Certified Network Defender

1. Ray Nicholson works as a senior cloud security engineer in TerraCloud Sec Pvt. Ltd. His organization deployed all applications in a cloud environment in various virtual machines. Using IDS, Ray identified that an attacker compromised a particular VM. He would like to limit the scope of the incident and protect other resources in the cloud. If Ray turns off the VM, what will happen?

A. The data required to be investigated will be lost

B. The data required to be investigated will be recovered

C. The data required to be investigated will be stored in the VHD

D. The data required to be investigated will be saved

Answer(s): A

---

2. An IT company uses two resource groups, named Production-group and Security-group, under the same subscription ID. Under the Production-group, a VM called Ubuntu18 is suspected to be compromised. As a forensic investigator, you need to take a snapshot (ubuntudisksnap) of the OS disk of the suspect virtual machine Ubuntu18 for further investigation and copy the snapshot to a storage account under Security-group.
Identify the next step in the investigation of the security incident in Azure?

A. Copy the snapshot to file share

B. Generate shared access signature

C. Create a backup copy of snapshot in a blob container

D. Mount the snapshot onto the forensic workstation

Answer(s): B

---

3. The GCP environment of a company named Magnitude IT Solutions encountered a security incident. To respond to the incident, the Google Data Incident Response Team was divided based on the different aspects of the incident.
Which member of the team has an authoritative knowledge of incidents and can be involved in different domains such as security, legal, product, and digital forensics?

A. Operations Lead

B. Subject Matter Experts

C. Incident Commander

D. Communications Lead

Answer(s): C

---

4. Jayson Smith works as a cloud security engineer in CloudWorld SecCo Pvt. Ltd. This is a third-party vendor that provides connectivity and transport services between cloud service providers and cloud consumers. Select the actor that describes CloudWorld SecCo Pvt. Ltd. based on the NIST cloud deployment reference architecture?

A. Cloud Broker

B. Cloud Auditor

C. Cloud Carrier

D. Cloud Provider

Answer(s): C

---

5. Brentech Services allows its clients to access (read, write, or delete) Google Cloud Storage resources for a limited time without a Google account while it controls access to Cloud Storage. How does the organization accomplish this?

A. Using BigQuery column-level security

B. Using Signed Documents

C. Using Signed URLs

D. Using BigQuery row-level-security

Answer(s): C

---

6. Daffod is an American cloud service provider that provides cloud-based services to customers worldwide.
Several customers are adopting the cloud services provided by Daffod because they are secure and cost-
effective. Daffod complies with the cloud computing law enacted in the US to realize the importance of information security in the economic and national security interests of the US.
Based on the given information, which law order does Daffod adhere to?

A. FERPA

B. CLOUD

C. FISMA

D. ECPA

Answer(s): C

---

7. Simon recently joined a multinational company as a cloud security engineer. Due to robust security services and products provided by AWS, his organization has been using AWS cloud-based services. Simon has launched an Amazon EC2 Linux instance to deploy an application. He would like to secure Linux AMI.
Which of the following command should Simon run in the EC2 instance to disable user account passwords?

A. passwd -D < USERNAME >

B. passwd -l < USERNAME >

C. passwd -d < USERNAME >

D. passwd -L < USERNAME >

Answer(s): D

---

8. An organization with resources on Google Cloud regularly backs up its service capabilities to ensure high availability and reduce the downtime when a zone or instance becomes unavailable owing to zonal outage or memory shortage in an instance. However, as protocol, the organization must frequently test whether these regular backups are configured.
Which tool's high availability settings must be checked for this?

A. MySQL Database

B. Always on Availability Groups (AGs)

C. SQL Server Database Mirroring (DBM)

D. Google Cloud SQL

Answer(s): D

---

9. Shannon Elizabeth works as a cloud security engineer in VicPro Soft Pvt. Ltd. Microsoft Azure provides all cloud-based services to her organization. Shannon created a resource group (ProdRes), and then created a virtual machine (myprodvm) in the resource group. On myprodvm virtual machine, she enabled JIT from the Azure Security Center dashboard.
What will happen when Shannon enables JIT VM access?

A. It locks down the inbound traffic from myprodvm by creating a rule in the network security group

B. It locks down the inbound traffic to myprodvm by creating a rule in the Azure firewall

C. It locks down the outbound traffic from myprodvm by creating a rule in the network security group

D. It locks down the outbound traffic to myprodvm by creating a rule in the Azure firewall

Answer(s): B

---

10. William O'Neil works as a cloud security engineer in an IT company located in Tampa, Florid

A. To create an access key with normal user accounts, he would like to test whether it is possible to escalate privileges to obtain AWS administrator account access. Which of the following commands should William try to create a new user access key ID and secret key for a user?

