



Limes Academy

List of Courses 2020/2021



LIMES
SECURITY

What Limes Academy Offers

Through Limes Academy, we offer training packages in the following areas: **Security Awareness, Industrial/OT Security and Security Engineering.**



Security Awareness Training

Starting from page 10



Industrial/OT Security Training

Starting from page 16



Security Engineering Training

Starting from page 26

Why Limes Security?

All Limes Academy classes are held by our experienced industrial security experts, bringing you a combined experience of over a decade in industrial cybersecurity through education and consulting practice. You benefit not only from excellent training content,

but also from a wealth of practical experience. Additionally, every class includes practical exercises, making the respective topics even clearer and more tangible for the participants.

+ Interactive training

The trainings are deliberately designed to spark participant discussion. By engaging in considerations of their own and exchanging viewpoints with others, participants retain much more of the knowledge conveyed during the training.

+ Professional expertise

All classes are conducted by our seasoned security experts who bring a great deal of experience from everyday project work.

+ Exercise labs

In practical exercises we simulate attack and defense scenarios.

+ Training material

The course materials are provided in high quality color printing so that you can take the knowledge straight home with you.

+ In-house classes

We offer individually customized classes for your employees.

+ International security training institutes

Limes Security provides security trainers for the renowned SANS Institute and TÜV®.

+ Certification

At the end of every training, participants receive a certificate of completion. For some courses it is possible to obtain a TÜV® personal certificate by passing an official exam.

About Limes Security

Limes Security is a highly professional consulting firm that has achieved a clear market position within a few years through consistently good work. Limes Security stands for professionalism and methodical know-how at the highest level. The company's goal is the highest possible level of security, specializing in vendor-independent, customized security solutions in the areas of secure software development and industrial security. Limes Security GmbH is an owner-operated compa-

ny. The Limes Security team consists of top experts with years of experience in challenging projects. Without exception, the consultants at Limes Security are professionals trained at the best universities and technical colleges in Europe and abroad, and are closely networked with the international security community. Many years of experience in cyber security in an industrial environment are at the service of Limes Security clients.

Our Services

Regardless of whether you are a world market leader in wind energy, a software development company or an Internet of Things pioneer, global player in industrial plant construction or urban infrastructure operation - Limes Security has just the right service for every business:

Secure operation of industrial facilities
We assist you with identifying technical and organizational weaknesses in your organization, aid you in setting up effective and efficient security organizations and implement appropriate countermeasures.

Secure development of products and solutions
We help you to identify defects in your products and solutions, assist with the setup of secure development practices and coach you to deal with vulnerabilities in the long run.

Training and certification of industrial staff
We enable you to build and integrate security capabilities into your organization through top-class security trainings and certification of your staff.

References

These companies and many others rely on the security competence of Limes Security.



Knowledge Transfer

Limes Academy offers courses in various formats so that you can participate in the optimal training adapted to your learning style. Regardless of whether you want to take part in an online class with other participants or prefer personal training in your company: At Limes Academy, you will find a learning format that meets your individual requirements.

In-House

The training is conducted by a Limes Academy trainer specifically for your company, department, or team. The training takes place on site at your company, in a training center, or at a company location of your choice.

In-House Online

The training is conducted by a Limes Academy trainer specifically for your company, department, or team. The training takes place online and is held using your company's infrastructure or the infrastructure of Limes Security.

Public

Public courses at selected locations, held by a Limes Academy trainer.

Public Online

The training is conducted live by a Limes Academy trainer in an interactive virtual classroom. The class can be attended worldwide.

E-Learning

An online learning experience available for all security awareness courses in German and English. Participants can work through the learning content at their own pace.



Overview of Trainings

100 Security Awareness Training

AWT.101 IT Security Awareness	Page 10
AWT.102 OT Security Awareness	Page 11
AWT.103 Zero Downtime: Blackout Edition	Page 12

200 Industrial/OT Security Training

Industrial/OT Security Foundation

ICS.201 Industrial/OT Security Foundation	Page 16
---	---------

Industrial/OT Security Advanced

ICS.211 Technical OT Security	Page 18
ICS.212 OT Security Management	Page 20

Industrial/OT Security Additions

ICS.221 Assessing OT	Page 22
ICS.222 Incident Handling Essentials	Page 23
ICS.231 Industrial/OT Security Updater	Page 24

300 Security Engineering Training

Secure Coding

SEC.301 Secure Coding Java	Page 26
SEC.302 Secure Coding C#	Page 27
SEC.303 Secure Coding Web	Page 28

Secure Development Lifecycle

SEC.311 Secure Product Development with IEC 62443-4-1	Page 29
SEC.312 Secure Development of IoT Components	Page 30

Security Testing

SEC.321 Security Testing Foundation	Page 31
SEC.322 Wireless Security	Page 32

System Hardening

SEC.331 System Hardening Windows	Page 33
SEC.332 System Hardening Linux	Page 34

Our Trainers

Unsurpassed Professional Expertise

Our trainers are all academically trained and seasoned security experts with several years of consulting experience in industry and software development.

The additional benefit for you as a participant: In addition to excellent training content, you can also share in a wide range of experience and knowledge from practical experience for practical use.

Speaker Profiles

Specialized in **A** = Awareness Training **I** = ICS/OT Training **S** = Security Engineering Training

Lucas Brandstätter

A I



supports with his knowledge in the ISMS (ISO 27000) and OSMS (IEC 62443) area, companies in the introduction of management systems. In the course of risk analyses and penetration tests, he checks systems for untapped potential for improvement. In training courses he emphasizes interactive feedback from the participants.

Peter Eder-Neuhauser

A I



shows the importance of integrated risk management, incident handling, coordinated IT governance, threat and gap analyses, privacy impact assessments and awareness through his research focus on malware propagation in IT/OT networks, specific mitigation measures and secure architecture.

Thomas Brandstetter

A I



is our broad-spectrum antibiotic against security ignorance. As a Stuxnet Incident Handler and former head of Siemens Product-CERT, he knows industrial security from all life cycle phases. He is Professor of IT and Cyber Security at the University of Applied Sciences St. Pölten and is certified for CISSP, GSEC, GICSP and GRID.

Simon Hornbachner

A I S



has worked for several years in the areas of security operations and infrastructure operations and therefore knows „the other side“ very well - what it means to have to implement cyber security in daily work. It is therefore of particular concern to him to establish a concrete reference to the daily work of the participants in the contents taught.

