Number: 312-40
Passing Score: 800.0
Time Limit: 120.0
File Version: 2.0

Exam Code: 312-40

Exam Name: Certified Cloud Security Engineer (CCSE)

Exam A

QUESTION 1
The tech giant TSC uses cloud for its operations. As a cloud user, it should implement an effective risk management lifecycle to measure and monitor high and critical risks regularly. Additionally, TSC should define what exactly should be measured and the acceptable variance to ensure timely mitigated risks. In this case, which of the following can be used as a tool for cloud risk management?

A. Information System Audit and Control Association
B. Cloud Security Alliance
C. Committee of Sponsoring Organizations
D. CSA CCM Framework

Correct Answer: D
Section:
Explanation:
The CSA CCM (Cloud Controls Matrix) Framework is a cybersecurity control framework for cloud computing, developed by the Cloud Security Alliance (CSA). It is designed to provide a structured and standardized set of security controls that help organizations assess the overall security posture of their cloud infrastructure and services.
Here's how the CSA CCM Framework serves as a tool for cloud risk management:
1.Comprehensive Controls: The CCM consists of 197 control objectives structured in 17 domains covering all key aspects of cloud technology.
1.Risk Assessment: It can be used for the systematic assessment of a cloud implementation, providing guidance on which security controls should be implemented.
1.Alignment with Standards: The controls framework is aligned with the CSA Security Guidance for Cloud Computing and other industry-accepted security standards and regulations.
1.Shared Responsibility Model: The CCM clarifies the shared responsibility model between cloud service providers (CSPs) and customers (CSCs).
1.Monitoring and Measurement: The CCM includes metrics and implementation guidelines that help define what should be measured and the acceptable variance for risks.
CSA's official documentation on the Cloud Controls Matrix (CCM), which outlines its use as a tool for cloud risk management1.
An article providing a checklist for CSA's Cloud Controls Matrix v4, which discusses how it can be used for managing risk in cloud environments2.

QUESTION 2
A private IT company named Altitude Solutions conducts its operations from the cloud. The company wants to balance the interests of corporate stakeholders (higher management, employees, investors, and suppliers) to achieve control on the cloud infrastructure and facilities (such as data centers) and management of applications at the portfolio level. Which of the following represents the adherence to the higher management directing and controlling activities at various levels of the organization in a cloud environment?

A. Risk Management
B. Governance
C. Corporate Compliance
D. Regulatory Compliance

Correct Answer: B
Section:
Explanation:
Governance in a cloud environment refers to the mechanisms, processes, and relations used by various stakeholders to control and to operate within an organization. It encompasses the practices and policies that ensure the integrity, quality, and security of the data and services.
Here's how governance applies to Altitude Solutions:
1.Stakeholder Interests: Governance ensures that the interests of all stakeholders, including higher management, employees, investors, and suppliers, are balanced and aligned with the company's objectives.
1.Control Mechanisms: It provides a framework for higher management to direct and control activities at various levels, ensuring that cloud infrastructure and applications are managed effectively.
1.Strategic Direction: Governance involves setting the strategic direction of the organization and making decisions on behalf of stakeholders.
1.Performance Monitoring: It includes monitoring the performance of cloud services and infrastructure to ensure they meet the company's strategic goals and compliance requirements.
1.Risk Management: While governance includes risk management as a component, it is broader in scope, encompassing overall control and direction of the organization's operations in the cloud.

A white paper on cloud governance best practices and strategies.
Industry guidelines on IT governance in cloud computing environments.

QUESTION 3
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

Correct Answer: D
Section:
Explanation:
To prevent employees from accessing restricted or inappropriate web pages, the security team of TechnoSoft Pvt. Ltd. should implement URL filtering.
1.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.
1.Implementation:
oPolicy Definition: The security team defines policies that categorize websites and determine which categories should be blocked.
oFiltering Solution: A URL filtering solution is deployed, which can be part of a firewall, a secure web gateway, or a standalone system.
oEnforcement: The URL filter enforces the policies by inspecting web requests and allowing or blocking access based on the URL's classification.
1.Benefits of URL Filtering:
oControl Web Access: Helps control employee web usage by preventing access to non-work-related or inappropriate sites.
oEnhance Security: Reduces the risk of exposure to web-based threats such as phishing, malware, and other malicious content.
oCompliance: Assists in maintaining compliance with organizational policies and regulatory requirements.
Best Practices for Implementing Web Filtering and Monitoring.
Guide to URL Filtering Solutions for Enterprise Security.

QUESTION 4
Chris Noth has recently joined CloudAppSec Private Ltd. as a cloud security engineer. Owing to several instances of malicious activities performed by former employees on his organization's applications and data that reside in an on-premises environment, in 2010, his organization adopted cloud computing and migrated all applications and data to the cloud. Chris would like to manage user identities in cloud-based services and applications. Moreover, he wants to reduce the risk caused by the accounts of former users (employees) by ensuring that the users who leave the system can no longer log in to the system. Therefore, he has enforced an IAM standard that can automate the provisioning and de-provisioning of users when they enter and leave the system. Which of the following IAM standards is implemented by Chris Noth?

A. SCIM
B. XACML
C. OpenID
D. OAuth

Correct Answer: A
Section:
Explanation:
Chris Noth is looking to manage user identities and automate the provisioning and de-provisioning of users in cloud-based services and applications. The IAM standard that supports this functionality is SCIM (System for Cross-domain Identity Management).
1.SCIM Overview: SCIM is an open standard designed to manage user identity information across different domains. It simplifies user management in cloud-based applications and services by allowing for automated user

provisioning and de-provisioning1.
1.Automated Provisioning: With SCIM, when new users are added to an organization's system, their identities can be automatically provisioned across various cloud services without manual intervention1.
1.Automated De-provisioning: Similarly, when users leave the organization or their roles change, SCIM can ensure that their access is automatically revoked or adjusted across all connected services. This reduces the risk of former employees retaining access to sensitive systems and data1.
1.Why Not the Others?:
oXACML (eXtensible Access Control Markup Language) is used for defining access control policies, not for identity provisioning.
oOpenID is an authentication standard that allows users to be authenticated by certain co-operating sites using a third-party service, without the need for passwords.
oOAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.
MajorKey Tech: What is Provisioning and De-provisioning in IAM1.
SailPoint: What is automated provisioning?2.
Nestmeter: Streamlining Security: User Provisioning and Deprovisioning with IAM3.

QUESTION 5
Cosmic IT Services wants to migrate to cloud computing. Before migrating to the cloud, the organization must set business goals for cloud computing as per the guidelines of a standard IT governance body. Which standard IT governance body can help the organization to set business goals and objectives for cloud computing by offering the IT governance named COBIT (Control Objective for Information and Related Technology)?

A. International Standards Organization (ISO)
B. Cloud Security Alliance (CSA)
C. Information System Audit and Control Association (ISACA)
D. Committee of Sponsoring Organizations (COSO)

Correct Answer: C
Section:
Explanation:
Cosmic IT Services is looking to set business goals and objectives for cloud computing using the COBIT framework. The IT governance body that offers COBIT (Control Objectives for Information and Related Technology) is the Information System Audit and Control Association (ISACA).
1.COBIT Overview: COBIT is a framework for developing, implementing, monitoring, and improving IT governance and management practices. It is a comprehensive framework that aligns IT goals with business objectives1.
1.ISACA's Role: ISACA is the organization that developed and maintains the COBIT framework. It provides guidance, benchmarks, and other materials for managing and governing enterprise IT environments1.
1.Setting Business Goals: By utilizing COBIT, Cosmic IT Services can establish a structured approach to align IT processes with business goals, ensuring that their cloud computing initiatives support the overall objectives of the organization1.
1.Why Not the Others?:
oISO (International Standards Organization) develops and publishes a wide range of proprietary, industrial, and commercial standards, but it is not the governing body for COBIT.
oCSA (Cloud Security Alliance) specializes in best practices for security assurance within cloud computing, and while it provides valuable resources, it does not govern COBIT.
oCOSO (Committee of Sponsoring Organizations) focuses on internal control, enterprise risk management, and fraud deterrence, but does not offer COBIT.
ISACA: COBIT | Control Objectives for Information Technologies1.
CIO: What is COBIT? A framework for alignment and governance2.
ITSM Docs: IT Governance COBIT3.

QUESTION 6
Christina Hendricks recently joined an MNC as a cloud security engineer. Owing to robust provisions for storing an enormous quantity of data, security features, and cost-effective services offered by AWS, her organization migrated its applications and data from an on-premises environment to the AWS cloud. Christina's organization generates structured, unstructured, and semi-structured data. Christina's team leader asked her to store block-level data in AWS storage services. Which of the following AWS storage services should be used by Christina to store block-level data?

A. Amazon EBS
B. Amazon Glacier
C. Amazon EFS
D. Amazon S3

Correct Answer: A

Section:
Explanation:
1.Block-Level Storage: Block-level storage is a type of data storage typically used for storing file systems and handling raw storage volumes. It allows for individual management of data blocks1.
1.Amazon EBS: Amazon Elastic Block Store (Amazon EBS) provides high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale2.
1.Data Types: Amazon EBS is suitable for structured, unstructured, and semi-structured data, making it a versatile choice for Christina's organization's needs2.
1.Use Cases: Common use cases for Amazon EBS include databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows2.
1.Exclusion of Other Options: Amazon Glacier is for long-term archival storage, Amazon EFS is for file storage, and Amazon S3 is for object storage. These services do not provide block-level storage like Amazon EBS does3.
AWS's official page on Amazon EBS2.
AWS's explanation of block storage1.

