Oracle Cloud Infrastructure Security Professional (2023): Hands-on Workshop

Oracle Cloud Infrastructure

DURATION	MODULES	COURSE CODE
4 Days	**18 Lectures**	**—**

Course Overview

This course will be delivered with a live lab. This is a complete course for security administrators, who want to learn about the security features available on Oracle Cloud. It covers security in every aspect of Oracle Cloud. You will get to gain hands-on experience in working with network security, Vault, Master Encryption Key, Data Safe, Web Application Firewall, Cloud Guard, Security Zones and more.

What You Will Learn

Module 1: Security Introduction

- Shared Security Model
- Zero Trust Security
- Concept
- Principles
- Security Design and Controls
- Platform Security
- Physical Security: Data Center Site & Inside Data Center
- Operational Security
- Secure Connectivity
- Data and Application Protection
- Culture of Trust and Compliance

Module 2: Security Services Overview

- Security Services Introduction
- Use Cases and Security Services
- Object Storage Security

Module 3: Identity and Access Management (IAM)

- Introduction
- What is OCI IAM?
- OCI Identity Concepts
- Resources and Identifying OCI Resources (OCIDs)
- Identity Domains
- Use Cases
- Types
- Authentication & Authorization
- AuthN, AuthZ
- Principals, Subjects Clause, Actions Clause
- Policies
- Common Policies

Compartments: Resource Compartments, Access, Interaction, Multiple Regions, Nested Compartments

- Quotas and Budgets on Compartments
- Policy Inheritance and Attachment: Inheritance, Attachment
- Conditional Policies, Conditions, Examples
- Advanced Policies
- Permissions, Network Sources, Tag-Based Access Control, Dynamic Groups
- Federation
- Concepts, User Groups Mapping, User Types
- Federating with Identity Providers
- Understanding Sign-In Options, New Account Creation
- When to Use OCI IAM and IDCS

Module 4: Infrastructure Security – Networking

- Introduction to Virtual Cloud Network (VCN)
- OCI Architecture Overview
- VCN Basics: CIDR Notation, IP Address Range, Subnets
- VCN Security
- Security Lists (SL), Network Security Groups (NSG), SL + NSG
- Stateful & Stateless Security Rules
- Bastion Host
- Demos: SL + NSG, Stateful & Stateless Rules
- VCN Connectivity
- Connectivity Options: Site-to-Site VPN (IPSec), FastConnect
- VPN & FastConnect Configuration Workflow, Use Cases, Providers
- VCN Peering
- Local Peering (Within Region), Remote Peering (Across Regions)
- Transit Routing: Hub & Spoke, Route Tables, Private Access to Oracle Services
- DNS Service
- OCI DNS Management, Capabilities, Private DNS
- IAM Policies for Networking Admins/Users

Module 5: Infrastructure Security – Load Balancer

- Load Balancing Concepts
- Flexible vs Fixed Load Balancer, HTTP/2 Support
- Public vs Private Load Balancer, Regional & AD-specific Subnets
- Policies, Health Checks, SSL Handling
- Demo: SSL Termination, Certificates, Listeners
- Bastion Overview

Module 6: Infrastructure Security – Compute and OS Management

- Compute Best Practices & Security Recommendations
- Shielded Instances
- OS Management Service
- Overview, Oracle Linux & Windows, Enterprise-Class Support
- OSMS for Oracle Linux, Instance Details, Package Updates, Software Sources
- Fleet Management: Managed Instance Groups
- CVEs, Scheduled Jobs, Metrics & Alarms
- Dedicated Virtual Machine Hosts
- Example Scenarios, Shapes, Limitations
- Vulnerability Scanning
- Sources, Setup

Module 7: Security for Container Engine for Kubernetes (OKE)

- IAM Policies and RBAC
- Controlling Cluster Access, RBAC Authorizer
- Kubernetes Secrets
- Encryption at Rest in etcd
- Cluster Security
- Pod Security Policies, SecurityPolicy Admission Controller
- Node Pool Security
- Node Instance Security Options
- Network Security for Pods
- Subnet Security Lists, Network Policies, Using Calico
- Multi-Tenant Considerations
- Namespaces-as-a-Service, Clusters-as-a-Service Models
- OKE Recommendations
- Image Security
- Container Image Signing & Scanning, Viewing Scan Results

Module 8: Security for Oracle Functions

- IAM Policies for Invoke and Management Access
- Network Sources and IP Restrictions
- Private Network Support for Functions
- NSG Usage for Functions