Gandalf Denk

A I S



is an Oracle Certified Associate and Trainer for Secure Coding and certified GIAC Mobile Device Security Analyst (GMOB). He loves solving tricky problems - whether creating secure applications or trying to hack them. During training sessions he shares his experiences and likes to challenge participants with complex exercises.

Our Trainers

Speaker Profiles

Specialized in **A** = Awareness Training **I** = ICS/OT Training **S** = Security Engineering Training

Johannes Klick

A I



is a passionate researcher and OT security expert. His research interests focus on OT security and global Internet scanning for threat assessments. He has given presentations at internationally recognised conferences like Chaos Communication Camp, PHDays Russia and Black Hat USA.

Peter Panholzer

A I S



is veteran of the first hour for industrial security and secure software development. He is a certified ISO 27001 auditor, member of the OVE working group on IEC 62443, hacker and for over ten years trainer for secure coding. He loves to give the participants tricky tasks and to assist them with the right security tips.

Phillipp Kreimel

A I



brings technical security expertise to training courses and penetration tests through his years of experience in industrial security research in the production and energy sectors. He is certified according to GIAC Response and Industrial Defense (GRID) and is a lecturer for IT security at the University of Applied Sciences St. Pölten.

Kerstin Reisinger

A I



is an Offensive Security Certified Professional and trainer for Industrial Security. As a long-standing, experienced project manager in complex OT security projects, she supports industrial companies and energy suppliers with a great deal of technical knowledge. She likes to incorporate this experience into her classes as war stories.

Daniel Marzin

A I



is a certified Offensive Security Certified Professional with focus and know-how in the OT sector. With his experience he conducts security assessments and network restructuring in industrial and pharmaceutical companies. As application developer he also knows the other side. He shares his experience in the form of security trainings.

Tobias Zillner

A I S



concentrates mainly on current hacking techniques and reverse engineering of wireless communication, in addition to his focus on OT security. He regularly speaks at international security conferences and is active in teaching at the University of Vienna and the University of Applied Sciences St. Pölten.

The Employee as the Target

Most successful attacks start by exploiting human nature to invade internal networks. Your employees must learn to understand where security risks lurk in

their daily work - regardless of whether they work in management, production, or marketing.

Training Contents

In our tried and tested Security Awareness training, we impart the required self-competence that employees need in order to immediately identify risks and avoid negligent behavior. Limes Security brings experiences from attack campaigns, vivid demos, and exciting

war stories to accomplish that. We use entertaining explanations of the most essential security rules that every employee of a modern company should know in order not to be a security risk for their own company.



Awareness

**AWT.101
IT Security
Awareness**

**AWT.102
OT Security
Awareness**

**AWT.103
Zero Downtime:
Blackout Edition**

Security for Everyone Through E-Learning

Security is a topic that affects all employees of a company. Unfortunately, however, it is often not feasible to have every single employee participate in a training course for a day or longer. The solution here is obvious: time and location independent training through

e-learning modules. Limes Security therefore also offers the IT and OT security awareness basics in the form of e-learning modules, so that your employees can conduct the training conveniently in the office at a time that suits them.

E-Learning at a Glance

There are six modules in total, each module taking between five and ten minutes. At the end of each module there is a short repetition of the most important elements in the form of a quiz. After module 6 there is a final review of the acquired knowledge from all subject areas. The modules are provided in the standardized SCORM format and are compatible with common e-learning platforms.

The Modules in Detail

- # **Module 1:** Information security and current threats
- # **Module 2:** Unprotected areas and external persons
- # **Module 3:** Information, social media and passwords
- # **Module 4:** Downloads, programs and e-mails
- # **Module 5:** External media, personal devices and public Wi-Fi
- # **Module 6:** Detecting attacks and reporting suspicious cases



www.limesecurity.com

What can you as an employee contribute to protection?

Security awareness means that you as an employee are aware that the protection of the company's physical and informative assets is in your hands (security awareness).

CONCLUSION:

IT security awareness measures train and support employees so that they can recognize their responsibility and meet this challenge.



Pricing Information

Limes Security uses a user-based pricing model for the e-learning modules. This means that you pay for exactly the number of users who need to be trained. The pricing model is also progressive. This means that the more users are trained, the lower the average price per user gets.

Please contact us and ask for matching company packages for your specific number of employees.

Request a Demo

Are you interested in a demo of the e-learning content? Contact us and get access to our demo e-learning software.

AWT.101 IT Security Awareness

 4 hours

 All employees

 No Notebook necessary

 Course material and certificate of completion

 400.- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house / In-house online
Public / Public online
E-Learning

IT Security Awareness

The IT Security Awareness training serves as a basis for every employee in the company to impart a basic understanding for security or to refresh pre-existing security knowledge.

Training Contents

- # What is information security?
- # Who are the attackers?
- # Recent attacks, incidents, and hacking demo
- # Secure rules of conduct
 - Dealing with programs, software and emails
 - Dealing with passwords and password policies
 - Handling USB sticks and other external media
 - Handling your own equipment in the company (Bring your own Device – BYOD)
 - Handling information
 - Physical security
- # Recognize attacks and report suspicious cases
- # Security in the private environment

Your Benefits

- # Impart a basic understanding of security for all employees.
- # Create security awareness in the participants for an increased security level in their own company.
- # Refresh already known rules of conduct for secure actions within the company.

Registration

You will find an overview of all current dates as well as the registration for the **AWT.101 IT Security Awareness Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



AWT.102 OT Security Awareness

 4 hours

 All employees

 No Notebook necessary

 Course material and certificate of completion

 400.- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house / In-house online
Public / Public online
E-Learning

OT Security Awareness

The OT Security Awareness training serves as a basis for every employee in the OT area to impart a basic understanding of security or to refresh pre-existing security knowledge. In contrast to the AWT.101 IT Security Awareness training, this course highlights concrete examples and rules of conduct specifically for the OT area.

Training Contents

- # What is included in Operational Technology (OT)?
- # Who is attacking industrial control systems?
- # Recent attacks, incidents and OT-specific hacking demo
- # Secure rules of conduct
 - Dealing with programs, software and emails
 - Dealing with passwords and password policies
 - Handling USB sticks and other external media
 - Physical security
- # Recognizing attacks and reporting suspicious cases
- # Top 10 OT security risks

Your Benefits

- # Impart a basic understanding of security for all employees in the OT sector.
- # Create security awareness in the participants for an increased security level in their own company.
- # Refresh already known rules of conduct for secure actions within the company.
- # Detect and prevent risky behavior in industrial plants.

