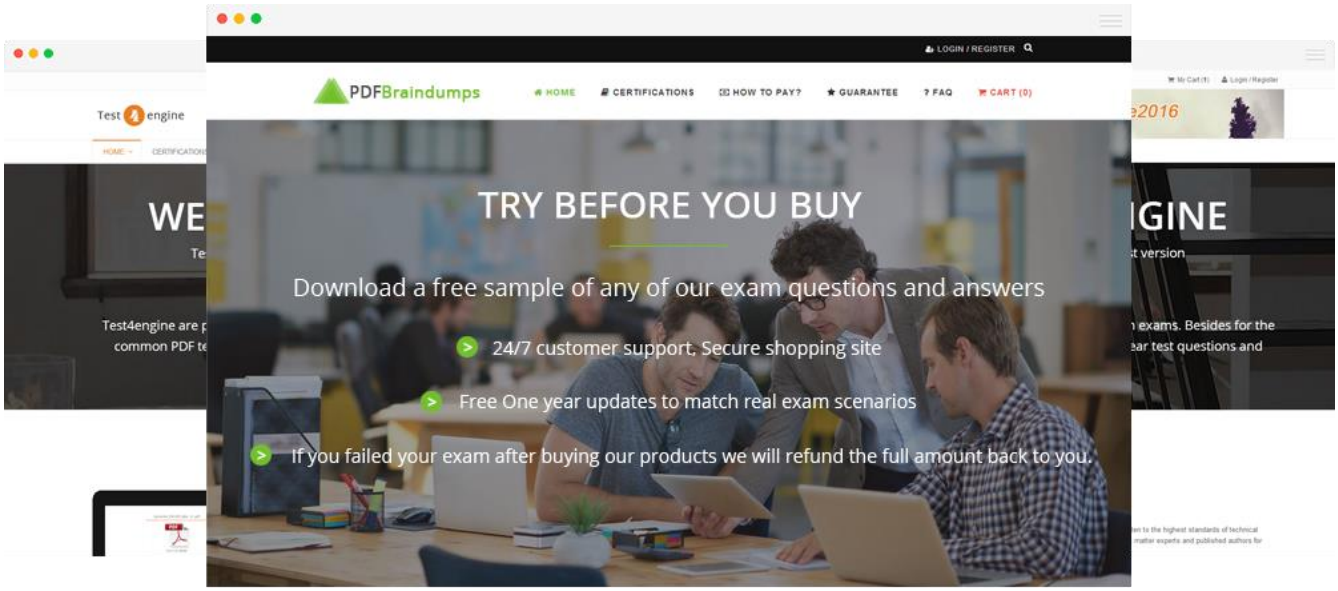
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **GCSA**

Title : GIAC Cloud Security Automation

Vendor : GIAC

Version : DEMO

NO.1 Which security control is most effective in protecting microservices from unauthorized access?
Response:
A. Firewalls
B. Load balancers
C. Service-specific authentication and authorization
D. Serverless computing
Answer: C

NO.2 Which two risks are associated with improper secrets administration?
(Choose Two)
Response:
A. Unauthorized access to sensitive data
B. Hardcoding credentials in application code
C. Enhanced system performance
D. Increased monitoring complexity
Answer: A,B

NO.3 Which of the following is an example of runtime security protection?
Response:
A. Web Application Firewall (WAF)
B. Static code analysis
C. Manual vulnerability scans
D. Reducing monitoring intervals
Answer: A

NO.4 What are the benefits of using Configuration Management as Code?
Select all that apply
Response:
A. Enhanced reproducibility and consistency across environments
B. Increased manual intervention in infrastructure setup
C. Faster recovery from infrastructure failures
D. Decreased visibility into system configurations
Answer: A,C

NO.5 What is the purpose of canary deployment?
Response:
A. To test new features on a small subset of users
B. To deploy updates to all users simultaneously
C. To roll back changes in case of failures
D. To monitor server performance
Answer: A

NO.6 Which tool is commonly used for configuration management in cloud environments?

Response:
A. Kubernetes
B. Puppet
C. Terraform
D. Docker
Answer: B

NO.7 How does cloud infrastructure integration contribute to DevOps practices?
Response:
A. It introduces unnecessary complexity to the development process
B. It facilitates scalability, flexibility, and automation
C. It hinders collaboration between development and operations teams
D. It slows down the deployment pipeline
Answer: B

NO.8 What is the primary security concern associated with containers in cloud environments?
Response:
A. Limited scalability
B. Poor isolation between containers
C. Increased operational costs
D. Lack of monitoring tools
Answer: B

NO.9 What role do container orchestration tools play in container security?
Response:
A. They decrease the visibility into the health and performance of containers.
B. They automatically fix any security vulnerabilities within containers.
C. They help in managing and scaling containers securely and efficiently.
D. They simplify networking between containers to the extent that no firewall rules are required.
Answer: C

NO.10 What is the purpose of runtime security protection in cloud environments?
Response:
A. To detect and prevent attacks in real-time
B. To increase system performance
C. To reduce the number of users
D. To limit monitoring capabilities
Answer: A

NO.11 In the context of GCSA, what role does Infrastructure as Code (IaC) play in cloud security?
Response:
A. It reduces the flexibility of cloud resources.
B. It enhances the physical security of cloud servers.

C. It enables the automated setup and maintenance of cloud environments.
D. It increases the dependency on manual interventions.
Answer: C

NO.12 Which two security practices should be followed when using infrastructure as code? (Choose Two)
Response:
A. Conducting security reviews of IaC templates
B. Hardcoding credentials in IaC files
C. Using automated testing to detect security issues
D. Disabling version control for infrastructure code
Answer: A,C

NO.13 Which security feature of Kubernetes is used to manage sensitive information like passwords, OAuth tokens, and SSH keys?
Response:
A. Namespaces
B. Service accounts
C. Secrets
D. Persistent volumes
Answer: C

NO.14 What is the purpose of a Content Delivery Network (CDN) in cloud environments?
Response:
A. Increase latency for users
B. Improve the speed and availability of content delivery
C. Reduce scalability
D. Centralize content delivery to one location
Answer: B

NO.15 How can Infrastructure as Code contribute to security in cloud environments? (Select all that apply)
Response:
A. By enabling consistent security configurations across environments
B. By automating security testing of cloud resources
C. By encrypting sensitive data in infrastructure code
D. By restricting access to infrastructure code repositories
Answer: A,B