Publication date : 01/16/2024

Course : SOC (Security Operations Center) Analyst course

Practical course - 8d - 56h00 - Ref. ASR
Price : 5370 CHF E.T.

BEST

At the end of the course, the learner will be able to perform the functions of a Security Operations Center (SOC) analyst, mainly detecting and analyzing intrusions, anticipating and implementing the necessary protection measures.

Teaching objectives

At the end of the training, the participant will be able to:

- Understanding the organization of a SOC
- Understanding the SOC analyst's job
- Understanding the tools used by SOC analysts
- Identify key issues through use cases
- Learn to detect intrusions
- Managing incidents
- Optimizing information system security

Intended audience

System and network technicians and administrators, IT managers, security consultants, engineers, technical managers, network architects, project managers...

Prerequisites

Familiarity with the ANSSI security guide, knowledge of networks, introductory course in cybersecurity or equivalent.

Practical details

Hands-on work

Numerous practical exercises on setting up and using SOC analyst tools, intrusion detection, the most common problems and post-incident analysis.

PARTICIPANTS

System and network technicians and administrators, IT managers, security consultants, engineers, technical managers, network architects, project managers...

PREREQUISITES

Familiarity with the ANSSI security guide, knowledge of networks, introductory course in cybersecurity or equivalent.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

Composition de la formation

SOC analyst, the job

Ref. ASH - 2 days ★ 4 / 5

Log collection and analysis, a SIEM to optimize your IS security

Ref. LCA - 3 days ★ 4 / 5

Forensic analysis

Ref. AFB - 3 days ★ 4 / 5

Course schedule

1 The SOC (Security Operation Center)

- What is a SOC?
- What is it used for? Why are more and more companies using it?
- SOC functions: logging, monitoring, audit and security reporting, post-incident analysis.
- The benefits of a SOC.
- SOC solutions.
- SIM (Security Information Management).
- SIEM (Security Information and Event Management).
- SEM (Security Event Management).
- Example of a monitoring strategy.

2 The SOC analyst's job

- What does a SOC analyst do?
- What are its skills?
- Monitor and sort alerts and events.
- Know how to prioritize alerts.

3 Information gathering

- Heterogeneous sources. What is a safety event?
- Security Event Information Management (SIEM). Events collected from the IS.
- Equipment system logs (firewalls, routers, servers, databases, etc.).
- Passive collection in listening mode and active collection.

4 Optimizing IS security: tools, best practices, pitfalls to avoid

- Overview of solutions and products.
- Syslog.
- The SEC.
- Splunk software.
- French legislation.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 Intrusion detection, the main issues

- Understand network protocols (TCP, UDP, ARP, ICMP, routers, firewalls, proxies, etc.).
- Attacks on TCP/IP (spoofing, denial of service, session theft, SNMP attacks, etc.).
- Intelligence gathering, trace search, network scans.
- Trojans, backdoors, browser bugs, Covert Channels, distributed denial-of-service agents...
- Attacks and exploitation of vulnerabilities (takeover, DDoS, buffer overflow, RootKits, etc.).

6 How do you manage an incident?

- Signs of successful IS intrusion.
- What have the hackers achieved? How far did they get?
- How do you react to a successful intrusion?
- Which servers are affected?
- Find the entry point and fill it.
- The Unix/Windows toolbox for evidence retrieval.
- Clean-up and return to production of compromised servers.

7 Analyze incidents for better protection: forensic analysis

- Computer forensics: types of computer crime, role of the computer investigator.
- Modern cybercrime.
- Digital proof.

8 Forensic analysis of a Windows operating system

- Acquisition, analysis and response.
- Understanding start-up processes.
- Collect volatile and non-volatile data.
- How the password system and Windows registry work.
- Analysis of data contained in RAM and Windows files.
- Cache analysis, cookie and browsing history, event history.

Dates and locations

REMOTE CLASS
2026 : 21 May, 25 June, 1 Oct., 5 Nov.