Registration

You will find an overview of all current dates as well as the registration for the **AWT.102 OT Security Awareness Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



AWT.103 Zero Downtime: Blackout Edition

🕒 2 hours

👥 All employees

📖 No Notebook necessary

📄 Course material and certificate of completion

€ On request

🗨️ DE EN German or English

💡 No prior knowledge necessary

🧠 In-house

ICS Cyber Security Simulation Game Zero Downtime

As a contestant, transform yourself from an affected person to an involved participant: In the ICS cyber security simulation game, you become the defender of your corporate assets. Several teams compete against each other and learn to simulate reality.

The simulation game is based on a serious thought: The participants learn about current IT threat scenarios and adequate security concepts as countermeasures at the forefront. Through the direct involvement of each individual, the learning content is firmly and sustainably anchored; at the same time teamwork is

essential. In the end, the company that has best mastered the challenges is declared the winner.

The simulation game is moderated by a Limes Security expert and the results are summarized briefly after each round. The participants play in groups at a table with a game board in combination with a tablet. No special previous knowledge is required to participate, and the simulation game is also suitable for beginners.

Your Benefits

- # Get to know important security measures and concepts in a playful manner.
- # Apply effective countermeasures to security threats as a contestant.
- # Learn about the effects and consequences of certain security measures and concepts.
- # Upgrade your company event or conference with this hands-on experience!



Registration

An overview of all current dates and the registration for **AWT.103 Zero Downtime: Blackout Edition** can be found under the link on the right or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



Secure Digitization for Technicians and Decision Makers

In addition to increased security requirements, technical changes in the area of industrial security have become new challenges for manufacturers, system integrators and operators of industrial plants. A consequence of this rapid change is that industrial secu-

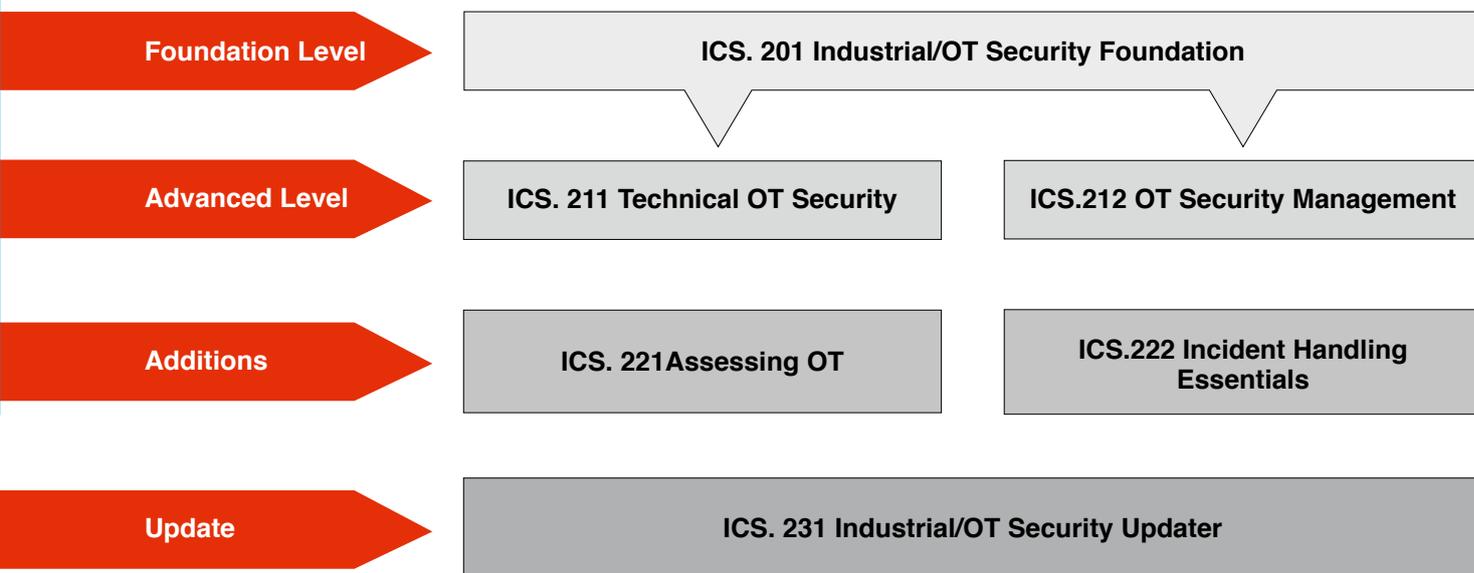
urity today works completely differently than the familiar world of industrial automation of the past decades. Limes Security provides clarity, gives guidelines for action and imparts competence for the correct handling of security topics in an industrial environment.

Training Contents

The training contents have been selected based on the experience gained from many industrial projects and are aimed at the challenges facing the industry in practice. Our training courses impart the security basics (foundation) urgently needed by industrial personnel as well as advanced knowledge for deci-

sion-makers and technicians and special topics (additions). Through practical examples and war stories from our trainers, you develop all the skills required for secure digitization in industry.

For some courses it is possible to obtain a TÜV® person certificate by passing an official exam



OT Security Courses with Personal Certification

In addition to increased security requirements, technical changes in the area of industrial security have become new challenges for manufacturers, system integrators and operators of industrial plants. A consequence of this rapid change is that industrial security today works completely differently than the familiar world of industrial automation of the past decades. Limes Security and TÜV AUSTRIA Academy provide clarity, give guidelines for action and impart competence for the correct handling of security topics in an industrial environment.

Limes Security offers a personal certification scheme in cooperation with TÜV AUSTRIA (<https://www.tuv-akademie.at/en/>). The Limes Security Academy's high-quality and practical OT security training courses - from "Practitioner" to "Manager" - are divided into three modules, each taking 2.5 days. The exam, conducted by TÜV AUSTRIA, can be taken immediately after the end of the training on the third day.

Who benefits from a personal certificate?

This certification is perfectly suited for employees from the industrial sector who want to visibly improve their qualifications in the field of security and also want to provide proof of their knowledge in this area. **The certification is therefore aimed at companies from the following sectors:** industrial component manufacturers, manufacturing industry, mechanical engineers, system integrators, plant operators, energy suppliers, operators of critical infrastructure

Persons in the function: maintenance, production technicians, plant planners and plant engineers, persons responsible for plant IT, future operations managers and production managers

Due to changed regulatory requirements and industrial security standards (NIS directive, IEC 62443), it is becoming increasingly important for industrial component manufacturers, system integrators and plant operators to be able to provide evidence of qualified personnel. The OT security personal certification scheme provides significant help in this context.

