ICS Practitioners Security course outline (2 days)

The NCSC and CIISec certified **ICS Practitioners Security Course** is 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.

Siker have worked in partnership with the National Cyber Security Centre (NCSC), the Centre for the Protection of National Infrastructure (CPNI) in the UK and leading Critical National Infrastructure (CNI) organisations.

Who should attend?

If you are a Practitioner involved with ICS procurement/implementation/audit/maintenance or part of an ICS environment supply chain and/or people who need full awareness of the security risks to these environments, including:

- Site/Asset User or Operator
- Site/Asset IT/ICS Support engineer
- Site/Asset Physical security/Facilities Management professional

….**then this course is for you!**

It provides the attendee with the knowledge to fully understand the security risks facing your ICS environments including the Supply Chain. In addition, it discusses how to forward plan to help mitigate and reduce these risks as well as identifying and responding to a cyber incident.

Pre-Requisites

There are no pre-requisites for this course and no laptop is required. A handbook of supporting material is provided. Attendees can earn 12 CPE credits.

What you will learn on this course

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

- How to identify what current and emerging threats your ICS environments face
- Where your ICS environments may be vulnerable
- What actions you need to take to secure those environments and help reduce the risk
- How to prepare for and handle a cyber security incident in those environments

Course Duration

The course consists of 2 days classroom training. Day one covers the current and emerging ICS risk landscape and Day 2 covers operational security, risk reduction planning and Incident Response.

Course Contents

Part 1: Background (what is an ICS, what are the threats and vulnerabilities)

- ICS description and terminology
- ICS Vs IT. Differences and similarities
- Threats to ICS
- ICS vulnerabilities
- Known ICS security incidents

Part 2: Securing ICS (what can be done to secure an ICS)

- Secure architecture and design
- Securing existing and legacy systems
- Security risk management
- Operational security
- Vendor management
- Building security into procurement processes

Part 3: Security Incident Management (what to do when the worst happens and roles and responsibilities)

- Security incident identification
- Security incident response
- Security incident recovery
- Planning and preparation

Part 4: Cyber Incident Exercise

- Cyber interactive exercise

What training should follow on from this?

This course is a Foundation level course but it can be used as preparation for more advanced training such as the Siker ***ICS405: Securing ICS* course**; *SANS ICS410: ICS/SCADA Security Essentials* and the GIAC Global Industrial Control Systems Professional (GICSP) certification.

For more information go to www.sikercyber.com

Certified Training

in association with National Cyber Security Centre

iisp Accredited Course.