Leading an OT/ICS Cyber Incident

1 day | **No equipment needed**

Course code: ICS211

One of the first steps in an OT/ICS cyber risk approach is to start with an understanding of when an incident happens, are you prepared for what could manifest? Do your teams understand who will be doing what and, most importantly, who will lead the Incident response effort and what do they need.

This course will focus on some of the challenges you may face including understanding the difference between Leading and Managing the incident. Whilst the majority of the skills will be non-technical, you need to properly prepare for leading a technical team.

Who Should Attend?

If you are in a position where you may be called upon to lead an Incident Response acting as Incident Commander, then this course is for you. This could include newly promoted OT/ICS senior staff who want to ensure they understand the OT/ICS Cyber incident management process better.

What You Will Learn.

This course will examine the requirements of those who may be called in to lead an Incident including:

- What is an OT/ICS Cyber incident?
- What is the difference between an Event and an Incident?
- What is the difference between Managing and Leading?
- What makes an Incident Commander?

This course will benefit your organisation by providing you with the means to lead a cyber incident management team working within a complex OT/ICS environment. It will promote an understanding of the need for a unified approach to leading including the need for integrated command, communication and information/intelligence sharing.

Prerequisites.

This course covers the main subject areas of cyber incident response and because of the limited time, assumes a basic knowledge of most of the relevant areas. For those who may be new to the role or maybe have only minimal knowledge, it is recommended that you undertake the Siker course - ICS202: ICS Cyber Incident Response Fundamentals.

Course Outline.

The course will cover three main sessions with multiple breakout exercises.

Session 1 – What is an OT Incident?

- What is an Incident?
- How could it differ between OT and other business areas?
- How does an attack develop?
- What are the main Incident Response methodologies?

Session 2 – To Lead or Manage?

- What is the difference between Leadership and Management?
- Introduction to the Planning P.
- Who comprises an IR team?
- How to calculate Severity Level.

Session 3 – Being an Incident Commander.

- What is an Incident Commander?
- What are they responsible for?
- What is an Incident Action Plan?
- Communication!