INFOSECTRAIN

CLOUD SECURITY
PRACTITIONER TRAINING COURSE

INFOSECTRAIN

Why Cloud Security Practitioner Training Program with InfoSecTrain?

InfosecTrain is a proficient technology and security training and consulting organization across the globe, specializing in various IT security courses and services. You can leverage the following benefits with InfosecTrain:

- We provide hands-on experience with our lab sessions.
- We can help you present your qualifications and work experience for the designated profile.
- We offer a flexible training schedule.
- We provide recorded videos after the session to each participant.
- We provide post-training assistance.
- We also deliver a certificate of participation to each candidate.

Target Audience

- Any IT professional who wants to start exploring what's cloud? And how to securely configure it?
- Security professionals wanting to explore the security features of cloud
- IT professionals intending to excel in their career opportunities with cloud security skills.

Pre-Requisites

- Knowledge of IT infrastructure (Network, Endpoint, Appliances, etc.)
- Understanding of Basic Security
- Basic knowledge of why Risk, Compliance, and Governance are needed?
- Basic Understanding BCP/DR

CAREER BENEFITS OF
CLOUD SECURITY PRACTITIONER

$148,000

$131,409

$100,687

Cloud Administrators

Cloud Engineers

Cloud Analysts
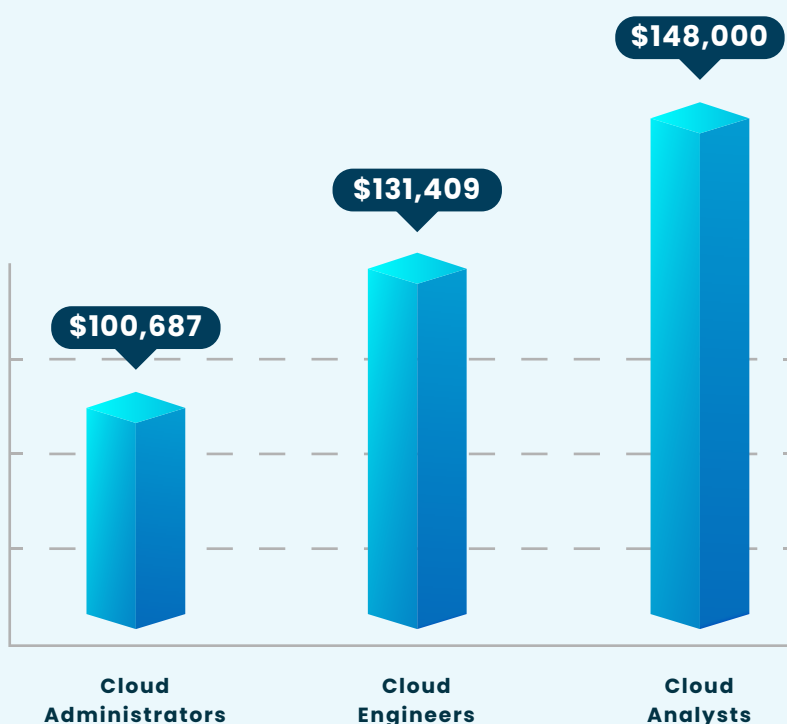
HIRING COMPANIES

ORACLE

IBM

Shell

accenture

amdocs

"Source: Glassdoor"

Course Objectives

- Evaluating cloud storage methods

- Developing and implementing a GRC framework

- Implementing and maintaining cloud security on different cloud platforms

- Exploring various cloud security concepts and components in-depth

- Understanding cloud security threats, Incident Response, risk management in the cloud, application security and secure deployment

- Learning cloud security audit management and its various components

- Comprehending cloud computing architectural framework

- Apprehending information management and data security

- Understanding governance and enterprise risk management

Course Content

Module1: Cloud Basics and Models

> Evolution of infrastructure technology

> Dedicated Server vs Virtual private server vs Shared hosting

> What is Virtualization?

> Type 1 and Type 2 Hypervisor

> What is Cloud?

> Different Vendors and Work

> Benefits of cloud

> Type of Cloud

> Shared model of cloud

> Service provided by cloud

> Challenges in cloud

Module2: Deploy and Understand Compute and Configuration

> Secure Instance/Virtual Machine Deployment

> Host Configuration Management

> Image Management

> Cloud Storage: Disk for Compute

> **Hands-On:** Deploy a Virtual Machine.

