Publication date : 05/02/2024

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

Practical course - 2d - 14h00 - Ref. LOG
Price : 1730 CHF E.T.

This training course will give you an overview of supervision issues, the legal obligations involved in data retention, and the skills you need to quickly 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

Hands-on work

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

Course schedule

1 Introduction

- Information systems security.
- Supervision and logging issues.
- Standardization possibilities.
- What are the advantages of centralized supervision?
- Market solutions.

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 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.

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

3 Syslog

- Syslog protocol.
- The client part and the server part.
- Centralize event logs with Syslog.
- Is Syslog enough? Advantages and disadvantages.

Hands-on work
Installation and configuration of Syslog. Example of data analysis and correlation.

4 The SEC program

- Introducing SEC (Simple Event Correlator).
- Configuration file and rules.
- How do you detect interesting patterns?
- Correlation and analysis with SEC.

Hands-on work
Installation and configuration of SEC. Example of data analysis and correlation.

5 Splunk software

- MapReduce architecture and framework. How do you collect and index data?
- Exploiting machine data. Transaction authentication.
- Integration with LDAP directories and Active Directory servers.
- Other software on the market: Syslog, SEC (Simple Event Correlator), ELK (Elastic suite), Graylog, OSSIM, etc.

Hands-on work
Installation and configuration of software (Splunk, ELK or other). Example of data analysis and correlation.

6 French legislation

- How long logs are kept. Scope of use and legislation. The CNIL. Employment law.
- The IT charter, its content and the validation process.
- How do you set up an IT charter?
- Its contribution to the safety chain.

Hands-on work
Example of an IT charter.

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.

7 Conclusion

- Best practices. Pitfalls to avoid. Choosing the right tools. The future for these applications.

Dates and locations

REMOTE CLASS
2026 : 16 Mar., 22 June, 5 Oct., 16 Nov.