QUESTION 7
Ewan McGregor works as a cloud security engineer in a multinational company that develops software and applications for eCommerce companies. Owing to the robust services provided by AWS for developing applications and software, his organization migrated to the AWS cloud in 2010. To test whether it is possible to escalate privileges to obtain AWS administrator account access, Ewan attempt to update the login profile with regular user accounts. Which of the following commands should Ewan try to update an existing login profile?

A. aws iam update-login-profile -- user-name < password > -- password < username >
B. aws iam update-login-profile -- user-name < username > -- password < password >
C. aws iam update-login-profile -- user-name < password > -- password < username >
D. aws iam update-login-profile -- password < password > -- user-name < username >

Correct Answer: B
Section:
Explanation:
To update an existing login profile for an IAM user, the correct AWS CLI command syntax is as follows:
aws iam update-login-profile --user-name <username> --password
Here's the breakdown of the command:
1.aws iam update-login-profile: This is the AWS CLI command to update the IAM user's login profile.
1.--user-name <username>: The --user-name flag specifies the IAM username whose login profile Ewan wants to update.
1.--password : The --password flag followed by sets the new password for the specified IAM user.
It's important to replace <username> with the actual username and with the new password Ewan wishes to set.
AWS CLI documentation on the update-login-profile command1.

QUESTION 8
InternSoft Solution Pvt. Ltd. is an IT company located in Boston, Massachusetts. The IT and InfoSec teams of the organization uses CASP to customize access rules and automate compliance policies. Using CASP solutions, they could access the account activities in the cloud, which makes it easy for them to achieve compliance, data security, and threat protection. What is CASP?

A. It is a CASB that uses APIs
B. It is a WAF that uses proxies
C. It is a CASB that uses proxies
D. It is a RASP that uses APIs

Correct Answer: A
Section:
Explanation:
CASP in the context of cloud security refers to a Cloud Access Security Broker (CASB) that uses APIs to customize access rules and automate compliance policies.
1.CASB Defined: A CASB is a security policy enforcement point that sits between cloud service consumers and cloud service providers. It ensures secure access to cloud applications and data by managing and enforcing data security policies and practices1.
1.APIs in CASB: APIs are used by CASBs to integrate with cloud services and enforce security policies. This allows for real-time visibility and control over user activities and sensitive data across all cloud services1.

1.Functionality Provided by CASP:
oCustomize Access Rules: CASBs allow organizations to tailor access controls based on various factors such as user role, location, and device.
oAutomate Compliance Policies: They help automate the enforcement of compliance policies, making it easier for organizations to adhere to various regulations.
oMonitor Account Activities: CASBs provide insights into account activities in the cloud, aiding in threat detection and response.
What is a CASB Cloud Access Security Broker? - CrowdStrike1.

QUESTION 9
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?

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

Correct Answer: A
Section:
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.
1.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.
1.Functionality:
oLog Analysis: Event Threat Detection continuously analyzes the logs generated by Google Cloud services.
oThreat Detection: It automatically detects the presence of threats like malware, SSH brute force attempts, and cryptomining activities.
oAlerts 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.
1.Why Not the Others?:
oWeb 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.
oContainer 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.
oSecurity 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 10
An IT organization named WITEC Solutions has adopted cloud computing. The organization must manage risks to keep its business data and services secure and running by gaining knowledge about the approaches suitable for specific risks. Which risk management approach can compensate the organization if it loses sensitive data owing to the risk of an activity?

A. Risk mitigation
B. Risk acceptance
C. Risk avoidance
D. Risk transference

Correct Answer: D
Section:
Explanation:
In risk management, the approach that can compensate an organization for the loss of sensitive data due to the risks of an activity is known as risk transference.
1.Risk Transference: This approach involves transferring the risk to a third party, typically through insurance or outsourcing. In the context of data loss, an organization can purchase a cyber insurance policy that would provide financial compensation in the event of a data breach or loss1.

1.How It Works:
oInsurance Policies: Cyber insurance policies can cover various costs associated with data breaches, including legal fees, notification costs, and even the expenses related to public relations efforts to manage the reputation damage.
oContracts and Agreements: When outsourcing services or functions that involve sensitive data, contracts can include clauses that hold the service provider responsible for any data loss or breaches, effectively transferring the risk away from the organization.
1.Benefits of Risk Transference:
oFinancial Protection: Provides a financial safety net that helps the organization recover from the loss without bearing the entire cost.
oFocus on Core Business: Allows the organization to focus on its core activities without the need to allocate excessive resources to manage specific risks.
Key Considerations in Protecting Sensitive Data Leakage Using Data Loss Prevention Tools1.
Data Risk Management: Process and Best Practices2.

QUESTION 11
The TCK Bank adopts cloud for storing the private data of its customers. The bank usually explains its information sharing practices to its customers and safeguards sensitive data. However, there exist some security loopholes in its information sharing practices. Therefore, hackers could steal the critical data of the bank's customers. In this situation, under which cloud compliance framework will the bank be penalized?

A. GLBA
B. ITAR
C. NIST
D. GDPR

Correct Answer: D
Section:
Explanation:
If TCK Bank has security loopholes in its information sharing practices that lead to the theft of customer data, it could be penalized under the General Data Protection Regulation (GDPR) compliance framework.
1.GDPR Overview: GDPR is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas1.
1.Penalties Under GDPR: The GDPR imposes heavy penalties for non-compliance or breaches, which can be up to 20 million or 4% of the annual global turnover of the organization, whichever is greater1.
1.Relevance to TCK Bank: If TCK Bank operates within the EU or deals with the data of EU citizens, it must comply with GDPR. Any security loopholes that lead to data breaches can result in significant penalties under this framework.
GDPR Compliance: What You Need to Know1.
Understanding GDPR Penalties and Fines2.
GDPR Enforcement Tracker3.

QUESTION 12
Jerry Mulligan is employed by an IT company as a cloud security engineer. In 2014, his organization migrated all applications and data from on-premises to a cloud environment. Jerry would like to perform penetration testing to evaluate the security across virtual machines, installed apps, and OSes in the cloud environment, including conducting various security assessment steps against risks specific to the cloud that could expose them to serious threats. Which of the following cloud computing service models does not allow cloud penetration testing (CPEN) to Jerry?

A. DBaaS
B. laaS
C. PaaS
D. SaaS

Correct Answer: D
Section:
Explanation:
In the cloud computing service models, SaaS (Software as a Service) typically does not allow customers to perform penetration testing. This is because SaaS applications are managed by the service provider, and the security of the application is the responsibility of the provider, not the customer.
Here's why SaaS doesn't allow penetration testing:
1.Managed Service: SaaS providers manage the security of their applications, including regular updates and patches.

1.Shared Environment: SaaS applications often run in a shared environment where multiple customers use the same infrastructure, making it impractical for individual customers to conduct penetration testing.
1.Provider's Policies: Most SaaS providers have strict policies against unauthorized testing, as it could impact the service's integrity and availability for other users.
1.Alternative Assessments: Instead of penetration testing, SaaS providers may offer security assessments or compliance certifications to demonstrate the security of their applications.
Oracle's FAQ on cloud security testing, which states that penetration and vulnerability testing are not allowed for Oracle SaaS offerings1.
Cloud Security Alliance's article on pentesting in the cloud, mentioning that CSPs often have policies describing which tests can be performed and which cannot, especially in SaaS models2.

QUESTION 13
In a tech organization's cloud environment, an adversary can rent thousands of VM instances for launching a DDoS attack. The criminal can also keep secret documents such as terrorist and illegal money transfer docs in the cloud storage. In such a situation, when a forensic investigation is initiated, it involves several stakeholders (government members, industry partners, third-parties, and law enforcement). In this scenario, who acts as the first responder for the security issue on the cloud?

A. Incident Handlers
B. External Assistance
C. Investigators
D. IT Professionals

Correct Answer: A
Section:
Explanation:
In the event of a security issue on the cloud, such as a DDoS attack or illegal activities, Incident Handlers are typically the first responders. Their role is to manage the initial response to the incident, which includes identifying, assessing, and mitigating the threat to reduce damage and recover from the attack.
Here's the role of Incident Handlers as first responders:
1.Incident Identification: They quickly identify the nature and scope of the incident.
1.Initial Response: Incident Handlers take immediate action to contain and control the situation to prevent further damage.
1.Communication: They communicate with internal stakeholders and may coordinate with external parties like law enforcement if necessary.
1.Evidence Preservation: Incident Handlers work to preserve evidence for forensic analysis and legal proceedings.
1.Recovery and Documentation: They assist in the recovery process and document all actions taken for future reference and analysis.
Industry best practices on incident response, highlighting the role of Incident Handlers as first responders.
Guidelines from cybersecurity frameworks outlining the responsibilities of Incident Handlers during a cloud security incident.

QUESTION 14
Scott Herman works as a cloud security engineer in an IT company. His organization has deployed a 3-tier web application in the same Google Cloud Virtual Private Cloud. Each tier (web interface (UI), API, and database) is scaled independently of others. Scott Herman obtained a requirement that the network traffic should always access the database using the API and any request coming directly from the web interface to the database should not be allowed. How should Scott configure the network with minimal steps?

