

Limes Academy

List of Courses 2023/2024

OT Security
Cost (COSTE)



LIMES
SECURITY



LIMES
SECURITY

What Limes Academy Offers

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



Security Awareness Training

starting from page 10



OT Security Training

starting from page 17



Security Engineering Training

starting from page 28

Why Limes Academy?

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.

+ Individual training formats	Our trainings take place at selected training centers, at our locations, or as online courses. Certain training content is also available in the form of e-learning. We also offer customized training exclusively for your company.
+ Interactive trainings	The training content taught is complemented by practical exercises. Discussions stimulate the exchange of experiences between the course participants and help comprehend the acquired knowledge.
+ Training materials	Training materials will be provided to you in high quality color print or digital format.
+ Expertise	All trainings are held by our experienced security experts who bring lots of experience from project practise.
+ Relevance	New incidents and security developments are continuously integrated into the training content. You benefit from the latest security knowledge.
+ Certificates	At the end of each training you will receive a certificate of participation. For some courses, it is possible to take an exam to attain a TÜV® persons certificate.

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 to help achieve an optimal level of security for our customers, specializing in vendor-independent, customized security solutions in the areas of secure software development and industrial security.

Limes Security GmbH is an owner-operated company. 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, a global player in industrial plant construction, or an 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.
- # **Customer-specific education programs**
At customer request, we can customize our courses to fit company-specific education programs.

References

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



Are you looking for a perfectly tailored educational experience for your team?

Limes Academy will gladly support you in training your employees. We will put together a training program tailored specifically to your requirements. Based on already existing training content, the training can be individually adapted to your requirements.

We gear the content and examples to your employees' prior knowledge, your industry and relevant standards / specifications / norms both regulatory and internally from your company.

We adapt duration and delivery (on-site, online) of the training to the availability of your employees.

We customize existing exercises or implement new ones based on the specific expertise of your participants.

Send us an inquiry!

<https://limessecurity.com/inhouse-training/>



Book a Public Course

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



There you can 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.

Supply of the training material

Limes Security supplies the participants with training material that is individually adapted to the customer's needs.

Certificate of participation

At the end of the training, the participants will receive a certificate of completion.

Optional exam and persons certificate

For certain trainings, participants can, if desired, take an official exam to attain a persons certificate through our certification partner.

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

Certain training courses can also be taken as e-learning via the Limes Academy learning platform. If desired, the learning content can also be provided for the company's own LMS in SCORM format. This is particularly suitable for on-demand training needs as well as company-wide training programs.



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 **O** = OT Security Training **S** = Security Engineering Training

Lucas Brandstätter **A O**



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

Gandalf Denk **A 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.

Thomas Brandstetter **A O**



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

Peter Eder-Neuhauser **A O**



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.

Nino Fürthauer **A O**



supports customers as a penetration tester to better secure web applications, infrastructure and systems against attacks. As product owner for the certification trainings offered by Limes Security in cooperation with TÜV Austria, he places special emphasis on every little detail.

Florian Gerstmayer **A O S**



worked for several years as a project manager and embedded software developer, where he designed and implemented secure products. Thus, he knows from personal experience which topics need to be addressed in the management of systems, as well as implemented as a developer in a holistic concept, and is happy to pass this on to others.

Simon Hornbachner-Reisinger **A O 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.

Sixtus Leonhardsberger **A O**



is an OT Security Specialist with a focus on penetration testing of OT environments and embedded devices/IoT devices. In addition to his passion for technical OT security topics, he also shares his experience from consulting projects on securing networks and architectures with the training participants.

Peter Panholzer **A O 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.

Kerstin Reisinger **A O**



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.

Tobias Zillner **A O 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.

100 Security Awareness Training

AWT.101 IT Security Awareness	p. 10
AWT.102 OT Security Awareness	p. 11
AWT.103 Zero Downtime: Blackout Edition	p. 12
AWT.104 Cybersecurity Awareness	p. 13

200 OT Security Training

OT Security Foundation	
ICS.201 OT Security Fundamentals	p. 17
ICS.205 Certified OT Security Practitioner (COSP)	p. 18
OT Security Advanced	
ICS.211 Certified OT Security Technical Expert (COSTE)	p. 20
ICS.212 Certified OT Security Manager (COSM)	p. 22
OT Security Additions	
ICS.221 Assessing OT	p. 24
ICS.222 Incident Handling Essentials	p. 25
ICS.223 IEC 62443 Fundamentals, Concepts and Usage	p. 26

300 Security Engineering Training

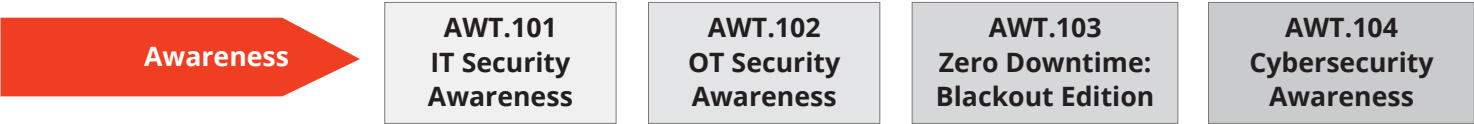
Secure Coding	
SEC.302 Secure Coding C#	p. 28
SEC.303 Secure Coding Web	p. 30
Secure Development	
SEC.311 Secure Product Development with IEC 62443-4-1	p. 32
SEC.321 Security Testing Foundation	p. 34


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.





