CAS Cyber Security Expert («CSECAS»)

In this CAS course, you will address the offensive security aspect in hands-on exercises and learn the tools for IT administrators and security analysts. Their aim is to increase the effectiveness of their IT security measures.

Duration: 17.5 days
Price: 17'200.–
Course documents: Digicomp courseware and accompanying books

Content

Cyber security specialists are currently in high demand. Especially offensive security approaches are of great importance for the defense against modern attack scenarios. Therefore you will receive several days of Ethical Hacking Hands-on-Training with KALI LINUX™ and other penetration testing tools. After completing the CAS, you will possess profound skills in the field of offensive information security and will be able to check the effectiveness of associated cyber security measures. In the study concept, special emphasis is placed on practical implementation.

Exam preparation and presentation CAS thesis and OPST exam (3.5 days)

The participants conduct an OSSTMM-compliant security audit of an infrastructure on their own or in a group. The methods and techniques learned during the training are practically applied and tested in a penetration testing scenario. Together with the client, the framework of the audit is defined and carried out using the OSSTMM method. The conclusion of the CAS work represents a presentation of the audit results to the co-students. A representative of the management and a technician of the client will also be present.

Key Learnings

- Knowledge of definitions and principles of the Information Security Management System (ISMS)
- Knowledge of the position of ISO/IEC 27001 within the framework of the Information Security Management System (ISMS)
- Knowledge of the concepts and contents of the Information Security Management System (ISMS)
- Overview of the Security Controls of ISO/IEC 27001
- Knowledge of current scenarios of attacks on networks and systems
- Keeping your knowledge up to date with sound sources
- Proposing measures to protect network and system security
- Practical implementation aids for the implementation of protective measures
- Independent application of the most important hacking tools and assessment of the dangers they pose
- Explaining advanced hacking methods and proposing countermeasures
- Testing the security of your own company in test environments (hacking labs) with ethical hacking methods based on KALI Linux
- Knowing creative approaches to combining hacking methods
- Integrating offensive insights into cyber security strategies
- Ideal preparation for the official OPST certification exam recognized by the Institute for Security and Open Methodologies (ISECOM) and La Salle University in Barcelona
- Know the basics of OSSTMM
- Knowledge of the practical applications of a security tester
- Knowledge of the tools for security testing and how to use them
- Know various attacks on web applications (including underlying databases and backends) that you then execute yourself
- Knowledge of the basics of secure software development (OWASP)
- In-depth examination of various potential hazard scenarios
- Targeted addressing and presentation of final security reports according to OSSTMM

Methodology & didactics

The following learning methods are used within the scope of this training

- Active teaching conversations with the participants
- Reflection and exchange of experiences from one's own practice in the context of theory
- Discussion and analysis of examples from the learning material
- Practical tasks for the transfer of the acquired knowledge and competences to one's own person

Throughout the entire course, you will work on practical tasks adapted to your level, which support the practical transfer of what you have learned.

- According to HWZ, the CAS has a total expenditure of 15 ECTS, which is 300 working hours. About 1/3 of these hours are spent in class and the rest is homework, exam preparation and CAS work
- The CAS work itself is about 40-60 working hours including presentation
- For the rest of the homework, the previous knowledge is very important

Target audience

This course is aimed at information security managers, information system architects, security testers, security auditors, security consultants, security engineers, network engineers and system administrators.

Requirements

Experience in projects and in the daily use of information technologies, IT systems and networks is required. Basic knowledge of information security, analogous to the following course, is also desired:

- The basics of IT security («P2S»)

Certification

1. ISO/IEC 27001 Foundation
    - is completed after the 1st module «Course: ISO/IEC 27001 Foundation («IS27F»)»
2. EXIN Ethical Hacker Foundation
    - to complete the 4th module «Course: Cyber Security Tester – Hands-on Professional («HAK2»)» separately
3. OSSTMM OPST
    - Completed on the last day of the course
    - The candidate must demonstrate the acquired skills in a penetration testing scenario.
    - The OPST certification was also recognized for the «Master in Information Technology Security» diploma awarded by La Salle University in Barcelona. This facility is part of La Salle's international education network, which also includes Manhattan College in New York and La Salle University in Philadelphia. All OPST certificates bear both the ISECOM and La Salle seals of approval as a sign of their prestige.
4. Presentation of CAS thesis at Digicomp Academy
    - Separate appointment by arrangement
5. A total of 15 ECTS points will be awarded by the HWZ

Information session

- CAS Cyber Security Expert

Additional information

Module sequence / dates
The sequence of the modules must be set up and adhered to. However, this does not apply to the modules «ISO/IEC 27001 Foundation» and «Create secure websites». You can complete these courses at a later date within the CAS training. You are free to choose the dates for the modules.

The following topics are not covered in this CAS

- In-depth study of Information Security Management Systems (ISMS)
- Enterprise Risk Management
- IT Law (Data Protection Act, ...)
- Leadership in Information Security

The CAS and ECTS points are awarded by our partner, University of Applied Sciences in Business Administration Zurich (HWZ).

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/cyber-security-offense/training-course-cas-cyber-security-expert