Overview of the personal certification scheme

Training & examination for Certified OT Security Practitioner TÜV® (COSP)

Level 1: Training series Operational Technology Security, course ICS.201 Industrial Security Foundation

Prerequisites: No prior knowledge required; basic information security knowledge beneficial



Training & examination for Certified OT Security Technical Expert TÜV® (COSTE)

Level 2: Training series Operational Technology Security, course ICS.211 Technical OT Security

Prerequisites: Completed training including examination for Certified OT Security Practitioner TÜV® (COSP) or Certified OT Security Manager TÜV® (COSM) or an equivalent training course or proven relevant professional experience of at least 38 hours per week.



Training & examination for Certified OT Security Manager TÜV® (COSM)

Level 2: Training series Operational Technology Security, course ICS.212 OT Security Management

Prerequisites: Completed training including examination for Certified OT Security Practitioner TÜV® (COSP) or Certified OT Security Technical Expert TÜV® (COSTE) or an equivalent training course or proven relevant professional experience of at least 38 hours per week



Details About the Certification

Limes Security has found a reliable and strong partner in TÜV AUSTRIA Academy in the area of personal certification. TÜV AUSTRIA is an internationally active certification body for the certification of persons, products and systems. Various accreditations, official authorizations and commercial law licenses are the basis for globally recognized certificates. Each certification procedure of persons strictly complies with the stringent provisions of the international standard ISO/IEC 17024. Person certificates of TÜV AUSTRIA create trust and offer you a clear advantage in the professional world.

Certification procedure

The exams for an OT security person certificate are carried out in writing during physical trainings or through an online platform provided by TÜV AUSTRIA specifically for examination purposes during online trainings. Every applicant needs to provide a photo ID; for the online examination the use of a webcam is therefore mandatory.

During the exam, candidates have 90 minutes to answer a total of 30 questions in multiple choice mode. The course materials provided may be used during the examination.

After positive completion of the exam, the TÜV AUSTRIA Person Certificate can be used to prove that a certain knowledge can be competently applied and implemented.

Cost

The certification fee includes the issue of one certificate. Duplicate certificates are charged separately. Certificates are issued in German or English, but can be issued in other languages on request. Each examination or part of an examination may be repeated once free of charge on one of the next examination dates depending on the available spots. Additional dates will be charged according to time and expense.

Validity

In order to ensure that your knowledge is always up to date with current technical and organizational developments, the validity of your certificate is time-limited. The TÜV AUSTRIA Person Certificates for OT security are valid for three years.

ICS.201 Industrial/OT Security Foundation



Training without certification: 2.5 days
Training with certification: 3 days



German or
English



Training without certification: 1.935,- euros plus VAT
Training + certification incl. exam: 2.550,- euros plus VAT



Own Notebook
required

Industrial/OT Security Foundation

Everyone involved in a modern industrial system needs basic security knowledge in order to recognize security problems and avoid endangering industrial operations through their own behavior. Within the framework of the Foundation training, the participants are taught those security competencies through up-to-date specialist content, practical exercises and entertaining experiences from industrial security consulting activities, which are not only essential for their work in the changed environment of increasing digitalization, but also decisive.

Training Contents

Day 1

- # Introduction to Operational Technology (OT)
 - History of ICS/OT
 - ICS/OT components and terminology
 - ICS/OT process types
- # IT vs. OT Security
 - Safety vs. Security
 - Characteristics of ICS systems vs. IT systems
 - ICS security vs. IT security
- # Security Essentials
 - IT security objectives
 - Primer of network protocols
 - Primer of cryptography
 - Overview of secure network protocols
 - Primer of network security

Day 2

- # OT security threats and attack vectors
 - OT attackers
 - Conducting an attack
 - Attack campaigns and patterns
 - OT security risk factors
 - Open Source Intelligence: Shodan and Google Dorks
 - ICS Top 10 / Attack trees

- # Overview of OT standards
 - BDEW Whitepaper
 - Cyber Security Procurement Language for Control Systems
 - ISO 27019
 - NERC CIP
 - NIST 800-82 and CSF
 - ISO 27000
 - IEC 62443
 - NIS directive
 - TISAX

Day 3

- # Well-proven security measures for OT
 - Defense in Depth
 - Organisational security measures
 - Security assessments and reviews
 - Configuration management
 - Network and communication security
 - Component security
 - Access control



No prior knowledge necessary



In-house / In-house online
Public / Public online



Course material and certificate of completion
Option for person certificate!

» **If you only want to obtain the person certificate for this training, please contact us.**

The Training is Particularly Recommended for ...

- # System integrators
- # Plant operators, planners, and technicians
- # Maintenance workers
- # Production technicians
- # Plant electricians
- # Machine operators
- # Plant IT managers
- # Future plant managers and production managers
- # Employees who work directly with OT
- # Managers whose employees work with OT
- # IT employees with responsibility for OT assets
- # Employees who are responsible for the procurement, planning or operation of OT assets

After the Training the Participants Should ...

- # have a confident feeling in dealing directly with OT security.
- # have a basic understanding of OT technologies and terminology.
- # have gained a basic awareness of OT security standards and their areas of application.
- # know the most important security measures for the OT area.
- # be able to make a contribution to protecting industrial operations in their area of responsibility



**Certified OT Security Practitioner
TÜV® (COSP)**

Registration

You will find an overview of all current dates as well as the registration for the **ICS.201 Industrial/OT Security Foundation Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



ICS.211 Technical OT Security

⏴ Training without certification: 2.5 days
Training with certification: 3 days

DE EN German or English

€ Training without certification: 1.935,- euros plus VAT
Training + certification incl. exam: 2.550,- euros plus VAT

📖 Own Notebook required

Industrial Security Advanced: Technical OT Security

Particularly technicians and engineers are increasingly expected in industrial operations to make or prepare the right decisions regarding appropriate technical security measures and security technologies.