 1,5 hours


 All employees


 No laptop computer required


 Course material and certificate of completion


 On request


 German or English


 No prior knowledge required


 In-house / In-house online


 1,5 hours


 All employees


 No laptop computer required

 Course material and certificate of completion

 On request

 German or English

 No prior knowledge required

 In-house / In-house online

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 the registration for the **AWT.101 IT Security Awareness Training** via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/awt-101/>





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 for plant personnel
 - 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.
- # Detect and prevent risky behavior in industrial plants.

Registration

You will find the registration for the **AWT.102 OT Security Awareness Training** via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/awt-102/>





AWT.103 Zero Downtime: Blackout Edition

AWT.104 Cybersecurity Awareness

 2 hours

 All employees


 No laptop computer required


 On request


 German or English


 No prior knowledge required


 In-house


 4 hours


 All employees


 No laptop computer required

 430,- Euro plus VAT

 German or English

 No prior knowledge required

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

 Course material and certificate of completion

Cyber Security Simulation Game Zero Downtime

In Zero Downtime, the cyber security simulation game, you become the defender of your corporate assets. Several teams compete against each other and learn playfully 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 online, or 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!



“The 0 Downtime workshop was very effective in engaging and challenging our top management to better understand the cybersecurity risks of our organization and their crucial role for better preparedness and incident response. I believe it was a definite success to bring cybersecurity awareness and culturalization to EDPD. I am a fan of 0 Downtime!” N. Medeiros, EDPD

Registration

The registration for **AWT.103 Zero Downtime: Blackout Edition** can be found via the adjacent link or by scanning the QR code.

<https://limessecurity.com/academy/awt-103/>



Cybersecurity Awareness

The Cybersecurity Awareness Training is designed as a basis for every employee in the IT/OT area to gain a basic understanding of security or to refresh already existing security knowledge. In contrast to purely theoretical training courses, concrete examples and rules of conduct are considered here specifically for the respective area of activity of the participants and existing prejudices in cyber security are tested for their truth content.

Training Contents

- # What is cybersecurity all about?
- # Who are the attackers of industrial systems?
- # Current attacks, incidents & IT/OT specific hacking demo.
- # Secure Rules of Conduct:
 - Dealing with programs, software and emails
 - Dealing with passwords & password policies
 - Dealing with USB sticks and other external media Physical security
- # Physical security
- # Detecting attacks & reporting suspicions
- # Top 10 cybersecurity risks

Your Benefits

- # Imparting a basic understanding of cybersecurity to all employees
- # Creating cybersecurity awareness among participants for an increased security level in their own company
- # Refreshing of already known rules of conduct for safe actions in the company

Registration

The registration for the **AWT.104 Cybersecurity Awareness Training** can be found via the adjacent link or by scanning the QR code.

