DevOps Institute: DevSecOps Foundation - Including Exam

Duration: 2 Days **Course Code: DEVSOF** **Delivery Method: Virtual Learning**

Overview:

Integrating security practices into DevOps, such as Security as Code, is a way for security practitioners to operate and contribute value with less friction. Security practices must adapt dynamically to ensure data security and privacy issues are not left behind in the fast-paced world of DevOps

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

Target audience:
- Anyone involved or interested in learning about DevSecOps strategies and automation
- Anyone involved in Continuous Delivery toolchain architectures
- Compliance Team
- Delivery Staff
- DevOps Engineers
- IT Managers
- IT Security Professionals, Practitioners, and Managers
- Maintenance and support staff
- Managed Service Providers
- Project & Product Managers
- Quality Assurance Teams
- Release Managers
- Scrum Masters
- Site Reliability Engineers
- Software Engineers
- Testers

Prerequisites:

None

Testing and Certification

Exam Details

Questions: 40

Languages: English, Brazilian Portuguese, Chinese

Format: Multiple Choice

Passing Score: 65%

Delivery: Web-based

Duration: 60 minutes

Open Book: Yes

Content:

Cyber Threat Landscape (CTL)

Tactics, techniques and procedures (TTPs) describe how threat agents orchestrate and manage attacks. Threat Models optimize security by identifying objectives and vulnerabilities such as OWASP top ten, before defining counter-measures. Continuous Delivery practices are engaged to realize continuous governance, risk management and compliance.

Responsive DevSecOps Model

Security is made continuously adaptive and auditable by breaking security silos, cultivating a symbiotic relationship between security and other business units. Security specific practices and integrated toolsets as code (such as security scans) enable automated security KPIs and observable security practices into the DevOps value stream.

DevSecOps Stakeholders

Gaps between traditional waterfall security cultures and fast-paced DevOps cultures, are removed by building collaboration and trust. Through improving credibility, reliability and empathy while reducing self-interest. Decisions are based on advice from everyone affected and people with expertise using systems thinking. Shared metrics assure adaptable governance using discipline, with automation, transparency and accountability.

Realizing DevSecOps Outcomes

Security is built into the value stream efficiently with empowered development teams implementing features securely, shift-left security testing, tools for automated feedback. Culture improvements instead of policy enforcements ensure security and software engineers are continuously cross-skilling and collaborating.

Pipelines ; Continuous Compliance

Security test and scanning tools are integrated into the CI/CD pipeline to finding known vulnerabilities (published CVEs) and common software weaknesses (CWEs). Repetitive security tasks are automated such as configurations, Fuzz testing and long running security tasks. Compliance as Code helps in automating compliance requirements to foster collaboration, repeatability, and continuous compliance.

DevSecOps Practices

Security is integrated into people, process, technology and governance practices. Continuous security practices for DevSecOps are implemented in onboarding processes for stakeholders. Security practices and outcomes are monitored and improved using data-driven decision making and response patterns. Lean and value stream thinking ensure that security does not cause waste, delays or constraints for flow.

Getting Started

Value Stream Mapping establishes where security activities and bottlenecks currently happen. Collaborative design of a target value state map addresses security requirements, communication and automation improvements. Scope of the design includes practices for Artifact Management, Risk Management, Identity Access Management, Secrets Management, Encryption, Governance, Risk and Compliance, Monitoring and Logging, Incident response and learning

Learning Using Outcomes

Continuous DevSecOps learning programs are implemented to meet evolving security requirements for the organization and individuals using strategies such as lunch and learns, mentoring, professional education, employee learning plans, structured training classes, Dojos, retrospective learning, gamification, and DevOps Institute SKILup Days.

Additional Information:

Preparation
Instructor-Led, Exam Prep, SKILup eLearning, Self-Study

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/