

EC Council

112-55

EC-Council DevSecOps Essentials (DSE)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/112-55>

Latest Version: 6.0

Question: 1

In the context of application architectures, what does the term 'scalability' refer to?

- A. The ability to function without errors
- B. The capacity to increase or decrease performance and cost in response to changes in application and system processing demands
- C. The complexity of the user interface
- D. The security measures integrated into the application

Answer: B

Question: 2

What is the primary goal of integrating security threat modeling in the plan stage of DevSecOps?

- A. To identify potential security threats and vulnerabilities early in the development lifecycle.
- B. To postpone security considerations until the testing phase.
- C. To focus solely on external threats, ignoring internal security risks.
- D. To implement threat modeling only after deployment.

Answer: A

Question: 3

How does integrating security into the CI/CD pipeline benefit DevSecOps?

- A. It ensures security measures are only considered during post-deployment.
- B. It embeds security practices throughout the software development lifecycle, enhancing security without slowing down operations.
- C. It encourages ignoring security during early stages of development.
- D. It isolates security practices from the rest of the development process.

Answer: B

Question: 4

Which development methodology emphasizes customer collaboration over contract negotiation?

- A. Agile
- B. Waterfall
- C. V-model
- D. Spiral

Answer: A

Question: 5

What is a key characteristic of modern application architectures compared to traditional ones?

- A. Reduced scalability and adaptability
- B. Longer development cycles
- C. Increased dependency on monolithic structures
- D. Emphasis on modularity and microservices

Answer: D

Question: 6

Which pillar of DevSecOps emphasizes ongoing assessment and adaptation of security practices?

- A. Continuous Integration
- B. Continuous Delivery
- C. Continuous Monitoring
- D. Continuous Development

Answer: C

Question: 7

How does Compliance as Code (Cac) facilitate regulatory compliance in DevSecOps?

- A. By manually tracking compliance requirements.
- B. By embedding compliance checks into the automation pipelines, ensuring continuous adherence to regulatory standards.
- C. By eliminating the need for compliance monitoring.
- D. By focusing only on compliance at the end of the development cycle.

Answer: B

Question: 8

Why is the use of Infrastructure as Code (IaC) tools important in DevSecOps?

- A. To manually set up and manage infrastructure.
- B. To increase the time required to provision infrastructure.
- C. To automate the provisioning and management of infrastructure using code.
- D. To eliminate the need for version control in infrastructure setups.

Answer: C

Question: 9

Which methodology introduced the concept of continuous integration and continuous deployment (CI/Cd)?

- A. Waterfall
- B. Agile
- C. Spiral
- D. DevOps

Answer: D

Question: 10

Why is threat modeling important in secure application development?

- A. It is only useful after a breach has occurred.
- B. It helps in identifying, evaluating, and mitigating potential security threats early in the development process.
- C. It focuses exclusively on physical security threats.
- D. It decreases the understanding of potential security issues.

Answer: B

Thank You for Trying Our Product
Special 16 USD Discount Coupon: NSZUBG3X
Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>