<https://limessecurity.com/academy/awt-104/>



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 security today

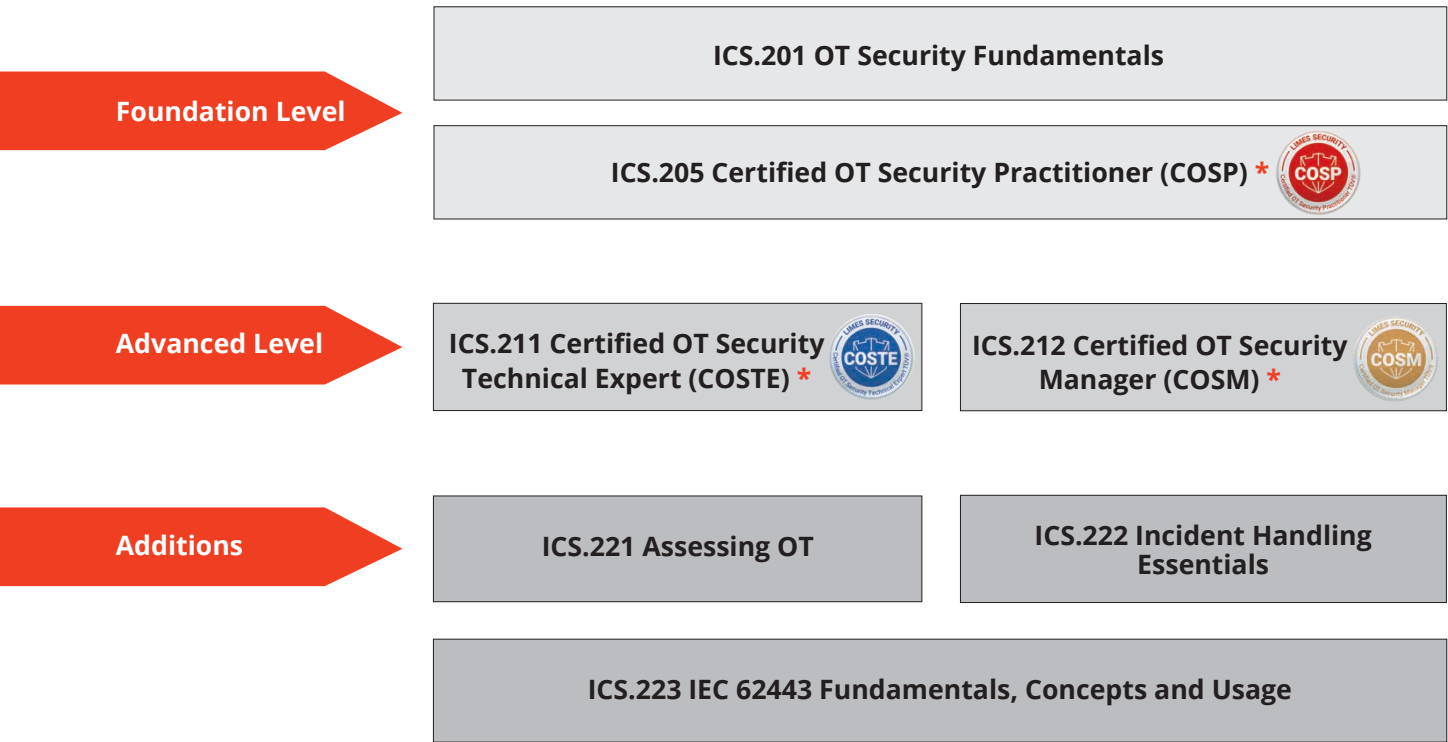
works completely differently than the familiar world of industrial automation of the past decades. Limes Security provides clarity, gives guidelines for action and imparts competence for the correct handling of security topics in an industrial environment.

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 level) urgently needed by industrial personnel as well as advanced knowledge for

decisionmakers and technicians (advanced level) 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 certain courses it is possible to obtain a TÜV® persons certificate by passing an official.*



OT Security Courses with Persons 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 Academy 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 Academy offers a persons certification scheme in cooperation with TÜV AUSTRIA Academy (<https://www.tuv-akademie.at/en/>). The high-quality and practical OT security training courses by Limes Academy - 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 persons 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.

People with the roles of: system integrators, plant operators, planners, technicians, maintenance staff, production technicians, plant electricians, machine operators, plant IT managers, future plant and production managers; employees working directly with OT, managers whose employees work with OT, IT staff responsible for OT assets, employees responsible for the procurement, planning or operation of OT assets.

Due to changed regulatory requirements and industrial security standards (NIS directive, EU Cyber Resilience Act, 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 persons certification scheme provides significant help in this context.

Overview of the persons certification scheme

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

Level 1: Training series Operational Technology Security, course ICS.205 Certified OT Security Practitioner (COSP)

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 Certified OT Security Technical Expert (COSTE)

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 work experience of at least 6 months, averaging at least 20 hours per week



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

Level 2: Training series Operational Technology Security, course ICS.212 Certified OT Security Manager (COSM)

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 work experience of at least 6 months, averaging at least 20 hours per week



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 through an online platform provided by TÜV AUSTRIA. 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.

For public trainings, the certification can be taken immediately after the last training day. For in-house training, the certification exam can be taken online on one of the specified exam days. An overview of the current exam days can be found online:

<https://limessecurity.com/en/academy/#exam-registration>

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 Persons Certificates for OT security are valid for three years.

Digital Badges



In addition to the persons certificate, digital badges can be obtained as well. We partnered with Credly to offer a digital version of our certification. Add your Limes Academy badge to your email signature or digital resume and on social media to validate your OT security expertise. The badge contains verified metadata that describes your qualifications and the process required to earn them.

What are the benefits of Limes Academy digital badges?

- Easily manage, share and verify your OT security qualifications
- Secure verification adds credibility to your OT security achievements
- Badges provide employers and peers with concrete evidence

Claim Badge now: <https://limessecurity.com/en/academy/claim-digital-badge/>



3 hours	All employees	No laptop computer required	Course material and certificate of completion
On request	German or English	No prior knowledge required	In-house/In-house online e-learning

OT Security Fundamentals

The training course „ICS.201 OT Security Fundamentals“ is the perfect introduction to the topic of OT security. The course creates common understanding of OT security and provides guidance on how to work with it. Real incidents, practical knowledge from OT projects as well as case studies and findings from OT security assessments are used to teach participants how to understand and question the current security status of their OT environment.

