Course : Securing your virtualized environment

Synthesis course - 2d - 14h00 - Ref. VMW
Price : 2020 CHF E.T.

★★★★⯪ **4,2 / 5**

This course will provide you with a technical overview of solutions for ensuring the security of your virtualized environments: from the main weaknesses of virtualized architectures to the optimum implementation of security solutions.

Teaching objectives

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

- ✓ Identify security threats in virtualized environments
- ✓ Understanding attack typologies
- ✓ Secure virtual data centers, VMs, servers and workstations
- ✓ Evaluate available tools and techniques

Intended audience

IT managers, production/operations managers and system or network administrators.

Prerequisites

Basic knowledge of technical architecture (systems and networks) and IT security.

Course schedule

1 Introduction to safety

- Safety: reactive, proactive, predictive.
- Internal and external threats.
- Fields of application (servers, workstations, clients, applications).

2 Virtualization techniques

- Context isolation, hypervirtualization, paravirtualization.
- I/O virtualization, classic and container.
- Unikernel systems, microviewers.

PARTICIPANTS
IT managers, production/operations managers and system or network administrators.

PREREQUISITES
Basic knowledge of technical architecture (systems and networks) and IT 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.

3 Safety in the industrial environment

- Reason's model.
- Organizations and disasters.
- Backups, replications, DRP.
- Trusted third party, man-in-the-middle attack.

4 Security in a virtualized environment

- Industrial benefits, risks.
- Diapers to watch out for.
- The Zero Trust security model: a new paradigm?
- Microsegmentation.
- Defense in depth.
- Security domains: network, system, management, applications.

5 Security with VMware

- OSI layers.
- VLANs, routing, virtual switches, VSS, VDS, N1KV, VXLAN and logical switches.
- Certification services provider, AD, LDAP, Nis, VMware NSX Edge.
- System security principles: trusted zones (DMZ), password policy.
- Encryption algorithms, public and private keys, self-signed certificates, trusted authority.

6 VMware application security

- Antivirus: VMsafe API, vShield Endpoint.
- Application mapping, flow management.
- Isolation: application sandboxing, containers.
- VMware Photon, ieVM.
- API protection.

7 Prediction, prevention, detection and remediation

- Overview of tools (Nessus, Nmap, Kali).
- Intrusion detection and testing.
- Logs, machine learning.
- Behavioral analysis.
- Risks and criticality: vCenter Operations Manager (VMware).
- Risk mapping.
- Supervision and monitoring, alarms.

8 Management security

- ACL, simple authentication, roles and privileges.
- Social engineering.
- BYOD, shadow IT (rogue IT).
- Virtual infrastructure hardening plan.
- Update and backup management.

Dates and locations

REMOTE CLASS

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.

2026 : 2 June, 24 Nov.