DevSecOps Implementation and Agile Security Integration Training Course



14 - 18 Dec 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #CYB5409_272382

Course Introduction / Overview:

In today's fast-paced digital landscape, the integration of security into the development and operations lifecycle is no longer optional but a critical necessity. This course provides a comprehensive, A-to-Z exploration of DevSecOps, a cultural and technical shift that embeds security practices into the heart of the agile and DevOps frameworks. Moving beyond the traditional model where security is a final, often rushed, checkpoint, this program champions the "shift-left" philosophy, ensuring security is a shared responsibility from the very first line of code. As highlighted by security experts like Jim Manico, a proponent of secure coding practices, building secure software requires a proactive, not reactive, approach. This training course from BIG BEN Training Center is meticulously designed to equip participants with the skills to implement robust security automation, conduct continuous security testing, and foster a security-first mindset within their teams. We will delve into practical strategies for integrating security tools and processes into CI/CD pipelines, securing cloud-native applications, and managing vulnerabilities effectively, transforming your organization's approach to software development and delivery.

Target Audience / This training course is suitable for:

- DevOps Engineers.
- Security Professionals and Architects.
- Software Developers and Engineers.
- Quality Assurance and Testing Professionals.
- IT Managers and Team Leaders.
- System and Network Administrators.
- Release Managers and Engineers.
- Product Owners and Managers.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Technology and Software Development.
- E-commerce and Retail.
- Telecommunications.
- Government Agencies and Public Sector Organizations.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT).
- Information Security (InfoSec) or Cybersecurity.
- Software Development and Engineering.
- Quality Assurance (QA).
- Operations and Infrastructure.
- Research and Development (R&D).
- Project Management Office (PMO).

Course Offerings:

By the end of this course, the participants will have able to:

- Integrate security practices seamlessly into every phase of the Software Development Lifecycle (SDLC).
- Implement and automate security testing tools within CI/CD pipelines.
- Apply secure coding principles to prevent common vulnerabilities.
- Conduct effective threat modeling for agile and DevOps projects.
- Secure containerized environments using Docker and Kubernetes best practices.
- Manage infrastructure as code (IaC) with a focus on security and compliance.
- Develop a strategy for continuous security monitoring and incident response.
- Foster a culture of security awareness and shared responsibility across teams.
- Implement compliance as code to meet regulatory requirements efficiently.
- Establish a security champions program to scale security expertise.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants can apply their new skills immediately in their work environments. This course moves beyond theoretical lectures to focus on hands-on learning and real-world application. The curriculum is structured around a blend of expert-led instruction, detailed case studies of successful DevSecOps implementations, and collaborative group exercises that simulate real-life challenges. Participants will engage in hands-on labs to configure security tools, write secure code, and automate security checks in a CI/CD pipeline. Team-based workshops will encourage problem-solving and peer-to-peer learning, allowing attendees to discuss and develop strategies for overcoming cultural and technical hurdles. Throughout the course, continuous feedback is provided by the instructor to guide learning and reinforce key concepts. This dynamic and engaging approach ensures a deep understanding of DevSecOps principles and practices, empowering participants to drive meaningful security improvements within their organizations.

Course Agenda (Course Units):

Unit One Foundations of DevSecOps and Agile Security

- Introduction to DevOps and its core principles.
- The evolution from DevOps to DevSecOps.
- Understanding the "Shift Left" security paradigm.
- Key principles and benefits of integrating security into agile workflows.
- Building a culture of shared security responsibility.
- Identifying common security bottlenecks in traditional development.
- The role of automation in a DevSecOps framework.

Unit Two Secure Software Development Lifecycle (SSDLC)

- Integrating security requirements into user stories and backlogs.
- Introduction to threat modeling methodologies (e.g., STRIDE, PASTA).
- Conducting threat modeling sessions in an agile sprint.
- Secure coding standards and best practices (OWASP Top 10).
- Static Application Security Testing (SAST) tools and integration.
- Peer code reviews as a security practice.
- Managing and prioritizing identified vulnerabilities.

Unit Three Integrating Security into the CI/CD Pipeline

- Anatomy of a secure CI/CD pipeline.
- Automating security in the build and integration phases.
- Dynamic Application Security Testing (DAST) strategies.
- Interactive Application Security Testing (IAST) and its role.
- Software Composition Analysis (SCA) for managing open-source risk.
- Implementing security gates and quality checks in the pipeline.
- Secrets management strategies for CI/CD environments.

Unit Four Securing Modern Infrastructure and Applications

- Security principles of Infrastructure as Code (IaC).
- Scanning IaC templates (e.g., Terraform, CloudFormation) for vulnerabilities.
- Introduction to container security concepts.
- Securing Docker files and container images.
- Runtime security for containers and Kubernetes orchestration.
- Cloud-native security best practices for AWS, Azure, and GCP.
- Implementing security in microservices architecture.

Unit Five Governance, Monitoring, and Continuous Improvement

- Implementing Compliance as Code for regulatory adherence.
- Continuous security monitoring and logging strategies.
- Automated alerting and incident response in a DevSecOps context.
- Measuring DevSecOps success with key performance indicators (KPIs).
- The role and structure of a Security Champions program.
- Advanced vulnerability management and remediation workflows.
- Future trends and the evolution of DevSecOps.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Beyond tools and automation, how can an organization fundamentally measure the cultural shift required for a successful DevSecOps transformation?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by adopting a holistic and strategic perspective on DevSecOps, moving beyond a narrow focus on specific tools. While many courses concentrate on the technical implementation of security scanners and pipeline configurations, this program emphasizes the foundational pillars of a successful transformation: culture, process, and technology. We delve deeply into the human element, providing actionable strategies for fostering a culture of shared security ownership and establishing effective programs like security champions. The curriculum is built around practical, real-world case studies and scenarios, ensuring that participants learn not just the "how" but also the "why" behind each practice. Rather than simply listing tools, we teach the principles of selecting, integrating, and scaling security solutions to fit an organization's unique context. The course content is designed to be tool-agnostic where principles are concerned, empowering participants with a versatile skill set that remains relevant as technologies evolve. It focuses on building resilient systems and processes, enabling attendees to return to their organizations as strategic leaders capable of driving sustainable and impactful security improvements.