Updated on 12/17/2024

Sign up

EBIOS Risk Manager Certification Training

3 days (21 hours)

PRESENTATION

Master IT risk management with our EBIOS Manager training course. Immersive, educational workshops to help you understand this famous analysis method. We'll teach you the fundamentals of IT security threat management through a captivating educational approach. You'll learn how to detect and prioritize threats through hands-on exercises. What's more, our methodology is based on the analysis of real-life situations, an indispensable method for understanding the real origin of risks, SR/OV combinations, and concepts such as ATT&CK and CAPEC. Our EBIOS Manager training course is perfect if you want to master IT risk management methodically, thanks to the application of effective management strategies. On completion of the course, you will be able to take the EBIOS Manager certification, free of charge, on the last day of the course.

OBJECTIVES

- Understanding the EBIOS Risk Manager method and its various use cases
- Managing and assessing risks
- Get the resources and tools you need for optimal risk assessment
- Be ready to take the exam at the end of the session

TARGET AUDIENCE

- IT security professionals
- SSI
- IS Project Managers
- Security Consultants

Prerequisites

Knowledge of information systems security risk management.

EBIOS Risk certification training program

Manager

Day 1: Course objectives and structure

- Group introduction
- Global aspects
- Training objectives and schedule
- Educational approach
- Learning assessment

Initial presentation of the EBIOS Risk Manager method

- Risk management fundamentals
- Introduction to EBIOS Risk Manager
- Focus on IT security (priority threats)
- Key definitions of EBIOS Risk Manager
- Exercise 1: Understanding key terms
- Central idea and workshop of the EBIOS Risk Manager method
- Summary

Workshop 1: "Security framework and foundation

- Workshop presentation
- Defining the scope of the study and the project
- Defining the professional and technical field
- Identification of feared events and assessment of their severity
- Defining the security base
- Exercise 2: Identifying feared events
- Workshop summary

Section 4 - Workshop 2: "Risk origins

- Introduction to the workshop
- Identification of sources of risk (SR) and their Target Objectives (TO)
- Assessing the suitability of combinations
- Evaluation of SR/OV combinations and selection of the highest priorities for analysis
- Assessing the severity of strategic scenarios
- Exercise 3: Evaluating SR/OV combinations
- Summary

Day 2: Workshop 3: "Strategic scenarios

- Introduction
- Assessment of the threat level associated with stakeholders
- Digital threat mapping of the ecosystem and critical stakeholders
- Exercise 4: Assessing the threat level associated with stakeholders
- Development of strategic scenarios
- Exercise 5: Developing strategic scenarios
- Defining safety measures for the ecosystem
- Workshop summary

Workshop 4: "Operational scenarios

- Introduction
- Development of operational scenarios
- Probability evaluation
- Advanced (Threat modeling, ATT&CK, CAPEC)
- Exercise 6: Creating an operational scenario
- Workshop summary

Workshop 5: "Risk management

- Introduction
- Summary of risk scenarios
- Defining management strategy
- Definition of safety measures in a Continuous Safety Improvement Plan (CSIP)
- Assessment and documentation of residual risks
- Setting up a risk monitoring framework
- Exercise 7: Developing a PACS (Continuous Improvement Safety Plan)
- Conclusion

Day 3: Taking the EBIOS Manager exam

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as enrolment is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the format selected. This

The questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.