

# Cloud Security

## Security Concepts in Automated Data Centers

The advent of the cloud in the daily working environment does not only entail advantages, but also some risks. One of these risks refers to the topic of cloud security. No matter whether a cloud is operated on-premises or hosted, the operator of the cloud platform has to think carefully about cloud security beforehand. In this environment, conventional protection measures quickly reach their limits. Modern cloud security methods, in contrast, offer effective protection on the one hand, but also options of flexibility and scalability of the cloud, on the other hand. The course gives a holistic overview as well as a sound know-how basis on the topic of cloud security, along with a presentation of current threats and possible solution approaches by different vendors.

### Course Contents

- Setup of a Cloud Data Center from a Security Viewpoint
- Network Security
- Hard- and Software Firewalls
- Security Concepts with SDN
- Virtualization Security
- Hypervisor Security
- Design Examples with Cisco, VMware, and Others
- Workplace Security
- Identity and Access Management
- Bring Your Own Device

**E-Book** You will receive the comprehensive documentation package of the ExpertTeach Networking series – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

### Target Group

The course at hand addresses technicians and pre-sales staff concerned with the setup of cloud security.

### Prerequisites

Basic network and IT knowledge should be available. In addition, the participant should be able to define basic terms of the cloud and cloud infrastructure. Ideally, the participant has the knowledge taught in the course Cloud Deployment - Getting Started, Development and Migration.

### This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

[www.expertech-training.com/go/CLSE](http://www.expertech-training.com/go/CLSE)

### Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

### Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

### Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	2 Days	€ 1,595
Online Training	2 Days	€ 1,595
Date/course venue	Course language German 	
16/03-17/03/23  Frankfurt	16/03-17/03/23  Online	

Status 11/12/2022



# Table of Contents

## Cloud Security – Security Concepts in Automated Data Centers

<b>1 Introduction to Cloud Security</b>	3.2.4 IDS and IPS	4.2.3 What is a directory service?
1.1 Cloud Security Basics	3.2.5 Malware Protection	4.2.4 Active Directory
1.2 Cloud Security - Organizational Aspects	3.2.6 Identity Based Firewalling	4.3 Authentication in the network (SSO)
1.2.1 Data protection and compliance	3.2.7 Market and functional overview	4.3.1 Single sign-on
1.2.2 Multi-Cloud	3.2.8 Palo Alto	4.3.2 Security Assertion Markup Language (SAML)
1.2.3 Responsibilities in Cloud Security	3.2.9 Fortinet	4.3.3 Open Authentication 2 (OAuth2)
1.2.4 Public cloud: What should be considered?	3.2.10 Cisco	4.4 Information about user activity
1.2.5 Overview of compliance programs	3.3 Security and Network Function Virtualization	4.5 Example: Microsoft Azure Active Directory
1.3 Application security in cloud environments	3.3.1 Security vulnerabilities of NFV	4.6 Security and identity management
1.3.1 OWASP Top 10	3.3.2 Protective measures	4.7 Example: Keystone from OpenStack
<b>2 Private Cloud and Virtualization Security</b>	3.3.3 NFV Security Management Lifecycle	<b>5 Access to the cloud</b>
2.1 Physical access	3.3.4 NFV Security Framework	5.1 Setting up cloud infrastructures
2.2 Network Security in Virtualized Environments	3.4 Concepts with SDN	5.1.1 Hybrid Cloud: Impact on all layers
2.3 Data Center Edge Security	3.4.1 Realization of the VNF FG	5.2 VPNs at a glance
2.4 Data Center Core Security	3.4.2 Advantages of the VNF FG	5.2.1 MPLS VPNs
2.5 Security in the Aggregation Layer	3.5 Example based on ACI from Cisco	5.2.2 IP VPNs
2.5.1 IP access lists	3.5.1 Use of device packages	5.3 VPN gateways for cloud connectivity
2.5.2 Quality of Service	3.5.2 Service Graphs Templates	5.3.1 Cloud-based VPN
2.6 Security in the Access Layer	3.5.3 Virtual router (CSR1000v)	5.4 Example: MS Express Route
2.7 Virtualization	3.5.4 Example of virtual edge router: Juniper vMX	5.5 vCloud Air Hybrid Cloud Manager
2.8 Introduction to SAN Security	3.6 Example: Deploying Networks in Azure	5.6 Cisco CloudCenter
2.9 Server security in virtualized environments	3.6.1 Subnets	<b>6 Danger from the user</b>
2.10 Hypervisor Security	3.6.2 Routing	6.1 Security measures for clients
2.10.1 VMware	3.6.3 DNS	6.1.1 Anti-virus programs
2.10.2 KVM	3.7 Security features	6.1.2 Personal firewalls
2.10.3 Hyper-V	3.7.1 User-defined routes (UDR)	6.1.3 Patch management
2.10.4 Container virtualization (Docker)	3.7.2 Network Security Groups (NSG)	6.1.4 Hard disk encryption
2.11 Example based on OpenStack	3.7.3 DDoS protection	6.2 Security awareness measures
2.12 Example based on VMware NSX	3.7.4 Firewall	6.2.1 Involving users
2.12.1 NSX Distributed Firewall	3.8 Coupling of networks	6.2.2 Reveal reasons
2.12.2 Edge Devices	3.8.1 Peerings	6.2.3 Making restrictions understandable
2.12.3 Check Point vSec	3.8.2 Gateways (for VPN etc.)	6.3 Cisco AMP
<b>3 Public Cloud: IaaS protection etc.</b>	3.8.3 Hybrid vs. cloud-only	6.4 The concept of proxies
3.1 Service Virtualization	<b>4 Access permissions and management</b>	6.4.1 Transparent proxies
3.1.1 Local Server Load Balancing	4.1 User accounts and passwords	6.4.2 Reverse proxies
3.1.2 Virtual Firewalls - Contexts	4.1.1 Access via CLI	6.4.3 Generic proxies
3.2 Next Generation Firewalls	4.1.2 Default parameters	6.4.4 Application Layer Gateways
3.2.1 Stateful Inspection	4.2 Identity management	6.4.5 Mode of operation
3.2.2 Content Awareness and URL Filtering	4.2.1 Central user management	6.4.6 Limitations
3.2.3 Bot detection	4.2.2 Market and function overview	6.4.7 Web proxies



### ExperTech GmbH

Waldstraße 94 • 63128 Dietzenbach • Phone: +49 6074 4868-0 • Fax: +49 6074 4868-109  
 info@expertech.de • www.expertech-training.com

