Certified SOC Analyst (CSA)

Description

Why choose the Certified SOC Analyst (CSA) training?

The Certified SOC Analyst (CSA) training is designed for professionals looking to gain cybersecurity expertise. This course covers key processes and technologies used in Security Operations Centers (SOC), enabling you to identify, analyze, and effectively respond to security threats. Through a hands-on approach and real-time exercises, you will learn how to interpret security events and master modern tools like Splunk and ELK.

Enhance your expertise in cybersecurity

Joining this training will provide you with a deep understanding of threat detection strategies and incident management. By learning to use SIEM solutions and developing your incident response skills, you will become a key player in protecting critical infrastructures. With structured, practical content, this training is an excellent springboard for SOC analysts or anyone looking to specialize in cybersecurity.

Course Content
Module 1: Security Operations Center

- Introduction to SOC
- Roles and responsibilities
- Tools used in SOC

Module 2: CIO cyber threats and attack techniques

- Understanding CIO threats
- Common attack techniques
- Practical case studies

Module 3: Incidents, events, and logging

- Types of security incidents
- Event logging
- Log analysis

Module 4: Incident detection and event management

- Incident detection tools
- Managing security incidents
- Best practices in event management

Module 5: Advanced incident detection with Threat Intelligence

- Using Threat Intelligence solutions
- Identifying emerging threats
- Automating incident response

Module 6: Security incident response

- Incident response processes
- Collaboration with IRT teams
- Writing incident reports

Documentation

- Digital course materials included

Exam

- This course prepares to the Certified SOC Analyst (CCSA) + certification
- In order to receive the Certified SOC Analyst (CCSA) +, learners must pass two exams: 312-39.
- Number of questions: 150
- Duration: 4 hours
- If you wish to take this exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- SOC analysts
- Cybersecurity analysts
- Network administrators
- IT security professionals

Prerequisites

- Basic knowledge of cybersecurity
- Understanding of networks and telecom
- Familiarity with logging concepts
- Experience with SIEM solutions

Objectives

- Master the basics of SOC
- Learn to monitor and analyze log files
- Identify threats with IOC indicators
- Administer SIEM solutions
- Detect and manage security incidents
- Develop threat analysis reports

Description
Certified SOC Analyst (CSA) training
Niveau

Intermédiaire

Classroom Registration Price (CHF)

3950

Virtual Classroom Registration Price (CHF)

3800

Duration (in Days)

3

Reference

CSA