

DUMPS ARENA

Specialist - Infrastructure Security Exam

EMC DES-9131

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

The project manager of a data center has a budget of \$1,500,000 to install critical infrastructure systems. The project will take 24 months to complete.

The project manager is working with the project management team, security experts, and stakeholders to identify cyber risks. After reviewing the project plan, the CIO wants to know why so many risk identification meetings are requested.

What a valid reason for the repeated risk identification meetings?

- A. Identify new risks
- B. Update the company risk register
- C. Transfer risk to other project team members
- D. Prevent all risk

ANSWER: B**QUESTION NO: 2**

What database is used to record and manage assets?

- A. Configuration Management Database
- B. Asset Inventory Management Database
- C. High Availability Mirrored Database
- D. Patch Management Inventory Database

ANSWER: A**Explanation:**

Reference: https://en.wikipedia.org/wiki/Configuration_management_database

QUESTION NO: 3 - (DRAG DROP)**DRAG DROP**

Match the security event to its description.

Select and Place:

Event	Description
Denial of Service	Non-authorized person with access to places where they should not have, or having access to systems and resources not designated to them
Attrition security event	Generated by behaviors from users, employees, contributors, or vendors who violate company policies
Misuse	Service or workload is overwhelmed, or has no available resources to perform its task
Intrusion event	When a user downloads a message with malicious links, images, attachments, or scripts
Email security event	Generated by brute force attacks to compromise, degrade, or destroy systems, networks, and services

ANSWER:

Event	Description
Intrusion event	
Misuse	
Denial of Service	
Email security event	
Attrition security event	

Explanation:

QUESTION NO: 4

Which category addresses the detection of unauthorized code in software?

- A. PR.DS
- B. DE.DP
- C. PR.AT
- D. DE.CM

ANSWER: D

Explanation:

Reference: https://vufind.carli.illinois.edu/vf-rou/Record/rou_346654/TOC

QUESTION NO: 5

What must be included in the CMDB?

- A. Inventory of uninstalled software
- B. Software End User Licensing Agreements
- C. Dependencies of installed components
- D. Known vulnerabilities of installed software

ANSWER: C

Explanation:

Reference: <https://docs.servicenow.com/bundle/london-servicenow-platform/page/product/configuration-management/concept/cnfig-mgmt-andcmdb.html>

QUESTION NO: 6

What should an organization use to effectively mitigate against password sharing to prevent unauthorized access to systems?

- A. Access through a ticketing system
- B. Frequent password resets
- C. Strong password requirements
- D. Two factor authentication

ANSWER: D

QUESTION NO: 7

Which mechanism within the NIST Cybersecurity Framework describes a method to capture the current state and define the target state for understanding gaps, exposure, and prioritize changes to mitigate risk?

- A. Functions
- B. Profiles

- C. Tiers
- D. Categories

ANSWER: C

QUESTION NO: 8

What must be done before returning a compromised laptop to normal operations in the environment?

- A. Perform a virus scan
- B. Eliminate the root cause of the compromise
- C. Re-image the device
- D. Device cannot be returned to the environment

ANSWER: C

QUESTION NO: 9

What are the five functions of the NIST Framework Core?

- A. Identify, Protect, Detect, Respond, and Recover
- B. Governance, Identify, Recover, Respond, and Recover
- C. Protect, Detect, Respond, Governance, and Recover
- D. Identify, Respond, Protect, Detect, and Governance

ANSWER: A

Explanation:

Reference <https://www.nist.gov/cyberframework/online-learning/five-functions>

QUESTION NO: 10

A new employee is starting work at your company. When should they be informed of the company's security policy?

- A. Based on human resource policy
- B. After the first security infraction

C. Annual security policy review

D. During regular security awareness sessions

ANSWER: D