ICS Security Incident Response Fundamentals

Course code: ICS202

2 days	12 CPEs	No equipment needed

The **ICS Security Incident Response Fundamentals** course has been designed to provide those at Practitioner or equivalent level with an understanding of the current cyber incident response challenges facing their ICS environments. This includes an understanding of what an Incident is and how this approach may differ in an ICS Environment. This would also benefit those participating in or engaging with an ICS Incident Response team for the first time. This knowledge is vital when managing the day to day running of all aspects of security incident response for those environments.

This course will show students how to best protect and support their organisations cyber incident response process and provide an understanding of the stages of the IR process, including the information required to be able to create an effective IR plan (based upon the ICS4ICS processes). Template plans will be provided for student to complete and take away.

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.

Who Should Attend

- Anyone new to cyber security in an ICS Incident Response 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

What you will Learn

We want staff who may be called in to help resolve a cyber incident to understand what it is they are walking into. This will help calm the panic and provide a swifter response to the incident which, in turn, leads to a quicker return to normal operations. This includes:

- Being able to articulate the difference between an Incident and an Event and be able to identify both.
- Understand the 6-stage process for Incident Response
- Identify the key roles that make up a standard Incident Response Team
- Understand the legal and regulatory aspects of cyber incident response
- Handle different types of incidents

Session Descriptions

Session 1: Introduction to the Incident Handling Process
Contents:

- What is an Incident and an Event and how do they differ?
- What is Incident Response?
- The challenges of ICS Incident Response
- The IR lifecycle

Session 2: Preparation
Contents:

- Obtaining Leadership support
- ICS IR Plans
- Who gets involved?
- What makes the CSIRT?
- Jump Kit and Grab Bags

Session 3: Identification
Contents:

- Classification Levels
- Managing the Information Flow
- Evidence

Session 4: Containment
Contents:

- What is Containment?
- Short-term Containment
- Long-term Containment
- Investigations

Session 5: Eradication
Contents:

- The main aims of eradication
- Remove or restore?
- Improvement after

Session 6: Recovery
Contents:

- Recovery Objectives
- Validation
- Post-Incident Monitoring

Session 7: Lessons Learned
Contents:

- The Report
- Management Considerations
- Bringing it all together

Pre-Requisites

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