CloudSecurityAlliance.CCSK.v2026-01-26.q253

Exam Code:	CCSK
Exam Name:	Certificate of Cloud Security Knowledge v5 (CCSKv5.0)
Certification Provider:	Cloud Security Alliance
Free Question Number:	253
Version:	v2026-01-26
# of views:	112
# of Questions views:	2530
https://www.dumpsdb.com/dumps/Cloud-Security-Alliance/CCSK/CloudSecurityAlliance.CCSK.v2026-01-26.q253	

NEW QUESTION: 1
Which of the following is NOT one of the common networks underlying in Cloud Infrastructure?
A. Service Network
B. Management Network
C. Security Network
D. Storage Network
Answer: C (LEAVE A REPLY)
If you are a cloud provider (including managing a private cloud), physical segregation of networks composing your cloud is important for both operational and security reasons. We most commonly see at least three different networks which are isolated onto dedicated hardware since there is no functional or traffic overlap:
1. The service network for communications between virtual machines and the Internet. This builds the network resource pool for the cloud users.
2. The storage network to connect virtual storage to virtual machines.
3. A management network for management and API traffic.
Ref: Reference: CSA Security GuidelinesV.4 (reproduced here for the educational purpose)

NEW QUESTION: 2
What is a key characteristic of serverless functions in terms of execution environment?
A. They need continuous monitoring by the user
B. They run on dedicated long-running instances

C. They require pre-allocated server space
D. They are executed in isolated, ephemeral environments
Answer: D (LEAVE A REPLY)
Serverless functions are designed to run in isolated, ephemeral environments, meaning that each execution is independent and temporary. These functions are typically event-driven and executed on-demand, without the need for pre-allocated server resources. Once the function finishes executing, the environment is discarded, making it highly efficient and scalable. This architecture abstracts away infrastructure management, allowing developers to focus on the code itself.

NEW QUESTION: 3
What key activities are part of the preparation phase in incident response planning?
A. Implementing encryption and access controls
B. Establishing a response process, training, communication plans, and infrastructure evaluations
C. Creating incident reports and post-incident reviews
D. Developing malware analysis procedures and penetration testing
Answer: B (LEAVE A REPLY)
The preparation phase in incident response planning involves activities that set the foundation for a successful response to potential security incidents. These activities typically include:
Establishing a response process: Defining clear procedures for how incidents will be detected, analyzed, and mitigated.
Training: Ensuring that all relevant personnel are trained on their roles and responsibilities during an incident.
Communication plans: Creating communication protocols to ensure that all stakeholders are informed during an incident.
Infrastructure evaluations: Assessing the existing security infrastructure to ensure it is capable of supporting incident response efforts.
Implementing encryption and access controls is important for security but is not specifically part of the preparation phase for incident response. Creating incident reports and post-incident reviews is typically part of the post-incident phase, after the response is completed. Developing malware analysis procedures and penetration testing is more related to ongoing security operations and testing rather than the preparation phase of incident response.

NEW QUESTION: 4
What primary aspects should effective cloud governance address to ensure security and compliance?
A. Encryption, redundancy, data integrity, and scalability
B. Decision making, prioritization, monitoring, and transparency

C. Service availability, disaster recovery, load balancing, and latency
D. Authentication, authorization, accounting, and auditing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
Identifying the specific threats against servers and determine the effectiveness of existing security controls in counteracting the threats. is known as:
A. Risk Mitigation
B. Risk Assessment
C. Risk Management
D. Risk Determination
Answer: (SHOW ANSWER)
like this, which has similar-looking answers should be carefully answered Risk Management is overall process which covers from identifying threats to ultimately review the effectiveness of the controls.

NEW QUESTION: 6
Centralization of log streams is charactertic of which devices?
A. IDS
B. IPS
C. SIEM
D. DLP
Answer: (SHOW ANSWER)
SIEM is a combination of Security Incident Management(SIM)and Security Event Management(SEM).
A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralised reporting.

NEW QUESTION: 7
The intermediary that provides connectivity and transport of cloud services between the CSPs and the cloud service consumers is called:
A. Cloud Service Broker
B. Cloud Access Service Broker
C. Cloud Reseller
D. Cloud Carrier
Answer: D (LEAVE A REPLY)
All the terms given as options are very important and candidate is expected to know them and differentiate between them

NEW QUESTION: 8
According to ENISA(European Network and Information Security Agency) document on Security risk and recommendation. Isolation Failure is:
A. Organizational Risk
B. Management Risk
C. Technical Risk
D. Compliance Risk
Answer: (SHOW ANSWER)
Isolation failure is defined as:
Multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure(e.g, so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks).

NEW QUESTION: 9
When comparing different Cloud Service Providers (CSPs), what should a cybersecurity professional be mindful of regarding their organizational structures?
A. All CSPs use the same organizational structure and terminology
B. Different CSPs may have similar structures but use varying terminology
C. CSPs have vastly different organizational structures and identical terminology
D. Terminology difference in CSPs does not affect cybersecurity practices.
Answer: (SHOW ANSWER)
When comparing different Cloud Service Providers (CSPs), it is important to recognize that while they may have similar organizational structures - such as divisions for security, compliance, and support - they often use varying terminology to describe their services, roles, and responsibilities. Understanding these differences is crucial for cybersecurity professionals to ensure proper alignment of security practices, controls, and policies across different cloud platforms.
CSPs typically have variations in organizational structure and terminology. While the structure can vary, it is not usually "vastly" different in terms of core functions. Differences in terminology can have implications for understanding security roles, policies, and practices, affecting how cybersecurity tasks are performed.

NEW QUESTION: 10
In which type of environment is it impractical to allow the customer to conduct their own audit, making it important that the data center operators are required to provide auditing for the customers?
A. Long distance relationships
B. Distributed computing arrangements

C. Single tenant environments
D. Multi-tenant environments
E. Multi-application, single tenant environments
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following BEST describes a benefit of Infrastructure as Code (IaC) in cybersecurity contexts?
A. Reduces the need for security auditing
B. Enables consistent security configurations through automation
C. Increases manual control over security settings
D. Increases scalability of cloud resources
Answer: B (LEAVE A REPLY)
Infrastructure as Code (IaC) helps maintain consistency in security configurations through automation, reducing the likelihood of misconfigurations. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 12
Which of the following is used for governing and configuring cloud resources and is a top priority in cloud security programs?
A. Management Console
B. Management plane
C. Orchestrators
D. Abstraction layer
Answer: B (LEAVE A REPLY)
The management plane is used for governing and configuring cloud resources and is considered a top priority in cloud security programs. It provides the tools and interfaces for administrators to manage, configure, and control cloud resources, such as virtual machines, storage, and networking. It is critical to secure the management plane because it often has access to sensitive configurations and the ability to modify cloud environments, making it a prime target for attacks.
Management Console is an interface that interacts with the management plane, but it is not the underlying system for governance and configuration. Orchestrators are used to automate the management and deployment of cloud resources but are not the primary component for governing and securing cloud environments. Abstraction layer refers to the layer that hides the complexity of underlying infrastructure, but it does not directly govern or configure cloud resources.

NEW QUESTION: 13
What is a potential concern of using Security-as-a-Service (SecaaS)?
A. Intelligence sharing

B. Scaling and costs
C. Deployment flexibility
D. Lack of visibility
E. Insulation of clients
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following best describes the responsibility for security in a cloud environment?
A. Cloud Service Customers (CSCs) are solely responsible for security in the cloud environment. The Cloud Service Providers (CSPs) are accountable.
B. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities.
The exact allocation of responsibilities depends on the technology and context.
C. Cloud Service Providers (CSPs) are solely responsible for security in the cloud environment. Cloud Service Customers (CSCs) have an advisory role.
D. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities.The allocation of responsibilities is constant.
Answer: B (LEAVE A REPLY)
The shared security responsibility model in cloud environments clarifies that CSPs and CSCs both have roles, with specific responsibilities varying based on the service model (IaaS, PaaS, SaaS). In IaaS, CSCs handle more security, while CSPs manage most security in SaaS. Reference: [CCSK Study Guide, Domain 1 - Cloud Security Scope and Responsibilities][source 16].

NEW QUESTION: 15
Which of the following is a key consideration in Data security but does not feature in Data Security Life cycle?
A. Storage Location
B. Storage Device
C. Storage protocol
D. Access Method
Answer: A (LEAVE A REPLY)
The lifecycle represents the phases information passes through but doesnt address its location or how it is accessed.

NEW QUESTION: 16
Which of the following events should be monitored according to CIS AWS benchmarks?
A. Regular file backups
B. Data encryption at rest
C. Successful login attempts
D. Unauthorized API calls

Answer: D (LEAVE A REPLY)
According to the CIS AWS (Center for Internet Security AWS) benchmarks, unauthorized API calls should be closely monitored because they indicate potential security threats or malicious activity within the AWS environment. Monitoring unauthorized API calls helps detect unauthorized access, misconfigurations, or attempts to exploit cloud resources. It's a key part of maintaining a secure AWS environment and helps ensure compliance with security best practices.
Regular file backups are important but not specifically a focus of the CIS AWS benchmarks. Data encryption at rest is a security best practice but monitoring unauthorized API calls directly addresses access control and security within the environment. Successful login attempts are important but monitoring failed login attempts (as opposed to successful ones) is generally a better practice for identifying suspicious activity.

NEW QUESTION: 17
What is an essential security characteristic required when using multi-tenant technologies?
A. Segmented and segregated customer environments
B. Limited resource allocation
C. Resource pooling
D. Abstraction and automation
Answer: A (LEAVE A REPLY)
In multi-tenant technologies, the fundamental security requirement is segmented and segregated customer environments. Multi-tenancy means that multiple customers (tenants) share the same physical or virtual infrastructure while maintaining logical separation to prevent data leakage and unauthorized access between tenants.
To ensure security and compliance in multi-tenant environments, providers implement:
* Network segmentation (VLANs, Virtual Private Clouds)
* Isolation mechanisms (such as virtual firewalls and access control lists)
* Data isolation through encryption and access controls
* Hypervisor-based isolation in virtualized environments
The goal is to create strong logical isolation between tenants to mitigate risks like data leakage, guest- hopping attacks, and unauthorized access.
Why Other Options Are Incorrect:

* B. Limited resource allocation: While resource limits may help performance management, they do not inherently ensure security in multi-tenant settings.
* C. Resource pooling: Though fundamental to cloud computing, it does not address the isolation needed for secure multi-tenancy.
* D. Abstraction and automation: These are key elements in cloud computing but do not directly address multi-tenant security.
References:
CSA Security Guidance v4.0, Domain 7: Infrastructure Security
Cloud Computing Security Risk Assessment (ENISA) - Isolation Failure
Cloud Controls Matrix (CCM) v3.0.1 - Infrastructure and Virtualization Security Domain

NEW QUESTION: 18
Which of the following is a common security issue associated with serverless computing environments?
A. High operational costs
B. Misconfigurations
C. Limited scalability
D. Complex deployment pipelines
Answer: B (LEAVE A REPLY)
Serverless environments are vulnerable to misconfigurations, which can expose sensitive data and resources, making security configurations critical. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security]

NEW QUESTION: 19
What is true of security as it relates to cloud network infrastructure?
A. You should apply cloud firewalls on a per-network basis.
B. You should deploy your cloud firewalls identical to the existing firewalls.
C. You should always open traffic between workloads in the same virtual subnet for better visibility.
D. You should implement a default allow with cloud firewalls and then restrict as necessary.
E. You should implement a default deny with cloud firewalls.
Answer: E (LEAVE A REPLY)
Explanation

NEW QUESTION: 20
Why is it important to control traffic flows between networks in a cybersecurity context?
A. To increase the speed of data transmission
B. To reduce the blast radius of attacks
C. To simplify network architecture
D. To reduce the amount of data stored

Answer: B (LEAVE A REPLY)
Controlling traffic flows between networks is critical in a cybersecurity context toreduce the blast radius of attacks. By segmenting networks and implementing controls such as firewalls, organizations can limit the lateral movement of attackers, containing breaches and minimizing their impact.
From theCCSK v5.0 Study Guide, Domain 9 (Network Security), Section 9.2:
"Controlling traffic flows between networks is a fundamental cybersecurity practice to reduce the blast radius of attacks. Network segmentation and micro-segmentation limit an attacker's ability to move laterally within the environment, containing breaches and protecting critical assets." Option B (To reduce the blast radius of attacks) is the correct answer.
Option A (To increase the speed of data transmission) is incorrect because traffic control focuses on security, not speed.
Option C (To simplify network architecture) is incorrect because segmentation may increase complexity.
Option D (To reduce the amount of data stored) is incorrect because traffic control does not directly affect data storage.
Reference:
CCSK v5.0 Study Guide, Domain 9, Section 9.2: Network Segmentation and Traffic Control.

NEW QUESTION: 21
A cloud storage architecture that caches content close to locations of high demand is known as:
A. Volume Data
B. Block Data
C. Ephemeral Storage
D. Content Delivery Network(CDN)
Answer: D (LEAVE A REPLY)
A content delivery network(CDN) is a system of distributed servers(network) that deliver pages and other Web content to a user. based on the geographic locations of the user. the origin of the webpage and the content delivery server.

NEW QUESTION: 22
Use elastic servers when possible and move workloads to new instances.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 23

How does DevSecOps fundamentally differ from traditional DevOps in the development process?

A. DevSecOps removes the need for a separate security team.

B. DevSecOps focuses primarily on automating development without security.

C. DevSecOps reduces the development time by skipping security checks.

D. DevSecOps integrates security into every stage of the DevOps process.

Answer: D (LEAVE A REPLY)

DevSecOps stands forDevelopment, Security, and Operationsand represents the integration of security practices within the DevOps process from the very beginning. The key difference between traditional DevOps and DevSecOps is thatDevSecOps embeds security as a core componentrather than an afterthought.

In traditional DevOps, security is often handled as a separate process at the end of the development lifecycle. However, this can lead to vulnerabilities being identified late, increasing the cost and effort required to fix them.

In DevSecOps, security is "baked in" from the start,involving practices such as:

Automated security testing:Integrating security checks into CI/CD pipelines.

Continuous monitoring:Real-time threat detection during development and production.

Collaboration:Cross-functional teams working together to maintain security at each stage.

Why Other Options Are Incorrect:

A . Removes the need for a separate security team:This is false as DevSecOps does not eliminate security teams; it integrates them within the development lifecycle.

B . Focuses on automating development without security:The opposite is true; DevSecOps specifically focuses on integrating security.

C . Reduces development time by skipping security checks:This contradicts the core principle of DevSecOps, which enhances security without sacrificing speed.

Reference:

CSA Security Guidance v4.0, Domain 10: Application Security

Cloud Computing Security Risk Assessment (ENISA) - DevSecOps Best Practices Cloud Controls Matrix (CCM) v3.0.1 - DevOps and Continuous Integration/Continuous Deployment (CI/CD)

NEW QUESTION: 24

What is a primary benefit of implementing micro-segmentation within a Zero Trust Architecture?

A. Simplifies network design and maintenance

B. Enhances security by isolating workloads from each other

C. Increases the overall performance of network traffic

D. Reduces the need for encryption across the network

Answer: B (LEAVE A REPLY)

The primary benefit of implementing micro-segmentation within a Zero Trust Architecture is that it enhances security by isolating workloads from each other. Micro-segmentation

involves dividing the network into smaller, isolated segments, so that even if an attacker gains access to one part of the network, they cannot easily move laterally to other parts. This is crucial in a Zero Trust model, which assumes that threats may exist both inside and outside the network, and security is enforced at a granular level for each workload. Simplifying network design is not a benefit of micro-segmentation; in fact, it can add complexity due to the increased number of network segments. Increased network performance is not a primary outcome of micro- segmentation, which may introduce overhead. Reducing the need for encryption is incorrect because micro- segmentation doesn't eliminate the need for encryption; it works alongside encryption to provide better security.

NEW QUESTION: 25
Which of the following is one of the five essential characteristics of cloud computing as defined by NIST?
A. Nation-state boundaries
B. Measured service
C. Multi-tenancy
D. Hybrid clouds
E. Unlimited bandwidth
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Inability of customer to leave, migrate, Or transfer to an alternate cloud service provider because of technical or nontechnical constraints. is known as:
A. Vendor Limit
B. Vendor lock-out
C. Vendor lock-in
D. Vendor Lock
Answer: C (LEAVE A REPLY)
Vendor lock-in is a situation in which a customer using a product or service cannot easily transition to a competitor's product or service. Vendor lock-in is usually the result of proprietary technologies that are incompatible with those of competitors.

NEW QUESTION: 27
What is the main purpose of multi-region resiliency in cloud environments?
A. To increase the number of users in each region
B. To ensure compliance with regional and international data laws
C. To reduce the cost of deployments and increase efficiency
D. To improve fault tolerance through deployments across multiple regions
Answer: (SHOW ANSWER)

Multi-region resiliency in cloud environments is primarily used to improve fault tolerance by deploying applications and services across multiple geographical regions. This strategy ensures that if one region experiences an outage or failure, the application or service can failover to another region, maintaining availability and minimizing downtime. Multi-region deployments help organizations ensure business continuity, disaster recovery, and high availability.
Increasing the number of users in each region is not the main purpose of multi-region resiliency. While multi- region deployment can help with compliance, the primary goal is fault tolerance and availability, not compliance with data laws. While multi-region deployment may offer some efficiency benefits, the main purpose is not cost reduction; it's about ensuring reliability and availability.

NEW QUESTION: 28
What is the primary purpose of cloud governance in an organization?
A. To increase data transfer speeds within the cloud environment
B. To reduce the cost of cloud services
C. To ensure compliance, security, and efficient management aligned with the organization's goals
D. To eliminate the need for on-premises data centers
Answer: C (LEAVE A REPLY)
Cloud governance establishes controls and policies that align with the organization's goals for security, compliance, and efficient management in the cloud. Reference: [Security Guidance v5, Domain 2 - Cloud Governance]

NEW QUESTION: 29
Why is it important to capture and centralize workload logs promptly in a cybersecurity environment?
A. To simplify application debugging processes
B Primarily to reduce data storage costs
B. Logs may be lost during a scaling event
C. To comply with data privacy regulations
Answer: C (LEAVE A REPLY)
In a cybersecurity environment, it is important to capture and centralize workload logs promptly because logs may be lost during a scaling event. When workloads are scaled up or down, such as when cloud resources are dynamically allocated, logs may not be properly captured or may be overwritten if they are not centralized and stored in a reliable, persistent location. Centralizing logs ensures that valuable security data is not lost during these events and can be accessed for incident detection, analysis, and response.

NEW QUESTION: 30

Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

A. False

B. True

Answer: (SHOW ANSWER)

NEW QUESTION: 31

What is a common characteristic of default encryption provided by cloud providers for data at rest?

A. It is not available without an additional premium service

B. It always requires the customer's own encryption keys

C. It uses the cloud provider's keys, often at no additional cost

D. It does not support encryption for data at rest

Answer: C (LEAVE A REPLY)

Many cloud providers offer default encryption for data at rest, which is typically enabled automatically for data stored within the cloud. In these cases, the encryption is often done using the cloud provider's keys as part of the provider's security infrastructure, and it is usually provided at no additional cost to the customer. This ensures that data is protected while at rest, reducing the risk of unauthorized access.

NEW QUESTION: 32

Which of the following is a common exploitation factor associated with serverless and container workloads?

A. Poor Documentation

B. Misconfiguration

C. Insufficient Redundancy

D. Low Availability

Answer: B (LEAVE A REPLY)

Misconfiguration is one of the most prevalent risks in serverless and container-based environments. Given the complex nature of container orchestration (e.g., Kubernetes), CI/CD pipelines, and ephemeral infrastructure, simple missteps-such as overly permissive roles or exposed ports-can lead to significant vulnerabilities.

