Fraunhofer IOSB

Building cybersecurity expertise amongst IT/OT managers and engineers

Education initiative by Kaspersky Lab and Fraunhofer IOSB

Audience

- Information Technology (IT) specialists
- Operational Technology (OT) specialists
- Information Security (IS) specialists

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 and great trainers with practical experience and deep knowledge.

Objectives of the 2-day training

Participants will learn:
- The difference between IT and OT networks
- How to bridge the gaps (understanding) between IT and OT
- How easy it is to launch an attack (including simple hacking demos)
- Basic defense measures and how to apply them
- Applicable laws and standards

Participants receive a certificate upon successful completion of the course.

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

Objects to discover	Understanding	Knowledge
IT and OT networks	Roles and responsibilities for information security professionals	Network basics: typical topology, components, protocols, design practices
Industrial Control Systems (ICS)	Risk management process/procedures/ outcome	Information security basics: attack, attacker profile, threat, vulnerability, etc.
Security measures	Need for compliance with regulations and standards	Countermeasures: segmentation, firewalling, access control for devices, users, services, etc.
Attacks	Need for trust in third parties/supply chain	Malware attacks + APT + social engineering
Attacker view	Nature of incidents, security, safety, defense in depth	Hardening measures and recommendations
Defender view	Security policy	
	Patch strategies	
	IT ⟷ OT	

The skills developed in our training will enable participants to:

- Recognize the relevance of ICS vulnerabilities
- Recognize social engineering, phishing
- Recognize an incident in an OT environment and initiate an appropriate response
- Use selected tools for incident handling
- Configure an industrial firewall, IDS, etc.
- Analyze control network traffic, recognize protocols and monitor them

Our training courses can be customized according to your requirements, provided in your organization or company.

Advanced Industrial Cybersecurity in Practice

Want to learn more? Contact us:

Contact – FH: christian.haas@iosb.fraunhofer.de;
gerhard.sutschet@iosb.fraunhofer.de

Contact – KL: Dmitry.Petrovichev@kaspersky.com;
Christel.Gampig-Avila@kaspersky.com

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky Lab'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 ics.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 are control and automation technology, and information and knowledge management. 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.

www.kaspersky.com

Kaspersky® Industrial CyberSecurity

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/ics**