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

Updated 09/17/2024

Sign up

OSTH™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN THE PRICE OF THE TH-200 COURSE

3 days (21 hours)

PRESENTATION

Would you like to centralize and optimize the management of your business processes? With our preparation for OSTH certification, it is totally possible to integrate monitoring tools or management and analysis. This will help your operations run more smoothly and automate repetitive tasks for greater efficiency.

During OSTH™ training, you'll learn how to use features like workflow management, task automation, real-time performance monitoring as well as integration with other information systems.

Topics covered will include interface customization, advanced reporting tools, and access to a collaborative platform for better team coordination. We'll also explore integrated security mechanisms to protect data.

With this training, you'll acquire skills in project management, business process automation and data analysis.

Once you've completed our preparation, you'll be eligible for passage to OSTH™ certification.

OBJECTIVES

- Implement and manage security measures to ensure that systems and networks remain secure against threats
- Master the fundamental concepts of threat hunting
- Identify the motivations and techniques of threat actors
- Writing and communicating threat-hunting reports effectively
- Analyze and detect threats from network data

- Using IoCs to identify malicious activity

TARGET AUDIENCE

- Web intrusion testers
- Ethical hackers
- IT security specialists
- SOC Analysts

Prerequisites

- Solid grounding in TCP/IP networks
- Knowledge of Linux and Windows operating systems
- Basic understanding of cybersecurity concepts

Software requirements

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

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

OSTH™ CERTIFICATION TRAINING PROGRAM

Concepts and practices of threat hunting

- Introduction to threat hunting
- The basics of proactive cyber defense
- Threat hunting life cycle
- Commonly used tools and technologies
- Threat detection strategies
- Case studies: real-life examples of threat hunting

Overview of the threat landscape

- Types and motivations of threat actors
- Common attack techniques used by cybercriminals
- Studies of APT (Advanced Persistent Threats) groups
- Analysis of current cyberthreat trends
- Threat mapping and MITRE ATT&CK techniques

Communication and reporting for threat hunters

- The importance of communication in the hunt for threats
- Writing technical reports for safety teams
- Presentation of results to stakeholders
- Collaboration with internal and external teams
- Threat-hunting investigation documentation practices
- Use of automated reporting tools

Hunting for network data

- Introduction to network data analysis for threat hunting
- Monitoring and collecting network logs
- Detecting anomalies in network traffic
- Techniques for detecting malicious behavior
- Use solutions such as Wireshark, Zeek, and Suricata
- Practical exercises in network attack detection

The hunt for end points

- Endpoint threat identification and analysis
- Endpoint investigation techniques (EDR, XDR)
- Collecting artifacts: logs, processes, memory
- Detection of fileless and persistence attacks
- Endpoint malware analysis techniques
- Practical examples and case studies

Threat hunting with IoCs

- Introduction to Indicators of Compromission (IoCs)
- Sources of information on IoCs: CTI, Threat Intelligence Platforms
- Integration and correlation of IoCs with security tools
- IoC-based detection methods
- Using IoCs for proactive hunting
- Case studies: threat hunting with real-time IoCs
-
-

Companies concerned

This training 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 on entry to the training program 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 objectives.

This 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. This questionnaire also enables us to anticipate any connection or internal security difficulties within the company (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.