These workloads require strict configuration management, automated scanning, and secure defaults to prevent breaches. Unlike traditional servers, containers and functions spin up and down rapidly, making traditional visibility tools insufficient.
This is discussed thoroughly in Domain 8: Virtualization and Containers, where the CCSK guidance identifies misconfiguration as a leading cause of cloud-native exploitation.
Reference:
CSA Security Guidance v4.0 - Domain 8: Virtualization and Containers

NEW QUESTION: 33
The entity that has the primary relationship with an individual from whom his/her PII is collected is known as:
A. Data Controller
B. Data processor
C. Data custodian
D. Data Manager
Answer: A (LEAVE A REPLY)
The data controller(typically the entity that has the primary relationship with an individual) is prohibited from collecting and processing personal data unless certain criteria are met. For example, if the data subject has consented to the collection and proposed uses of his or her data, then the controller may collect and process data, according to the consent agreement.
Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance

NEW QUESTION: 34
Which of the following best describes the advantage of custom application level encryption?
A. It simplifies the encryption process by centralizing it at the network level
B. It enables ownership and more granular control of encryption keys
C. It reduces the need for encryption by enhancing network security
D. It delegates the control of keys to third-party providers
Answer: B (LEAVE A REPLY)
Custom application-level encryption provides organizations with precise control over what is encrypted and who manages the encryption keys. Unlike network-level encryption, this method allows sensitive fields (e.g., credit card numbers) to be encrypted before data even enters the storage or processing pipeline.
This approach enables compliance with strict data privacy laws and protects data from being decrypted by unauthorized actors-even cloud providers. Organizations can enforce key rotation policies and maintain exclusive key access.
This is detailed in Domain 11: Data Security and Encryption, which recommends application-level encryption for sensitive data protection, particularly in regulated industries.

Reference:
CSA Security Guidance v4.0 - Domain 11: Data Security and Encryption

NEW QUESTION: 35
Which of the following is NOT a cloud computing characteristic that impacts incidence response?
A. Object-based storage in a private cloud.
B. The possibility of data crossing geographic or jurisdictional boundaries.
C. The on demand self-service nature of cloud computing environments.
D. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.
E. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
How does SASE enhance traffic management when compared to traditional network models?
A. It solely focuses on user authentication improvements
B. It replaces existing network protocols with new proprietary ones
C. It filters traffic near user devices, reducing the need for backhauling
D. It requires all traffic to be sent through central data centers
Answer: C (LEAVE A REPLY)
SASE reduces latency and enhances performance by filtering traffic closer to the user, avoiding the need to backhaul traffic to a central data center. Reference: [Security Guidance v5, Domain 7 - Network Security]

NEW QUESTION: 37
Which of the following is NOT a characteristic of cloud computing?
A. On-demand self service
B. Resource Pooling
C. Metered service
D. Reduced personnel cost
Answer: D (LEAVE A REPLY)
The characteristics of cloud computing are
1. 0n-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms(e.g, mobile phones, tablets, laptops and workstations).

3. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction(e.g, country, state or datacenter).
Examples of resources include storage, processing, memory and network bandwidth.
4. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at anytime.
5. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service(e.g, storage, processing, bandwidth and active user accounts).
Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

NEW QUESTION: 38
When mapping functions to lifecycle phases, which functions are required to successfully process data?
A. Create and Use
B. Create and Store
C. Create, Use, Store, and Delete
D. Create, Store, Use, and Share
E. Create, Store, and Use
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
What type of logs record interactions with specific services in a system?
A. (Service and Application Logs
B. Security Logs
C. Network Logs
D. Debug Logs
Answer: A (LEAVE A REPLY)
Service and Application Logs record interactions with specific services within a system. These logs track how users and systems interact with various applications and services, such as API calls, service requests, and responses. They are essential for monitoring service performance, troubleshooting issues, and auditing service usage.
Security Logs primarily focus on security-related events, such as unauthorized access attempts or security breaches. Network Logs capture network traffic data and information about the movement of data across a network. Debug Logs are typically used for

debugging purposes and may include detailed technical information, but they do not specifically track service interactions like service and application logs do.

NEW QUESTION: 40
Which concept focuses on maintaining the same configuration for all infrastructure components, ensuring they do not change once deployed?
A. Component credentials
B. Immutable infrastructure
C. Infrastructure as code
D. Application integration
Answer: B (LEAVE A REPLY)
Immutable infrastructure maintains static configurations after deployment, ensuring consistency and preventing unauthorized changes. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security]

NEW QUESTION: 41
According to NIST, what is cloud computing defined as?
A. A shared set of resources delivered over the Internet
B. A model for more-efficient use of network-based resources
C. A model for on-demand network access to a shared pool of configurable resources
D. Services that are delivered over the Internet to customers
Answer: C (LEAVE A REPLY)
NIST defines cloud computing as on-demand network access to a shared pool of configurable resources, aligning with the essential characteristics of cloud services. Reference: [Security Guidance v5, Domain 1 - Cloud Computing Models]

NEW QUESTION: 42
Which of the following items is NOT an example of Security as a Service (SecaaS)?
A. Intrusion detection
B. Authentication
C. Spam filtering
D. Web filtering
E. Provisioning
Answer: E (LEAVE A REPLY)

NEW QUESTION: 43
Which cloud deployment model involves a cloud and a datacenter, bound together by technology to enable data and application portability?
A. Hybrid cloud
B. Public cloud
C. Multi-cloud

D. Private cloud

Answer: A (LEAVE A REPLY)

Thehybrid clouddeployment model involves integrating a private cloud (or on-premises datacenter) with a public cloud, bound together by technology that enablesdata and application portability. This allows workloads to move seamlessly between environments, leveraging the benefits of both private and public clouds.

From theCCSK v5.0 Study Guide, Domain 1 (Cloud Computing Concepts and Architectures), Section 1.3:

"A hybrid cloud combines on-premises infrastructure (or a private cloud) with a public cloud, integrated through technology that allows data and application portability. This model enables organizations to maintain sensitive workloads on-premises while leveraging the scalability of public cloud services." Option A (Hybrid cloud) is the correct answer.

Option B (Public cloud) is incorrect because it involves only cloud provider resources, not a datacenter.

Option C (Multi-cloud) is incorrect because it refers to using multiple public cloud providers, not a datacenter.

Option D (Private cloud) is incorrect because it does not inherently include integration with a public cloud.

References:

CCSK v5.0 Study Guide, Domain 1, Section 1.3: Cloud Deployment Models.

NEW QUESTION: 44

What defines easiness to move and reuse application components regardless of the provider, platform,

0S, infrastructure, location, storage, format of data or APIs, how well applications work together, and how well new applications work with other solutions present in the business, organization, or provider's existing architecture?

A. Scalability

B. Elasticity

C. Portability

D. Interoperability

Answer: D (LEAVE A REPLY)

Interoperability is an important characteristic.

Definition: Interoperability

Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customer.

NEW QUESTION: 45

Which aspect is most important for effective cloud governance?

A. Formalizing cloud security policies

B. Implementing best-practice cloud security control objectives

C. Negotiating SLAs with cloud providers
D. Establishing a governance hierarchy
Answer: (SHOW ANSWER)
A governance hierarchy provides a structured approach to managing cloud services, ensuring policies and controls are effectively enforced. Reference: [Security Guidance v5, Domain 2 - Cloud Governance]

NEW QUESTION: 46
What is a key advantage of using Infrastructure as Code (IaC) in application development?
A. It removes the need for manual testing.
B. It eliminates the need for cybersecurity measures.
C. It enables version control and rapid deployment.
D. It ensures zero configuration drift by default.
Answer: C (LEAVE A REPLY)
Infrastructure as Code (IaC)allows organizations toautomate cloud infrastructure managementusing code-based templatesinstead of manual configuration.
Key Benefits of IaC:
* Version Control & Automation
* IaC uses version control systems (e.g., Git) to track changes in infrastructure.
* Developers can quickly deploy infrastructure updates, reducing human errors.
* Ensuresconsistent, repeatable deploymentsacross environments.
* Rapid & Scalable Deployments
* EnablesCI/CD (Continuous Integration/Continuous Deployment)pipelines.
* Automates infrastructure provisioning, reducingdeployment time from hours to minutes.
* Works withTerraform, AWS CloudFormation, Ansible, and Kubernetes manifests.
* Security & Compliance Enhancements
* Policies as Code (PaC) & Security as Code (SaC) enforce security best practices.
* Cloud Security Posture Management (CSPM)scans IaC for misconfigurations.
* Reducesshadow IT risksby enforcingpre-approved infrastructure templates.
* Prevents Configuration Drift
* RegularIaC re-application (desired state enforcement)ensuresconsistent infrastructure settings.
* Eliminatesmanual misconfigurations that lead to security vulnerabilities.
This is extensively covered in:
* CCSK v5 - Security Guidance v4.0, Domain 6 (Management Plane and Business Continuity)
* Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) - Infrastructure and Configuration Management Controls.

NEW QUESTION: 47
Which governance domain deals with evaluating how cloud computing affects compliance with internal
security policies and various legal requirements, such as regulatory and legislative?
A. Compliance and Audit Management
B. Governance and Enterprise Risk Management
C. Information Governance
D. Legal Issues: Contracts and Electronic Discovery
E. Infrastructure Security
Answer: (SHOW ANSWER)

NEW QUESTION: 48
What is the primary focus during the Preparation phase of the Cloud Incident Response framework?
A. Developing a cloud service provider evaluation criterion
B. Deploying automated security monitoring tools across cloud services
C. Establishing a Cloud Incident Response Team and response plans
D. Conducting regular vulnerability assessments on cloud infrastructure
Answer: C (LEAVE A REPLY)
The Preparation phase focuses on setting up an incident response team and developing plans to handle incidents efficiently when they occur. Reference: [Security Guidance v5, Domain 11 - Incident Response]

NEW QUESTION: 49
Who is responsible for Data Security in Software as a Service(SaaS) service mode?
A. Cloud Service Provider
B. Cloud Customer
C. Cloud Carrier
D. It's a shared responsibility between Cloud Service Provider and Cloud Customer
Answer: B (LEAVE A REPLY)
Remember that data security will always remain responsibility of the cloud customer in all service models

NEW QUESTION: 50
Which one is NOT considered as one of the building blocks of the cloud computing?
A. RAM
B. CPU
C. Clock
D. Networking
Answer: (SHOW ANSWER)
The question is asking for an exception by using "NOT"
The building blocks of cloud computing are composed of random access memory (RAM), the central processing unit(CPU), storage, and networking.

NEW QUESTION: 51
Which of the following best describes the shift-left approach in software development?
A. Relies only on automated security testing tools
B. Emphasizes post-deployment security audits
C. Focuses on security only during the testing phase
D. Integrates security early in the development process
Answer: (SHOW ANSWER)
The shift-left approach in software development refers to integrating security measures early in the development process, rather than waiting until later stages (such as post-deployment) to address security issues. By shifting security "left" in the software development lifecycle, teams can identify and address potential vulnerabilities and risks early, reducing costs and improving the overall security of the application.

NEW QUESTION: 52
What can be implemented to help with account granularity and limit
blast radius with laaS an PaaS?
A. Maintaining tight control of the primary account holder credentials
B. Configuring role-based authentication
C. Configuring secondary authentication
D. Establishing multiple accounts
E. Implementing least privilege accounts
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Your SLA with your cloud provider ensures continuity for all services.
A. False
B. True
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 54
Which of the following from the governance hierarchy provides specific goals to minimize risk and maintain a secure environment?
A. Implementation guidance
B. Control objectives
C. Policies
D. Control specifications
Answer: B (LEAVE A REPLY)
Control objectives are specific goals or outcomes designed to minimize risk and maintain a secure environment. They are part of a broader governance framework and provide clear, measurable targets that organizations aim to achieve in order to meet security, compliance, and operational goals. Control objectives help guide the implementation of security measures and ensure the organization's security posture aligns with its risk management strategy.
Implementation guidance provides detailed instructions on how to implement controls but does not set specific goals. Policies define the high-level principles and rules that guide behavior and decision-making, but they are more general than control objectives. Control specifications typically define how specific controls are implemented but do not establish the overarching goals that guide risk management.

NEW QUESTION: 55
In a cloud environment spanning multiple jurisdictions, what is the most important factor to consider for compliance?
A. Relying on the cloud service provider's compliance certifications for all jurisdictions
B. Focusing on the compliance requirements defined by the laws, regulations, and standards enforced in the jurisdiction where the company is based
C. Relying only on established industry standards since they adequately address all compliance needs
D. Understanding the legal and regulatory requirements of each jurisdiction where data originates, is stored, or processed
Answer: (SHOW ANSWER)
In a cloud environment that spans multiple jurisdictions, it is crucial to understand the legal and regulatory requirements of each jurisdiction where data originates, is stored, or is processed. Different regions or countries have varying laws, regulations, and compliance standards regarding data privacy, protection, and security. Organizations must ensure they meet all applicable requirements in each jurisdiction to avoid potential legal issues, fines, and reputational damage.

NEW QUESTION: 56
IT Risk management is best described in:
A. FIPS 140-2

B. ISO 27005
C. NIST SP800-14
D. ISO 27017
Answer: B (LEAVE A REPLY)
IS027005 standards describes IT Risk Management process

NEW QUESTION: 57
Which of the following will not be provided by cloud services when requested by the customer?
A. DLP solution results
B. SIEM logs
C. Details of security controls
D. Geographical locations of the datacentre
Answer: (SHOW ANSWER)
The cloud service provider will not provide the details of security controls as it will harm the security of its infrastructure if the adversaries knows the details.

NEW QUESTION: 58
Which strategic approach is most appropriate for managing a multi-cloud environment that includes multiple IaaS and PaaS providers?
A. Allow each department to manage their own cloud services independently.
B. Use a single security tool for all providers.
C. Rely on each provider's native security features with limited additional oversight.
D. Implement strict governance and monitoring procedures across all platforms.
Answer: D (LEAVE A REPLY)
In a multi-cloud environment, organizations must implement centralized governance, security policies, and monitoring to:
* Ensure compliance across multiple providers (AWS, Azure, Google Cloud, etc.).
* Standardize security policies to avoid inconsistencies and misconfigurations.
* Use Cloud Security Posture Management (CSPM) tools to automate security compliance and misconfiguration detection.
* Prevent cloud sprawl by enforcing identity and access policies across multiple providers.
This aligns with:
* CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Risk Management)
* CSA's Cloud Security Alliance (CCM) - Cloud Security Operations Best Practices.

NEW QUESTION: 59
In the Incident Response Lifecycle, which phase involves identifying potential security events and examining them for validity?
A. Post-Incident Activity
B. Detection and Analysis

C. Preparation
D. Containment, Eradication, and Recovery
Answer: B (LEAVE A REPLY)
The Detection and Analysis phase involves identifying incidents and determining their impact. It is crucial to validate events to understand if they constitute a security incident.
Reference: [Security Guidance v5, Domain 11 - Incident Response]

NEW QUESTION: 60
What is a key advantage of using Infrastructure as Code (IaC) in application development?
A. It removes the need for manual testing.
B. It eliminates the need for cybersecurity measures.
C. It enables version control and rapid deployment.
D. It ensures zero configuration drift by default.
Answer: (SHOW ANSWER)
Infrastructure as Code (IaC)allows organizations toautomate cloud infrastructure managementusingcode-based templatesinstead of manual configuration.
Key Benefits of IaC:
IaC uses version control systems (e.g., Git) to track changes in infrastructure.
Developers can quickly deploy infrastructure updates, reducing human errors.
Ensuresconsistent, repeatable deploymentsacross environments.
Rapid & Scalable Deployments
EnablesCI/CD (Continuous Integration/Continuous Deployment)pipelines.
Automates infrastructure provisioning, reducingdeployment time from hours to minutes.
Works withTerraform, AWS CloudFormation, Ansible, and Kubernetes manifests.
Security & Compliance Enhancements
Policies as Code (PaC) & Security as Code (SaC) enforce security best practices.
Cloud Security Posture Management (CSPM)scans IaC for misconfigurations.
Reducesshadow IT risksby enforcingpre-approved infrastructure templates.
Prevents Configuration Drift
RegularIaC re-application (desired state enforcement)ensuresconsistent infrastructure settings.
Eliminatesmanual misconfigurations that lead to security vulnerabilities.
This is extensively covered in:
CCSK v5 - Security Guidance v4.0, Domain 6 (Management Plane and Business Continuity) Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) - Infrastructure and Configuration Management Controls.

NEW QUESTION: 61
In the context of cloud security, which approach prioritizes incoming data logsfor threat detection by applying multiple sequential filters?
A. Cascade-and-filter approach

B. Parallel processing approach
C. Streamlined single-filter method
D. Unfiltered bulk analysis
Answer: A (LEAVE A REPLY)
TheCascade-and-filter approachis a method used in cloud security to handle incoming data logs efficiently.
It prioritizes logs for threat detection byapplying multiple sequential filters, where each filter progressively narrows down the data. This approach helps in:
* Layered threat detection:Early filters eliminate non-critical data, while subsequent filters perform more detailed analysis.
* Efficient processing:Reduces the volume of data passed through advanced and resource-intensive filters.
* Improved accuracy:Allows focusing on the most relevant security events.
For example, in a cloud environment, the first filter might check for known malicious IP addresses, the second might look for suspicious file types, and subsequent filters may perform behavioral analysis or anomaly detection.
Why Other Options Are Incorrect:
* B. Parallel processing approach:This method processes logs simultaneously, not sequentially, and is less efficient for prioritizing threats.
* C. Streamlined single-filter method:Uses a single filter for all data, which lacks depth and thoroughness in identifying complex threats.
* D. Unfiltered bulk analysis:This approach is resource-intensive and inefficient, as it does not prioritize or filter logs.
References:
CSA Security Guidance v4.0, Domain 9: Incident Response
Cloud Computing Security Risk Assessment (ENISA) - Log Management and Threat Detection Cloud Controls Matrix (CCM) v3.0.1 - Logging and Monitoring Domain

NEW QUESTION: 62
What process involves an independent examination of records, operations, processes, and controls within an organization to ensure compliance with cybersecurity policies, standards, and regulations?

A. Risk assessment
B. Audit
C. Penetration testing
D. Incident response
Answer: B (LEAVE A REPLY)
Auditing is an independent review process that validates adherence to policies, regulations, and standards. It is essential in assessing security posture. Reference: [Security Guidance v5, Domain 3 - Compliance]

NEW QUESTION: 63
Which of the following best describes the primary purpose of image factories in the context of virtual machine (VM) management?
A. Automating the VM image creation processes
B. Managing network configurations for VMs
C. Providing backup solutions for VM images
D. Enhancing security of VM images
Answer: A (LEAVE A REPLY)
Correct Option: A. Automating the VM image creation processes
Image factories are tools or systems designed to automate the building and maintenance of virtual machine images. They ensure that images are consistently created, updated, and patched, which is essential for maintaining a secure and manageable cloud infrastructure.
From the CSA Security Guidance v4.0 - Domain 8: Virtualization and Containers:
"Image factories are systems that automate the creation of virtual machine images. They help ensure that base images are consistently built and can include controls for security, configuration management, and compliance."
- Domain 8: Virtualization and Containers, CSA Security Guidance v4.0
These factories often integrate with CI/CD pipelines to streamline deployment and reduce human error - a key concern in cloud security operations.
Why the Other Options Are Incorrect:
* B. Managing network configurations for VMs# This task is typically handled by orchestration layers or cloud networking tools, not image factories.
* C. Providing backup solutions for VM images# Image factories are not responsible for backups; they are focused on creation, not preservation.
* D. Enhancing security of VM images# While image factories can embed security best practices during creation, their primary purpose is automation, not security enhancement per se.
* Main Topic: Virtualization and Containers
* Source: CSA Security Guidance v4.0, Domain 8 - Virtualization and Containers

NEW QUESTION: 64
Select the best definition of "compliance" from the options below.

A. The diligent habits of good security practices and recording of the same.
B. The process of completing all forms and paperwork necessary to develop a defensible paper trail.
C. The development of a routine that covers all necessary security measures.
D. The timely and efficient filing of security reports.
E. The awareness and adherence to obligations, including the assessment and prioritization of corrective actions deemed necessary and appropriate.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 65
In the context of cloud security, which approach prioritizes incoming data logsfor threat detection by applying multiple sequential filters?
A. Cascade-and-filter approach
B. Parallel processing approach
C. Streamlined single-filter method
D. Unfiltered bulk analysis
Answer: A (LEAVE A REPLY)
TheCascade-and-filter approachis a method used in cloud security to handle incoming data logs efficiently. It prioritizes logs for threat detection byapplying multiple sequential filters, where each filter progressively narrows down the data. This approach helps in:
Layered threat detection:Early filters eliminate non-critical data, while subsequent filters perform more detailed analysis.
Efficient processing:Reduces the volume of data passed through advanced and resource-intensive filters.
Improved accuracy:Allows focusing on the most relevant security events.
For example, in a cloud environment, the first filter might check for known malicious IP addresses, the second might look for suspicious file types, and subsequent filters may perform behavioral analysis or anomaly detection.
Why Other Options Are Incorrect:
B . Parallel processing approach:This method processes logs simultaneously, not sequentially, and is less efficient for prioritizing threats.
C . Streamlined single-filter method:Uses a single filter for all data, which lacks depth and thoroughness in identifying complex threats.
D . Unfiltered bulk analysis:This approach is resource-intensive and inefficient, as it does not prioritize or filter logs.
Reference:
CSA Security Guidance v4.0, Domain 9: Incident Response
Cloud Computing Security Risk Assessment (ENISA) - Log Management and Threat Detection Cloud Controls Matrix (CCM) v3.0.1 - Logging and Monitoring Domain

NEW QUESTION: 66

Which of the following storages is typically used for swap files and other temporary storage needs and is terminated with its instance?

