CloudSecurityAlliance.CCSK.v2026-04-21.q144

Exam Code:	CCSK
Exam Name:	Certificate of Cloud Security Knowledge v5 (CCSKv5.0)
Certification Provider:	Cloud Security Alliance
Free Question Number:	144
Version:	v2026-04-21
# of views:	112
# of Questions views:	1440
https://www.freepdfdumps.com/CloudSecurityAlliance.CCSK.v2026-04-21.q144.html	

NEW QUESTION: 1
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 cloudaccount credentials is an aspect of identity and access management, not related to risk registries.

NEW QUESTION: 2
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][16 source].

NEW QUESTION: 3
What is one primary operational challenge associated with using cloud-agnostic container strategies?
A. Limiting deployment to a single cloud service
B. Establishing identity and access management protocols
C. Reducing the amount of cloud storage used
D. Management plane compatibility and consistent controls
Answer: D (LEAVE A REPLY)
One of the primary operational challenges associated with using cloud-agnostic container strategies is ensuring management plane compatibility and consistent controls across multiple cloud environments. Cloud-agnostic strategies aim to make containers portable between different cloud providers. However, each cloud provider has its own management tools, APIs, and security controls, which can lead to complexities in maintaining consistent policies, monitoring, and management practices across different cloud environments. Limiting deployment to a single cloud service is contrary to the goal of a cloud-agnostic strategy, which seeks to avoid reliance on a single cloud provider. Establishing identity and access management protocols is important but not unique to cloud-agnostic strategies; IAM challenges exist regardless of cloud approach. Reducing the amount of cloud storage used is a general optimization concern, not specifically related to cloud-agnostic containers.

NEW QUESTION: 4
How does network segmentation primarily contribute to limiting the impact of a security breach?
A. By reducing the threat of breaches and vulnerabilities
B. Confining breaches to a smaller portion of the network
C. Allowing faster data recovery and response
D. Monitoring and detecting unauthorized access attempts
Answer: (SHOW ANSWER)
Network segmentation isolates sections of the network, limiting the spread of a breach and containing it to a specific segment. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 5
How can key management be leveraged to prevent cloud providers from inappropriately accessing customer data?
A. Select cloud providers within the same country as customer

B. Segregate keys from the provider hosting data
C. Stipulate encryption in contract language
D. Use strong multi-factor authentication
E. Secure backup processes for key management systems
Answer: (SHOW ANSWER)

NEW QUESTION: 6
In Identity and Access Management (IAM) containment, why is it crucial to understand if an attacker escalated their identity?
A. It aids in determining the source IP of the attacker.
B. Because it simplifies the recovery process and increases the response time.
C. To prevent further unauthorized access and limit the management plane blast radius.
D. To facilitate the eradication of malware.
Answer: C (LEAVE A REPLY)
Privilege escalationis a majorcloud security riskbecause attackers can:
Gain administrative access to cloud environments.
Modify security configurations, disable logs, and exfiltrate sensitive data.
Expand the attack blast radius, compromising multiple cloud resources.
To mitigateidentity escalation threats, security teams must:
Implement strong IAM policies with least privilege access.
Use Multi-Factor Authentication (MFA) and Just-in-Time (JIT) access.
Monitor IAM logs for unusual privilege escalations and lateral movements.
This is detailed in:
CCSK v5 - Security Guidance v4.0, Domain 12 (Identity, Entitlement, and Access Management) Cloud Controls Matrix (CCM) - IAM Controls and Privilege Escalation Prevention.

NEW QUESTION: 7
CCM: A hypothetical start-up company called "ABC" provides a cloud based IT management solution. They are growing rapidly and therefore need to put controls in place in order to manage any changes in their production environment. Which of the following Change Control & Configuration Management production environment specific control should they implement in this scenario?
A. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
B. Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant)-impacting (physical and virtual) applications and system- system interface (API) designs and configurations, infrastructure network and systems components.

C. All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
D. None of the above
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
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: 9
Why is a service type of network typically isolated on different hardware?
A. It manages resource pools for cloud consumers
B. It requires unique security
C. It has distinct functions from other networks
D. It requires distinct access controls
E. It manages the traffic between other networks
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following statements best defines the "authorization" as a component of identity, entitlement, and access management?
A. Checking data storage to make sure it meets compliance requirements
B. Establishing/asserting the identity to the application
C. Enforcing the rules by which access is granted to the resources
D. The process of specifying and maintaining access policies

E. Giving a third party vendor permission to work on your cloud solution
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Why is early integration of pre-deployment testing crucial in a cybersecurity project?
A. It identifies issues before full deployment, saving time and resources.
B. It increases the overall testing time and costs.
C. It allows skipping final verification tests.
D. It eliminates the need for continuous integration.
Answer: (SHOW ANSWER)
Integrating testing early helps identify security vulnerabilities and configuration issues before they reach production, reducing remediation costs and time. Reference: [Security Guidance v5, Domain 10 - Application Security]

NEW QUESTION: 12
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: 13
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: 14
Which term describes any situation where the cloud consumer does
not manage any of the underlying hardware or virtual machines?
A. Serverless computing
B. Abstraction
C. Virtual machineless
D. Container
E. Provider managed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
When mapping functions to lifecycle phases, which functions are required to successfully process data?
A. Create, Store, and Use
B. Create and Store
C. Create, Store, Use, and Share
D. Create, Use, Store, and Delete
E. Create and Use
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
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: 17
In the IaaS shared responsibility model, which responsibility typically falls on the Cloud Service Provider (CSP)?
A. Encrypting data at rest
B. Ensuring physical security of data centers
C. Managing application code
D. Configuring firewall rules
Answer: B (LEAVE A REPLY)
In the Infrastructure as a Service (IaaS) shared responsibility model, the Cloud Service Provider (CSP) is typically responsible for securing the physical infrastructure, which includes the physical security of data centers, servers, networking hardware, and the physical security controls that protect them from unauthorized access or damage. Encrypting data at rest is typically the responsibility of the consumer, though the CSP may offer tools to help with this. Managing application code is the responsibility of the consumer, as they control and deploy the applications on the infrastructure provided by the CSP. Configuring firewall rules is also the responsibility of the consumer, as they manage the configuration of the virtual network, including security rules like firewalls.

NEW QUESTION: 18
Which aspect of cybersecurity can AI enhance by reducing false positive alerts?
A. Anomaly detection
B. Assisting analysts
C. Threat intelligence
D. Automated responses
Answer: A (LEAVE A REPLY)
AI can enhance anomaly detection in cybersecurity by analyzing large volumes of data and identifying patterns that deviate from normal behavior. By using machine learning algorithms, AI can improve the accuracy of anomaly detection, reducing false positive alerts. This helps security teams focus on genuine threats while minimizing distractions from irrelevant alerts.

Assisting analysts is a valid benefit of AI, but reducing false positives directly improves anomaly detection capabilities. Threat intelligence refers to gathering and analyzing information about potential threats but isn't directly focused on reducing false positives in the same way as anomaly detection. Automated responses can be part of AI's role in cybersecurity, but reducing false positives is more directly related to improving anomaly detection.

NEW QUESTION: 19
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: 20
What is true of searching data across cloud environments?
A. You might not have the ability or administrative rights to search or access all hosted data.
B. Search and discovery time is always factored into a contract between the consumer and provider.
C. The cloud provider must conduct the search with the full administrative controls.
D. All cloud-hosted email accounts are easily searchable.
E. You can easily search across your environment using any E-Discovery tool.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
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 entry log
B. An access log
C. An entitlement matrix
D. A validation process
E. A support table
Answer: (SHOW ANSWER)

NEW QUESTION: 22

What is known as a code execution environment running within an operating system that shares and uses the resources of the operating system?
A. Abstraction
B. Platform-based Workload
C. Virtual machine
D. Container
E. Pod
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
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: (SHOW ANSWER)
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: 24
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: 25
In a cloud context, what does entitlement refer to in relation to a user's permissions?
A. The authentication methods a user is required to use when accessing the cloud environment.
B. The level of technical support a user is entitled to from the cloud service provider.
C. The resources or services a user is granted permission to access in the cloud environment.

