



CST ACADEMY
CYBER SECURITY TRANSFORMATION



SEMINARS & TRAININGS

FOR YOUR COMPANY

It is a proven fact that developing or increasing knowledge and competence in the field of information security can make a significant contribution to protecting your company from attacks. The training of your employees is a crucial component. For this reason, we have incorporated our know-how from many years of experience in the analysis and consulting of IT security topics into our seminars, trainings and workshops. This enables us to offer a wide range of individual training modules for very different target groups.

The mission of the CST Academy is to provide expert knowledge to where it is needed and to build competence to be stronger together against potential attackers. From students to top managers. This range of seminars and trainings combines and reflects just that, and I am proud of it.

Get an overview and decide on the right module for you and your employees. If you haven't found the one that's just right for you, just get in touch with us.



In our online event calendar you will find upcoming dates for many seminars, webinars and workshops. Subscribers to our CST Academy News also have the advantage of regularly receiving personal invitations to upcoming or new events.

Mareike Clemens

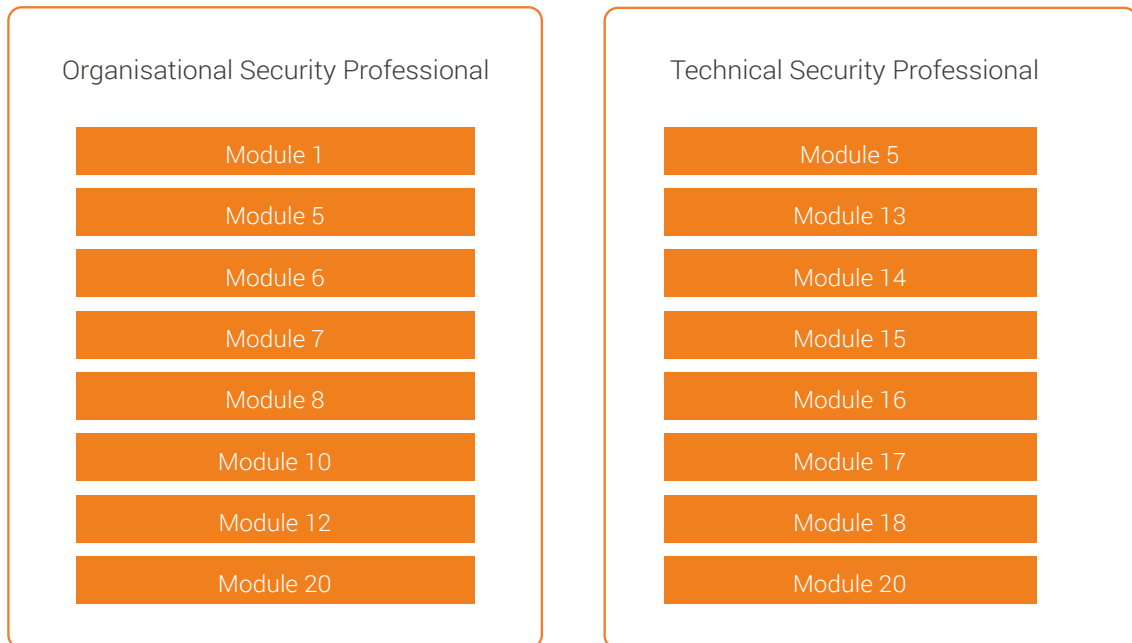
CST Academy

Phone: +49 6102 8631-550

Email: academy@usd.de



Our recommendations



You can book all modules individually in both sequence and quantity. Above we have compiled combination options for you in order to achieve a specialization. Furthermore, we are happy to assist you in the selection of suitable modules to define a training program tailored to your company.

Seminars, Workshops, Lectures and Trainings

Module 1: usd Basic Seminar: Implementation of an ISMS according to ISO 27001

Standards such as ISO 27001 provide guidance for implementing a structured information security management system. But how do you proceed? How can you establish the topic in your own company? Our seminar provides the necessary basic knowledge, initial tools for the introduction and best practices for further development.

 6 - 8 hours  suitable for career starters

 Individual on-site group seminar / Individual online group seminar

 no restricted target group / max. 12 persons

Module 2: usd Basic Seminar: PCI DSS Foundation

With the Payment Card Industry Data Security Standard (PCI DSS), the credit card industry has issued an internationally valid security standard. The security requirements it contains follow best practice approaches and serve to protect credit card data. Since 2004, PCI DSS has been mandatory for all companies that store, process or forward credit card data. The seminar provides you with the necessary background and basic knowledge of the standard and thus supports you in the successful planning and implementation of your PCI DSS project.