A. Content Deliver

B. Ephemeral Storage

C. Object based Storage

D. Raw Storage

Answer: (SHOW ANSWER)

Ephemeral storage: This type of storage is relevant for SaaS instances and exists only as long as its instance is up. It is typically used for swap files and other temporary storage needs and is terminated with its instance.

NEW QUESTION: 67

What is it called when you lose control of the amount of content on your image store?

A. Data Loss

B. Sprawl

C. Media Contention

D. Media Sanitization

Answer: B (LEAVE A REPLY)

Sprawl occurs when you lose control of the amount of content on your image store. Unnecessary images may be created and run. Each additional image running is another potential point of compromise for an attacker.

NEW QUESTION: 68

Which is the leading industry leading standard you will recommend to a web developer when designing web application or an API for a cloud solution?

A. ISO 27001

B. SOC2

C. FIPS 140

D. OWASP

Answer: (SHOW ANSWER)

OWASP is an open project and is leading industry standard for designing web applications and its security.

NEW QUESTION: 69

What refers refer the model that allows customers to scale their computer and/ or storage needs with little or no intervention from or prior communication with the provider. The services happen in real time?

A. Broad network access

B. On-demand self-service

C. Resource pooling

D. Rapid elasticity

Answer: B (LEAVE A REPLY)
It is the characteristic of 0n-demand self-service that allows customers to scale their computer and/ or storage needs with little or no intervention from or prior communication with the provider

NEW QUESTION: 70
What are the primary security responsibilities of the cloud provider in compute virtualizations?
A. Enforce isolation and configure the security settings
B. Monitor and log workloads and configure the security settings
C. Enforce isolation and maintain a secure virtualization infrastructure
D. Maintain a secure virtualization infrastructure and configure the security settings
E. Enforce isolation and monitor and log workloads
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
What tool allows teams to easily locate and integrate with approved cloud services?
A. Contracts
B. Shared Responsibility Model
C. Service Registry
D. Risk Register
Answer: C (LEAVE A REPLY)
A Service Registry lists approved services, making it easy for teams to find and integrate compliant services. Reference: [CCSK Knowledge Guide, Domain 3 - Risk and Compliance Tools]

NEW QUESTION: 72
Which practice ensures container security by preventing post-deployment modifications?
A. Implementing dynamic network segmentation policies
B. Employing Role-Based Access Control (RBAC) for container access
C. Regular vulnerability scanning of deployed containers
D. Use of immutable containers
Answer: D (LEAVE A REPLY)
Immutable containers are not altered post-deployment, ensuring the integrity of the deployed environment and reducing the risk of unauthorized modifications. Reference: [CCSK v5 Curriculum, Domain 8 - Cloud Workload Security][source 16].

NEW QUESTION: 73
Lack of standard data formats and service interfaces can lead to:
A. Vendor lock out
B. Vendor lock in

C. Denial of Service
D. API Mis-management
Answer: B (LEAVE A REPLY)
Lack of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability, makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-House IT environment.

NEW QUESTION: 74
What is a key component of governance in the context of cybersecurity?
A. Defining roles and responsibilities
B. Standardizing technical specifications for security control
C. Defining tools and technologies
D. Enforcement of the Penetration Testing procedure
Answer: A (LEAVE A REPLY)
A key component of governance in cybersecurity is defining roles and responsibilities. Governance ensures that the right people within an organization are assigned specific duties related to security and that they are held accountable for those responsibilities. This helps establish clear lines of authority and accountability, ensuring that everyone knows what they are responsible for in terms of security practices, policies, and procedures.
While standardizing technical specifications, defining tools and technologies, and enforcing penetration testing are important elements of a cybersecurity strategy, defining roles and responsibilities is essential for overall governance to ensure that security practices are consistently followed.

NEW QUESTION: 75
What is a primary benefit of using Identity and Access Management (IAM) roles/identities provided by cloud providers instead of static secrets?
A. They lower storage costs
B. They reduce the risk of credential leakage
C. They facilitate data encryption
D. They improve system performance
Answer: (SHOW ANSWER)
Using IAM roles/identities provided by cloud providers instead of static secrets (like passwords or API keys) significantly reduces the risk of credential leakage. IAM roles enable dynamic and temporary credentials, meaning that they are automatically rotated and do not need to be manually stored or managed. This eliminates the need for hardcoding sensitive credentials into code or configuration files, which can often lead to accidental exposure or misuse if not properly secured.
Lowering storage costs is not a direct benefit of using IAM roles over static secrets. Facilitating data encryption is important for security, but IAM roles are not specifically

focused on data encryption. Improving system performance is not a primary benefit of using IAM roles over static secrets. The main advantage is security-related, specifically the reduction in credential leakage risks.

NEW QUESTION: 76
Which of the following is a primary purpose of establishing cloud risk registries?
A. In order to establish cloud service level agreements
B. To monitor real-lime cloud performance
C. To manage and update cloud account credentials
D. Identify and manage risks associated with cloud services
Answer: D (LEAVE A REPLY)
A cloud risk registry is primarily used to identify and manage risks associated with cloud services. It serves as a tool for documenting, tracking, and assessing potential risks to the organization that arise from using cloud services. This includes risks related to security, compliance, availability, and performance. The risk registry helps organizations prioritize and mitigate these risks effectively to ensure the security and resilience of their cloud infrastructure.
Establishing SLAs is related to cloud contract management but not the primary purpose of a risk registry.
Monitoring real-time cloud performance is a performance monitoring task, not the focus of a risk registry.
Managing cloud account credentials is an aspect of identity and access management, not related to risk registries.

NEW QUESTION: 77
What is a core tenant of risk management?
A. Risk insurance covers all financial losses, including loss of customers.
B. You can manage, transfer, accept, or avoid risks.
C. If there is still residual risk after assessments and controls are in place, you must accept the risk.
D. The provider is accountable for all risk management.
E. The consumers are completely responsible for all risk.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
One of key focus of ISO 27001 standard is:
A. Find the data breaches in the organization
B. Develop ISMS (Information Security management system)
C. Define organizational structure
D. Put security controls in place
Answer: B (LEAVE A REPLY)
ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).
An ISMS is a systematic approach to managing sensitive company information so that it remains secure.
It includes people, processes and IT systems by applying a risk management process.

NEW QUESTION: 79
Where does the encryption engine and key reside when doing file-level encryption?
A. On the instance attached to the system
B. Encryption engine resides on the server and keys on the client side
C. On the KMS attached to the system
D. On the client side
Answer: (SHOW ANSWER)
File-level encryption: Database servers typically reside on volume storage. For this deployment, you are encrypting the volume or folder of the database, with the encryption engine and keys residing on the instances attached to the volume.
External file system encryption protects from media theft, lost backups, and external attack but does not protect against attacks with access to the application layer, the instances 0S, or the data

NEW QUESTION: 80
What are the encryption options available for SaaS consumers?
A. Client/application and file/folder encryption
B. Object encryption Volume storage encryption
C. Any encryption option that is available for volume storage, object storage, or PaaS
D. Provider-managed and (sometimes) proxy encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which aspects are most important for ensuring security in a hybrid cloud environment?
A. Use of encryption for all data at rest
B. Implementation of robust IAM and network security practices

C. Regular software updates and patch management
D. Deployment of multi-factor authentication only
Answer: B (LEAVE A REPLY)
The correct answer isB. Implementation of robust IAM and network security practices.
Ahybrid cloud environmentinvolves integrating private and public cloud infrastructures. This setup requires enhanced security practices to manage the complexity and diverse security requirements of both environments.
Key Aspects:
Identity and Access Management (IAM):Ensures secure authentication and authorization across both private and public clouds.
Network Security:Includes securing data in transit, implementing network segmentation, and protecting communication between cloud environments.
Unified Security Policies:Establishing consistent policies and access controls across both environments.
Visibility and Monitoring:Continuous monitoring of network traffic and access logs to detect potential threats.
Why Other Options Are Incorrect:
A . Encryption for data at rest:Important but not the most comprehensive security measure for hybrid environments.
C . Software updates and patch management:While essential, these practices alone do not address the complex challenges of a hybrid setup.
D . Multi-factor authentication only:MFA enhances authentication security but does not cover the broader security requirements of a hybrid cloud.
Real-World Context:
Organizations using services likeAWS Direct ConnectorAzure ExpressRouteto integrate on-premises environments with the public cloud must implement robust IAM and network security practices to maintain secure and compliant data flows.
Reference:
CSA Security Guidance v4.0, Domain 7: Infrastructure Security
Cloud Computing Security Risk Assessment (ENISA) - Hybrid Cloud Security Cloud Controls Matrix (CCM) v3.0.1 - Network and IAM Domains

NEW QUESTION: 82
Which of the following is NOT a component of Software Defined Perimeter as defined by Cloud Security Alliance Working group on SDP?
A. SDP Client
B. SDP Controller
C. SDP Gateway
D. SDP Host
Answer: D (LEAVE A REPLY)

The CSA Software Defined Perimeter Working Group has developed a model and specification that combines device and user authentication to dynamically provision network access to resources and enhance security. SDP includes three components:
An SDP client on the connecting asset (e.g. a laptop).
* The SDP controller for authenticating and authorizing SDP clients and configuring the connections to SDP gateways.
* The SDP gateway for terminating SDP client network traffic and enforcing policies in communication with the SDP controller. Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

NEW QUESTION: 83
What is true of security as it relates to cloud network infrastructure?
A. You should apply cloud firewalls on a per-network basis.
B. You should implement a default deny with cloud firewalls.
C. You should implement a default allow with cloud firewalls and then restrict as necessary.
D. You should deploy your cloud firewalls identical to the existing firewalls.
E. You should always open traffic between workloads in the same virtual subnet for better visibility.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following is NOT a key subsystem recommended for monitoring in cloud environments?
A. Network
B. Disk
C. CPU
D. Cable
Answer: D (LEAVE A REPLY)
Network, CPU and Disk(storage) are key subsystems in cloud environment that should be monitored.

NEW QUESTION: 85
What is a cloud workload in terms of infrastructure and platform deployment?
A. A network of servers connected to execute processes
B. A collection of physical hardware used to run applications
C. A single software application hosted on the cloud
D. Application software deployable on infrastructure/platform
Answer: (SHOW ANSWER)
A cloud workload refers to the application software or services that are deployed and run on cloud infrastructure or platform. It can include a variety of computing tasks such as

processing data, running applications, or performing computations, depending on the type of workload. Cloud workloads are typically virtualized and managed within cloud environments, utilizing resources like compute, storage, and networking provided by the cloud infrastructure or platform.
A network of servers connected to execute processes refers more to the underlying infrastructure, not the workload itself. A collection of physical hardware used to run applications describes the infrastructure, not the workload. A single software application hosted on the cloud is a partial description but doesn't capture the broader concept of workloads, which could include multiple services or applications.

NEW QUESTION: 86
What is a key advantage of using Policy-Based Access Control (PBAC) for cloud-based access management?
A. PBAC eliminates the need for defining and managing user roles and permissions.
B. PBAC is easier to implement and manage compared to Role-Based Access Control (RBAC).
C. PBAC allows enforcement of granular, context-aware security policies using multiple attributes.
D. PBAC ensures that access policies are consistent across all cloud providers and platforms.
Answer: C (LEAVE A REPLY)
PBAC enables highly specific access control based on multiple attributes, enhancing flexibility and security in cloud environments. Reference: [CCSK v5 Curriculum, Domain 5 - IAM][source 16].

NEW QUESTION: 87
What process involves an independent examination of records, operations, processes, and controls within an organization to ensure compliance with cybersecurity policies, standards, and regulations?
A. Risk assessment
B. Audit
C. Penetration testing
D. Incident response
Answer: (SHOW ANSWER)
Auditing is an independent review process that validates adherence to policies, regulations, and standards. It is essential in assessing security posture. Reference: [Security Guidance v5, Domain 3 - Compliance]
[16†source].

NEW QUESTION: 88

In the context of Software-Defined Networking (SDN), what does decoupling the network control plane from the data plane primarily achieve?

A. Enables programmatic configuration

B. Decreases network security

C. Increases hardware dependency

D. Increases network complexity

Answer: (SHOW ANSWER)

The correct answer isA. Enables programmatic configuration.

InSoftware-Defined Networking (SDN), the control plane and data plane are decoupled, meaning that thenetwork intelligence (control plane)is separated from thetraffic forwarding functions (data plane). This separation allows network control to be directly programmable, rather than embedded within the hardware.

Key Benefits of Decoupling:

Programmatic Configuration:Network administrators can program the network dynamically using software applications. This programmability enablesautomated, flexible, and efficient network management.

Centralized Control:The control plane is managed from acentralized controller, which can adjust network configurations in real-time.

Reduced Hardware Dependency:Since the control logic is no longer embedded in individual hardware devices, it is easier to use commodity hardware andstandardized interfaces.

Agility and Scalability:Organizations can rapidly deploy new services and update configurations without altering the underlying hardware.

Why Other Options Are Incorrect:

B . Decreases network security:Decoupling does not inherently decrease security. In fact, centralized control can enhance security through consistent policy enforcement.

C . Increases hardware dependency:The opposite is true. SDN reduces dependency on proprietary hardware by enabling software-based management.

D . Increases network complexity:While SDN introduces new software components, it simplifies network management bycentralizing control and reducing hardware configuration complexities.

Real-World Example:

In a cloud environment, SDN controllers likeOpenDaylightorCisco ACIallow fordynamic routing,load balancing, andtraffic managementthrough APIs. This flexibility supportsautomated scaling and traffic optimization.

Reference:

CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - SDN and Network Virtualization

Cloud Controls Matrix (CCM) v3.0.1 - Network Security Domain

NEW QUESTION: 89

A framework of containers for all components of application security. best practices. catalogued and leveraged by the ORGANIZATION is called:

A. ANF

B. ONF

C. CAF

D. DAF

Answer: B (LEAVE A REPLY)

Please notice that the question is asked for the organisation and therefore, ONF is the correct answer. If the similar question is asked for a particular application then answer would ANF

NEW QUESTION: 90

Which of the following is a common risk factor related to misconfiguration and inadequate change control in cybersecurity?

A. Failure to update access controls after employee role changes

B. Lack of sensitive data encryption

C. Lack of 3rd party service provider specialized in patch management procedures

D. Excessive SBOM focus

Answer: A (LEAVE A REPLY)

Correct Option: A. Failure to update access controls after employee role changes This falls under one of the most common risk factors related to cloud misconfiguration and poor change management. Misconfiguration errors often stem from insufficient change control, especially in dynamic environments like the cloud. According to CSA's Security Guidance v4.0, poor governance of identity and access management (IAM) changes - such as not updating access privileges when user roles change - introduces serious security risks.

"Cloud computing is dynamic by nature. This places more importance on automation and proper governance, especially for identity and access control. Failure to remove or update access permissions after personnel changes leads to orphaned or over-permissioned accounts, which are prime targets for attackers."

- Domain 2: Governance and Enterprise Risk Management, CSA Security Guidance v4.0

Also highlighted in ENISA's Cloud Risk Assessment:

"Loss of governance includes failing to maintain proper control over access privileges and role assignments. Poor change management and inadequate configuration reviews can leave systems open to unauthorized access."

- ENISA Cloud Computing Risk Assessment, Section R.2: Loss of Governance Why the Other Options Are Incorrect:

B . Lack of sensitive data encryption: While encryption is critical, it is not directly tied to change control or misconfiguration, but rather falls under Data Security and Encryption domain.

C . Lack of 3rd party service provider specialized in patch management procedures: This refers more to vendor management and Security-as-a-Service, not internal change control or misconfigurations.
D . Excessive SBOM focus: Software Bill of Materials (SBOM) is important for supply chain transparency, but excessive focus on it isn't a typical misconfiguration or change control risk.
Reference:
CSA Security Guidance v4.0 - Domain 2: Governance and Enterprise Risk Management
ENISA Cloud Computing Security Risk Assessment - R.2 Loss of Governance

NEW QUESTION: 91
What would you call logic/procedures running on a shared database platform as?
A. Virtual Machine
B. Container
C. Platform-based Workload
D. Serverless Computing
Answer: C (LEAVE A REPLY)
Platform-based workloads: This is a more complex category that covers workloads running on a shared platform that aren't virtual machines or containers, such as logic/procedures running on a shared database platform. Imagine a stored procedure running inside a multitenant database, or a machine- learning job running on a machine-learning Platform as a Service. Isolation and security are totally the responsibility of the platform provider, although the provider may expose certain security options and controls.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

NEW QUESTION: 92
Which of the following is a common exploitation factor associated with serverless and container workloads?
A. Poor Documentation
B. Misconfiguration
C. Insufficient Redundancy
D. Low Availability

Answer: B (LEAVE A REPLY)
Misconfiguration is one of the most prevalent risks in serverless and container-based environments. Given the complex nature of container orchestration (e.g., Kubernetes), CI/CD pipelines, and ephemeral infrastructure, simple missteps-such as overly permissive roles or exposed ports-can lead to significant vulnerabilities.
These workloads require strict configuration management, automated scanning, and secure defaults to prevent breaches. Unlike traditional servers, containers and functions spin up and down rapidly, making traditional visibility tools insufficient.
This is discussed thoroughly inDomain 8: Virtualization and Containers, where the CCSK guidance identifies misconfiguration as a leading cause of cloud-native exploitation.
Reference:CSA Security Guidance v4.0 - Domain 8: Virtualization and Containers

NEW QUESTION: 93
Who is responsible for the safe custody, transport, data storage. and implementation of business rules in relation to the privacy?
A. Data controller
B. Data owner
C. Data custodian
D. Data processor
Answer: C (LEAVE A REPLY)
Data custodians are responsible for the safe custody. transport. data storage. and implementation of business rules

NEW QUESTION: 94
ENISA: A reason for risk concerns of a cloud provider being acquired is:
A. Arbitrary contract termination by acquiring company
B. Mass layoffs may occur
C. Resource isolation may fail
D. Provider may change physical location
E. Non-binding agreements put at risk
Answer: E (LEAVE A REPLY)

NEW QUESTION: 95
Which of the following processes leverages virtual network topologies to run more smaller and more isolated networks without incurring additional hardware costs?
A. VLANs
B. Grid networking
C. Micro-segmentation
D. Converged Networking
Answer: C (LEAVE A REPLY)
Explanation:

This type of question are asked to create confusion.
Following are the five phases of SDLC:
1. Planning and requirements analysis: Business and security requirements and standards are being determined. This phase is the main focus of the project managers and stakeholders. Meetings with managers, stakeholders, and users are held to determine requirements. The software development lifecycle calls for all business requirements(functional and nonfunctional)to be defined even before initial design begins. Planning for the quality-assurance requirements and identification of the risks associated with the project are also conducted in the planning stage. The requirements are then analyzed for their validity and the possibility of incorporating them into the system to be developed.
2. Defining: The defining phase is meant to clearly define and document the product requirements to place them in front of the customers and get them approved. This is done through a requirement specification document, which consists of all the product requirements to be designed and developed during the project lifecycle.
3. Designing: System design helps in specifying hardware and system requirements and helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model. Threat modeling and secure design elements should be undertaken and discussed here.
4. Developing: Upon receiving the system design documents, work is divided into modules or units and actual coding starts. This is typically the longest phase of the software development lifecycle. Activities include code review, unit testing, and static analysis.
5. Testing: After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase. During this phase, unit testing, integration testing, system testing, and acceptance testing are conducted.

NEW QUESTION: 96
Cloud customer and cloud service provider are jointly responsible legally for data breach or data loss in absence of any written clause regarding same in contract or SLA.
A. True
B. False
Answer: B (LEAVE A REPLY)
This is false, because, unless, specified cloud customer is legally liable for any loss to data

NEW QUESTION: 97
Ben was working on a project and hosted all its data on a public cloud. The project is now complete and he wants to remove the data Which of the following is best option for him in order to leave no remanence?
A. Data-overwriting
B. Physically destroy the media

C. Cryptographic erasure
D. Zeroing
Answer: C (LEAVE A REPLY)
All the options given are correct methods of destroying data but when it comes to data in cloud. the most suitable method is cryptographic erasure.
Definition: Cryptographic Erasure
Cryptographic erasure is the process of using encryption software (either built-in or deployed) on the entire data storage device. and erasing the key used to decrypt the data.