Training Contents

- # Introduction:
 - What is OT security and why is it important
- # Insights from OT security incidents
 - Stuxnet, Triton, Colonial Pipeline, Solar Winds, Industroyer 1 & 2
 - Alternatively: industry-specific or company-specific incidents
 - Changes in the OT threat landscape
- # Important security aspects in the OT environment
 - Challenges
 - Disruption of availability
 - Problems with integrity
 - Loss of confidentiality
 - Common security problems in OT environments
- # Risk mitigation strategies for plant engineering, maintenance and operations personnel
 - Benefits of security requirements for industrial plants
 - General security principles
 - Organizational measures
 - Security measures for networks and communication
 - Security measures for OT components
- # Conclusion
 - Behavior in case of incidents
 - Sources for further information
 - Conclusions and key take-aways

Registration

The registration for the **ICS.201 OT Security Fundamentals Training** can be found via the adjacent link or by scanning the QR code.

<https://limessecurity.com/academy/ics-201/>



ICS.205 Certified OT Security Practitioner (COSP)



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



Training without certification: 1.990,- euros plus VAT
Training + certification incl. exam: 2.715,- euros plus VAT



German or
English



Own laptop computer
required



No prior knowledge
required



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



Course material and certificate
of completion
Optional persons certificate!

» If you only want to attain the persons
certificate without participating in the
course, please contact us.

Applied OT Security

The training „ICS.205 Certified OT Security Practitioner (COSP)“ is the perfect choice for every participant preparing for a role or function with some OT security responsibilities. The training conveys essential OT security know-how, gives an introduction to common standards and explains practical actions for the secure operation of industrial systems. Existing skills in the areas of maintenance, industrial automation, as well as instrumentation and control technology are enhanced with the ability to include the security perspective in networked industrial systems.

Training Contents

Day 1

Introduction to Operational Technology (OT)

- IT security objectives
- Evolution of OT
- OT components and terminology
- OT incidents

IT essentials

- Network protocols
- Crypto refresher
- Network security basics
- Secure network protocols

Day 2

IT vs. OT Security

- Safety vs. Security
- Characteristics of OT systems vs. IT systems

Security threats and attack vectors

- OT attackers
- OT attack vectors
- OT risk factors and threats

OT standards overview

- NIS directive
- IEC 62443
- ISO 27000 & ISO 27019
- NIST 800-82 und CSF
- and many more

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
- Identity and access management

This 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, participants should ...

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



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

Registration

The registration for the **ICS.205 Certified OT Security Practitioner (COSP)** can be found via the adjacent link or by scanning the QR code.

<https://limessecurity.com/academy/ics-205/>



ICS.211 Certified OT Security Technical Expert (COSTE)



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



Training without certification: 2.250,- euros plus VAT
Training + certification incl. exam: 2.975,- euros plus VAT



German or
English



Own laptop computer
required



ICS.201 OT Security Fundamentals
or ICS.205 Applied OT Security
Training recommended



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



Course material and certificate
of completion
Optional persons certificate!

» If you only want to attain the persons
certificate without participating in the
course, please contact us.

OT Security Advanced: Technical OT Security

The training „Certified OT Security Technical Expert (COSTE)“ aims to consolidate and deepen the existing knowledge of people with relevant professional experience in IT and OT security. The technical focus of this training provides the necessary understanding of protocols and components used as well as in-depth security knowledge of threats, current attack campaigns and the use of technical defense measures. The training enables the participants to make or prepare the right decisions regarding appropriate technical security measures and security technologies and thus to increase the security level of plant networks using proven methods and technologies.

Training Contents

Day 1

- # Introduction
 - OT threat landscape
 - Procurement of a secure system
 - Risk analysis according to IEC 62443-3-2
- # OT protocols
 - Common wired and wireless OT protocols
 - Understanding OT protocols on a technical level
 - Wireless protocols in OT environments
 - Securing industrial protocols
 - Network and protocol analysis with Wireshark

Day 2

- # Network-based attacks
 - MAC address spoofing
 - Denial-of-service attacks
 - Network sniffing
 - Protocol spoofing
 - Man-in-the-middle attacks

- # Improving OT network security
 - Network segmentation
 - Using firewalls in OT networks

Day 3

- # Applying security measures in OT
 - Security requirements and implementation
 - User management
 - Credential management
 - Host hardening
 - System monitoring and network detection
 - Anomaly and threat detection
 - Remote access
 - Backup and recovery
 - OT security market guide
 - OT security trends
- # Final Challenge

This 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

Self-assessment questionnaire

Our self-assessment questionnaire gives you an idea of whether you are a suitable candidate for the Certified OT Security Technical Expert training. More information:

<https://limessecurity.com/en/academy/ics-211/#costequestionnaire>



Registration

The registration for the **ICS.211 Certified OT Security Technical Expert (COSTE)** can be found via the adjacent link or by scanning the QR code.

After the training, participants should ...