D. The ability for a user to grant access permissions to other users in the cloud environment.

Answer: C (LEAVE A REPLY)

In a cloud context, entitlement refers to the specific resources or services a user is granted permission to access based on their roles or permissions. This includes access to applications, data, or cloud services, and is typically managed through Identity and Access Management (IAM) systems, which define what users can do and what they can access within the cloud environment.

NEW QUESTION: 26

A cloud deployment of two or more unique clouds is known as:

A. A Community Cloud

B. Jericho Cloud Cube Model

C. A Private Cloud

D. Infrastructures as a Service

E. A Hybrid Cloud

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

What is the purpose of the "Principle of Least Privilege" in Identity and Access Management (IAM)?

A. To minimize the risk of unauthorized access by assigning access rights based on role requirements

B. To streamline access across diverse systems or organizations

C. To continuously monitor user activity for suspicious behavior

D. To implement multiple layers of security checks for access control

Answer: (SHOW ANSWER)

The Principle of Least Privilege (PoLP) is a foundational concept in IAM, highlighted in the CSA Security Guidance v4.0 - Domain 12: Identity, Entitlement, and Access Management. It ensures users, systems, and processes are granted only the permissions necessary to perform their tasks - and nothing more.

"Least privilege refers to granting the minimum level of access - or permissions - needed for users or services to perform their required functions, thereby reducing the attack surface and limiting potential damage from misuse or compromise."

- CSA Security Guidance v4.0, Domain 12

This principle:

Reduces the likelihood of accidental or malicious misuse

Limits damage in the case of credential theft

Supports compliance with least privilege mandates in frameworks like ISO/IEC 27001 and NIST Incorrect options:

B is related to federation, not least privilege

C involves monitoring and analytics, not permission assignment
D is about defense in depth, which is broader than PoLP
Reference:
CSA Security Guidance v4.0 - Domain 12: IAM
CCM v3.0.1 - IAM-01, IAM-05 (Covers least privilege and role-based access control)

NEW QUESTION: 28
What is a key consideration when implementing AI workloads to ensure they adhere to security best practices?
A. AI workloads do not require special security considerations compared to other workloads.
B. AI workloads should be openly accessible to foster collaboration and innovation.
C. AI workloads should be isolated in secure environments with strict access controls.
D. Security practices for AI workloads should focus solely on protecting the AI models.
Answer: C (LEAVE A REPLY)
AI workloads often require isolation and strict access controls to prevent unauthorized access and safeguard sensitive data involved in machine learning processes. Reference: [CCSK Study Guide, Domain 8 - AI Workload Security]

NEW QUESTION: 29
APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches. Which one of the five characteristics is described as: a consumer can unilaterally provision computing capabilities such as server time and network storage as needed.
A. On-demand self-service
B. Resource pooling
C. Measured service
D. Broad network access
E. Rapid elasticity
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?

A. Functional Testing
B. Dynamic Application Security Testing (DAST)
C. Code Review
D. Static Application Security Testing (SAST)
E. Unit Testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
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: (SHOW ANSWER)
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: 33
ENISA: "VM hopping" is:
A. Looping within virtualized routing systems.
B. Instability in VM patch management causing VM routing errors.
C. Lack of vulnerability management standards.
D. Using a compromised VM to exploit a hypervisor, used to take control of other VMs.

E. Improper management of VM instances, causing customer VMs to be commingled with other customer systems.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
In the context of FaaS, what is primarily defined in addition to functions?
A. Data storage
B. Network configurations
C. User permissions
D. Trigger events
Answer: (SHOW ANSWER)
In the context of Function as a Service (FaaS), trigger events are primarily defined in addition to the functions themselves. FaaS allows you to run individual functions in response to events, such as HTTP requests, file uploads, database changes, or messages in a queue. These trigger events initiate the execution of the serverless function, making them a core part of FaaS architecture.
Data storage is not directly defined by FaaS, as storage is typically managed separately (e.g., cloud storage or databases). Network configurations are not the main focus of FaaS, since cloud providers manage the underlying network infrastructure. User permissions may be relevant but are typically handled through identity and access management (IAM), not directly tied to the definition of a FaaS function.

NEW QUESTION: 35
Why is governance crucial in balancing the speed of adoption with risk control in cybersecurity initiatives?
A. Only involves senior management in decision-making
B. Speeds up project execution irrespective of and focuses on systemic risk
C. Ensures adequate risk management while allowing innovation
D. Ensures alignment between global compliance standards
Answer: (SHOW ANSWER)
Governance in cybersecurity is crucial because it provides the framework to ensure that security risks are adequately managed while still allowing the organization to adopt new technologies and innovations at a reasonable pace. Effective governance helps organizations balance the need for security controls with the need for agility and speed in adopting new solutions. It ensures that risks are identified, assessed, and mitigated without unnecessarily slowing down progress or stifling innovation.
Without governance, there is a risk that security concerns may be overlooked, or too many restrictions might be placed on adoption, leading to delays or failure to innovate. Proper governance strikes the right balance between security and agility.

NEW QUESTION: 36

The Software Defined Perimeter (SDP) includes which components?
A. Client, Firewall, and Gateway
B. Controller, Firewall, and Gateway
C. Client, Controller, Firewall, and Gateway
D. Client, Controller, and Firewall
E. Client, Controller, and Gateway
Answer: E (LEAVE A REPLY)

NEW QUESTION: 37
When implementing a Zero Trust (ZT) strategy, which approach is considered fundamental for ensuring enterprise security and connectivity?
A. Allowing unrestricted access to resources within local networks but restricting cloud access
B. Implementing perimeter-based security as the primary defense mechanism
C. Enforcing strict access control and verification for all users and devices
D. Only allowing trusted devices to connect to local/office networks
Answer: C (LEAVE A REPLY)
The core tenet of Zero Trust is that no entity-internal or external-should be trusted by default. Every request for access must be authenticated, authorized, and encrypted based on granular access policies and continuous validation of identity, device health, location, and behavior.
ZT eliminates reliance on traditional network perimeter models (which B and A describe), focusing instead on microsegmentation and dynamic policy enforcement to prevent lateral movement within a network.
This approach is detailed in Domain 7: Infrastructure Security of the CCSK guidance. It emphasizes identity-aware access control, continuous monitoring, and contextual risk assessment as foundational elements of a secure Zero Trust framework.
Reference:
CSA Security Guidance v4.0 - Domain 7: Infrastructure Security

NEW QUESTION: 38
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][16source].

NEW QUESTION: 39
What does orchestration automate within a cloud environment?
A. Monitoring application performance
B. Manual configuration of security policies
C. Installation of operating systems
D. Provisioning of VMs, networking and other resources
Answer: (SHOW ANSWER)
In a cloud environment, orchestration automates the provisioning and management of various cloud resources, including virtual machines (VMs), networking, storage, and other infrastructure components. Cloud orchestration involves the use of software to coordinate and automate tasks that would otherwise require manual intervention, improving efficiency, scalability, and consistency across the environment.
Monitoring application performance is typically handled by monitoring tools, not orchestration. Manual configuration of security policies is something that can be automated through policy management but is not the focus of orchestration. Installation of operating systems is part of provisioning resources, but orchestration primarily focuses on automating the overall management of infrastructure and services, not just the installation of operating systems.

