Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

D-CSF-SC-23 Practice Questions
D-CSF-SC-23 Practice Test
D-CSF-SC-23 Practice Exam
D-CSF-SC-23 Exam Questions
D-CSF-SC-23 Study Guide

PASS

killexams.com

DELL-EMC

D-CSF-SC-23

NIST Cybersecurity Framework 2023 Certification

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/D-CSF-SC-23

Question: 343

Following a ransomware attack, an organization revises its Business Continuity Plan. Which role does the Business Impact Analysis serve in this revision?

A. Lists hardware repair vendors
B. Details employee training attendance logs
C. Establishes recovery time objectives and critical system dependencies for streamlined restoration
D. Documents maintenance window schedules

Answer: C

Explanation: The BIA defines recovery time objectives and dependencies essential for designing an effective, prioritized continuity plan post-incident.

Question: 344

A security engineer integrates automated discovery tools with CMDB (Configuration Management Database). The CMDB records the operational criticality for each device. How does this information support disaster recovery planning?

A. It replaces the need for business impact analysis.
B. It enables prioritization of recovery efforts based on criticality levels.
C. It ensures all devices are backed up daily without exception.
D. It provides access control enforcement parameters.

Answer: B

Explanation: Knowing the operational criticality allows disaster recovery teams to allocate resources and restore critical devices first, minimizing downtime impact and aligning with recovery time objectives.

Question: 345

In a scenario where a major data breach affects customer personal data, what process should be first to reduce business impact and comply with the NIST Cybersecurity Framework?

A. Restoring services immediately without forensic investigation
B. Removing all incident logs to prevent legal exposure

C. Immediate communication to regulatory authorities and affected individuals as required
D. Delaying notification until full recovery completes

Answer: C

Explanation: Immediate communication to regulators and affected customers as required by law minimizes regulatory penalties and supports trust restoration. Removing logs violates evidence preservation; skipping investigation risks repeated breaches, and delaying notification harms compliance and reputation.

Question: 346

An audit shows 15% of inventory assets are missing classification labels after a quarterly review. Which KPI reflects proper remediation to meet NIST compliance?

A. Total number of assets discovered.
B. Reduction of unclassified assets to less than 5% within 30 days.
C. Number of security patches applied.
D. Total incidents detected.

Answer: B

Explanation: A KPI targeting the reduction of unclassified assets ensures the inventory classification controls are enforced and improves asset management compliance.

Question: 347

To construct an effective IRP per NIST CSF 2.0 RS.RP-1 on September 20, 2026, for a defense contractor handling CUI, the plan must integrate Govern (GV.PO-05) policy with Respond processes. Template includes: 1. Define IR Team roles (CSIRT lead, forensics analyst); 2. Incident classification matrix (Low: <10 assets, High: >100 or CUI); 3. Playbook for ransomware: Isolate via VLAN pruning command switchport trunk allowed vlan remove 10-20; 4. Testing via quarterly TTX with MTTR target <4 hrs (formula MTTR = Detection + Containment + Eradication + Recovery times). If Tier 4 profile requires annual red team validation, what core element ensures alignment with ID.RA-7 communication strategy?

A. Team roles list without classification
B. Appendix with escalation flowchart: Severity High -> Notify CISO in <15 min via secure Slack #ir-channel, integrated with RA-7 stakeholder mapping
C. Playbook command isolated
D. MTTR formula without testing

Answer: B

Explanation: RS.RP-1 mandates executable IRPs with integrated Govern policies and ID.RA-7 for risk comms, using flowcharts for escalation in CUI environments, per SP 800-61 Rev. 3's lifecycle. This ensures Tier 4 validation via red teams, unlike isolated elements.

Question: 348

Your security team requires a report showing how many assets have high-impact data but lack encryption. Which inventory attribute combination best facilitates this report?

A. Asset software versions.
B. Asset owner's contact information only.
C. IP address and subnet mask.
D. Data classification and encryption status metadata.

Answer: D

Explanation: Combining data classification with encryption status allows identification of vulnerable assets needing protection enhancement.

Question: 349

BCP for a virtual reality metaverse platform disrupted by avatar hijacking on April 21, 2026, supports timely recovery with immersion recovery time: IRT = (User_Sessions * Latency_ms) / (GPU_Instances * Sync_Rate), Sessions=10k, Latency=50, Rate=60fps. Which Unity C# script with Photon PUN, for Oculus Quest, best facilitates normal operations resumption?

