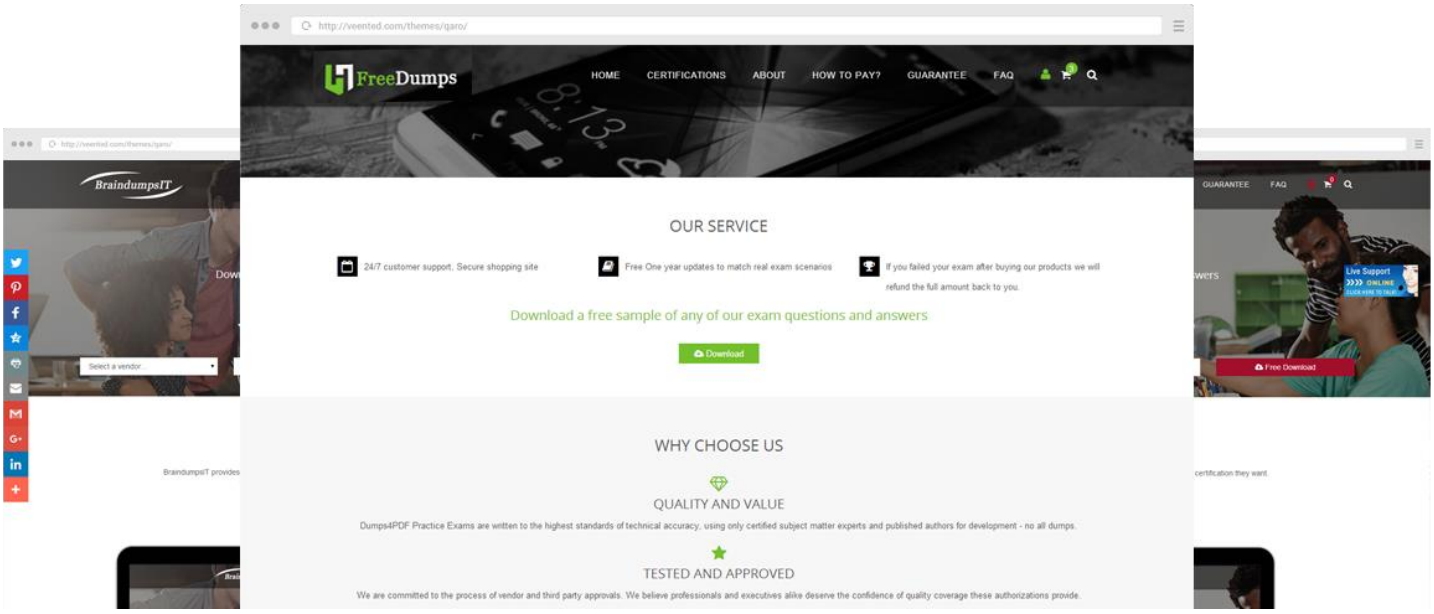
FreeDumps



WHAT PEOPLE SAY

Disclaimer Policy: The site does not guarantee the content of the comments. Because of the different time and the changes in the scope of the exam, it can produce different effect. Before you purchase the dump, please carefully read the product introduction from the page. In addition, please be advised the site will not be responsible for the content of the comments and contradictions between users.

> *Can not believe C2040-440! it is really same with the exam*

ATWOOD

> *If you want to pass exam casually I advise you to purchase study guide. A2010-578 study guide have a part of questions with real test.*

MILES

http://www.freedumps.top

Latest valid dumps torrent and free demo for certification exam prep

Exam : **312-40**

Title : EC-Council Certified Cloud Security Engineer (CCSE)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 SecureSoft Solutions Pvt. Ltd. is an IT company that develops mobile-based applications. Owing to the secure and cost-effective cloud-based services provided by Google, the organization migrated its applications and data from on premises environment to Google cloud. Sienna Miller, a cloud security engineer, selected the Coldlinc Storage class for storing data in the Google cloud storage bucket. What is the minimum storage duration for Coldline Storage?

