Certified DevOps Security Practitioner

NETWORK INTELLIGENCE
Global cybersecurity provider

A 12 Hours DevOps Security Training

Asia & Middle East

Dates : September 27 -29 , 2021

Time : 6 00 Am – 10 00 Am GMT

Mode : Online

Course Fees:

Non ISACA/ISC2 Members: USD $ 200 ISACA/ISC2 Member: USD $ 160

Objectives of the Course

This training focuses on Embedding security into the DevOps processes is referred to as DevSecOps. While DevOps addresses the business need of rapidly delivering products and release code in order to satisfy customer demands, it is important that security must work in tandem with Agile and DevOps processes.

In traditional development methods, security is kept at the very end of the release process.

Hence, security has been viewed as a bottleneck to the rapid development methodologies such as Agile along with the software delivery pipeline.

This results in a major contention and distrust between development and security teams unless they work in tandem.

Just as DevOps addresses the traditional silos between Development and Operations, DevSecOps seeks to address the silos between Dev, Ops and Security teams. Automated application security further facilitates reducing friction and removing bottlenecks in the CI/CD cycle.

In this course, we will be learning how DevSecOps is implemented in a company by using various programming languages and open source tools. It will be helpful to jumpstart in understanding and exposure to various security automation possibilities which can be integrated in DevOps related to application or infrastructure security.

Who should attend

- Entrepreneurs, Business Owners
- Cloud Solutions Providers, Senior Managers
- Security Automation Team
- DevSecOps & Devops Team
- Aws & Azure Professionals
- Developers
- Compliance team
- Risk Management Professionals
- Security Enthusiasts

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 Analaysis
        - Hands-on Open Source Tools
        (gitrob/trufflehog,open source static code scanner) any one
        - Dynamic Analysis
        - Hands-on Open Source Tools (zap
- Security Testing
    - Git Attack & Best Pratice
    - Jenkins Attack & Best Practice
- Case Study
- Shift Secure Left
- OWASP Proactive Controls
- Using Infrastructure as Code
- The ‘HoneyMoon’ Effect
- SDOMM or DSOMM(Maturity Model)

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

“Remember….. you are the Centre of Security”

COURSE CONTENT

Day 3:

- Security Automation
- CaseStudy
- 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

Examination – The participants would need to undergo an online examination after the training. On successfully clearing the examination, the participant would be awarded with the DevOPs Security certificate.

“Remember….. you are the Centre of Security”

Lead Trainer

Lionel Faleiro,
Practice Lead
Network Intelligence

Lionel is passionate about training and working in DFIR. He comes with an experience of almost 10 years in IT and Cybersecurity.
He began as a SysAdmin then a Security Trainer and now leads the Forensic Practice at the firm.
He has solved numerous cases during his tenure at Network Intelligence and is an avid gamer as well.

Registration link : https://forms.office.com/r/DBXnUL2DXk