A. By adding tags to each tier and setting up firewall rules to allow the desired traffic flow
B. By adding tags to each tier and setting up routes to allow the desired traffic flow
C. By setting up software-based firewalls on individual VMs
D. By adding each tier to a different subnetwork

Correct Answer: A
Section:
Explanation:
In Google Cloud Virtual Private Cloud (VPC), network tags are used to apply firewall rules to specific instances. Scott can use these tags to control the traffic flow between the tiers of the web application. Here's how he can configure the network:
1.Assign Network Tags: Assign unique network tags to the instances in each tier -- for example, 'ui-tag' for the web interface, 'api-tag' for the API, and 'db-tag' for the database.
1.Create Firewall Rules: Create firewall rules that allow traffic from the API tier to the database tier by specifying the 'api-tag' as the source filter and 'db-tag' as the target filter.
1.Restrict Direct Access: Ensure that there are no rules allowing direct traffic from the 'ui-tag' to the 'db-tag', effectively blocking any direct requests from the web interface to the database.
1.Apply Rules: Apply the firewall rules to the respective instances based on their tags.

By using network tags and firewall rules, Scott can ensure that the database is only accessible via the API, and direct access from the UI is not permitted.
Google Cloud documentation on setting up firewall rules and using network tags1.

QUESTION 15
VenturiaCloud is a cloud service provider that offers robust and cost-effective cloud-based services to cloud consumers. The organization became a victim of a cybersecurity attack. An attacker performed a DDoS attack over the cloud that caused failure in the entire cloud environment. VenturiaCloud conducted a forensics investigation. Who among the following are the first line of defense against cloud security attacks with their primary role being responding against any type of security incident immediately?

A. Law Advisors
B. Incident Handlers
C. Investigators
D. IT Professionals

Correct Answer: B
Section:
Explanation:
Incident Handlers are typically the first line of defense against cloud security attacks, with their primary role being to respond immediately to any type of security incident. In the context of a cybersecurity attack such as a DDoS (Distributed Denial of Service), incident handlers are responsible for the initial response, which includes identifying, managing, recording, and analyzing security threats or incidents in real-time.
Here's how Incident Handlers function as the first line of defense:
1.Immediate Response: They are trained to respond quickly to security incidents to minimize impact and manage the situation.
1.Incident Analysis: Incident Handlers analyze the nature and scope of the incident, including the type of attack and its origin.
1.Mitigation Strategies: They implement strategies to mitigate the attack, such as rerouting traffic or isolating affected systems.
1.Communication: They communicate with relevant stakeholders, including IT professionals, management, and possibly law enforcement.
1.Forensics and Recovery: After an attack, they work on forensics to understand how the breach occurred and on recovery processes to restore services.
An ISACA journal article discussing the roles of various functions in information security, highlighting the first line of defense1.
An Australian Cyber Security Magazine article emphasizing the importance of identity and access management (IAM) as the first line of defense in securing the cloud2.

QUESTION 16
Sandra, who works for SecAppSol Technologies, is on a vacation. Her boss asked her to solve an urgent issue in an application. Sandra had to use applications present on her office laptop to solve this issue, and she successfully rectified it. Despite being in a different location, she could securely use the application. What type of service did the organization use to ensure that Sandra could access her office laptop from a remote area?

A. Amazon AppStream 2.0
B. Amazon Elastic Transcoder Service
C. Amazon SQS
D. Amazon Simple Workflow

Correct Answer: A
Section:
Explanation:
Amazon AppStream 2.0 is a fully managed application streaming service that allows users to access desktop applications from anywhere, making it the service that enabled Sandra to access her office laptop applications remotely. Here's how it works:
1.Application Hosting: AppStream 2.0 hosts desktop applications on AWS and streams them to a web browser or a connected device.
1.Secure Access: Users can access these applications securely from any location, as the service provides a secure streaming session.
1.Resource Optimization: It eliminates the need for high-end user hardware since the processing is done on AWS servers.
1.Central Management: The organization can manage applications centrally, which simplifies software updates and security.
1.Integration: AppStream 2.0 integrates with existing identity providers and supports standard security protocols.
AWS documentation on Amazon AppStream 2.0, detailing how it enables remote access to applications1.
An AWS blog post explaining the benefits of using Amazon AppStream 2.0 for remote application access2.

QUESTION 17
Alice, a cloud forensic investigator, has located, a relevant evidence during his investigation of a security breach in an organization's Azure environment. As an investigator, he needs to sync different types of logs generated by Azure resources with Azure services for better monitoring. Which Azure logging and auditing feature can enable Alice to record information on the Azure subscription layer and obtain the evidence (information related to the operations performed on a specific resource, timestamp, status of the operation, and the user responsible for it)?

A. Azure Resource Logs
B. Azure Storage Analytics Logs
C. Azure Activity Logs
D. Azure Active Directory Reports

Correct Answer: C
Section:
Explanation:
Azure Activity Logs provide a record of operations performed on resources within an Azure subscription. They are essential for monitoring and auditing purposes, as they offer detailed information on the operations, including the timestamp, status, and the identity of the user responsible for the operation.
Here's how Azure Activity Logs can be utilized by Alice:
1.Recording Operations: Azure Activity Logs record all control-plane activities, such as creating, updating, and deleting resources through Azure Resource Manager.
1.Evidence Collection: For forensic purposes, these logs are crucial as they provide evidence of the operations performed on specific resources.
1.Syncing Logs: Azure Activity Logs can be integrated with Azure services for better monitoring and can be synced with other tools for analysis.
1.Access and Management: Investigators like Alice can access these logs through the Azure portal, Azure CLI, or Azure Monitor REST API.
1.Security and Compliance: These logs are also used for security and compliance, helping organizations to meet regulatory requirements.
Microsoft Learn documentation on Azure security logging and auditing, which includes details on Azure Activity Logs1.
Azure Monitor documentation, which provides an overview of the monitoring solutions and mentions the use of Azure Activity Logs2.

QUESTION 18
Rick Warren has been working as a cloud security engineer in an IT company for the past 4 years. Owing to the robust security features and various cost-effective services offered by AWS, in 2010, his organization migrated to the AWS cloud environment. While inspecting the intrusion detection system, Rick detected a security incident. Which of the following AWS services collects logs from various data sources and stores them on a centralized location as logs files that can be used during forensic investigation in the event of a security incident?

A. Amazon CloudWatch
B. AWS CloudFormation
C. Amazon CloudFront
D. Amazon CloudTrail

Correct Answer: D
Section:
Explanation:
Amazon CloudTrail is a service that provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In the context of forensic investigation, CloudTrail plays a crucial role:
1.Event Logging: CloudTrail collects logs from various AWS services and resources, recording every API call and user activity that alters the AWS environment.
1.Centralized Storage: It aggregates the logs and stores them in a centralized location, which can be an Amazon S3 bucket.
1.Forensic Investigation: The logs stored by CloudTrail are detailed and include information about the user, the time of the API call, the source IP address, and the response elements returned by the AWS service. This makes it an invaluable tool for forensic investigations.
1.Security Monitoring: CloudTrail logs can be continuously monitored and analyzed for suspicious activity, which is essential for detecting security incidents.
1.Compliance: The service helps with compliance audits by providing a history of changes in the AWS environment.
AWS's official documentation on CloudTrail, which outlines its capabilities and use cases for security and compliance1.
An AWS blog post discussing the importance of CloudTrail logs in security incident investigations2.
A third-party article explaining how CloudTrail is used for forensic analysis in AWS environments3.

QUESTION 19
A mid-sized company uses Azure as its primary cloud provider for its infrastructure. Its cloud security analysts are responsible for monitoring security events across multiple Azure resources (subscriptions, VMs, Storage, and SQL databases) and getting threat intelligence and intelligent security analytics throughout their organization. Which Azure service would the security analysts use to achieve their goal of having a centralized view of all the security events and alerts?

A. Azure RBAC
B. Azure Monitor
C. Azure Sentinel
D. Azure CDN

Correct Answer: C
Section:
Explanation:
Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. It provides intelligent security analytics and threat intelligence across the enterprise, making it the ideal service for cloud security analysts to have a centralized view of all security events and alerts.
Here's how Azure Sentinel can be utilized:
1.Centralized Security Management: Azure Sentinel aggregates data from all Azure resources, including subscriptions, VMs, Storage, and SQL databases.
1.Threat Detection: It uses advanced analytics and the power of AI to identify threats quickly and accurately.
1.Proactive Hunting: Security analysts can proactively search for security threats using the data collected by Sentinel.
1.Automated Response: It offers automated responses to reduce the volume of alerts and improve the efficiency of security operations.
1.Integration: Sentinel integrates with various sources, not just Azure resources, providing a comprehensive security view.
Microsoft's documentation on Azure Sentinel, which details its capabilities for centralized security event monitoring and threat intelligence1.

QUESTION 20
Scott Herman works as a cloud security engineer in an IT company. His organization has deployed a 3-tier web application in the same Google Cloud Virtual Private Cloud. Each tier (web interface (UI), API, and database) is scaled independently of others. Scott Herman obtained a requirement that the network traffic should always access the database using the API and any request coming directly from the web interface to the database should not be allowed. How should Scott configure the network with minimal steps?

