LIMES SECURITY

Course book 2024/2025

Limes Academy

What Limes Academy Offers

As part of the Limes Academy, we offer training packages in the areas of security awareness, OT security and security engineering.

starting from page 10

starting from page 18

starting from page 31

Why Limes Academy?

All Limes Academy classes are held by our experienced industrial security experts, bringing you a combined experience from 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 training courses are offered in selected training centers, at our company locations or as an online format. Selected training content is also offered as e-learning. We also offer individual training courses exclusively for your company.
+ **Interactive training**	The training content taught is complemented through practical exercises. Discussions encourage the exchange of experiences between the course participants and promote understanding of what has been learned.
+ **Training materials**	The training documents are provided to you in high-quality color print or in digital format.
+ **Expertise**	All training courses are held by our security experts, who have a wealth of experience from practical projects.
+ **Actuality**	New incidents and security developments are continuously integrated into the training content. Benefit from the latest security knowledge.
+ **Certification**	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. 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.

General Training Information

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.

Align the content and examples with the level of knowledge of your employees, your industry and relevant standards / specifications / norms, both regulatory and internally from your company.

Adapt the training duration and delivery method (on-site, online) to the availability of the employees to be trained.

Adapt existing exercises or implement new exercises tailored to the specific skills of your employees.

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**
  You select 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**
  You set a date for the training in coordination with Limes Security.
- **# Implementation of the training course**
  You determine 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 your needs.
- **# Certificate of participation**
  At the end of the training, the participants will receive a certificate of completion.
- **# Optional exam**
  For certain trainings, participants can, if desired, take an official exam to attain a persons certificate through our certification partner

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.

Inhouse

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.

Inhouse 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

Selected training courses can be attended as e-learning via the Limes Academy learning platform. On request, the learning content can also be made available for the company's own LMS in standard e-learning formats (Universal SCORM V1.2 or SCORM 2004 formats; xAPI). This is particularly suitable for demand-oriented training and company-wide training programs

Our Trainers

Unsurpassed 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 & Compliance 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

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.

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.

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.

Our Trainers

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.

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.

David Schauer A O

has an in-depth understanding of security from a technical and organizational perspective. In his projects, he uses this knowledge to build a bridge between technical requirements and management strategies. He shares his experience with the participants so that they can navigate securely in both security worlds.

Bettina Wächter A O

always has a clear overview and an eye for important details. With her knowledge of ISO 27000, IEC 62443 and NIS-2 as well as her experience in working with processes, she creates the organizational framework for the introduction of management systems. She values sustainable knowledge transfer.

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.

Übersicht

100 Security Awareness & Compliance Training

200 OT Security Training

300 Product and Solution Security Training

100 Security Awareness & Compliance Training

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 Content

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**	**AWT.104** **Cybersecurity Awareness**
Compliance	**AWT.111** **Cybersecurity Employee Training in Accordance with NISG (NIS-2)**		**AWT.112** **NIS-2 Workshop for Management**	

AWT.101 IT Security Awareness

1,5–3 hours

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 75,- plus VAT
Minimum number of participants: 30 people

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://limessecurity.com/academy/awt-101/

AWT.102 OT Security Awareness

1,5–3 hours

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 75,- plus VAT
Minimum number of participants: 30 people

No prior knowledge required

Inhouse / Inhouse 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 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

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://limessecurity.com/academy/awt-102/

AWT.103 Zero Downtime: Blackout Edition

2 hours

All employees

No laptop computer required

Costs: from € 4.110 plus VAT
Number of participants: up to 80 participants

No prior knowledge required

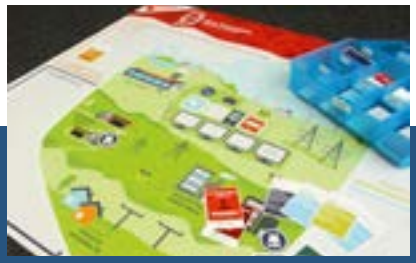
In-house / In-house online

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/

AWT.104 Cybersecurity Awareness

4 hours

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 485,- plus VAT
Minimum number of participants: 8 people

No prior knowledge required

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

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/

AWT.111 Cybersecurity Employee Training in Accordance with NISG (NIS-2)

2 hours

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 100,- plus VAT
Minimum number of participants: 30 people

No prior knowledge required

Inhouse / Inhouse online / **E-Learning**

Cybersecurity Employee Training

NISG (NIS-2) has made security a top priority in today's digital world. The aim of the training is for employees to not only understand the importance of cybersecurity for the company after completing this training, but also to have the skills and knowledge to better protect the company from cyber threats. The „Cybersecurity employee training according to NISG (NIS-2)" was therefore developed specifically for employees to prepare them for the challenges of cybersecurity. Employees are an essential key to the cybersecurity of companies and this training helps to meet the requirements of the NISG (NIS-2). This course serves as a foundation for every employee who comes into contact with network and information systems and provides a basic understanding of cyber hygiene. Experienced employees can use this training to refresh their existing security knowledge.