NEW QUESTION: 40
Which resilience tool helps distribute network or application traffic across multiple servers to ensure reliability and availability?
A. Redundancy
B. Auto-scaling
C. Load balancing
D. Failover
Answer: C (LEAVE A REPLY)
Load balancing is a key resilience strategy in both traditional and cloud environments. It evenly distributes network or application traffic across multiple servers to ensure no single server becomes a point of failure or overloaded, thereby improving system availability, performance, and fault tolerance.
In cloud infrastructure, load balancers may work at various OSI layers (Layer 4 or Layer 7) and are often integrated into cloud platforms as managed services (e.g., AWS Elastic Load

Balancer or Azure Load Balancer). They play a critical role in mitigating risks like traffic spikes, system failure, or regional outages.
This technique is described in Domain 7: Infrastructure Security of the CCSK guidance, which highlights tools like load balancing, redundant systems, and failover mechanisms to support cloud resilience and availability.
Reference:
CSA Security Guidance v4.0 - Domain 7: Infrastructure Security

NEW QUESTION: 41
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: B (LEAVE A REPLY)
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: 42
Which type of security tool is essential for enforcing controls in a cloud environment to protect endpoints?
A. Unified Threat Management (UTM).
B. Web Application Firewall (WAF).
C. Endpoint Detection and Response (EDR).
D. Intrusion Detection System (IDS).
Answer: C (LEAVE A REPLY)
Endpoint Detection and Response (EDR)is acritical security tool for cloud environmentsthatmonitors, detects, and responds to endpoint threats.
Why EDR is Essential for Cloud Security?
Real-Time Threat Detection & Response
EDRcontinuously monitors endpoint activity(e.g., cloud VMs, servers, containers).
Detectsanomalous behavior, malware, and unauthorized access attempts.
Automated Remediation & Forensics
UsesMachine Learning (ML) & AItoanalyze cloud endpoint telemetry.

Supportsautomated response actions (isolating infected endpoints, rolling back malicious changes).
Cloud-Native Security Integration
Works withCloud Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).
Enables proactive threat hunting in hybrid and multi-cloud environments.
Complements Other Cloud Security Tools
WAF (Web Application Firewall)protects againstweb-based attacks (OWASP Top 10)but doesnot provide endpoint security.
UTM (Unified Threat Management)is more suited fortraditional perimeter security (firewalls, IPS/IDS).
IDS (Intrusion Detection System)only detects threats, whereasEDR actively responds to them.
This aligns with:
CCSK v5 - Security Guidance v4.0, Domain 7 (Infrastructure Security)
Cloud Controls Matrix (CCM) - Endpoint Security Controls.

NEW QUESTION: 43
Which phase of the CSA secure software development life cycle (SSDLC) focuses on ensuring that an application or product is deployed onto a secure infrastructure?
A. Continuous Build, Integration, and Testing
B. Continuous Delivery and Deployment
C. Secure Design and Architecture
D. Secure Coding
Answer: B (LEAVE A REPLY)
The Continuous Delivery and Deployment phase emphasizes deploying applications securely, ensuring infrastructure security is prioritized during deployment. Reference: [CCSK v5 Curriculum, Domain 10 - Secure Development Lifecycle]

NEW QUESTION: 44
Which aspect of assessing cloud providers poses the most significant challenge?
A. Poor provider documentation and over-reliance on pooled audit
B. Inconsistent policy standards and the proliferation of provider requirements
C. Excessive details shared by the cloud provider and consequent information overload
D. Limited visibility into internal operations and technology
Answer: D (LEAVE A REPLY)
The most significant challenge in assessing cloud providers is the limited visibility into the provider's internal security controls, operations, and technology. Cloud customers often lack direct access to the infrastructure, policies, and mechanisms behind the cloud service due to the shared responsibility model and provider confidentiality.

According to CSA Security Guidance v4.0 - Domain 4: Compliance and Audit Management:
"The cloud customer's inability to see and assess the cloud provider's security controls and practices-known as limited visibility-is one of the most critical barriers to cloud assurance." (CSA Security Guidance v4.0, Domain 4: Compliance and Audit Management)
This is further echoed in CCM (Cloud Controls Matrix):
AAC-03 (Audit Assurance and Compliance) - "Cloud providers should make sufficient audit mechanisms available to allow the customer to assess control implementation. Lack of visibility significantly impacts trust and compliance validation." The other options may contribute to audit difficulties, but D represents the core, systemic challenge faced in cloud provider assessments.

NEW QUESTION: 45
What is the newer application development methodology and philosophy focused on automation of application development and deployment?
A. BusOps
B. Agile
C. SecDevOps
D. DevOps
E. Scrum
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following best describes a benefit of using VPNs for cloud connectivity?
A. VPNs are more cost-effective than any other connectivity option.
B. VPNs provide secure, encrypted connections between data centers and cloud deployments.
C. VPNs eliminate the need for third-party authentication services.
D. VPNs provide higher bandwidth than direct connections.
Answer: (SHOW ANSWER)
A VPN (Virtual Private Network) is commonly used to provide secure, encrypted connections between on- premises data centers and cloud deployments, ensuring that data transmitted across the internet is protected from unauthorized access. VPNs help safeguard sensitive information byencrypting the communication channel, offering confidentiality and integrity for the data in transit.
VPNs are not necessarily more cost-effective than other options like dedicated private connections or direct connect services, especially when considering performance and reliability. While VPNs provide secure connections, they do not eliminate the need for third-party authentication services, which are still important for controlling access. VPNs typically offer lower bandwidth and higher latency compared to direct connection solutions, which are designed for higher-performance use cases.

NEW QUESTION: 47
Which of the following best describes the primary purpose of cloud security frameworks?
A. To implement detailed procedural instructions for security measures
B. To organize control objectives for achieving desired security outcomes
C. To ensure compliance with all regulatory requirements
D. To provide tools for automated security management
Answer: B (LEAVE A REPLY)
Cloud security frameworks organize control objectives to guide security practices and achieve specific security goals. Reference: [CCSK Study Guide, Domain 3 - Cloud Governance]

NEW QUESTION: 48
How can web security as a service be deployed for a cloud consumer?
A. On the premise through a software or appliance installation
B. By proxying or redirecting web traffic to the cloud provider
C. None of the above
D. Both A and C
E. By utilizing a partitioned network drive
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
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: 50
Which of the following best describes the primary function of Cloud Detection and Response (CDR) in cybersecurity?
A. Detect and respond to security threats in the cloud
B. Manage cloud-based applications
C. Provide cost management for cloud services
D. Optimize cloud storage performance
Answer: A (LEAVE A REPLY)
Cloud Detection and Response (CDR) is an emerging capability that focuses specifically on detecting and responding to threats in cloud environments. While not deeply detailed in the core CSA Security Guidance v4.0, CDR is an evolution of traditional SIEM and endpoint detection strategies applied to cloud-native infrastructures.
In CSA Security Guidance v4.0 - Domain 9: Incident Response, it's made clear that:
"Security monitoring and detection capabilities in the cloud must be able to identify suspicious behavior, policy violations, and misconfigurations - often across multiple layers such as infrastructure, applications, and identity."
- CSA Security Guidance v4.0, Domain 9: Incident Response
CDR platforms typically include:
Threat detection across cloud workloads (e.g., compute, storage, IAM misuse) Real-time alerts Automated or manual response mechanisms Integration with cloud-native logging services like AWS CloudTrail, Azure Monitor, or GCP Audit Logs Incorrect options:
B is about application management, not threat detection.
C relates to cloud cost optimization tools.
D refers to cloud storage tuning, unrelated to threat detection.
Reference:
CSA Security Guidance v4.0 - Domain 9: Incident Response

