Securing ICS: Becoming a Global Industrial Cyber Security Professional course outline (5 days)

The **Securing ICS: Becoming a Global Industrial Cyber Security Professional (GICSP) Course** is designed to provide those at IT/operational level (or equivalent) with an understanding of today's cyber security challenges facing their ICS 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 combine the disciplines of IT, Operational Technology (OT), physical security and facilities management to show how to best support their organisations' cyber security and risk mitigation strategies for their ICS environments. In addition, it will provide the knowledge level required to challenge the GICSP certification.

Who should attend?

If you are an IT, OT or physical security professional responsible or accountable for any ICS environment and/or people working on securing these systems including:

- Business Technical/Engineering/Procurement Lead
- ICS Policy/Decision maker
- Site/Asset Single Point of Accountability (SPA) for security and/or incident response
- Site/Asset IT Manager
- Site/Asset Physical security/Facilities Management professional
- ICS Consultant
- Integration professional

….**then this course is for you!**

It provides an in-depth understanding across multiple industry sectors of what the current standards and regulations are, what the cyber risks are and the threats facing today's systems. In addition, it discusses how, through a lifecycle of a system, the need for accurate monitoring and assessment is required as well as how to forward pal to reduce these risks. Lastly, it discusses how to plan for, respond to and recover from, a cyber incident.

Pre-Requisites

There are no pre-requisites for this course and no laptop is required. However, all attendees need a good understanding of either basic IT or OT skills. A handbook of supporting material is provided which can be used by those challenging the exam.

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 manage a cyber security incident in those environments
- Prepare for challenging the GICSP exam

Course Duration

The course consists of 5 days of classroom training broken down into a mix of lectures, discussions and exercises.

Course Contents

The course follows a whole lifecycle approach for designing, implementing, monitoring and decommissioning an ICS and covers the following modules:

- ICS Basics (for non-OT attendees)
- Cyber security essentials (for the OT attendees)
- ICS security governance and security risk
- ICS Architecture
- ICS Hardening
- Access Management
- Physical Security
- ICS Security Assessments
- ICS Security monitoring
- Incident Management
- Exam Preparation

Exam

This course has been designed for an attendee to be trained to a level that allows them to challenge the GIAC GICSP certificate, although the exam is not included in the courser.

What training should follow on from this?

This course is a skilled level course that allows an attendee from either side of the firewall to have a base understanding of the 'other side' including how the same language may change and be misunderstood. There are many specialist courses that can follow on or compliment this course depending on industry sector.

For more information go to www.sikercyber.com