A. By adding tags to each tier and setting up firewall rules to allow the desired traffic flow
B. By adding tags to each tier and setting up routes to allow the desired traffic flow
C. By setting up software-based firewalls on individual VMs
D. By adding each tier to a different subnetwork

Correct Answer: A
Section:
Explanation:
In Google Cloud Virtual Private Cloud (VPC), network tags are used to apply firewall rules to specific instances. Scott can use these tags to control the traffic flow between the tiers of the web application. Here's how he can configure the network:
1.Assign Network Tags: Assign unique network tags to the instances in each tier -- for example, 'ui-tag' for the web interface, 'api-tag' for the API, and 'db-tag' for the database.
1.Create Firewall Rules: Create firewall rules that allow traffic from the API tier to the database tier by specifying the 'api-tag' as the source filter and 'db-tag' as the target filter.
1.Restrict Direct Access: Ensure that there are no rules allowing direct traffic from the 'ui-tag' to the 'db-tag', effectively blocking any direct requests from the web interface to the database.
1.Apply Rules: Apply the firewall rules to the respective instances based on their tags.
By using network tags and firewall rules, Scott can ensure that the database is only accessible via the API, and direct access from the UI is not permitted.
Google Cloud documentation on setting up firewall rules and using network tags1.

QUESTION 21
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?

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

Correct Answer: B
Section:
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:
1.Key Management: Azure Key Vault allows for the creation and control of encryption keys used to encrypt data.
1.Secrets Management: It can also manage other secrets such as tokens, passwords, certificates, and API keys.
1.Access Control: Key Vault provides secure access to keys and secrets based on Azure Active Directory identities.
1.Audit Logs: It offers monitoring and logging capabilities to track how and when keys and secrets are accessed.
1.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 22
A mid-sized company uses Azure as its primary cloud provider for its infrastructure. Its cloud security analysts are responsible for monitoring security events across multiple Azure resources (subscriptions, VMs, Storage, and SQL databases) and getting threat intelligence and intelligent security analytics throughout their organization. Which Azure service would the security analysts use to achieve their goal of having a centralized view of all the security events and alerts?

A. Azure RBAC
B. Azure Monitor
C. Azure Sentinel
D. Azure CDN

Correct Answer: C
Section:
Explanation:
Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. It provides intelligent security analytics and threat intelligence across the enterprise, making it the ideal service for cloud security analysts to have a centralized view of all security events and alerts.
Here's how Azure Sentinel can be utilized:
1.Centralized Security Management: Azure Sentinel aggregates data from all Azure resources, including subscriptions, VMs, Storage, and SQL databases.
1.Threat Detection: It uses advanced analytics and the power of AI to identify threats quickly and accurately.
1.Proactive Hunting: Security analysts can proactively search for security threats using the data collected by Sentinel.
1.Automated Response: It offers automated responses to reduce the volume of alerts and improve the efficiency of security operations.
1.Integration: Sentinel integrates with various sources, not just Azure resources, providing a comprehensive security view.
Microsoft's documentation on Azure Sentinel, which details its capabilities for centralized security event monitoring and threat intelligence1.

QUESTION 23
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?

A. Tier III

B. Tier I
C. Tier IV
D. Tier II

Correct Answer: B
Section:
Explanation:

Explore
The data center designed and constructed by Katie Holmes' team is a Tier I data center based on the description provided.
1.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.
1.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.
1.Operational Aspects:
oUptime: A Tier I data center typically has an uptime of 99.671%.
oMaintenance: 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 24
Sandra Oliver has been working as a cloud security engineer in an MNC. Her organization adopted the Microsoft Azure cloud environment owing to its on-demand scalability, robust security, and high availability features. Sandra's team leader assigned her the task to increase the availability of organizational applications; therefore, Sandra is looking for a solution that can be utilized for distributing the traffic to backend Azure virtual machines based on the attributes of the HTTP request received from clients. Which of the following Azure services fulfills Sarah's requirements?

A. Azure Application Gateway
B. Azure Sentinel
C. Azure ExpressRoute
D. Azure Front Door

Correct Answer: A
Section:
Explanation:
Azure Application Gateway is a web traffic load balancer that enables Sandra to manage traffic to her web applications. It is designed to distribute traffic to backend virtual machines and services based on various HTTP request attributes.
Here's how Azure Application Gateway meets the requirements:
1.Routing Based on HTTP Attributes: Application Gateway can route traffic based on URL path or host headers.
1.SSL Termination: It provides SSL termination at the gateway, reducing the SSL overhead on the web servers.
1.Web Application Firewall: Application Gateway includes a Web Application Firewall (WAF) that provides protection to web applications from common web vulnerabilities and exploits.
1.Session Affinity: It can maintain session affinity, which is useful when user sessions need to be directed to the same server.
1.Scalability and High Availability: Application Gateway supports autoscaling and zone redundancy, ensuring high availability and scalability.

Azure's official documentation on Application Gateway, which details its capabilities for routing traffic based on HTTP request attributes1.

QUESTION 25
An AWS customer was targeted with a series of HTTPS DDoS attacks, believed to be the largest layer 7 DDoS reported to date. Starting around 10 AM ET on March 1, 2023, more than 15,500 requests per second (rps) began targeting the AWS customer's load balancer. After 10 min, the number of requests increased to 2,50,000 rps.
This attack resembled receiving the entire daily traffic in only 10s. An AWS service was used to sense and mitigate this DDoS attack as well as prevent bad bots and application vulnerabilities. Identify which of the following AWS services can accomplish this.

A. AWS Amazon Direct Connect
B. Amazon CloudFront
C. AWS Shield Standard
D. AWS EBS

Correct Answer: C
Section:
Explanation:
AWS Shield Standard is a managed Distributed Denial of Service (DDoS) protection service that is automatically included with AWS services such as Amazon CloudFront and Elastic Load Balancing (ELB). It provides protection against common, most frequently occurring network and transport layer DDoS attacks.
Here's how AWS Shield Standard works to mitigate such attacks:
1.Automatic Protection: AWS Shield Standard provides always-on detection and automatic inline mitigations that minimize application downtime and latency.
1.Layer 7 Protection: It offers protection against layer 7 DDoS attacks, which target the application layer and are typically more complex than infrastructure attacks.
1.Integration with AWS Services: Shield Standard is integrated with other AWS services like ELB and CloudFront, providing a seamless defense mechanism.
1.Real-Time Visibility: Customers get real-time visibility into attacks via AWS Management Console and CloudWatch.
1.Cost-Effectiveness: There is no additional charge for AWS Shield Standard; it comes included with AWS services, making it a cost-effective solution for DDoS protection.
AWS Shield's official page detailing how it provides managed DDoS protection1.
AWS documentation on best practices for DDoS resiliency, mentioning AWS Shield's role in mitigation2.

QUESTION 26
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

Correct Answer: A
Section:
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:
1.Cloud Production Environment: The primary production application runs in the cloud, taking advantage of the cloud's scalability and flexibility.
1.On-Premises Recovery: The disaster recovery site is located in the organization's private data center, not in the cloud.
1.Data Replication: Data is replicated from the cloud to the on-premises data center to ensure that the backup is up-to-date.
1.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.
1.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.
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.

QUESTION 27
Dustin Hoffman works as a cloud security engineer in a healthcare company. His organization uses AWS cloud- based services. Dustin would like to view the security alerts and security posture across his organization's AWS account. Which AWS service can provide aggregated, organized, and prioritized security alerts from AWS services such as GuardDuty, Inspector, Macie, IAM Analyzer, Systems Manager, Firewall Manager, and AWS Partner Network to Dustin?

A. AWS Config
B. AWS CloudTrail
C. AWS Security Hub
D. AWS CloudFormation

Correct Answer: C
Section:
Explanation:
AWS Security Hub is designed to provide users with a comprehensive view of their security state within AWS and help them check their environment against security industry standards and best practices.
Here's how AWS Security Hub serves Dustin's needs:
1.Aggregated View: Security Hub aggregates security alerts and findings from various AWS services such as GuardDuty, Inspector, and Macie.
1.Organized Data: It organizes and prioritizes these findings to help identify and focus on the most important security issues.
1.Security Posture: Security Hub provides a comprehensive view of the security posture of AWS accounts, helping to understand the current state of security and compliance.
1.Automated Compliance Checks: It performs automated compliance checks based on standards and best practices, such as the Center for Internet Security (CIS) AWS Foundations Benchmark.
1.Integration with AWS Services: Security Hub integrates with other AWS services and partner solutions, providing a centralized place to manage security alerts and automate responses.
AWS's official documentation on Security Hub, which outlines its capabilities for managing security alerts and improving security posture.
An AWS blog post discussing how Security Hub can be used to centralize and prioritize security findings across an AWS environment.

QUESTION 28
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?

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

Correct Answer: B
Section:
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:
1.Create Snapshot: First, a snapshot of the VM's disk is created to capture the state of the VM at the point of compromise.
1.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.
1.Maintain Integrity: This step ensures that the original snapshot remains unaltered and can be used as evidence, maintaining the chain of custody.
1.Forensic Analysis: After the backup copy is secured, the snapshot can be mounted onto the forensic workstation for detailed analysis.
1.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 29
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?

