Cybersecurity engineer, part-time (15 months) (Titre RNCP)

by DataScientest

Practical course - 32d - 224h00 - Ref. 3CS

Price : 11990 CHF E.T.

NEW

Become a cybersecurity expert to protect and secure infrastructures and data. A cybersecurity engineer is a specialist who plays a vital role in protecting corporate infrastructures and sensitive data against cyber-attacks. This distance learning course combines synchronous exchanges with an expert trainer, practical exercises and e-learning modules. Based on the Learning By Doing pedagogy, you will carry out a red thread project in a team to put your knowledge into practice. When you enroll, you will be assigned to one of the Datascientest promotions. At the end of the course, you'll be awarded a "Data, Network and System Security Manager" RNCP level 7 certificate, issued by HEXAGONE and registered with the RNCP under n°RNCP37796. Contact us now to find out about upcoming dates!

Teaching objectives

At the end of the training, the participant will be able to:

- Define an organization's cybersecurity strategy.
- Develop and manage an organization's cybersecurity processes.
- Maintain the security of an organization's information system.
- Manage cybersecurity incidents and crises.

Intended audience

Anyone with an interest in cybersecurity who wants to retrain or upgrade their skills.

Prerequisites

A degree or diploma at bac+3 level in IT.

PARTICIPANTS

Anyone with an interest in cybersecurity who wants to retrain or upgrade their skills.

PREREQUISITES

A degree or diploma at bac+3 level in IT.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

Certification

At the end of the course, the pedagogical team will evaluate the learner's project with a written report and a distance defense. Validation of the skills developed during the Cybersecurity Engineer training course will enable you to obtain : A certificate in "Data, network and systems security management", a level 7 RNCP certification issued by HEXAGONE and registered with the RNCP under n°RNCP37796.

Practical details

Digital activities

Online courses and exercises, group masterclasses, question/answer sessions, support classes, e-mail coaching, red thread projects, individualized career coaching, social learning.

Mentoring

An expert trainer accompanies learners throughout their training. He or she regularly discusses the learner's project and provides individual mentoring. Several trainers also lead the various masterclasses (group classes) and answer learners' questions at any time from a dedicated forum. In addition, numerous question-and-answer sessions can be organized to help learners.

Pedagogy and practice

Upon registration, the learner is assigned to a class (dates to be defined at the time of registration) and receives a training schedule. The training program is divided into "Sprint" sessions lasting several weeks on a dedicated theme. Each week, the learner is invited to a time of exchange with the trainer, in the form of a masterclass (group class) or mentoring sessions (individual). For 80% of the time, the learner works independently on the teaching platform. All modules include practical exercises to put into practice the concepts developed in class. Learners are also required to work in pairs or trios on a common theme throughout the course. This will enable them to develop and gain recognition for their skills. In addition, themed events and workshops are regularly offered to enable learners to discover the latest innovations in cybersecurity. In order to follow the course effectively, we estimate that between 8 and 10 hours of work are required per week.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

Course schedule

1 Upcoming session dates

- November 2025: Start date 04/11/25
- January 2026: Start date 01/13/26

2 System and network fundamentals

- Network basics.
- Linux & Windows system fundamentals.
- Programming and scripting.

3 Cybersecurity and SOC fundamentals

- Introduction to cybersecurity.
- Legal guide.
- SOC architecture and organization.

4 Network security with Stormshield

- Certified Stormshield Network Administrator.

5 Cryptography & System hardening

- Cryptography and IGC.
- System hardening.

6 SIEM Splunk

- Introduction Splunk.
- Basic commands.
- Reports and visualization.

7 Ethical Hacking

- Intrusion testing methodology.
- Hacking techniques.
- Report writing.

8 APT & Mitre ATT&CK

- APT attack study.
- Framework Mitre ATT&CK.
- Adversary Emulation.

9 Intrusion detection

- Intrusion detection rule.
- Analyze events and qualify incidents.
- Cyber Threat Intelligence.

10 Forensics & incident response

- Incident response.
- Computer Forensics.
- Cybercrisis preparation and management.

11 Cybersecurity engineers

- The role of the cybersecurity engineer.
- Cyber Watch.
- Raising awareness.

12 Implementation of SSI standards

- Introduction to CRM.
- ISO 27001 Lead Implementer.
- Other safety standards.

13 Indicators and project monitoring

- Cybersecurity audits.
- Safety indicators.

14 Risk analysis

- ISO 27005 RM.
- Ebios Risk Manager.
- Other risk analysis methodologies.

15 Incident management and business continuity

- ISO 27035.
- PCI/PRI.
- Other safety standards.