A. using PUN2; using System; class TimelyBCP : MonoBehaviour { float sessions = 8000; float lat = 60; int gpus = 15; float rate = 50; void Update() { float recovery_time = (sessions * lat) / (gpus * rate); if (recovery_time <= 8000) { PhotonNetwork.JoinRoom("metaverse-safe"); } } public void OnPhotonJoinRoomFailed(object[] codeAndMsg) { StartCoroutine(ResyncUsers()); } IEnumerator ResyncUsers() { yield return new WaitForSeconds(2f); PhotonNetwork.Instantiate("secure_avatar", Vector3.zero, Quaternion.identity); } }
B. using Photon.Pun; using UnityEngine; public class BCPRecovery : MonoBehaviourPunCB { public float userSessions = 10000f; public float latency = 50f; public int gpuInstances = 20; public float syncRate = 60f; void Start() { float irt = (userSessions * latency) / (gpuInstances * syncRate); if (irt < 10000) { PhotonNetwork.ConnectUsingSettings(); } else { Debug.Log("Delay Recovery"); } } [PunRPC] void ResumeAvatars() { foreach (var player in PhotonNetwork.PlayerList) { player.TagObject = "secured"; } } public override void OnConnectedToMaster() { photonView.RPC("ResumeAvatars", RpcTarget.All); } }

C. #if UNITY_ANDROID using Photon.Realtime; public class ImmersionSupport : MonoBehaviourPunCallbacks { private float calcIRT(float sess, float ms, int inst, float fps) { return (sess * ms) / (inst * fps); } void Awake() { float irt_val = calcIRT(12000, 40, 25, 70); if (irt_val > 12000) { PhotonNetwork.Disconnect(); } else { PhotonNetwork.LoadLevel("recovered_scene"); } } public override void OnPlayerEnteredRoom(Player newPlayer) { if (newPlayer.IsLocal) { newPlayer.SetCustomProperties(new Dictionary { {"secured", true} }); } } #endif }
D. using UnityEngine; using Photon.Pun; public class NormalOpsBCP : MonoBehaviour { [SerializeField] float maxIRT = 9000f; void OnEnable() { float sessions = 9500; float delay = 55; int instances = 18; float fps = 55; float irt = (sessions * delay) / (instances * fps); if (irt < maxIRT) { var roomOptions = new RoomOptions { MaxPlayers = 100 }; PhotonNetwork.CreateRoom("bcp-room", roomOptions); } } [PunRPC] void SyncImmersion() { Camera.main.fieldOfView = 90f; // Resume VR } }

Answer: B

Explanation: BCP supports recovery by calculating immersion metrics to gate reconnection, per NIST CSF 2.0 Recovery (RC.RP-01). The script computes irt=(10k50)/(2060)≈4167 <10000, connects and RPCs ResumeAvatars to secure all players, resuming hijacked states. OnConnectedToMaster ensures master-sync.

Question: 350

In a scenario where a logistics company migrates to Kubernetes clusters, the security team documents a baseline configuration mandating PodSecurityPolicies with forbidden sysctls (e.g., kernel.msgmni=65536) and RBAC roles limited to read-only for namespaces. A pod escalation vulnerability was exploited due to drift. Why is baseline documentation indispensable for such containerized environments?

A. To train ML models on baseline patterns for predictive anomaly detection in cluster metrics
B. To calculate risk exposure via equations like Risk Score = Likelihood * Impact * (1 - Baseline Adherence Percentage)
C. To archive audit trails in ELK stacks for correlating baseline violations with threat hunting queries
D. To enforce policy-as-code using OPA Gatekeeper policies that validate manifests against baseline YAML schemas pre-deployment

Answer: D

Explanation: The creation and documentation of a baseline configuration in NIST CSF 2.0 PR.IP-1 is essential for defining enforceable secure defaults in dynamic environments like Kubernetes, where drifts can escalate privileges and enable container escapes. By codifying PodSecurityPolicies and RBAC in YAML, the baseline integrates with Open Policy Agent (OP
A. to admission-control deployments, rejecting non-compliant manifests that violate sysctl limits or role bindings, thus preventing exploits like those in CVE-2023-XXXX pod escalations. This addresses the

protect function's goal of risk mitigation through least privilege; in logistics, where supply chain delays from breaches cost millions, the documentation provides a single source of truth for compliance (e.g., SOC 2), automates remediation via webhooks, and supports blue-green deployments, ensuring operational continuity while hardening against runtime threats.

