Eccouncil 312-40 Practice Questions

Shared by Valentine on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Katie Holmes has been working as a cloud security engineer over the past 7 years in an MNC. Since the outbreak of the COVID-19 pandemic, the cloud service provider could not provide cloud services efficiently to her organization. Therefore, Katie suggested to the management that they should design and build their own data center. Katie's requisition was approved, and after 8 months, Katie's team successfully designed and built an on-premises data center. The data center meets all organizational requirements; however, the capacity components are not redundant. If a component is removed, the data center comes to a halt. Which tier data center was designed and constructed by Katie's team?

Options:

A- Tier III
B- Tier I
C- Tier IV
D- Tier II

Answer:

B

Explanation:

Explore

The data center designed and constructed by Katie Holmes' team is a Tier I data center based on the description provided.

Tier I Data Center: A Tier I data center is characterized by a single path for power and cooling and no redundant components. It provides an improved environment over a simple office setting but is susceptible to disruptions from both planned and unplanned activity1.

Lack of Redundancy: The fact that removing a component brings the data center to a halt

indicates there is no redundancy in place. This is a defining characteristic of a Tier I data center, which has no built-in redundancy to allow for maintenance without affecting operations1.

Operational Aspects:

Uptime: A Tier I data center typically has an uptime of 99.671%.

Maintenance: Any maintenance or unplanned outages will likely result in downtime, as there are no alternate paths or components to take over the load1.

Data centre tiers - Wikipedia1.

Question 2

Question Type: MultipleChoice

Chris Evans has been working as a cloud security engineer in a multinational company over the past 3 years. His organization has been using cloud-based services. Chris uses key vault as a key management solution because it offers easier creation of encryption keys and control over them. Which of the following public cloud service providers allows Chris to do so?

Options:

A- AWS
B- Azure
C- GCP
D- Oracle

Answer:

B

Explanation:

Azure Key Vault is a cloud service provided by Microsoft Azure. It is used for managing cryptographic keys and other secrets used in cloud applications and services. Chris Evans, as a cloud security engineer, would use Azure Key Vault for the following reasons:

Key Management: Azure Key Vault allows for the creation and control of encryption keys used to encrypt data.

Secrets Management: It can also manage other secrets such as tokens, passwords, certificates,

and API keys.

Access Control: Key Vault provides secure access to keys and secrets based on Azure Active Directory identities.

Audit Logs: It offers monitoring and logging capabilities to track how and when keys and secrets are accessed.

Integration: Key Vault integrates with other Azure services, providing a seamless experience for securing application secrets.

Azure's official documentation on Key Vault, which outlines its capabilities for key management and security.

A guide on best practices for using Azure Key Vault for managing cryptographic keys and secrets.

Question 3

Question Type: MultipleChoice

GlobalCloud is a cloud service provider that offers various cloud-based secure and cost-effective services to cloud consumers. The customer base of this organization increased within a short period; thus, external auditing was performed on GlobalCloud. The auditor used spreadsheets, databases, and data analyzing software to analyze a large volume of dat

a. Based on the given information, which cloud-based audit method was used by the auditor to collect the objective evidence?

Options:

A- Gap Analysis
B- CAAT
C- Striping
D- Re-Performance

Answer:

B

Explanation:

Computer-Assisted Audit Techniques (CAATs) are tools and methods used by auditors to analyze

large volumes of data efficiently and effectively. The use of spreadsheets, databases, and data analyzing software to scrutinize a large volume of data and collect objective evidence is indicative of CAATs.

Here's how CAATs operate in this context:

Data Analysis: CAATs enable auditors to handle and analyze large datasets that would be impractical to assess manually.

Efficiency: These techniques improve audit efficiency by automating certain parts of the audit process.

Effectiveness: CAATs enhance the effectiveness of audits by allowing auditors to identify trends, anomalies, and patterns in the data.

Software Utilization: The use of specialized audit software is a hallmark of CAATs, enabling auditors to perform complex analyses.

Objective Evidence: CAATs help in collecting objective evidence by providing a transparent and systematic approach to data analysis.

An article defining CAATs and discussing their advantages and disadvantages1.

A resource explaining the role and benefits of CAATs in auditing information systems2.

A publication detailing how CAATs allow auditors to independently access and test the reliability of client systems3.

Question 4

Question Type: MultipleChoice

Veronica Lauren has an experience of 4 years as a cloud security engineer. Recently, she joined an IT company as a senior cloud security engineer. In 2010, her organization became a victim of a cybersecurity attack in which the attacker breached her organization's cloud security perimeter and stole sensitive information. Since then, her organization started using Google cloud-based services and migrated the organizational workload and data in the Google cloud environment. Veronica would like to detect security breaches in her organization's cloud security perimeter. Which of the following built-in service of Google Security Command Center can help Veronica in monitoring her organization's cloud logging stream and collect logs from one or multiple projects to detect security breaches such as the presence of malware, brute force SSH attempts, and cryptomining?

