



Certified DevOps Security Practitioner
By Network Intelligence

Certified DevOps Security Practitioner (CDSP)

Empower DevOps Velocity, Fortify Security Strength

Batch 1: Asia & Middle East

Date: 20 -22, May 2024

Timing: 6:00 am – 10:00 am GMT

Mode of training: Online

Batch 2: Americas & Europe

Date: 27- 29, May 2024

Timing: 1:00 pm – 5:00 pm GMT

Mode of training: Online

Course Fee:

USD 249 for regular Attendee

USD 219 for ISACA/ISC2 Members



Certified DevOps Security Practitioner
By Network Intelligence

Introduction

DevOps Security" typically encompasses an overview of the integration of security practices within DevOps methodologies. It involves understanding how to seamlessly embed security into the DevOps pipeline, ensuring that security is not an afterthought but an integral part of the development process. This introductory session would likely cover fundamental concepts such as threat modeling, secure coding practices, vulnerability management, compliance automation, and the use of security tools and technologies in a DevOps environment.

Why DevOps is important?

DevOps Security is vital because it integrates security practices into the development process, ensuring that software is built with security in mind from the start. This approach helps mitigate risks, ensures compliance, and enables faster response to security incidents, ultimately saving time and costs while enhancing overall security posture.



Certified Devops Security Practitioner
By Network Intelligence

Objectives

- **Increased Collaboration:** Enhancing communication and collaboration between development, operations, and other stakeholders to streamline processes and achieve common goals.
- **Faster Delivery:** Accelerating the delivery of software and updates through automation, continuous integration, and continuous deployment practices.
- **Improved Quality:** Enhancing the quality of software by implementing automated testing, code reviews, and monitoring throughout the development lifecycle.
- **Increased Efficiency:** Optimizing workflows, reducing manual tasks, and eliminating bottlenecks to improve the efficiency of development and operations teams.
- **Enhanced Reliability:** Building more reliable and resilient systems by implementing practices such as infrastructure as code, automated provisioning, and monitoring.



Course Content

Day 1:

- Intro DevOps Culture
- DevOps Principles
- Overview of DevOps Tools
- DevOps CI/CD Pipelining
- Security & Compliance Challenges in DevOps
- Regulation
- Security Compliance
- Cloud Service threats
- Rapid releases
- New Technology (Microservices)
- Security challenges in CI/CD
- Case Study
- Injecting Security into CI/CD

- Hands-on Open-Source Tools
- (npm,owasp dependency checker,retire.js) any one
- Static Analysis
- Dynamic Analysis
- Hands-on Open-Source Tools (zap)
- Security Testing
- Git Attack & Best Practice
- Jenkins Attack & Best Practice
- Case Study
- Shift Secure Left
- OWASP Proactive Controls
- Using Infrastructure as Code
- The 'HoneyMoon' Effect
- SDOMM or DSOMM(Maturity Model)

In line with these objectives, we announce a 3-day 12-hour online training on “Certified DevOps Security Practitioner (CDSP)”.



Course Content

Day 2:

- Microservice Security
- What is Docker?
- Overview of Docker Components
- Security Concerns with Containers
- Attacking Docker Containers Misconfiguration(Hands-on)
- Auditing Docker Containers(Hands-on)
- Kubernetes Attacking and Defending

Day 3:

- Security Automation
- Case Study
- Security Policy
- Framework(BDD, Robot)
- Introduction to ansible(Iaac)
- Ansible overview
- Hands-on Security Automation
- Security Automation Compliance
- Hands-on Inspec
- Intro to Cloud –DevSecOps (AWS, Azure)
- Serverless Security

In line with these objectives, we announce a 3-day 4-hours each, online training on “Certified DevOps Security Practitioner (CDSP)”.



Certified Devops Security Practitioner
By Network Intelligence

Trainer Details



Sanket Kamble,
Practice Lead – Assessment,
Network Intelligence

Sanket Kamble, a seasoned cybersecurity professional with over six years of experience, specializes in Vulnerability Assessment and Penetration Testing (VAPT), Configuration Review, Source Code Review, Cloud Security, DevSecOps, Technical Audit, and Compliance Standard-Specific VAPT. Certified as a Certified Ethical Hacker (CEH), eLearnSecurity Junior Penetration Tester (eJPT), and Certificate of Cloud Security Knowledge (CCSK), Sanket is dedicated to safeguarding organizations against cyber threats and ensuring security resilience.

Registration Link: <https://forms.office.com/r/US8cyPpRqm>