> **Hands-On:** Discuss disk option, image option

> **Hands-On:** What are scaling Options

> Application Security

> Threat Modelling

> Microsoft's Threat Modelling - Threat and Mitigation (Using STRIDE model)

> AWS Threat Modelling Suggestion

> Platform as a Service (PaaS) and Software as a Service (SaaS) Challenges

Module3: Deploy and Monitor Network Resources

> Private Cloud Networking

> Public Cloud Networking

> Network Segmentation

> **Hands-On:** Deploy Virtual Network

> Segment the Virtual Network

> Network Protection Services

> **Hands-On:** Allow Administrative Access

> **Hands-On:** Jump Server and Bastion Host

> **Hands-On:** VPN

> Cloud Logging Services

> Log Collection and Analysis

> Network Visibility

> **Hands-On:** Troubleshoot the virtual Network

> **Hands-On:** Enable the logging option

> Infrastructure as Code

> **Hands-On:** Deploy Network and VM using JSON

> Overview of Best practice for Network Security

Module4: Encrypt and Protect Data

> Storage Account

> Availability of Data

> **Hands-On:** Deploy storage account with availability option

> **Hands-On:** Encryption option

> **Hands-On:** Encryption option for disk storage

> Data Identification and Classification

> Data at Rest Encryption

> Data in Transit Encryption

> **Hands-On:** Deploy SQL Server

> **Hands-On:** Data classification and Identification

> **Hands-On:** Data Masking

> **Hands-On:** Data Encryption option

> Data Asset Management

> Lifecycle Management

> Cloud Access Security Brokers (CASB

Module5: Quick view of Containers

> What is Container as a Service
> **Hands-On:** Deploy Container
> Secure Container Image
> Control Container with the K8
> Security best practices for Container and Kubernetes

Module6: Control Your Identity and Access Management

> Lifecycle for Identity and Access Management
> Cloud Accounts
> Policies and Permissions
> Groups and Roles
> Temporary Credentials
> **Hands-On:** Create a cloud-based identity
> **Hands-On:** Apply roles to the account
> **Hands-On:** Create group
> **Hands-On:** Assign role
> Secrets Management
> Customer Account Management and External Access
> **Hands-On:** Enable MFA
> **Hands-On:** Different Security options and Service
> More IAM Best Practices
> **Hands-On:** Identity Audit with Identity governance feature in Azure

Module7: Detecting and Handling Cloud Incidents with Security Operation

> Handling Cloud Incidents
> Understand Cloud Incident Response
> Understand Cloud Incident Response Lifecycle
> Understand How SOAR Accelerates Incident Response
> **Hands-On:** Creating alerts using azure monitor service
> Security As a Service
> Cloud-Based SIEM Models
> 365 Defender
> AWS Guard Duty
> Microsoft Sentinel

Module8: Manage Business Continuity and Disaster Recovery

> Understanding Cloud Disaster Recovery and Business Continuity

> Designing Disaster Recovery and Business Continuity in Cloud

> **Hands-On:** Implementing Backup for VM

> **Hands-On:** Implementing DR for the storage account

> [MTTR, RPO, RTO]

Module9: Handling Legal Issues and Policy in Cloud

> Understand the laws impacting cloud computing

> Learn the cloud computing standards

> Describe the legal frameworks for data protection and privacy

> Learn audit planning and reporting in the cloud

> Describe outsourcing and vendor management

> **Hands-On:** Auditing Compliance of Azure Resources by creating Policy

> Assignments with Azure Policy

> Conducting Security Audit in AWS with AWS Trusted Advisor

Module10: Manage GRC for the cloud

> Understand GRC in the cloud

> Discuss cloud governance

> Understanding implement and maintain governance for cloud computing

> Discuss risk management in the cloud

> Understand risk management framework and process in the cloud

> Understand cloud compliance

> Learn to implement GRC in the cloud

> **Hands-On:** Deploying Policy for the restriction of deployment

> **Hands-On:** Enforce Compliance by Assigning In-built Policy and Creating Custom Policy in Azure

INFOSECTRAIN