DUMPSARENA

Certified in Cybersecurity

ISC2 CC

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1312

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Mix Questions	461
Topic 2, Security Principles	150
Topic 3, Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	149
Topic 4, Access Controls Concepts	170
Topic 5, Network Security	217
Topic 6, Security Operations	165
Total	1312

QUESTION NO: 1

A device found not to comply with the security baseline should be:

A. Disabled or separated into a quarantine area until a virus scan can be run

B. Disabled or isolated into a quarantine area until it can be checked and updated.

C. Placed in a demilitarized zone (DMZ) until it can be reviewed and updated

D. Marked as potentially vulnerable and placed in a quarantine area

ANSWER: B

Explanation:

Security baselines are used to guarantee that network devices, software, hardware and endpoints are configured consistently. Baselines ensure that all such devices comply with the security baseline set by the organization. Whenever a device is found not compliant with the security baseline, it may be disabled or isolated into a quarantine area until it can be checked and updated (see ISC2 Study Guide, chapter 5, module 2, under Configuration Management Overview). A DMZ is a protected boundary network between external and internal networks. Systems accessible directly from the Internet are permanently connected in this network, where they are protected by a firewall; however, a DMZ is not a quarantine area used to temporarily isolate devices.

QUESTION NO: 2

Which access control mechanism assigns access rights based on the sensitivity of the data being accessed?

A. Role-Based Access Control (RBAC).

B. Mandatory Access Control (MAC).

C. Discretionary Access Control (DAC).

D. Attribute-Based Access Control (ABAC).

ANSWER: B

Explanation:

Mandatory Access Control (MAC) assigns access rights based on the sensitivity of the data being accessed, ensuring that only users with the necessary security clearance can access classified information.

QUESTION NO: 3

Of the policies listed, which one is most likely to provide guidance on connecting a home computer to the work network via VPN?

A. AUP

B. BYOD

C. Data handling policy

D. None of the above

ANSWER: B

Explanation:

The Bring Your Own Device (BYOD) policy typically governs the use of personal devices, including connecting them to the work network via VPN.

QUESTION NO: 4

What is the name of the seventh layer of the OSI model?

A. Application

B. Session

C. Presentation

D. Network

ANSWER: A

Explanation:

The Application Layer is Layer 7 of the OSI model.

QUESTION NO: 5

Which of these is not an attack against an IP network?

A. Man-in-the-middle Attack

B. Fragmented Packet Attack

C. Side-channel Attack

D. Oversized Packet Attack

ANSWER: C

Explanation:

Man-in-the-middle attacks, oversized packet attacks and fragmented packet attacks are all typical IP network attacks (see ISC2 Study Guide, Chapter 4, Module 2, under Security of the Network). Side Channel Attacks are non-invasive attacks which extract information from devices (typically those running cryptographic algorithms) and are therefore not aimed at IP networks.

QUESTION NO: 6

Which are the components of an incident response plan?

A. Preparation -> Detection and Analysis -> Recovery -> Containment -> Eradication -> Post-Incident Activity

B. Preparation -> Detection and Analysis -> Containment -> Eradication -> Post-Incident Activity -> Recovery

C. Preparation -> Detection and Analysis -> Eradication -> Recovery -> Containment -> Post-Incident Activity

D. Preparation -> Detection and Analysis -> Containment, Eradication and Recovery -> Post-Incident Activity

ANSWER: D

Explanation:

The components commonly found in an incident response plan are (in this order): Preparation; Detection and Analysis;

Containment, Eradication and Recovery; Post-Incident Activity (see the ISC2 Chapter 2, Module 1, under Components of an Incident Response Plan).

QUESTION NO: 7

What is the purpose of a root cause analysis in security incident response?

A. To identify individuals responsible for security incidents

B. To prevent similar incidents from occurring in the future

C. To encrypt sensitive data during incident handling

D. To automate incident response procedures

ANSWER: B

Explanation:

Root cause analysis aims to identify the underlying causes of security incidents and develop preventive measures to mitigate future occurrences.

QUESTION NO: 8

Which of the following is a key component of an effective cyber incident response plan?

A. Ignoring security incidents

B. Establishing communication protocols and chains of command

C. Waiting for external assistance before taking any action

D. Blaming individuals for security incidents

ANSWER: B

Explanation:

Communication protocols and chains of command are essential components of an effective cyber incident response plan, ensuring that the appropriate personnel are notified and coordinated actions are taken in response to security incidents.

QUESTION NO: 9

Which network security mechanism is used to monitor and analyze network traffic for signs of potential security threats?

A. Intrusion Detection System (IDS)

B. Virtual Private Network (VPN)

C. Network Address Translation (NAT)

D. Dynamic Host Configuration Protocol (DHCP)

ANSWER: A

Explanation:

Intrusion Detection Systems (IDS) monitor and analyze network traffic for signs of potential security threats, such as suspicious activities and policy violations, in order to detect and respond to cyber attacks in real-time.

QUESTION NO: 10

In Change Management, which component addresses the procedures needed to undo changes?