Question: 351

A retail chain post a POS breach uses NIST CSF 2.0 to rebuild, focusing on the Identify Function's Risk Assessment category (ID.RA-06), with the vulnerability prioritization syntax: PRIORITY(Vuln) = CVSS_Base × Exploitability_Factor, scored for 200 assets showing high scores in payment gateways. To align with PCI DSS, they develop a Target Profile for Tier 3. Which component allows embedding this syntax in Profiles to map Core risks to regulatory tiers?

A. Core, which standardizes CVSS factors for retail
B. Tiers, which prioritize vulns based on PCI syntax
C. Informative References, which fix Exploitability_Factor values
D. Profiles, which enable syntax-integrated customizations of Core outcomes for tier-aligned regulatory compliance

Answer: D

Explanation: Profiles permit the integration of prioritization syntax into tailored Core alignments, supporting Target Profile creation for Tier 3 repeatability in PCI contexts, fulfilling the framework's risk assessment purpose.

Question: 352

Describing impact from a homomorphic encryption flaw in a privacy-preserving ad network on February 2, 2026, per NIST CSF 2.0 Recovery (RC.IM-01), with privacy budget: Budget = ε * ln(1/δ) - (Query_Count * Noise_σ^2), ε=1.0, δ=1e-5, σ=1. Which PyTorch code for differential privacy, with Opacus, best calculates revenue/reputation from exposed bids?

A. import torch; from opacus import PrivacyEngine; epsilon = 1.0; delta = 1e-5; query_count = 500; noise_sigma = 1.0; privacy_budget = epsilon * torch.log(1/deltA. - (query_count * noise_sigma**2); model = torch.nn.Linear(10, 1); privacy_engine = PrivacyEngine(model, sample_rate=0.01, alphas=[1, 2], noise_multiplier=noise_sigma, max_grad_norm=1.0); if privacy_budget < 0.5: rev_exposed = 2e6 * (1 - torch.exp(-query_count / 100)); rep_hit = privacy_budget * -100; print(f"Budget: {privacy_budget:.2f}, Rev Loss: ${rev_exposed:,.0f}, Rep: {rep_hit:.0f}")
B. import torch.nn as nn; from opacus.privacy_engine import PrivacyEngine; eps = 0.8; del_ta = 1e-4; queries = 400; sigma_n = 0.8; budget = eps * math.log(1/del_ta) - queries * sigma_n**2; net =

nn.Sequential(nn.Linear(5, 20), nn.ReLU()); engine = PrivacyEngine(net, noise_multiplier=sigma_n, max_grad_norm=0.5); exposed_frac = 1 - math.exp(-budget); rev_impact = exposed_frac * 1.5e6; reputation = -budget * 80 * queries / 400; print("Privacy:", budget, "Loss:", rev_impact, "Rep:", reputation)
C. from torch import tensor; epsilon_val = 1.2; delta_val = 1e-6; q_count = 600; sig = 1.2; ln_term = tensor.log(tensor(1)/delta_val); budget_calc = epsilon_val * ln_term - q_count * sig**2; if budget_calc > 0: model.train(); optimizer = torch.optim.SGD(model.parameters(), lr=0.01); for batch in dataloader: loss = criterion(model(batch)); loss.backward(); optimizer.step(); print(budget_calc); rev = budget_calc * 3e5; rep = (1 - budget_calc / 2) * 50;
D. import opacus; model = ...; pe = opacus.PrivacyEngine(model, delta=1e-5, epsilon=1.0, sample_size=1000); budget = pe.get_epsilon(delta=1e-5); # Advanced; but for formula: import math; eps=1; d=1e-5; qc=450; ns=0.9; pb = eps * math.log(1/D. - qc * ns**2; exposed = qc / 1000 * (1 - math.exp(-pb)); revenue_loss = exposed * 1.8e6; rep_damage = pb * -90; print(f"Budget {pb}, Exposed {exposed}, Rev ${revenue_loss}, Rep {rep_damage}")

Answer: A

Explanation: Impact description uses DP accounting for exposure quantification, per NIST CSF 2.0 Recovery (RC.IM-01). The code computes privacy_budget=1.0ln(1e5)≈11.51 - (5001)=6.51, <0.5 false but prints, rev_exposed=2e6*(1-exp(-5))=~2e6, rep_hit=-651. This models bid exposure.

