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

Updated 04/22/2024

Sign up

Training and preparation for OSDA™ Certification

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH EXP-301 COURSE

3 days (21 hours)

PRESENTATION

OSDA™ certification is an essential way of proving your skills in operations security and defensive analysis.

It attests to your mastery of the fundamental principles of IT security and your ability to detect, analyze and respond to security threats effectively.

The OSDA™ exam is made up of several modules covering a wide range of topics, including:

- corporate networks
- Server- and client-side attacks
- Escalating privileges

Each module tests your knowledge and skills in specific areas of operational security and defensive analysis.

Our OSDA™ training offers comprehensive preparation for the exam, providing in-depth educational content and practical exercises to reinforce your understanding of the concepts.

We cover every aspect of the certification program, focusing on practical skills and industry best practices.

OSDA™ training is constantly updated to reflect the latest trends and developments in IT security.

OBJECTIVES

- Understanding the principles of Lockheed-Martin Cyber Kill-Chain
- Acquire the skills needed to analyze Windows and Linux event logs
- Master the use of non-graphical scripts and commands
- Identify and evaluate server- and client-side attack logging artifacts
- Develop advanced privilege escalation skills on Windows systems

TARGET AUDIENCE

- Web intrusion testers
- Safety researchers
- Analysts SOC

Prerequisites

- Previous experience in operations security or defensive analysis is preferred
- Basic knowledge of Windows and Linux operating systems
- Familiarity with event detection and logging tools
- Practical experience with common IT security tools is a plus
- An understanding of the basic principles of reverse engineering and malware analysis would be an asset.

Software requirements

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

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

OSAD™ CERTIFICATION TRAINING PROGRAM

Introduction to the fundamentals of security and defensive analysis

- Understanding corporate networks and the DMZ
- Study of deployment environments
- Differentiation between core and edge network devices
- Analysis of virtual private networks (VPNs) and remote sites
- Exploring the stages of Lockheed-Martin's Cyber Kill-Chain
- Application of Cyber Kill-Chain to malware examples
  - Cryptomining
  - Ransomware

- Introduction to the MITRE ATT&CK Framework classifications
- Case analysis of OilRig, APT3 and APT28 campaigns with the MITRE ATT&CK Framework

Windows Endpoint Fundamentals

- Understanding Windows processes and services
- Exploring the structure and value types of the Windows Registry
- Using scripts and non-graphical commands to interact with Windows
- Creation of custom batch scripts, Visual Basic scripts and PowerShell functions
- Introduction to Windows event logs
- Event log analysis with Windows Event Viewer and PowerShell

Windows server-side attacks

- Analysis of credential abuse and attacks on web applications
- Evaluation of logging artifacts in command injection attacks
- Understanding binary attacks
  - via buffer overflows and generated artifacts
- Windows Defender Exploit Guard usage study
- Evaluation of logging artifacts generated by Windows Defender Exploit Guard

Windows client-side attacks

- Analysis of attacks via Microsoft Office software
- Use of social engineering and spearphishing techniques
- Evaluation of logging artifacts generated by phishing attacks
- PowerShell monitoring to detect attacks and suspicious activity
- Understanding PowerShell's extensive logging capabilities

Windows privilege escalation

- Understanding Windows integrity levels and UAC
- Detection of privilege escalation attempts
- Evaluation of logging artifacts created by UAC bypass techniques
- Use of privilege escalation techniques to SYSTEM
- Analysis of service permissions for privilege escalation

Introduction to Linux endpoints

- Understanding Linux applications and daemons
- Exploring Syslog infrastructure and daemon logging
- Web log analysis under Linux
- Automate defensive analysis with scripts
- Use DevOps tools to extend scripting capabilities
- Application of acquired skills in a real-life hunting scenario

Detection of network attacks and escapes

- Understanding network segmentation
- Using iptables to implement segmentation
- Detection of egress bypass attempts
- Understanding port forwarding and tunneling
- Use tools to detect tunneling attempts
- Application of Snort rules to detect attacks and C2 communications

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 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.