Training - Data Protection and Cybersecurity

DMCYBR-EN-D | **Distance only** | **5 days**

This course provides:

Level
Awareness

Public
IT staff and technical teams interested in cybersecurity. Engineers and technicians involved in data management and E&P data processing (G&G, national data base/reservoir engineering/production and field development). Data governance. Legal affairs. Human resources. Corporate risk management teams.

Objectives
Attendees will be able to implement the following skills:

- Define the elements of an Information Security Management System (ISMS)
- Describe network security fundamentals and evaluate the security configuration of networks
- Identify the steps of establishing a Security Operations Center (SOC);
- Describe the most common security attacks and their countermeasures
- Understand the security consequences of Cloud computing and define mitigating measures

Pedagogical & technical resources
Daily lecture, exercises, and case studies

Assessment of achievements

- Trainees are assessed throughout the training through practical application phases and interactions with the trainer
- A final on-the-spot evaluation may also be carried out at the end of the course and/or at the end of each module using tests designed to verify the learners' understanding and assimilation of the knowledge linked to the training objectives

Prerequisites
No prerequisites are necessary to follow this course

Responsable
IFP Training instructors, with expertise in the field and trained in modern teaching methods adapted to the specific needs of learners from the professional world

Program

INTRODUCTION TO CYBER SECURITY

Importance of cybersecurity, cyber-attacks and lessons learned, cyber warfare, what are we trying to protect, are we successful?

SETTING UP AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Starting with ISMS: overview of key concepts based on ISO 27001, key artifacts.
Introduction to risk management: purpose and specifics of risk management in an IT setting, qualitative vs. quantitative risk management.
Principles of information security policies and procedures: different kinds of documents: policies, procedures, guidelines and

standards, roles and objectives of policies & procedures, typical content and format.
Workshop writing information security policies and procedures part I: group-based exercise in writing a brand-new information security policy on a chosen topic.

SECURING INDUSTRIAL SYSTEMS

Introduction into securing industrial systems:

- Overview of industrial systems such as SCADA and DCS and the impact on the ISMS.
- Practical concerns and considerations around industrial systems.

Overview of the IEC 62443 standard: overview of the IEC 62443 standard which applies specifically for securing industrial systems.

SPECIAL TOPICS INFORMATION SECURITY

Cloud computing:

- Developments in cloud computing, applicability within industrial systems.
- IaaS, PaaS, SaaS.

Setting up a Cyber Security Operations Center (SOC): benefits and challenges of a SOC, building and operating an industrial SOC.
Summary and the way forward:

- Recap of the course.
- Keeping the momentum going, suggested practical next steps.

SETTING UP DATA SECURITY

Data security: best practices of securing the organization’s data, data breaches and their impact.
Hands-on exercises based on real cases: Data breach incident management/data handling ethics.

To French entities : IFP Training is referenced to DataDock ; you may contact your OPCO about potential funding.
Please contact our disabled persons referent to check the accessibility of this training program : referent.handicap@ifptraining.com