NEW QUESTION: 98
Which of the following best describes how cloud computing manages shared resources?
A. Through virtualization, with administrators allocating resources based on SLAs
B. Through abstraction and automation to distribute resources to customers
C. By allocating physical systems to a single customer at a time
D. Through manual configuration of resources for each user need
Answer: B (LEAVE A REPLY)
Cloud computing uses abstraction and automation to pool and distribute resources efficiently among multiple tenants. This allows dynamic allocation based on demand.
Reference: [CCSK v5 Curriculum, Domain 1 - Cloud Computing Models]

NEW QUESTION: 99
The basis for deciding which laws are most appropriate in a situation where conflicting laws exist. refers to:
A. The Restatement(Second) Conflict of Law
B. Doctrine of proper law
C. Tort law
D. Criminal law
Answer: (SHOW ANSWER)
The Restatement(Second) Conflict of Law refers to a collation of developments in common law that help the courts stay up with changes. Many states have conflicting laws. and judges use these restatements to assist them in determining which laws should apply when conflicts occur.

NEW QUESTION: 100
Why is consulting with stakeholders important for ensuring cloud security strategy alignment?
A. IT simplifies the cloud platform selection process
B. It reduces the overall cost of cloud services.
C. It ensures that the strategy meets diverse business requirements.
D. It ensures compliance with technical standards only.
Answer: C (LEAVE A REPLY)

Consulting with stakeholders is crucial for ensuring that the cloud security strategy aligns with the overall business objectives and needs. Stakeholders - such as business leaders, IT teams, legal, and compliance officers - bring unique perspectives on what the cloud strategy needs to accomplish, from security to compliance, scalability, and performance. By involving stakeholders, organizations can ensure that the security strategy supports business goals, addresses various concerns, and is comprehensive.
Simplifying the cloud platform selection process is a potential benefit but not the primary reason for consulting stakeholders. Selecting the right cloud platform is part of the broader strategy. Reducing the overall cost of cloud services is not necessarily the outcome of involving stakeholders, although cost considerations may be part of the discussion.
Ensuring compliance with technical standards only is too narrow; stakeholders help ensure compliance with both technical and business requirements.

NEW QUESTION: 101
What is a primary objective of cloud governance in an organization?
A. Implementing multi-tenancy and resource pooling.
B. To align cloud usage with corporate objectives
C. Simplifying scalability and automating resource management
D. Enhancing user experience and reducing latency
Answer: B (LEAVE A REPLY)
The primary objective of cloud governance in an organization is to align cloud usage with corporate objectives. Cloud governance ensures that the cloud resources, services, and strategies are used effectively and efficiently, supporting the organization's overall goals and priorities. It involves establishing policies, compliance measures, and management practices to ensure that cloud adoption and usage are aligned with business needs, security requirements, and regulatory obligations.
Implementing multi-tenancy and resource pooling is important for cloud infrastructure but is more related to the underlying technology rather than governance. Simplifying scalability and automating resource management are benefits of cloud environments, but they are more about cloud architecture and operations than governance. Enhancing user experience and reducing latency are concerns of performance optimization and user interface design, not the primary focus of cloud governance.

NEW QUESTION: 102
Which one of the following is an example of misuse or abuse of cloud services?
A. DDoS Attack
B. Account Hijacking
C. XSS attacks
D. Honeypot
Answer: A (LEAVE A REPLY)
Public cloud platform can be used to launch DDoS attack on other platforms.

Please note here and understand the meaning of phrase "abuse or misuse of cloud Services" This phrase means to launch attacks or campaign by using cloud as a platform. mostly. public cloud.

NEW QUESTION: 103
Which of the following is typically a policy set that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location?
A. Intrusion Detection System
B. Security Groups
C. API Gateway
D. Database Activity Monitor
Answer: (SHOW ANSWER)
SDN firewalls (e.g, security groups) can apply to assets based on more flexible criteria than hardware- based firewalls, since they aren't limited based on physical topology. (Note that this is true of many types of software firewalls, but is distinct from hardware firewalls). SDN firewalls are typically policy sets that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location (within a given virtual network).
Reference: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

NEW QUESTION: 104
What of the following is NOT an essential characteristic of cloud computing?
A. Measured Service
B. Resource Pooling
C. Third Party Service
D. Rapid Elasticity
E. Broad Network Access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Which type of AI workload typically requires large data sets and substantial computing resources?
A. Evaluation
B. Data Preparation
C. Training
D. Inference
Answer: C (LEAVE A REPLY)
Among AI workloads,Trainingrequires themost computational power and data resources.
Why AI Training is Computationally Intensive?
Large datasets:

AI models (e.g., deep learning, neural networks)require millions or billions of labeled data points.
Training involvesprocessing massive amounts of structured/unstructured data.
High computational power:
Training deep learning modelsinvolves runningmultiple passes (epochs) over data, adjusting weights, and optimizing parameters.
Requiresspecialized hardwarelikeGPUs (Graphics Processing Units),TPUs (Tensor Processing Units), andHPC (High-Performance Computing).
Long training times:
AI model training can takedays, weeks, or even monthsdepending on complexity.
Cloud platforms offerdistributed computing (multi-GPU training, parallel processing, auto-scaling).
Cloud AI Training Benefits:
Cloud providers (AWS, Azure, GCP) offer ML training serviceswithon-demand scalable compute instances.
Supportsframeworks like TensorFlow, PyTorch, and Scikit-learn.
This aligns with:
CCSK v5 - Security Guidance v4.0, Domain 14 (Related Technologies - AI and ML Security) Cloud AI Security Risks and AI Data Governance (CCM - AI Security Controls)

NEW QUESTION: 106
Which governance domain focuses on proper and adequate incident detection, response, notification, and remediation?
A. Data Security and Encryption
B. Information Governance
C. Compliance and Audit Management
D. Infrastructure Security
E. Incident Response, Notification and Remediation
Answer: (SHOW ANSWER)

NEW QUESTION: 107

In preparing for cloud incident response, why is updating forensics tools for virtual machines (VMs) and containers critical?

A. To comply with cloud service level agreements (SLAs)

B. To streamline communication with cloud service providers and customers

C. To ensure compatibility with cloud environments for effective incident analysis

D. To increase the speed of incident response team deployments

Answer: (SHOW ANSWER)

Updating forensics tools for virtual machines (VMs) and containers is critical because cloud environments can differ significantly from traditional on-premises environments. As cloud technologies evolve, it is important to ensure that forensic tools are compatible with the latest cloud infrastructure, such as VMs, containers, and serverless architectures. This ensures that the tools can effectively collect, analyze, and preserve evidence in the event of a security incident, allowing for accurate and efficient incident analysis.

Complying with cloud service level agreements (SLAs)) is not the primary reason for updating forensics tools, although some SLAs may require certain levels of incident response capabilities. Streamlining communication with cloud service providers and customers) is important, but the primary concern is the ability to analyze incidents, not just communication. Increasing the speed of incident response team deployments) is a consideration, but ensuring the tools are up to date and compatible is the main priority for effective incident analysis.

NEW QUESTION: 108

Which cloud service model requires the customer to manage the operating system and applications?

A. Platform as a Service (PaaS)

B. Network as a Service (NaaS)

C. Infrastructure as a Service (IaaS)

D. Software as a Service (SaaS)

Answer: (SHOW ANSWER)

In the Infrastructure as a Service (IaaS) model, the cloud provider delivers the basic infrastructure components such as virtual machines, storage, and networking resources. However, the customer is responsible for managing the operating system, applications, and any software configurations that run on the infrastructure.

This gives the customer more control over the environment while still benefiting from the cloud provider's hardware and scalability.

The provider manages the operating system, runtime, and infrastructure, and the customer is only responsible for managing the applications. NaaS focuses on network services, not the management of operating systems and applications. The provider manages everything, including the operating system and applications, and the customer simply uses the software.

NEW QUESTION: 109
Which approach is commonly used by organizations to manage identities in the cloud due to the complexity of scaling across providers?
A. Decentralization
B. Centralization
C. Federation
D. Outsourcing
Answer: (SHOW ANSWER)
Managing identities across multiple cloud providers is complex due to the need for scalability, interoperability, and consistent access control. Thefederationapproach is commonly used to address this challenge. Identity federation allows organizations to use a single set of credentials across different cloud providers by leveraging standards such as SAML, OAuth, or OpenID Connect. This enables seamless authentication and authorization without requiring separate identity management systems for each provider.
From theCCSK v5.0 Study Guide, Domain 6 (Identity, Entitlement, and Access Management), Section
6.3:
"Identity federation is a critical approach for managing identities in cloud environments, especially when scaling across multiple providers. Federation allows organizations to use a trusted identity provider (IdP) to authenticate users, enabling single sign-on (SSO) and consistent access control across disparate cloud services." Option C (Federation) is the correct answer.
* Option A (Decentralization) is incorrect because decentralizing identity management increases complexity and reduces consistency across providers.
* Option B (Centralization) is incorrect because, while centralized identity management may be used within a single organization, it does not scale effectively across multiple cloud providers without federation.
* Option D (Outsourcing) is incorrect because outsourcing identity management does not inherently address the scalability and interoperability challenges of cloud environments.
References:
CCSK v5.0 Study Guide, Domain 6, Section 6.3: Identity Federation.
CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Domain 11.

NEW QUESTION: 110
Who is responsible for the security of the physical infrastructure and virtualization platform?
A. The cloud provider
B. It depends on the agreement
C. The responsibility is split equally
D. The majority is covered by the consumer
E. The cloud consumer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?
A. Planned Outages
B. Resiliency Planning
C. Expected Engineering
D. Chaos Engineering
E. Organized Downtime
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 112
Which of the following is the key difference between cloud computing and traditional virtualization?
A. Abstraction
B. Classification
C. Isolation
D. Orchestration
Answer: (SHOW ANSWER)
Orchestration is the difference between cloud computing and traditional virtualization; virtualization abstracts resources. but it typically lacks the orchestration to pool them together and deliver them to customers on demand. instead relying on manual processes.
Ref: CSA Security Guidelines V4.0

NEW QUESTION: 113
Which statement best describes the impact of Cloud Computing on business continuity management?
A. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
B. The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.
C. Geographic redundancy ensures that Cloud Providers provide highly available services.
D. A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
E. Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
Answer: (SHOW ANSWER)

NEW QUESTION: 114

In the Incident Response Lifecycle, which phase involves identifying potential security events and examining them for validity?

A. Post-Incident Activity

B. Detection and Analysis

C. Preparation

D. Containment, Eradication, and Recovery

Answer: B (LEAVE A REPLY)

The Detection and Analysis phase involves identifying incidentsand determining their impact. It is crucial to validate events to understand if they constitute a security incident.

Reference: [Security Guidance v5, Domain 11 - Incident Response]

NEW QUESTION: 115

GRC is responsibility of _____ in the all cloud services models

A. Customer

B. Service Provider

C. Reseller

D. Cloud Access Security Broker(CASB)

Answer: (SHOW ANSWER)

GRC and data is responsibility of the customer in all service models according to shared responsibility model.

NEW QUESTION: 116

The individual's right to have data(PII) removed from a entity/ provider at anytime per their request. is known as:

A. Right of erasure

B. Right to be forgotten

C. Right to claim

D. Right to disclosure

Answer: B (LEAVE A REPLY)

Under this principle of "Right to be forgotten", any individual can notify any entity that has PII fort hat individual and instruct that entity to delete and destroy all of that individual's PII in that entity's control.

This is a very serious and powerful individual right, and compliance can be extremely difficult.

NEW QUESTION: 117

Which of the following best describes a primary focus of cloud governance with an emphasis on security?

A. Enhancing user experience with intuitive interfaces.

B. Maximizing cost savings through resource optimization.

C. Increasing scalability and flexibility of cloud solutions.
D. Ensuring compliance with regulatory requirements and internal policies.
Answer: D (LEAVE A REPLY)
Cloud governancefocuses onsecurity, risk management, and complianceto ensuredata protection, audit readiness, and regulatory adherence.
Key Elements of Cloud Security Governance:
Regulatory Compliance:
Organizations must comply withGDPR, HIPAA, PCI DSS, ISO 27001.
Cloud Security Posture Management (CSPM)helpsenforce complianceautomatically.
Security Policies & Controls:
Cloud governance frameworks includeIAM (Identity and Access Management), encryption policies, and workload isolation.
Organizations muststandardize security settingsacross multiple cloud environments.
Audit & Risk Management:
Implementcontinuous monitoring, security logging, and forensic readiness.
Risk-based access control policiesensuredata security across workloads.
Data Protection & Privacy:
Enforcingcloud-native security frameworks (e.g., Zero Trust, CASB, SIEM).
Data retention, access control, andincident responseareessential governance practices.
This is covered in:
CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Risk Management) Cloud Security Alliance's Cloud Controls Matrix (CCM) - Cloud Governance and Compliance Standards

NEW QUESTION: 118
Which of the following document defines the roles and responsibilities for risk management between a cloud provider and a cloud customer?
A. Risk Management Agreement
B. Service Level Agreement
C. Operational level Agreement
D. Contract
Answer: D (LEAVE A REPLY)
Contract defines defines the roles and responsibilities for risk management between a cloud provider and a cloud customer

NEW QUESTION: 119
What is the most effective way to identify security vulnerabilities in an application?
A. Performing code reviews of the application source code just prior to release
B. Relying solely on secure coding practices by the developers without any testing
C. Waiting until the application is fully developed and performing a single penetration test
D. Conducting automated and manual security testing throughout the development

Answer: (SHOW ANSWER)
The most effective way to identify security vulnerabilities in an application is to conduct automated and manual security testing throughout the development lifecycle. This approach ensures that security is continuously evaluated at every stage of development, rather than waiting until the end. Automated tools can help identify common vulnerabilities quickly, while manual testing allows for more in-depth analysis, including testing for complex, contextual security issues. This proactive and ongoing approach reduces the risk of vulnerabilities being overlooked and helps ensure that security is integrated into the application from the start.
Performing code reviews just prior to release is valuable, but it's not comprehensive enough. Security testing should be done early and continuously, not just before release.
Relying solely on secure coding practices is important but not sufficient. Even with secure coding practices, testing is essential to identify vulnerabilities.
Waiting for a single penetration test after development is not effective because waiting until the end can allow many vulnerabilities to go unnoticed during development, leaving the application exposed.

NEW QUESTION: 120
According to Cloud Security Alliance logical model of cloud computing, which of the following defines the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers.
A. Metastructure
B. Infostructure
C. Infrastructure
D. Applistructure
Answer: A (LEAVE A REPLY)
According to CSA Securityguidelines4.0. Metastucture is defined as the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.

NEW QUESTION: 121
Which benefit of automated deployment pipelines most directly addresses continuous security and reliability?
A. They enable consistent and repeatable deployment processes
B. They enhance collaboration through shared tools
C. They provide detailed reports on team performance
D. They ensure code quality through regular reviews
Answer: (SHOW ANSWER)
The most direct benefit of automated deployment pipelines in addressing continuous security and reliability is that they enable consistent and repeatable deployment processes. This ensures that the same steps are followed every time code is deployed, reducing

human error and inconsistencies that could introduce vulnerabilities or reliability issues. Automated pipelines can also include security checks, such as static code analysis, vulnerability scanning, and automated testing, all of which help ensure that security and reliability are maintained continuously.
Enhancing collaboration through shared tools is a benefit of automated pipelines but doesn't directly address security and reliability. Providing detailed reports on team performance is useful for team management but doesn't directly contribute to security or reliability. Ensure code quality through regular reviews can improve security indirectly but is not the most direct benefit when it comes to continuous security and reliability in the deployment process.

NEW QUESTION: 122
Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?
A. Chaos Engineering
B. Resiliency Planning
C. Expected Engineering
D. Planned Outages
E. Organized Downtime
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
What is a key advantage of using Policy-Based Access Control (PBAC) for cloud-based access management?
A. PBAC eliminates the need for defining and managing user roles and permissions.
B. PBAC is easier to implement and manage compared to Role-Based Access Control (RBAC).
C. PBAC allows enforcement of granular, context-aware security policies using multiple attributes.
D. PBAC ensures that access policies are consistent across all cloud providers and platforms.
Answer: (SHOW ANSWER)

PBAC enables highly specific access control based on multiple attributes, enhancing flexibility and security in cloud environments. Reference: [CCSK v5 Curriculum, Domain 5 - IAM][16 source].

NEW QUESTION: 124
In preparing for cloud incident response, why is it crucial to establish a cloud deployment registry?
A. To maintain a log of all incident response activities and have efficient reporting
B. To document all cloud services APIs
C. To list all cloud-compliant software
D. To track incident support options, know account details, and contact information
Answer: D (LEAVE A REPLY)
Establishing a cloud deployment registry is crucial for cloud incident response because it helps track critical information related to the cloud environment, such as incident support options, account details, and contact information for cloud service providers (CSPs). This registry provides a central place where key details about cloud services and deployments are documented, allowing the incident response team to quickly access necessary information, escalate issues to the appropriate CSP support teams, and coordinate response efforts effectively.

NEW QUESTION: 125
Which of the following is NOT atypical approach of Key Storage in cloud?
A. Internally managed
B. Externally managed
C. Cloud Service Provider Managed
D. Managed by the Third part
Answer: C (LEAVE A REPLY)
Remember, two key considerations when doing key management
1) Do not save it alongside data
2) Do not let cloud service provider manage the keys

NEW QUESTION: 126
What is the primary purpose of Cloud Infrastructure Entitlement Management (CIEM) in cloud environments?
A. Monitoring network traffic
B. Deploying cloud services
C. Governing access to cloud resources
D. Managing software licensing
Answer: C (LEAVE A REPLY)
Cloud Infrastructure Entitlement Management (CIEM) is primarily designed togovern access to cloud resources. It addresses the challenges of managing user entitlements and

permissions across multi-cloud and hybrid environments. CIEM solutions help organizations manageidentity and access rights, particularly in complex cloud infrastructures where multiple services and user roles are involved.
The primary functions of CIEM include:
* Access Governance:Ensuring that the right users have the appropriate level of access to cloud resources.
* Least Privilege Enforcement:Automatically identifying and eliminating excessive permissions.
* Access Monitoring and Auditing:Continuously tracking permission usage to detect unusual patterns or risks.
* Identity Lifecycle Management:Managing the creation, modification, and revocation of identities and their associated permissions.
Why CIEM is Important:
As cloud environments scale, manual management of user roles and permissions becomes unmanageable and prone to errors. CIEM tools automate this process, providingvisibility and control over cloud entitlementsto minimize the risk ofprivilege escalation and unauthorized access.
Why Other Options Are Incorrect:
* A. Monitoring network traffic:This falls under network security monitoring and is not related to entitlement management.
* B. Deploying cloud services:This involves cloud orchestration and provisioning, not entitlement management.
* D. Managing software licensing:CIEM is not concerned with license management, which is handled by software asset management tools.
References:
CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management
Cloud Computing Security Risk Assessment (ENISA) - Identity and Access Management
Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

NEW QUESTION: 127
Which of the followingIS0 Standard provides Code of practice for information security controls based on IS0/IEC 27002for cloud services?
A. ISO 27018
B. ISO 27034
C. ISO 27032
D. ISO 27017
Answer: (SHOW ANSWER)
IS0 27017 provides Code of practice for information security controls based on ISO/IEC27002 for cloud services.

NEW QUESTION: 128

Which of the following is a primary benefit of using Infrastructure as Code (IaC) in a security context?

A. Manual patch management

B. Ad hoc security policies

C. Static resource allocation

D. Automated compliance checks

Answer: D (LEAVE A REPLY)

The correct answer isD. Automated compliance checks.

Infrastructure as Code (IaC)is a key DevSecOps practice where infrastructure configurations are defined and managed through code. In a security context, the primary benefit of using IaC is the ability toautomate compliance checksand enforce security best practices consistently across environments.

Key Benefits of IaC in Security:

Automated Compliance:IaC allows for the embedding ofsecurity policies directly into configuration scripts.

This means that when infrastructure is deployed, it automatically adheres to compliance requirements (like NIST, CIS benchmarks).

Consistency and Repeatability:Since IaC scripts are version-controlled, any configuration changes are tracked, minimizing the risk ofconfiguration drift.

Security by Design:By coding security configurations (like IAM roles, network ACLs, encryption settings), organizations ensure that every deployment meets security standards.

Reduced Human Error:Automating infrastructure provisioning reduces manual errors that can lead to vulnerabilities.

Why Other Options Are Incorrect:

A: Manual patch management:IaC promotes automated and repeatable configurations, reducing the need for manual patching.

B: Ad hoc security policies:IaC encouragesstandardized and consistentpolicies rather than ad hoc management.

