Publication date : 07/24/2025

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

Practical course - 3d - 21h00 - Ref. LCA
Price : 2470 CHF E.T.

4,1 / 5

This training course will give you an overview of supervision issues, the legal obligations involved in data retention, and enable you to quickly master the skills needed to implement a software solution tailored to your needs.

Teaching objectives

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

- Know your legal obligations regarding data retention
- Log analysis approach
- Installing and configuring Syslog
- Understanding correlation and analysis with SEC

Intended audience

System and network administrators.

Prerequisites

Good knowledge of networks, systems and IS security.

Practical details

Numerous exercises and case studies will be proposed throughout the course.

Course schedule

1 Information gathering

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

Hands-on work

Log analysis procedure. Geolocating an address. Correlating logs from different sources, visualizing, sorting and searching for rules.

PARTICIPANTS

System and network administrators.

PREREQUISITES

Good knowledge of networks, systems and IS security.

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.

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.

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

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

Hands-on work

Installation and configuration of Syslog, SEC, Splunk, ELK and more. Example of data analysis and correlation.

3 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.
- Detect trojans, backdoors, browser bug exploits, covert channels, distributed denial-of-service agents...
- Attacks and exploitation of vulnerabilities (takeover, DDoS, buffer overflow, rootkits, etc.).

Dates and locations

REMOTE CLASS
2026 : 1 June, 9 Sep., 5 Oct., 16 Nov.

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.