- # have deepened and further consolidated existing knowledge in IT and OT security.
- # have a basic understanding of OT transmission technologies and protocols.
- # understand different network protection measures in the OT based on common attack patterns.
- # know the procedure for partitioning and zoning of an architecture.
- # have gained insights into the use of monitoring systems against attackers.
- # know how to technically implement security measures into OT operations.



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

<https://limessecurity.com/academy/ics-211/>



ICS.212 Certified OT Security Manager (COSM)



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



German or
English



ICS.201 OT Security Fundamentals or
ICS.205 Certified OT Security Practitioner
(COSP) Training recommended



Course material and certificate
of completion
Optional persons certificate!



Training without certification: 2.250,- euros plus VAT
Training + certification incl. exam: 2.975,- euros plus VAT



Own laptop computer
required



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

» If you only want to attain the persons
certificate without participating in the
course, please contact us.

OT Security Advanced: OT Security Management

The training „ICS.212 Certified OT Security Manager (COSM)“ 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. While organizational topics and process management are the main focus of this training, technical influencing factors are also discussed to better prepare the participants for future security decisions.

Training Contents

Day 1

- # Introduction
 - Overview, standards and frameworks
 - Tabletop exercise
- # Identify
 - Security governance and program management
 - ISMS improvement
 - Roles and responsibilities
 - System under Consideration (SuC)
 - Asset inventory
 - Risk management
 - Supply chain risk management

Day 2

- # Protect
 - Defense in depth
 - Network segmentation and zoning
 - Remote access
 - Systems security
 - Patch management
 - Identity and access management
 - Security awareness

- # Detect
 - Logging and monitoring
 - Anomaly detection
 - Vulnerability assessment

Day 3

- # Respond
 - Incident handling lifecycle
 - Post incident activities
- # Recover
 - System availability
 - Recovery planning
 - Backup

This 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

Self-assessment questionnaire

Our self-assessment questionnaire gives you an idea of whether you are a suitable candidate for the Certified OT Security Technical Expert training. More information:

<https://limesecurity.com/en/academy/ics-212/#costequestionnaire>



Registration

The registration for the **ICS.212 Certified OT Security Manager (COSM)** can be found via the adjacent link or by scanning the QR code.

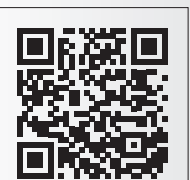
After the training,
participants
should ...

- # 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 a possible risk assessment procedure.
- # understand asset discovery and component classification capabilities.
- # understand asset discovery and component classification capabilities.
- # be able to define response plans and establish defined communication strategies for incident management.





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


<https://limesecurity.com/academy/ics-212/>





ICS.221 Assessing OT


 1 Day


 Technicians


 Own laptop computer required

 Course material and certificate of completion

 On request

 German or English

 ICS.211 Certified OT Security Technical Expert (COSTE)

 In-house / In-house online

OT Security Additions: Assessing OT

The training „ICS.221 Assessing OT“ 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 Security experts' many years of experience in conducting security assessments in an industrial environment.

Training Contents

- # Underground economy
- # Security testing requirements from IEC 62443 and ISO 27001
- # ICS asset discovery
- # Checking users and privileges
- # Configuration review of ICS systems
- # Verification of patch and software versions
- # Checking the perimeter protection
- # How to conduct 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


The registration for the **ICS.221 Assessing OT Training** can be found via the adjacent link or by scanning the QR code.


<https://limessecurity.com/academy/ics-221/>





ICS.222 OT Incident Handling Essentials


 1 Day


 Technicians and decision makers


 Own laptop computer required

 Course material and certificate of completion

 On request

 German or English

 ICS.201 OT Security Fundamentals or ICS.205 Certified OT Security Practitioner (COSP) recommended

 In-house / In-house online

OT Security Additions: Incident Handling Essentials

The training „ICS.222 OT Incident Handling Essentials“ 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 some “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 incident handling
- # Essentials and important terms
- # Incident response lifecycle
 - Preparation
 - Identification
 - Detection
 - Technical containment
 - Eradication
 - Recovery
- # Post incident process und lessons learnt

Your Benefits

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


Registration


The registration for the **ICS.222 Incident Handling Essentials Training** can be found via the adjacent link or by scanning the QR code.


<https://limessecurity.com/academy/ics-222/>





ICS.223 IEC 62443: Fundamentals, Concepts and Usage


 1 Day


 Interactive workshop


 No laptop computer required

 Course material and certificate of completion

 On request

 German or English

 No prior knowledge required

 In-house / In-house online

IEC 62443: Fundamentals, Concepts and Usage

In this mix of interactive workshop and classic training, participants are taught the most important terms and fundamental concepts of the 62443 series of standards. In group discussions and question rounds, the individual needs of the participants can be directly addressed. The experts from Limes Security also bring practical experience from years of applying the various parts of the standards in different industries, which difficulties and discussions repeatedly arise, and which approaches enable successful handling of the different standards. Concepts such as Zones & Conduits or Security Levels are also deepened in practical exercises.