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

Correct Answer: D
Section:
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.
1.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.
1.Quick Activation: In the event of a disaster, the warm standby environment can be quickly scaled up to handle the full production load12.
1.RTO and RPO: The warm standby approach is designed to achieve an RTO and RPO within minutes, which is essential for business-critical functions12.
1.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 30
You are the manager of a cloud-based security platform that offers critical services to government agencies and private companies. One morning, your team receives an alert from the platform's intrusion detection system indicating that there has been a potential breach in the system. As the manager, which tool you will use for viewing and monitoring the sensitive data by scanning storage systems and reviewing the access rights to critical resources via a single centralized dashboard?

A. Google Cloud Security Command Center
B. Google Cloud Security Scanner
C. Cloud Identity and Access Management (IAM)
D. Google Cloud Armor

Correct Answer: A
Section:
Explanation:
The Google Cloud Security Command Center (Cloud SCC) is the tool designed to provide a centralized dashboard for viewing and monitoring sensitive data, scanning storage systems, and reviewing access rights to critical resources.
1.Centralized Dashboard: Cloud SCC offers a comprehensive view of the security status of your resources in Google Cloud, across all your projects and services1.
1.Sensitive Data Scanning: It has capabilities for scanning storage systems to identify sensitive data, such as personally identifiable information (PII), and can provide insights into where this data is stored1.
1.Access Rights Review: Cloud SCC allows you to review who has access to your critical resources and whether any policies or permissions should be adjusted to enhance security1.
1.Alerts and Incident Response: In the event of a potential breach, Cloud SCC can help identify the affected resources and assist in the investigation and response process1.
Reference: Google Cloud Security Command Center is a security management and data risk platform for Google Cloud that helps you prevent, detect, and respond to threats from a single pane of glass. It provides security insights and features like asset inventory, discovery, search, and management; vulnerability and threat detection; and compliance monitoring to protect your services and applications on Google Cloud1.

QUESTION 31
An organization, PARADIGM PlayStation, moved its infrastructure to a cloud as a security practice. It established an incident response team to monitor the hosted websites for security issues. While examining network access logs using SIEM, the incident response team came across some incidents that suggested that one of their websites was targeted by attackers and they successfully performed an SQL injection attack.
Subsequently, the incident response team made the website and database server offline. In which of the following steps of the incident response lifecycle, the incident team determined to make that decision?

A. Analysis
B. Containment

C. Coordination and information sharing
D. Post-mortem

Correct Answer: B
Section:
Explanation:
The decision to take the website and database server offline falls under the Containment phase of the incident response lifecycle. Here's how the process typically unfolds:
1.Detection: The incident response team detects a potential security breach, such as an SQL injection attack, through network access logs using SIEM.
1.Analysis: The team analyzes the incident to confirm the breach and understand its scope and impact.
1.Containment: Once confirmed, the team moves to contain the incident to prevent further damage. This includes making the affected website and database server offline to stop the attack from spreading or causing more harm1.
1.Eradication and Recovery: After containment, the team works on eradicating the threat and recovering the systems to normal operation.
1.Post-Incident Activity: Finally, the team conducts a post-mortem analysis to learn from the incident and improve future response efforts.
Reference: The containment phase is critical in incident response as it aims to limit the damage of the security incident and isolate affected systems to prevent the spread of the attack12. Taking systems offline is a common containment strategy to ensure that attackers can no longer access the compromised systems1.

QUESTION 32
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

Correct Answer: A
Section:
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.
1.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.
1.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.
1.NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
1.AWS Cloud Security Best Practices
1.Azure Security Documentation

QUESTION 33
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

Correct Answer: B
Section:
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.
1.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.
1.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.
1.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.
1.Microsoft Azure Documentation on Shared Access Signatures (SAS)
1.Azure Security Best Practices and Patterns
1.Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing

QUESTION 34
SecureSoftWorld Pvt. Ltd. is an IT company that develops software solutions catering to the needs of the healthcare industry. Most of its services are hosted in Google cloud. In the cloud environment, to secure the applications and services, the organization uses Google App Engine Firewall that controls the access to the App Engine with a set of rules that denies or allows requests from a specified range of IPs. How many unique firewall rules can SecureSoftWorld Pvt. Ltd define using App Engine Firewall?

A. Up to 10000
B. Up to 1000
C. Up to 10
D. Up to 100

Correct Answer: B
Section:
Explanation:
Google App Engine Firewall allows organizations to create a set of rules that control the access to their App Engine applications. These rules can either allow or deny requests from specified IP ranges, providing a robust mechanism for securing applications and services hosted on the Google Cloud.
Here's how the rule limit applies to SecureSoftWorld Pvt. Ltd:
1.Rule Creation: SecureSoftWorld Pvt. Ltd can create firewall rules that specify which IP ranges are allowed or denied access to their App Engine services.
1.Rule Limit: The company can define up to 1000 individual firewall rules1.
1.Rule Priority: These rules are prioritized, meaning that rules with a lower priority number are evaluated before those with a higher number.
1.Default Rule: By default, any request that does not match a specific rule is allowed. However, this default action can be changed to deny, effectively blocking all traffic that does not match any of the defined rules.
1.Rule Management: The rules can be managed via the Google Cloud Console, the gcloud command-line tool, or the App Engine Admin API.
Google Cloud documentation explaining the App Engine firewall and the maximum number of rules1.

QUESTION 35
A new public web application is deployed on AWS that will run behind an Application Load Balancer (ALB). An AWS security expert needs to encrypt the newly deployed application at the edge with an SSL/TLS certificate issued by an external certificate authority. In addition, he needs to ensure the rotation of the certificate yearly before it expires. Which of the following AWS services can be used to accomplish this?

A. AWS Snowball
B. AWS Certificate Manager
C. AWS Cloud HSM
D. Amazon Elastic Load Balancer

Correct Answer: B

Section:
Explanation:
AWS Certificate Manager (ACM) is the service that enables an AWS security expert to manage SSL/TLS certificates provided by AWS or an external certificate authority. It allows the deployment of the certificate on AWS services such as an Application Load Balancer (ALB) and also handles the renewal and rotation of certificates.
Here's how ACM would be used for the web application:
1.Certificate Provisioning: The security expert can import an SSL/TLS certificate issued by an external certificate authority into ACM.
1.Integration with ALB: ACM integrates with ALB, allowing the certificate to be easily deployed to encrypt the application at the edge.
1.Automatic Renewal: ACM can be configured to automatically renew certificates provided by AWS. For certificates from external authorities, the expert can manually import a new certificate before the old one expires.
1.Yearly Rotation: While ACM does not automatically rotate externally provided certificates, it simplifies the process of replacing them by allowing the expert to import new certificates as needed.
AWS documentation on ACM, which explains how to import certificates and use them with ALB1.
AWS blog post discussing the importance of rotating SSL/TLS certificates and how ACM facilitates this process2.

QUESTION 36
A BPO company would like to expand its business and provide 24 x 7 customer service. Therefore, the organization wants to migrate to a fully functional cloud environment that provides all features with minimum maintenance and administration. Which cloud service model should it consider?

A. laaS
B. PaaS
C. RaaS
D. SaaS

Correct Answer: D
Section:
Explanation:
SaaS, or Software as a Service, is the ideal cloud service model for a BPO company looking to expand its business and provide 24/7 customer service with minimal maintenance and administration. SaaS provides a complete software solution that is managed by the service provider and delivered over the internet, which aligns with the needs of a BPO company for several reasons:
1.Fully Managed Service: SaaS offers a fully managed service, which means the provider is responsible for the maintenance, updates, and security of the software.
1.Accessibility: It allows employees to access the software from anywhere at any time, which is essential for 24/7 customer service operations.
1.Scalability: SaaS solutions are highly scalable, allowing the BPO company to easily adjust its usage based on business demands without worrying about infrastructure limitations.
1.Cost-Effectiveness: With SaaS, the BPO company can avoid upfront costs associated with purchasing, managing, and upgrading hardware and software.
1.Integration and Customization: Many SaaS offerings provide options for integration with other services and customization to meet specific business needs.
An article discussing how cloud computing services are becoming the new BPO style, highlighting the benefits of SaaS for BPO companies1.
A report on the impact of cloud services on BPOs, emphasizing the advantages of SaaS in terms of cost savings and quick response to customers1.

QUESTION 37
Thomas Gibson is a cloud security engineer who works in a multinational company. His organization wants to host critical elements of its applications; thus, if disaster strikes, applications can be restored quickly and completely. Moreover, his organization wants to achieve lower RTO and RPO values. Which of the following disaster recovery approach should be adopted by Thomas' organization?

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

Correct Answer: A
Section:
Explanation:
The Warm Standby approach in disaster recovery is designed to achieve lower Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) values. This approach involves having a scaled-down version of a fully functional environment running at all times in the cloud. In the event of a disaster, the system can quickly switch over to the warm standby environment, which is already running and up-to-date, thus ensuring a quick and complete restoration of applications.

Here's how the Warm Standby approach works:
1.Prepared Environment: A duplicate of the production environment is running in the cloud, but at a reduced capacity.
1.Quick Activation: In case of a disaster, this environment can be quickly scaled up to handle the full production load.
1.Data Synchronization: Regular data synchronization ensures that the standby environment is always up-to-date, which contributes to a low RPO.
1.Reduced Downtime: Because the standby system is always running, the time to switch over is minimal, leading to a low RTO.
1.Cost-Efficiency: While more expensive than a cold standby, it is more cost-effective than a hot standby, balancing cost with readiness.
An article discussing the importance of RPO and RTO in disaster recovery and how different strategies, including Warm Standby, impact these metrics1.
A guide explaining various disaster recovery strategies, including Warm Standby, and their relation to achieving lower RTO and RPO values2.

