DUMPSBOSS.

Specialist - Infrastructure Security Exam

EMC DES-9131

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1 - (DRAG DROP)

DRAG DROP

Match the security event to its description.

Select and Place:

ANSWER:

Explanation:

The completed matching is correct because it associates each event category with the security condition it describes. An intrusion event is an instance of unauthorized access or attempted access to systems and resources. This is the core meaning of intrusion detection and prevention: identifying activity that violates an access-control boundary. The National Institute of Standards and Technology describes intrusion detection as monitoring for attempts to compromise confidentiality, integrity, or availability, including unauthorized use of systems and resources; see the NIST intrusion-detection definition.

Misuse correctly covers activity by authorized or internal parties that violates organizational policy. Security events are not limited to external attackers; actions by users, employees, contractors, and vendors can create policy and compliance risk when their behavior is inappropriate or unauthorized. Denial of Service correctly identifies the condition in which a service or workload is overwhelmed and cannot provide resources to legitimate users. This directly affects availability, one of the essential security objectives described in the NIST availability definition.

Email security event correctly applies when a user downloads or opens a message containing malicious links, images, attachments, or scripts. Email is a common delivery channel for phishing and malware, so these message-based threats are handled as email security events. Finally, attrition security event correctly describes brute-force activity designed to compromise, degrade, or destroy systems, networks, and services. Attrition attacks attempt to exhaust, weaken, or damage computing capabilities over time. Together, the placed labels accurately classify unauthorized access, policy misuse, resource exhaustion, malicious email content, and destructive brute-force activity.

QUESTION NO: 2

Which NIST Cybersecurity Framework function should be executed before any others?

A. Respond

B. Protect

C. Recover

D. Identify

ANSWER: D

Explanation:

Identify is the correct answer because it establishes the organizational understanding needed to manage cybersecurity risk. Before an organization can appropriately select safeguards, prepare response activities, or plan recovery, it needs to understand its business context, critical assets, systems, data, dependencies, governance requirements, and the risks that apply to them. The Identify function includes asset management, business environment, governance, risk assessment, risk-management strategy, and supply-chain risk management. These activities provide the risk-informed foundation used to prioritize cybersecurity decisions and align them with organizational objectives.

In the original five-function NIST Cybersecurity Framework model used by this question, Identify is presented first because its outcomes inform the implementation and prioritization of the Protect, Detect, Respond, and Recover functions. In practice, cybersecurity activities are continuous and functions can operate concurrently; however, establishing an initial understanding of assets, business needs, and risk is the necessary starting point for a coherent program. NIST describes the framework functions and their role in organizing cybersecurity outcomes in the NIST Cybersecurity Framework five functions overview and in the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.

QUESTION NO: 3

Concerning a risk management strategy, what should the executive level be responsible for communicating?

A. Risk mitigation

B. Risk profile

C. Risk tolerance

D. Asset risk

ANSWER: C

Explanation:

Risk tolerance is correct because executive leadership establishes the organization’s boundaries for accepting, avoiding, transferring, or mitigating risk in pursuit of its mission and business objectives. Communicating that tolerance gives business units, system owners, security teams, and risk managers a common decision-making framework: they can determine when a risk may be accepted at their level and when it must be escalated for additional treatment or executive approval. This communication must be clear enough to guide consistent resource allocation, security-control selection, exception handling, and prioritization across the enterprise.

NIST describes risk tolerance as the level of risk or degree of uncertainty an organization is willing to accept, and places responsibility for defining and communicating the organization's risk management strategy with senior leaders and executives. A documented, communicated tolerance also supports alignment between cybersecurity activities and organizational objectives rather than treating risk decisions as isolated technical choices. See NIST SP 800-39, Managing Information Security Risk and NIST SP 800-37 Rev. 2, Risk Management Framework.

QUESTION NO: 4 - (SIMULATION)

Match the security event to its description.

ANSWER: Check the explanation for the answer

Explanation:

The draggable security events/descriptions are not included in the supplied simulation JSON, so an exact one-to-one placement cannot be determined. Use these standard DES-9131 security-event matches:

Security event — Any observable occurrence in a system, service, or network; it may or may not be security relevant (for example, a user logon or a firewall log entry).
Security alert — A notification generated by a security control indicating that suspicious activity or a potential security issue requires review.
Security incident — A confirmed or suspected violation of security policy, or an imminent threat of such a violation, requiring incident-response action.