Question: 353

An engineer is asked to design technical safeguards that protect systems from unauthorized changes, including configuration management and patching. This task is best aligned with which NIST CSF 2023 Category?

A. Identity Management and Access Control
B. Protective Technology
C. Risk Assessment
D. Respond Planning

Answer: B

Explanation: Protective Technology includes technical measures like configuration management, patch management, and protective controls to defend systems from unauthorized modifications.

Question: 354

After a supply chain breach September 2, 2026, After Action Report (AAR) per RC.IM-2 reviews: 1. Timeline: Detect T=0, Contain T=45 min; 2. Metrics: MTTR=3.2 hrs (formula as prior); 3. Root cause:

Vendor API vuln (CVSS 9.1); 4. Recs: Implement SBOM scanning with syft scan image:tag. If gaps in RS.RP-1, what review step for GV.RM-02?

A. Timeline without metrics
B. Risk update: Revise tolerance thresholds based on AAR, e.g., Vendor Risk Score +=20%, audited quarterly
C. Cause isolated
D. Rec without risk

Answer: B

Explanation: RC.IM-2 AARs feed GV.RM-02 risk strategy updates via score adjustments, per CSF 2.0 Govern-Risk Management and SP 800-61 Rev. 3 improvements.

Question: 355

For CSF 2.0 communications planning, a bank's asset inventory via ServiceNow CMDB (e.g., GlideRecord('cmdb_ci_server'); gr.addQuery('class', 'cmdb_ci_server'); gr.query(); while(gr.next()) { owners.add(gr.getValue('owned_by')); }) lists 500 servers owned by IT groups, with BIA flagging core banking apps at $5M/hour. Pre-built Slack bots (slack post --channel #ir --text "Alert: Server {{server_id}} down") use this for notifications. How does inventory support?

A. By adding query loops for performance tuning
B. By querying class types for hardware vs. software categorization
C. By populating owner fields for dynamic bot routing in escalation trees
D. By exporting GlideRecords to CSV

Answer: C

Explanation: CMDB queries extract owners for bot integration, enabling automated pings per BIA urgency ($5M/hour), streamlining RESPOND comms. This reduces manual errors; static lists outdated quickly in dynamic banks, delaying stakeholder awareness.

Question: 356

In a disaster recovery test scenario, after deploying the backup systems in a secondary site, which step is essential to validate readiness for actual failover?

A. Running simulated cyberattacks to test system immunity
B. Verifying data integrity and consistency between primary and backup sites

C. Skipping application-level testing and focusing on network connectivity only
D. Deferring user acceptance testing to the real disaster event

Answer: B

Explanation: Verifying data integrity and consistency between primary and backup sites ensures data accuracy and usability for disaster recovery. Network checks alone or skipping testing phases undermine confidence in restoration. User acceptance testing is also important but should occur during planned tests, not deferred.

Question: 357

Your Incident Response Plan includes communication with external vendors affected by a supply chain intrusion. What principle should govern this communication?

A. Communicate only after final report completion to vendors
B. Open channels like public forums or social media to speed information flow
C. Secure, documented communication channels with predefined points of contact and confidentiality provisions
D. Allow vendors to handle communications independently

Answer: C

Explanation: Communications with external vendors during incidents must occur over secure, documented channels with designated contacts to preserve confidentiality and consistency. Public forums risk data leaks. Waiting for final report delays mitigation. Independent vendor communication risks inconsistency.

Question: 358

An organization maintains an up-to-date asset inventory that includes hardware, software, data, and personnel roles. During a critical vulnerability scan, it is discovered that several IoT devices are missing from the inventory. Which of the following best explains the impact of this incomplete asset inventory on cybersecurity management?

A. It reduces the need for incident response activities because missing assets are less likely to be attacked.
B. It is irrelevant because these devices do not handle sensitive information.
C. It can lead to an inaccurate business impact analysis and ineffective disaster recovery plans.
D. It only affects the physical security domain and not the cybersecurity framework.

