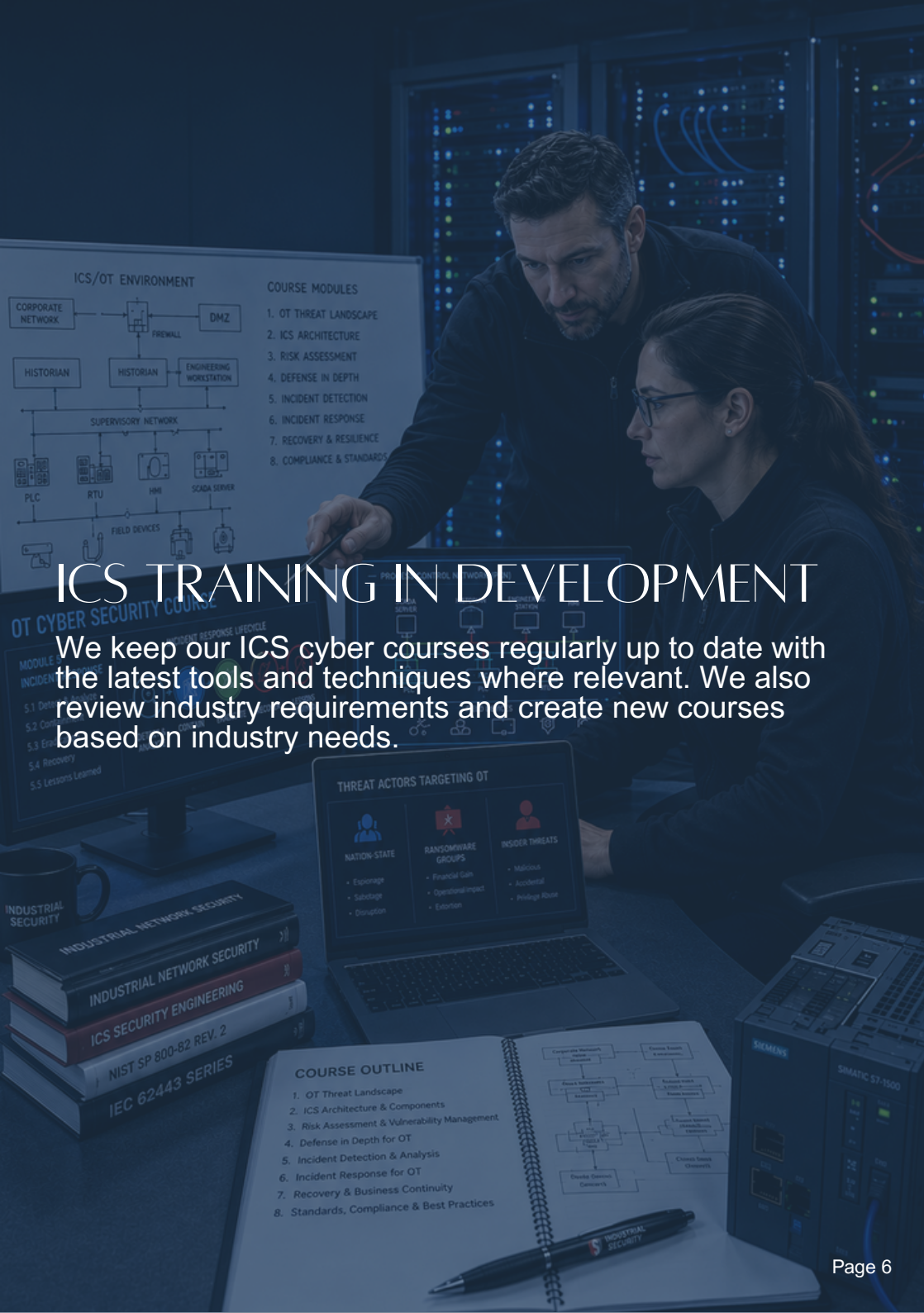
The five-day course has been designed to provide those at IT/OT operator or equivalent level with an enhanced understanding of today's cyber security challenges facing their ICS environments. This knowledge is vital for managing the day-to-day running of all aspects of security risk in those environments.

