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

CCSS-Security Coh350 MCQs
CCSS-Security Coh350 Exam Questions
CCSS-Security Coh350 Practice Test
CCSS-Security Coh350 TestPrep
CCSS-Security Coh350 Study Guide

killexams.com

COHESITY

Security (Coh350)

Cohesity Certified Security Specialist

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CCSS-Security

Question: 1201

Which recovery approach minimizes disruption while ensuring security in a distributed environment?

A. Staged recovery with segmented network access controls
B. Simultaneous global restore without restrictions
C. Complete shutdown of all networked devices until clean
D. Full reinstallation of all user devices simultaneously

Answer: A

Explanation: Staged recovery with network segmentation controls risk and limits impact, allowing secure validation at each stage.

Question: 1202

A company is conducting a security audit and needs to focus on the effectiveness of their logging practices. Which areas should they evaluate?

A. Completeness of logged data
B. Accessibility of log data for analysis
C. Frequency of log reviews
D. User feedback on logging tools

Answer: A,B,C

Explanation: Evaluating the completeness of logged data is crucial to ensure that all relevant activities are captured for security analysis. The accessibility of log data for analysis is important for enabling timely investigations. The frequency of log reviews should also be assessed to ensure that logs are being analyzed regularly for potential threats. User feedback on logging tools, while valuable for usability, is not a primary focus of a security audit.

Question: 1203

What is the significance of restricting SSH shell access to iris_cli rather than full shell access on Cohesity clusters?

A. Limits potential commands and mitigates exploitation risk
B. Reduces the need for authentication

C. Ensures faster data transfer
D. Allows anonymous scripting

Answer: A

Explanation: iris_cli restricts users to specific operational commands, reducing exposure to potential shell-level abuse or accidental misconfigurations.

Question: 1204

Which process ensures that changes to security-critical configurations require multiple administrators' approval?

A. Quorum enforcement
B. Full admin rights to one user
C. Disabling audit trails
D. Single factor authentication

Answer: A

Explanation: Quorum enforcement obliges consensus by multiple administrators for sensitive actions, minimizing risks of unilateral risky changes.

Question: 1205

A telecommunications provider evaluates Cohesity amid rising 5G-related cyber espionage threats, designing Zero Trust for subscriber data backups in hybrid telco clouds. Which principles address dynamic endpoint proliferation?

A. Adaptive authentication policies scaling with endpoint density, integrating device certificates for verification
B. Distributed immutability enforcement at the edge with central orchestration for policy consistency
C. Real-time encryption key rotation triggered by access frequency thresholds in high-mobility networks
D. Federated identity bridging with external IAMs to maintain zero trust across roaming data flows

Answer: A, D

Explanation: In telco with 5G endpoints, adaptive policies using device certs verify dynamic connections, scaling Zero Trust to proliferation without static perimeters. Federated IAM bridging ensures consistent identity validation across roaming, preventing trust gaps in hybrid flows. Distributed immutability supports edge but requires central policy for uniformity, while key rotation enhances but doesn't core-address endpoint dynamics.

Question: 1206

In a large financial enterprise deploying Cohesity DataProtect across a hybrid cloud environment, the security team identifies potential vulnerabilities in network protocols during a routine audit following a recent ransomware simulation exercise. To mitigate risks associated with unauthorized access to backup repositories, which of the following advanced configurations should be implemented to control network protocol access on the Cohesity cluster?

A. Configure IP-based access control lists (ACLs) on the cluster's management interfaces to restrict inbound connections solely to VLAN 10 for administrative protocols like SSH and HTTPS
B. Enable protocol-specific firewall rules using iptables to block all non-essential ports, including UDP 53 for DNS, while allowing only TCP 443 for encrypted management traffic
C. Implement role-based access control (RBAC) policies integrated with Active Directory to dynamically permit or deny protocol access based on user group membership during peak backup windows
D. Deploy network segmentation via VXLAN overlays to isolate backup traffic on dedicated virtual networks, enforcing protocol whitelisting for NFSv4 and SMB3 only between source hosts and the Cohesity nodes

Answer: A, B, D

Explanation: In Cohesity DataProtect deployments, controlling network protocol access begins with granular IP-based ACLs on management interfaces, which limit inbound traffic to specific VLANs for protocols such as SSH (TCP 22) and HTTPS (TCP 443), preventing lateral movement by threat actors in hybrid setups. Complementing this, iptables-based firewall rules are essential to disable unnecessary ports like UDP 53 (DNS) while permitting only secure channels, aligning with zero-trust principles to reduce the attack surface in audited environments post-simulation. Additionally, VXLAN-based segmentation isolates backup flows, whitelisting secure file protocols like NFSv4 and SMB3 to ensure only validated traffic reaches cluster nodes, enhancing resilience against protocol exploits in large-scale financial operations. RBAC, while

critical for user-level controls, does not directly govern network protocol access at the infrastructure layer.