QUESTION 38
Falcon Computers is an IT company that runs its IT infrastructure on the cloud. The organization must implement cloud governance in its corporate cloud environment to align its business vision with the cloud vision. Which of the following cloud governance components can help the organization to align the cloud vision and business vision?

A. Cloud center of excellence
B. Norms, models, reference architectures, best practices, guidelines, and policies
C. Processes for the cloud service lifecycle
D. Cloud business office

Correct Answer: A
Section:
Explanation:
1.Cloud Governance Framework: Cloud governance is a framework designed to ensure data security, system integration, and the deployment of cloud computing are properly managed1.
1.Alignment with Business Vision: The framework helps align cloud operations with business goals, which is essential for Falcon Computers to integrate its IT infrastructure with its business vision1.
1.Cloud Center of Excellence (CCoE): A CCoE is a cross-functional team that leads the cloud strategy, governance, and best practices in an organization and ensures that cloud services align with business objectives1.
1.Role of CCoE: The CCoE provides leadership, best practices, research, support, and training for all aspects of cloud computing. It helps to align cloud initiatives with business strategies, manage risks, and drive cloud adoption across the enterprise1.
1.Benefits: Implementing a CCoE can improve management of resources, enhance cloud security, help curb shadow IT, and reduce administrative overhead1.
CrowdStrike's article on Cloud Governance1.

QUESTION 39
An organization wants to implement a zero-trust access model for its SaaS application on the GCP as well as its on-premises applications. Which of the following GCP services can be used to eliminate the need for setting up a company-wide VPN and implement the RBAC feature to verify employee identities to access organizational applications?

A. Cloud Endpoints
B. Identity-Aware Proxy (IAP)
C. Cloud Security Scanner
D. Web Application and API Protection

Correct Answer: B
Section:
Explanation:
1.Zero Trust Access Model: The zero-trust model is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access1.
1.Eliminating VPNs: The zero-trust model can be implemented without the need for traditional VPNs by using cloud services that verify user identities and device security status before granting access to applications1.
1.Identity-Aware Proxy (IAP): Google Cloud's IAP enables the control of access to applications running on GCP, GKE, and on-premises, based on identity and context of the request (such as the user's identity, device security status, and IP address)1.
1.Role-Based Access Control (RBAC): IAP supports RBAC, which allows organizations to enforce granular access controls based on roles assigned to users within the organization2.
1.Benefits of IAP: By using IAP, organizations can secure their applications by ensuring that only authenticated and authorized users are able to access them. IAP works as a building block for a zero-trust approach on GCP1.
Google Cloud's explanation of applying zero trust to user access and production services1.

Google Cloud's documentation on Role-Based Access Control (RBAC)2.

QUESTION 40
An organization uses AWS for its operations. It is observed that the organization's EC2 instance is communicating with a suspicious port. Forensic investigators need to understand the patterns of the current security breach. Which log source on the AWS platform can provide investigators with data of evidentiary value during their investigation?

A. Amazon CloudTrail
B. Amazon CloudWatch
C. Amazon VPC flow logs
D. S3 Server Access Logs

Correct Answer: C
Section:
Explanation:
1.Understanding the Incident: When an EC2 instance communicates with a suspicious port, it's crucial to analyze network traffic to understand the patterns of the security breach1.
1.Log Sources for Forensic Investigation: AWS provides several log sources that can be used for forensic investigations, including AWS CloudTrail, AWS Config, VPC Flow Logs, and host-level logs1.
1.Amazon VPC Flow Logs: These logs capture information about the IP traffic going to and from network interfaces in a Virtual Private Cloud (VPC). They are particularly useful for understanding network-level interactions, which is essential in this case1.
1.Evidentiary Value: VPC flow logs can provide data with evidentiary value, showing the source, destination, and protocol used in the network traffic, which can help investigators identify patterns related to the security breach1.
1.Other Log Sources: While Amazon CloudTrail and Amazon CloudWatch provide valuable information on user activities and metrics, respectively, they do not offer the detailed network traffic insights needed for this specific forensic investigation1.
AWS Security Incident Response Guide's section on Forensics on AWS1.

QUESTION 41
Cindy Williams has been working as a cloud security engineer in an IT company situated in Austin, Texas. Owing to the robust security and cost-effective features provided by AWS, her organization adopted AWS cloud-based services. Cindy has deployed an application in the Amazon Elastic Compute Cloud (EC2) instance.
Which of the following cloud computing service model does the Amazon EC2 instance represent?

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

Correct Answer: B
Section:
Explanation:

Explore
1.Cloud Service Models: There are three primary cloud service models, which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)1.
1.Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It allows users to run virtual servers and manage storage, security, and networking1.
1.IaaS Definition: IaaS provides virtualized computing resources over the internet. In an IaaS model, a cloud provider hosts the infrastructure components traditionally present in an on-premises data center, including servers, storage, and networking hardware1.
1.EC2 as IaaS: Amazon EC2 falls under the IaaS category because it provides the hardware infrastructure, allows users to scale computing capacity up or down, and users pay only for the capacity they use1.
1.Exclusion of Other Models: EC2 is not PaaS because it does not provide a platform for developing, running, or managing applications. It's not SaaS as it doesn't deliver software over the internet. DaaS, or Desktop as a Service, provides virtual desktops, which is not the service EC2 offers1.
AWS's official documentation on Amazon EC21.

QUESTION 42
A multinational company decided to shift its organizational infrastructure and data to the cloud. Their team finalized the service provider. Which of the following is a contract that can define the security standards agreed upon by the service provider to maintain the security of the organizational data and infrastructure and define organizational data compliance?

A. Service Agreement
B. Service Level Agreement
C. Service Level Contract
D. Compliance Agreement

Correct Answer: B
Section:
Explanation:
1.Service Level Agreement (SLA): An SLA is a contract between a service provider and the customer that specifies, usually in measurable terms, what services the service provider will furnish1.
1.Security Standards in SLAs: SLAs often include security standards that the service provider agrees to maintain. This can cover various aspects such as data encryption, access controls, and incident response times1.
1.Data Compliance: The SLA can also define compliance with relevant regulations and standards, ensuring that the service provider adheres to laws such as GDPR, HIPAA, or industry-specific guidelines2.
1.Alignment with Business Needs: By clearly stating the security measures and compliance standards, an SLA helps ensure that the cloud services align with the multinational company's business needs and regulatory requirements1.
1.Other Options: While service agreements and contracts may contain similar terms, the term ''Service Level Agreement'' is specifically used in the context of IT services to define performance and quality metrics, making it the most appropriate choice for defining security standards and compliance in cloud services1.
DigitalOcean's article on Cloud Compliance1.
CrowdStrike's guide on Cloud Compliance2.

QUESTION 43
Bruce McFee works as a cloud security engineer in an IT company. His organization uses AWS cloud-based services. Because Amazon CloudFront offers low-latency and high-speed data delivery through a user-friendly environment, Bruce's organization uses the CloudFront content delivery network (CDN) web service for the fast and secure distribution of data to various customers throughout the world. How does CloudFront accelerate content distribution?

A. By sending the requests of end users to the nearest edge locations
B. By restricting the requests of end users from the nearest edge locations

C. By routing the requests of end users to the original source
D. By forwarding the requests of end users to the original source

Correct Answer: A
Section:
Explanation:

Explore
1.Content Delivery Network (CDN): Amazon CloudFront is a CDN that accelerates the delivery of content by caching it at edge locations that are closer to the end-users1.
1.Edge Locations: These are data centers located around the world that store cached copies of content so that it can be delivered more quickly to users1.
1.Low Latency: When a user requests content, DNS routes the request to the CloudFront Point of Presence (POP) that can best serve the request, typically the nearest CloudFront POP in terms of latency1.
1.Cache Check: CloudFront checks its cache for the requested object. If the object is in the cache, CloudFront returns it to the user1.
1.Cache Miss: If the object is not in the cache, CloudFront forwards the request to the origin server for the object, and then the origin server sends the object back to the edge location. As soon as the first byte arrives from the origin, CloudFront begins to forward the object to the user and adds it to the cache for the next time someone requests it1.
Amazon's official documentation on how CloudFront delivers content1.

QUESTION 44
Jordon Bridges has been working as a senior cloud security engineer in a multinational company. His organization uses Google cloud-based services. Jordon stored his organizational data in the bucket and named the bucket in the Google cloud storage following the guidelines for bucket naming. Which of the following is a valid bucket name given by Jordon?

A. company-storage-data
B. Company-storage-data
C. Company-Storage-Data
D. company storage data

Correct Answer: A
Section:
Explanation:
1.Bucket Naming Guidelines: Google Cloud Storage requires that bucket names must be unique, contain only lowercase letters, numbers, dashes (-), underscores (_), and dots (.), and start and end with a number or letter1.
1.Valid Bucket Name: Based on these guidelines, the valid bucket name from the options provided is 'company-storage-data' because it only contains lowercase letters, numbers, and dashes1.
1.Invalid Bucket Names: The other options are invalid because:

oOption B and C contain uppercase letters, which are not allowed1.
oOption D contains spaces, which are also not allowed1.
Google Cloud's documentation on bucket naming guidelines1.

