Industrial Cybersecurity Essentials Training Programs

[illegible]

Industrial Cybersecurity

Industrial Cybersecurity Basic Training

Course topics

- Differences and similarities between IT & OT security, discovering OT architecture information security basics: attacks, vulnerabilities, exploits & malware, threats
- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Attacker profiles for IT & OT
- Security policies & procedures
- Handling security incidents properly and in a timely manner
- Recognition of social engineering

Takeaways

- Information security basics: attacks, attacker profiles, threats, vulnerabilities, etc.
- How to recognize cyber security incidents, malware and social engineering attacks
- Cybersecurity rules and measures & recommendations for daily work

Course format

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

Duration

1 day

Group

10 - 25 people

More training options

For bigger groups of people, we recommend considering the online training on the Kaspersky Automated Security Awareness Platform, where all basic cybersecurity topics are covered, including a dedicated module on industrial cybersecurity. Visit k-asap.com to register for a free trial.

kaspersky

Industrial Cybersecurity Advanced Training

Course topics

- Overview of the current threat landscape, security issues, human factors, ICS network attacks
- Attacker profiles for IT & OT
- Differences and similarities between IT & OT security
- Providing recommendations on the implementation of Defense in Depth
- Network security in IT and ICS environments – special considerations
- Industrial network protocols
- Prevention, detection and mitigation techniques
- Compliance with industrial standards and legislation
- Cybersecurity roles and team structures
- Third party trust relationships
- Isolated network security
- Security incident response plan
- How the evolution of the Industrial Internet of Things (IoT) can affect ICS security

Takeaways

- Hardening measures & recommendations
- Recognizing and identifying security incidents
- Performing basic investigations
- Handling security incidents properly and in a timely manner
- Detailed investigation of real SCADA cybersecurity incidents
- Drawing up and implementing an effective incident response plan
- Countermeasures: segmentation, firewalling, access control for devices, users, services, etc.
- Malware attacks + APTs (Advanced Persistent Threat) + social engineering

This course includes highly customizable elements and can be adapted to run for 1 or 2 days, as preferred

Course format

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

Duration

2 days

Group

10 - 25 people