TestsExpert
Ultimate IT Test Preparation Material

GIAC

GCLD
GIAC Cloud Security Essentials

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

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Visit us at

Latest Version: 6.0

Question: 1

Which three considerations are key when maintaining the attack surface of compute resources through automation practices?
(Choose Three)
Response:

A. Automatically escalating privileges for convenience.
B. Periodically reviewing and adjusting security group configurations.
C. Automating the monitoring of network traffic to and from compute instances.
D. Regularly updating automation scripts to adhere to best security practices.
E. Disabling logging to increase performance.

Answer: B,C,D

Question: 2

Which of the following is a key advantage of using Infrastructure as Code (IaC) for provisioning cloud resources?
Response:

A. Increased dependency on manual documentation.
B. Slower deployment cycles.
C. Enhanced consistency and repeatability in resource provisioning.
D. Higher risk of configuration drift.

Answer: C

Question: 3

How does segmentation improve cloud network security?
Response:

A. By reducing the overall cost of the network
B. By limiting the scope of potential breaches
C. By increasing the speed of the network
D. By enhancing user accessibilities

Answer: B

Question: 4

Why is it essential to have a process for regularly reviewing and updating compute resource configurations in the cloud?
Response:

A. To ensure configurations remain overly permissive for user convenience.
B. To align with the latest cloud gaming trends.
C. To adapt to evolving security threats and maintain compliance.
D. To standardize configurations regardless of the workload.

Answer: C

Question: 5

During a cloud-focused penetration test, which of the following outcomes should be a key deliverable?
Response:

A. Comprehensive details on the social engineering tactics used.
B. Identification of all physical vulnerabilities within the data center.
C. Detailed findings on misconfigurations and vulnerabilities.
D. An exhaustive list of all employee names and roles.

Answer: C

Question: 6

What are the key benefits of integrating SIEM (Security Information and Event Management) solutions in cloud-based network security monitoring?
(Choose two)
Response:

A. Automated incident response
B. Enhanced user productivity
C. Real-time visibility and threat detection
D. Reduced need for data encryption

Answer: A,C

Question: 7

In a Platform as a Service (PaaS) setup, the cloud provider is responsible for securing the _____.
Response:

A. Data
B. Applications
C. Runtime
D. Endpoints

Answer: C

Question: 8

What role does compliance play in cloud risk management?
Response:

A. It guarantees the elimination of all cloud risks.
B. It provides a framework for legal and regulatory adherence.
C. It replaces the need for an internal risk management process.
D. It ensures automatic data encryption across all cloud services.

Answer: B

Question: 9

What mechanism ensures data privacy and security when accessing cloud services from various geographical locations?
Response:

A. Data localization
B. Geofencing
C. Virtual Private Network (VPN)
D. Content Delivery Network (CDN)

Answer: C

Question: 10

How do encryption and tunneling contribute to secure data transmission in cloud environments?

Response:

A. By ensuring data is publicly accessible
B. By verifying the identity of users accessing the data
C. By protecting data integrity and confidentiality during transit
D. By increasing the data transfer speed

Answer: C