

GIAC

GCSA
GIAC Cloud Security Automation

Questions And Answers PDF Format:

For More Information – Visit link below:
<https://www.certsgrade.com/>

Version = Product



Latest Version: 6.0

Question: 1

During the deployment pipeline, what is a recommended security control for ensuring the authenticity of software packages?

Response:

- A. Digital signatures
- B. Encrypted file systems
- C. Regular password changes
- D. Session timeout policies

Answer: A

Question: 2

How can Kubernetes access control be configured to limit permissions within a cluster?

Response:

- A. Role-Based Access Control (RBAC)
- B. Service Mesh integration
- C. IP whitelisting
- D. Multi-factor authentication (MFA)

Answer: A

Question: 3

What is the primary purpose of securing cloud architecture using Continuous Integration / Continuous Deployment / Continuous Delivery pipelines?

Response:

- A. To slow down the deployment process
- B. To ensure that all changes to the codebase are tracked and tested
- C. To eliminate the need for security measures
- D. To increase manual intervention in the deployment process

Answer: B

Question: 4

Which security consideration is relevant during the Continuous Integration (CI) phase of DevOps?

Response:

- A. Network encryption
- B. Penetration testing
- C. Code analysis and scanning
- D. User authentication

Answer: C

Question: 5

In the context of Compliance as Code, what role do policy definition languages play?

Response:

- A. They provide entertainment content for employees.
- B. They facilitate the creation of unambiguous compliance policies.
- C. They reduce the necessity for network security.
- D. They enhance the graphical user interface of management tools.

Answer: B

Question: 6

Why is it important to apply Compliance as Code principles in cloud environments?

Response:

- A. To reduce cloud storage costs
- B. To improve the aesthetic appeal of applications
- C. To ensure cloud configurations meet regulatory and policy standards
- D. To increase the physical size of the cloud infrastructure

Answer: C

Question: 7

What role does encryption play in serverless security?

(Select all that apply)

Response:

- A. Encrypting data in transit and at rest
- B. Encrypting serverless function code
- C. Encrypting user authentication tokens
- D. Ignoring encryption to improve performance

Answer: A,C

Question: 8

What are effective strategies for securing Configuration Management processes?

Select all that apply

Response:

- A. Regularly updating and patching CM tools and dependencies
- B. Restricting network access to essential services only
- C. Using weak passwords for enhanced usability
- D. Keeping default configurations for faster deployment

Answer: A,B

Question: 9

Which of the following are key components of Kubernetes security?

(Select all that apply)

Response:

- A. Namespaces
- B. Docker containers
- C. Service accounts
- D. Virtual machines

Answer: A,C

Question: 10

Which of the following is a benefit of integrating security practices into container orchestration?

Response:

- A. It eliminates the need for security monitoring tools.
- B. It allows for automated security scanning and policy enforcement.

-
- C. It ensures that containers are always run as root.
 - D. It increases the number of undetected security incidents.

Answer: B

For More Information – **Visit link below:**
<https://www.certsgrade.com/>

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

16 USD Discount Coupon Code: **NB4XKTMZ**



Visit us at <https://www.certsgrade.com/pdf/gcsa/>