NEW QUESTION: 51
Use elastic servers when possible and move workloads to new instances.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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: 53
Which principle reduces security risk by granting users only the permissions essential for their role?
A. Role-Based Access Control
B. Unlimited Access
C. Mandatory Access Control
D. Least-Privileged Access
Answer: D (LEAVE A REPLY)
The principle of least privilege limits access to only necessary permissions, reducing the risk of misuse and exposure of sensitive data. Reference: [CCSK v5 Curriculum, Domain 5 - IAM]

NEW QUESTION: 54
Which of the following best describes an authoritative source in the context of identity management?
A. A list of permissions assigned to different users
B. A network resource that handles authorization requests

C. A database containing all entitlements
D. A trusted system holding accurate identity information
Answer: D (LEAVE A REPLY)
An authoritative source in the context of identity management refers to a trusted system that contains accurate identity information. This system is considered the source of truth for identities, and other systems or services within the organization rely on it for the most up-to-date and verified identity details, such as usernames, attributes, roles, and permissions.
A list of permissions assigned to different users represents access control data but is not considered the authoritative source of identity. A network resource that handles authorization requests refers to authorization mechanisms but is not the authoritative source for identity. A database containing all entitlements could be part of an identity management system but is not necessarily the authoritative source for identity itself; it focuses more on access rights and entitlements.

NEW QUESTION: 55
What are the key outcomes of implementing robust cloud risk management practices?
A. Ensuring the security and resilience of cloud environments
B. Negotiating shared responsibilities
C. Transferring compliance to the cloud service provider via inheritance
D. Reducing the need for compliance with regulatory requirements
Answer: A (LEAVE A REPLY)
The key outcomes of implementing robust cloud risk management practices focus on ensuring the security and resilience of cloud environments. This involves identifying, assessing, and mitigating risks associated with the use of cloud services, such as security threats, data privacy issues, and service availability concerns. By adopting strong risk management practices, organizations can better protect their data, ensure business continuity, and maintain compliance with regulations, which ultimately strengthens the overall security and reliability of their cloud environments.
Negotiating shared responsibilities is an important aspect of cloud security but is not the direct outcome of risk management practices. It's about clarifying roles between the customer and provider. Transferring compliance to the cloud service provider via inheritance is not the complete picture. While cloud service providers may help with compliance, the responsibility for compliance and risk management is still shared.
Reducing the need for compliance withregulatory requirements is incorrect. Robust risk management practices help ensure compliance with regulatory requirements, not reduce the need for them.

NEW QUESTION: 56
Which statement best describes why it is important to know how data is being accessed?
A. The devices used to access data may have different ownership characteristics.

B. The devices used to access data have different storage formats.
C. The device may affect data dispersion.
D. The devices used to access data use a variety of applications or clients and may have different security characteristics.
E. The devices used to access data use a variety of operating systems and may have different programs installed on them.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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: D (LEAVE A REPLY)
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: 58
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: A (LEAVE A REPLY)
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: 59
CCM: A company wants to use the IaaS offering of some CSP. Which of the following options for using CCM is NOT suitable for the company as a cloud customer?
A. Use CCM to build a detailed list of requirements and controls that they want their CSP to implement
B. None of the above
C. Use CCM to help assess the risk associated with the CSP
D. Submit the CCM on behalf of the CSP to CSA Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry that documents the security controls provided by CSPs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
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: D (LEAVE A REPLY)

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: 61
What is an essential security characteristic required when using multi-tenanttechnologies?
A. Segmented and segregated customer environments
B. Limited resource allocation
C. Resource pooling
D. Abstraction and automation
Answer: (SHOW ANSWER)
In multi-tenant technologies, the fundamental security requirement issegmented 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 stronglogical isolationbetween tenants to mitigate risks likedata 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.
Reference:
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: 62
What is a primary benefit of implementing micro-segmentation within a Zero Trust Architecture?
A. Reduces the need for encryption across the network
B. Simplifies network design and maintenance
C. Enhances security by isolating workloads from each other
D. Increases the overall performance of network traffic
Answer: C (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: 63
How does centralized logging simplify security monitoring and compliance?
A. It consolidates logs into a single location.
B. It decreases the amount of data that needs to be reviewed.
C. It encrypts all logs to prevent unauthorized access.
D. It automatically resolves all detected security threats.
Answer: A (LEAVE A REPLY)
Centralized logging aggregates logs in one location, making it easier to monitor, analyze, and comply with regulatory requirements. Reference: [Security Guidance v5, Domain 6 - Security Monitoring]

NEW QUESTION: 64
What is the primary goal of implementing DevOps in a software development lifecycle?
A. To create a separation between development and operations
B. To eliminate the need for IT operations by automating all tasks
C. To enhance collaboration between development and IT operations for efficient delivery
D. To reduce the development team size by merging roles

Answer: (SHOW ANSWER)
DevOps aims to improve collaboration and integration between development and operations teams, streamlining delivery and enhancing software quality. Reference: [CCSK Study Guide, Domain 10 - DevOps & DevSecOps]

NEW QUESTION: 65
Which of the following best describes a primary risk associated with the use of cloud storage services?
A. Increased cost due to redundant data storage practices
B. Unauthorized access due to misconfigured security settings
C. Inherent encryption failures within all cloud storage solutions
D. Complete data loss due to storage media degradation
Answer: (SHOW ANSWER)
One of the primary risks associated with cloud storage services is unauthorized access due to misconfigured security settings. Cloud storage providers typically offer a range of configuration options for managing access, but if these settings are not properly configured (e.g., improper access control lists, missing encryption, or inadequate permissions), it can lead to unauthorized users gaining access to sensitive data. This is a common and significant risk in cloud environments, which is why securing and correctly configuring access controls is critical.

NEW QUESTION: 66
What is the primary function of a Load Balancer Service in a Software Defined Network (SDN) environment?
A. To create isolated virtual networks
B. To monitor network performance and activity
C. To distribute incoming network traffic across multiple destinations
D. To encrypt data for secure transmission
Answer: C (LEAVE A REPLY)
The correct answer isC. To distribute incoming network traffic across multiple destinations.
ALoad Balancer Servicein anSDN environmentis responsible forefficiently distributing network trafficacross multiple servers or instances. This ensures high availability, reliability, and optimized resource usage.
Key Functions:
Traffic Distribution:Balances incoming requests to various servers based on predefined algorithms (round-robin, least connections, etc.).
High Availability:Prevents server overload and reduces downtime by distributing workload.
Scalability:Automatically adjusts as the number of requests or available resources changes.
Health Monitoring:Continually checks server availability and responsiveness to avoid directing traffic to non-responsive instances.

Why Other Options Are Incorrect:
A . Isolated virtual networks:Creating isolated networks is a function of network virtualization, not load balancing.
B . Monitor network performance:Monitoring is done by network monitoring tools, not load balancers.
D . Encrypt data for secure transmission:Encryption is handled by security protocols like TLS/SSL, not load balancers.
Real-World Example:
Services likeAWS Elastic Load Balancer (ELB)andAzure Load Balancerensure that traffic is distributed efficiently across instances, maintaining performance and uptime.
Reference:
CSA Security Guidance v4.0, Domain 7: Infrastructure Security
Cloud Computing Security Risk Assessment (ENISA) - SDN and Load Balancing Cloud Controls Matrix (CCM) v3.0.1 - Network and Infrastructure Domains

NEW QUESTION: 67
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: D (LEAVE A REPLY)
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: 68
What is the purpose of access policies in the context of security?
A. Access policies encrypt sensitive data to protect it from disclosure and unrestricted access.
B. Access policies define the permitted actions that can be performed on resources.
C. Access policies determine where data can be stored.
D. Access policies scan systems to detect and remove malware infections.
Answer: B (LEAVE A REPLY)

Access policies are a critical component of security frameworks that specify and enforce the permitted actions that users or systems can perform on resources, such as files, applications, or services. These policies help ensure that only authorized individuals or systems have access to certain resources and that they can only perform authorized actions, such as reading, writing, or modifying the resources. Access policies are fundamental in managing security and preventing unauthorized access, misuse, or attacks. Access policies encrypt sensitive data is incorrect because encryption of sensitive data is typically handled by encryption policies, not access policies. Access policies determine where data can be stored is more related to data management policies rather than access control. Access policies scan systems for malware is related to security measures such as antivirus or anti-malware tools, not the scope of access control policies.

