insureTech Skills

CERTIFIED

Multi-Cloud Security AWS, Azure And Google

Launch Your Career in Multi-Cloud Security

Cloud Security (AWS, Azure And Google) Training

Multi-Cloud Security **(AWS, Azure & Google)** Training program is designed to teach you how to protect cloud systems and data from cyber threats. As cloud technology grows, companies need experts to secure their networks and data in the cloud.

This program covers **AWS, Azure & Google** the three most popular cloud platforms. You will learn to protect cloud environments and prevent attacks, ensuring your data stays safe. A Security Engineer develops, implements, and monitors their organizations security infrastructure to protect sensitive information.

Join the **Multi-Cloud Security (AWS, Azure & Google)** program and become an expert in securing cloud systems. Learn how to prevent data breaches, protect sensitive information, and secure cloud networks. Equip yourself with valuable skills and certifications that will open doors to exciting career opportunities in the world of cloud security.

Key **Feature** to Determine **Success**

- 30 Hours of Live Online Sessions
- Learn from Industry Experts
- Real-time Industry Cases Study
- Access to Recorded Sessions
- Hands-On Logging, Monitoring, Responding
- Extended Post Training Support
- Personalized Doubt Sessions
- Career Guidance and Mentorship
- Expert Career Services to Help You Land a Job

Program Review

Program Overview

Step into the future of cybersecurity with our Multi-Cloud Security Training Program, a power-packed hands-on learning journey designed for the modern cloud era. As organizations shift to AWS, Azure, and Google Cloud to accelerate innovation, the demand for skilled professionals who can secure multi-cloud environments has never been higher.

Transform your profile with the advanced multi-cloud security skills today's companies are actively seeking - combining real-world labs, advanced security concepts, practical tools, and industry best practices. From cloud identity and access control to threat detection, data protection, governance, and compliance, you'll learn how to build and defend secure cloud infrastructures across all three major platforms.

Designed for both beginners and working professionals, this training transforms you into a job-ready Cloud Security Specialist, capable of protecting enterprise-grade cloud workloads and mitigating emerging cyber threats. Whether you want to boost your career, switch to cloud security, or gain hands-on multi-cloud expertise, this program unlocks unlimited opportunities in one of the fastest-growing fields in tech.

Benefits of Having **Multi-Cloud Security Certification**

Career Benefits

- The demand for cloud security professionals is growing steadily at a rate of 115% from 2020 to 2025.
- As organizations increasingly migrate their operations to the cloud, the demand for experts who can secure these complex, distributed environments continues to soar.
- Increase Your Earning Potential
- $150,000+ Salary of Cloud Security Engineers
- 70% Increase Security roles and jobs

Professional Benefits

- Earn the status of a Cloud Security expert
- Enhance Job Security and Career Opportunities
- Stay Ahead of the Competition with Latest Skills
- Build your Credibility with Specialized Knowledge
- Security roles and jobs
- Cloud Computing Specialist
- Clout Support Engineer
- Cloud Security Architect:
- Secuirty Consultant
- Cloud Security Engineer

Achieving **AWS, Azure** and **Google** certifications positions you as a sought-after cloud expert, ready to defend and secure organizations' cloud environments.

Multi-Cloud Security (AWS, Azure And Google) Training Curriculum

Module 1: Introduction to Cloud Security

- Overview of Cloud Computing
- Key concepts in cloud security
- Difference between AWS and Azure security models

Module 2: Cloud Service

- Models and Risks
- Understanding IaaS, PaaS, and SaaS
- Risks associated with each model
- Security challenges in the cloud

Module 3: Identity and Access Management (IAM)

- Managing user access in AWS & Azure
- Implementing roles and permissions
- Multi-factor authentication (MFA) in cloud platforms

Module 4: Securing Cloud Networks

- Cloud network security basics
- Setting up VPC in AWS and Virtual
- Networks in Azure
- Firewalls, VPNs, and network segmentation

Module 5: Cloud Threats and Vulnerabilities

- Common cloud security threats
- Identifying vulnerabilities in cloud environments
- Cloud-specific attack methods