B. aws iam target_user -user-name create-access-key

C. aws iam create-access-key -user-name target_user

D. aws iam create-access-key target_user -user-name

E. aws iam -user-name target_user create-access-key

Answer(s): B

---

11. Colin Farrell works as a senior cloud security engineer in a healthcare company. His organization has migrated all workloads and data in a private cloud environment. An attacker used the cloud environment as a point to disrupt the business of Colin's organization. Using intrusion detection prevention systems, antivirus software, and log analyzers, Colin successfully detected the incident; however, a group of users were not able to avail the critical services provided by his organization. Based on the incident impact level classification scales, select the severity of the incident encountered by Colin's organization?

A. High

B. None

C. Low

D. Medium

Answer(s): A

---

12. Sam, a cloud admin, works for a technology company that uses Azure resources. Because Azure contains the resources of numerous organizations and several alerts are received timely, it is difficult for the technology company to identify risky resources, determine their owner, know whether they are needed, and know who pays for them. How can Sam organize resources to determine this information immediately?

A. By using tags

B. By setting up Azure Front Door

C. By configuring workflow automation

D. By using ASC Data Connector

Answer(s): A

---

13. Georgia Lyman works as a cloud security engineer in a multinational company. Her organization uses cloud-based services. Its virtualized networks and associated virtualized resources encountered certain capacity limitations that affected the data transfer performance and virtual server communication. How can Georgia eliminate the data transfer capacity thresholds imposed on a virtual server by its virtualized environment?

A. By allowing the virtual appliance to bypass the hypervisor and access the I/O card of the physical server directly

B. By restricting the virtual appliance to bypass the hypervisor and access the I/O card of the physical server directly

C. By restricting the virtual server to bypass the hypervisor and access the I/O card of the physical server directly

D. By allowing the virtual server to bypass the hypervisor and access the I/O card of the physical server directly

Answer(s): D

---

14. A client wants to restrict access to its Google Cloud Platform (GCP) resources to a specified IP range by making a trust-list. Accordingly, the client limits GCP access to users in its organization network or grants company auditors access to a requested GCP resource only. Which of the following GCP services can help the client?

A. Cloud IDS

B. VPC Service Controls

C. Cloud Router

D. Identity and Access Management

Answer(s): B

---

15. SecureSoft IT Pvt. Ltd. is an IT company located in Charlotte, North Carolina, that develops software for the healthcare industry. The organization generates a tremendous amount of unorganized data such as video and audio files. Kurt recently joined SecureSoft IT Pvt. Ltd. as a cloud security engineer. He manages the organizational data using NoSQL databases. Based on the given information, which of the following data are being generated by Kurt's organization?

A. Metadata

B. Structured Data

C. Unstructured Data

D. Semi-Structured Data

Answer(s): C

---

16. Global InfoSec Solution Pvt. Ltd. is an IT company that develops mobile-based software and applications. For smooth, secure, and cost-effective facilitation of business, the organization uses public cloud services. Now, Global InfoSec Solution Pvt. Ltd. is encountering a vendor lock-in issue.
What is vendor lock-in in cloud computing?

A. It is a situation in which a cloud consumer cannot switch to another cloud service broker without substantial switching costs

B. It is a situation in which a cloud consumer cannot switch to a cloud carrier without substantial switching costs

C. It is a situation in which a cloud service provider cannot switch to another cloud service broker without substantial switching costs

D. It is a situation in which a cloud consumer cannot switch to another cloud service provider without substantial switching costs

Answer(s): D

---

17. A web server passes the reservation information to an application server and then the application server queries an Airline service.
Which of the following AWS service allows secure hosted queue server-side encryption (SSE), or uses custom SSE keys managed in AWS
Key Management Service (AWS KMS)?

A. Amazon Simple Workflow

B. Amazon SQS

C. Amazon SNS

D. Amazon CloudSearch

Answer(s): B

---

18. A security incident has occurred within an organization's AWS environment. A cloud forensic investigation procedure is initiated for the acquisition of forensic evidence from the compromised EC2 instances. However, it is essential to abide by the data privacy laws while provisioning any forensic instance and sending it for analysis.
What can the organization do initially to avoid the legal implications of moving data between two AWS regions for analysis?

A. Create evidence volume from the snapshot

B. Provision and launch a forensic workstation

C. Mount the evidence volume on the forensic workstation

D. Attach the evidence volume to the forensic workstation

Answer(s): A

---

19. The cloud administrator John was assigned a task to create a different subscription for each division of his organization. He has to ensure all the subscriptions are linked to a single Azure AD tenant and each subscription has identical role assignments.
Which Azure service will he make use of?

A. Azure AD Privileged Identity Management

B. Azure AD Multi-Factor Authentication

C. Azure AD Identity Protection

D. Azure AD Self-Service Password Reset

Answer(s): A

---

20. An organization is developing a new AWS multitier web application with complex queries and table joins.
However, because the organization is small with limited staff, it requires high availability.
Which of the following Amazon services is suitable for the requirements of the organization?

A. Amazon HSM

B. Amazon Snowball

C. Amazon Glacier

D. Amazon DynamoDB

Answer(s): D