NEW QUESTION: 69
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: 70
Which of the following best describes the purpose of cloud security control objectives?
A. They are standards that cannot be modified to suit the unique needs of different cloud environments.
B. They focus on the technical aspects of cloud security with less consideration on the broader organizational goals.
C. They dictate specific implementation methods for securing cloud environments, tailored to individual cloud providers.
D. They provide outcome-focused guidelines for desired controls, ensuring measurable and adaptable security measures
Answer: D (LEAVE A REPLY)
Cloud security control objectives are designed to provide outcome-focused guidelines that help organizations achieve specific security goals in the cloud. These objectives are typically high-level and focused on the desired security outcomes, rather than dictating the exact technical implementation methods. This allows the security measures to be adaptable and applicable across different cloud environments and service models, while also being measurable to ensure effectiveness.

NEW QUESTION: 71
All cloud services utilize virtualization technologies.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
What primary aspects should effective cloud governance address to ensure security and compliance?
A. Service availability, disaster recovery, load balancing, and latency
B. Decision making, prioritization, monitoring, and transparency
C. Encryption, redundancy, data integrity, and scalability
D. Authentication, authorization, accounting, and auditing
Answer: B (LEAVE A REPLY)
Effective cloud governance focuses on managing and overseeing cloud resources to ensure that security, compliance, and business objectives are met. Key aspects include:
Decision making: Establishing clear processes for how decisions are made regarding cloud resource usage, security measures, and compliance strategies.
Prioritization: Ensuring that critical security and compliance risks are prioritized and addressed first.

Monitoring: Continuously monitoring cloud environments for security threats, performance issues, and compliance violations.
Transparency: Ensuring that governance activities are visible to stakeholders, enabling accountability and making it easier to demonstrate compliance with laws, regulations, and internal policies.
These aspects help organizations maintain control over their cloud environments while ensuring they meet security and regulatory requirements.

NEW QUESTION: 73
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: 74

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: 75

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.
Reference:
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: 76
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: 77
What is true of a workload?
A. It is always a virtual machine
B. It must be containerized
C. It does not require a hardware stack
D. It is configured for specific, established tasks
E. It is a unit of processing that consumes memory
Answer: E (LEAVE A REPLY)

NEW QUESTION: 78
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: (SHOW ANSWER)
The correct answer isD. Cloud Security Posture Management (CSPM).
Cloud Security Posture Management (CSPM) is a comprehensive tool designed to identify and remediate misconfigurations and compliance violations incloud 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 likeAWS Config,Azure Security Center, andGoogle Cloud Security

Command Centerautomate the process of checking forsecurity policy violationsandconfiguration 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 likePalo Alto Prisma CloudorAWS Configcan automatically detect ifIAM policiesare overly permissive or ifS3 bucketsare publicly accessible, helping to maintain compliance and reduce attack surfaces.
Reference:
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: 79
What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?
A. The actual size of the data and the storage format
B. The fragmentation and encryption algorithms employed
C. The physical location of the data and how it is accessed
D. The language of the data and how it affects the user
E. The implications of storing complex information on simple storage systems
Answer: E (LEAVE A REPLY)

NEW QUESTION: 80
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][16source].

NEW QUESTION: 81
Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?
A. More physical control over assets and processes.
B. Greater reliance on contracts, audits, and assessments due to lack of visibility or management.
C. Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
D. Decreased requirement for proactive management of relationship and adherence to contracts.
E. None of the above.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
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: 83
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. Multi-application, single tenant environments
B. Long distance relationships
C. Single tenant environments
D. Distributed computing arrangements
E. Multi-tenant environments
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Which of the following information security policies defines the use of an organization's IT resources?
A. Acceptable Use Policy
B. Remote Work Policy
C. Data Handling Policy
D. Use of Cloud Services Policy
Answer: A (LEAVE A REPLY)
"An Acceptable Use Policy (AUP) defines appropriate and prohibited uses of organizational IT resources, including cloud services."
- CSA Security Guidance v4.0 - Domain 2: Governance and Risk Management

NEW QUESTION: 85
How does the variability in Identity and Access Management (IAM) systems across cloud providers impact a multi-cloud strategy?
A. Adds complexity by requiring separate configurations and integrations.
B. Ensures better security by offering diverse IAM models.
C. Reduces costs by leveraging different pricing models.
D. Simplifies the management by providing standardized IAM protocols.
Answer: A (LEAVE A REPLY)
Each cloud provider may use different IAM protocols and configurations, increasing complexity and requiring customized integration for each cloud environment. Reference: [CCSK Study Guide, Domain 5 - Identity and Access Management]

NEW QUESTION: 86
If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, how is the information likely to be obtained?
A. It would require an act of war
B. It may require a subpoena of the provider directly
C. It would require a previous access agreement
D. It would require a previous contractual agreement to obtain the application or access to the environment
E. It would never be obtained in this situation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
What is a commonly used method by which hybrid cloud integrates data centers with public cloud?
A. Using VPN or dedicated links

B. Using peer-to-peer networks
C. Using local area network (LAN)
D. Using satellite connections
Answer: (SHOW ANSWER)
"Hybrid cloud deployments commonly use secure network connections such as VPNs or dedicated links (e.g., Direct Connect or ExpressRoute) to integrate on-premises data centers with public cloud environments."
- CSA Security Guidance v4.0 - Domain 1.1.2.3: Deployment Models
Reference:
CSA Security Guidance v4.0 - Domain 1

NEW QUESTION: 88
What is a common characteristic of Platform as a Service (PaaS)?
A. Satisfies compliance and security requirements
B. Integration with application development frameworks and middleware capabilities
C. Limited configuration options increases security risks
D. Fully hosted application stack
Answer: B (LEAVE A REPLY)
Platform as a Service (PaaS) provides a development and deployment environment with resources that enable users to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.
According to CSA Security Guidance v4.0 - Domain 1: Cloud Computing Concepts and Architectures:
"PaaS adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools that are supported by the stack." (CSA Security Guidance v4.0, Domain 1) This integration with app development and middleware is the key defining feature of PaaS.

NEW QUESTION: 89
Which cloud-based service model enables companies to provide client-based access for partners to databases or applications?
A. Infrastructure-as-a-service (IaaS)
B. Platform-as-a-service (PaaS)
C. Identity-as-a-service (IDaaS)
D. Software-as-a-service (SaaS)
E. Desktop-as-a-service (DaaS)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90

Which feature in cloud enhances security by isolating deployments similar to deploying in distinct data centers?

A. A single deployment for all applications

B. Shared deployments for similar applications

C. Randomized deployment configurations

D. Multiple independent deployments for applications

Answer: (SHOW ANSWER)

Multiple independent deployments help isolate workloads, reducing the potential impact of a breach by confining it to a single deployment environment. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 91

Which statement best describes the Data Security Lifecycle?

A. The Data Security Lifecycle has five stages, is circular, and varies in that some data may never pass through all stages.

B. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages.

C. The Data Security Lifecycle has six stages, is strictly linear, and never varies.

D. The Data Security Lifecycle has five stages, can be non-linear, and is distinct in that data must always pass through all phases.

E. The Data Security Lifecycle has six stages, can be non-linear, and is distinct in that data must always pass through all phases.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 92

What Identity and Access Management (IAM) process decides to permit or deny a subject access to system objects like networks, data, or applications?

A. Authorization

B. Federation

C. Authentication

D. Provisioning

Answer: (SHOW ANSWER)

The correct answer isA. Authorization. In Identity and Access Management (IAM),authorizationis the process of determining whether a subject (user, application, or device) has the right to access a specific system object, such as networks, data, or applications. Authorization decisions are made after successful authentication and are based on the subject's permissions, roles, or attributes.
Key Characteristics of Authorization:
Decision Making:Determines if access ispermitted or deniedbased on policies or permissions.
Role and Attribute-Based Access:Often uses Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) mechanisms to enforce policies.
Post-Authentication Process:Occursafter authenticationhas verified the user's identity.
Resource-Specific:Determines the level of access or specific operations (like read, write, execute) a user is allowed.
Example Scenario:
When a user logs into a cloud platform, the system firstauthenticatesthe user (verifies their identity) and thenauthorizestheir access to specific resources, such as viewing data in an S3 bucket or managing a VM instance. The access policies define what actions the authenticated user can perform.
Why Other Options Are Incorrect:
B . Federation:Involves linking a user's identity across multiple systems or domains but does not decide access permissions.
C . Authentication:The process of verifying a user's identity, typically through passwords, biometrics, or multi-factor authentication (MFA), but it does not determine resource access.
D . Provisioning:Refers to creating and managing user accounts and permissions, but it does not make real-time access decisions.
Real-World Context:
In cloud environments, services like AWS IAM or Azure AD use policies toauthorizeuser actions after they have beenauthenticated. For instance, an AWS IAM policy might allow a user to list S3 buckets but deny deletion.
Reference:
CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management
Cloud Computing Security Risk Assessment (ENISA) - IAM and Access Control
Cloud Controls Matrix (CCM) v3.0.1 - Identity and Access Management Domain

NEW QUESTION: 93
Why is it important to capture and centralize workload logs promptly in a cybersecurity environment?
A. To simplify application debugging processesB Primarily to reduce data storage costs
B. Logs may be lost during a scaling event
C. To comply with data privacy regulations
Answer: (SHOW ANSWER)

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: 94
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: (SHOW ANSWER)
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: 95
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: 96
Vulnerability assessments cannot be easily integrated into CI/CD pipelines because of provider restrictions.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
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: 98
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: 99
Why is it important to plan and coordinate response activities for incidents affecting the Cloud Service Provider (CSP)?
A. It eliminates the need for monitoring systems
B. It ensures a systematic approach, minimizing damage and recovery time
C. It guarantees that no incidents will occur in the future
D. It reduces the frequency of security audits required
Answer: B (LEAVE A REPLY)
Correct Option: B. It ensures a systematic approach, minimizing damage and recovery time Effective incident response planning is critical in cloud environments due to the

shared responsibility model. When an incident affects the CSP, cloud customers must be prepared to coordinate response activities, ensure clarity of roles, and maintain continuity of operations.
From CSA Security Guidance v4.0 - Domain 9: Incident Response:
"Organizations must establish systematic and coordinated incident response plans for cloud incidents. This helps to reduce the impact, minimize damage, and shorten recovery time. Coordination with the CSP is vital to ensure responsibilities are understood and executed."
- Domain 9: Incident Response, CSA Security Guidance v4.0
The guidance emphasizes that preparation and communication channels with CSPs should be defined in advance, as delays in joint response can significantly increase the scope and impact of incidents.
Why the Other Options Are Incorrect:
A . It eliminates the need for monitoring systems
➤ Incorrect. Monitoring remains essential for detecting incidents early. Planning and monitoring serve different functions.
C . It guarantees that no incidents will occur in the future
➤ No system is immune to incidents. Planning reduces impact, but does not prevent incidents entirely.
D . It reduces the frequency of security audits required
➤ Audits are required based on compliance and regulatory needs, not on incident response planning.

NEW QUESTION: 100
How does virtualized storage help avoid data loss if a drive fails?
A. Data loss is unavoidable with drive failures
B. Full back ups weekly
C. Drives are backed up, swapped, and archived constantly
D. Incremental backups daily
E. Multiple copies in different locations
Answer: (SHOW ANSWER)

NEW QUESTION: 101
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: 102
When leveraging a cloud provider, what should be considered to ensure application security requirements are met?
A. Fully rely on cloud provider's security features
B. Cloud providers guarantee complete security compliance
C. Assume default settings are adequate for all applications
D. Customize additional security measures to address gaps
Answer: D (LEAVE A REPLY)

Application security in the cloud must be viewed as a shared responsibility. Providers deliver basic security features, but custom configurations and additional controls are often needed to meet organizational requirements.
From CSA Security Guidance v4.0 - Domain 10: Application Security:
"Cloud consumers should not assume default security settings are sufficient. Security features provided by cloud service providers often require additional configuration and hardening. Custom security controls may be needed to address specific organizational risks and compliance needs." (CSA Security Guidance v4.0, Domain 10)

NEW QUESTION: 103
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: 104
ENISA: Which is a potential security benefit of cloud computing?
A. ISO 27001 certification
B. Greater compatibility with customer IT infrastructure
C. More efficient and timely system updates
D. Lock-In
E. Provider can obfuscate system O/S and versions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
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: C (LEAVE A REPLY)
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: 106
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. Governance and Enterprise Risk Management
B. Infrastructure Security
C. Information Governance
D. Compliance and Audit Management
E. Legal Issues: Contracts and Electronic Discovery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
How does running applications on distinct virtual networks and only connecting networks as needed help?
A. It reduces the blast radius of a compromised system
B. It enables you to configure applications around business groups
C. It provides dynamic and granular policies with less management overhead
D. It locks down access and provides stronger data security
E. It reduces hardware costs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
In federated identity management, what role does the identity provider (IdP) play in relation to the relying party?
A. The IdP relies on the relying party to authenticate and authorize users.
B. The relying party makes assertions to the IdP about user authorizations.
C. The IdP and relying party have no direct trust relationship.
D. The IdP makes assertions to the relying party after building a trust relationship.
Answer: D (LEAVE A REPLY)
In federated identity management, the identity provider (IdP) is responsible for authenticating users and making assertions about their identity to the relying party (which could be a service or application that trusts the IdP). The IdP and the relying party establish a trust relationship in advance, which allows the IdP to assert that a user is authenticated, often in the form of security tokens or assertions like SAML or OpenID Connect.
The IdP that authenticates users and makes assertions, not the relying party. The relying party does not make assertions to the IdP; the relying party relies on assertions made by the IdP. The IdP and relying party do have a direct trust relationship in federated identity management.

NEW QUESTION: 109
What is defined as the process by which an opposing party may obtain private documents for use in litigation?
A. Scope
B. Discovery
C. Subpoena
D. Custody
E. Risk Assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 110
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: (SHOW ANSWER)
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: 111
Containers are highly portable code execution environments.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
Which technique is most effective for preserving digital evidence in a cloud environment?
A. Analyzing management plane logs
B. Regularly backing up data
C. Isolating the compromised system
D. Taking snapshots of virtual machines
Answer: D (LEAVE A REPLY)
Taking snapshots of virtual machines (VMs) is one of the most effective techniques for preserving digital evidence in a cloud environment. Snapshots capture the entire state of a VM, including its memory, configuration, and disk contents at a particular point in time. This allows investigators to preserve evidence as it was at the moment of the incident, enabling detailed analysis without altering the original state of the system.
While isolating the compromised system is important to prevent further damage, snapshots are more directly useful for preserving evidence. Backing up data and analyzing management plane logs are also valuable for incident response, but they don't capture the complete state of a compromised system as effectively as snapshots do.

