Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

PASS

DELL-EMC

DES-9131

Specialist - Systems Administrator, Infrastructure Security

QUESTION: 52
The network security team in your company has discovered a threat that leaked partial data on a compromised file server that handles sensitive information. Containment must be initiated and addresses by the CSIRT. Service disruption is not a concern because this server is used only to store files and does not hold any critical workload. Your company security policy required that all forensic information must be preserved. Which actions should you take to stop data leakage and comply with requirements of the company security policy?

A. Disconnect the file server from the network to stop data leakage and keep it powered on for further analysis.
B. Shut down the server to stop the data leakage and power it up only for further forensic analysis.
C. Restart the server to purge all malicious connections and keep it powered on for further analysis.
D. Create a firewall rule to block all external connections for this file server and keep it powered on for further analysis.

Answer: C

QUESTION: 53
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

Reference:
https://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjjw_fHytHgAhWvyqYKH
XaVAWcQFjAAegQ ICRAC
&url=https%3A%2F%2Fwww.nist.gov%2Fdocument%2Fdraft-cybersecurity-
framework-v11- corexlsx&usg=AOvVaw2wFipKqwxx2QnhlcVB2A7g

QUESTION: 54
A CISO is looking for a solution to lower costs, enhance overall efficiency, and improve the reliability of monitoring security related information. Which ISCM feature is recommended?

A. Reporting
B. Provisioning
C. Automation
D. Collection

Answer: C

Reference:
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf (19)

QUESTION: 55
What is the primary objective of establishing governance and risk management processes for an organization?

A. Manage assets effectively in accordance with local laws
B. Minimize cybersecurity risks in conjunction with compliance processes
C. Determine compliance controls in accordance with national laws
D. Establish recovery time objectives for critical infrastructure

Answer: B

QUESTION: 56
During what activity does an organization identify and prioritize technical, organizational, procedural, administrative, and physical security weaknesses?

A. Table top exercise
B. Penetration testing
C. Vulnerability assessment
D. White box testing

Answer: C

QUESTION: 57
Refer to the exhibit.

Action	Category	System	Risk Rank		Maturity		Priority	Cost
			SRC	TGT	SRC	TGT		
Detection Processes	A	ENG, FIN, Sales	3	8	4	6	7	4
		HR, EXEC	7	8	9	9	3	4
Security Continuous Monitoring	B	ENG, FIN, SALES, HR, EXEC	5	8	5	6	4	3
Anomalies and Events	C	ENG, FIN, SALES, HR, EXEC	6	8	5	7	6	6

Your organization's security team has been working with various business units to understand their business requirements, risk tolerance, and resources used to create a Framework Profile. Based on the Profile provided, what entries correspond to labels A, B, and C?

A. A: PR.IP
B: DE.CM
C: DE.AE

B. A: PR.DS
B: DE.AE
C: DE.CM

C. A: DE.AE
B: PR.DS
C: RS.CO

A. Option A
B. Option B
C. Option C

Answer: A

QUESTION: 58
Which document is designed to limit damage, reduce recovery time, and reduce costs where possible to the organization?

A. Business Impact Analysis
B. Business Continuity Plan
C. Risk Assessment Strategy
D. Incident Response Plan

Answer: B

QUESTION: 59
A security audit of the systems on a network must be performed to determine their compliance with security policies. Which control should be used for the audit?

A. PR.DS
B. DE.CM
C. RS.MI
D. ID.AM

Answer: A

QUESTION: 60
In accordance with PR.MA, an organization has just truncated all log files that are more than 12 months old. This has freed up 25 TB per logging server. What must be updated once the truncation is verified?

A. SDLC
B. IRP
C. Baseline
D. ISCM

Answer: C

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*