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

Updated 10/30/2024

Sign up

OSIR™ training (IR-200)

ALL-IN-ONE: EXAM INCLUDED IN IR-200 COURSE FEE

5 days (35 hours)

PRESENTATION

Would you like to improve security incident management and strengthen your organization's defenses against cyber attacks? With our OSIR™ (OffSec Incident Response) certification preparation, you can develop essential skills to detect, analyze, contain, eradicate and recover from security incidents, while reducing the risks to your organization.

During OSIR™ training, you'll learn how to use incident response tools such as intrusion detection systems (IDS), security event management solutions (SIEM) and forensic tools.

You will also be trained to manage communications during a security crisis, write technical reports, and coordinate efforts within teams.

Various topics will be covered, such as malware analysis, securing network access points, managing suspicious artifacts, and restoring compromised systems. We'll also explore best practices in post-incident monitoring to prevent recurrence.

With this training, you'll gain skills in incident response management and active defense, while effectively preparing for the OSIR™ exam.

After completing this training, you'll be ready to take the OSIR™ certification and apply your skills in a professional environment.

OBJECTIVES

- Understanding the incident response lifecycle
- Identify and analyze common cyber attacks
- Using forensic tools for incident management
- Eradicate threats and restore compromised systems
- Write technical reports and communicate effectively

TARGET AUDIENCE

- SOC Analysts
- Blue Team Specialists
- Incident Responders

Prerequisites

- Solid grounding in TCP/IP networks
- Knowledge of Linux and Windows operating systems
- Understanding of cybersecurity concepts, including threat and vulnerability management

Software requirements

- **Kali Linux** --> Download here

Note: Ambient IT does not own OSIR™, this certification belongs to OffSec ® Services LLC.

OUR OSIR™ CERTIFICATION TRAINING PROGRAM

Incident response concepts and practices

- Introduction to incident response
- Fundamentals of cyber defense
- Incident response lifecycle
- Tools commonly used for incident response
- Incident detection strategies
- Case studies: real-life incidents

Overview of the cyberattack landscape

- Types of cyber attack (phishing, ransomware, etc.)
- Motivations of the attackers : Hacktivism, cybercrime, industrial espionage

- Common attack techniques: brute force attacks, SQL injections and vulnerability exploitation
- Study APT (Advanced Persistent Threats) groups: Understanding the tactics and APT group methods
- Analysis of current cybersecurity trends: evolving threats, new attack vectors
- Attack mapping with MITRE ATT&CK: Using the MITRE framework

Incident analysis and evidence management

- Incident investigation: Collect, preserve and analyze digital evidence
- Log and artifact analysis techniques: Analysis of system, network and application logs to trace incidents
- Forensic tools: Use of tools such as Autopsy, FTK Imager, for investigations post-incident
- Malware analysis methodology: Detect, analyze and neutralize active malware
- Incident impact assessment: Measuring the impact of attacks on critical assets
- Documentation of investigations: Writing techniques

Threat eradication and system restoration

- Malware cleaning and removal
- Analysis of entry points used
- Eradication scripts and automations
- Post-eradication test
- Recovery of compromised data
- Preventing future incidents

Recovery and return to operational status

- Restore affected systems
- Checking for security updates
- Post-recovery monitoring
- Post-incident communication
- Economic and reputational impact assessment
- Continuous improvement plan

Communication practices and incident reporting

- The importance of communication in incident response
- Writing technical reports
- Presentation of results to stakeholders
- Collaboration with internal and external teams
- Incident documentation
- Use of reporting tools

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.