ICS Security Incident Response Fundamentals course outline (1 day)

The **ICS Security Incident Response (IR) Fundamentals Course** provides attendees with an understanding of the security risks to today's Industrial Control System environments and explains what can be done to prepare for, respond to and, subsequently, recover from a cyber incident that affects the control system or part of it.

The course will follow the CREST best practice guidelines, describing the 6 stage process for cyber incident management and helping attendees understand what their role in the process may be.

Who should attend?

If you are a…

- Business Technical/Engineering/Procurement Lead
- ICS user of operator
- Site/Asset Single Point of Accountability (SPA) for security and/or incident response
- Site/Asset IT support practitioner
- Site/Asset Physical security/Facilities Management professional

….**then this course is for you!**

It provides a high-level understanding of what the current cyber security risks are and how to forward plan to identify when an incident is occurring and how to respond..

Pre-Requisites

There are no pre-requisites for this course and no laptop is required. A handbook of supporting material is provided.

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
- What the 6 stage CREST process is
- How to prepare for and manage a cyber security incident in those environments

Course Duration

The course consists of 1 day of classroom training. Part one covers the current and emerging ICS risk landscape including what the indicators of compromise in recent incidents were and Part 2 covers cyber Incident Response culminating in a short table top exercise.

Course Contents

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

- ICS Vs IT. Differences and similarities and how this may impact the IR process
- Current and emerging risks to ICS
- Known ICS security incidents

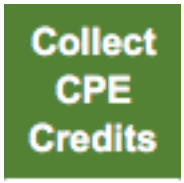
Part 2: Securing Incident Management (what to do when the worst happens!)

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

Part 3: Incident Exercise

- Interactive table top cyber incident exercise

Continuing Professional Development



Attendees who require to record CPE credits e.g. (ISCI)², IET, ISACA, etc can earn 7 CPE credits for attending the course. Individuals are responsible for entering accurate membership or ID numbers on registration to ensure that relevant details are included on course certificates.

What training should follow on from this?

This course is an awareness level course but it can be used as preparation for more advanced training such as the Siker ***ICS203: ICS Practitioners Security*** course and ***ICS405: Securing ICS*** course and the GIAC Global Industrial Control Systems Professional (GICSP) certification.

For more information go to www.sikercyber.com