Multi-Cloud Security (AWS, Azure And Google) Training Curriculum

Module 6: Cloud Security Monitoring and Logging

- Monitoring cloud resources in AWS & Azure
- Using CloudWatch (AWS) and Azure
- Monitor for logging
- Identifying and responding to security incidents

Module 7: Cloud Compliance & Regulatory Standards

- Overview of key regulations (GDPR, HIPAA, etc.)
- Ensuring compliance in cloud environments
- Implementing security controls for regulatory requirements

Module 8: Securing Cloud Applications

- Best practices for securing cloud-based applications
- Web application firewalls (WAF) in AWS & Azure
- Penetration testing for cloud apps

Module 9: Incident Response & Disaster Recovery in the Cloud

- Creating an incident response plan for the cloud
- Managing cloud-based disaster recovery
- High availability and fault tolerance

Module 10: Cloud Security Automation and AI

- Automating cloud security tasks
- Using AI and machine learning to detect threats
- Best practices for cloud security automation
- Automation and AI

Module 11: Hands-On Labs

- Real-world simulations for cloud
- security Working with AWS and Azure security tools
- Practical exercises in securing cloud environments

Multi-Cloud Security (AWS, Azure And Google) Training Curriculum

Module 12: Google Cloud Fundamentals: Core Infrastructure

- Introducing Google Cloud
- Resources and Access in the Cloud
- Virtual Machines and Networks in the Cloud
- Storage in the Cloud
- Containers in the Cloud
- Applications in the Cloud
- Prompt Engineering

Module 13: Networking in Google Cloud: Fundamentals

- Welcome to Networking in Google Cloud
- VPC Networking Fundamentals
- Sharing VPC Networks
- Network Monitoring and Logging

Module 14: Networking in Google Cloud: Routing and Addressing

- Welcome to Networking in Google Cloud
- Network Routing and Addressing in Google Cloud
- Private Connection Options

Module 15: Managing Security in Google Cloud

- Foundations of Google Cloud Security
- Securing Access to Google Cloud
- Identity and Access Management (IAM)
- Configuring Virtual Private Cloud for Isolation and Security

Multi-Cloud Security (AWS, Azure And Google) Training Curriculum

Module 16: Security Best Practices in Google Cloud

- Welcome to Security Best Practices in Google Cloud
- Securing Compute Engine: Techniques and Best Practices
- Securing Cloud Data: Techniques and Best Practices
- Application Security: Techniques and Best Practices
- Securing Google Kubernetes Engine: Techniques and Best Practices

