KASPERSKY lab

Kaspersky Industrial CyberSecurity Training and Awareness Programs

www.kaspersky.com/ics

Leverage Kaspersky Lab's industrial cybersecurity knowledge, experience and threat intelligence through these innovative educational programs.

Human error is responsible for around 80% of all cybersecurity incidents. When these incidents can lead to the breakdown of critical systems or can bring industrial processes to a complete halt, human error becomes expensive and potentially lethal.

In an environment where the threat landscape is constantly evolving, and targeted attacks capitalizing in human weakness are on the increase, one of your best defenses is a workforce for whom cyber-safe working practices are automatic and instinctive.

To achieve this, all your employees need to have a basic awareness of the dangers, and of how to work securely. Those directly engaged in IT/OT cybersecurity must also possess the advanced skills essential to effective threat management and mitigation, as well as to prevention and detection.

Kaspersky Industrial CyberSecurity Training and Awareness courses have been developed specifically to enable critical infrastructure operators, utilities providers and manufacturing businesses to better protect their industrial environments against the disruption and damage caused by cyber-incidents and attacks.

THE COURSES

(All training courses are offered in English)

<table>
<tr><th>CyberSecurity Awareness</th><th colspan="2">CyberSecurity Skills Development and Training</th></tr>
<tr><td>For your Engineers / Industrial Floor Workers:</td><td>For IT/OT Professionals:</td><td>For IT/OT Security Professionals:</td></tr>
<tr><td>Basic Cybersafety</td><td rowspan="3">Advanced Industrial CyberSecurity in Practice</td><td>ICS Penetration Testing for Professionals</td></tr>
<tr><td>For Management:</td><td rowspan="2">ICS Digital Forensics for Professionals</td></tr>
<tr><td>Industrial Cybersafety Games</td></tr>
</table>

INDUSTRIAL CYBERSECURITY AWARENESS

On-site and online interactive training modules and cybersafety games training for all employees who interact with industrial computerized systems – on the industrial floor, control room or in the back-office – and for their managers.

Organizations spend millions on cybersecurity awareness programs, but few CISOs are really satisfied with the results. What's wrong?
Most cybersecurity awareness training is too general, too long, too technical and essentially negative. This does not play to people's core strengths – their decision-making and learning abilities - and as a result can render training ineffectual. And it doesn't reflect the real-world cybersecurity challenges specific to industrial workforces.

So organizations are seeking more sophisticated behavioral support approaches (such as corporate culture development) that focus on issues specific to their working environment and deliver a quantifiable and worthwhile return on their investment.

Kaspersky Lab Industrial CyberSecurity Awareness courses work by:
- Changing behavior – stimulating the individual's commitment to working safely and responsibly, building a corporate environment where "I care about cybersafety, because everyone does here – it's part of the job".
- Combining a motivational approach, gamification, learning techniques, simulated attacks based on real-life industrial situations, and in-depth interactive cybersecurity skills training.

HOW IT WORKS – IN DETAIL

Comprehensive but straightforward – Training covers a wide range of security issues, from basic cyber-hygiene rules to malware attacks, data leaks and safe social networking, through a series of simple exercises.
We use learning techniques – group dynamics, interactive modules, and gamification based on real-life industrial workplace scenarios – to make the learning process engaging and relevant.

Accessible – Our 1-day Cybersafety Awareness course can be taught on-site or at any venue, while Kaspersky Industrial Protection Simulation (KIPS), our Industrial CyberSecurity Gaming program, is designed to be played on-line or face-to-face as preferred. To ensure an immersive, real-world learning environment, there are specific KIPS variants for different industries, such as water treatment, or power generation and transmission.

Continuous motivation – We create teachable moments by gamification and competition, and then re-enforce these training moments throughout the year via online simulated attack exercises, assessment and training campaigns.

Changing beliefs – Employees learn the importance of their own role in protecting against specific threats – how they can avoid becoming victims and exposing themselves and their workplace to danger and to attack.