Answer: C

Explanation: An incomplete asset inventory negatively impacts business impact analysis, disaster recovery, and incident response efforts since unknown or unmanaged devices represent blind spots, increasing risk exposure and impairing the organization's ability to plan and respond effectively.

Question: 359

A nonprofit's BCP leverages BIA indicating donor database inaccessibility for 24 hours risks $5M funding loss. In NIST CSF 2.0, how does this pair support Protect through access controls?

A. By enforcing ABAC policies with attributes like role=admin AND time
B. By computing funding probabilities post-BCP using Bayesian networks informed by BIA outage histories
C. By gamifying BCP training with BIA scenarios to boost employee recall rates above 90%
D. By federating BCP alerts via MQTT protocols tied to BIA critical thresholds for IoT donor kiosks

Answer: A

Explanation: Per NIST CSF 2.0 PR.AC-3, the BCP and BIA role in Protect is to tailor access during disruptions, with BIA impacts ensuring controls remain granular yet resilient. For the nonprofit, the $5M loss informs Attribute-Based Access Control (ABAC) that restricts admin actions outside BIA-defined windows, preventing insider abuse amid chaos. This maintains data integrity; the synergy supports least privilege, complies with GDPR, and enables audit logs for post-event reviews, safeguarding mission-critical funding streams.

Question: 360

While creating baseline configurations, team members are debating whether to include user-installed applications. According to NIST CSF best practices, how should these be handled?

A. Document installations but allow exceptions case-by-case without enforcement
B. Allow unrestricted installation for user productivity
C. Include all current user-installed applications regardless of risk
D. Exclude unauthorized user-installed applications by defining allowed software baselines and enforcing via endpoint management

Answer: D

Explanation: Defining allowed software baselines and blocking unauthorized applications reduces risk from unsupported or vulnerable software, maintaining baseline integrity.

Question: 361

VPN breach September 23, 2026; contain RS.MI-1: openvpn --config server.conf --kill-client 192.168.1.100. Sessions=50, kill time= Sessions * Disconnect_Sec=2=100 sec, what integrates with RADIUS for auth reset?

A. Kill without RADIUS
B. radclient -x auth client.cfg : disconnect , verify with radwho
C. Config reload isolated
D. Time without integrate

Answer: B

Explanation: RS.MI-1 terminates OpenVPN sessions with RADIUS disconnect, verified, aligning CSF 2.0 Access Control and SP 800-61 Rev. 3 VPN threats.

Question: 362

A utility company monitors for ICS anomalies using NIST CSF 2.0's Detect Function's External Information category (DE.AE-05), with threat intel integration score: Score = (Integrated_Alerts / Total_Alerts) × 100 = 65%. Which Detect category aligns DE.AE-05 to enhance shared threat awareness?

A. Continuous Monitoring
B. Adverse Event Analysis
C. Event Detection
D. Monitoring

Answer: B

Explanation: Adverse Event Analysis category in Detect, housing DE.AE-05, processes information on potential adverse events from external intel, aligning with Detect's identification goal. The score formula quantifies integration, supporting cross-Function links to Govern for strategy.

Question: 363

A defense contractor aligning to CSF 2.0 is assessing assets for CMMC Level 3 compliance, identifying a SCADA system controlling drone assembly lines with PLCs programmed in IEC 61131-3 ladder logic,

processing 1GB sensor data daily and dependent on Windows Server 2019 domains for authentication via LDAP binds on port 389. A vulnerability scan reveals unpatched MS17-010, potentially allowing lateral movement with a CVSS score of 10.0. Which assets must be protected to mitigate mission-critical risks, per ID.AM-5 dependencies mapping?

A. External dependencies like LDAP servers and sensor feeds, internal systems like PLCs, and facilities with assembly lines
B. Critical data flows from sensors, software dependencies in ladder logic code, and devices as PLC hardware
C. Organizational assets including personnel training records, communication flows via Modbus TCP, and supply chain firmware updates
D. All upstream dependencies on Windows domains, downstream impacts on drone output, and governance oversight committees

Answer: B

Explanation: ID.AM-5 requires mapping dependencies and upstream/downstream impacts, classifying the SCADA's sensor data flows (1GB/day), software (IEC 61131-3 code), and devices (PLCs) as critical due to MS17-010's high CVSS enabling control system compromise, directly threatening defense production. Protection involves patching protocols, air-gapped segmentation for PLCs, and dependency graphing tools to visualize LDAP/Modbus flows. This focus on core elements over external or governance aspects ensures resilience, as unaddressed dependencies could extend incident response timelines beyond 4-hour RTOs defined in BIA.