NEW QUESTION: 113
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: (SHOW ANSWER)
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: 114
What is the primary purpose of the CSA Security, Trust, Assurance, and Risk (STAR) Registry?
A. To provide cloud service rate comparisons
B. To certify cloud services for regulatory compliance
C. To document security and privacy controls of cloud offerings
D. To manage data residency and localization requirements
Answer: C (LEAVE A REPLY)
The CSA STAR Registry provides transparency by listing security and privacy controls of CSPs, helping customers assess provider security. Reference: [CCSK Overview, STAR Registry]

NEW QUESTION: 115
How does artificial intelligence pose both opportunities and risks in cloud security?
A. AI enhances security without any adverse implications
B. AI mainly reduces manual work with no significant security impacts
C. AI enhances detection mechanisms but could be exploited for sophisticated attacks
D. AI is only beneficial in data management, not security
Answer: C (LEAVE A REPLY)
While AI improves threat detection, it also introduces risks as attackers can use it to develop advanced attack methods. Organizations must balance these risks. Reference: [CCSK Study Guide, Domain 12 - AI and Security]

NEW QUESTION: 116
What are the encryption options available for SaaS consumers?
A. Client/application and file/folder encryption
B. Any encryption option that is available for volume storage, object storage, or PaaS
C. Object encryption Volume storage encryption
D. Provider-managed and (sometimes) proxy encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
In the context of FaaS, what is primarily defined in addition to functions?
A. Data storage
B. Network configurations
C. Trigger events

D. User permissions

Answer: (SHOW ANSWER)

In the context of Function as a Service (FaaS), trigger events are primarily defined in addition to the functions themselves. FaaS allows you to run individual functions in response to events, such as HTTP requests, file uploads, database changes, or messages in a queue. These trigger events initiate the execution of the serverless function, making them a core part of FaaS architecture.

Data storage is not directly defined by FaaS, as storage is typically managed separately (e.g., cloud storage or databases). Network configurations are not the main focus of FaaS, since cloud providers manage the underlying network infrastructure. User permissions may be relevant but are typically handled through identity and access management (IAM), not directly tied to the definition of a FaaS function.

NEW QUESTION: 118

What is one significant way Artificial Intelligence, particularly Large Language Models, is impacting IT and security?

A. Eliminating the need for encryption

B. Replacing all IT personnel

C. Automating threat detection and response

D. Standardizing software development languages

Answer: C (LEAVE A REPLY)

Artificial Intelligence (AI), including Large Language Models (LLMs), is significantly impacting IT and security by enablingautomation of threat detection and response. AI-driven tools can analyze vast amounts of data in real-time, identify patterns indicative of threats, and respond faster than human operators, improving security operations efficiency and effectiveness.

From theCCSK v5.0 Study Guide, Domain 12 (Emerging Technologies), Section 12.4: "AI and machine learning, including Large Language Models, are transforming cloud security by automating threat detection and response. These technologies can process and analyze security logs, network traffic, and user behavior to identify anomalies and potential threats, enabling rapid incident response and reducing the burden on security teams." Option C (Automating threat detection and response) is the correct answer.

Option A (Eliminating the need for encryption) is incorrect because AI does not eliminate the need for encryption; encryption remains a fundamental security control.

Option B (Replacing all IT personnel) is incorrect because AI augments, rather than replaces, IT and security personnel.

Option D (Standardizing software development languages) is incorrect because AI does not primarily focus on standardizing development languages.

Reference:

CCSK v5.0 Study Guide, Domain 12, Section 12.4: AI and Machine Learning in Cloud Security.

NEW QUESTION: 119
Which technique involves assessing potential threats through analyzing attacker capabilities, motivations, and potential targets?
A. Threat modeling
B. Vulnerability assessment
C. Incident response
D. Risk assessment
Answer: A (LEAVE A REPLY)
Threat modeling is the technique used to assess potential threats by analyzing attacker capabilities, motivations, and potential targets. It involves identifying, understanding, and prioritizing potential security threats in the context of a system or application. By considering the attackers' possible objectives and methods, organizations can design security controls to mitigate these risks proactively.
Vulnerability assessment focuses on identifying and evaluating vulnerabilities in a system, but it does not explicitly analyze attacker behavior or motivations. Incident response involves responding to security incidents after they occur, not proactively assessing potential threats. Risk assessment involves evaluating potential risks to an organization, but threat modeling specifically focuses on understanding and mitigating potential threats, making it a more targeted technique for this purpose.

NEW QUESTION: 120
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: (SHOW ANSWER)
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: 121
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: (SHOW ANSWER)
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: 122

In the context of incident response, which phase involves alerts validation to reduce false positives and estimates the incident's scope?

A. Preparation

B. Post-Incident Analysis

C. Detection & Analysis

D. Containment, Eradication, & Recovery

Answer: C (LEAVE A REPLY)

The Detection & Analysis phase of incident response involves the validation of alerts to reduce false positives and estimating the scope of the incident. During this phase, security teams assess whether the alerts indicate an actual incident, investigate the nature and severity of the threat, and determine the affected systems, data, and potential impact. This phase is critical for accurately identifying the scope of the issue and ensuring appropriate actions are taken in subsequent phases, such as containment and eradication.

NEW QUESTION: 123

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: 124

How does serverless computing impact infrastructure management responsibility?

A. Requires extensive on-premises infrastructure

B. Shifts more responsibility to cloud service providers

C. Increases workload for developers

D. Eliminates need for cloud service providers

Answer: B (LEAVE A REPLY)

Serverless computing shifts infrastructure management responsibility to the CSP, allowing customers to focus on application logic rather than infrastructure. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security]

NEW QUESTION: 125
In the shared security model, how does the allocation of responsibility vary by service?
A. Shared responsibilities should be consistent across all services.
B. Based on the per-service SLAs for security.
C. Responsibilities are the same across IaaS, PaaS, and SaaS in the shared model.
D. Responsibilities are divided between the cloud provider and the customer based on the service type.
Answer: D (LEAVE A REPLY)
The division of security responsibilities changes according to the service model. In IaaS, CSCs handle more security responsibilities, while in SaaS, the CSP manages more of the security aspects. Reference: [Security Guidance v5, Domain 1 - Shared Responsibility Model][17 source].

NEW QUESTION: 126
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: D (LEAVE A REPLY)
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: 127
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: 128
ENISA: Which is not one of the five key legal issues common across all scenarios:
A. Intellectual property
B. Data protection
C. Outsourcing services and changes in control
D. Globalization
E. Professional negligence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 129
Why is it essential to include key metrics and periodic reassessment in cybersecurity governance?
A. To meet legal requirements and avoid fines
B. To ensure effective and continuous improvement of security measures
C. To document all cybersecurity incidents and monitor them overtime
D. To reduce the number of security incidents to zero
Answer: B (LEAVE A REPLY)
Including key metrics and periodic reassessment in cybersecurity governance is essential for ensuring the effective and continuous improvement of security measures. Metrics provide a way to assess the current state of security, identify gaps, and measure progress over time. Periodic reassessment allows organizations to adapt to emerging threats and vulnerabilities, ensuring that security controls remain relevant and effective as the threat landscape evolves.
While meeting legal requirements is important, the primary reason for metrics and reassessment is continuous improvement, not just legal compliance. Documenting cybersecurity incidents is important, but the main focus of key metrics and reassessment is improving and adapting security strategies. Zero security incidents is not feasible; the goal is to reduce incidents and manage risk, not to eliminate all incidents entirely.