QUESTION 45
IntSecureSoft Solutions Pvt. Ltd. is an IT company that develops software and applications for various educational institutions. The organization has been using Google cloud services for the past 10 years. Tara Reid works as a cloud security engineer in IntSecureSoft Solutions Pvt. Ltd. She would like to identify various misconfigurations and vulnerabilities such as open storage buckets, instances that have not implemented SSL, and resources without an enabled Web UI. Which of the following is a native scanner in the Security Command Center that assesses the overall security state and activity of virtual machines, containers, network, and storage along with the identity and access management policies?

A. Log Analytics Workspace
B. Google Front End
C. Security Health Analytics
D. Synapse Analytics

Correct Answer: C
Section:
Explanation:
1.Security Command Center: Google Cloud's Security Command Center is designed to provide centralized visibility into the security state of cloud resources1.
1.Native Scanners: It includes native scanners that assess the security state of virtual machines, containers, networks, and storage, along with identity and access management policies1.
1.Security Health Analytics: Security Health Analytics is a native scanner within the Security Command Center. It automatically scans your Google Cloud resources to help identify misconfigurations and compliance issues with Google security best practices2.
1.Functionality: Security Health Analytics can detect various misconfigurations and vulnerabilities, such as open storage buckets, instances without SSL/TLS, and resources without an enabled Web UI, which aligns with Tara Reid's requirements2.
1.Exclusion of Other Options: The other options listed do not serve as native scanners within the Security Command Center for the purposes described in the question1.
Google Cloud's documentation on Security Command Center1.
Medium article on Google Cloud's free vulnerability scanning with Security Command Center2.

QUESTION 46
Samuel Jackson has been working as a cloud security engineer for the past 12 years in VolkSec Pvt. Ltd., whose applications are hosted in a private cloud. Owing to the increased number of users for its services, the organizations is finding it difficult to manage the on-premises data center. To overcome scalability and data storage issues, Samuel advised the management of his organization to migrate to a public cloud and shift the applications and data. Once the suggestion to migrate to public cloud was accepted by the management, Samuel was asked to select a cloud service provider. After extensive research on the available public cloud service providers, Samuel made his recommendation. Within a short period, Samuel along with his team successfully transferred all applications and data to the public cloud. Samuel's team would like to configure and maintain the platform, infrastructure, and applications in the new cloud computing environment. Which component of a cloud platform and infrastructure provides tools and interfaces to Samuel's team for configuring and maintaining the platform, infrastructure, and application?

A. Physical and Environment Component
B. Compute Component
C. Management Component
D. Virtualization Component

Correct Answer: C
Section:
Explanation:
1.Cloud Platform Components: Cloud platforms typically consist of several components, including compute, storage, networking, virtualization, and management1.
1.Management Component: The management component of a cloud platform provides the necessary tools and interfaces for configuring and maintaining the platform, infrastructure, and applications2.
1.Tools and Interfaces: These tools and interfaces allow cloud security engineers like Samuel and his team to manage resource allocation, monitor system performance, configure network settings, and ensure security compliance2.
1.Role in Cloud Environments: In cloud environments, the management component is crucial for maintaining operational efficiency, ensuring that resources are used optimally, and that the cloud infrastructure aligns with

organizational goals2.
1.Exclusion of Other Components: While the physical and environment component, compute component, and virtualization component are essential parts of cloud infrastructure, they do not primarily provide tools for configuration and maintenance. The management component is specifically designed for this purpose1.
IBM's explanation of cloud service models1.
AWS's overview of the cloud adoption framework2.

QUESTION 47
Andrew Gerrard has been working as a cloud security engineer in an MNC for the past 3 years. His organization uses cloud-based services and it has implemented a DR plan. Andrew wants to ensure that the DR plan works efficiently and his organization can recover and continue with its normal operation when a disaster strikes.
Therefore, the owner of the DR plan, Andrew, and other team members involved in the development and implementation of the DR plan examined it to determine the inconsistencies and missing elements. Based on the given scenario, which of the following type of DR testing was performed in Andrew's organization?

A. Plan Review
B. Simulation
C. Stimulation
D. Table-top exercise

Correct Answer: A
Section:
Explanation:
1.Disaster Recovery (DR) Testing: DR testing is a critical component of a disaster recovery plan (DRP). It ensures that the plan is effective and can be executed in the event of a disaster1.
1.Plan Review: A plan review is a type of DR testing where stakeholders involved in the development and implementation of the DRP closely examine the plan to identify any inconsistencies or missing elements1.
1.Purpose of Plan Review: The goal of a plan review is to ensure that the DRP is comprehensive, up-to-date, and capable of being implemented as intended. It involves a thorough examination of the plan's components1.
1.Scenario in Question : In the scenario described, Andrew Gerrard and his team are reviewing their DRP to determine inconsistencies and missing elements. This aligns with the activities involved in a plan review1.
1.Exclusion of Other Options: While simulation tests and table-top exercises are also types of DR testing, they involve more active testing of the DRP's procedures. Since the scenario specifically mentions examining the plan for inconsistencies and missing elements, it indicates a plan review rather than a simulation or exercise1.
LayerLogix's article on Disaster Recovery Testing in 20231.

QUESTION 48
A cloud organization, AZS, wants to maintain homogeneity in its cloud operations because the CPU speed measured by AZS varies and the measurement units lack consistency in the standards. For example, AWS defines the CPU speed with Elastic Compute Unit, Google with Google Compute Engine Unit, and Microsoft with clock speed. Here, which cloud computing standard can leverage frameworks and architectures specific to the cloud for maintaining homogeneity in operations?

A. occ
B. DMTF
C. NIST
D. CSA

Correct Answer: C
Section:
Explanation:

Explore
1.Cloud Computing Standards: Cloud computing standards are essential for ensuring consistency and interoperability among different cloud service providers1.
1.Homogeneity in Operations: Maintaining homogeneity in operations across various cloud platforms requires a standard that provides frameworks and architectures specific to cloud computing1.
1.NIST's Role: The National Institute of Standards and Technology (NIST) has developed a cloud computing standards roadmap that includes frameworks and architectures for cloud computing. This roadmap aims to promote cloud computing standards and ensure homogeneity in operations1.
1.CPU Speed Measurement: NIST's standards can help organizations like AZS to have a consistent approach to measuring CPU speed across different cloud providers, despite the different units of measurement used by AWS, Google, and Microsoft1.
1.Exclusion of Other Options: While other organizations like DMTF and CSA contribute to cloud standards, NIST is specifically recognized for its work in creating a comprehensive framework that addresses the need for homogeneity in cloud operations1.
NIST Cloud Computing Standards Roadmap1.

QUESTION 49
Trevor Holmes works as a cloud security engineer in a multinational company. Approximately 7 years ago, his organization migrated its workload and data to the AWS cloud environment. Trevor would like to monitor malicious activities in the cloud environment and protect his organization's AWS account, data, and workloads from unauthorized access. Which of the following Amazon detection services uses anomaly detection, machine learning, and integrated threat intelligence to identify and classify threats and provide actionable insights that include the affected resources, attacker IP address, and geolocation?

A. Amazon Inspector
B. Amazon GuardDuty
C. Amazon Macie
D. Amazon Security Hub

Correct Answer: B
Section:
Explanation:
1.Amazon GuardDuty: It is a threat detection service that continuously monitors for malicious activity and unauthorized behavior across your AWS accounts and workloads1.
1.Anomaly Detection: GuardDuty uses anomaly detection to monitor for unusual behavior that may indicate a threat1.
1.Machine Learning: It employs machine learning to better identify threat patterns and reduce false positives1.
1.Integrated Threat Intelligence: The service utilizes threat intelligence feeds from AWS and leading third parties to identify known threats1.
1.Actionable Insights: GuardDuty provides detailed findings that include information about the nature of the threat, the affected resources, the attacker's IP address, and geolocation1.
1.Protection Scope: It protects against a wide range of threats, including compromised instances, reconnaissance by attackers, account compromise risks, and instance compromise risks1.
AWS's official documentation on Amazon GuardDuty1.

QUESTION 50
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?

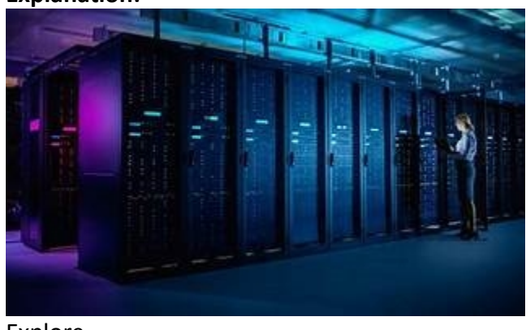
A. Cloud Auditor
B. Cloud Carrier

C. Cloud Provider
D. Cloud Broker

Correct Answer: D
Section:
Explanation:
1.Cloud Service Integration: As cloud services become more complex, organizations like Melissa George's may require assistance in managing and integrating these services1.
1.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.
1.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.
1.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.
1.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.
GeeksforGeeks article on Cloud Stakeholders as per NIST1.

QUESTION 51
Rachel McAdams works as a senior cloud security engineer in a cloud service provider company. Owing to the robust services and security features provided by her organization, the number of cloud consumers continues to increase. To mee the increasing cloud consumer requirements, her organization decided to build more data centers. Therefore, Rachel's organization formed a new team to design and construct data centers. Rachel is also part of the team and was given the responsibility of designing the data center. How can Racheal maintain a stable temperature in the HVAC unit?

