Question #1 *Topic 1*

Which practice best helps mitigate security risks by minimizing root/core access and restricting deployment creation?

A. Enforcing the principle of 'trust and eventually verify on demand'

B. Disabling multi-factor authentication for staff and focusing on decision makers' accounts

C. Deploying applications with full access and applying restrictions based on the need to object

D. Enforcing the principle of least privilege

Suggested Answer: *D*

unrulyBuidl 1 month, 3 weeks ago

Selected Answer: D

D is the correct answer because - the principle of least privilege ensures only the DevOps team/member can deploy and no one else.

upvoted 1 times

tomqrlz 5 months ago

Selected Answer: D

d is correct

upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *D*

SM_2026 5 days, 2 hours ago

Selected Answer: D

D is Correct, as cloud agnostic denotes Multicloud and hence Management plan poses operational challenge for compatibility with various cloud vendors

upvoted 1 times

Question #3 *Topic 1*

How can the use of third-party libraries introduce supply chain risks in software development?

A. They are usually open source and do not require vetting

B. They might contain vulnerabilities that can be exploited

C. They fail to integrate properly with existing continuous integration pipelines

D. They might increase the overall complexity of the codebase

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Which aspect is most important for effective cloud governance?

A. Establishing a governance hierarchy

B. Implementing best-practice cloud security control objectives

C. Formalizing cloud security policies

D. Negotiating SLAs with cloud providers

Suggested Answer: *B*

Community vote distribution

B (100%)

Rickio 4 months, 1 week ago

Selected Answer: C

A. Establishing a governance hierarchy: This is important for organization, but a hierarchy without policies has no rules to enforce.

B. Implementing best-practice cloud security control objectives: While these are vital for managing security, they are a subset of governance. Controls are the "how," whereas governance (policy) is the "why" and "what." You cannot effectively choose or audit controls if you haven't first defined your goals through policy.

D. Negotiating SLAs with cloud providers: This is a part of vendor management. While critical for business operations, it is too narrow to be the "most important" aspect of overall cloud governance.

upvoted 1 times

Ray_Parash 1 year ago

Selected Answer: B

The most important aspect for effective cloud governance is the implementation of strong frameworks and policies. These form the foundation of cloud governance by providing structure and guidelines that align IT capabilities with the business objectives. Policies are implemented with the help of control objectives

upvoted 2 times

Question #5 *Topic 1*

What are the essential characteristics of cloud computing as defined by the NIST model?

A. Resource sharing, automated recovery, universal connectivity, distributed costs, fair pricing

B. High availability, geographical distribution, scaled tenancy, continuous resourcing, market pricing

C. On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service

D. Equal access to dedicated hosting, isolated networks, scalability resources, and automated continuous provisioning

Suggested Answer: *C*

Community vote distribution

C (100%)

Necron 10 months, 2 weeks ago

Selected Answer: C

NIST definition

upvoted 1 times

Question #6 *Topic 1*

Which of the following best describes the responsibility for security in a cloud environment?

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

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 Customers (CSCs) are solely responsible for security in the cloud environment. The Cloud Service Providers (CSPs) are accountable.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

When comparing different Cloud Service Providers (CSPs), what should a cybersecurity professional be mindful of regarding their organizational structures?

A. All CSPs use the same organizational structure and terminology.

B. Different CSPs may have similar structures but use varying terminology.

C. CSPs have vastly different organizational structures and identical terminology.

D. Terminology difference in CSPs does not affect cybersecurity practices.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Why is identity management at the organization level considered a key aspect in cybersecurity?

A. It replaces the need to enforce the principles of the need to know

B. It ensures only authorized users have access to resources

C. It automates and streamlines security processes in the organization

D. It reduces the need for regular security training and auditing, and frees up cybersecurity budget

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following cloud essential characteristics refers to the capability of the service to scale resources up or down quickly and efficiently based on demand?

A. On-Demand Self-Service

B. Broad Network Access

C. Resource Pooling

D. Rapid Elasticity

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

In a hybrid cloud environment, why would an organization choose cascading log architecture for security purposes?

A. To convert cloud logs into on-premise formats.

B. To reduce the number of network hops for log collection

C. To facilitate efficient central log collection

D. To use CSP's analysis tools for log analysis.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

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)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

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

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

B. To streamline communication with cloud service providers and customers

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

D. To increase the speed of incident response team deployments

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

What is the primary function of Privileged Identity Management (PIM) and Privileged Access Management (PAM)?

