ICS203: **ICS Practitioners Security course**

2 day course	**12** CPEs	No equipment needed

The NCSC Certified Training **ICS Practitioners Security course,** which has also been accredited as CIISec Accredited Training, has been designed to provide those at Practitioner or equivalent level with an understanding of today's cyber security challenges facing their ICS environments. This would also benefit those engaging with an ICS environment for the first time. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments.

This course will show students how to best protect and support their organisations cyber security and risk mitigation/reduction strategies for the ICS environments. All students have the option to undertake the associated exam to qualify for the **APMG 'ICS Security Foundation' digital badge**.

Siker have worked in partnership with the UK's National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI) as well as leading Critical National Infrastructure companies to produce this short course.

There are no pre-requisites for this course and a laptop is not required. In addition, a course handbook is provided.

Session Descriptions

Session 1: Background
Contents:

- An exploration of ICS terminology and a description of the elements involved
- What are the differences and similarities between IT and OT?
- What does your ICS Attack Surface look like?
- An introduction to ICS Security risk
- What Threats to your ICS exist?
- Where might your environment be vulnerable
- A discussion of ICS Security incidents

Session 2: Securing ICS
Contents:

- What is the Purdue model and how does it work in reality?
- Securing legacy and existing systems
- How to plan to reduce the security risk to your ICS environments
- Best Practice Operational Security
- How to understand Vendor and Supply Chain risk
- How to build security into the procurement process

Session 3: Security Incident Management
Contents:

- Security Incident identification
- Security Incident response
- Security Incident Recovery
- Planning and Preparation

Session 4: Cyber Incident Tabletop Exercise
Contents

- ICS Cyber Interactive exercise

Wrap Up/Exam

Who Should Attend?

- Anyone new to cyber security in an ICS environment
- Non-ICS staff who need to understand ICS terminology and how it differs from their current roles
- If you are a professional working in an ICS environment including:
  - Site/Asset Operators
  - Procurement/Contract staff
  - Supply chain staff
  - Site/Asset IT Support engineers
  - Site/Asset Physical Security/Facilities Manager staff

"A thorough and comprehensive review in a short 2-day course, highlighting many key areas to take away and review."
Bob W, Energy company attendee – Feb 2018

"Instructor very knowledgeable. mixed the learning with relevant anecdotes"
Joe C, UK Govt attendee – Apr 2021

What You Will Learn

By the end of the course you will be familiar with:

- How to identify the current and emerging threats to your ICS environments
- Where your ICS environments may be vulnerable
- What actions you may need to take to secure those environments and help reduce the risk to your organisation, nation and supply chain
- How to prepare for and handle a cyber security incident in an ICS environment
- The need for structured Security Awareness and Training

Accreditation

This course has been assessed under the NCSC Certified training scheme and Chartered Institute of Information Security (CIISec) Accredited Training scheme. Those students who pass the associated exam will qualify for the APMG digital badge for ICS Security Foundation.

Attendees can earn 12 CPEs.

CyBOK Knowledge Areas

This course aligns to the following Knowledge Areas:

- Cyber-Physical Systems
- Distributed Systems Security
- Risk Management and Governance
- Security Operations and Incident Management

What training follows on from this course?

This course is a Foundation level course, but it can also be used as preparation for more advanced training such as the Siker *ICS405: Securing ICS* course as well as the GIAC Global Industrial Cyber Security Professional (GICSP) certification.

For further information visit: https://sikercyber.com/product/ics203-ics-practitioners-security/