 6 - 8 hours  suitable for career starters

 Individual on-site group seminar / Individual online group seminar

 no restricted target group / max. 12 persons

Module 3: PCI Best Practice Workshop Online

Now an established tradition: In our role as an accredited PCI Assessor, we provide information on news relating to PCI standards and convey practical knowledge for implementation in the company. This interactive workshop offers you the opportunity to ask questions to our experienced QSAs and to exchange experiences among persons responsible for PCI in other companies.

 2 - 3 hours

 Single-place booking

 Persons responsible for PCI compliance in the company

Module 4: usd Basic Seminar: Secure Coding

Security at the application level is becoming more and more important. Today, web applications are increasingly attracting the attention of hackers and criminals and are the cause of numerous, current security incidents. Our security experts have therefore developed this seminar as an introduction to the topic: From secure software development to identifying vulnerabilities and learning appropriate countermeasures. In this seminar, you will learn the basics.



6 - 8 hours



Individual on-site group seminar / Individual online group seminar



Software developers, quality managers, and IT security experts (rough basic knowledge of web application development required) / max. 12 persons

Module 5: usd Advanced Seminar: Secure Coding

This seminar provides a deeper insight into the topic of secure coding. Because today, web applications are increasingly attracting the attention of hackers and criminals and are the cause of numerous, current security incidents. In 2 days, our security experts combine the theoretical content of the usd Basic seminar: Secure Coding (Module 4) with practical exercises to be performed by the participants.



2 days



Individual on-site group seminar



Software developers, quality managers, and IT security experts (rough basic knowledge of web application development required) / max. 12 persons



Module 6: Incident Response Tabletop

Data theft and hacker attacks on companies happen almost daily. Ensuring that your employees respond quickly and in a coordinated manner in such a case is critical to protecting your business. How well that works is a measure of the quality of your incident response plan. How do your employees react in an emergency? Where are the necessary documents kept? Who is responsible for what task?

In the Incident Response Tabletop, your employees play through defined emergency processes together with one of our experts, thus gaining confidence in the event of an emergency. Another advantage is that this workshop meets the compliance requirements of current IT security standards: IT-Grundschutz Compendium of the Federal Office for Information Security (BSI), PCI DSS, ISO/IEC 27001:2013 and others. The basis for the Incident Response Tabletop is an incident that is individually tailored to your company. Together with you, we develop a suitable scenario in advance that incorporates your guidelines and processes.

Here you can find **more information** on the procedure.



Individual on-site workshop / Individual online workshop



Chief information security officer, IT security manager, staff responsible for BCM, CERT staff, staff responsible for applications, IT infrastructure staff / max. 12 persons

Module 7: Live Hacking Demonstration

More than almost any other method, live hacking impressively and at the same time entertainingly demonstrates how easy it is to gain access to third-party data or to spy on others. Whether used individually or integrated into an existing event, live hacking is the ideal way to raise awareness among employees in your company. We offer a large portfolio of live hacking topics that are ideally tailored to the target group and their needs, either individually or in combination.

Here you will find our **list of topics**.



2 hours



suitable for career starters



Individual on-site event / Individual online event



no restricted target group / max. 25 persons

Module 8: Excursion into the Darknet

What is the Darknet? How does it work? Is it only used for illegal purposes? Our security experts will explain what the Darknet is, how it can be accessed and how it is used by criminals. During a live access via the TOR browser, they will also show which "products" are offered via the Darknet and which assets are particularly worth protecting in this context.

 2 hours  suitable for career starters

 Individual on-site event / Individual online event

 no restricted target group / max. 25 persons

Module 9: (Web based training) Phishing in the context of banks

This training, available at our used Security Awareness Platform, is specifically tailored to the needs of bank employees. Practical examples from the industry help employees, recognize and defend against phishing attacks in their daily work.

 individual  suitable for career starters

 Individual processing on the used Security Awareness Platform

 no restricted target group

Module 10: (Web based training) Information security for data owners

Regulatory requirements are increasingly calling data owners to account when it comes to protecting corporate assets. With this training, available on our used Security Awareness Platform, we prepare data owners for their new role and explain what tasks they will have to perform.

 individual  suitable for career starters

 Individual processing on the used Security Awareness Platform

 Data owners, application owners, BISOs, CBISOs

Module 11: (Web based training) Data privacy protection

What do I have to consider when handling personal data? What do retention periods, reporting requirements and TOM mean? In this training on our used Security Awareness Platform or as a individual group seminar, we answer these and other questions so that your employees can meet the legal requirements.

 individual  suitable for career starters

 Individual processing on the used Security Awareness Platform or as Individual on-site event / Individual online event

 No restricted target group

Module 12: Training: Identification of protection requirements in the role of the BISO

Regulatory requirements are increasingly calling data owners to account when it comes to protecting corporate assets. With this training, we individually address the roles and responsibilities of application owners and teach the Information Security Compliance Evaluation (ISCE) process.