C: Static resource allocation:IaC is dynamic and scalable, allowing for automatic scaling and configuration management rather than static resource setups.

Real-World Example:

Using tools likeTerraformorAWS CloudFormation, organizations can defineIAM policies, security group rules, and data encryption settingsas part of the infrastructure code. These configurations are then automatically checked for compliance against established policies during deployment.

Security and Compliance in IaC:

Organizations can integrate tools likeTerraform ComplianceorAWS Config Rulesto automatically verify that infrastructure settings align withregulatory requirementsandinternal security policies.

References:

CSA Security Guidance v4.0, Domain 10: Application Security
Cloud Computing Security Risk Assessment (ENISA) - Infrastructure as Code Best Practices Cloud Controls Matrix (CCM) v3.0.1 - Configuration and Change Management Domain

NEW QUESTION: 129
Which ISO standards addresses Privacy in the cloud environment?
A. ISO 27017
B. ISO 27018
C. ISO 27034
D. ISO 27032
Answer: B (LEAVE A REPLY)
ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

NEW QUESTION: 130
As we move from Software as a Service Model towards Infrastructure as a service Model. security responsibility decreases from towards cloud consumer from that of Cloud Service Provider.
A. True
B. False
Answer: B (LEAVE A REPLY)
The answer is False. This is a very tricky question and it has to be read and understood well before answering.
It is always the other way around. Cloud consumer's security increases when you move from Software as a service model to Infrastructure as a Service Model.

NEW QUESTION: 131
Whose responsibility is to maintain security incident and event management(SIEM) capabilities in PaaS (Platform as a Service) model?
A. Cloud Carrier
B. Cloud Service provider
C. Cloud Customer
D. Cloud Access Security Broker
Answer: B (LEAVE A REPLY)
In forms of service models, it is cloud service provider's responsibility to maintain security incident and event management(SIEM) capabilities

NEW QUESTION: 132

What are the most important practices for reducing vulnerabilities in virtual machines (VMs) in a cloud environment?

A. Disabling unnecessary VM services and using containers

B. Encryption for data at rest and software bill of materials

C. Using secure base images, patch and configuration management

D. Network isolation and monitoring

Answer: (SHOW ANSWER)

To reduce vulnerabilities in virtual machines (VMs) in a cloud environment, it is critical to use secure base images that are free from known vulnerabilities, ensure regular patching to fix any discovered security issues, and implement configuration management to ensure that VMs are properly configured according to security best practices. This combination of practices ensures that VMs are both secure from the start and remain secure over time as new vulnerabilities are discovered.

Disabling unnecessary VM services and using containers is a good security practice but does not directly address vulnerabilities in VMs specifically. Encryption and SBOM is important for securing data and understanding dependencies but does not specifically focus on reducing vulnerabilities in VMs. Network isolation and monitoring are key network security practices but do not directly address the security of the VMs themselves.

NEW QUESTION: 133

CCM: The following list of controls belong to which domain of the CCM?

GRM 06 - Policy GRM 07 - Policy Enforcement GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews GRM 10 - Risk Assessments GRM 11 - Risk Management Framework

A. Governance and Retention Management

B. Governance and Risk Management

C. Governing and Risk Metrics

Answer: B (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 134

How is encryption managed on multi-tenant storage?

A. Multiple keys per data owner

B. One key per data owner

C. C for data subject to the EU Data Protection Directive; B for all others

D. Single key for all data owners

E. The answer could be A, B, or C depending on the provider

Answer: B (LEAVE A REPLY)

NEW QUESTION: 135

Which term describes any situation where the cloud consumer does

not manage any of the underlying hardware or virtual machines?
A. Virtual machineless
B. Serverless computing
C. Container
D. Provider managed
E. Abstraction
Answer: (SHOW ANSWER)

NEW QUESTION: 136
When creating business strategies for cloud migration. which is the most important aspect?
A. Due Diligence when inspecting technologies and choosing cloud provider
B. Choosing the right auditor
C. Hiring a cloud broker
D. Valuating current staff for their capabilities
Answer: A (LEAVE A REPLY)
Due Diligence is most important aspect when considering adoption to the cloud

NEW QUESTION: 137
How does cloud adoption impact incident response processes in cybersecurity?
A. It only affects data storage and not incident response
B. It has no significant impact on incident response processes
C. It simplifies incident response by consolidating processes
D. It introduces different processes, technologies, and governance models
Answer: D (LEAVE A REPLY)
Cloud adoption transforms how incident response (IR) is conducted. Unlike traditional IT environments, cloud environments involve shared responsibility, provider collaboration, and remote orchestration. This shift requires security teams to adjust response strategies, tools, and governance to effectively detect, analyze, and remediate incidents.
Cloud-specific tools (e.g., CSP logs, API calls, auto-scaling environments) must be incorporated into IR plans. Coordination with cloud service providers is often necessary to access logs, enforce controls, or conduct forensics.

This transformation is outlined in Domain 9: Incident Response, which stresses that effective IR in the cloud must be pre-planned and adapted to each provider and cloud model.
Reference:
CSA Security Guidance v4.0 - Domain 9: Incident Response

NEW QUESTION: 138
Which of the following leverages virtual network topologies to run more. smaller. and more isolated networks without incurring additional hardware costs that historically make such models prohibitive?
A. VLANS
B. Micro LANs
C. Micro segmentation
D. BitVLANS
Answer: C (LEAVE A REPLY)
Micro segmentation(also sometimes referred to as hyper segregation) leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive. Since the entire networks are defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software- defined environments.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

NEW QUESTION: 139
Why is identity management at the organization level considered a key aspect in cybersecurity?
A. It replaces the need to enforce the principles of the need to know
B. It ensures only authorized users have access to resources
C. It automates and streamlines security processes in the organization
D. It reduces the need for regular security training and auditing, and frees up cybersecurity budget
Answer: B (LEAVE A REPLY)
Identity management at the organizational level is a key aspect of cybersecurity because it ensures that only authorized users can access specific resources, systems, or data. By controlling and managing user identities, roles, and permissions, identity management helps enforce security policies, preventing unauthorized access and potential breaches. This is a fundamental practice in maintaining confidentiality, integrity, and availability within an organization.

NEW QUESTION: 140
Which of the following are two most effective ways of protection against data breaches in the cloud environment?

A. Contracts and SLAs
B. Data Loss Prevention techniques and Web Application Firewall
C. Encryption and Honeypot
D. Multifactor Authentication and Encryption
Answer: D (LEAVE A REPLY)
Multifactor Authentication and Encryption are most effective protect mechanisms against data breaches in cloud environment. Other options do form part of overall security strategy in cloud but Option D is the strongest contender for the answer.

NEW QUESTION: 141
Which of the following is a common security issue associated with serverless computing environments?
A. High operational costs
B. Misconfigurations
C. Limited scalability
D. Complex deployment pipelines
Answer: (SHOW ANSWER)
Serverless environments are vulnerable to misconfigurations, which can expose sensitive data and resources, making security configurations critical. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security][16†source].

NEW QUESTION: 142
In which deployment model should the governance strategy consider the minimum common set of controls comprised of the Cloud Service Provider contract and the organization's internal governance agreements?
A. Hybrid
B. Public
C. PaaS
D. Private
E. IaaS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
Which of following is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor?
A. VM rootkit
B. VM Escape
C. VM HBR
D. VM DOS
Answer: B (LEAVE A REPLY)

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker access to the host operating system and all other virtual machines(VMs) running on that host.

NEW QUESTION: 144
Which of the following is true about access policies in cybersecurity?
A. They are used to monitor real-time network traffic
B. They are solely concerned with user authentication methods
C. They provide data encryption protocols for secure communication
D. They define permissions and network rules for resource access
Answer: D (LEAVE A REPLY)
Access policies in cybersecurity are critical for managing and controlling how users and devices access resources within a network or cloud environment. These policies are primarily concerned with defining permissions and rules that govern access to resources. They help organizations implement role-based access control (RBAC) or attribute-based access control (ABAC), which specify who can access what resources and under what conditions.
In the context of cloud computing, access policies are typically enforced using Identity and Access Management (IAM) tools and services, which allow administrators to define and manage the permissions associated with user identities. Access policies include various rules that specify allowed or denied actions based on roles, user attributes, device types, or network conditions.
For example, in the AWS environment, access policies are written in JSON and define permissions for services like EC2, S3, or RDS. Similarly, Azure uses Role-Based Access Control (RBAC) to manage resource access policies.
Access policies are not concerned with real-time monitoring (option A), user authentication methods (option B), or encryption protocols (option C). Instead, they explicitly focus on defining access permissions and controlling how resources are utilized.
Reference:
CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management
Cloud Computing Security Risk Assessment (ENISA) - Identity and Access Management section Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

NEW QUESTION: 145
ENISA: A reason for risk concerns of a cloud provider being acquired is:
A. Arbitrary contract termination by acquiring company
B. Resource isolation may fail
C. Provider may change physical location
D. Mass layoffs may occur
E. Non-binding agreements put at risk

Answer: E (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 146
ENISA: Which is not one of the five key legal issues common across all scenarios:
A. Professional negligence
B. Outsourcing services and changes in control
C. Data protection
D. Globalization
E. Intellectual property
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
What is known as the interface used to connect with the metastructure and configure the cloud environment?
A. Management plane
B. Administrative access
C. Identity and Access Management
D. Cloud dashboard
E. Single sign-on
Answer: (SHOW ANSWER)

NEW QUESTION: 148
When configured properly, logs can track every code, infrastructure, and configuration change and connect it back to the submitter and approver, including the test results.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 149
What is the primary purpose of secrets management in cloud environments?
A. Optimizing cloud infrastructure performance
B. Managing user authentication for human access
C. Securely handling stored authentication credentials
D. Monitoring network traffic for security threats
Answer: (SHOW ANSWER)
Secrets management focuses on securely storing and managing sensitive information, such as API keys and passwords, to prevent unauthorized access. Reference: [Security Guidance v5, Domain 8 - Secrets Management]

NEW QUESTION: 150

Which of the following best describes the concept of AI as a Service (AIaaS)?
A. Selling AI hardware to enterprises for internal use
B. Hosting and running AI models with customer-built solutions
C. Offering pre-built AI models to third-party vendors
D. Providing software as an AI model with no customization options
Answer: B (LEAVE A REPLY)
AI as a Service (AIaaS) refers to cloud-based services that provide organizations with access to pre-built or customizable AI models and infrastructure. These services allow businesses to host and run AI models, often with the ability to tailor them to meet their specific needs. AIaaS enables customers to leverage AI capabilities without needing to build the underlying infrastructure or develop complex AI models from scratch.

NEW QUESTION: 151
What is a key benefit of using customer-managed encryption keys with cloud key management service (KMS)?
A. Customers can bypass the need for encryption
B. Customers retain control over their encryption keys
C. Customers can share their encryption keys more easily
D. It reduces the computational load on the cloud service provider
Answer: (SHOW ANSWER)
The correct answer isB. Customers retain control over their encryption keys.
Usingcustomer-managed encryption keys (CMEK)with a cloudKey Management Service (KMS)allows the customer toretain full control over the encryption keysused to encrypt their data. This is crucial in maintaining data sovereignty, privacy, and compliance with regulatory requirements.
Key Benefits of Customer-Managed Encryption Keys:
* Key Ownership and Control:Unlike cloud provider-managed keys, CMEK ensures that the customer has full authority over the key's lifecycle, including creation, rotation, and deletion.
* Enhanced Security:Customers can enforce strict access controls and audit who accesses the keys.
* Compliance:Many regulations (like GDPR or HIPAA) mandate that data owners maintain control over encryption keys.
* Data Privacy:Even though the data is stored on the cloud, the provider cannot access unencrypted data without the customer's permission.
* Flexibility:Customers can choose when to revoke or rotate keys, which directly impacts data availability and access.
Why Other Options Are Incorrect:
* A. Bypass the need for encryption:CMEK does not eliminate the need for encryption; it strengthens it by giving customers direct control.

* C. Share encryption keys more easily:Sharing encryption keys can increase security risks, and CMEK is designed to restrict, not ease, key sharing.
* D. Reduces computational load on the cloud service provider:CMEK does not impact the computational load. It focuses on key management and control rather than reducing processing overhead.
Real-World Example:
InAWS KMS, using CMEK allows customers to bring their own keys (BYOK) and manage them directly through AWS Key Management Service. Similar practices exist inGoogle Cloud KMSandAzure Key Vault, where customers can generate and control their own encryption keys.
Practical Use Case:
A healthcare provider using a cloud service to store patient records may use CMEK to ensure that sensitive data is encrypted under keys they control, ensuring compliance with regulations likeHIPAA.
References:
CSA Security Guidance v4.0, Domain 11: Data Security and Encryption
Cloud Computing Security Risk Assessment (ENISA) - Key Management and Encryption
Cloud Controls Matrix (CCM) v3.0.1 - Data Protection and Encryption Domain

NEW QUESTION: 152
Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?
A. Infrastructure
B. Infostructure
C. Datastructure
D. Metastructure
E. Applistructure
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Which is the most important trust mechanism between cloud service provider and cloud customer?

A. Meeting SLA requirements
B. Contract
C. Audit reports
D. Logging and Monitoring reports
Answer: (SHOW ANSWER)
Contract is the most important document which defines trust and relationship between cloud service provider and the customer.

NEW QUESTION: 154
Which standard offers guidelines for information security controls applicable to the provision and use of cloud services?
A. ISO 27018
B. ISO 27017
C. ISO 15048
D. ISO 27034
Answer: A (LEAVE A REPLY)
ISO 270017 provides guidance on the information security aspects of cloud computing. recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO 27k standards.

NEW QUESTION: 155
Whose responsibility is to maintain Data Loss Prevention mechanisms in SaaS(Software as a Service) model ?
A. Cloud Carrier
B. Cloud Service provider
C. Cloud Customer
D. Cloud Access Security Broker
Answer: (SHOW ANSWER)
Although clouds customer is legally responsible for data that he stores on the cloud but Cloud Service Provider has to maintain data loss prevention mechanisms

NEW QUESTION: 156
Which of the following best describes the responsibility for security in a cloud environment?
A. Cloud Service Customers (CSCs) are solely responsible for security in the cloud environment. The Cloud Service Providers (CSPs) are accountable.
B. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities.
The exact allocation of responsibilities depends on the technology and context.
C. Cloud Service Providers (CSPs) are solely responsible for security in the cloud environment. Cloud Service Customers (CSCs) have an advisory role.

D. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities.The allocation of responsibilities is constant.

Answer: (SHOW ANSWER)

The shared security responsibility model in cloud environments clarifies that CSPs and CSCs both have roles, with specific responsibilities varying based on the service model (IaaS, PaaS, SaaS). In IaaS, CSCs handle more security, while CSPs manage most security in SaaS. Reference: [CCSK Study Guide, Domain 1 - Cloud Security Scope and Responsibilities]

NEW QUESTION: 157

What is the primary reason dynamic and expansive cloud environments require agile security approaches?

A. To reduce costs associated with physical hardware

B. To simplify the deployment of virtual machines

C. To quickly respond to evolving threats and changing infrastructure

D. To ensure high availability and load balancing

Answer: (SHOW ANSWER)

Agile security approaches allow organizations to adapt to the rapid changes and emerging threats characteristic of cloud environments. Reference: [Security Guidance v5, Domain 4 - Organization Management]

NEW QUESTION: 158

Private clouds can be hosted off-premises as well.

A. True

B. False

Answer: (SHOW ANSWER)

It is true. This is how Private cloud is defined.

Private Cloud: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premises or off-premises.

NEW QUESTION: 159

Logs, documentation, and other materials needed for audits and compliance and often serve as evidence of compliance activities are known as:

A. Log Trail

B. Documented Evidence

C. Proof of Audit

D. Artifacts

Answer: D (LEAVE A REPLY)

Artifacts are the logs, documentation, and other materials needed for audits and compliance; they are the evidence to support compliance activities. Both providers and customers have responsibilities for producing and managing their respective artifacts.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

NEW QUESTION: 160
Which of the following best describes the multi-tenant nature of cloud computing?
A. Cloud customers operate independently without sharing resources
B. Cloud customers share a common pool of resources but are segregated and isolated from each other
C. Multiple cloud customers are allocated a set of dedicated resources via a common web interface
D. Cloud customers share resources without any segregation or isolation
Answer: (SHOW ANSWER)
The multi-tenant nature of cloud computing refers to the model where multiple cloud customers share a common pool of resources (such as computing power, storage, etc.), but each customer's data and applications are segregated and isolated from the others to ensure privacy, security, and independent performance. This approach allows cloud providers to efficiently use resources while ensuring that each tenant's environment is protected and operates independently.

NEW QUESTION: 161
Which of the authentication is more secured?
A. Password Authentication
B. Biometric Authentication
C. Single Sign-on
D. Multifactor Authentication
Answer: (SHOW ANSWER)
Multifactor authentication is more secured than the rest because it has more than one aspect to authentication Multifactor authentication is composed of, at a minimum, two of the following aspects- something you know, something you are, or something you have. Something you know can be a password, passphrase, and so on. Something you have can be something like a number-generating transmit a number or fob, a smartphone capable of receiving text messages, or even a phone that can receive a call and then to the individual but that is only accessible from a very specific phone number.
Something you are is a biometric trait of yourself, as a living creature. This could be as unique and specific as your DNA fingerprint, or as cursorily general as a photograph.

NEW QUESTION: 162
A defining set of rules composed of claims and attributes of the entities in a transaction, which is used to determine their level of access to cloud-based resources is called what?

A. An entitlement matrix
B. A validation process
C. A support table
D. An entry log
E. An access log
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
Which one of the following is not a risk mitigation strategy?
A. Avoidance
B. Acceptance
C. Transfer
D. Suppression
Answer: D (LEAVE A REPLY)
Following are the risk mitigation strategies

NEW QUESTION: 164
Which one of the following is not one the cloud deployment models?
A. Public
B. Private
C. Joint
D. Community
Answer: C (LEAVE A REPLY)
The four cloud deployment models are
1. Public
2. Private
3. Hybrid
4. Community

NEW QUESTION: 165
How can virtual machine communications bypass network security controls?
A. Most network security systems do not recognize encrypted VM traffic
B. VM images can contain rootkits programmed to bypass firewalls
C. VM communications may use a virtual network on the same hardware host
D. Hypervisors depend upon multiple network interfaces
E. The guest OS can invoke stealth mode
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Which of the following best describes the role of program frameworks in defining security components and technical controls?

A. Program frameworks evaluate the performance of individual security tools
B. Program frameworks focus on implementing specific security technologies
C. Program frameworks help organize overarching security policies and objectives
D. Program frameworks primarily define compliance requirements for regulations
Answer: C (LEAVE A REPLY)
Program frameworksplay a critical role in cloud security by helping toorganize overarching security policies and objectives. Frameworks suchas NIST CSF, ISO 27001, or the CSA Cloud Controls Matrix (CCM) provide structured guidance for defining security components, aligning technical controls with business objectives, and ensuring a comprehensive security program.
From theCCSK v5.0 Study Guide, Domain 3 (Governance and Enterprise Risk Management), Section
3.2:
"Program frameworks, such as the CSA CCM or NIST Cybersecurity Framework, provide a structured approach to organizing security policies, objectives, and technical controls. These frameworks help organizations align their security programs with business goals and ensure comprehensive coverage of security requirements." Option C (Program frameworks help organize overarching security policies and objectives) is the correct answer.
* Option A (Evaluate the performance of individual security tools) is incorrect because frameworks focus on strategy, not tool performance.
* Option B (Focus on implementing specific security technologies) is incorrect because frameworks guide policy, not technology implementation.
* Option D (Primarily define compliance requirements) is incorrect because compliance is a subset of framework objectives, not the primary role.
References:
CCSK v5.0 Study Guide, Domain 3, Section 3.2: Security Program Frameworks.

NEW QUESTION: 167
What technology is commonly used to establish an encrypted tunnel between a remote user's device and a private network over the public Internet?
A. Virtual Private Network (VPN)

B. Domain Name System (DNS)
C. Network Address Translation (NAT)
D. Virtual Local Area Network (VLAN)
Answer: A (LEAVE A REPLY)
Correct Option: A. Virtual Private Network (VPN)
A Virtual Private Network (VPN) is a widely used technology that enables secure communication over untrusted networks like the public Internet. It works by creating an encrypted tunnel between the user's device and the internal private network, thereby ensuring data confidentiality, integrity, and authentication.
From CSA Security Guidance v4.0 - Domain 7: Infrastructure Security:
"Remote access solutions, such as VPNs, are commonly used to provide users with secure access to cloud or on-premises resources. VPNs create encrypted tunnels that protect data in transit, preventing unauthorized disclosure or tampering over public networks."
- Domain 7: Infrastructure Security, CSA Security Guidance v4.0
This makes VPNs a fundamental security control when users are working remotely and need access to sensitive or internal systems.
Why the Other Options Are Incorrect:
B . Domain Name System (DNS)
➤ DNS translates domain names to IP addresses. It does not provide encryption or secure tunneling.
C . Network Address Translation (NAT)
➤ NAT modifies IP address information but does not encrypt data or create tunnels.
D . Virtual Local Area Network (VLAN)
➤ VLANs segment network traffic within a LAN. They do not secure remote communications over the Internet.

