Practice Exam Questions

DELL Technologies

DES-9131

Specialist

Infrastructure Security Exam

EXAMAIDES

PASS YOUR EXAM AT FIRST TRY

Total Question: 60 QAs

Question No: 1
What are the four tiers of integration within the NIST Cybersecurity Framework?
A. Selective, Repeatable, Partial, and Adaptive
B. Partial, Risk Informed, Repeatable, and Adaptive
C. Corrective, Risk Informed, Repeatable. and Adaptive
D. Risk Informed, Selective, Repeatable, and Partial
Answer: B

Question No: 2
What procedure is designed to enable security personnel to detect, analyze, contain, eradicate, respond, and recover from malicious computer incidents such as a denial-of-service attack?
A. Disaster Recovery Plan
B. Emergency Analysis Plan
C. Crisis Communication Plan
D. Incident Response Plan
Answer: D

Question No: 3
What determines the technical controls used to restrict access to USB devices and help prevent their use within a company?
A. Block use of the USB devices for all employees
B. Written security policy prohibiting the use of the USB devices
C. Acceptable use policy in the employee HR on-boarding training
D. Detect use of the USB devices and report users
Answer: A

Question No: 4
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: B

Question No: 5
What process is used to identify an organization's physical, digital, and human resource, as required in their Business Impact Analysis?
A. Risk Management Strategy
B. Risk Assessment
C. Risk Treatment
D. Asset Inventory

Answer: D

Question No: 6
What supports an organization in making risk management decisions to address their security posture in real time?
A. Baseline reporting
B. Continuous monitoring
C. User access reviews
D. Video surveillance
Answer: A

Question No: 7
When should event analysis be performed?
A. Only when requested by an auditor
B. Routinely for all events collected on a mission critical system
C. Only at the discretion of an authorized security analyst
D. After an event is triggered by the detection system
Answer: B

Question No: 8
What type of system processes information, the loss of which would have a debilitating impact to an organization?
A. Mission critical
B. Security critical
C. Business critical
D. Safety critical
Answer: A

Question No: 9
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: 10
The CSF recommends that the Communication Plan for an IRP include audience, method of communication, frequency, and what other element?
A. Incident category
B. Message criteria
C. Incident severity
D. Templates to use

Answer: B

Question No: 11
What is the main goal of a gap analysis in the Identify function?
A. Determine security controls to improve security measures
B. Determine actions required to get from the current profile state to the target profile state
C. Identify gaps between Cybersecurity Framework and Cyber Resilient Lifecycle pertaining to that function
D. Identify business process gaps to improve business efficiency
Answer: B

Question No: 12
DRAG DROP
Rank order the relative severity of impact to an organization of each plan, where "1" signifies the most impact and "4" signifies the least impact.
Select and Place:

Backup Plan	1
Disaster Recovery Plan	2
Recovery Plan	3
Business Continuity Plan	4

Answer:

Backup Plan	Disaster Recovery Plan
Disaster Recovery Plan	Business Continuity Plan
Recovery Plan	Disaster Recovery Plan
Business Continuity Plan	Backup Plan

Question No: 13
What does a security benchmark help define?
A. Whether or not the organization should implement ISCM
B. The Baseline, or "as is" state
C. Which step of the DRP to execute first
D. What parts of the Baseline are appropriate
Answer: D

Question No: 14
In which function is the SDLC implemented?
A. Respond
B. Protect
C. Detect
D. Recover
Answer: A

Question No: 15
Which category addresses the detection of unauthorized code in software?
A. PR.DS
B. DE.DP
C. PR.AT
D. DE.CM
Answer: D

Question No: 16
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

Question No: 17
The CSIRT team is following the existing recovery plans on non-production systems in a PRE-BREACH scenario. This action is being executed in which function?
A. Protect
B. Recover
C. Identify
D. Respond
Answer: A

Question No: 18
What is a consideration when performing data collection in Information Security Continuous Monitoring?
A. Data collection efficiency is increased through automation.
B. The more data collected, the better chances to catch an anomaly.
C. Collection is used only for compliance requirements.
D. Data is best captured as it traverses the network.
Answer: A

Question No: 19
An organization has a policy to respond “ASAP” to security incidents. The security team is having a difficult time prioritizing events because they are responding to all of them, in order of receipt.
Which part of the IRP does the team need to implement or update?
A. Scheduling of incident responses
B. ‘Post mortem’ documentation
C. Classification of incidents
D. Containment of incidents
Answer: C