Question: 364

Which parameter in a continuous inventory system most effectively supports forensic investigation post-incident?

A. Password policies applied to asset users.
B. Asset color assigned by physical location.
C. Name of vendor who supplied the asset.
D. Historical change logs detailing asset configuration and ownership changes.

Answer: D

Explanation: Historical logs allow tracing asset alterations prior to incidents, essential for comprehensive forensic analysis.

Question: 365

During cybersecurity training, employees must understand data security principles. Which training approach best supports the Protect function’s data security subcategory?

A. Monthly email reminders with cybersecurity terminology only
B. General IT policy read-through without interactive elements
C. Scenario-based training that includes simulated data breach examples and response steps
D. Allowing optional attendance for training sessions

Answer: C

Explanation: Scenario-based interactive training ensures users internalize data security principles through simulated real-life situations, increasing awareness and preparedness.

Question: 366

A security team is configuring protective technologies on cloud infrastructure. Which advanced setting should be enabled to align with the latest NIST Protect function standards?

A. Grant unrestricted API access to internal developers
B. Disable logging to reduce storage costs
C. Limit encryption to data at rest only
D. Real-time configuration monitoring with automated rollback to baseline settings if deviations occur

Answer: D

Explanation: Real-time configuration monitoring with automatic rollback enforces baseline consistency, quickly mitigating configuration drift or unauthorized changes, a key element of the Protect function.

Question: 367

In NIST CSF 2.0, subcategory DE.AE-01 explains continuous monitoring's role in baseline establishment for a logistics firm's SIEM, using Sigma rule for Zeek DNS tunneling detection. What YAML syntax with detection logic and threshold for domain generation >50 unique in 1h?

A. title: DNS Tunneling; detection: selection: EventID: 3008; condition: selection | count(Domain) by SrcIP > 50 | window 1h; level: high
B. id: dns_tunnel; fields: zeek.dns; filter: dns$query gt 50 unique domains/hour; detection: threshold num_events 50 time_window 3600s by src_ip; falsepositives: legitimate DGA
C. title: 'Suspicious DNS Query Volume'; logsource: product: zeek; detection: selection: query: '*'; condition: query | stats dc(domain) as unique_domains by orig_h > 50 | where unique_domains > threshold; tags: [attack.t1071]
D. rule: DNS_Anomaly; query: event.module:zeek and event.dataset:dns; agg: { unique_queries: { terms:

{ field: dns.question.name.keyword, size: 100 } } }; threshold: { value: 50, window: 1h }; by: [source.ip]

Answer: D

Explanation: DE.AE-01's continuous baselines benefit predictive defense, identifying tunneling via high entropy domains. The Sigma YAML uses Elasticsearch DSL for Zeek logs, terms agg on dns.question.name for unique count >50 in 1h by source.ip, with windowed threshold. This detects exfil (ATT&CK T1048), reducing false positives via size=100. Benefits: 65% faster threat ID per SANS 2024; CSF 2.0 analysis subcats integrate ML for entropy H=-∑p log p. Verified against Suricata converters.

Question: 368

A telecom operator detects 5G core signaling storms on September 14, 2026, with tcpdump -i any -w storm.pcap 'diameter', capturing 200K sessions. Contain via RS.MI-3: isolate VLANs using Cisco ACL: access-list 101 deny ip 10.1.1.0 0.0.0.255 any; int vlan 10; ip access-group 101 in. If storm affects 35% base stations, formula Containment_Time = (Sessions_K / ACL_Deploy_Sec=30) * Impact%=200/30*35=233.3 min projected, what command sequence best contains while minimizing outage?

A. Impact percentage calculation standalone
B. Run tcpdump capture without ACL deployment
C. VLAN isolation command without verification
D. Apply ACL then verify with show access-lists | include matches >1000, followed by SNMP trap to NMS

Answer: D

Explanation: RS.MI-3 in CSF 2.0 requires rapid containment actions like ACLs to limit expansion, verified via show commands and SNMP for 5G resilience, aligning with SP 800-61 Rev. 3's Respond Mitigation. Sequence ensures efficacy, reducing outage from projected 233 min.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.