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

Updated on 12/05/2025

Sign up

CDSA Certification Training

All-In-One: Preparation & Exam included in the price

3 days (21 hours)

Presentation

Our CDSA Certification training course will enable you to validate your practical and technical skills in defensive security and become an SOC analyst. The role of the SOC analyst is to detect, analyze and respond to security threats affecting corporate information systems.

Our training program will teach you all the steps and techniques involved in an SOC analysis, and will enable you to take the CDSA certification exam at the end of the 3 days.

At the end of this course, you'll be able to identify, exploit and document vulnerabilities, and propose solutions to strengthen and optimize security.

Objectives

- Understand the fundamental concepts of defensive cybersecurity and how an SOC works.
- Master the collection, analysis and correlation of system, network and application logs.
- Identify malicious activity from SIEM data.
- Investigate real incidents involving attacks on Windows, Active or the network.
- Efficient use of threat hunting, forensics and malware detection tools.
- Write clear, usable incident reports
- Prepare for and pass the official CDSA certification exam.

Target audience

- SOC Analyst

- Cybersecurity Analysts
- Security Consultants
- System administrators

Prerequisites

- Solid knowledge of IT security
- Fundamental notions of threat detection
- Knowledge of scripting languages such as Python or Ruby

CDSA Certification Training Program

SOC & Incident Management

- Understanding the role of the SOC
- Steps in the incident management cycle
  - NIST
  - WITHOUT
- Incident triage and escalation techniques
- Use of ticketing and team communication tools
- Writing incident reports
- Incident simulations in controlled environments

SIEM and Tactical Analysis

- SIEM architecture and operation
- Log collection and ingestion
  - Windows
  - Linux
  - Network
- Creating dashboards and queries
- Incident analysis via Splunk
- Threat detection via Elastic Stack
- Investigation with multi-source log correlation

Log and Analysis Event

- Identify suspicious behavior
- Exploring Windows event logs
- Authentication and network connection logs
- Multiple event correlation
- Evtx, Sysmon, Winlogbeat for detailed analysis

Network analysis & IDS/IPS

- Packet analysis fundamentals
- Analysis of PCAPs linked to real threats
- Analysis of attack patterns
- Using Snort, Suricata as IDS/IPS
- NetFlow flow analysis and security alerts
- Deploying a network detection environment

Windows & Active Directory attacks

- Introduction to Active Directory
- Kerberoasting, DCSync, Pass-the-Ticket
- Creating custom detection rules
- Analysis of malicious PowerShell scripts

Malware analysis

- Types of malware
  - Ransomware
  - Info-stealer
  - Droppers
- Static analysis of a malicious binary
- Unscrambling malicious JavaScript code
- Sandbox and dynamic analysis techniques
- Extracting Indicators of Compromise

Threat Hunting & Forensics

- Proactive detection via hypothesis
- Introduction to digital forensics
- Post-mortem compromise analysis
- Creating threat response playbooks

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, 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.