NEW QUESTION: 168
What is the most significant security difference between traditional infrastructure and cloud computing?
A. Intrusion detection options
B. Mobile security configuration options
C. Network access points
D. Management plane
E. Secondary authentication factors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
All cloud services utilize virtualization technologies.
A. True
B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 170
Which of the following best describes a key aspect of cloud risk management?
A. A structured approach for performance optimization of cloud services
B. A structured approach to identifying, assessing, and addressing risks
C. A structured approach to establishing the different what/if scenarios for cloud vs on-premise decisions
D. A structured approach to SWOT analysis
Answer: B (LEAVE A REPLY)
A key aspect of cloud risk management is taking a structured approach to identify, assess, and address risks related to using cloud services. This includes evaluating potential risks such as security vulnerabilities, data privacy issues, service outages, and compliance challenges. Effective risk management helps organizations proactively mitigate potential threats, ensuring the cloud environment is secure, compliant, and resilient.
A structured approach for performance optimization of cloud services is more related to performance management, not risk management. A structured approach to establishing the different what/if scenarios for cloud vs on-premise decisions refers to decision-making scenarios, not the identification and management of risks. A structured approach to SWOT analysis) is a strategic planning tool that focuses on strengths, weaknesses, opportunities, and threats, but it is not specifically focused on cloud risk management.

NEW QUESTION: 171
Your cloud and on-premises infrastructures should always use the same network address ranges.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172
What is the primary function of Data Encryption Keys (DEK) in cloud security?
A. To increase the speed of cloud services
B. To encrypt application data
C. To directly manage user access control
D. To serve as the primary key for all cloud resources
Answer: (SHOW ANSWER)
The primary function ofData Encryption Keys (DEK)in cloud security is toencrypt application data. DEKs are used to encrypt and decrypt specific data objects, such as files or database records, ensuring data confidentiality in cloud environments.
From theCCSK v5.0 Study Guide, Domain 10 (Data Security and Encryption), Section 10.3:

"Data Encryption Keys (DEKs) are used to encrypt and decrypt application data in cloud environments. DEKs are typically managed by key management services and applied to specific data objects to ensure confidentiality and protect against unauthorized access."
Option B (To encrypt application data) is the correct answer.
* Option A (Increase speed) is incorrect because encryption does not enhance performance.
* Option C (Manage user access control) is incorrect because DEKs are for encryption, not access control.
* Option D (Primary key for all resources) is incorrect because DEKs are specific to data encryption, not resource management.
References:
CCSK v5.0 Study Guide, Domain 10, Section 10.3: Encryption and Key Management.

NEW QUESTION: 173
What method can be utilized along with data fragmentation to enhance security?
A. IDS
B. Encryption
C. Organization
D. Insulation
E. Knowledge management
Answer: (SHOW ANSWER)

NEW QUESTION: 174
What is a key consideration when handling cloud security incidents?
A. Monitoring network traffic
B. Focusing on technical fixes
C. Cloud service provider service level agreements
D. Hiring additional staff
Answer: C (LEAVE A REPLY)
SLAs play a key role in cloud incident management as they define response expectations and support arrangements between CSPs and CSCs. Reference: [CCSK Study Guide, Domain 11 - Incident Response]

NEW QUESTION: 175
Which of the following enhances Platform as a Service (PaaS) security by regulating traffic into PaaS components?
A. Intrusion Detection Systems
B. Hardware Security Modules
C. Network Access Control Lists
D. API Gateways
Answer: D (LEAVE A REPLY)

API Gateways enhance Platform as a Service (PaaS) security by regulating traffic into and out of PaaS components. They act as an intermediary between external requests and the PaaS applications, helping to enforce security policies such as authentication, authorization, rate limiting, input validation, and logging. API gateways help protect PaaS components by controlling which traffic is allowed to reach the services, thereby reducing exposure to potential attacks.
Intrusion Detection Systems (IDS) are used to detect potential threats in a network, but they don't specifically regulate traffic into PaaS components like API Gateways do. Hardware Security Modules (HSMs) are used for managing encryption keys and cryptographic operations but do not directly regulate traffic to PaaS components. Network Access Control Lists (NACLs) control traffic at the network layer but are generally used for controlling traffic to/from virtual machines or subnets rather than for PaaS components specifically.

NEW QUESTION: 176
Which of the following best describes the Identity Provider (IdP) and its role in managing access to deployments?
A. The IdP is used for authentication purposes and does not play a role in managing access to deployments.
B. The IdP manages user, group, and role mappings for access to deployments across cloud providers.
C. The IdP solely manages access within a deployment and resides within the deployment infrastructure.
D. The IdP is responsible for creating deployments and setting up access policies within a single cloud provider.
Answer: (SHOW ANSWER)
An Identity Provider (IdP) is responsible for authentication and authorization, particularly by managing user identities and their roles across various systems and services. In a cloud environment, the IdP facilitates the management of user, group, and role mappings that determine which users have access to which resources, including deployments across different cloud providers. The IdP acts as the central authority for managing identities and ensuring that users are granted appropriate access based on their roles and credentials.

NEW QUESTION: 177
ISO 27001 certification can be taken as proof to achieve Third-party assessment level in CSA star program.
A. True
B. False
Answer: A (LEAVE A REPLY)

The CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC
27001:2013 management system standard together with the CSA Cloud Controls Matrix.

NEW QUESTION: 178
Which cloud service model requires the customer to manage the operating system and applications?
A. Platform as a Service (PaaS)
B. Network as a Service (NaaS)
C. Infrastructure as a Service (IaaS)
D. Software as a Service (SaaS)
Answer: C (LEAVE A REPLY)
In the Infrastructure as a Service (IaaS) model, the cloud provider delivers the basic infrastructure components such as virtual machines, storage, and networking resources. However, the customer is responsible for managing the operating system, applications, and any software configurations that run on the infrastructure. This gives the customer more control over the environment while still benefiting from the cloud provider's hardware and scalability.
The provider manages the operating system, runtime, and infrastructure, and the customer is only responsible for managing the applications. NaaS focuses on network services, not the management of operating systems and applications. The provider manages everything, including the operating system and applications, and the customer simply uses the software.

NEW QUESTION: 179
"Cloud provider acquisition" as a risk fall under which of the following categories?
A. Technical risk
B. Policy and Organizational Risk
C. Legal Risk
D. Environmental Risk
Answer: B (LEAVE A REPLY)
Cloud provider acquisition comes under Policy and Organizational Risk and can be categorised as follows.
As in any new IT market, competitive pressure, an inadequate business strategy, lack of financial support, etc, could lead some providers to go out of business or at least to force them to restructure their service portfolio offering. In other words, it is possible that in the short or medium term some cloud computing services could be terminated.

NEW QUESTION: 180

Which practice minimizes human error in long-running cloud workloads' security management?

A. Increasing manual security audits frequency

B. Converting all workloads to ephemeral

C. Restricting access to workload configurations

D. Implementing automated security and compliance checks

Answer: D (LEAVE A REPLY)

Automating security and compliance checks helps minimize human error in long-running cloud workloads by continuously monitoring for security vulnerabilities, misconfigurations, or compliance issues without relying on manual intervention. This approach ensures consistent, repeatable security processes and can quickly identify and address potential risks, reducing the chances of oversight or mistakes that might occur with manual management.

Manual audits and restrictions can help but do not fully address the continuous nature of cloud workload security, which is why automation is critical for minimizing errors in long-running workloads.

NEW QUESTION: 181

According to CSA Security Guidelines, there are four layers of Logical Model for cloud computing. Which of the following is not one of the layers as defined by Cloud Security Alliance?

A. Infrasturcture

B. Metastructure

C. Applistructure

D. Softstructure

Answer: (SHOW ANSWER)

The four layers of Logical Model for cloud computing according to Cloud Security Alliance are:

1. Infrastructure: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts.

2. Metastructure: The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.

3. Infostructure: The data and information. Content in a database, file storage, etc.

4. Applistructure: The applications deployed in the cloud and the underlying application services used to build them. For example, Platform as a Service features like message queues, artificial intelligence analysis, or notification services.

NEW QUESTION: 182
Which of the following best describes a risk associated with insecure interfaces and APIs?
A. Ensuring secure data encryption at rest
B. Man-in-the-middle attacks
C. Increase resource consumption on servers
D. Data exposure to unauthorized users
Answer: (SHOW ANSWER)
Insecure interfaces and APIs can expose data to unauthorized users, which is a significant security risk. If the API or interface is not properly secured with authentication, authorization, and encryption measures, attackers may exploit vulnerabilities to gain unauthorized access to sensitive data or control over cloud services. This can lead to data breaches and loss of confidentiality.
Ensuring secure data encryption at rest is important, but it is not directly related to insecure interfaces and APIs, which are more about securing data during transmission or interaction. Man-in-the-middle attacks can occur if APIs and interfaces are not properly secured with encryption, but this is a more specific type of attack rather than the primary risk. Increased resource consumption on servers is not typically associated with insecure interfaces or APIs. This might be a result of other issues, like poorly optimized APIs.

NEW QUESTION: 183
Which of the following cloud computing models primarily provides storage and computing resources to the users?
A. Function as a Service (FaaS)
B. Platform as a Service (PaaS)
C. Software as a Service (SaaS)
D. Infrastructure as a Service (Iaa
Answer: D (LEAVE A REPLY)
Infrastructure as a Service (IaaS) primarily provides users with storage, computing resources, and networking capabilities. In the IaaS model, cloud providers offer virtualized computing resources over the internet. Users can rent servers, storage, and networking equipment without needing to manage the physical hardware themselves. This allows for flexible scaling and resource management according to the users' needs.

FaaS focuses on serverless computing where users run code in response to events. PaaS provides a platform that allows users to develop, run, and manage applications without worrying about the underlying infrastructure. SaaS delivers fully managed applications over the internet, where users access software without managing the infrastructure.

NEW QUESTION: 184
Erin has a picture which he wants to store in the cloud and would like to share its URL so that his friends can see the picture. What type of cloud storage would you recommend for him?
A. Raw storage
B. Block Storage
C. Object Storage
D. Glacier
Answer: C (LEAVE A REPLY)
Object storage(also referred to as object-based storage) is a general term that refers to the way in which we organize and work with units of storage, called objects.
Every object contains three things:
The data itself: The data can be anything you want to store, from a family photo to a400,000-page manual for assembling an aircraft.
An expandable amount of metadata: The metadata is defined by whoever creates the object storage; it contains contextual information about what the data is, what it should be used for, its confidentiality, or anything else that is relevant to the way in which the data is used.
A globally unique identifier: The identifier is an address given to the object in order for the object to be found over a distributed system. This way, it's possible to find the data without having to know the physical location of the data(which could exist within different parts of a data center or different parts of the world).

NEW QUESTION: 185
What is an important step in conducting forensics on containerized and serverless environments?
A. Implementing endpoint detection and response (EDR) solutions
B. Isolating network traffic and analyzing network packets frequently
C. Regularly updating antivirus and anti-malware software
D. Capturing container logs and snapshots, and leveraging serverless execution logs
Answer: (SHOW ANSWER)
The CSA Security Guidance v4.0, Domain 9: Incident Response highlights that traditional forensic techniques don't always apply in cloud-native environments like containers and serverless platforms. Instead, forensic investigators must capture ephemeral data such as logs, snapshots, and execution traces early and often.

"Forensic techniques must adapt to cloud-native environments such as containers and serverless. Important forensic data - including container logs, snapshots, and function execution logs - may be short-lived or non-persistent, so timely collection is critical."
- CSA Security Guidance v4.0, Domain 9: Incident Response
Key points:
Containers and serverless functions are often short-lived.
You need to capture logs and memory state before they're destroyed.
Serverless platforms (like AWS Lambda, Azure Functions) often provide execution logs via services like CloudWatch or Application Insights.
Incorrect options:
A: EDR is typically focused on traditional endpoints, not containers/serverless.
B: Useful in general, but not specific or always applicable to serverless/container forensics.
C: Antivirus doesn't apply well to ephemeral or function-based environments.
Reference:
CSA Security Guidance v4.0 - Domain 9: Incident Response (Container and Serverless Forensics) CCM v3.0.1 - DSI-05, IVS-04 (Covers logging and snapshot control)

NEW QUESTION: 186
Audits should be robustly designed to reflect best practice, appropriate resources, and tested protocols and standards. They should also use what type of auditors?
A. Independent auditors
B. Certified by CSA
C. Auditors working in the interest of the cloud provider
D. Auditors working in the interest of the cloud customer
E. None of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 187
An important consideration when performing a remote vulnerability test of a cloud-based application is to
A. Obtain provider permission for test
B. Use techniques to evade cloud provider's detection systems
C. Use application layer testing tools exclusively
D. Use network layer testing tools exclusively
E. Schedule vulnerability test at night
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 188
What mechanism does passwordless authentication primarily use for login?
A. SMS-based codes

B. Biometric data
C. Local tokens or certificates
D. OAuth tokens
Answer: C (LEAVE A REPLY)
Passwordless authentication removes the reliance on traditional passwords and instead relies on strong, cryptographic-based login mechanisms. The primary technology behind passwordless authentication is the use of local tokens or certificates, particularly implemented through protocols like FIDO2 and WebAuthn.
These mechanisms work by storing a private key on the user's device (like a hardware security module or TPM), while the public key is stored with the cloud service. When a login attempt is made, the system uses asymmetric cryptography to verify the user-without ever transmitting a secret like a password.
"Passwordless authentication is enabled by mechanisms such as biometric verification and secure local credentials like hardware-bound certificates or tokens. The use of cryptographic authenticators (such as FIDO2) is becoming the cornerstone of secure, phishing-resistant authentication."
- Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Domain 12: Identity, Entitlement, and Access Management Also supported by the Cloud Controls Matrix (CCM) under IAM-12:
"Utilize multifactor authentication or strong authentication mechanisms such as cryptographic tokens or certificates for user access to cloud services."
- Cloud Controls Matrix v3.0.1 (IAM-12)

NEW QUESTION: 189
APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following functionalities is provided by Data Security Posture Management (DSPM) tools?
A. Firewall management and configuration
B. User activity monitoring and reporting
C. Encryption of all data at rest and in transit
D. Visualization and management for cloud data security
Answer: D (LEAVE A REPLY)
Data Security Posture Management (DSPM) tools are designed to help organizations visualize, monitor, and manage the security of their data in the cloud. These tools help ensure that data is properly classified, protected, and compliant with relevant regulations

and standards. DSPM tools typically provide capabilities like identifying and managing sensitive data, assessing security risks, and ensuring data security posture is aligned with best practices.
The other options are not the primary focus of DSPM tools:
Firewall management relates to network security rather than data security.
User activity monitoring is more about identity and access management or security information and event management (SIEM).
Encryption is important for data protection but is not the primary function of DSPM, which focuses more on data visibility and management.

NEW QUESTION: 191
An organization deploys an AI application for fraud detection. Which threat is MOST likely to affect its AI model's accuracy?
A. Adversarial attacks
B. DDoS attacks
C. Third-party services
D. Jailbreak attack
Answer: A (LEAVE A REPLY)
Correct Option: A. Adversarial attacks
Adversarial attacks are specifically designed to deceive AI and machine learning models by feeding them crafted inputs that result in incorrect outputs. These attacks are highly effective against AI models, especially in areas like fraud detection, where accuracy is critical.
From CSA Security Guidance v4.0 - Domain 13: Security as a Service (SecaaS) and related AI-focused security discussions:
"AI models are vulnerable to adversarial inputs, where attackers introduce subtle perturbations to input data that are imperceptible to humans but cause the AI system to make wrong decisions. These attacks degrade the accuracy and reliability of machine learning models."
- CSA Guidance on AI Security (in Security as a Service domain)
Adversarial ML is a well-recognized field of AI security, where the goal of the attacker is to intentionally corrupt or manipulate input data, thereby lowering the performance or biasing the output of the model.
Why the Other Options Are Incorrect:
B . DDoS attacks
➤ Affects availability, not accuracy. DDoS can cause downtime but doesn't interfere with model predictions.
C . Third-party services
➤ May introduce supply chain or dependency risks, but they don't directly impact the AI model's accuracy unless involved in training data pipelines.
D . Jailbreak attack

➤ More relevant to LLMs (Large Language Models) or chatbots, not structured AI fraud detection models.

NEW QUESTION: 192
A company plans to shift its data processing tasks to the cloud. Which type of cloud workload best describes the use of software emulations of physical computers?
A. Platform as a Service (PaaS)
B. Serverless Functions (FaaS)
C. Containers
D. Virtual Machines (VMs)
Answer: (SHOW ANSWER)
The correct answer isD. Virtual Machines (VMs). In the context of cloud computing,Virtual Machines (VMs)are software-based emulations of physical computers. They run an operating system (OS) and applications just like a physical machine would. VMs are often hosted on physical servers using hypervisors, which allow multiple VMs to run on a single physical machine, thereby sharing resources like CPU, memory, and storage.
Why Virtual Machines (VMs) are Suitable for Data Processing:
Full OS Environment:VMs provide a complete operating system environment, making them suitable for running complex data processing tasks that require specific OS configurations.
Isolation:Each VM operates independently, providing isolation between different workloads, which is essential when processing sensitive or diverse data sets.
Scalability:Cloud providers offer VM scaling options to meet the demands of data processing workloads.
Compatibility:VMs can run legacy applications that may not be compatible with newer cloud-native technologies.
Why Other Options Are Incorrect:
A . Platform as a Service (PaaS):PaaS provides a platform for developing and deploying applications without managing underlying infrastructure. It is not directly related to VM-based processing.
B . Serverless Functions (FaaS):Serverless computing abstracts the infrastructure and is used for running discrete functions rather than emulating entire machines.
C . Containers:Containers package applications and dependencies but share the host OS kernel. They are lightweight compared to VMs and do not fully emulate physical computers.
Real-World Example:
If a company moves a data processing application that was traditionally run on an on-premises physical server to the cloud, they might choose VMs on services like AWS EC2, Azure Virtual Machines, or Google Compute Engine to maintain the same OS environment and application compatibility.
Reference:
CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - Virtualization Risks Cloud Controls Matrix (CCM) v3.0.1 - Infrastructure as a Service (IaaS) Domain

NEW QUESTION: 193
In a cloud environment, what does the Shared Security Responsibility Model primarily aim to define?
A. The division of security responsibilities between cloud providers and customers
B. The relationships between IaaS, PaaS, and SaaS providers
C. The compliance with geographical data residency and sovereignty
D. The guidance for the cloud compliance framework
Answer: A (LEAVE A REPLY)
The Shared Security Responsibility Model clarifies which security responsibilities are managed by the CSP and which by the CSC, based on the service model. Reference: [CCSK Study Guide, Domain 1 - Cloud Security Models]

NEW QUESTION: 194
Which type of cloud workload would be most appropriate for running isolated applications with minimum resource overhead?
A. Containers
B. Function as a Service (FaaS)
C. AI Workloads
D. Virtual Machines (VMs)
Answer: A (LEAVE A REPLY)
Containersare the most appropriate cloud workload for running isolated applications with minimum resource overhead. Containers provide lightweight, isolated environments that share the host operating system, reducing resource consumption compared to virtual machines (VMs). They are ideal for microservices and applications requiring isolation without the overhead of a full VM.
From theCCSK v5.0 Study Guide, Domain 2 (Cloud Infrastructure and Platform Security), Section 2.5:
"Containers are lightweight, portable, and isolated environments that share the host OS kernel, making them highly efficient for running applications with minimal resource overhead. Unlike VMs, which require a full guest OS, containers provide application isolation with significantly lower resource demands." Option A (Containers) is the correct answer.
Option B (Function as a Service) is incorrect because FaaS is designed for event-driven, short-lived functions, not for running full applications.
Option C (AI Workloads) is incorrect because AI workloads are a category of tasks, not a specific workload type, and may run on VMs or containers.
Option D (Virtual Machines) is incorrect because VMs include a full guest OS, resulting in higher resource overhead compared to containers.