Module 17: Mitigating Security Vulnerabilities on Google Cloud

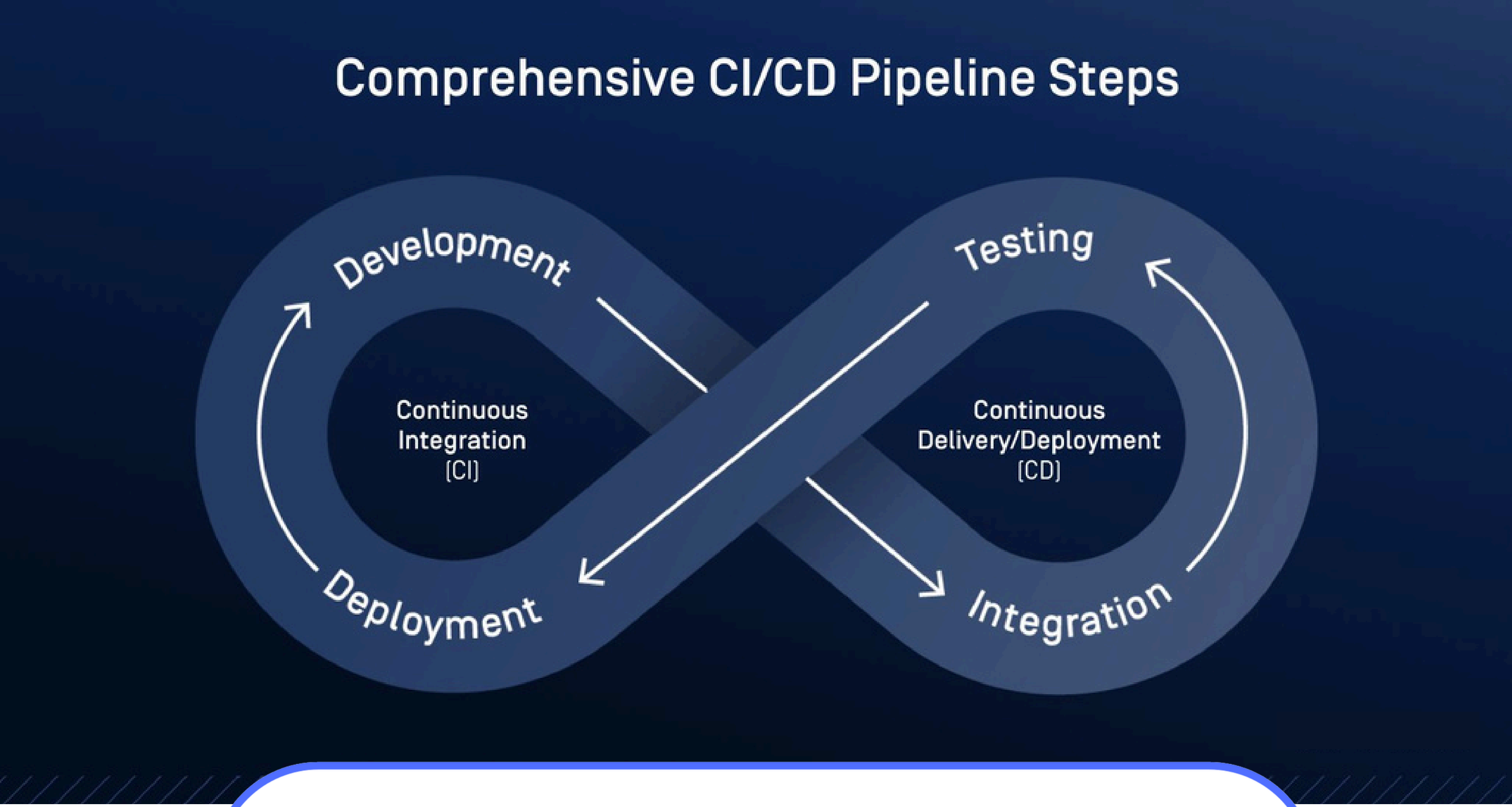
- Protecting against Distributed Denial of Service Attacks (DDoS)
- Content-Related Vulnerabilities: Techniques and Best Practices
- Monitoring, Logging, Auditing and Scanning

Module 18: Logging and Monitoring in Google Cloud

- Introduction to Google Cloud Operations Suite
- Monitoring Critical Systems
- Alerting Policies
- Advanced Logging and Analysis
- Working with Audit Logs

Module 19: Observability in Google Cloud

- Configuring Google Cloud Services for Observability
- Monitoring Google Cloud Network
- Investigating Application Performance Issues
- Optimizing the Costs for Google Cloud Observability


Comprehensive CI/CD Pipeline Steps
Development
Testing
Continuous Integration (CI)
Continuous Delivery/Deployment (CD)
Deployment
Integration

CI/CD Pipeline Security & DevSecOps Integration

As organizations adopt Continuous Integration (CI) and Continuous Delivery (CD) for faster development and deployment, security must be embedded into every stage of the software delivery lifecycle.

This section focuses on securing CI/CD pipelines across AWS, Azure, and Google Cloud, ensuring that code, dependencies, and deployment environments are safe from vulnerabilities and threats.