A. Encrypt data transmitted over the network

B. Manage the risk of elevated permissions

C. Monitor network traffic and detect intrusions

D. Ensure system uptime and reliability

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

What key characteristic differentiates cloud networks from traditional networks?

A. Cloud networks are software-defined networks (SDNs)

B. Cloud networks rely on dedicated hardware appliances

C. Cloud networks are less scalable than traditional networks

D. Cloud networks have the same architecture as traditional networks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

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 over time

D. To reduce the number of security incidents to zero

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

What is a primary objective of cloud governance in an organization?

A. Implementing multi-tenancy and resource pooling.

B. To align cloud usage with corporate objectives

C. Simplifying scalability and automating resource management.

D. Enhancing user experience and reducing latency

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

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

A. Increasing manual security audits frequency

B. Converting all workloads to ephemeral

C. Restricting access to workload configurations

D. Implementing automated security and compliance checks

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

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

A. Simplifies network design and maintenance

B. Enhances security by isolating workloads from each other

C. Increases the overall performance of network traffic

D. Reduces the need for encryption across the network

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

What is one of the primary advantages of including Static Application Security Testing (SAST) in Continuous Integration (CI) pipelines?

A. Identifies code vulnerabilities early in the development

B. Increases the speed of deployment to production

C. Improves runtime performance of the application

D. Enhances the user interface of the application

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which aspect of a Cloud Service Provider's (CSPs) infrastructure security involves protecting the interfaces used to manage configurations and resources?

A. Management plane

B. Virtualization layers

C. Physical components

D. PaaS/SaaS services

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Which of the following is a common security issue associated with serverless computing environments?

A. Complex deployment pipelines

B. High operational costs

C. Limited scalability

D. Misconfigurations

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Which of the following best describes the Identity Provider (IdP) and its role in managing access to deployments?

A. The IdP is used for authentication purposes and does not play a role in managing access to deployments.

B. The IdP manages user, group, and role mappings for access to deployments across cloud providers.

C. The IdP solely manages access within a deployment and resides within the deployment infrastructure.

D. The IdP is responsible for creating deployments and setting up access policies within a single cloud provider.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

In a cloud computing incident, what should be the initial focus of analysis due to the ephemeral nature of resources and centralized control mechanisms?

A. Management plane activity logs

B. Network perimeter monitoring

C. Endpoint protection status

D. Physical hardware access

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

How does artificial intelligence pose both opportunities and risks in cloud security?

A. AI is only beneficial in data management, not security

B. AI enhances detection mechanisms but could be exploited for sophisticated attacks

C. AI mainly reduces manual work with no significant security impacts

D. AI enhances security without any adverse implications

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

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 (WAF)

D. Intrusion Detection System (IDS)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Why is consulting with stakeholders important for ensuring cloud security strategy alignment?

A. It simplifies the cloud platform selection process.

B. It reduces the overall cost of cloud services.

C. It ensures that the strategy meets diverse business requirements.

D. It ensures compliance with technical standards only.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

In the context of cloud security, what is the primary benefit of implementing Identity and Access Management (IAM) with attributes and user context for access decisions?

A. Simplifies regulatory compliance by using a single sign-on mechanism.

B. Reduces log analysis requirements

C. Enhances security by supporting authorizations based on the current context and status

D. These are required for proper implementation of RBAC

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Which aspect of cloud architecture ensures that a system can handle growing amounts of work efficiently?

A. Scalability

B. Security

C. Reliability

D. Performance

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

What is the primary role of Identity and Access Management (IAM)?

A. To encrypt data at rest and in transit

B. Ensure only authorized entities access resources

C. To monitor and log all user activities and traffic

D. Ensure all users have the same level of access

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which Identity and Access Management (IAM) principle focuses on implementing multiple security layers to dilute access power, thereby averting a misuse or compromise?

A. Continuous Monitoring

B. Federation

C. Segregation of Duties

D. Principle of Least Privilege

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

What is the primary purpose of the CSA Security, Trust, Assurance and Risk (STAR) Registry?

A. To manage data residency and localization requirements

B. To document security and privacy controls of cloud offerings

C. To certify cloud services for regulatory compliance

D. To provide cloud service rate comparisons

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

What is a key characteristic of serverless functions in terms of execution environment?

A. They need continuous monitoring by the user

B. They run on dedicated long-running instances

C. They require pre-allocated server space

D. They are executed in isolated, ephemeral environments

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

In a containerized environment, what is fundamental to ensuring runtime protection for deployed containers?

A. Deploying container-specific antivirus scanning

B. Full packet network monitoring

C. Using static code analysis tools in the pipeline

D. Implementing real-time visibility

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

Which concept focuses on maintaining the same configuration for all infrastructure components, ensuring they do not change once deployed?