 4 hours  suitable for career starters

 Individual on-site workshop / Individual online workshop

 Data owners, application owners, BISOs, CBISOs / max. 12 persons

Module 13: Training: Security Champions

When introducing DevSecOps methods, one of the success factors is to promote acceptance of the security organization within the company. We therefore recommend training and establishing qualified contacts for security issues (so-called "security champions") directly in the IT and project organization. Security champions reduce the inhibition threshold against contact with the security organization and they know the pain points of the respective IT and project organization.

 4 blocks of 2 hours each plus "homework"

 Individual on-site workshop / Individual online workshop

 Employees in the IT and project organizations / max. 12 persons

Module 14: Seminar: IT security basics

The situation regarding IT security is more critical than ever. Attackers are becoming stronger and stronger and developing more complex attack methods. However, the more colleagues are engaged with the topic of IT security and have mastered the basics, the better prepared you will be. This group seminar with theory content, critical discussions, and consideration of real-world case studies is a great foundation training. How do you recognize threats? What appropriate countermeasures can be defined at the organizational and technical level? What might concepts for comprehensive security management look like?

 6 blocks of 3 hours each  suitable for career starters

 Individual on-site group seminar / Individual online group seminar


 no restricted target group / max. 12 persons

Module 15: Training: Secure system operation

This training provides important security relevant content for administrators in system operations. Common questions and problems of this target group are considered, and the general understanding of system hardening, patch and change management, alerting and monitoring is improved.

 6 - 8 hours

 Individual on-site workshop / Individual online workshop

 IT administrators for Linux and Windows / max. 12 persons

Module 15A: Training: PCI DSS – Technical scoping for administrators

This training provides important PCI DSS and security related content for administrators in system operations. Common questions and problems of this target group are considered, with a special focus on systems in the PCI scope: typical systems in the scope, requirements for these systems and regularly recurring requirements.

 6 - 8 hours

 Individual on-site workshop / Individual online workshop

 IT administrators for Linux and Windows / max. 12 persons

Module 16: Mentoring of company pentest managers

We provide advice and support for the initial implementation of a vulnerability testing process in the context of technical security analyses - from briefing or training of the responsible employees in the context of a pentest workflow to the establishment of a continuous vulnerability management.



individual



On-site coaching / online coaching



responsible employees in the context of a pentest workflow

Module 17: Internship with a usd HeroLab Pentester

Are unauthorized persons able to penetrate your systems and applications? To test this, you have hired the security analysts of usd HeroLab. They use professional tools to gather information and try to penetrate your systems and applications in a targeted, individual and inventive way. This simulation of a real attack will deliver high quality results for you.

Our internship offers you a unique opportunity: not only do you read the final pentest report, but you also have the chance to review together with the responsible pentester how he proceeded and which vulnerabilities he uncovered in your system or application.



individual and target group-oriented



On-site internship / (online internship on request)



Persons responsible for the systems and applications under investigation

Module 18: usd Advanced Seminar: Understanding A Hacker's Mind

A great introduction to pentesting. Only if you know and understand the relevant threats in IT system landscapes can you take effective countermeasures. In our usd Advanced Seminar, we show you with the help of theory and a lot of practice which intentions, methods and tools a hacker uses and go into more detail on how you can protect your systems in the best possible way.



2 days



suitable for career starters



Individual on-site group seminar



System administrators, IT operations managers, information security officers (ISOs). In principle, however, it is also suitable for all others interested in IT security who would like to understand how attackers proceed and how to protect their own IT systems against such attacks. A basic understanding of technical aspects of IT should be brought along in order to be able to follow the practical examples / max. 12 participants

Module 19: usd PentestLab

The PentestLab is the heart of our technology environment. With a constantly growing number of pre-configured server environments, different technologies and vulnerabilities of varying degrees of difficulty, pentesters can train their methodological skills, creativity and stamina in "real life pentesting". The platform is used by our own pentesters for training and further education and is also the technical basis for the regularly held usd Hacking Night at the CST Academy and Hacker Contests at universities.



individual



in the usd PentestLab



Knowledge of Kali Linux and working with virtual machines is required. This module is a great supplement to modules 18 and 22.