Training Contents

- # What is information security?
- # What are network and information systems?
- # Secure handling of information
- # Change in the threat landscape
- # What does „NIS" mean?
- # Who and what is affected?
- # Secure rules of conduct
  - Dealing with passwords and password policies
  - Dealing with programs, software and emails
  - Handling USB sticks and other external media
  - Handling your own equipment in the company (Bring your own Device – BYOD)
  - Physical security
  - Defense-in-depth approach

Your Benefits

- # Creating security awareness among the participants for an increased level of security in the company
- # Knowledge and confidence to act in accordance with the awareness-raising measures required by the NISG (NIS-2)
- # Communication of recommendations for secure working practices for all employees
- # Recognition and avoidance of risky behavior in the company

Registration

The registration for the **AWT.111 Cybersecurity Employee Training in Accordance with NISG (NIS-2)** can be found via the adjacent link or by scanning the QR code.

https://limessecurity.com/academy/awt-111

AWT.112 NIS-2 Workshop for Management

1 hour

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 150,- plus VAT
Minimum number of participants: 10 people

No prior knowledge required

Inhouse /
Inhouse online

NIS-2 Workshop for Management

The „NIS-2 Workshop for Management" is a specially designed workshop that offers people in management positions a comprehensive but compact overview of the personal obligations and liabilities arising from NIS-2. This workshop supports managers in your company to efficiently implement the requirements of NIS-2 and promote a suitable security culture. It offers practical insights and strategies that can be applied directly in practice.

Training Contents

The workshop will address the following topics with the participants:

- NIS 2 Directive and NIS 2 Law: explanation of the legal framework and requirements laid down by the NIS 2 Directive and the NIS 2 Law.
- Security culture: Importance of a strong security culture in the company and how this can be promoted.
- Risk management: Tasks in cybersecurity risk management and discussion of suitable appropriate technical, operational and organizational risk management measures in accordance with NIS 2.
- Measures, obligations and fines: Overview of the measures required to comply with NIS 2, the obligations of companies and the possible fines for non-compliance.
- Current incidents: Analysis of up-to-date security incidents and discussion of the resulting learning points.

Your Benefits

- Understanding of the requirements and obligations arising from the NIS-2 directive and the NIS-2 law to meet the company's compliance requirements
- Know how to promote a strong security culture in the company
- Practical insights and experience on suitable risk management measures as an essential building block for creating a robust and resilient digital environment in the company

Registration

The registration for the **AWT.112 NIS-2 Workshop for Management** can be found via the adjacent link or by scanning the QR code.

https://limessecurity.com/academy/awt-112

E-Learning

Several Limes Academy courses are available as e-learning options for large-scale training programs and self-paced learning.

Awareness	**AWT.102** **OT Security Awareness**
Compliance	**AWT.111** **Cybersecurity Employee Training in Accordance with NISG (NIS-2)**
Foundation	**ICS.201** **OT Security Fundamentals**

E-learning courses can be an essential building block for the successful achievement of your company's training objectives. Our e-learning offer supports the further qualification of your most important assets - your employees - with the following five advantages:

Relevant and up-to-date information at the push of a button
Up-to-date security know-how is imparted through interactive learning and can be carried out at your own pace, enabling efficient and flexible training.

Teaching important security skills
that will be required to a large extent by the „engineers of the future" in a digitalized industry.

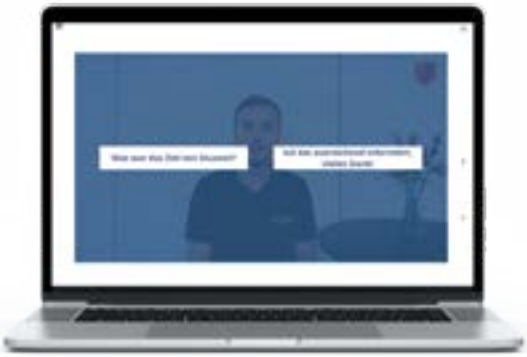
Q&A sessions with experts
provide the opportunity to enrich e-learning with interactive live sessions

Company-wide awareness
designed to educate large groups of OT employees and ensure that all OT employees, including suppliers, understand the most important security aspects.