Training Contents

Day 1

- # Introduction
 - Procurement of a secure system
 - IEC 62443 risk analysis
- # ICS/OT protocols
 - Overview Wired and Wireless Protocols
 - Industrial Protocol Details
 - Profinet and Profibus / Modbus
 - IEC 60870-5-104 / IEC 61850 / IEC 62351
 - OPC and OPC UA
 - Hart and Wireless Hart
 - Bacnet / DNP3 / CANbus / EtherNet/IP
 - S7comm / MQTT
 - Wireless Protocol Details
 - Bluetooth / Wi-Fi / cellular network / ZigBee
 - SATCOM / LoRa and LoRaWAN
 - Securing industrial protocols

Day 2

- # Network-based attacks
 - Denial of service attacks
 - Sniffing
 - Man in the middle attacks
 - SMB relay
 - Incident handling introduction

Advanced OT Network Security

- Network segmentation
- ICS firewall
 - Policies / recommendations / ICS-specific firewall topics
- Honeypots
 - Examples for honeypots in OT
 - ICS honeypots and scanning
- Concluding exercise

Day 3

- # Applying security measures in OT
 - Overview of security requirements and implementation
 - User management
 - Credential management
 - Host hardening
 - System monitoring and network detection
 - Remote access
 - Backup and recovery
 - IEC 62443 certification
- # Lockpicking challenge and Q&A



ICS.201 Industrial/OT Security Foundation training recommended



In-house / In-house online
Public / Public online



Course material and certificate of completion
Option for person certificate!

» **If you only want to obtain the person certificate for this training, please contact us.**

The Training is Particularly Recommended for ...

- # System integrators
- # Plant operators, planners, and technicians
- # Maintenance workers
- # Production technicians
- # Plant IT managers
- # Future plant managers and production managers
- # Employees who are responsible for the procurement, planning or operation of OT assets
- # IT employees with responsibility for OT assets

After the Training the Participants Should ...

- # further consolidate and deepen existing knowledge in IT and OT security.
- # know how to technically implement security measures in the OT operation.
- # have a basic understanding of OT transmission technologies and protocols.
- # understand different network protection measures in the OT through the Purdue model.
- # know the procedure for partitioning and zoning of an architecture according to IEC 62443 including the security levels.
- # have gained insight into the use of honeypot systems against attackers.
- # understand the relationship between physical security and OT security.



**Certified OT Security
Technical Expert TÜV® (COSTE)**

Registration

You will find an overview of all current dates as well as the registration for the **ICS.211 Technical OT Security Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



ICS.212 OT Security Management



Training without certification: 2.5 days
Training with certification: 3 days



German or
English



Training without certification: 1.935,- euros plus VAT
Training + certification incl. exam: 2.550,- euros plus VAT



Own Notebook
required

Industrial Security Advanced: OT Security Management

The OT Security Management training provides those responsible for operations, project and production managers and decision-makers in general with the knowledge they need to implement security in industrial operations. Participants learn all necessary skills to recognize dangers early on, to increase the security level and to lastingly avoid security vulnerabilities. The focus is on organizational topics and process management, in addition technical influencing factors are also discussed, which prepare the participants better for future security decisions.

Training Contents

Day 1

- # Overview of security standards and frameworks
- # Case study: OT security incident in the absence of OT security management
- # Organisational measures and ISMS
- # Definition of the system under consideration (SUC)
- # Asset management
- # Risk management
- # Supply chain management
- # Classification of information

Day 2

- # Partitioning and zoning
- # Secure remote access
- # Component security (hardening)
- # Identity and access management
- # Awareness training
- # Patch management

Day 3

- # Incident handling
- # Logging and monitoring
- # Anomaly detection
- # Vulnerability assessment
- # Incident response planning
- # Backup
- # System availability



ICS.201 Industrial/OT Security Foundation training recommended



In-house / In-house online
Public / Public online



Course material and certificate of completion
Option for person certificate!

» **If you only want to obtain the person certificate for this training, please contact us.**

The Training is Particularly Recommended for ...

- # System integrators
- # Plant operators, planners and technicians
- # Maintenance workers
- # Production technicians
- # Plant IT managers
- # Future plant managers and production managers
- # Employees who are responsible for the procurement, planning or operation of OT assets
- # IT employees with responsibility for OT assets

After the Training the Participants Should ...

- # be able to securely manage their responsible operating areas and assess risks.
- # have refreshed and deepened their existing knowledge of OT security and related standards.
- # have gained a basic understanding of the risk assessment procedure.
- # understand asset discovery and component classification capabilities.
- # have developed a holistic view of security processes.
- # be able to define response plans and establish defined communication strategies for incident management.



**Certified OT Security Manager
TÜV® (COSM)**

Registration

You will find an overview of all current dates as well as the registration for the **ICS.212 OT Security Management Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



ICS.221 Assessing OT



1 day



Technicians



Own Notebook
required



Course material and
certificate of completion



774,- euros
plus VAT



German or
English



ICS.211 Technical
OT Security Training



In-house / In-house online
Public / Public online

Industrial/OT Security Additions: Assessing OT

The Assessing OT training provides participants with the basics to be able to professionally conduct security tests in industrial plants. Which tools should be used for which application? Which test cases are intrusive and therefore less suitable for OT? What information is relevant in the context of an OT security audit? In this course, participants benefit in particular from the Limes experts' many years of experience in conducting security assessments in an industrial environment.

Training Contents

- # Underground Economy
- # Security test requirements from IEC 62443 and ISO 27001
- # ICS Asset Discovery
- # Checking users and authorizations
- # Configuration review of ICS systems
- # Verification of patch and software versions
- # Checking the perimeter protection
- # Procedure for an ICS security test
- # Testing the BSI ICS Top 10
- # Use and configuration of test tools for productive environments

Your Benefits

- # View networks and systems through the eyes of an attacker and identifying potential attack vectors and security issues.
- # Know what has to be considered during a security check in an industrial environment.
- # Know how the results of a security audit can lead to an increased level of security.

Registration

You will find an overview of all current dates as well as the registration for the **ICS.221 Assessing OT Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



ICS.222 Industrial/OT Incident Handling Essentials



1 day



Technicians and Decision makers



Own Notebook required



Course material and certificate of completion



774,- euros plus VAT



German or English



ICS.201 Industrial/OT Security Foundation Training recommended



In-house / In-house online Public / Public online

Industrial/OT Security Additions: Incident Handling Essentials

The Incident Handling Essentials training provides participants with the necessary basics to prepare for security incidents in an industrial environment. The most important technical and organizational preparations will be discussed along with the “DOs and DON'Ts”. This course is particularly interesting for plant operators, integrators and service providers who want to prepare for an emergency to be able to more easily prevent damage caused by virus attacks, ransomware or hacking.