A. Rachel can design HVAC such that the heat generated by the data center equipment is taken outside and cool air to supply the equipment is taken inside
B. Rachel can design HVAC such that the cool air and heat generated by data center equipment should remain outside to stabilize the temperature
C. Rachel can design HVAC such that the cool air and heat generated by data center equipment should remain inside to stabilize the temperature
D. Rachel can design HVAC such that the heat generated by the data center equipment is taken inside and cool air to supply the equipment is taken outside

Correct Answer: A
Section:
Explanation:

Explore
1.HVAC Function: The primary function of an HVAC (Heating, Ventilation, and Air Conditioning) system in a data center is to remove the excess heat generated by the equipment to prevent overheating1.
1.Heat Removal: The HVAC system should be designed to take the heat generated by the data center equipment outside. This is typically achieved through a combination of air conditioning and ventilation systems1.
1.Cool Air Supply: Simultaneously, the system must supply cool air inside to maintain the equipment at optimal operating temperatures. This is often done using chilled water systems, air conditioners, and controlled airflow management1.
1.Temperature Stability: Maintaining a stable temperature within the recommended range is crucial for the longevity and reliability of data center equipment. The American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) recommends keeping data center temperatures between 64 and 81 degrees Fahrenheit2.
1.Design Considerations: Rachel should consider the layout of the data center, the heat output of the equipment, and the local climate to design an HVAC system that effectively manages the temperature1.
Uptime Institute Blog on Data Center Cooling Best Practices1.
CED Engineering on HVAC Cooling Systems for Data Centers3.
Tate's blog on How Temperatures Affect Data Centers2.

QUESTION 52
AWS runs 35+ instances that are all CentOS machines. Updating these machines manually is a time-intensive task that may lead to missed updates for some instances and create vulnerabilities. Which of the following can be used to prevent each port of each instance from being opened to access the machine and install updates?

A. AWS Security Hub
B. AWS Systems Manager
C. Amazon Glacier
D. Amazon Snowball

Correct Answer: B
Section:

QUESTION 53
AWS runs 35+ instances that are all CentOS machines. Updating these machines manually is a time-intensive task that may lead to missed updates for some instances and create vulnerabilities. Which of the following can be used to prevent each port of each instance from being opened to access the machine and install updates?

A. AWS Security Hub
B. AWS Systems Manager
C. Amazon Glacier
D. Amazon Snowball

Correct Answer: B
Section:

QUESTION 54
The organization TechWorld Ltd. used cloud for its business. It operates from an EU country (Poland and Greece). Currently, the organization gathers and processes the data of only EU users. Once, the organization experienced a severe security breach, resulting in loss of critical user data. In such a case, along with its cloud service provider, the organization should be held responsible for non-compliance or breaches. Under which cloud compliance framework will the company and cloud provider be penalized?

A. GDPR
B. NIST
C. ITAR
D. HIPAA

Correct Answer: A
Section:
Explanation:
1.GDPR: The General Data Protection Regulation (GDPR) is the primary law regulating how companies protect EU citizens' personal data1.
1.Applicability: GDPR applies to all organizations operating within the EU, as well as organizations outside of the EU that offer goods or services to customers or businesses in the EU1.
1.Data Breaches: In the event of a data breach, organizations are required to notify the appropriate data protection authority within 72 hours, if feasible, after becoming aware of the breach2.
1.Penalties: Organizations that do not comply with GDPR can face hefty fines. For serious infringements, GDPR states that companies can be fined up to 4% of their annual global turnover or 20 million (whichever is greater)1.
1.Responsibility: Both the data controller and the processor will be held responsible for not adhering to the GDPR rules, which includes security breaches resulting in the loss of user data1.
GDPR Info on fines and penalties1.
EDPB Guidelines on personal data breach notification under GDPR2.

QUESTION 55
On database system of a hospital maintains rarely-accessed patients' data such as medical records including high-resolution images of ultrasound reports, MRI scans, and X-Ray reports for years. These records occupy a lot of space and need to be kept safe as it contains sensitive medical data. Which of the following Azure storage services best suitable for such rarely-accessed data with flexible latency requirement?

A. Azure Backup: Restore-as-a-Service
B. Azure File Sync
C. Azure Archive Storage
D. Azure Recovery Services Vault

Correct Answer: C
Section:
Explanation:
1.Data Characteristics: The hospital's database system contains rarely-accessed, sensitive medical records, including high-resolution images, which require secure and cost-effective long-term storage1.
1.Azure Archive Storage: Azure Archive Storage is designed for data that is rarely accessed and has flexible latency requirements. It offers a cost-effective solution for storing large volumes of data that does not need to be accessed frequently1.
1.Security and Compliance: Azure Archive Storage provides secure storage for sensitive medical data, ensuring compliance with healthcare regulations such as HIPAA and GDPR1.
1.Cost Efficiency: By using Azure Archive Storage, the hospital can significantly reduce storage costs compared to storing data on higher-performance tiers that are intended for frequently accessed data1.
1.Exclusion of Other Options: Azure Backup and Azure Recovery Services Vault are primarily used for backup and disaster recovery, not for archiving. Azure File Sync is used for syncing files across multiple locations and is not optimized for archival purposes1.
Microsoft Azure's official page on Azure Archive Storage1.

QUESTION 56
Chris Noth has been working as a senior cloud security engineer in CloudAppSec Private Ltd. His organization has selected a DRaaS (Disaster Recovery as a Service) company to provide a disaster recovery site that is fault tolerant and consists of fully redundant equipment with network connectivity and real-time data synchronization. Thus, if a disaster strikes Chris' organization, failover can be performed to the disaster recovery site with minimal downtime and zero data loss. Based on the given information, which disaster recovery site is provided by the DRaaS company to Chris' organization?

A. Hot Site
B. Cold Site
C. Remote site
D. Warm Site

Correct Answer: A
Section:
Explanation:
1.Disaster Recovery as a Service (DRaaS): DRaaS is a third-party service that provides organizations with a secondary site infrastructure, which employs cloud computing for application and data recovery from synchronous or asynchronous replication1.
1.Fault Tolerance and Redundancy: A fault-tolerant disaster recovery site with fully redundant equipment ensures that all critical systems and components have backups ready to take over in case of failure1.
1.Real-Time Data Synchronization: This feature ensures that data is continuously mirrored to the disaster recovery site, allowing for real-time recovery and zero data loss during failover1.
1.Hot Site: A hot site is a fully operational offsite data center equipped with hardware and software, network connectivity, and real-time data synchronization. It is ready to assume operation at a moment's notice, which aligns with the description provided1.
1.Minimal Downtime: The use of a hot site allows for minimal downtime during a disaster, as the site is already running and can take over immediately without the need to set up or configure equipment1.
Flexential's explanation of Disaster Recovery as a Service (DRaaS)1.

QUESTION 57
Richard Roxburgh works as a cloud security engineer in an IT company. His organization was dissatisfied with the services of its previous cloud service provider. Therefore, in January 2020, his organization adopted AWS cloud-based services and shifted all workloads and data in the AWS cloud. Richard wants to provide complete security to the hosted applications before deployment and while running in the AWS ecosystem. Which of the following automated security assessment services provided by AWS can be used by Richard to improve application security and check the application for any type of vulnerability or deviation from the best practices automatically?

A. AWS CloudFormation
B. Amazon Inspector
C. AWS Control Tower

D. Amazon CloudFront

Correct Answer: B
Section:
Explanation:
1.Amazon Inspector: It is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS1.
1.Automated Scans: Amazon Inspector automatically scans workloads, such as Amazon EC2 instances, containers, and Lambda functions, for vulnerabilities and unintended network exposure1.
1.Security Best Practices: It checks for deviations from best practices and provides detailed findings that include information about the nature of the threat, the affected resources, and recommendations for remediation1.
1.Integration with AWS: As an AWS-native service, Amazon Inspector is well-integrated into the AWS ecosystem, making it suitable for Richard's requirements to secure applications before deployment and while running1.
1.Exclusion of Other Options: AWS CloudFormation is used for infrastructure as code, AWS Control Tower for governance, and Amazon CloudFront for content delivery, none of which are automated security assessment services1.
AWS's official page on Amazon Inspector1.

QUESTION 58
Cindy Williams works as a cloud security engineer in an IT company located in Seattle, Washington. Owing to the cost-effective security, governance, and storage features provided by AWS, her organization adopted AWS cloud-based services. Cindy would like to detect any unusual activity in her organization's AWS account. She would like to obtain the event history of her organization's AWS account activity for security analysis and resource change tracking. Which of the following AWS service enables operational auditing, compliance, governance, and risk auditing for her organization's AWS account?

A. AWS CloudFormation
B. AWS Security Hub
C. AWS Config
D. AWS CloudTrail

Correct Answer: D
Section:
Explanation:
1.AWS CloudTrail: AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account1.
1.Event History: CloudTrail records actions taken by a user, role, or an AWS service as events. This includes actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs1.
1.Security Analysis: By providing a history of AWS account activity, CloudTrail enables security analysis and resource change tracking, which is essential for detecting unusual activities1.
1.Compliance: CloudTrail supports compliance by providing an immutable log of all the management events that occurred within the AWS account, which is crucial for audit trails1.
1.Operational Auditing: It allows organizations to conduct operational auditing by keeping track of user and API activity on AWS, which can be used to identify security incidents1.
AWS CloudTrail User Guide1.