Training Contents

- # Overview IEC 62443
 - Structure and certification
 - Important terms and definitions
- # Concepts
 - Risk analysis according to IEC 62443-3-2
 - Zones & conduits
 - Security & maturity levels
- # Standard parts in details
 - System Security with 2-4, 3-3, 4-1 and 4-2
 - IACS/OT Security Management with 2-1 & 2-4
 - Integration with ISO 27001

Your Benefits

- # Efficiently introduce a large number of participants to the IEC 62443 series of standards
- # Current internal challenges and questions can be addressed directly during the course under the guidance of a Limes Security IEC 62443 expert
- # Have the training individualized to your needs, or highlight your most important focus topics

Registration

The registration for the **ICS.223 IEC 62443 Fundamentals, Concepts and Usage** can be found via the adjacent link or by scanning the QR code.

<https://limessecurity.com/academy/ics-223/>



300 Security Engineering Training

Secure Products Through Improved 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 operate and which measures best protect against them.

Training Contents

The secure coding trainings 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 training „Secure

Product Development with IEC 62443-4-1“ shows participants how to integrate security into their software development process using the IEC 62443-4-1 standard part to make their products sustainably secure. 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.302
Secure Coding C#

SEC.303
Secure Coding Web

Secure Development Lifecycle

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

Security Testing

SEC.321
Security Testing Foundation



2 Days



C# developers



1.576,- euros plus VAT



German or English



Own laptop computer required



Experience in C# development



Course material and certificate of completion



In-house / In-house Online

Secure Coding for C#

During the training „Secure Coding C#“, 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 and digital signatures are discussed. Participants 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 in ASP.NET core.

Training Contents

Day 1

- # Introduction to IT security
 - History of malware and other attacks
 - Types of cyber attackers
 - IT security 101
- # Cryptography
 - Encryption
 - Hashing
 - Signatures
 - Public-key infrastructure and certificates
 - Transport Layer Security (TLS)
- # Authentication & authorization (part 1)
 - Authorization concepts
 - Passwords
 - Session management

Day 2

- # Authentication & authorization (part 2)
 - Multi-factor authentication
 - Cross-site request forgery
 - Forwards and open redirects
- # Injection attacks
 - SQL injection (SQLi)
 - Cross-site scripting (XSS)
 - Server-side template injection
 - OS command injection

This training is particularly recommended for ...

- # developers, where the training provides a mix of knowledge for both frontend and backend developers.
The training offers most value for developers with up to five years of professional experience.

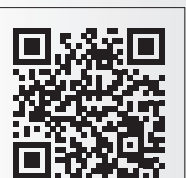
After the training, participants should ...

- # understand how attacks work and start thinking like an attacker.
- # understand why secure software development is important and how to implement it.
- # understand the necessary steps to develop software securely.
- # be capable to integrate security into their development activities.

Registration

The registration for the training **SEC.302 Secure Coding C#** can be found via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/sec-302/>





2 Days



1.576,- euros plus VAT



Developers and testers



German or English



Own laptop computer required



Experience with web technologies



Course material and certificate of completion



In-house / In-house Online

Secure Coding Web

The training „Secure Coding Web“ covers security concepts for the web, such as Transport Layer Security (TLS) and cross-origin resource sharing (CORS). It explains how session management can be securely implemented. It then details the anatomy of the most common web attacks, such as cross-site scripting, cross-site request forgery, and SQL injection, and discusses how to avoid them. In addition, more complex web attacks such as web cache poisoning, web socket injection attacks und attack on authentication frameworks like OpenID and OAuth2 are explained. Finally, best practices are explained to improve code quality through code reviews, and how to implement a secure software development process in your organization in general. Practical exercises in the different topics will be conducted for better understanding.

Training Contents

Day 1

- # Introduction to IT security
 - History of malware and other attacks
 - Types of cyber attackers
 - IT security 101 „OSINT“
- # Cryptography
 - Encryption
 - Hashing
 - Signatures
 - Public-key infrastructure and certificates
 - Transport Layer Security (TLS)
- # Access control (part 1)
 - JSON Web Tokens
 - OAuth2
 - OpenID

Day 2

- # Access control (part 2)
 - Cross-origin resource sharing
 - Cross-site request forgery
 - Web socket security
- # Injection Attacks
 - SQL injection
 - Cross-site scripting (XSS)
 - Web cache poisoning
- # Revision
 - Code review
 - Static and dynamic code analysis
 - Secure software development lifecycle

This training is particularly recommended for ...

- # developers, where the training provides a mix of knowledge for both frontend and backend developers.

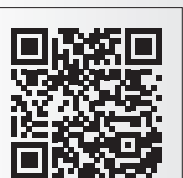
After the training, participants should ...

- # understand how attacks work and start thinking like an attacker.
- # understand why secure software development is important and how to implement it.
- # understand the necessary steps to develop software securely.
- # be capable to integrate security into their development activities.

