# DevSecOps Foundation Certification

## About DevOpsSchool

DevOpsSchool is a unit of "Cotocus PVT ltd" and a leading platform which helps IT organizations and professionals to learn all the emerging technologies and trend which helps them to learn and embrace all the skills, intelligence, innovation and transformation which requires to achieve the end result, quickly and efficiently. We provide over 40 specialized programs on DevOps, Cloud, Containers, Security, AI, ML and on Big data that are focused on industry requirement and each curriculum is developed and delivered by leading experts in each domain and aligned with the industry standards.

## About Course

DevSecOps Foundation Certification is a specialized credential designed for professionals seeking to enhance their understanding of DevSecOps, a critical aspect of modern software development and IT security practices. DevSecOps stands for Development, Security, and Operations, and it integrates security practices within the DevOps pipeline. The goal of DevSecOps is to ensure that security is a part of the development process from the very beginning, rather than being an afterthought. The certification focuses on embedding security practices into the entire software development lifecycle (SDLC), promoting collaboration between development, operations, and security teams.

The DevSecOps Foundation Certification equips IT professionals with the foundational knowledge and skills necessary to implement security best practices within DevOps processes. This certification provides an understanding of key concepts such as continuous integration and continuous delivery (CI/CD), automated security testing, vulnerability scanning, and monitoring in the DevOps environment. By achieving this certification, professionals demonstrate their ability to bridge the gap between development, security, and operations to create secure and reliable applicationss.

Co-coordinator – Akanksha Kumari

Call/WhatsApp: - +1 (469) 756-6329

Mail Address: -
contact@DevOpsSchool.com


Secondary contact – Patrick

Call/WhatsApp: - +91 7004 215 841

Mail Address: -contact@DevOpsSchool.com

| Duration | 5 days |
|---|---|
| Mode | Online (Instructor-led, live & Interactive) |
| Projects (Real time scenario based) | 1 |

| FEATURES | DEVOPSSCHOOL | OTHERS |
|---|:---:|:---:|
| Faculty Profile Check | ✔ | ✘ |
| Lifetime Technical Support | ✔ | ✘ |
| Lifetime LMS access | ✔ | ✘ |
| Top 25 Tools | ✔ | ✘ |
| Interviews Kit | ✔ | ✘ |
| Training Notes | ✔ | ✘ |
| Step by Step Web Based Tutorials | ✔ | ✘ |
| Training Slides | ✔ | ✘ |
| Training + Additional Videos | ✔ | ✘ |

## Training

DevOps As part of this course, you would be strong in DevOps technology. You would learn Linux, Python, DevOps, Docker, Jira, Git, SonarQube, Maven, Ansible, Jenkins, Kubernetes, Datadog, Splunk, NewRelic, Terraform and various other stacks related to this methodology.

## Projects

As part of this initiative, trainer would help you to execute one real time scenario based project, doing it end to end and step by step to visualize a real agile work environment in any organization.

## Interview

As part of this, you would give complete DevSecOps Foundation Certification interview preparations Kit. This interview kit will help you organize your application and interview with eas

# AGENDA : DEVSECOPS FOUNDATION CERTIFICATION

## Day 1 - Introduction to DevSecOps and Security in the DevOps Lifecycle

### Introduction to DevSecOps

- What is DevSecOps and why is it important?
- The evolution of DevSecOps: Integrating security into DevOps
- The role of DevSecOps in modern IT and cloud environments

### DevSecOps Lifecycle

- Overview of the DevSecOps lifecycle: Plan, Code, Build, Test, Release, Deploy, Operate, Monitor
- Key differences between traditional security models and DevSecOps
- Benefits of integrating security into DevOps practices.

### Security in the DevOps Pipeline

- The need for security automation in CI/CD pipelines
- Key concepts in security integration for DevOps: Shift-left security, Continuous security, and Immutable infrastructure
- Security best practices for DevOps teams.

### Hands-On Activity

- Set up a basic CI/CD pipeline with integrated security checks using a DevSecOps tool (e.g., Snyk, SonarQube).

# Day 2 - Secure Development Practices and Tools

## Secure Coding Practices

- The importance of secure coding in the DevSecOps process

- Common coding vulnerabilities and how to prevent them (SQL injection, XSS, etc.)

- Secure coding frameworks and tools (OWASP Top 10, Secure Coding Guidelines).

## Static and Dynamic Analysis

- Introduction to Static Application Security Testing (SAST)

- Introduction to Dynamic Application Security Testing (DAST)

- Tools for static and dynamic analysis (e.g., Fortify, Checkmarx, OWASP ZAP).

## Infrastructure as Code (IaC) Security

- Importance of securing infrastructure as code

- Common IaC vulnerabilities and how to mitigate them

- Tools for IaC security (e.g., Terraform, AWS CloudFormation, Checkov).

## Hands-On Activity

- Implement static analysis in the CI/CD pipeline using a tool like SonarQube.

# Day- 3  Automation, Containerization, and Cloud Security

## Security Automation

- The role of security automation in DevSecOps

- Automating security testing in the CI/CD pipeline

- Automating compliance checks and vulnerability scanning.

## Containerization and Security

- Understanding containerization and its security implications

- Securing Docker images and Kubernetes environments

- Tools for container security (e.g., Aqua Security, Twistlock, Clair).

## Cloud Security and Compliance

- Key security challenges in cloud environments (AWS, Azure, Google Cloud)

- Best practices for securing cloud infrastructure

- Cloud security tools and frameworks (e.g., AWS Inspector, Azure Security Center).

## Hands-On Activity

- Implement vulnerability scanning for Docker images in a CI/CD pipeline.

# Day – 4 Incident Management, Monitoring, and Continuous Compliance

## Incident Management in DevSecOps

- Best practices for incident detection and response in DevSecOps

- Automating incident response workflows

- Integrating security monitoring with DevOps tools.


## Continuous Monitoring and Logging

- The role of monitoring in DevSecOps

- Best practices for logging and monitoring security events

- Tools for continuous security monitoring (e.g., Splunk, ELK Stack, Prometheus).

## Continuous Compliance

- The importance of continuous compliance in DevSecOps

- Tools for continuous compliance automation (e.g., Chef InSpec, OpenSCAP)

- Integrating security into audit and compliance processes.

## Hands-On Activity

- Set up continuous monitoring and logging using open-source tools (e.g., ELK Stack or Prometheus)

# Days – 5  Advanced DevSecOps Topics and Certification Exam Preparation

## DevSecOps for Advanced Threats

- Protecting against advanced persistent threats (APTs) in DevSecOps

- Securing the software supply chain

- Threat modeling and risk assessment in DevSecOps.

## Building a DevSecOps Culture

- The importance of collaboration between development, security, and operations teams

- Fostering a security-first mindset across teams

- Training and awareness for continuous improvement.

## Certification Exam Preparation

- Key concepts and topics to focus on for the DevSecOps Foundation Certification exam

- Review of practice questions and exam structure

- Tips for exam success.

## Final Hands-On Activity

- End-to-end DevSecOps pipeline implementation, integrating secure coding practices, vulnerability scanning, and incident response.

# Thank you!

Connect with us for more info

Call/WhatsApp: - +91 968 682 9970

Mail: - contact@DevOpsSchool.com

www.DevOpsSchool.com