A. Infrastructure as code

B. Application integration

C. Component credentials

D. Immutable infrastructure

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Which of the following strategies best enhances infrastructure resilience against Cloud Service Provider (CSP) technical failures?

A. High Availability within one data center

B. Local backup

C. Single-region resiliency

D. Multi-region resiliency

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

What's the difference between DNS Logs and Flow Logs?

A. DNS Logs record domain name resolution requests and responses, while Flow Logs record info on source, destination, protocol.

B. They play identical functions and can be used interchangeably.

C. They represent the logging of different networking solutions, and DNS Logs are more suitable for a ZTA implementation.

D. DNS Logs record all the information about the network behaviour, including source, destination, and protocol, while Flow Logs users applications behavior.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

Which aspect of cybersecurity can AI enhance by reducing false positive alerts?

A. Anomaly detection

B. Assisting analysts

C. Threat intelligence

D. Automated responses

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

Which of the following best describes the primary benefit of utilizing cloud telemetry sources in cybersecurity?

A. They encrypt cloud data at rest

B. They provide visibility into cloud environments

C. They enhance physical security

D. They reduce the cost of cloud services

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

In securing virtual machines (VMs), what is the primary role of using an “image factory" in VM deployment?

A. To encrypt data within VMs for secure storage

B. To facilitate direct manual intervention in VM deployments

C. To enable rapid scaling of virtual machines on demand

D. To ensure consistency, security, and efficiency in VM image creation

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

What's the best way for organizations to establish a foundation for safeguarding data, upholding privacy, and meeting regulatory requirements in cloud applications?

A. By implementing end-to-end encryption and multi-factor authentication

B. By conducting regular security audits and updates

C. By deploying intrusion detection systems and monitoring

D. By integrating security at the architectural and design level

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

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 (IaaS)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

Which areas should be initially prioritized for hybrid cloud security?

A. IAM and networking

B. Data center infrastructure and architecture

C. Application development and deployment

D. Cloud storage management and governance

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

Which of the following is used for governing and configuring cloud resources and is a top priority in cloud security programs?

A. Management Console

B. Management plane

C. Orchestrators

D. Abstraction layer

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

What is the main purpose of multi-region resiliency in cloud environments?

A. To increase the number of users in each region

B. To ensure compliance with regional and international data laws

C. To reduce the cost of deployments and increase efficiency

D. To improve fault tolerance through deployments across multiple regions

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

What is the primary purpose of secrets management in cloud environments?

A. Monitoring network traffic for security threats

B. Securely handling stored authentication credentials

C. Managing user authentication for human access

D. Optimizing cloud infrastructure performance

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

How does the variability in Identity and Access Management (IAM) systems across cloud providers impact a multi-cloud strategy?

A. Reduces costs by leveraging different pricing models

B. Simplifies the management by providing standardized IAM protocols

C. Ensures better security by offering diverse IAM models

D. Adds complexity by requiring separate configurations and integrations

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

Which principle reduces security risk by granting users only the permissions essential for their role?

A. Mandatory Access Control

B. Unlimited Access

C. Least-Privileged Access

D. Role-Based Access Control

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

In preparing for cloud incident response, why is it crucial to establish a cloud deployment registry?

A. To maintain a log of all incident response activities and have efficient reporting

B. To document all cloud services APIs

C. To list all cloud-compliant software

D. To track incident support options, know account details, and contact information

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

What is an advantage of using Kubernetes for container orchestration?

A. Limited deployment options

B. Automation of deployment and scaling

C. Increased hardware dependency

D. Manual management of resources

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

What is the primary function of landing zones or account factories in cloud environments?

A. Provide cost-saving recommendations for cloud resources

B. Consistent configurations and policies for new deployments

C. Enhance the performance of cloud applications

D. Automate the deployment of microservices in the cloud

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

What is a primary objective during the Detection and Analysis phase of incident response?

A. Developing and updating incident response policies

B. Validating alerts and estimating the scope of incidents

C. Performing detailed forensic investigations

D. Implementing network segmentation and isolation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

Which of the following BEST describes a benefit of Infrastructure as Code (IaC) in cybersecurity contexts?

A. Increases scalability of cloud resources

B. Enables consistent security configurations through automation

C. Increases manual control over security settings

D. Reduces the need for security auditing

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

Which term describes the practice in cloud compliance where a customer acquires a set of pre-approved regulatory or standards-based controls from a compliant provider?

