Fraunhofer IOSB

Applied Industrial Cybersecurity

2020

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Applied Industrial Cybersecurity

Building cybersecurity expertise among IT/OT managers and engineers

Audience

- Information Technology (IT) managers and engineers
- Operational Technology (OT) managers and engineers

Course Prerequisites
Participants should have a basic understanding of the relevant technologies, communication networks and security.

Methods
Interactive modules, games, hands-on exercises, attack examples, simulations on a real hardware setup, hacking demonstrations and great trainers with practical experience and in-depth knowledge.

Education initiative by Kaspersky and Fraunhofer IOSB

Kaspersky and Fraunhofer IOSB are working together to address industrial cybersecurity and awareness challenges. Faced with a significant security skills shortage in the field of industrial control systems and operational technology, the provision of quality content for specialists looking to develop their careers has never been more important.

Kaspersky and Fraunhofer IOSB have collaborated to develop new training courses for IT/OT managers and engineers. The "Applied Industrial Cybersecurity" course is based on the combined knowledge and technical expertise of Kaspersky and Fraunhofer IOSB.

Objectives of the 2-day training

- Grasp the differences between IT and OT networks and learn how to bridge the gaps
- Experience the impact of ICS vulnerabilities (including hacking demos)
- Recognize incidents in an OT environment and initiate an appropriate response
- Master advanced topics on industrial networks, information security and countermeasures
- Understand risk management processes, procedures and outcomes
- Get to know basic defense measures and how to apply them

Our training courses can be customized according to your requirements.

Objects to discover

Industrial Control Systems (ICS)

IT and OT networks

ICS vulnerabilities

Security measures

Attacks and attacker perspectives

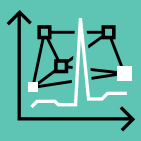
Defender perspectives

Risk management

Incident handling

Applicable laws and standards

Understanding



Nature of incidents, security, safety, defense in depth

Roles and responsibilities of information security professionals

Risk management processes and procedures

Need for compliance with regulations and standards

Need for trust in third parties/supply chain

Security policy

Patch strategies

Differences between IT and OT

Knowledge

Industrial Networks: typical topology, components, protocols, design practices

Information security: attacks, attacker profiles, threats, vulnerabilities,

Countermeasures: segmentation, firewalling, access control for devices, users, services

Hardening measures and recommendations

Malware attacks, APT, social engineering

Incident handling

About Kaspersky ICS CERT

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things.

Contact us at ics-cert-query@kaspersky.com.

About Fraunhofer IOSB

Established on January 1, 2010, the Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation (FH) grew to become Europe's largest research institute in the field of image acquisition, processing and analysis. IOSB's other areas of activity include control and automation technology, and information and knowledge management.
The three core competencies of Optronics, System Technologies and Image Exploitation give the institute its distinctive profile. FH's IT security lab for industrial automation provides an ideal test environment to simulate real-world scenarios and analyze the effects. To this end, the IT security lab includes a specific smart factory with genuine automation components controlling a simulated production plant. All the network levels of a factory environment, including typical components such as Industrial Ethernet, industrial firewalls and wireless components, are in place.

Learn more at www.iosb.fraunhofer.de.

About Kaspersky

Kaspersky is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and the consistency of industrial processes.

Learn more at www.kaspersky.com.

Kaspersky ICS CERT: ics-cert.kaspersky.com
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com