A. Disaster and Recover

B. Rollback

C. Request for Change

D. Request for Approval

ANSWER: B

Explanation:

In Change Management, the Request For Change (RFC) is the first stage of the request: it formalizes the change from the stakeholders' point of view. The next phase is the Approval phase, where each stakeholder reviews the change, identifies and allocates the corresponding resources, and eventually either approves or rejects the change (appropriately documenting the approval or rejection). Finally, the Rollback phase addresses the actions to take when the monitoring change suggests a failure or inadequate performance.

QUESTION NO: 11

The name, age, location and job title of a person are all examples of:

A. Attributes

B. Biometric factors

C. Account permissions

D. Identity factors

ANSWER: A

Explanation:

Attributes such as a person's name, age, location, job title, and even characteristics such as height or hair color, may all be associated with their identity. None of these describe biometric factors used for authentication. Identity factors are something you know, are or have. Account permissions determine what an authenticated person (a user) can do, and not attributes related to the user's identity.

QUESTION NO: 12

What is the primary purpose of a compensating control within an organization's security framework?

A. To replace all primary security controls with more advanced technologies

B. To act as the main defense mechanism against cyber threats

C. To provide an alternative security measure when primary controls cannot meet compliance requirements or security objectives

D. To serve exclusively as a physical security measure, such as fencing or lighting

ANSWER: C

Explanation:

A compensating control, also known as an alternative control, is a security measure that is used when compliance requirements or other security objectives cannot be met with existing controls. Compensating controls are often implemented when the normal mitigating controls are unavailable or impractical【51†source】.

QUESTION NO: 13

What is the difference between an incident and a disaster in the context of incident response?

A. Incidents have a higher impact than disasters

B. Disasters involve physical damage, while incidents are purely digital

C. Incidents are smaller in scale and can usually be handled by internal resources, while disasters require external assistance and have a broader impact

D. Incidents are caused by human error, while disasters are caused by natural events

ANSWER: C

Explanation:

Incidents are typically smaller in scale and can be handled by internal resources, whereas disasters are more severe, requiring external assistance and having a broader impact on operations and resources.

QUESTION NO: 14

Which access control mechanism uses predefined roles to assign access rights to users?

A. Role-Based Access Control (RBAC).

B. Mandatory Access Control (MAC).

C. Discretionary Access Control (DAC).

D. Attribute-Based Access Control (ABAC).

ANSWER: A

Explanation:

Role-Based Access Control (RBAC) uses predefined roles to assign access rights to users, simplifying access management by grouping users with similar responsibilities and access requirements.

QUESTION NO: 15

What access control principle ensures that access rights are granted based on the user's role within the organization?

A. Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Role-Based Access Control (RBAC).

ANSWER: D

Explanation:

Role-Based Access Control (RBAC) ensures that access rights are granted based on the user's role within the organization, simplifying access management by grouping users with similar responsibilities and access requirements.

QUESTION NO: 16

What is a key component of security operations in cybersecurity?

A. Implementing security controls on network devices

B. Conducting regular vulnerability assessments

C. Training end-users on security best practices

D. Detecting and responding to security incidents

ANSWER: D

Explanation:

Security operations in cybersecurity involve detecting and responding to security incidents effectively to minimize their impact on organizational assets and operations.

QUESTION NO: 17

Which policy outlines the appropriate use of personal devices in the workplace?

A. Data handling policy

B. Password policy

C. Acceptable use policy

D. Bring Your Own Device (BYOD) policy

ANSWER: D

Explanation:

The Bring Your Own Device (BYOD) policy outlines the appropriate use of personal devices in the workplace, including security measures and limitations on how these devices can be used to access organizational resources.

QUESTION NO: 18

Which of the following is NOT a feature of a cryptographic hash function?

A. Deterministic

B. Unique

C. Useful

D. Reversible

ANSWER: D

Explanation:

A cryptographic hash function should be unique, deterministic, useful, tamper-evident (also referred to as 'the avalanche effect' or 'integrity assurance') and non-reversible (also referred to as 'one-way').

Nonreversible means it is impossible to reverse the hash function to derive the original text of a message from its hash output value (see ISC2 Study Guide, chapter 5, module 1, under Encryption Overview). Thus, the 'reversible' feature is not a feature of a hash function.

QUESTION NO: 19

What is the primary purpose of a firewall in network security?

A. To authenticate users accessing the network

B. To encrypt data transmissions over the network

C. To prevent unauthorized access to the network

D. To monitor and analyze network traffic for security threats

ANSWER: C

Explanation:

Firewalls are used in network security to prevent unauthorized access to the network by monitoring and controlling incoming and outgoing network traffic based on predefined security rules.

QUESTION NO: 20

Which cloud service model provides the most suitable environment for customers who want to install their custom operating system?

A. SaaS

B. SLA

C. IaaS

D. PaaS

ANSWER: C

Explanation:

Infrastructure as a Service (IaaS) is a cloud service model that allows the customer to manage the computing resources (including the operating systems). Software as a Service (SaaS) is a model that provides customers with access to software applications (typically on a subscription-based or pay-per-use model) but does not allow them to access the underlying infrastructure. Platform as a Service (PaaS) is a service model that provides a platform for building, deploying and managing applications; however, like SaaS, it does not offer the ability to access the underlying infrastructure (including the operating system). An SLA is simply a service-level agreement (and not a cloud service deployment model) (see ISC2 Study Guide, chapter 4, module 3).