Industrial Cybersecurity Training programs

kaspersky

Digital forensics and incident response in ICS

ICS presents many specific challenges and constraints when it comes to digital forensics. Tools and technologies developed for IT environments are often inappropriate or simply useless. Thus, evidence collection, for example, becomes a manual process. In addition, special attention must be given to rapidly regaining control and bringing the system or devices back to a safe state. Working with our digital forensics specialists, participants will explore the unique aspects of ICS digital forensics. The course content ranges from identifying a genuine incident to data collection, examination, analysis and reporting in industrial environments, developing the hands-on skills and approaches required to become an expert investigator of ICS incidents.

Learning objectives

- Conduct successful forensic investigations in ICS environments
- Create an effective Digital Forensics plan for an ICS environment
- Collect physical and digital evidence and deal with it appropriately
- Apply the specific tools and instruments of digital forensics to ICS software (SCADA) and hardware (PLC)
- Find traces of intrusion based on uncovered artifacts
- Reconstruct incidents and use timestamps, including timestamps from ICS software and hardware
- Provide expert reporting and actionable recommendations

Course topics

Day 1: Incident response basics and differences between IT and OT digital forensics
Day 2: ICS network protocols and device architecture, threat hunting in ICS networks
Day 3: Digital forensics in X86/X86 systems, including ICS-specific software, threats and risks
Day 4: Digital forensics in OT devices, case study based on publicly known attacks and Kaspersky investigations
Day 5: Lab work simulating real-world investigations

Training prerequisites

All course participants need to an understanding of IT administration, networking and security practices. System administration skills for Windows, Linux, and Virtual Systems are also necessary.
It is desirable, but not necessary to have malware analysis skills, as well as knowledge about the architecture of industrial control systems, their protection and security problems.

Course format

Onsite instructor led lessons with presentations and case studies, hands-on exercises

Duration

5 days

Group

Up to 10 people

Who can benefit:

- IT and OT IS professionals
- Fraud Investigators
- Auditors
- CSIRT and SOC analysts who would like to become ICS Digital Forensics professionals and understand the major differences between IT and ICS digital forensics strategies
- Police and military personnel and other security personnel who deal with cyber investigations in ICS environments