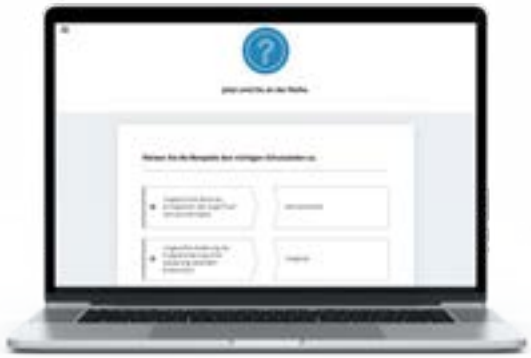
Time- and location-independent learning
is possible in our own learning management system (LMS) or your LMS (Universal SCORM V1.2 or SCORM 2004 formats; xAPI).

E-learning courses have gotten a bad reputation. Many of our customers report that their employees avoid e-learning courses because they often find them poorly structured, outdated and hardly engaging. However, as e-learning courses are a valuable tool for reaching a broad target group, we have aligned our e-learning offering with current best practices for creating effective and engaging learning content. In this way, participants are involved in the subject matter in an interactive and practical way through the use of various media formats and feedback methods.

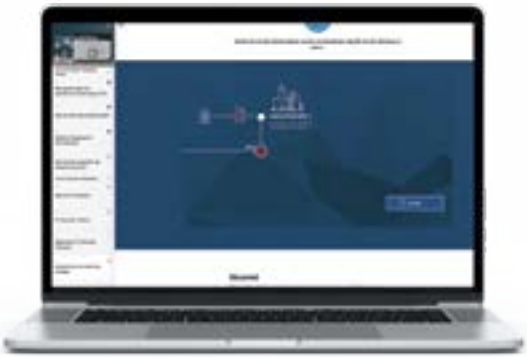
Interactive infographics offer in-depth information through clickable areas and promote visual learning.



Interactive videos and scenarios offer the opportunity for making decisions in a personalized learning path and the simulation of practical application.



Interactive quizzes encourage active participation and allow self-assessment for deeper understanding.



Current incidents and security developments are regularly updated and supplemented.

Curious?

To give you a taste of the quality and effectiveness of our courses, we offer a brief insight into our e-learning courses here.

limessecurity.com/academy/elearning-preview

200 OT Security Training

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

he 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.

Foundation Level

- **ICS.201 OT Security Fundamentals**
- **ICS.205 Certified OT Security Practitioner (COSP) ***

Advanced Level

- **ICS.211 Certified OT Security Technical Expert (COSTE) ***
- **ICS.212 Certified OT Security Manager (COSM) ***

Additions

- **ICS.221 Assessing OT**
- **ICS.222 Incident Handling Essentials**
- **ICS.223 IEC 62443 Fundamentals, Concepts and Usage**

*** 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

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 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 and in-house training courses, the certification can be taken immediately after the last day of training

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.

Recertification

Current information on recertification can be found here: **https://limessecurity.com/de/academy/re-certification/**

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/

ICS.201 OT Security Fundamentals

3 hours

All employees

No laptop computer required

Course material and certificate of completion

Cost/Participant: € 330,- plus VAT
Minimum number of participants: 15 people

No prior knowledge required

Inhouse / Inhouse 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)

3 days

Own laptop computer required

Cost/Participant: € 2.915,- plus VAT (incl. certification)
Minimum number of participants: 8 people

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

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.**

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 T 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)

3 days

Own laptop computer required

Cost/Participant: € 3.200,- plus VAT (incl. certification)
Minimum number of participants: 8 people

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

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.**

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

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.

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

Certified OT Security Technical Expert TÜV® (COSTE)

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.