Reference:
CCSK v5.0 Study Guide, Domain 2, Section 2.5: Containers and Virtualization.

NEW QUESTION: 195
Which practice ensures container security by preventing post-deployment modifications?
A. Implementing dynamic network segmentation policies
B. Employing Role-Based Access Control (RBAC) for container access
C. Regular vulnerability scanning of deployed containers
D. Use of immutable containers
Answer: D (LEAVE A REPLY)
Immutable containers are not altered post-deployment, ensuring the integrity of the deployed environment and reducing the risk of unauthorized modifications. Reference: [CCSK v5 Curriculum, Domain 8 - Cloud Workload Security]

NEW QUESTION: 196
Which of the following statements best defines the "authorization" as a component of identity, entitlement, and access management?
A. Establishing/asserting the identity to the application
B. The process of specifying and maintaining access policies
C. Giving a third party vendor permission to work on your cloud solution
D. Checking data storage to make sure it meets compliance requirements
E. Enforcing the rules by which access is granted to the resources
Answer: A (LEAVE A REPLY)

NEW QUESTION: 197
Which of the following statements best describes an identity federation?
A. A library of data definitions
B. The connection of one identity repository to another
C. Identities which share similar attributes
D. A group of entities which have decided to exist together in a single cloud
E. Several countries which have agreed to define their identities with

similar attributes
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the vulnerabilities is inherited from general software development practice in PaaS environment?
A. Backdoors
B. DDoS
C. Cross
D. DNS spoofing
Answer: (SHOW ANSWER)
As a general practice of software development. Developer tend to leave backdoors so that they can come back later to fix issues.

NEW QUESTION: 199
Which aspect is most important for effective cloud governance?
A. Formalizing cloud security policies
B. Implementing best-practice cloud security control objectives
C. Negotiating SLAs with cloud providers
D. Establishing a governance hierarchy
Answer: B (LEAVE A REPLY)
A governance hierarchy provides a structured approach to managing cloud services, ensuring policies and controls are effectively enforced. Reference: [Security Guidance v5, Domain 2 - Cloud Governance]

NEW QUESTION: 200
What is the best way to ensure that all data has been removed from a public cloud environment including all media such as back-up tapes?
A. Allowing the cloud provider to manage your keys so that they have the ability to access and delete the data from the main and back-up storage.
B. Practice Integration of Duties (IOD) so that everyone is able to delete the encrypted data.
C. Keep the keys stored on the client side so that they are secure and so that the users have the ability to delete their own data.
D. Both B and D.
E. Maintaining customer managed key management and revoking or deleting keys from the key management system to prevent the data from being accessed again.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 201

In the context of cloud workload security, which feature directly contributes to enhanced performance and resource utilization without incurring excess costs?

A. Fixed resource allocations

B. Unlimited data storage capacity

C. Increased on-premise hardware

D. Elasticity of cloud resources

Answer: (SHOW ANSWER)

Elasticity of cloud resources is a key feature that directly contributes to enhanced performance and resource utilization while avoiding excess costs. Cloud elasticity allows resources (such as compute power, storage, and network bandwidth) to automatically scale up or down based on demand. This ensures that organizations are only using the resources they need at any given time, optimizing both performance and cost-efficiency. Fixed resource allocations do not provide the flexibility needed to optimize resource utilization and can lead to either over-provisioning (wasting resources) or under-provisioning (affecting performance). Unlimited data storage capacity is not typical in all cloud environments and does not directly impact resource optimization or performance. Increased on-premise hardware is unrelated to cloud workload security, as it refers to traditional, non-cloud infrastructure.

NEW QUESTION: 202

When establishing a cloud incident response program, what access do responders need to effectively analyze incidents?

A. Access limited to log events for incident analysis

B. Unlimited write access for all responders at all times

C. Full-read access without any approval process

D. Persistent read access and controlled write access for critical situations

Answer: D (LEAVE A REPLY)

When establishing a cloud incident response program, responders need persistent read access to resources, such as logs, configurations, and system data, in order to analyze and investigate incidents effectively. This access allows them to view and understand the nature of the incident, the affected systems, and any potential risks. In critical situations, controlled write access is necessary to take remedial actions, such as stopping malicious processes, patching vulnerabilities, or implementing other immediate security measures, but write access should be restricted and carefully managed to prevent misuse or errors. Access limited to log events is too restrictive, as responders need more than just log events to fully analyze incidents. Unlimited write access for all responders is too broad and dangerous; unrestricted write access could lead to accidental or malicious changes to critical systems. Full-read access without any approval process could be dangerous if it allows responders too much access without appropriate oversight, potentially violating privacy or security policies.

NEW QUESTION: 203
Which tool is most effective for ensuring compliance and identifying misconfigurations in cloud management planes?
A. Data Security Posture Management (DSPM)
B. SaaS Security Posture Management (SSPM)
C. Cloud Detection and Response (CDR)
D. Cloud Security Posture Management (CSPM)
Answer: D (LEAVE A REPLY)
The correct answer is D. Cloud Security Posture Management (CSPM).
Cloud Security Posture Management (CSPM) is a comprehensive tool designed to identify and remediate misconfigurations and compliance violations in cloud management planes. It helps organizations maintain secure and compliant cloud environments by continuously monitoring configurations against industry standards and best practices.
Key Functions of CSPM:
* Configuration Management: Identifies misconfigurations and alerts administrators to fix them.
* Compliance Monitoring: Continuously assesses cloud environments against compliance frameworks such as CIS, NIST, GDPR, and others.
* Automated Remediation: Automatically fixes known configuration errors based on predefined policies.
* Visibility: Provides a comprehensive view of security and compliance risks across multi-cloud environments.
* Risk Assessment: Analyzes risks related to identity, data exposure, and network configurations.
Why CSPM is Most Effective:
Cloud environments are dynamic, and maintaining secure configurations is challenging. CSPM solutions like AWS Config, Azure Security Center, and Google Cloud Security Command Center automate the process of checking for security policy violations and configuration drift.
Why Other Options Are Incorrect:
* A. Data Security Posture Management (DSPM): Focuses on data security, data loss prevention, and data governance, rather than configuration and compliance management.
* B. SaaS Security Posture Management (SSPM): Specifically targets SaaS applications, managing security settings and compliance of cloud-based software rather than infrastructure.
* C. Cloud Detection and Response (CDR): Focuses on threat detection and incident response rather than configuration management and compliance.
Real-World Example:
A CSPM tool like Palo Alto Prisma Cloud or AWS Config can automatically detect if IAM policies are overly permissive or if S3 buckets are publicly accessible, helping to maintain compliance and reduce attack surfaces.

References:
CSA Security Guidance v4.0, Domain 4: Compliance and Audit Management
Cloud Computing Security Risk Assessment (ENISA) - Cloud Security Monitoring Cloud Controls Matrix (CCM) v3.0.1 - Cloud Configuration Management Domain

NEW QUESTION: 204
In a hybrid cloud environment, why would an organization choose cascading log architecture for security purposes?
A. To reduce the number of network hops for log collection
B. To facilitate efficient central log collection
C. To use CSP's analysis tools for log analysis
D. To convert cloud logs into on-premise formats
Answer: B (LEAVE A REPLY)
Cascading log architecture enables centralized collection of logs from various sources, enhancing visibility and simplifying security monitoring in hybrid environments. Reference: [Security Guidance v5, Domain 6 - Security Monitoring]

NEW QUESTION: 205
Big data includes high volume, high variety, and high velocity.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 206
ENISA: Lock-in is ranked as a high risk in ENISA research, a key underlying vulnerability causing lock in is:
A. Audit or certification not available to customers
B. Unclear asset ownership
C. No source escrow agreement
D. Lack of information on jurisdictions
E. Lack of completeness and transparency in terms of use
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following is not one of the essential characteristics as defined by NIST 800-145?
A. Broad Network Access
B. On-demand Shelf service
C. Rapid Elasticity
D. Resource Pooling
Answer: (SHOW ANSWER)

The key characteristic is on-demand self-service and not shelf" service.

NEW QUESTION: 208
Which aspect of assessing cloud providers poses the most significant challenge?
A. Inconsistent policy standards and the proliferation of provider requirements.
B. Limited visibility into internal operations and technology.
C. Excessive details shared by the cloud provider and consequent information overload.
D. Poor provider documentation and over-reliance on pooled audit.
Answer: (SHOW ANSWER)
One of the biggest challenges incloud security risk assessmentisthe lack of transparencyregardingcloud provider operations and security controls.
Key Issues with Limited Visibility:
* Cloud providers manage infrastructure at a global scale:
* Customerscannot directly inspectsecurity implementations.
* Rely onthird-party attestationslikeSOC 2, ISO 27001, CSA STARinstead of direct assessments.
* Multi-tenancy complexities:
* Cloud customersshare infrastructurewith other tenants.
* Data isolation mechanisms (e.g., virtual private clouds, encryption)must be trustedwithout direct verification.
* Regulatory compliance challenges:
* Organizations handling sensitive data (e.g., healthcare, finance)requirestrict controls.
* Cloud providers may not offer sufficient audit logsor control overdata residency and processing.
* Incident response limitations:
* In traditional IT, organizations controllog access, forensic analysis, and recovery.
* In the cloud,incident investigation depends on the provider's logging and notification practices.
Thisvisibility issueis extensively covered in:
* CCSK v5 - Security Guidance v4.0, Domain 4 (Compliance and Audit Management)
* ENISA's Cloud Computing Risk Assessment (Limited visibility into cloud provider security policies)

NEW QUESTION: 209
Which plane in a network architecture is responsible for controlling all administrative actions?
A. Forwarding plane
B. Management plane
C. Data plane
D. Application plane
Answer: B (LEAVE A REPLY)

TheManagement planein a network architecture is responsible for controlling all administrative actions, including configuration, management, monitoring, and maintenance of network devices and services. It provides the interface for administrators to interact with the network, perform system management tasks, and enforce policies.
The management plane typically includes functions such as:
Configuration management
Monitoring and logging
Administrative access control
Policy enforcement
In the context of cloud environments, the management plane also includes APIs and web-based consoles that allow administrators to manage virtual resources. Due to its critical role in controlling network and system settings, securing the management plane is of utmost importance to prevent unauthorized access and potential control over the entire network infrastructure.
Why Other Options Are Incorrect:
A . Forwarding plane:Responsible for the actual forwarding of data packets through the network based on predefined rules. It does not handle administrative functions.
C . Data plane:Responsible for data transmission and the forwarding of packets through the network but does not involve management tasks.
D . Application plane:This is not a commonly used term in network architecture, and it generally refers to application-specific functions rather than network administration.
Reference:
CSA Security Guidance v4.0, Domain 6: Management Plane and Business Continuity
Cloud Computing Security Risk Assessment (ENISA) - Management Interface
Compromise Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

NEW QUESTION: 210
When your bank or credit card company sends you a notification of changes in how it collects or shares data, it is sending that notification in compliance with:
A. HIPAA
B. GDPR
C. FERPA
D. ISO 27001
Answer: B (LEAVE A REPLY)
Under GDPR. it is mandatory to notify consumers how their data will be used

NEW QUESTION: 211
Cloud architectures necessitate certain roles which are extremely high-risk. Examples of such roles include CP system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident response. They are known

as high-risk because their malicious activities can lead to abuse of high privilege roles and can impact confidentiality, integrity and availability of data.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 212
Which of the following best describes a primary focus of cloud governance with an emphasis on security?
A. Enhancing user experience with intuitive interfaces.
B. Maximizing cost savings through resource optimization.
C. Increasing scalability and flexibility of cloud solutions.
D. Ensuring compliance with regulatory requirements and internal policies.
Answer: D (LEAVE A REPLY)
Cloud governance focuses on security, risk management, and compliance to ensure data protection, audit readiness, and regulatory adherence.
Key Elements of Cloud Security Governance:
* Regulatory Compliance:
* Organizations must comply with GDPR, HIPAA, PCI DSS, ISO 27001.
* Cloud Security Posture Management (CSPM) helps enforce compliance automatically.
* Security Policies & Controls:
* Cloud governance frameworks include IAM (Identity and Access Management), encryption policies, and workload isolation.
* Organizations must standardize security settings across multiple cloud environments.
* Audit & Risk Management:
* Implement continuous monitoring, security logging, and forensic readiness.
* Risk-based access control policies ensure data security across workloads.
* Data Protection & Privacy:
* Enforcing cloud-native security frameworks (e.g., Zero Trust, CASB, SIEM).
* Data retention, access control, and incident response are essential governance practices.
This is covered in:
* CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Risk Management)

* Cloud Security Alliance's Cloud Controls Matrix (CCM) - Cloud Governance and Compliance Standards

NEW QUESTION: 213
What is the primary objective of posture management in a cloud environment?
A. Automating incident response procedures
B. Optimizing cloud cost efficiency
C. Continuous monitoring of configurations
D. Managing user access permissions
Answer: C (LEAVE A REPLY)
The primary objective of posture management in a cloud environment is to ensure that cloud configurations are continuously monitored to ensure compliance with security policies, best practices, and regulatory requirements. Posture management involves assessing and maintaining the security posture by identifying misconfigurations, vulnerabilities, or non-compliant resources, and ensuring that the cloud environment remains secure and aligned with organizational policies.
Automating incident response procedures is important but is not the primary focus of posture management, which focuses more on proactive configuration and security monitoring. Optimizing cloud cost efficiency is a key concern in cloud management, but it is not the main focus of posture management, which deals with security and compliance. Managing user access permissions is related to Identity and Access Management (IAM), which is a separate aspect of cloud security from posture management.

NEW QUESTION: 214
Which of the following best describes the relationship between a cloud provider and the customer?
A. Contract
B. Operational level Agreement
C. Service Level Agreement
D. Privacy Level Agreement
Answer: A (LEAVE A REPLY)
Contract is the most suitable answer here. It can be argued that Service Level Agreement could also be an answer but SLA is a negotiation/agreement for minimum service-levels expected. Contract is the document that defines the relation-ship between Cloud service provider and customer

NEW QUESTION: 215
The amount of risk that the leadership and stakeholders of an organization are willing to accept is know as:
A. Risk Acceptance
B. Residual Risk

C. Risk Tolerance
D. Risk Residual
Answer: C (LEAVE A REPLY)
Risk tolerance is the amount of risk that the leadership and stakeholders of an organization are willing to accept. It varies based on asset and you shouldn't make a blanket risk decision about a particular provider; rather, assessments should align with the value and requirements of the assets Ref: Security Guidance v4.0 Copyright2017, Cloud Security Alliance(used for educational purpose here)

NEW QUESTION: 216
Without virtualization, there is no cloud.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 217
What is the process to determine any weaknesses in the application and the potential ingress, egress, and actors involved before the weakness is introduced to production?
A. STRIDE
B. Threat Detection
C. Threat Modelling
D. Vulnerability Assessment
Answer: C (LEAVE A REPLY)
Threat modelling is performed once an application design is created. The goal of threat modelling is to determine any weaknesses in the application and the potential ingress, egress, and actors involved before the weakness is introduced to production. It is the overall attack surface that is amplified by the cloud, and the threat model has to take that into account.

NEW QUESTION: 218
Which of the following pose the biggest risk in the organization?
A. People
B. Technology
C. Access Controls
D. DDoS Attacks
Answer: A (LEAVE A REPLY)
People pose the biggest risk in the organization.
People form the biggest risk as they can expose the sensitive data accidentally or on purpose.
Disgruntled employees or careless employees form a great threat to the organization.

NEW QUESTION: 219
Which of the following best describes the concept of Measured Service in cloud computing?
A. Cloud systems allocate a fixed immutable set of measured services to each customer.
B. Cloud systems offer elastic resources.
C. Cloud systems provide usage reports upon request, based on manual reporting.
D. Cloud systems automatically monitor resource usage and provide billing based on actual consumption.
Answer: D (LEAVE A REPLY)
The correct answer isD. Cloud systems automatically monitor resource usage and provide billing based on actual consumption.
Measured Service is one of theessential characteristics of cloud computingas defined by theNIST (National Institute of Standards and Technology). It implies that cloud systems automatically control and optimize resource usage by leveraging ametering capability. This capability tracks and reports resource consumption (such as CPU, storage, or bandwidth), which is used for billing, monitoring, and planning.
Key Characteristics:
Automatic Monitoring:Cloud platforms continuously track resource usage without manual intervention.
Billing Based on Usage:Customers are billed based on the actual consumption of resources (pay-as-you-go model).
Transparency:Users can view detailed usage reports to understand their resource utilization and associated costs.
Resource Optimization:Providers use these metrics to optimize resource allocation and improve efficiency.
Why Other Options Are Incorrect:
A: Fixed immutable set of measured services:This contradicts the concept of elasticity and resource pooling in cloud computing.
B: Elastic resources:While elasticity is a cloud characteristic, it does not directly define measured service.
C: Manual reporting:Measured service is aboutautomated, real-time monitoring and billing, not manual data gathering.
Real-World Example:
In AWS, services likeAmazon CloudWatchautomatically collect and provide usage metrics, and the AWS Billing Console shows the cost associated with each resource.
References:
CSA Security Guidance v4.0, Domain 1: Cloud Computing Concepts and Architectures
NIST SP 800-145 - The NIST Definition of Cloud Computing Cloud Controls Matrix (CCM) v3.0.1 - Metering and Billing Domain

NEW QUESTION: 220

Which of the following is most commonly used to program Application Programming Interface(API)?

A. SOAP

B. JSON

C. HTTP

D. REST

Answer: D (LEAVE A REPLY)

APIs are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over Hl'-P/S and thus work well across diverse environments.

Reference: CSA Security GuidelinesV.4 (reproduced here for the educational purpose)

NEW QUESTION: 221

Which of the following statements are NOT requirements of governance and enterprise risk management in a cloud environment?

A. Respect the interdependency of the risks inherent in the cloud supply chain and communicate the corporate risk posture and readiness to consumers and dependent parties.

B. Inspect and account for risks inherited from other members of the cloud supply chain and take active measures to mitigate and contain risks through operational resiliency.

C. Both B and C.

D. Negotiate long-term contracts with companies who use well-vetted software application to avoid the transient nature of the cloud environment.

E. Provide transparency to stakeholders and shareholders demonstrating fiscal solvency and organizational transparency.

Answer: (SHOW ANSWER)

NEW QUESTION: 222

CCM: The following list of controls belong to which domain of the CCM?

GRM 06 - Policy GRM 07 - Policy Enforcement GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews GRM 10 - Risk Assessments GRM 11 - Risk Management Framework

A. Governance and Retention Management

B. Governing and Risk Metrics

C. Governance and Risk Management

Answer: C (LEAVE A REPLY)

NEW QUESTION: 223

What is critical for securing serverless computing models in the cloud?

A. Disabling console access completely or using privileged access management

B. Validating the underlying container security

C. Managing secrets and configuration with the least privilege
D. Placing serverless components behind application load balancers
Answer: (SHOW ANSWER)
In serverless computing models, the primary security concern is ensuring that secrets (such as API keys, database credentials, etc.) and configuration settings are handled securely. The principle of least privilege means that these secrets and configurations should only be accessible by the minimum set of functions or services that truly need them, reducing the attack surface. Proper management of secrets and configurations ensures that unauthorized access or misuse is prevented.
Disabling console access completely or using privileged access management is important for securing any environment, but it is not specifically tied to serverless models. Validating the underlying container security is more relevant to containerized environments rather than serverless computing, which abstracts away infrastructure management. Placing serverless components behind application load balancers is useful for routing traffic but is not specifically critical for securing the serverless model itself. Managing secrets and access controls is a more direct concern for securing serverless environments.

