AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/07/2024

Sign up

CyberSecurity crisis management training

4 days (28 hours)

PRESENTATION

Our exclusive "Cybersecurity Crisis Management" training course will help you meet the challenges of IT security. Ransomware, phishing, SQL injections: cybercriminals are vying with each other to undermine the protection of your infrastructure.

Our course program is divided into four parts, which are essential for understanding and establishing a cybersecurity crisis/risk management plan. We begin with an introduction to IT security, covering in detail the main concepts involved in protecting both networks and applications.

Next, we'll define the notion of "crisis": "what is a crisis?" and "how can we remedy it? ?". You'll learn about the different types of crisis and how to identify them. We'll focus on creating a crisis plan by assessing impacts, metrics and responsibilities.

As is often the case, we'll include a practical section to help you apply the concepts discussed above, through a series of exercises based on realistic scenarios.

OBJECTIVES

- Identifying cybersecurity risk issues
- Understanding cybersecurity categories
- Understanding the typology of cybercrime tools
- Know the fundamentals of crisis management
- Drawing up a crisis management plan in the event of a cyber attack

TARGET AUDIENCE

- IT security project managers
- SSI technicians

- Auditors
- CISO / RSSI
- Highly critical engineers or administrators

Prerequisites

Basic knowledge of cybersecurity.

Programme of our CyberSecurity crisis management training course

Day 1 - The issues

- The challenges of cybersecurity risks
  - Overview of cyberthreats in France
  - The challenges
- Tripartite doctrine
  - Confidentiality
  - Integrity
  - Availability
- Cybersecurity categories
  - Network security
  - Application security
  - Information security
  - Operational safety
  - Resilience and business continuity
  - Acculturation and training of users :
- The risks
  - What is a risk?
  - What are the most common threats?
- A typology of cybercrime tools
- Best practices in cybersecurity

Day 2 - The fundamentals of crisis management

- Understanding the fundamentals of crisis management
- What is a crisis?
  - Incident
  - Accident
  - Emergency situation
  - Crisis
- What is crisis management?
  - Incident detection
  - Qualification
  - Climbing
  - Crisis management protocol invoked
- Crisis protocol invocation process

- Crisis units
  - Operational crisis unit
  - Decision-making crisis unit

Day 3 - The management plan

- Formalizing a crisis management plan in the event of a cyber attack
  - Metric
  - Impact assessment
  - RACI matrix
  - Roles and responsibilities
  - Communication channels
- Communication
  - Internal communication
  - External communication
  - Specific communication
- Crisis scenarios
  - Partial unavailability of the information system
  - Total unavailability of the information system
  - Loss of dependency (exogenous edge effects)
- Key elements for drafting the deliverable

Day 4 - Exercises

- Crisis management protocol drafting exercise
  - Teamwork based on a supplied scenario
- Crisis management exercise
  - Teamwork based on the previous crisis protocol exercise

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 registration is finalized, the learner receives a self-assessment questionnaire which enables 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 for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which 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.