A. Automated compliance

B. Attestation inheritance

C. Audit inheritance

D. Compliance inheritance

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

Which of the following is the MOST common cause of cloud-native security breaches?

A. Vulnerabilities in cloud provider's physical infrastructure

B. IAM failures

C. Lack of encryption for data at rest

D. Inability to monitor cloud infrastructure for threats

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

In cloud environments, why are Management Plane Logs indispensable for security monitoring?

A. They provide real-time threat detection and response

B. They detail the network traffic between cloud services

C. They track cloud administrative activities

D. They report on user activities within applications

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

Which best practice is recommended when securing object repositories in a cloud environment?

A. Encrypting the access paths only

B. Using access controls as the sole security measure

C. Encrypting only sensitive objects

D. Encrypting all objects in the repository

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

Why is it important to capture and centralize workload logs promptly in a cybersecurity environment?

A. To simplify application debugging processes

B. Primarily to reduce data storage costs

C. Logs may be lost during a scaling event

D. To comply with data privacy regulations

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

Which of the following enhances Platform as a Service (PaaS) security by regulating traffic into PaaS components?

A. Intrusion Detection Systems (IDS)

B. Hardware Security Modules (HSMs)

C. Network Access Control Lists (NACLs)

D. API Gateways

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

What is the primary purpose of Identity and Access Management (IAM) systems in a cloud environment?

A. To encrypt data to ensure its confidentiality

B. To govern identities' access to resources in the cloud

C. To monitor network traffic for suspicious activity

D. To provide a backup solution for cloud data

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

Which of the following best describes a risk associated with insecure interfaces and APIs?

A. Ensuring secure data encryption at rest

B. Man-in-the-middle attacks

C. Increase resource consumption on servers

D. Data exposure to unauthorized users

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

Which type of controls should be implemented when required controls for a cybersecurity framework cannot be met?

A. Detective controls

B. Preventive controls

C. Compensating controls

D. Administrative controls

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

Which approach is essential in identifying compromised identities in cloud environments where attackers utilize automated methods?

A. Deploying behavioral detectors for IAM and management plane activities

B. Relying on IP address and connection header monitoring

C. Implementing full packet capture and monitoring

D. Focusing exclusively on signature-based detection for known malware

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

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 lifecycle

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

In the shared security model, how does the allocation of responsibility vary by service?

A. Shared responsibilities should be consistent across all services.

B. Responsibilities are the same across IaaS, PaaS, and SaaS in the shared model.

C. Responsibilities are divided between the cloud provider and the customer based on the service type.

D. Based on the per-service SLAs for security.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

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

A. Disabling unnecessary VM services and using containers

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

C. Using secure base images, patch and configuration management

D. Network isolation and monitoring

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

Which of the following best describes an aspect of PaaS services in relation to network security controls within a cloud environment?

A. They override the VNet/VPC's network security controls by default

B. They do not interact with the VNet/VPC's network security controls

C. They require manual configuration of network security controls, separate from the VNet/VPC

D. They often inherit the network security controls of the underlying VNet/VPC

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #95 *Topic 1*

What is a key consideration when handling cloud security incidents?

A. Hiring additional staff

B. Monitoring network traffic

C. Focusing on technical fixes

D. Cloud service provider service level agreements

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

Which of the following is a primary purpose of establishing cloud risk registries?

A. In order to establish cloud service level agreements (SLAs)

B. To monitor real-time cloud performance

C. To manage and update cloud account credentials

D. Identify and manage risks associated with cloud services

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 1*

Which of the following from the governance hierarchy provides specific goals to minimize risk and maintain a secure environment?

A. Implementation guidance

B. Control objectives

C. Policies

D. Control specifications

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

Which of the following best describes the concept of AI as a Service (AIaaS)?

A. Selling AI hardware to enterprises for internal use

B. Hosting and running AI models with customer-built solutions

C. Offering pre-built AI models to third-party vendors

D. Providing software as an AI model with no customization options

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

What is a key advantage of using Policy-Based Access Control (PBAC) for cloud-based access management?

A. PBAC allows enforcement of granular, context-aware security policies using multiple attributes.

B. PBAC eliminates the need for defining and managing user roles and permissions.

C. PBAC is easier to implement and manage compared to Role-Based Access Control (RBAC).

D. PBAC ensures that access policies are consistent across all cloud providers and platforms.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

What is a cloud workload in terms of infrastructure and platform deployment?

A. A network of servers connected to execute processes

B. A collection of physical hardware used to run applications

C. A single software application hosted on the cloud

D. Application software deployable on infrastructure/platform

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!