A. 60 days

B. 120 days

C. 50 days

D. 90 days

Answer: D

NO.2 Gabriel Bateman has been working as a cloud security engineer in an IT company for the past 5 years. Owing to the recent onset of the COVID-19 pandemic, his organization has given the provision to work from home to all employees. Gabriel's organization uses Microsoft Office 365 that allows all employees access files, emails, and other Office programs securely from various locations on multiple devices. Who among the following is responsible for patch management in Microsoft Office 365?

A. Both Gabriel's organization and Microsoft share responsibilities for patch management

B. Gabriel's organization should outsource patch management to a third party

C. Gabriel's organization is entirely responsible for patch management

D. Microsoft is entirely responsible for patch management

Answer: D

NO.3 Rachael Taylor works as a cloud security engineer in CyTech Private Ltd whose previous cloud service provider used to levy high charges for resource utilization. Rachael would like to check resource utilization to Identify resources that are not in use. but the cloud service provider did not have the provision that allows cloud consumers to view resource utilization. Because AWS provides various cloud-based services, including resource utilization and a secure environment to cloud consumers, her organization adopted AWS cloud-based services. Rachael would like to view operational performance, resource utilization, and overall demand patterns, including metrics such as disk reads and writes, CPU utilization, and network traffic. Which of the following AWS services fulfills Racheal's requirements?

A. Amazon CloudWatch Security

B. Amazon CloudTrail Security

C. Amazon Route 53 Security

D. Amazon CloudFront Security

Answer: A

NO.4 Luke Grimes has recently joined a multinational company as a cloud security engineer. The company has been using the AWS cloud. He would like to reduce the risk of man-in-the-middle attacks in all Redshift clusters.

Which of the following parameters should Grimes enable to reduce the risk of man-in-the-middle attacks in all Redshift clusters?

A. wlm_ssl

B. enable_user_ssl

C. require_ssl
D. fips_ssl
Answer: C
Explanation:
To reduce the risk of man-in-the-middle attacks in all Redshift clusters, Luke Grimes should enable the require_ssl parameter. This setting ensures that connections to Amazon Redshift clusters are required to use encryption in transit, which is crucial for securing data and preventing eavesdropping or manipulation of network traffic.
SSL (Secure Sockets Layer): SSL is a standard security technology for establishing an encrypted link between a server and a client-typically a web server (website) and a browser, or a mail server and a mail client1.
require_ssl Parameter: By setting the require_ssl parameter to true, Luke will enforce that all connections to the Redshift clusters use SSL encryption. This helps to protect against man-in-the-middle attacks by encrypting the data as it travels between the client and the Redshift cluster2.
Implementation Steps:
Navigate to the Redshift service in the AWS Management Console.
Select the appropriate cluster and go to its properties.
Under the database configurations, locate the Parameter group settings.
Edit the parameters and set require_ssl to true.
Save the changes to enforce SSL for all connections to the cluster.
Reference:
AWS Security Hub: Amazon Redshift controls1.
AWS RedShift Enforce SSL | Security Best Practice2.

NO.5 Melissa George is a cloud security engineer in an IT company. Her organization has adopted cloud-based services. The integration of cloud services has become significantly complicated to be managed by her organization. Therefore, her organization requires a third-party to consult, mediate, and facilitate the selection of a solution. Which of the following NIST cloud deployment reference architecture actors manages cloud service usage, performance, and delivery, and maintains the relationship between the CSPs and cloud consumers?
A. Cloud Auditor
B. Cloud Carrier
C. Cloud Provider
D. Cloud Broker
Answer: D
Explanation:
Cloud Service Integration: As cloud services become more complex, organizations like Melissa George's may require assistance in managing and integrating these services1.
Third-Party Assistance: A third-party entity, known as a cloud broker, can provide the necessary consultation, mediation, and facilitation services to manage cloud service usage and performance1.
Cloud Broker Role: The cloud broker manages the use, performance, and delivery of cloud services, and maintains the relationship between cloud service providers (CSPs) and cloud consumers1.
NIST Reference Architecture: According to the NIST cloud deployment reference architecture, the cloud broker is an actor who helps consumers navigate the complexity of cloud services by offering management and orchestration between users and providers1.

