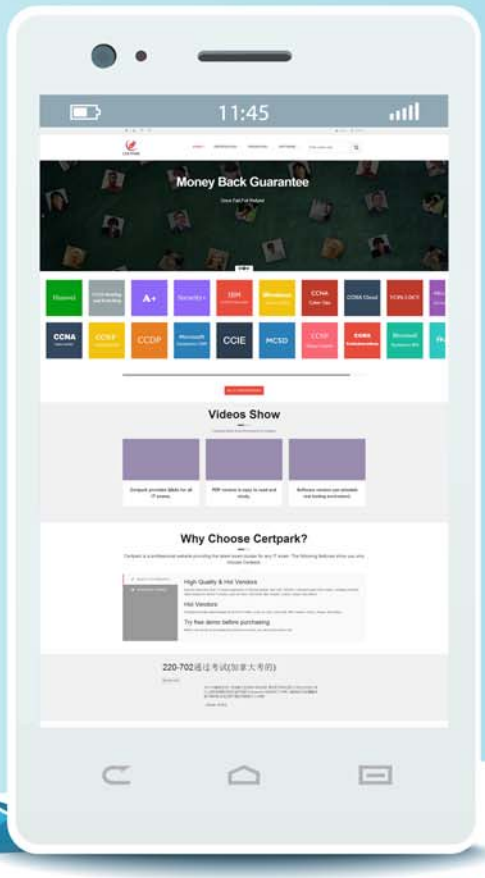
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **312-40**

Title : Certified Cloud Security Engineer (CCSE)

Version : DEMO

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: A
Explanation:
When Ray Nicholson, the senior cloud security engineer, identifies that an attacker has compromised a particular virtual machine (VM) using an Intrusion Detection System (IDS), his priority is to limit the scope of the incident and protect other resources in the cloud environment.
Turning off the compromised VM may seem like an immediate protective action, but it has significant implications:
1. Shutdown Impact: When a VM is turned off, its current state and all volatile data in the RAM are lost. This includes any data that might be crucial for forensic analysis, such as the attacker's tools and running processes.
2. Forensic Data Loss: Critical evidence needed for a thorough investigation, such as memory dumps, active network connections, and ephemeral data, will no longer be accessible.
3. Data Persistence: While some data is stored in the Virtual Hard Disk (VHD), not all
of the forensic data can be retrieved from the disk image alone. Live analysis often provides insights that cannot be captured from static data.
Thus, by turning off the VM, Ray risks losing essential forensic data that is necessary for a complete investigation into the incident.
Reference:
1. NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
2. AWS Cloud Security Best Practices
3. Azure Security Documentation

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: B
Explanation:
When an IT company suspects that a VM called Ubuntu18 in the Production-group has been

compromised, it is essential to perform a forensic investigation. The process of taking a snapshot and ensuring its integrity and accessibility involves several steps:
1. Snapshot Creation: First, create a snapshot of the OS disk of the suspect VM,
named ubuntudisksnap. This snapshot is a point-in-time copy of the VM's disk, ensuring that all data at that moment is captured.
2. Snapshot Security: Next, to transfer this snapshot securely to a storage account under the Security-group, a shared access signature (SAS) needs to be generated. A SAS provides delegated access to Azure storage resources without exposing the storage account keys.
3. Data Transfer: With the SAS token, the snapshot can be securely copied to a storage account in the Security-group. This method ensures that only authorized personnel can access the snapshot for further investigation.
4. Further Analysis: After copying the snapshot, it can be mounted onto a forensic workstation for detailed examination. This step involves examining the contents of the snapshot for any malicious activity or artifacts left by the attacker.
Generating a shared access signature is a critical step in ensuring that the snapshot can be securely accessed and transferred without compromising the integrity and security of the data.
Reference:
1. Microsoft Azure Documentation on Shared Access Signatures (SAS)
2. Azure Security Best Practices and Patterns
3. Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing

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: C
Explanation:
In the context of a security incident within the GCP environment of Magnitude IT Solutions, the Google Data Incident Response Team would be organized to address various aspects of the incident effectively. Among the team, the role with the authoritative knowledge of incidents and involvement in different domains such as security, legal, product, and digital forensics is the Incident Commander.
Here’s why:
1. Authority and Responsibility: The Incident Commander (IC) is typically responsible for the overall management of the incident response. This includes making critical decisions, coordinating the efforts of the entire response team, and ensuring that all aspects of the incident are addressed.
2. Cross-Functional Involvement: The IC has the expertise and authority to interact with various domains such as security (to understand and mitigate threats), legal (to ensure compliance and manage legal risks), product (to understand the impact on services), and digital forensics (to guide the investigation and evidence collection).

3. Leadership and Coordination: The IC leads the response effort, ensuring that all team members, including Subject Matter Experts (SMEs), Operations Leads, and Communications Leads, are working in sync and that the incident response plan is effectively executed.
4. Communication: The IC is the primary point of contact for internal and external stakeholders, ensuring clear and consistent communication about the status and actions being taken in response to the incident.
In summary, the Incident Commander is the central figure with the authoritative knowledge and cross-functional involvement necessary to manage a security incident comprehensively.
Reference:
1. NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide
2. Google Cloud Platform Incident Response and Management Guidelines
3. Cloud Security Alliance (CSA) Incident Response Framework

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: 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: C