Options:

A- Event Threat Detection
B- Web Security Scanner
C- Container Threat Detection
D- Security Health Analytics

Answer:

A

Explanation:

To monitor the organization's cloud logging stream and detect security breaches, Veronica Lauren can utilize the Event Threat Detection service within Google Security Command Center.

Event Threat Detection: This built-in service of Google Security Command Center is designed to monitor cloud logs across multiple projects and detect threats such as malware, brute force SSH attempts, and cryptomining1. It uses threat intelligence and advanced analytics to identify and alert on suspicious activity in real time.

Functionality:

Log Analysis: Event Threat Detection continuously analyzes the logs generated by Google Cloud services.

Threat Detection: It automatically detects the presence of threats like malware, SSH brute force attempts, and cryptomining activities.

Alerts and Findings: When a potential threat is detected, Event Threat Detection issues findings that are integrated into the Security Command Center dashboard for further investigation.

Why Not the Others?:

Web Security Scanner: This service is primarily used for identifying security vulnerabilities in web applications hosted on Google Cloud, not for monitoring logs for security breaches.

Container Threat Detection: While this service is useful for detecting runtime threats in containers, it does not provide the broad log analysis capabilities that Event Threat Detection offers.

Security Health Analytics: This service provides automated security scanning to detect misconfigurations and compliance violations in Google Cloud resources, but it is not specifically focused on the real-time threat detection provided by Event Threat Detection.

Security Command Center overview | Google Cloud1.

Question 5

Question Type: MultipleChoice

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?

Options:

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.

AWS's official documentation on AWS CloudFormation1.

Question 6

Question Type: MultipleChoice

Global CyberSec Pvt. Ltd. is an IT company that provides software and application services related to cybersecurity. Owing to the robust security features offered by Microsoft Azure, the organization adopted the Azure cloud environment. A security incident was detected on the Azure cloud platform. Global CyberSec Pvt. Ltd.'s security team examined the log data collected from various sources. They found that the VM was affected. In this scenario, when should the backup copy of the snapshot be taken in a blob container as a page blob during the forensic acquisition of the compromised Azure VM?

Options:

A- After deleting the snapshot from the source resource group
B- Before mounting the snapshot onto the forensic workstation
C- After mounting the snapshot onto the forensic workstation
D- Before deleting the snapshot from the source resource group

Answer:

D

Explanation:

In the context of forensic acquisition of a compromised Azure VM, it is crucial to maintain the integrity of the evidence. The backup copy of the snapshot should be taken before any operations that could potentially alter the data are performed. This means creating the backup copy in a blob container as a page blob before mounting the snapshot onto the forensic workstation.

Here's the process:

Create Snapshot: First, a snapshot of the VM's disk is created to capture the state of the VM at the point of compromise.

Backup Copy: Before the snapshot is mounted onto the forensic workstation for analysis, a backup copy of the snapshot should be taken and stored in a blob container as a page blob.

Maintain Integrity: This step ensures that the original snapshot remains unaltered and can be used as evidence, maintaining the chain of custody.

Forensic Analysis: After the backup copy is secured, the snapshot can be mounted onto the forensic workstation for detailed analysis.

Documentation: All steps taken during the forensic acquisition process should be thoroughly documented for legal and compliance purposes.

Microsoft's guidelines on the computer forensics chain of custody in Azure, which include the process of handling VM snapshots for forensic purposes1.

Question 7

Question Type: MultipleChoice

Global CloudEnv is a cloud service provider that provides various cloud-based services to cloud consumers. The cloud service provider adheres to the framework that can be used as a tool to systematically assess cloud implementation by providing guidance on the security controls that should be implemented by specific actors within the cloud supply chain. It is used as the standard to assess the security posture of organizations on the Security, Trust, Assurance, and Risk (STAR) registry. Based on the given information, which of the following cybersecurity control frameworks does Global CloudEnv adhere to?

Options:

A- CDMI
B- CSA CCM
C- CSA CAIQ
D- ITU-T X.1601

Answer:

B

Explanation:

The Cloud Security Alliance's Cloud Controls Matrix (CSA CCM) is a cybersecurity control framework that is specifically designed for cloud computing environments. It provides a detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

Here's how the CSA CCM is used:

Assessment Tool: The CSA CCM serves as a tool for organizations to systematically assess their cloud implementations.

Guidance on Security Controls: It provides guidance on which security controls should be implemented by specific actors within the cloud supply chain.

STAR Registry: The CSA CCM is used as the standard for organizations to report their security posture on the CSA's Security, Trust, Assurance, and Risk (STAR) registry.