Module 20: Introduction to DevSecOps and Pipeline Security

- Understanding the DevSecOps Culture and Principles
- The Need for Security in CI/CD Pipelines
- Shared Responsibility in DevOps Security
- Identifying Security Risks in Build, Test, and Deploy Phases

Module 21: Secure CI/CD Design

- Designing Secure Pipelines for AWS CodePipeline, Azure DevOps, and Google Cloud Build
- Managing Secrets Securely using:
  - AWS Secrets Manager
  - Azure Key Vault
  - Google Secret Manager
- Using Environment Isolation and Least Privilege in Build Agents
- Artifact Integrity Validation and Secure Storage

Module 22: Code and Dependency Security

- Implementing Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Container Image Scanning (Trivy, Aqua, Clair)
- Dependency and Package Vulnerability Scanning (OWASP Dependency-Check, Snyk)
- Automating Security Checks in Pipelines

Module 23: Security Automation in Pipelines

- Integrating SonarQube and OWASP ZAP for Automated Security Scans
- Automating Compliance Checks with Terraform and Policy as Code
- Using Git Hooks and Pre-Commit Scanners
- Integrating Security Alerts with Slack, Teams, or Email
- Implementing Automated Rollbacks on Security Failure

Module 24: Continuous Monitoring and Incident Response

- Monitoring Build Activities and Pipeline Logs
- Setting up Alerts for Unauthorized Pipeline Modifications
- Using Cloud SIEM Tools (AWS Security Hub, Azure Sentinel, Chronicle SIEM)
- Incident Handling and Recovery in DevOps Pipelines
- Post-Deployment Verification and Threat Hunting

Module 25: Hands-On Labs (CI/CD Security)

- Building a Secure CI/CD Pipeline with Jenkins and GitHub
- Integrating SonarQube for Static Code Analysis
- Scanning Docker Images Before Deployment
- Secrets Management in Azure DevOps Pipeline
- Automating Security Tests with OWASP ZAP in a Multi-Cloud Setup
- Real-Time Monitoring of Cloud Deployments for Threat Detection

What Will You **Learn?**

Multi-Cloud Security Fundamentals

- Understand core security principles in multi-cloud environments.
- Understand core security principles in multi-cloud environments.

Identity & Access Management (IAM)

- Manage user roles and permissions across AWS, Azure & GCP.
- Manage user roles and permissions across AWS, Azure & GCP.

.

Data Protection & Encryption

- Apply encryption for data at rest and in transit.
- Apply encryption for data at rest and in transit.
- Use cloud-native tools to safeguard sensitive information.

Cloud-Native Security Tools

- Work with Google SCC, Azure Defender, and AWS Security Hub.
- Strengthen cloud environments using native security tools.

Monitoring & Incident Response

- Use monitoring and logging tools to detect threats.
- Apply incident-response methods to resolve cloud issues.

Secure Multi-Cloud Architecture

- Design secure and scalable multi-cloud architectures.
- Follow best practices for compliant cloud deployments.

Compliance & Standards

- Align with NIST, GDPR, ISO 27001, CIS.
- Ensure regulatory compliance across clouds.

Vulnerability Assessment & Remediation

- Conduct security assessments across multiple clouds.
- Apply remediation techniques to strengthen cloud security posture.

Who Can Join This **Course?**

The following types of candidates can join this course :–

- Cloud Engineers
- IT Security Professionals
- Cloud Architects
- Cybersecurity Analysts
- Professionals preparing for cloud security certifications (AWS. Security Specialty, Microsoft Azure AZ-500, Google Professional Cloud Security Engineer)

Pre-**requisites**

Participants should be familiar with:-

- Basics of cloud computing and IT security.
- Fundamental concepts of cloud deployment models (IaaS, PaaS, SaaS).
- At least one cloud platform such as AWS, Azure, or GCP.
- Basic networking concepts including IP addresses, firewalls, and VPNs.

Our Distinctness:-

- Open to any candidate who has the understanding and eagerness to learn Multi-Cloud Security.
- Training focuses not only on certification but real excellence in planning, designing, and scaling cloud implementations across 70+ cloud services.

Ask your queries to our experts?

☎ *+91 7902091373*
+91 7060219796

www.insuretechskills.tech

@ *support@insuretechskills.tech*

insuretech_skills

@insuretech_skills1

insureTech Skills