Other Actors: While cloud auditors, cloud carriers, and cloud providers play significant roles within the cloud ecosystem, they do not typically mediate between CSPs and consumers in the way that a cloud broker does1.
Reference:
GeeksforGeeks article on Cloud Stakeholders as per NIST1.

NO.6 An Azure organization wants to enforce its on-premises AD security and password policies to filter brute-force attacks. Instead of using legacy authentication, the users should sign in to on-premises and cloud-based applications using the same passwords in Azure AD. Which Azure AD feature can enable users to access Azure resources?

A. Azure Automation

B. Azure AD Connect

C. Azure AD Pass Through Authentication

D. Azure Policy

Answer: C

Explanation:
Azure AD Pass-Through Authentication (PTA) allows users to sign in to both on-premises and cloud-based applications using the same passwords. This feature is part of Azure Active Directory (AD) and helps organizations enforce their on-premises AD security and password policies in the cloud, thereby providing a seamless user experience while maintaining security.
Here's how Azure AD PTA works:
Integration with On-Premises AD: Azure AD PTA integrates with an organization's on-premises AD to apply the same security and password policies to cloud resources.
Authentication Request Handling: When a user signs in, the authentication request is passed through to the on-premises AD for validation.
Brute-Force Attack Protection: By enforcing the on-premises AD security policies, Azure AD PTA helps to filter out brute-force attacks.
No Passwords Stored in the Cloud: User passwords remain on-premises and are not stored in Azure AD, which enhances security.
Simple Sign-On Experience: Users enjoy a simple sign-on experience with the same set of credentials across on-premises and cloud services.
Reference:
Microsoft's documentation on deploying on-premises Microsoft Entra Password Protection, which works with Azure AD PTA1.
A step-by-step guide on implementing Azure AD Password Protection on-premises, which complements the PTA feature2.
An overview of Azure AD Password Protection and Smart Lockout features, which are part of the broader Azure AD security framework3.

NO.7 James Harden works as a cloud security engineer in an IT company. James' organization has adopted a RaaS architectural model in which the production application is placed in the cloud and the recovery or backup target is kept in the private data center. Based on the given information, which RaaS architectural model is implemented in James' organization?

A. From-cloud RaaS

B. By-cloud RaaS

C. To-cloud RaaS

D. In-cloud RaaS

Answer: A

Explanation:

The RaaS (Recovery as a Service) architectural model described, where the production application is placed in the cloud and the recovery or backup target is kept in the private data center, is known as "From-cloud RaaS." This model is designed for organizations that want to utilize cloud resources for their primary operations while maintaining their disaster recovery systems on-premises.

Here's how the From-cloud RaaS model works:

Cloud Production Environment: The primary production application runs in the cloud, taking advantage of the cloud's scalability and flexibility.

On-Premises Recovery: The disaster recovery site is located in the organization's private data center, not in the cloud.

Data Replication: Data is replicated from the cloud to the on-premises data center to ensure that the backup is up-to-date.

Disaster Recovery: In the event of a disaster affecting the cloud environment, the organization can recover its applications and data from the on-premises backup.

Control and Compliance: This model allows organizations to maintain greater control over their recovery processes and meet specific compliance requirements that may not be fully addressed in the cloud.

Reference:

Industry guidelines on RaaS architectural models, explaining the different approaches including From-cloud RaaS.

A white paper discussing the benefits and considerations of various RaaS deployment models for organizations.