Registration

The registration for the training **SEC.303 Secure Coding Web** can be found via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/sec-303/>



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

 2 Days

 1.576,- euros plus VAT

 Development manager, product manager, developer

 German or English

 Own laptop computer required

 No prior knowledge required

 Course material and certificate of completion

 In-house / In-house Online
Public / Public Online

Secure Product Development with IEC 62443-4-1

If you do not want to leave security and thus the quality of your products to chance, you must take a proactive approach. Only by integrating security into the development processes and by building an organization that knows how to deal professionally with security issues can high-quality products be created that meet market requirements. The training „Secure Product Development with IEC-62443-4-1“ teaches participants how security can be integrated into product development with the help of the IEC-62443-4-1 standard in order to make products lastingly secure.

Training Contents

- Day 1**
 - # Introduction to IEC 62443-4-1
 - Principles and requirements
 - # Security management
 - Product classification
 - Security organization
 - Security trainings
 - Integrity protection
 - Security of the development environment
 - Selection of secure components
 - # Specification of security requirements
 - # Secure by design and secure implementation
- Day 2**
 - # Security Verification & Validation Testing
 - # PSIRT & Security Update Management
 - # Security Guidelines

This training is particularly recommended for ...

- # Head of development
- # Process owner product development
- # Product development manager
- # Product owner
- # Scrum master
- # Product developer

After the training, participants should ...

- # understand and be able to implement the standard requirements of IEC 62443-4-1.
- # understand what secure product development involves and what is needed for it in the organization.
- # understand what a Threat Model is and what is required to develop one.
- # know suitable methods and appropriate measures for integrating security into the product development process.
- # know useful tools to verify and improve product security.
- # be able to face ongoing challenges such as dealing with legacy code, third-party component updates, or communicating vulnerabilities.

Registration

The registration for the training **SEC.311 Secure Product Development with IEC 62443-4-1** can be found via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/sec-311/>



SEC.321 Security Testing Foundation



2 Days



1.576,- euros plus VAT



Tester



German or English



Own laptop computer required



Experience with web technologies



Course material and certificate of completion



In-house / In-house Online

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. 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 we discuss how to deal with their results.

Training Contents

Day 1

- # Introduction
 - Guidelines and standards
 - Threat modeling
 - Definition of scope and test cases
 - Preparation of the testing environment
- # Security testing for cryptography
 - Encryption
 - Hashes
 - Digital signatures
 - TLS
- # Security testing for web applications
 - OWASP Top 10 and OWASP ASVS
 - Testing with Burp Suite
 - Other tools for web application testing
- # Security testing for mobile applications
 - Exposed components
 - Locally stored data

Day 2

- # Security testing for authentication
 - Bypassing authentication schemes
 - Brute-forcing attacks
 - Directory traversal attacks
 - Privilege escalations
- # Security testing of propriety interfaces and protocols
 - Fuzzing
 - Analysis and testing tools
- # Security testing for system hardening
 - System hardening
 - Discovery tools
 - Automatic vulnerability scans
 - Configuration testing
- # Collection and processing of results
 - What information is important?
 - Vulnerability management

This training is particularly recommended for ...

- # Software testers and software developers who want to get an insight into the basics of security testing

After the training, participants should ...

- # understand how attacks work and start thinking like an attacker.
- # be able to use automated testing tools to efficiently cover recurring test cases.
- # be able to document identified vulnerabilities in a meaningful way to facilitate tracking and retesting.

Registration

The registration for the training **SEC.321 Security Testing Foundation** can be found via the adjacent link or by scanning the QR code.

<https://limesecurity.com/academy/sec-321/>



Conditions of Participation

1. SCOPE OF APPLICATION

These General Terms and Conditions of Participation apply to the provision of training, E-Learning and further training measures by Limes Security GmbH (hereinafter referred to as Limes Security).

2. REGISTRATION AND ORDER

At www.limessecurity.com/en/academy you will find the complete training offer with all details and can register there directly. Registration becomes binding upon confirmation of registration from Limes Security or TÜV Austria Akademie. Places are limited and will therefore be allocated in the order of registration. Please note the registration deadline of at least 5 working days before the start of the training.

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 for payment immediately after invoicing without deductions and stating the invoice number. A surcharge of 7% will be charged for payment by credit card (PayPal). We will send you the invoice to the e-mail address you provided in the registration form before the start of the training. Unless otherwise stated in the order confirmation, the participation fee is per person and event date and includes digital training materials as well as lunch and drinks during breaks for public trainings. E-learning trainings do not include digital training materials, unless stated otherwise. Travel costs for our trainers for in-house trainings are not included in the training price and are offered separately.

4. EXAMINATION AND CERTIFICATE FEE

The currently valid examination and certificate fee can be found in the course program of the TÜV AUSTRIA Academy. If you decide to cancel your registration for the examination, you must do so in writing and there will be no charge for this up to 7 working days before the examination date. After that or in case of non-attendance, the full examination fee will be charged. The examination and certificate fee includes the issue of a certificate (German or English). The fee for an additional certificate can be found in the course program of the TÜV AUSTRIA Academy. It is possible to repeat the examination once free of charge, on the date scheduled by the certification body. Further examination repetitions will be charged according to time and effort. Unless agreed separately, E-Learning trainings generally do not include certification.

