Immersive chain - Information systems risks

by Reality Academy

Practical course - 0,5d - 00h40 - Ref. 8CB

Price : 95 € E.T.

NEW

Prévenir les cyberattaques avec des mises en situation à 360° dans le quotidien de collaborateurs confrontés à des tentatives de cybercriminalité. Renforcez la vigilance de vos collaborateurs en les sensibilisant aux menaces telles que le phishing, l'ingénierie sociale et les ransomwares. Réduisez les risques et protégez les données de votre entreprise en développant des réflexes de cybersécurité essentiels.

Teaching objectives

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

- Identify the main cyber-attack techniques and detect the signs of attempted fraud or digital intrusion.
- Analyze the potential vulnerabilities and threats associated with handling sensitive data in your professional environment.
- Apply best cybersecurity practices to secure equipment, exchanges and confidential company information.

PARTICIPANTS

PREREQUISITES

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.

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

Practical details

Digital activities

By Reality Academy training courses are immersive and interactive. Learning by doing is a powerful skills-building tool: immersed in a virtual classroom, the learner selects his or her training course and plunges into the scenario. They experience a situation, make a decision in the 1st person and live the direct consequences.

Mentoring

The tutoring option offers personalized support from an ORSYS trainer who is an expert in the field. Adapted to the needs, abilities and pace of each learner, this tutoring combines asynchronous follow-up (personalized corrections of exercises, unlimited exchanges by message...) and individual synchronous exchanges. The result: better understanding, skills development and lasting commitment to training.

Pedagogy and practice

Get advice and feedback from leading experts. Discover their tricks of the trade and the reasons behind their successes through real-life testimonials. Learners take part in an active discovery exercise to complement and/or reinforce the expert's notional input, and benefit from feedback tailored to their response. During each course, discover operational cases created by experts to help learners put into practice what they have just learned. Find a complete and effective summary sheet! Each learner can keep a written record of what they've learned and the advice they've received.

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 Cybersecurity essentials

Digital activities

Enjeu : Les cyberattaques ciblent de plus en plus les entreprises, mettant en péril la sécurité des données et la continuité des activités. Identifier ces menaces est essentiel pour les contrer. Ce que je vis : En immersion dans des scénarios réalistes, vous êtes confronté à des cyberattaques et apprenez à les repérer, réagir efficacement et renforcer votre vigilance.

2 Protecting sensitive data

Digital activities

Enjeu : La protection des données sensibles est un enjeu majeur pour les entreprises. Une mauvaise gestion peut entraîner des pertes financières, des atteintes à la réputation et des sanctions légales. Ce que je vis : À travers des mises en situation interactives, vous apprenez à reconnaître les risques liés à la gestion des données et à adopter des comportements adaptés pour limiter les fuites et les attaques.