NO.8 Kevin Williamson has been working as a cloud security engineer in a startup IT company. The business performed by his organization does not require live updating. A DRaaS company provided a disaster recovery site to Kevin's organization with little or no equipment, backup services with no network connectivity, it does not perform automatic failover. and involves data synchronization with a high risk of data loss. Based on the given information, which of the following disaster recovery sites is provided by the DRaaS company to Kevin's organization?

A. Hot Site

B. Warm Site

C. Remote site

D. Cold Site

Answer: D

Explanation:

Cold Site: A cold site is a disaster recovery site with minimal infrastructure. It typically has little or no equipment, no live network connectivity, and no automatic failover. Data synchronization might involve significant delays, and there is a higher risk of data loss compared to hot or warm sites. Cold sites are cost-effective but require more time to become operational during a disaster.

Hot Site: A fully operational site with real-time data replication, live network connectivity, and immediate failover capability. It is designed for minimal downtime and data loss but is expensive to maintain.

Warm Site: A partially equipped site that has some equipment and network connectivity but does not have real-time data replication or full automatic failover. It offers a middle ground between cost and recovery time.
Remote Site: This term can sometimes be used generically for any off-site disaster recovery location, but it does not describe the specific characteristics of the site provided in this scenario.
Since the DRaaS company provided a site with minimal equipment, no network connectivity, no automatic failover, and a high risk of data loss, it fits the definition of a Cold Site.

NO.9 Steven Smith has been working as a cloud security engineer in an MNC for the past 4 years. His organization uses AWS cloud-based services. Steven handles a complex application on AWS that has several resources and it is difficult for him to manage these resources. Which of the following AWS services allows Steven to make a set of related AWS resources easily and use or provision them in an orderly manner so that he can spend less time managing resources and more time on the applications that run in the AWS environment?

A. AWS CloudFormation

B. AWS Control Tower

C. AWS Config

D. Amazon CloudFront

Answer: A

Explanation:
AWS CloudFormation: AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS1.
Resource Management: You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you1.
Complex Applications: For complex applications with multiple resources, CloudFormation allows you to manage related resources as a single unit, called a stack1.
Automation: CloudFormation automates the provisioning and updating of your infrastructure in a safe and controlled manner, with rollbacks and staged updates1.
Benefits: By using AWS CloudFormation, Steven can define his infrastructure in code and use this to create and manage his AWS resources, which simplifies the management of complex applications1.
Reference:
AWS's official documentation on AWS CloudFormation1.

NO.10 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:
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.
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.
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.
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:
Microsoft Azure Documentation on Shared Access Signatures (SAS)
Azure Security Best Practices and Patterns
Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing

NO.11 TeratInfo Pvt. Ltd. is an IT company that develops software products and applications for financial organizations. Owing to the cost-effective storage features and robust services provided by cloud computing, TeratInfo Pvt. Ltd. adopted cloud-based services. Recently, its security team observed a dip in the organizational system performance. Susan, a cloud security engineer, reviewed the list of publicly accessible resources, security groups, routing tables, ACLs, subnets, and IAM policies. What is this process called?

A. Checking audit and evidence-gathering features in the cloud service

B. Checking for the right implementation of security management

C. Testing for virtualization management security

D. Performing cloud reconnaissance

Answer: D
Explanation:
The process that Susan, a cloud security engineer, is performing by reviewing the list of publicly accessible resources, security groups, routing tables, ACLs, subnets, and IAM policies is known as performing cloud reconnaissance.
Cloud Reconnaissance: This term refers to the process of gathering information about the cloud environment to identify potential security issues. It involves examining the configurations and settings of cloud resources to detect any misconfigurations or vulnerabilities that could be exploited by attackers.
Purpose of Cloud Reconnaissance:
Identify Publicly Accessible Resources: Determine if any resources are unintentionally exposed to the

public internet.
Review Security Groups and ACLs: Check if the access control lists (ACLs) and security groups are correctly configured to prevent unauthorized access.
Examine Routing Tables and Subnets: Ensure that network traffic is being routed securely and that subnets are configured to segregate resources appropriately.
Assess IAM Policies: Evaluate identity and access management (IAM) policies to ensure that they follow the principle of least privilege and do not grant excessive permissions.
Outcome of Cloud Reconnaissance: The outcome of this process should be a comprehensive understanding of the cloud environment's security posture, which can help in identifying and mitigating potential security risks.
Reference:
Cloud Security Alliance: Cloud Reconnaissance and Security Best Practices.
NIST Cloud Computing Security Reference Architecture.