This course will show students how to combine the disciplines of IT, Operational Technology (OT), Physical Security, or Facilities Management to best support their organisations' cyber security and risk reduction strategies for their ICS environments across multiple industry sectors. In addition, it will provide students with the knowledge required to challenge the GICSP® certification.



FOR MORE INFORMATION ABOUT OUR ICS COURSES

Head over to our website: <https://sikercyber.com/ics-courses/>



ICS TRAINING IN DEVELOPMENT

We keep our ICS cyber courses regularly up to date with the latest tools and techniques where relevant. We also review industry requirements and create new courses based on industry needs.



- COURSE MODULES
1. OT THREAT LANDSCAPE
 2. ICS ARCHITECTURE
 3. RISK ASSESSMENT
 4. DEFENSE IN DEPTH
 5. INCIDENT DETECTION
 6. INCIDENT RESPONSE
 7. RECOVERY & RESILIENCE
 8. COMPLIANCE & STANDARDS



- COURSE OUTLINE
1. OT Threat Landscape
 2. ICS Architecture & Components
 3. Risk Assessment & Vulnerability Management
 4. Defense in Depth for OT
 5. Incident Detection & Analysis
 6. Incident Response for OT
 7. Recovery & Business Continuity
 8. Standards, Compliance & Best Practices

INDUSTRIAL SECURITY

INDUSTRIAL NETWORK SECURITY

ICS SECURITY ENGINEERING

NIST SP 800-82 REV. 2

IEC 62443 SERIES

ICS TRAINING IN DEVELOPMENT OVERVIEWS

INDUSTRIAL CONTROL FUNDAMENTALS FOR ALL (ICS115)

This two-day course is designed to provide an introduction to aspects of Operational Technology design and use in industrial applications. The aims of the course are to provide an understanding of ICS design, configuration, operations and maintenance principles in a real-world context. At the outset of the course, students will be presented with a statement that defines the requirement for a simple industrial process system.

LEADING AN OT/ICS CYBER INCIDENT (ICS211)

One of the first steps in an OT/ICS cyber risk approach is to understand when an incident occurs and whether you are prepared for what could manifest. Do your teams understand who will do what, and, most importantly, who will lead the incident response effort and what they need? This course will focus on some of the challenges you may face, including understanding the difference between leading and managing the incident. Whilst the majority of the skills will be non-technical, you need to properly prepare for leading a technical team.

OT SUPPLY CHAIN SECURITY

Follow-on from ICS203, this 2-day course covers detailed aspects of supply chain attacks and controls. It will introduce key topics related to supply chain attacks: device attacks, third-party access management for consumers, and secure device and software updates.

INDUSTRY 4.0 SECURITY – IIOT ENVIRONMENTS

A 2-day course covering specialised areas of IIoT architectures and the associated security risks. These risks will be mitigated through appropriately selected high- and low-level controls.

THREAT MODELLING FOR ICS PRACTITIONERS

A 2-day course covering the fundamentals of IIoT security, with a specific focus on the process of threat modelling for ICS & IIoT environments.

SECURING EMBEDDED DEVICES FOR ICS PRACTITIONERS

A 2-day course covers security topics relating to embedded devices. The core topics will include hardware, application and firmware security, and network security threats and how to mitigate them.



"I am passionate about securing Critical National Infrastructure, and Siker has designed a range of industry-recognised training courses to combat the ever-growing cyber threat towards these systems."

Tim Harwood
Chief Executive Officer



education@sikercyber.com



+44 (0)20 3441 7642



<https://sikercyber.com>



@sikercyber



<https://www.linkedin.com/company/siker-cyber>



<https://www.facebook.com/SikerCyber>