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

ICS.212 Certified OT Security Manager (COSM)

3 days

Own laptop computer required

Cost/Participant: € 3.200,- plus VAT (incl. certification)
Minimum number of participants: 8 people

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

Govern
- Security governance and program management
- Roles and responsibilities
- System under Consideration-
- Supply chain risk management

Identifiy
- Improvement
- Asset inventory
- 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

Tag 3

Respond
- Incident handling lifecycle
- Post incident activities

Recover
- System availability
- Recovery planning
- Backup

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

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-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://limessecurity.com/academy/ics-212/

ICS.221 Assessing OT

1 Day

Technicians

Own laptop computer required

Course material and certificate of completion

Cost/Participant: € 770,- plus VAT
Minimum number of participants: 10 people

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

Cost/Participant: € 770,- plus VAT
Minimum number of participants: 10 people

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
  - Basics and terms
  - OT incident handling
  - Incident handling lifecycle
- # Preparation
  - Measures and defintions
  - Incident report template
- # Detection and analysis
  - Common types of indicators
  - Alert sources
  - MITRE ATT&CK
  - Hands-on: Analysis of an OT incidents
- # Containment, eradication and recovery
- # Post-incident activities

Your Benefits

- # Improve the ability to recognize security incidents as such early on
- # Understand the correct treatment of incidents in OT
- # Know what preparations need to be made in the company‘s own OT operations for security incidents

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

Cost/Participant: € 770,- plus VAT
Minimum number of participants: 10 people

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 Product and Solution Security 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 product and solution security training courses, experienced trainers from Limes Security impart the knowledge of how attackers operate and which measures best protect against them.

Training Contents

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 for OT and (I)IoT" shows participants how to integrate security into their software development process with the help of standards on order 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 Development Lifecycle

SEC.311 Secure product development for OT and (I)IoT

Security Testing

SEC.321 Security Testing Foundation

SEC.311 Secure product development for OT and (I)IoT

2,5 days

Cost/Participant: € 1.925,- plus VAT
Minimum number of participants: 8 people

Head of development, project managers, product managers, developers, quality managers, architects, tester, CE representatives

Develop products compliant with the Cyber Resilien Act, Machinery Regulation, IEC 62443-4-1 and Co

If you don't want to leave security, and therefore the quality of your products, to chance, you need to take a proactive approach. Only the integration of security into development processes and an organization that knows how to deal with this topic in a professional way will result in high-quality products that meet market requirements. The „Secure product development for OT and (I)IoT" training course teaches participants how security can be integrated into product development in order to make their products sustainably secure.

Training contents

Day 1

Overview of regulations
- Machinery regulation
- Radio Equipment Directive (RED)
- Cyber Resilience Act (CRA)

Overview of standards
- IEC 62443 in general
- IEC 62443-4-1 principles and requirements

Security Management
- Product classification
- Security organization
- Security training
- Integrity protection
- Securing the development environment
- Selection of secure components

Day 2

Specification of security requirements
- Product security environment-
- Safety & Security
- Threat analysis

Secure design & development
Security verification & validation testing

Day 3

Vulnerability management
Security update management
Security documentation

Own laptop computer required

Course material and certificate of completion

No prior knowledge required

Inhouse / Inhouse Online
Public / Public Online

The training is particularly recommended for manufacturers of ...

- # OT components
- # Machinery
- # IoT products
- # Embedded solutions

After the training, participants should ...

- # understand the connection between safety and security.
- # know regulatory and normative requirements and can implement them
- # understand what secure product development entails and what is needed in the organization to achieve it.
- # 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://limessecurity.com/academy/sec-311/

SEC.321 Security Testing Foundation

2 Days

Cost/Participant: € 1.540,- plus VAT
Minimum number of participants: 8 people

Tester

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.

The training can also be provided with a focus on security testing for embedded devices. The web topics are then replaced by relevant security testing topics from firmware, hardware and system hardening, as well as content for testing proprietary protocols and interfaces.

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 hardnening
  - System hardening
  - Discovery tools
  - Automatic vulnerability scans
  - Configuration testing
- # Collection and processing of results
  - What information is important?
  - Vulnerability management

Own laptop computer required

Course material and certificate of completion

Experience with web technologies

In-house / In-house Online

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://limessecurity.com/academy/sec-321/

Validity of the course book

This course book is valid from July 1st, 2024; previous offers lose their validity.
The stated prices are valid for registration or order until June 30th, 2025.
In the event of deviations in content, the information on the website applies.

www.limessecurity.com

Extract from the conditions of participation for trainings
You can find the full terms and conditions at https://limessecurity.com/teilnahmebedingungen/.

The prices listed are in euros plus the legal value added tax. These are due for payment 15 days after invoicing. If a training does not take place, any payments already made in respect of participation shall be refunded to the participant without deductions. Cancellations for trainings must be made in writing and are free of charge up to 7 working days before the start of the event. 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. In case of no-show or cancellation from the (first) day of the event, the full attendance fee will be charged; rebooking is no longer possible. We will gladly accept a substitute participant.

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_2024,
Typesetting and printing errors excepted.

https://limessecurity.com/de/teilnahmebedingungen

LIMES SECURITY