NEW QUESTION: 130

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: A (LEAVE A REPLY)
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: 131
Which approach creates a secure network, invisible to unauthorized users?
A. Firewalls
B. Software-Defined Perimeter (SDP)
C. Virtual Private Network (VPN)
D. Intrusion Detection System (IDS)
Answer: (SHOW ANSWER)
An SDP creates a "dark" network, visible only to authorized users, enhancing security by hiding infrastructure from potential attackers. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 132
What is true of security as it relates to cloud network infrastructure?
A. You should deploy your cloud firewalls identical to the existing firewalls.

B. You should implement a default allow with cloud firewalls and then restrict as necessary.
C. You should apply cloud firewalls on a per-network basis.
D. You should always open traffic between workloads in the same virtual subnet for better visibility.
E. You should implement a default deny with cloud firewalls.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 133
After an incident has been identified and classified, which activity is typically performed during the Containment, Eradication, and Recovery phase of incident response?
A. Documenting lessons learned and finalizing reports
B. Restoring systems to operational status while preventing recurrence
C. Monitoring network traffic for anomalies
D. Identifying and classifying security threats
Answer: (SHOW ANSWER)
According to the CSA Security Guidance v4.0, Domain 9: Incident Response, the Containment, Eradication, and Recovery phase follows detection and analysis. This phase focuses on limiting the damage, removing the threat, and restoring systems to a secure operational state.
"After detection and analysis, containment, eradication, and recovery are necessary to prevent further damage and restore systems."
"Recovery is the process of restoring affected systems and services to a fully operational state in a controlled and safe manner." This includes activities such as:
Removing malware or compromised systems
Rebuilding or restoring from backups
Applying patches
Validating that vulnerabilities are fixed
Monitoring for any recurrence
Incorrect options:
A refers to the Post-Incident Activity phase.
C is part of Detection and Analysis.
D is also part of the initial phase of the incident response cycle.
Reference:
CSA Security Guidance v4.0 - Domain 9: Incident Response (Section: Containment, Eradication, and Recovery)

NEW QUESTION: 134
In the initial stage of implementing centralized identity management, what is the primary focus of cybersecurity measures?
A. Developing incident response plans

B. Integrating identity management and securing devices
C. Implementing advanced threat detection systems
D. Deploying network segmentation
Answer: (SHOW ANSWER)
In the initial stage of implementing centralized identity management, the primary focus of cybersecurity measures is to integrate identity management (such as Single Sign-On (SSO), Role-Based Access Control (RBAC), and user directories) and secure devices that interact with the identity management system. This ensures that only authorized users and devices can access the network and resources, helping to establish a strong foundation for secure and efficient identity and access management.
Developing incident response plans is important but typically comes after establishing core security controls like identity management. Implementing advanced threat detection systems is a later stage security measure, after foundational controls like identity management are in place. Deploying network segmentation is a useful security strategy, but it is not the primary focus in the early stages of centralized identity management.

NEW QUESTION: 135
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: B (LEAVE A REPLY)
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.
Reference:
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: 136
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: D (LEAVE A REPLY)
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: 137
In the context of server-side encryption handled by cloud providers, what is the key attribute of this encryption?
A. The data is encrypted using symmetric encryption.
B. The data is not encrypted in transit.
C. The data is encrypted using customer or provider keys after transmission to the cloud.
D. The data is encrypted before transmission to the cloud.
Answer: (SHOW ANSWER)
In the context of server-side encryption handled by cloud providers, the data is encrypted after transmission to the cloud using either provider-managed keys or customer-managed keys. The cloud provider takes responsibility for encrypting the data when it is stored in the cloud, ensuring that the data at rest is protected.
Server-side encryption typically uses symmetric encryption for performance reasons, but this attribute is not what defines the encryption process. Also, server-side encryption focuses on protecting data once it's in the cloud, not before transmission. Encryption in transit is typically handled separately from server-side encryption and applies to data as it moves between the client and the cloud.

NEW QUESTION: 138
Which feature of cloud networks ensures strong separation between customer environments?
A. Virtual local area network (VLANs)

B. Resource pooling
C. Software-defined networking
D. Elasticity
Answer: A (LEAVE A REPLY)
Correct Option: A. Virtual Local Area Networks (VLANs)
VLANs are widely used in cloud and traditional environments to provide logical separation of network traffic. In a multi-tenant cloud environment, VLANs help ensure that one customer's network traffic is isolated from another's, providing a key layer of segmentation and security.
From CSA Security Guidance v4.0 - Domain 7: Infrastructure Security:
"To isolate tenants in multi-tenant environments, cloud providers often rely on mechanisms such as VLANs, VXLANs, or other software-defined networking technologies. VLANs ensure that different customer environments remain logically separated even though they share the same physical infrastructure."
- Domain 7: Infrastructure Security, CSA Security Guidance v4.0
Why the Other Options Are Incorrect:
B . Resource pooling
➤ Refers to shared infrastructure in the cloud. It enables multi-tenancy but does not enforce separation between tenants.
C . Software-defined networking (SDN)
➤ SDN provides flexibility and programmability in networking. While it can support separation, VLANs are the actual mechanism used for enforcing it.
D . Elasticity
➤ Elasticity refers to scaling resources up/down based on demand. It has nothing to do with tenant isolation or network separation.

NEW QUESTION: 139
For third-party audits or attestations, what is critical for providers to publish and customers to evaluate?
A. Network or architecture diagrams including all end point security devices in use
B. Scope of the assessment and the exact included features and services for the assessment
C. Service-level agreements between all parties
D. Full API access to all required services
E. Provider infrastructure information including maintenance windows and contracts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
Which component is primarily responsible for filtering and monitoring HTTP/S traffic to and from a web application?
A. Anti-virus Software

B. Load Balancer
C. Web Application Firewall
D. Intrusion Detection System
Answer: C (LEAVE A REPLY)
A Web Application Firewall (WAF) is primarily responsible for filtering and monitoring HTTP/S traffic to and from a web application. It is designed to protect web applications by filtering and monitoring traffic for malicious requests, such as SQL injection, cross-site scripting (XSS), and other common application-layer attacks. A WAF helps secure web applications by analyzing the HTTP/S traffic and blocking any harmful requests before they reach the application.
Anti-virus Software is used to detect and remove malicious software on endpoints and devices but is not designed to filter HTTP/S traffic specifically for web applications. Load Balancer is used to distribute network traffic across multiple servers to ensure performance and reliability, but it does not focus on security filtering. Intrusion Detection System (IDS) monitors network traffic forsuspicious activity but operates at a different level of the network stack and is not focused solely on web application traffic.

NEW QUESTION: 141
How can Identity and Access Management (IAM) policies on keys ensure adherence to the principle of least privilege?
A. By rotating keys on a regular basis
B. By using default policies for all keys
C. By specifying fine-grained permissions
D. By granting root access to administrators
Answer: C (LEAVE A REPLY)
Fine-grained permissions enable specific control over who can access certain resources, thus enforcing the least privilege principle. Reference: [Security Guidance v5, Domain 5 - IAM]

NEW QUESTION: 142
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: (SHOW ANSWER)
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: 143
Which of the following items is NOT an example of Security as a Service (SecaaS)?
A. Web filtering
B. Authentication
C. Intrusion detection
D. Provisioning
E. Spam filtering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
Which opportunity helps reduce common application security issues?
A. Decreased use of micro-services
B. Default deny
C. Elastic infrastructure
D. Segregation by default
E. Fewer serverless configurations
Answer: C (LEAVE A REPLY)