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

Practical course - 3d - 21h00 - Ref. LCA
Price : 2100 € 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.

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.

PARIS LA DÉFENSE
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.