- Functions Container Security
- Limited Permissions, Image Signing & Scanning
- Functions Image Scanning & Signing

Module 1: Data and Database Security Fundamentals

- Encryption Basics
- Encryption at Rest and In-Transit
- Symmetric Encryption
- Asymmetric Encryption
- Encryption Concepts
- Hardware Security Module (HSM)
- Vault Overview
- OCI Vault, Vaults, Keys
- Master and Data Encryption Keys
- Master Encryption Keys: Protection Modes
- Wrapping Keys, Rotating Keys
- Importing and Exporting Keys
- Cryptographic and Management Endpoints
- Crypto Operations

Module 2: OCI Vault Integration

- OCI Services Integration with Vault
- Encryption Using Oracle-Managed Keys
- Encryption Using Customer-Managed Keys
- OCI Object Storage Integration with Vault
- Back up and Replicate Vaults and Keys
- Backup
- Restore
- Cross-Region Replication

Module 3: Secrets Management

- Introduction to Secrets
- What is a Secret?
- Secret Rules

Module 4: Data Safe

- Overview of Data Safe
- Architecture Options
- Registering Oracle Databases with Data Safe
- Private vs Public Endpoints
- Data Safe Capabilities
- Security Assessment
- User Assessment
- Data Discovery

- Data Masking
- Activity Auditing

Module 5: OCI Storage Security

- Object Storage Security
- Public Buckets, Pre-Authenticated Requests (PAR)
- Sample Policies
- Data Durability and Encryption
- Data Integrity
- Managing Access and Authentication
- Object Lifecycle Management
- Object Storage Replication and Cross-Region Copy
- Limitations, Versioning, Integration with Features
- Data Retention
- Object Storage Data Retention and Integration
- Logging
- File Storage Security
- In-Transit Encryption
- Four Layers of Security
- Block Storage
- Local NVMe SSD Devices
- Block and Boot Volume Online Resize
- Backup and Restore, Clone, Volume Groups

Module 6: Oracle Database Security

- Data Vulnerabilities and Database Security in OCI
- Controlled Access and Safeguarding Databases
- Data Encryption and Database Patching
- Security Assessment

Module 7: Application Security

- Securing Applications in the Cloud
- Multiple Layers of Defense
- Web Application Firewall (WAF)
- OCI WAF Architecture, PoPs, Use Cases
- OWASP Rules, Service Components
- Origin Management, Protection Rules, Access Control
- Bot Management, Caching Rules, Threat Intelligence
- Shared Responsibility Model and Benefits
- IAM Policies, Getting Started Workflow and Demo
- API Gateway Security
- Network Security Groups (NSG), Security Lists
- mTLS Support and Custom Trust Stores
- Certificates Management

- Certificate Authorities, Root Certificates, Self-Signed Certificates
- TLS Connections, Mutual TLS
- Certificate Profiles, Rules, Integrations
- Use Cases: Public, Private, Code Signing

Module 8: Cloud Security Posture Management (CSPM)

- Overview of CSPM
- Problem with Cloud Security
- Capabilities, DevSecOps, Outcomes, Benefits
- Enable Cloud Guard

Typical Roles, Concepts: Targets, Detectors, Detector Rules & Recipes, Problems & Responders

- Scenarios and Demo: Public Bucket
- Managing Detector Recipes, Responder Recipes, Managed Lists, Notifications
- Security Zones and Security Advisor

Module 9: Security Operations

- Managing Security Operations
- Priorities in Security
- Observability and Management
- Key Services Overview
- Monitoring: Metrics, Alarms

Logging Service: Log Groups, Types of Logs, Searching Logs, Viewing Audit Events

Ingesting Logs from Sources: Compute, Object Storage, Cloud Services, On-Demand Upload

- Management Agent Installation and Workflow
- Service Connector for Ingestion
- Logging Analytics Overview
- Dashboards and Advanced Analysis (Log Clustering)
- OCI Audit Service: Viewing Audit Logs
- Events Service

Module 10: Regulatory Compliance

- Importance of Compliance
- Standards, Policies, Procedures
- Regulations and Standards
- Cloud Paradigm and 360-Degree Compliance Strategy in OCI
- Basic Security Considerations
- Security Best Practices for a Tenant
- Compliance Documents
- Penetration and Vulnerability Testing
- Permitted Testing and Rules of Engagement