5. ACCOMMODATION

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

6. EXECUTION AND CANCELLATION

Limes Security reserves the right to cancel the trainings offered if the minimum number of participants is not reached (with the exception of E-Learning trainings). Limes Security also reserves the right to change trainers and venues as well as to change dates and the program schedule. Participants will be informed of any changes in good time. If a training does not take place, any payments already made in respect of participation shall be refunded to the participant without deductions. Further claims by the client are excluded; this also includes the case that a participant misses a seminar day through their own fault.

7. TRAINING TIMES

The specified training times, in particular the training duration as well as the end times, are to be understood as indicative values which can be influenced by interactive elements or discussions with the participants. Our trainers strive to offer the best possible learning experience for training participants. However, there is no claim to exact adherence to the training time. If at least 80% of the training units are attended, the participant will receive a certificate of attendance. Training times for E-Learning trainings can be chosen freely and individually by the participant. After successful completion, E-Learning users also receive a certificate of attendance.

8. REVOCATION AND CANCELLATIONS

Cancellations for trainings must be made in writing and are free of charge up to 7 working days before the start of the event. 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 training registration. From 6 working days up 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 follow-up training on the same topic is made 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 Limes 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 when the declaration of withdrawal becomes effective and must be paid regardless of the reasons for withdrawal. The cancellation fee shall not apply if the customer names a substitute participant who meets the admission requirements and pays the participation fee.

E-learning trainings begin on the day the login details are provided. The login details shall be provided at the latest within 7 working days of receipt of full payment by Limes Security or by an agreed deadline. Cancellations of E-Learning trainings that have already been purchased are not possible.

9. CHANGES OF BOOKING

A desired rebooking to another training or another date must be made by the customer by e-mail. Whether a rebooking is possible, and under what conditions, is to be assessed by Limes Security on a case-by-case basis. There is no right to rebooking.

10. 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.

11. COPYRIGHTS AND LICENSING

All training content and materials, including E-Learning trainings, are protected by copyright for Limes Security GmbH. For E-Learnings, the participant or his organization receives a license for use for an agreed period of time. The term "material" includes all printed materials as well as all digital media, virtual machines or digital assets offered by Limes Security and intended for use in a Limes Security training. Training materials are intended for the personal use of the training participant only. For all training materials provided, regardless of media format and purpose, it is prohibited to present, copy, reproduce or distribute and create derivative works with or without modification without the express prior written consent of Limes Security. Furthermore, the training material may not be used commercially in any way without the express written consent of Limes Security.

Conditions of Participation

The recipient of this agreement must pay a penalty of EUR 10.000 for each violation of this agreement. If a personal certificate was acquired as part of the training, it will be withdrawn from the recipient of the agreement. Payment of the contractual penalty does not release the recipient from compliance with this agreement. The right to assert claims for damages against the recipient of the agreement by the provider of the agreement is expressly reserved.

12. IMAGE, SOUND AND FILM RECORDINGS

Limes Security GmbH reserves the right to record a training for internal quality assurance purposes. The recordings will not be used for marketing or other public purposes. A provision of this recording to third parties or even participants of the training is not intended, with the exception of the disclosure to the client, if this disclosure was ordered as part of the training offer. The execution of a recording is announced by Limes Security GmbH at the start of a training. The recording can be interrupted at the request of a participant for questions or requests to speak. The recording of E-Learning trainings by the participant is explicitly prohibited.

13. DATA PROTECTION

Limes Security uses the data of customers or participants to process the booked service/purchased product. For this purpose, it may be necessary to forward the personal data to cooperation partners. The data handling is a necessary prerequisite for the execution of the contract. Depending on the type of training booked, it may be necessary to forward the data to external certification bodies for issuing the training completion documents.

14. 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 trainings lead to a delayed start or complete cancellation of a training 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 material. Limes Security accepts no liability for the theft or loss of items brought by the customer.

Grant opportunities

Under certain conditions, our courser are eligible for a grant of up to 50% of the participation fee. For more information, visit our website.



Imprint

Publisher: Limes Security GmbH, Softwarepark 49, 4232 Hagenberg; Phone: +43 720 510251; Email: office@limessecurity.com
Company Register Number: 390566 m; VAT-ID: ATU67652729; Responsible for the content: Limes Security GmbH
Design: Contentschmiede, Kremsmünster, V6.0_06_2023, Typesetting and printing errors excepted.

Validity of the Course Book

This list of courses is valid from July 1st, 2023; previous offers lose their validity.
The stated prices are valid for registration or order until June 30th, 2024.
In the event of deviations in content, the information on the website applies.



LIMES
SECURITY