

**Fundamentals of DevSecOps**

**Course Number:** DVOP-162  
**Duration:** 2 days

**Overview**

DevSecOps (Development, Security, and Operations) is an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire Software Development Life Cycle (SDLC). This DevSecOps Fundamentals training course teaches attendees how to prioritize security and compliance in their workflows.

**Prerequisites**

All participants must have attended [DevOps Fundamentals](file:////training/devops-fundamentals) or have comparable experience implementing basic DevOps principles.

**Materials**

All DevSecOps training attendees receive comprehensive courseware.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computers for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will work well.

**Objectives**

* Have a thorough understanding of DevSecOps
* Implement a process where products and services have safety and security incorporated into the architecture
* Architect DevSecOps strategies and automation

**Outline**

* Introduction
* DevSecOps Origin and Evolution
  + DevOps beginnings
  + DevSecOps values and manifestos
  + CALMS and SaC (security as code)
  + DevSecOps and the Three Ways
  + DevSecOps outcomes
* The Security- and Cyber-Threat Landscape
  + Cyber Thread Industrial Landscape
    - Threat definition
    - Source of threats
    - Outcomes and results
  + Threat (type) models
    - STRIDE
  + MITRE ATT and CK
  + Who/what do we protect from?
    - Published common flaws
    - OWASP top ten
    - EU agency cybersecurity rankings
    - Threat actors and agents
  + What do we protect?
    - protection metrics
    - continuous compliance
* Building a DevSecOps Model
  + Responsiveness
    - How, what, to/from whom?
  + KPI(s): Key Performance Indicators
    - Redesigning change management
  + DevSecOps maturity and implementation model
  + Resilience through responsiveness
    - Building a (compliant) model
    - Outcomes
* DevSecOps Safety Culture
  + DevSecOps "state of mind" and practices
  + The Trust Algorithm
  + Definition of a safety culture
  + Westrum and Laloux typologies
  + DevSecOps stakeholders
    - Types
    - Collaboration
  + Governance
* DevSecOps Best Practices
  + Current assessment
    - Continuous security map/definition
    - Security in the DevOps flow
    - Practices and (shift security left) outcomes
  + Security and the CI/CD pipeline
  + Cloud and container security
  + The target state
    - Artifact, risk, identity, access, and secrets management
  + Perils of a DevOps pipeline
  + Building a secure DevOps pipeline
    - SAST / DAST / IAST / RASP tools
    - Continuous compliance
    - SIEM (security information and event management)
* Learning DevSecOps
  + The Third Way (continuous experimentation and learning)
  + Security training (as policy)
  + DevSecOps Dojos
  + Security Chaos Engineering and gamification
  + Learning through experiences, innovation, retrospectives
  + Continuous learning forever
* Conclusion