Training Contents

- # Introduction to Security Incident Handling: Basics and terms
- # The lifecycle of an incident in six steps
- # Technical and organizational prerequisites: How do I prepare for incident handling?
- # Asset Identification and Network Security
- # Monitoring: What role do tools play in detection?
- # Rules of conduct in case of an incident “DO's and DON'Ts”
- # Case Study: CrashOverride and TRISIS
- # CERTs & Co.: Where can I get information about threats and external assistance?

Your Benefits

- # Learn to use techniques and methods for maintenance of industrial operation
- # Get to know best practice during a potential ICS security incident
- # Deal with the topic of weak points and incident handling in your own company

Registration

You will find an overview of all current dates as well as the registration for the **ICS.222 Incident Handling Essentials Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



ICS.231 Industrial/OT Security Updater

 4 hours

 Technicians and Decision makers

 No Notebook necessary

 Course material and certificate of completion

 400,- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house / In-house online
Public / Public online

Industrial/OT Security Updater

The Industrial/OT Security Updater training course serves as a refresher and update course for the participants to inform them about organizational and technical innovations and progress in the field of security.

Training Contents

- # New security features in ICS protocols
- # Innovations in the area of compliance and regulations
- # News about IEC 62443
- # ICS vulnerabilities and attack campaigns
- # Innovations in security technologies

Your Benefits

- # Efficiently refresh the knowledge you've already acquired in just four hours.
- # Learn about the most important innovations from the technical as well as from the organizational world of security.
- # Stay one step ahead of attackers with information about current ICS vulnerabilities and attack campaigns

Registration

You will find an overview of all current dates as well as the registration for the **ICS.231 Updater Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



Secure Products Through Superior Know-How

How can security vulnerabilities be avoided right from the start? Only through appropriate training and improvement of the security expertise of developers and project members. We teach the “DOs and DON'Ts” in theory and in practical exercises. In the security en-

gineering training courses, experienced trainers from Limes Security impart the knowledge of how attackers proceed and which measures best protect against them.

Training Contents

The Secure Coding training provides the participants with the knowledge and understanding for the development of secure products so that they can be implemented in their own projects. The Security Testing training teaches the participants to take the perspective of an attacker, allowing them to efficiently identify vulnerabilities in their products. The System Hard-

ening training gives system administrators the tools they need to protect a digital infrastructure against both internal and external attacks. All courses are accompanied by practical exercises that illuminate both the attacker and the defender's side, imparting a multi-layered picture.

Secure Coding

SEC.301
Secure Coding Java

SEC.302
Secure Coding C#

SEC.303
Secure Coding Web

Secure Development Lifecycle

SEC.311 Secure Product Development with IEC 62443-4-1

SEC.312 Secure Development of IoT Components

Security Testing

SEC.321
Security Testing Foundation

SEC.322
Wireless Security

System Hardening

SEC.331 System Hardening Windows

SEC.332 System Hardening Linux

SEC.301 Secure Coding Java

 3 days

 Java developers

 Own Notebook required

 Course material and certificate of completion

 2.322,- euros plus VAT

 German or English

 Experience in web technologies and Java

 In-house Public

Secure Coding Java

The Secure Coding training for Java teaches the correct usage of exception handling, multi-threading and other Java-specific methods that are necessary as a basis for developing robust code. In addition, various cryptographic technologies will be discussed, including encryption, hashing and digital signatures. Classical web attacks such as cross-site scripting, SQL injection and cross-site request forgery will be explained as well as how applications can be protected against them. Practical exercises are used to create a deep understanding of the different subject areas. In order to further increase the code quality, the correct handling of code reviews is demonstrated as well as how the learned techniques can be integrated into the Secure Development Lifecycle.

Training Contents

- # Introduction to IT security
- # Preparation for an attack
- # Attacks on input parameters
 - SQL injections, Cross-site scripting (XSS)
 - Overflow, underflow and upcasting
 - Code injections, deserialization
 - Web Application Firewalls
- # Sniffing of login data or tokens
- # Attacks on a thick client
- # Attacks on sessions and authentication
- # Secure development lifecycle

Your Benefits

- # Understand how attacks work and start thinking like an attacker.
- # Understand what steps are necessary for a secure software development.
- # Be capable to integrate secure development into your area of responsibility.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.301 Secure Coding Java Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.302 Secure Coding C#

 3 days

 C# developers

 Own Notebook required

 Course material and certificate of completion

 2.322,- euros plus VAT

 German or English

 Experience with C# development

 In-house Public

Secure Coding für C#

During the Secure Coding for C# training, different C# language features will be introduced that can contribute to the stability of the code and are necessary as a basis for the development of robust code. In addition, cryptographic concepts such as encryption, hashing or digital signatures are discussed. You will learn how to achieve robust session management using meaningful access controls. Classic web attacks such as cross-site scripting and SQL injection are explained and how to protect against them is demonstrated. Finally, we discuss how code reviews and static analyses are performed to achieve optimal code quality. For a better understanding, the topics are explained using practical exercises.

Training Contents

- # Introduction to IT security
- # Cryptography
- # Authentication and authorization
- # Injection attacks
 - SQL injections, OS command injection, Cross site scripting (XSS)
- # C# language security
 - Data types, encapsulation, exception handling, logging
 - Multi-threading, code signing
- # Secure communication
- # Revision

Your Benefits

- # Understand how attacks work and start thinking like an attacker.
- # Understand what steps are necessary for a secure software development.
- # Be capable to integrate secure development into your area of responsibility.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.302 Secure Coding C# Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



SEC.303 Secure Coding Web

 2 days



Developers
and testers



Own Notebook
required



Course material and
certificate of completion

 1.548,- euros
plus VAT



German or
English



Experience in web
technologies



In-house
Public

Secure Coding Web

As part of the Secure Coding Web training, security concepts on the web will be discussed, including Transport Layer Security (TLS) and Cross-origin Resource Sharing (CORS). How session management can be securely implemented will be explained. Then the anatomy of the most common web attacks such as cross-site scripting, cross-site request forgery and SQL injections is discussed together with how to avoid them. In addition, more complex web attacks such as XML external entities, broken authentication, and security misconfiguration are explained. It concludes with an explanation of how code reviews can lead to improved code quality and how a secure development life cycle can be implemented in your organization. For a better understanding practical exercises are built into the topics.