Comprehensive Framework: The CCM encompasses a wide range of security topics and is considered one of the most comprehensive frameworks for cloud security.

Industry Standard: It is widely recognized and used as an industry standard for cloud security assurance and compliance.

The CSA CCM is referenced in numerous industry publications and is recommended by cloud security professionals for organizations looking to enhance their cloud security posture.

The CSA's STAR registry lists organizations that have adopted the CCM framework, providing transparency and assurance in cloud security.

Question 8

Question Type: MultipleChoice

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?

Options:

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.

Cloud Security Alliance: Cloud Reconnaissance and Security Best Practices.

NIST Cloud Computing Security Reference Architecture.

Question 9

Question Type: MultipleChoice

Scott Herman works as a cloud security engineer in an IT company located in Ann Arbor, Michigan. His organization uses Office 365 Business Premium that provides Microsoft Teams, secure cloud storage, business email, premium Office applications across devices, advanced cyber threat protection, and device management.

Which of the following cloud computing service models does Microsoft Office 365 represent?

Options:

A- DaaS
B- laaS
C- PaaS
D- SaaS

Answer:

D

Explanation:

SaaS, or Software as a Service, is a cloud computing model where software applications are delivered over the internet. Users subscribe to the service rather than purchasing and installing software on individual devices. Microsoft Office 365 fits this model as it provides access to various applications such as Microsoft Teams, secure cloud storage, business email, and more through a subscription service. Users can access these services from any device, provided they have an internet connection.

Here's a breakdown of how Office 365 aligns with the SaaS model:

Subscription-Based: Office 365 operates on a subscription model, where users pay a recurring fee to use the service.

Cloud-Hosted Applications: The suite includes cloud-hosted versions of traditional Microsoft applications, as well as new tools like Microsoft Teams.

Managed by Provider: Microsoft manages the infrastructure, security, and updates for these applications, relieving users from these responsibilities.

Accessible from Anywhere: As a cloud service, Office 365 can be accessed from anywhere, on any device with internet connectivity.

Business Services: It includes business services like email and device management, which are typical features of SaaS offerings.

Microsoft's description of Office 365 as a cloud-based service1.

Microsoft Azure's definition of SaaS, mentioning Office 365 as an example2.

Microsoft support page explaining Microsoft 365 as a subscription service3.

Question 10

Question Type: MultipleChoice

Trevor Noah works as a cloud security engineer in an IT company located in Seattle, Washington. Trevor has implemented a disaster recovery approach that runs a scaled-down version of a fully functional environment in the cloud. This method is most suitable for his organization's core business-critical functions and solutions that require the RTO and RPO to be within minutes. Based on the given information, which of the following disaster recovery

approach is implemented by Trevor?

Options:

A- Backup and Restore
B- Multi-Cloud Option
C- Pilot Light approach
D- Warm Standby

Answer:

D

Explanation:

The Warm Standby approach in disaster recovery involves running a scaled-down version of a fully functional environment in the cloud. This method is activated quickly in case of a disaster, ensuring that the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are within minutes.

Scaled-Down Environment: A smaller version of the production environment is always running in the cloud. This includes a minimal number of resources required to keep the application operational12.

Quick Activation: In the event of a disaster, the warm standby environment can be quickly scaled up to handle the full production load12.

RTO and RPO: The warm standby approach is designed to achieve an RTO and RPO within minutes, which is essential for business-critical functions12.

Business Continuity: This approach ensures that core business functions continue to operate with minimal disruption during and after a disaster12.

Reference: Warm Standby is a disaster recovery strategy that provides a balance between cost and downtime. It is less expensive than a fully replicated environment but offers a faster recovery time than cold or pilot light approaches12. This makes it suitable for organizations that need to ensure high availability and quick recovery for their critical systems.

Question 11

Question Type: MultipleChoice

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?

Options:

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:

A

Explanation:

To manage multiple subscriptions under a single Azure AD tenant with identical role assignments, Azure AD Privileged Identity Management (PIM) is the service that provides the necessary capabilities.

Link Subscriptions to Azure AD Tenant: John can link all the different subscriptions to the single Azure AD tenant to centralize identity management across the organization1.

Manage Role Assignments: With Azure AD PIM, John can manage, control, and monitor access within Azure AD, Azure, and other Microsoft Online Services like Office 365 or Microsoft 3652.

Identical Role Assignments: Azure AD PIM allows John to configure role assignments that are consistent across all subscriptions. He can assign roles to users, groups, service principals, or managed identities at a particular scope3.

Role Activation and Review: John can require approval to activate privileged roles, enforce just-in-time privileged access, require reason for activating any role, and review access rights2.

Reference: Azure AD PIM is a feature of Azure AD that helps organizations manage, control, and monitor access within their Azure environment. It is particularly useful for scenarios where there are multiple subscriptions and a need to maintain consistent role assignments across them23.