NEW QUESTION: 224
The containment phase of the incident response lifecycle requires taking systems offline.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 225
According to NIST, what is cloud computing defined as?
A. A shared set of resources delivered over the Internet
B. A model for more-efficient use of network-based resources
C. Services that are delivered over the Internet to customers
D. A model for on-demand network access to a shared pool of configurable resources
Answer: D (LEAVE A REPLY)
NIST defines cloud computing as on-demand network access to a shared pool of configurable resources, aligning with the essential characteristics of cloud services.
Reference: [Security Guidance v5, Domain 1 - Cloud Computing Models]

NEW QUESTION: 226
What is an advantage of using Kubernetes for container orchestration?
A. Limited deployment options
B. Manual management of resources
C. Automation of deployment and scaling
D. Increased hardware dependency
Answer: (SHOW ANSWER)

Kubernetes provides automated deployment, scaling, and management of containerized applications, which enhances operational efficiency and scalability. Reference: [CCSK v5 Curriculum, Domain 8 - Cloud Workload Security]

NEW QUESTION: 227
Which of the following is a primary benefit of using Infrastructure as Code (IaC) in a security context?
A. Manual patch management
B. Ad hoc security policies
C. Static resource allocation
D. Automated compliance checks
Answer: (SHOW ANSWER)
The correct answer isD. Automated compliance checks.
Infrastructure as Code (IaC)is a key DevSecOps practice where infrastructure configurations are defined and managed through code. In a security context, the primary benefit of using IaC is the ability toautomate compliance checksand enforce security best practices consistently across environments.
Key Benefits of IaC in Security:
Automated Compliance:IaC allows for the embedding ofsecurity policies directly into configuration scripts. This means that when infrastructure is deployed, it automatically adheres to compliance requirements (like NIST, CIS benchmarks).
Consistency and Repeatability:Since IaC scripts are version-controlled, any configuration changes are tracked, minimizing the risk ofconfiguration drift.
Security by Design:By coding security configurations (like IAM roles, network ACLs, encryption settings), organizations ensure that every deployment meets security standards.
Reduced Human Error:Automating infrastructure provisioning reduces manual errors that can lead to vulnerabilities.
Why Other Options Are Incorrect:
A . Manual patch management:IaC promotes automated and repeatable configurations, reducing the need for manual patching.

B . Ad hoc security policies:IaC encouragesstandardized and consistentpolicies rather than ad hoc management.
C . Static resource allocation:IaC is dynamic and scalable, allowing for automatic scaling and configuration management rather than static resource setups.
Real-World Example:
Using tools likeTerraformorAWS CloudFormation, organizations can defineIAM policies, security group rules, and data encryption settingsas part of the infrastructure code. These configurations are then automatically checked for compliance against established policies during deployment.
Security and Compliance in IaC:
Organizations can integrate tools likeTerraform ComplianceorAWS Config Rulesto automatically verify that infrastructure settings align withregulatory requirementsandinternal security policies.
Reference:
CSA Security Guidance v4.0, Domain 10: Application Security
Cloud Computing Security Risk Assessment (ENISA) - Infrastructure as Code Best Practices Cloud Controls Matrix (CCM) v3.0.1 - Configuration and Change Management Domain

NEW QUESTION: 228
Which type of AI workload typically requires large data sets and substantial computing resources?
A. Evaluation
B. Data Preparation
C. Training
D. Inference
Answer: C (LEAVE A REPLY)
Among AI workloads, Training requires the most computational power and data resources.
Why AI Training is Computationally Intensive?
* Large datasets:
* AI models (e.g., deep learning, neural networks) require millions or billions of labeled data points.
* Training involves processing massive amounts of structured/unstructured data.
* High computational power:
* Training deep learning models involves running multiple passes (epochs) over data, adjusting weights, and optimizing parameters.
* Requires specialized hardware like GPUs (Graphics Processing Units), TPUs (Tensor Processing Units), and HPC (High-Performance Computing).
* Long training times:
* AI model training can take days, weeks, or even months depending on complexity.

* Cloud platforms offer distributed computing (multi-GPU training, parallel processing, auto-scaling).
* Cloud AI Training Benefits:
* Cloud providers (AWS, Azure, GCP) offer ML training services with on-demand scalable compute instances.
* Supports frameworks like TensorFlow, PyTorch, and Scikit-learn.
This aligns with:
* CCSK v5 - Security Guidance v4.0, Domain 14 (Related Technologies - AI and ML Security)
* Cloud AI Security Risks and AI Data Governance (CCM - AI Security Controls)

NEW QUESTION: 229
Which cloud storage technology is basically a virtual hard drive for instanced or VMs?
A. Object storage
B. Volume storage
C. Application
D. Database
E. Platform
Answer: (SHOW ANSWER)

NEW QUESTION: 230
When designing a cloud-native application that requires scalable and durable data storage, which storage option should be primarily considered?
A. Network Attached Storage (NAS)
B. Block storage
C. File storage
D. Object storage
Answer: D (LEAVE A REPLY)
Object storage is highly scalable and suitable for cloud-native applications that require durability and efficient storage of unstructured data. Reference: [CCSK Study Guide, Domain 9 - Data Storage Types]

NEW QUESTION: 231
Which attack surfaces, if any, does virtualization technology introduce?
A. Configuration and VM sprawl issues
B. Virtualization management components apart from the hypervisor
C. All of the above
D. The hypervisor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 232

What is the primary purpose of implementing a systematic data/asset classification and catalog system in cloud environments?
A. To automate the data encryption process across all cloud services
B. To reduce the overall cost of cloud storage solutions
C. To apply appropriate security controls based on asset sensitivity and importance
D. To increase the speed of data retrieval within the cloud environment
Answer: C (LEAVE A REPLY)
Classification and cataloging help assign security controls and manage data based on its sensitivity and criticality. Reference: [CCSK v5 Curriculum, Domain 9 - Data Security]

NEW QUESTION: 233
What process involves an independent examination of records, operations, processes, and controls within an organization to ensure compliance with cybersecurity policies, standards, and regulations?
A. Risk assessment
B. Audit
C. Penetration testing
D. Incident response
Answer: B (LEAVE A REPLY)
Auditing is an independent review process that validates adherence to policies, regulations, and standards. It is essential in assessing security posture. Reference: [Security Guidance v5, Domain 3 - Compliance]
[source 16].

NEW QUESTION: 234
Which of the following statements best reflects the responsibility of organizations regarding cloud security and data ownership?
A. Cloud providers are responsible for everything under the 'limited O responsibilities clauses.' The customer and the provider have joint accountability.
B. Cloud providers assume full responsibility for the security obligations, and cloud customers are accountable for overall compliance.
C. Data ownership rights are solely determined by the cloud provider, leaving organizations with no control or accountability over their data.
D. Organizations are accountable for the security and compliance of their data and systems, even though they may lack full visibility into their cloud provider's infrastructure.
Answer: D (LEAVE A REPLY)
TheShared Responsibility Modelin cloud computing establishes that:
Cloud providersare responsible for securing the underlyinginfrastructure, networking, and hardware.
Customers (organizations)are responsible for securingdata, identity and access management (IAM), encryption, and complianceobligations.

Data ownershipremainswith the customer, even though visibility into cloud infrastructure may belimited.
The major security challenge in cloud computing is thatorganizations lack full control over cloud infrastructurebut must still ensure that security policies align withregulatory requirements (e.g., GDPR, HIPAA, PCI DSS).
This principle is outlined in:
CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Enterprise Risk Management) Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) - Data Security and Governance.

NEW QUESTION: 235
Which of following responsibilities can never be transferred. even during cloud adoption?
A. Security
B. Governance
C. Infrastructure
D. Application Development
Answer: (SHOW ANSWER)
The primary issue to remember when governing cloud computing is that an organization can never outsource responsibility for governance, even when using external providers. This is always true, cloud or not, but is useful to keep in mind when navigating cloud computing's concepts of shared responsibility models Ref: CSA Security Guidelines V4.0

NEW QUESTION: 236
Which Cloud Service Provider (CSP) security measure is primarily used to filter and monitor HTTP requests to protect against SQL injection and XSS attacks?
A. CSP firewall
B. Virtual Appliance
C. Web Application Firewall
D. Intrusion Detection System
Answer: C (LEAVE A REPLY)
A Web Application Firewall (WAF) is primarily used to filter and monitor HTTP requests to protect web applications from various types of attacks, including SQL injection and cross-site scripting (XSS). WAFs work by analyzing incoming traffic and blocking malicious requests based on predefined rules or patterns, thus preventing attackers from exploiting vulnerabilities in web applications.
CSP firewall is more focused on general network security, not specifically on application layer attacks like SQL injection or XSS. Virtual Appliance refers to a virtualized instance of a security appliance, but it is not specifically designed for protecting against SQL injection and XSS attacks like a WAF. Intrusion Detection System (IDS) is used for detecting suspicious network activity and potential intrusions, but it is not focused on filtering web application traffic like a WAF.

NEW QUESTION: 237
Which provides guidelines for organizational information security standards including the selection, implementation, and management of controls taking into consideration the organization's information security risk environments?
A. ISO 27001
B. ISO 27002
C. NIST 800-9
D. FIPS 140-2
Answer: B (LEAVE A REPLY)
ISO 27002 is a standard which provides detailed description of security controls and how they need to implemented to provide effective ISMS.

NEW QUESTION: 238
Which approach is commonly used by organizations to manage identities in the cloud due to the complexity of scaling across providers?
A. Decentralization
B. Centralization
C. Federation
D. Outsourcing
Answer: C (LEAVE A REPLY)
Managing identities across multiple cloud providers is complex due to the need for scalability, interoperability, and consistent access control. Thefederationapproach is commonly used to address this challenge. Identity federation allows organizations to use a single set of credentials across different cloud providers by leveraging standards such as SAML, OAuth, or OpenID Connect. This enables seamless authentication and authorization without requiring separate identity management systems for each provider.
From theCCSK v5.0 Study Guide, Domain 6 (Identity, Entitlement, and Access Management), Section 6.3:
"Identity federation is a critical approach for managing identities in cloud environments, especially when scaling across multiple providers. Federation allows organizations to use a trusted identity provider (IdP) to authenticate users, enabling single sign-on (SSO) and consistent access control across disparate cloud services." Option C (Federation) is the correct answer.
Option A (Decentralization) is incorrect because decentralizing identity management increases complexity and reduces consistency across providers.
Option B (Centralization) is incorrect because, while centralized identity management may be used within a single organization, it does not scale effectively across multiple cloud providers without federation.
Option D (Outsourcing) is incorrect because outsourcing identity management does not inherently address the scalability and interoperability challenges of cloud environments.

Reference:
CCSK v5.0 Study Guide, Domain 6, Section 6.3: Identity Federation.
CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Domain 11.

NEW QUESTION: 239
What is a primary benefit of implementing Zero Trust (ZT) architecture in cloud environments?
A. Reduced attack surface and simplified user experience.
B. Eliminating the need for multi-factor authentication.
C. Increased attack surface and complexity.
D. Enhanced privileged access for all users.
Answer: (SHOW ANSWER)
Zero Trust (ZT) security architectureis amodern cloud security approachthat operates on the principle of" Never Trust, Always Verify." Primary Benefits of Zero Trust in Cloud:
Minimizes Attack Surface
Traditional security modelsassume trust within an internal network.
Zero Trust eliminates implicit trustand enforcescontinuous verification of user identities.
Reduces the risk ofdata breaches, insider threats, and lateral movement attacks.
Strong Authentication & Access Controls
Multi-Factor Authentication (MFA) & Just-in-Time (JIT) accessare mandatory inZero Trust models.
Usescontext-based access policies (device, location, behavior analytics)to enforceadaptive security.
Micro-Segmentation & Least Privilege Access
Restricts access to only necessary applications, minimizing lateral movement in cloud environments.
Micro-segmentation isolates workloads, reducing the impact of breaches.
Cloud-Native Zero Trust Integration
Cloud providers(AWS, Azure, Google Cloud)offerZero Trust Network Access (ZTNA)solutions.
Cloud Security Posture Management (CSPM)continuously scans cloud environments for security compliance.
This aligns with:
CCSK v5 - Security Guidance v4.0, Domain 12 (Identity, Entitlement, and Access Management) Zero Trust Cloud Security Architecture (CSA Zero Trust Working Group).

NEW QUESTION: 240
What's the best way for organizations to establish a foundation for safeguarding data, upholding privacy, and meeting regulatory requirements in cloud applications?
A. By implementing end-to-end encryption and multi-factor authentication
B. By conducting regular security audits and updates

C. By deploying intrusion detection systems and monitoring
D. By integrating security at the architectural and design level
Answer: D (LEAVE A REPLY)
The best way for organizations to establish a foundation for safeguarding data, upholding privacy, and meeting regulatory requirements in cloud applications is by integrating security at the architectural and design level. This approach ensures that security is built into the application from the start, rather than being added as an afterthought. By incorporating security features like encryption, access controls, and compliance measures during the design and development phases, organizations can better protect sensitive data, reduce vulnerabilities, and meet regulatory requirements more effectively.
While implementing encryption, multi-factor authentication, conducting audits, and deploying monitoring tools are also important, they are part of the overall security strategy rather than the foundational approach. Integrating security into the architecture ensures a more comprehensive, proactive security posture.

NEW QUESTION: 241
Which areas should be initially prioritized for hybrid cloud security?
A. Cloud storage management and governance
B. Data center infrastructure and architecture
C. IAM and networking
D. Application development and deployment
Answer: C (LEAVE A REPLY)
Identity and Access Management (IAM) and networking are essential for secure hybrid cloud environments, as they control access and communication across diverse environments. Reference: [Security Guidance v5, Domain 5 - IAM]

NEW QUESTION: 242
Which of the following is NOT one of the vulnerabilities that can lead of risk of "abuse of high privilege roles" or "Cloud provider malicious insider"?
A. AAA Vulnerabilities
B. System and 0S vulnerabilities
C. Poor enforcement of role definitions

D. Lack of data centre hardware redundancy
Answer: D (LEAVE A REPLY)
Redundancy has nothing to do with abuse of high privilege roles. All others can lead to risk of risk of
"abuse of high privilege roles" or "Cloud provider malicious insider"

NEW QUESTION: 243
Network logs from cloud providers are typically flow records, not full packet captures.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 244
In the context of IaaS, what are the primary components included in infrastructure?
A. Network configuration tools, storage encryption, and virtualization platforms
B. Compute, network, and storage resource pools
C. User authentication systems, application deployment services, and database management
D. Load balancers, firewalls, and backup solutions
Answer: (SHOW ANSWER)
Correct Option: B. Compute, network, and storage resource pools
In the Infrastructure as a Service (IaaS) model, the term "infrastructure" refers to the core physical and virtualized building blocks that form the basis of a cloud environment. These components are abstracted and pooled to offer on-demand provisioning to cloud consumers.
From the CSA Security Guidance v4.0 - Domain 1: Cloud Computing Concepts and Architectures:
"Infrastructure: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts."
- Section 1.1.4 Logical Model, CSA Security Guidance v4.0
Furthermore:
"IaaS consists of a facility, hardware, an abstraction layer, an orchestration (core connectivity and delivery) layer to tie together the abstracted resources, and APIs to remotely manage the resources and deliver them to consumers."
- Section 1.1.3.1 Infrastructure as a Service, CSA Security Guidance v4.0 These are commonly referred to as resource pools, and form the foundation of what IaaS delivers: virtual machines (compute), virtual networks (networking), and object/block storage systems (storage).
Why the Other Options Are Incorrect:
A . Network configuration tools, storage encryption, and virtualization platforms

➤ These are supporting technologies and security tools, not the actual infrastructure components that make up IaaS.
C . User authentication systems, application deployment services, and database management
➤ These fall under PaaS (Platform as a Service) and SaaS. IaaS does not manage applications or authentication; it provides the foundation upon which these services run.
D . Load balancers, firewalls, and backup solutions
➤ These are add-on services or features, not the core infrastructure components of IaaS. While often used alongside IaaS, they are not the essential building blocks of infrastructure.
Main Topic: Cloud Computing Concepts and Architectures
Source: CSA Security Guidance v4.0, Domain 1, Sections 1.1.3.1 & 1.1.4

NEW QUESTION: 245
Lack of CPU or network bandwidth and intermittent access to provisioned resources are examples of which of the following cloud risk?
A. Isolation failure
B. Software vulnerabilities
C. API vulnerabilities
D. Resource Exhaustion
Answer: D (LEAVE A REPLY)
They are all examples of resource exhaustion

NEW QUESTION: 246
Who is responsible for infrastructure security in Infrastructure as a service(IaaS) model?
A. Cloud Service provider
B. Cloud Service User
C. Cloud Service Architect
D. Shared responsibility between cloud service provider and cloud service customer
Answer: D (LEAVE A REPLY)
Infrastructure security is shared responsibility between cloud service provider and cloud customer.

NEW QUESTION: 247
Any given processor and memory will nearly always be running multiple workloads, often from different tenants.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 248

Which of the following is true about access policies in cybersecurity?
A. They are used to monitor real-time network traffic
B. They are solely concerned with user authentication methods
C. They provide data encryption protocols for secure communication
D. They define permissions and network rules for resource access
Answer: D (LEAVE A REPLY)
Access policies in cybersecurity are critical for managing and controlling how users and devices access resources within a network or cloud environment. These policies are primarily concerned with defining permissions and rules that govern access to resources. They help organizations implement role-based access control (RBAC) or attribute-based access control (ABAC), which specify who can access what resources and under what conditions.
In the context of cloud computing, access policies are typically enforced using Identity and Access Management (IAM) tools and services, which allow administrators to define and manage the permissions associated with user identities. Access policies include various rules that specify allowed or denied actions based on roles, user attributes, device types, or network conditions.
For example, in the AWS environment, access policies are written in JSON and define permissions for services like EC2, S3, or RDS. Similarly, Azure uses Role-Based Access Control (RBAC) to manage resource access policies.
Access policies are not concerned with real-time monitoring (option A), user authentication methods (option B), or encryption protocols (option C). Instead, they explicitly focus on defining access permissions and controlling how resources are utilized.
References:
CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management
Cloud Computing Security Risk Assessment (ENISA) - Identity and Access Management section
Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

NEW QUESTION: 249
In cloud environments, why are Management Plane Logs indispensable for security monitoring?
A. They provide real-time threat detection and response
B. They detail the network traffic between cloud services
C. They track cloud administrative activities
D. They report on user activities within applications
Answer: C (LEAVE A REPLY)
Management Plane Logs are indispensable for security monitoring because they track administrative activities related to the management of cloud resources. These logs capture actions such as user logins, configuration changes, access control modifications, and resource provisioning or decommissioning. By monitoring these logs, organizations can detect unauthorized or suspicious administrative actions, ensuring that only authorized

personnel are making changes to critical cloud resources. This helps prevent configuration errors, privilege escalation, and potential attacks targeting the management plane.
Other options refer to different aspects of security monitoring but are not specifically related to the role of Management Plane Logs.

NEW QUESTION: 250
Which of the following best describes the shared responsibility model in cloud security?
A. Cloud providers handle physical infrastructure security while customers handle workload security.
B. Cloud providers handle both infrastructure and workload security.
C. Neither cloud providers nor customers are responsible for security.
D. Customers handle both infrastructure and workload security.
Answer: (SHOW ANSWER)
The shared responsibility model is a key concept in cloud security. According to the CSA Security Guidance v4.0, Domain 1, Section 1.2.1, the responsibility for security is shared between the cloud provider and the customer, depending on the service model (IaaS, PaaS, SaaS).
Specifically:
"Infrastructure as a Service: Just like PaaS, the provider is responsible for foundational security, while the cloud user is responsible for everything they build on the infrastructure."
"At a high level, security responsibility maps to the degree of control any given actor has over the architecture stack." This means the cloud provider handles the physical security (data center, servers, etc.), while the customer is responsible for securing the workloads they deploy on the infrastructure, such as their applications, data, configurations, and access controls.
Incorrect Options:
B is incorrect because providers do not manage your workload or data security.
C is false - both parties share responsibilities.
D is incorrect because customers do not manage the cloud's physical infrastructure.
Reference:
CSA Security Guidance v4.0 - Domain 1, Section 1.2.1: "Cloud Security and Compliance Scope and Responsibilities"

NEW QUESTION: 251
Which cloud security model type provides generalized templates for helping implement cloud security?
A. Reference architectures
B. Design patterns
C. Controls models or frameworks
D. Conceptual models or frameworks
E. Cloud Controls Matrix (CCM)

Answer: (SHOW ANSWER)

NEW QUESTION: 252
What goal is most directly achieved by implementing controls and policies that aim to provide a complete view of data use and exposure in a cloud environment?
A. Enhancing data governance and compliance
B. Simplifying cloud service integrations
C. Increasing cloud data processing speed
D. Reducing the cost of cloud storage
Answer: A (LEAVE A REPLY)
Implementing these controls supports data governance and compliance by providing visibility into data handling and potential exposures. Reference: [Security Guidance v5, Domain 9 - Data Security]

NEW QUESTION: 253
In preparing for cloud incident response, why is it crucial to establish a cloud deployment registry?
A. To document all cloud services APIs
B. To maintain a log of all incident response activities and have efficient reporting
C. To track incident support options, know account details, and contact information
D. To list all cloud-compliant software
Answer: (SHOW ANSWER)
Establishing a cloud deployment registry is crucial for cloud incident response because it helps track critical information related to the cloud environment, such as incident support options, account details, and contact information for cloud service providers (CSPs). This registry provides a central place where key details about cloud services and deployments are documented, allowing the incident response team to quickly access necessary information, escalate issues to the appropriate CSP support teams, and coordinate response efforts effectively.