Training Contents

- # Introduction to IT security
- # Cryptography
- # Authentication and authorization
 - Password authentication, brute force attacks
 - Secure session management, forwards and redirects, security frameworks
- # Injection attacks
 - SQL injections, OS command injection, XML injection
 - Cross site scripting (XSS), cross site request forgery (CSRF)

Your Benefits

- # Understand how web attacks work and start thinking like an attacker.
- # Understand what steps are necessary to develop secure web applications.
- # Learn how to integrate secure software development processes into your area of responsibility.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.303 Secure Coding Web Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.311 Secure Product Development with IEC 62443-4-1

 2 days

 Developers and project managers

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house Public

Secure Product Development with IEC 62443-4-1

If you don't want to leave the security and the quality of your products to chance, you have to choose a proactive approach. Only by integrating security into the development processes and by having an organization that knows how to deal with the topic professionally can high-quality products that meet the needs of the market be created. The Secure Product Development with IEC 62443-4-1 training teaches the participants how security can be integrated into software development with the help of the IEC 62443-4-1 standard section security in order to make their products lastingly secure.

Training Contents

- # Introduction to IEC 62443-4-1 (principles and requirements)
- # Security management (product classification, security organization, security training, integrity protection, protection of the development environment, selection of secure components)
- # Specification of security requirements
- # Secure by design and secure implementation
- # Security verification and validation testing
- # PSIRT and security update Management
- # Security guidelines

Your Benefits

- # Know suitable methods and get familiar with the measures to integrate security into your development processes.
- # Be capable to use useful tools to review and improve your product security.
- # Overcome constant challenges such as legacy code, updates from third-party vendors or communication of vulnerabilities.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.311 Secure Product Development with IEC 62443-4-1 Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.312 Secure Development of IoT Components

 2 days

 Developer

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house Public

Secure Development of IoT Components

Component security starts here. More and more devices communicate with each other and are interconnected. In addition to numerous advantages, this development also brings new challenges and threats, especially in terms of security. Like security in most IT areas, IoT security requires an end-to-end approach that includes addressing security issues during the design phase.

How can security vulnerabilities be avoided right from the start? What threats do I need to protect my system against? What security measures do I need to use?

Training Contents

- # Introduction to IoT-Security
- # Attacks, threats and risks in the real world
- # Threat modeling
- # Security testing & toolset for attackers
- # Guidelines and standards (IEC 62443, OWASP IoT Security, ENISA, NIST)
- # Secure system design
- # Secure updates
- # Secure storage and cloud connectivity
- # IoT communication protocols
- # Secure development lifecycle basics
- # Vulnerability disclosure

Your Benefits

- # Acquire a solid foundation for implementing security in IoT systems.
- # Know security concepts that are applicable to a wide range of IoT devices.
- # Gain a solid, technical understanding of the typical attacks, threats and risks that IoT entails.
- # Be able to look at an IoT system from the perspective of an attacker.
- # Learn how to identify relevant assets.
- # Understand defense principles and create defense strategies.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.312 Secure Development of IoT Components Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.321 Security Testing Foundation

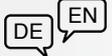
 2 days

 Testers

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 Experience in web technologies

 In-house Public

Security Testing Foundation

The Security Testing Foundation training teaches the basic concepts of security testing. A structured procedure is presented along with how security tests for an application can be organized. Subsequently, cross-site scripting and SQL injection attacks will be discussed with a focus on web applications and their anatomy will be explained and practiced using real-world examples. During the training, well-known hacking tools will be used again and again to give the participants a tangible picture of reality. Finally, tools are presented with which automated security scans can be carried out and how their results are to be dealt with.

Training Contents

- # Introduction to security testing
- # Preparing a security test
- # Security testing for cryptography
- # Security testing for web applications
- # Security testing for authentication
- # Security testing of proprietary interfaces
- # Security testing for system hardening
- # Result collecting and reporting

Your Benefits

- # Understand how attacks work and start thinking like an attacker.
- # Know how to use automated testing tools to efficiently cover recurring test cases.
- # Be capable to document identified vulnerabilities in a meaningful way to facilitate traceability and re-testing.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.321 Security Testing Foundation Training** under the adjacent link or by scanning the QR code.

<https://limessecurity.com/limes-academy/termine/>



SEC.322 Wireless Security

 2 days

 Testers

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 Experience in coding

 In-house Public

Wireless Security

This course introduces participants to the analysis and evaluation of the security of wireless communications and the typical problems, identification of wireless signals and best practices for testing wireless communications. RF theory, software-defined radio (SDR), the basics of radio and digital signal processing are discussed to provide a solid basis for understanding the security implications in this area. Special attention is paid to possible attack methods and test scenarios. Multiple exercises facilitate rapid progress in understanding the background and allow participants to make assessments and to test wireless communication themselves. In addition, excerpts from known vulnerabilities in real world products and standards are presented to underline the importance of the topic.

Training Contents

- # Radio-frequency (RF) introduction and theory
- # Introduction Software Defined Radio (SDR) and GNU Radio
- # Receiving and sending signals
- # Signal analysis
- # Modulation types and encodings
- # Introduction to reverse engineering
- # From signal to bits
- # Replay and injection attacks
- # Attack vectors in wireless communication

Your Benefits

- # Learn to perform a security analysis of wireless devices and identify typical problems.
- # Understand the fundamentals of RF theory, SDR and digital signal processing to build a solid foundation for understanding the security implications in this area.
- # Be able to identify possible attack vectors and test scenarios.
- # Have gained insight into known vulnerabilities in wireless device products and standards.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.322 Wireless Security Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.331 System Hardening Windows

 2 days

 System administrators

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house Public

System Hardening Windows

The System Hardening Windows training teaches system administrators how to operate a secure Windows-based system. The theoretical concepts of server hardening will be discussed, as well as concrete practical measures in the areas of user and network configuration, installation of updates, firewall configuration and the secure configuration of daemon services.

Training Contents

- # Attacker map
- # Hardware and software inventory
- # Secure configurations
- # Controlled access, malware defense and boundary defense
- # Data recovery and data protection, incident response and audit readiness
- # User configuration, features, and role configuration, network configuration, and NTP configuration
- # Update Installation
- # Firewall configuration and configuration of remote access
- # Service configuration
- # Additional hardening measures
- # Logging and monitoring

Your Benefits

- # Know how to improve your asset inventory and monitor the system landscape.
- # Understand how access management systems work and how to use them effectively.
- # Gain a deeper knowledge about hardening measures for Windows-based systems.
- # Be capable to lastingly reduce the attack area on your Windows systems and increase your company's security level.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.331 System Hardening Windows Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



SEC.332 System Hardening Linux

 2 days

 System administrators

 Own Notebook required

 Course material and certificate of completion

 1.548,- euros plus VAT

 German or English

 No prior knowledge necessary

 In-house Public

System Hardening Linux

The System Hardening Linux training teaches system administrators how to run a secure Linux-based system. The theoretical concepts of server hardening will be discussed, as well as concrete practical measures in the areas of user and network configuration, installation of updates, firewall configuration and the secure configuration of daemon services.