NO.12 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

NO.13 TechnoSoft Pvt. Ltd. is a BPO company that provides 24 * 7 customer service. To secure the organizational data and applications from adversaries, the organization adopted cloud computing. The security team observed that the employees are browsing restricted and inappropriate web pages. Which of the following techniques will help the security team of TechnoSoft Pvt. Ltd. in preventing the employees from accessing restricted or inappropriate web pages?
A. Data Loss Prevention (DLP)
B. Cloud access security broker (CASB)
C. Geo-Filtering
D. URL filtering
Answer: D
Explanation:
To prevent employees from accessing restricted or inappropriate web pages, the security team of TechnoSoft Pvt. Ltd. should implement URL filtering.
URL Filtering: This technique involves blocking access to specific URLs or websites based on a defined set of rules or categories. It is used to enforce web browsing policies and prevent access to sites that are not permitted in the workplace.
Implementation:
Policy Definition: The security team defines policies that categorize websites and determine which categories should be blocked.
Filtering Solution: A URL filtering solution is deployed, which can be part of a firewall, a secure web gateway, or a standalone system.

Enforcement: The URL filter enforces the policies by inspecting web requests and allowing or blocking access based on the URL's classification.
Benefits of URL Filtering:
Control Web Access: Helps control employee web usage by preventing access to non-work-related or inappropriate sites.
Enhance Security: Reduces the risk of exposure to web-based threats such as phishing, malware, and other malicious content.
Compliance: Assists in maintaining compliance with organizational policies and regulatory requirements.
Reference:
Best Practices for Implementing Web Filtering and Monitoring.
Guide to URL Filtering Solutions for Enterprise Security.

NO.14 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: B

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:
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.
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).
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.
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:
NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide

Google Cloud Platform Incident Response and Management Guidelines
Cloud Security Alliance (CSA) Incident Response Framework

NO.15 Thomas Gibson is a cloud security engineer working in a multinational company. Thomas has created a Route 53 record set from his domain to a system in Florida, and a similar record to machines in Paris and Singapore.
Assume that network conditions remain unchanged and Thomas has hosted the application on Amazon EC2 instance; moreover, multiple instances of the application are deployed on different EC2 regions. When a user located in London visits Thomas's domain, to which location does Amazon Route 53 route the user request?

A. Singapore

B. London

C. Florida

D. Paris

Answer: B

Explanation:
Amazon Route 53 uses geolocation routing to route traffic based on the geographic location of the users, meaning the location from which DNS queries originate1. When a user located in London visits Thomas's domain, Amazon Route 53 will likely route the user request to the location that provides the best latency or is geographically closest among the available options.
Geolocation Routing: Route 53 will identify the geographic location of the user in London and route the request to the nearest or most appropriate endpoint.
Routing Decision: Given the locations mentioned (Florida, Paris, and Singapore), Paris is geographically closest to London compared to Florida and Singapore.
Latency Consideration: If latency-based routing is also configured, Route 53 will route the request to the region that provides the best latency, which is likely to be Paris for a user in London2.
Final Routing: Therefore, the user request from London will be routed to the machines in Paris, ensuring a faster and more efficient response.
Reference:
Amazon Route 53's routing policies are designed to optimize the user experience by directing traffic based on various factors such as geographic location, latency, and health checks12. The geolocation routing policy, in particular, helps in serving traffic from the nearest regional endpoint, which in this case would be Paris for a user located in London1.