BLACKBIRD FOR TRAINING

Cloud DevSecOps and CI/CD Pipeline Security

28 December 2026 – 1 January 2027
Kuala Lumpur (Malaysia)



Cloud DevSecOps and CI/CD Pipeline Security

Ref: 3255281_201766 **Date:** 28 December 2026 – 1 January 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

In today's cloud-driven digital era, cybersecurity is no longer an isolated function — it's an integral part of the entire software development lifecycle. As organizations increasingly adopt cloud platforms and automated deployment models, integrating security within every development and operational stage has become critical.

This course provides a comprehensive understanding of how to embed security practices within cloud-based development and operational workflows. Participants will learn how to secure continuous integration and continuous delivery CI/CD pipelines against threats, ensure compliance, and maintain resilient and trustworthy systems.

Through practical sessions and case studies, learners will gain the knowledge and tools needed to design secure architectures, automate security checks, and lead teams toward a proactive security culture.

Course Objectives

- Understand the fundamental concepts of Cloud DevSecOps and its importance in modern environments.
- Identify the components and security risks within CI/CD pipelines.
- Apply best practices for integrating security into every phase of the development lifecycle.
- Implement automated security testing and compliance monitoring.
- Analyze vulnerabilities within cloud infrastructures and deployment systems.
- Build secure configurations and manage credentials safely.
- Design effective incident response and recovery strategies.
- Foster collaboration between development, security, and operations teams to achieve unified goals.

Course Outlines

Day 1: Foundations of Cloud Security and DevSecOps

- Overview of cloud security concepts and shared responsibility models.
- Introduction to DevSecOps principles and benefits.
- Comparing traditional security vs. integrated DevSecOps approaches.
- Common threats in cloud and hybrid environments.
- Secure coding fundamentals within cloud applications.
- Case studies of organizations implementing DevSecOps successfully.



Day 2: Architecture of CI/CD Pipelines

- Understanding CI/CD pipeline structures and workflows.
- Identifying critical security checkpoints across build and deployment stages.
- Integrating code review and static analysis tools.
- Managing secrets and credentials across environments.
- Implementing secure configuration management.
- Strategies for vulnerability assessment and risk mitigation.

Day 3: Automation and Security Tools

- Role of automation in improving security efficiency.
- Setting up automated scanning and compliance verification.
- Integrating container security within DevSecOps pipelines.
- Using monitoring and alerting tools for continuous visibility.
- Implementing role-based access control and identity management.
- Hands-on application of automated defense mechanisms.

Day 4: Securing Cloud Infrastructure and Applications

- Advanced strategies to protect cloud-native architectures.
- Securing APIs, databases, and microservices in the cloud.
- Network segmentation and environment isolation techniques.
- Hardening containers and virtual machines.
- Detecting and responding to misconfigurations.
- Aligning practices with global cloud security standards.

Day 5: Security Testing and Incident Response

- Conducting penetration tests within CI/CD environments.
- Validating compliance with organizational and regulatory policies.
- Interpreting and acting upon vulnerability reports.
- Building a structured incident response plan.
- Post-incident analysis and continuous improvement.
- Final workshop: connecting theoretical concepts to real-world execution.



Why Attend this Course: Wins & Losses!

- Gain a holistic understanding of cloud-based DevSecOps practices.
- Learn how to protect CI/CD pipelines from modern cyber threats.
- Enhance decision-making and leadership capabilities in secure development.
- Improve efficiency through security automation and continuous compliance.
- Strengthen collaboration between technical and security teams.
- Minimize risks and operational downtime through proactive defense.
- Align security objectives with business goals and innovation strategies.
- Advance your professional credibility in cybersecurity and cloud management.

Conclusion

Embedding security into every stage of the cloud development lifecycle is not just a best practice — it's a necessity for organizational resilience. This course equips participants with the technical and strategic knowledge to safeguard CI/CD pipelines, secure cloud environments, and implement continuous security at scale.

By mastering these principles, professionals can lead their teams toward a culture of security-driven innovation, ensuring that cloud transformations remain both agile and safe.