If the simulation instead presents specific attack types, the selectable event names and descriptions (or the simulation image) are required to provide the exact matches.

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:

A CMDB must include the dependencies of installed components because its central purpose is to record configuration items and the relationships between them. A configuration item can be a server, operating system, database, application, network device, or another managed component. Recording how these items depend on one another enables an organization to understand the potential operational and business impact of a change, incident, outage, or security event. For example, a CMDB relationship can show that an application relies on a particular database and that the database runs on a specific server. This relationship information supports impact analysis, change planning, incident troubleshooting, service mapping, and controlled configuration management. A list of components without their dependencies is only an inventory; it does not provide the contextual relationship data needed for a functional CMDB. ServiceNow describes a CMDB as a repository that stores information about configuration items and the relationships among them, while ITIL configuration management similarly emphasizes managing configuration information and relationships to support service management decisions. See ServiceNow: What is a CMDB? and AXELOS: ITIL service configuration management.

QUESTION NO: 6

An organization uses a third-party cloud provider to host a mission-critical application.

Which activity is most important for managing the cybersecurity risk introduced by this relationship?

A. Assessing the provider's security requirements and controls

B. Using the provider's default service configuration

C. Transferring all cybersecurity responsibility to the provider

D. Removing the application from the asset inventory

ANSWER: A

Explanation:

Assessing the provider's security requirements and controls is correct because third-party services can introduce risks to organizational data, systems, availability, compliance obligations, and incident-response capabilities. The organization must understand the provider's security practices and determine whether they meet applicable business, regulatory, contractual, and risk-management requirements.

The assessment should address areas such as data protection, access control, logging, vulnerability management, incident notification, resiliency, subcontractor use, and the provider's responsibility boundaries. These requirements should be documented in contracts and monitored throughout the relationship rather than assessed only before onboarding. NIST addresses supply-chain risk management in NIST SP 800-161 Rev. 1.

QUESTION NO: 7

You need to review your current security baseline policy for your company and determine which security controls need to be applied to the baseline and what changes have occurred since the last update.

Which category addresses this need?

A. ID.AM

B. PR.IP

C. PR.MA

D. ID.SC

ANSWER: B

Explanation:

PR.IP is the appropriate category because it covers Information Protection Processes and Procedures in the NIST Cybersecurity Framework. This category addresses the organizational processes used to establish, maintain, and improve safeguards that protect systems and information. Reviewing a security baseline policy, identifying the controls that must be included in that baseline, and tracking changes since its prior revision are configuration-management and protection-process activities.

In particular, the PR.IP category includes the outcome that baseline configurations of information technology and industrial control systems are created and maintained while incorporating security principles. A current, controlled baseline gives the organization a defined security standard against which systems and policy changes can be assessed. Periodic review also supports keeping documented protection processes current as technologies, threats, business requirements, and risk decisions evolve. Applying PR.IP therefore ensures that baseline controls are documented, governed, maintained, and updated through an established process rather than treated as a one-time technical configuration.

The NIST Cybersecurity Framework Core identifies PR.IP under the Protect function and defines its relevant outcomes: NIST Cybersecurity Framework. NIST configuration-management guidance further describes maintaining secure baseline configurations and controlling changes: NIST SP 800-128.

QUESTION NO: 8

The Backup Recovery Plan is dependent on what effort?

A. PR.DS

B. RTO

C. BIA

D. SDLC

ANSWER: C

Explanation:

BIA is correct because a Business Impact Analysis provides the business basis for designing a backup and recovery plan. The BIA identifies critical business processes, the systems and data that support them, the consequences and timing of an outage, and the order in which capabilities must be restored. Those findings allow the organization to select appropriate backup scope, retention, storage protection, recovery resources, and restoration priorities.

Importantly, the BIA establishes recovery requirements such as acceptable downtime and data loss tolerance for each service. The backup and recovery plan then implements controls and procedures capable of meeting those requirements, including the frequency of backups, use of offsite or immutable copies, recovery testing, and documented restoration steps. A plan that is based on the BIA is therefore aligned with actual operational and mission impact rather than applying the same recovery approach to every system.

NIST SP 800-34 Rev. 1 describes the BIA as a foundational contingency-planning activity used to characterize system impact and determine recovery priorities and requirements. See NIST SP 800-34 Rev. 1 and NIST's publication record for Contingency Planning Guide for Federal Information Systems.