Training Contents

- # Attacker map
- # Hardware and software inventory
- # Secure configurations
- # Controlled access, malware defense and boundary defense
- # Data recovery and data protection, incident response and audit readiness
- # User configuration, network configuration, and NTP configuration
- # Package management and update installation
- # Firewall configuration and iptables
- # Daemon configuration and securing SSH access
- # SELinux and other hardening measures
- # Logging and monitoring

Your Benefits

- # Know how to improve your asset inventory and monitor the system landscape.
- # Understand how access management systems work and how to use them effectively.
- # Gain a deeper knowledge about hardening measures for Linux-based systems.
- # Be capable to lastingly reduce the attack area on your Linux systems and increase your company's security level.

Registration

You will find an overview of all current dates as well as the registration for the **SEC.332 System Hardening Linux Training** under the adjacent link or by scanning the QR code.

<https://limesecurity.com/limes-academy/termine/>



General Training Information

Room for Discussion

The structure and content of the training courses are deliberately designed to spark discussion among the participants. After all, the contents are much better memorized by engaging in considerations of your own and by exchanging viewpoints with other parti-

cipants.

During the training sessions, questions, deliberations, or comments on known situations and solutions in your own company are expressly welcome.

Book a Public Course

To book one of our courses, please go to <https://limesecurity.com/limes-academy/termine/> and find out about the next public training dates on your topic.

You can then easily register for our public courses on the website.



Procedure for In-House Trainings

- # **Coordination of training contents**
The client selects the training content which is adapted to the respective needs.
- # **Adaptation of the training course**
Limes Security adapts the exercises and documents to the individually selected content.
- # **Selection of a date**
The client sets a date for the training in coordination with Limes Security.
- # **Implementation of the training course**
The client determines the location of the training as well as the time frame.

- # **Provision of the training material** provides the participants with documents that are individually adapted to the customer's needs.
- # **Certificate**
At the end of the training the participants will receive a certificate of completion.
- # **Optional certification**
At the end of selected trainings an official certification can be carried out by one of our certification partners.

Conditions of Participation

1. SCOPE OF APPLICATION

These general conditions of participation apply to the implementation of training courses and further training measures by Limes Security.

2. REGISTRATION AND ORDER

At www.limessecurity.com/limes-academy you will find the complete course offer with all details and can register there directly. The registration becomes binding with a registration confirmation from Limes Security or TÜV Austria Akademie. The places for participants are limited and will therefore be allocated in the order of registration.

3. PARTICIPATION FEES AND TERMS OF PAYMENT

The prices listed in the list of courses or on the website are valid plus the legal value added tax. These are due immediately after invoicing without deductions and under indication of the invoice number to the payment. Before the start of the course we will send the invoice to the e-mail address given by you in the registration form. Unless otherwise stated in the order confirmation, the participation fee is per person and event and includes training material, lunch and drinks during breaks. Travel costs for our trainers for in-house training courses are not included in the course price and are offered separately.

4. ACCOMMODATION

Hotel reservations and costs for accommodation and meals outside seminar times are at the customer's expense.

5. EXECUTION AND CANCELLATION

Limes Security reserves the right to cancel the offered courses if the minimum number of participants is not reached. Limes Security also reserves the right to change trainers and venues as well as dates and program schedules. Participants will be informed of changes in good time. If a course does not take place, payments already made in respect of participation will be refunded to the participant without deductions. Further claims of the client are excluded, this also includes if the participant misses a seminar day due to his own fault.

6. REVOCATION AND CANCELLATIONS

Cancellations must be made in writing and are free of charge up to 7 working days (Mon-Fri) before the event begins. The cancellation deadline is only deemed to have been met if the written notice of cancellation is received within the deadline at the e-mail address provided for the course registration. From within 6 working days (Mon-Fri) to 1 working day before the start of the event, 30% of the participation fee will be charged for cancellations. If a registration for a subsequent date of the same course topic is received during this period, a reduced cancellation fee of 10% will be charged. There is no entitlement to a subsequent date, the corresponding new registration must be confirmed by Lime Security. In case of no-show or cancellation from the (first) day of the event, the full attendance fee will be charged. The cancellation fee is due with the effective date of the cancellation and is payable regardless of the reasons for cancellation. The cancellation fee shall not apply if the customer names a substitute participant who meets the admission requirements and pays the participation fee.

Conditions of Participation

7. CHANGES OF BOOKING

A desired change of booking to another course or another date must be made by the customer by e-mail. Whether a rebooking is possible and under which conditions is to be judged by Limes Security on a case-by-case basis. There is no right to rebooking.

8. IN-HOUSE TRAINING

Please get in touch with us in good time so that your desired appointment can be taken into account. The reservation can be made only after presentation of the written order.

9. COPYRIGHTS AND DATA PROTECTION

All course contents and documents are protected by copyright for Limes Security GmbH. Course materials are only intended for the personal use of the course participant. They may not be copied, passed on, translated or reproduced in any other way without the written consent of Limes Security. The data of the customer and/or the participants are recorded in our CRM system and only used by Limes Security for internal purposes of contract fulfilment.

10. LIABILITY

Limes Security is only liable for damages which can be proven to be based on an intentional or grossly negligent breach of duty within the framework of the contractual relationship or which are typical damages within the scope of the foreseeable. Should seminars lead to a delayed start or complete cancellation of a seminar due to force majeure, no liability will be assumed. Limes Security accepts no liability for damages that may be attributable to incomplete or incorrect information in the training documents. Limes Security accepts no liability for the theft or loss of items brought by the customer.

Imprint

Publisher: Limes Security GmbH, Softwarepark 26, 4232 Hagenberg, Tel: +43 720 510251, Email: office@limesecurity.com
Company register number 390566 m, Linz Regional Court, VAT ID number: ATU 676 527 29
Responsible for the content: Limes Security GmbH, Design: Contentschmiede, Kremsmünster, V3.0_06_2020
Typesetting and printing errors excepted.

Validity of the Course Book

This list of courses is valid from July 1st, 2020; previous offers lose their validity.
The stated prices are valid for registration or order until June 30th, 2021.
In the event of deviations in content, the information on the website applies.