Module 20: Theorie Seminar: Introduction in pentesting

During a penetration test, or pentest for short, the analyst performing the test slips into the role of an attacker. Before he can even launch an attack, thorough preparation is required: the pentester must have mastered the relevant Kali Linux tools and gathered sufficient information about the target system and known vulnerabilities. Our theory seminar guides the participants through all phases - from the methodology in Kali Linux to the creation of the final pentest report.



several weeks



Individual on-site group seminar / Individual online group seminar



People interested in IT security who want to understand how pentesters work. A basic understanding of technical aspects of IT should be brought along in order to be able to follow the practical examples / max. 12 persons.

Module 21: Practical Seminar: Pentesting

Would you like to not only get access to usd PentestLab and take over our virtual machines, but also discuss your results with others and learn more about the vulnerabilities found there? Then this is the right hands-on seminar for you! Participants can try out attack methods and protection measures for networks, systems and applications in the secured environment of the usd PentestLab. During set modules, pentest-specific topics, such as a selection of OWASP Top 10 web vulnerabilities, are covered and results of the practical sessions are discussed.



several weeks



Individual on-site group seminar



Knowledge of Kali Linux and working with virtual machines is required. / max. 8 persons

Module 22: Event: Hacking Day

Participants will gain insights into the everyday working life of a professional usd HeroLab pentester. The job requires a variety of skills. What are those exactly and what does a typical day at usd HeroLab look like? Are there any typical days at all? But we don't just talk about hacking on the day, we also do it - together with the participants. No matter if MySQL, PHP, Axis, Tomcat, JBoss, ftp, webdav, or snmp - a variety of technologies will be examined for vulnerabilities under the guidance of trained security analysts.



1 day



suitable for career starters



individual on-site event



Knowledge of Kali Linux is required / max. 12 persons

CST Academy Community events

In the CST Academy event calendar, we publish events covering current topics and exciting questions for the community throughout the year.

usd Webinars

usd Webinars - compact, interactive, up-to-date. Several times a year, we offer free one-hour webinars on current or practice-relevant IT security topics.



1 hour



suitable for career starters

Online / German and English / free-of-charge

CST Academy Cyber Security Forum

We invite everyone to this compact evening event to exchange ideas on important developments in the world of cyber security and to identify common fields of action. Regardless of profession, technical background and level of knowledge. From students to top managers.



3 hours

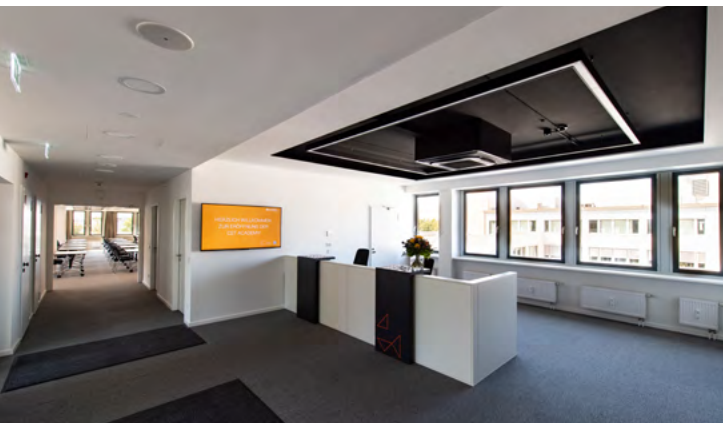


suitable for career starters

On-Site / German / free-of-charge

Use the high quality conference facilities of the CST Academy

The 550 sqm conference floor with air-conditioning and separate entrance was completely renovated in 2018 and impresses with state-of-the-art conference technology and light-flooded rooms. The total of three conference rooms in different sizes can be flexibly furnished with seating. The lounge with kitchenette and the roof terrace invite you to relax.



Our three conference rooms are each equipped with state-of-the-art conference technology, screens or projectors and can be flexibly furnished with seating:

- 1 plenary room for about 60 persons
- 1 board room for about 12 persons
- 1 board room for about 8 persons



usd AG

Frankfurter Str. 233, Forum C1
63263 Neu-Isenburg
Germany

Phone: +49 6102 8631-550

Email: academy@usd.de

www.usd.de/en | usd.de/en/cst-academy