Building a corporate cybersafety culture – We train management to become security advocates; a culture where cybersafety becomes second nature is best achieved through management commitment and example, and cannot simply be imposed.

Positive and collaborative – We demonstrate how cybersafety practices make a positive contribution to overall operational efficiency and productivity, and promote more effective cooperation with other internal departments, including the IT/OT Security team.

Measurable – We provide tools to measure employee skills, along with corporate-level assessments analyzing workforce attitudes to cybersecurity in their daily work.

CYBERSECURITY SKILLS DEVELOPMENT AND TRAINING

These courses offer a broad curriculum in cybersecurity topics and techniques for those directly involved with, or planning to be involved with, the security of industrial systems and technologies. All are available either in-class on customer premises or at a local or regional Kaspersky Lab office, if preferred.

Participants benefit from working and learning alongside our global experts, who provide inspiration through their own experience at the 'sharp end' of cybercrime prediction, prevention, detection, and response.

Courses include both theoretical classes and hands-on 'labs'. On completion of each course, participants will be invited to complete an evaluation to validate their knowledge.

GROW YOUR ORGANIZATIONAL EXPERTISE

These training courses allow organizations to improve their cybersecurity knowledge pool in three main areas:

- Fundamental knowledge of industrial control systems cybersecurity
- ICS Penetration Testing
- ICS Digital Forensics

Advanced Industrial CyberSecurity in Practice
Provides your IT/OT professionals with a new insight into your threat landscape and the attack vectors targeting your industrial environment, and arms them with all the skills needed to draw up a basic incident response plan.

ICS Penetration Testing for Professionals
Enables IT/OT security professionals to conduct comprehensive and thorough pentests in industrial environments, and to make expert recommendations for appropriate remedial action.

ICS Digital Forensics for Professionals
Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments, and to provide expert analysis and recommendations.

THE COURSES IN DETAIL

Topics	Duration	Outcomes/Skills Gained
Advanced Industrial CyberSecurity in Practice		
• Overview of current threat landscape, security issues, human factors, ICS network attacks • Network security in IT and ICS environments – special considerations • Case study demonstrating the use of prevention, detection and mitigation techniques • Compliance with industrial standards and legislation • Network topologies and how network security technologies work • Cybersecurity roles and team structures • Common security mistakes.	1 – 2 days	• Understand current industrial cyberthreats and how to combat cyber-incidents targeting your industry or organization • Recognize and identify security incidents • Perform simple investigations • Draw up and implement an effective incident response plan. This course includes highly customized elements, and can be adapted to run over 1 or 2 days as preferred. Leads to certification.
ICS Penetration Testing for Professionals		
• Introduction to ICS components, architectures and deployment in industries including: – Electric power generation & distribution – Oil & Gas – Transportation • Practical pentesting techniques as applied to these and other ICS environments • Creating an ICS Pentest Plan – considerations and constraints • Information gathering • SCADA and PLC systems vulnerability analyses • Results analysis and reporting • Practical Labs.	5 days	• Understand and analyze vulnerabilities in industrial control systems • Create an effective ICS Pentesting Plan • Conduct safe, successful pentests on SCADA, PLCs and other elements of ICS • Make expert recommendations for remedial action. Leads to certification.
ICS Digital Forensics for Professionals		
• Introduction to ICS components, architectures and deployment in industries including: – Electric power generation & distribution – Oil & Gas – Transportation • Recognizing and working with the challenges and constraints of ICS • Digital Forensics techniques as applied to ICS environments • Creating an ICS Digital Forensics Plan • Manual forensic data acquisition and preservation – working with RTOS and ICS protocols • Artefacts analysis and anomaly verification • Reporting • Practical Labs.	4 days	•Conduct successful forensic investigations in ICS environments. • Create an effective Digital Forensics Plan for ICS • Collect physical and digital evidence and deal with it appropriately • Apply the tools and instruments of digital forensics to SCADA and PLC • Find traces of intrusion based on artefacts uncovered • Reconstruct incidents and use time stamps • Provide expert reporting and actionable recommendations. Leads to certification.

KICS-Education Whitepaper, December 2016