Question: 1207

In a multi-tenant environment, a user reports that they can access data belonging to another tenant. What should be the immediate action taken to address this issue?

A. Review and modify the user's access permissions
B. Disable the user's account immediately
C. Investigate potential misconfigurations in tenant isolation
D. Notify all tenants about the breach

Answer: A,C

Explanation: The immediate action should involve reviewing and modifying the user's access permissions to ensure they align with their role and responsibilities. Investigating potential misconfigurations in tenant isolation is crucial to identify how the access occurred. Disabling the user's account may be necessary but should be done after understanding the situation, while notifying all tenants may cause unnecessary panic if the issue is contained.

Question: 1208

Why is the Cohesity grub password protected, and what security principle does disabling single user mode enforce?

A. To prevent unauthorized boot changes; ensures system integrity
B. To allow easy recovery; enforces accountability
C. To enable multi-factor authentication; ensures user convenience
D. To disable BIOS access; enforces audit logging

Answer: A

Explanation: Password protecting the grub bootloader and disabling single user mode prevent unauthorized physical or remote boot-time changes, maintaining system integrity and reducing attack vectors at the system startup level.

Question: 1209

Which of the following best describes the role of remote syslog servers in Cohesity audit logging?

A. They store application performance metrics
B. They manage user authentication
C. They generate random test alerts
D. They provide centralized, off-cluster storage of audit logs for security and compliance

Answer: D

Explanation: Remote syslog servers collect and store audit logs from the Cohesity cluster centrally. This offloading protects logs from local compromise, improves security by preserving integrity, and facilitates compliance audits.

Question: 1210

A gaming company battles cheat engine threats, evaluating third-party for Cohesity securing player data. Which detect in-game data tampering?

A. Anti-cheat from Easy Anti-Cheat for scanning game server backups in Cohesity
B. Behavioral analytics from Splunk for player action anomalies in logs
C. Encryption for telemetry from Virtru to protect in-transit game data to backups
D. Fraud detection from Feedzai for real-time validation before ingestion

Answer: A, B, D

Explanation: In gaming, Easy Anti-Cheat scans backups for cheats. Splunk analyzes player behaviors. Feedzai validates fraud in real-time. Virtru protects transit but not detection.

Question: 1211

A VR/AR content creator's Cohesity backups over 6G prototypes face protocol slicing vulnerabilities. Practices:

A. Slice-aware protocol enforcement in Cohesity, allocating dedicated network slices for immersive content backups with QoS isolation
B. Embed haptic feedback loops in protocol ACKs, verifying VR data integrity via tactile simulation proxies
C. Utilize 6G URLLC modes for low-latency protocol handshakes, prioritizing Cohesity

sessions in AR rendering pipelines
D. Integrate spatial computing tags in encrypted payloads, enabling 3D-aware decryption for VR recovery

Answer: A, C

Explanation: 6G Cohesity leverages slicing for isolated backups and URLLC for low-latency handshakes. Haptic and spatial tags are content-specific, not protocol security.

Question: 1212

A company is implementing multitenancy security in their Cohesity environment. Which of the following configurations should be considered to ensure proper isolation between tenants?

A. Assign unique admin roles for each tenant
B. Use a shared storage pool for all tenants
C. Implement separate network segments for each tenant
D. Enable audit logs for each tenant's activities

Answer: A,C,D

Explanation: To ensure proper isolation between tenants in a multitenant environment, it is essential to assign unique admin roles for each tenant, implement separate network segments to avoid cross-tenant access, and enable audit logs for monitoring tenant activities. Using a shared storage pool can lead to potential data leakage between tenants.

Question: 1213

A logistics firm dealing with international trade data evaluates third-party solutions in Cohesity's design to counter cross-border ransomware variants. Which are pertinent for global incident response orchestration?

A. Integration with ServiceNow for ITSM ticketing of Cohesity alerts in distributed ops centers
B. Threat hunting platforms like FireEye for deep forensic analysis of encrypted backups
C. Global CDN providers like Akamai for geo-redundant vault distribution with DDoS mitigation
D. Compliance automation tools from OneTrust for automated retention policy alignment across jurisdictions

Answer: A, B

Explanation: In logistics, ServiceNow integration tickets Cohesity alerts for coordinated response across borders, enhancing orchestration. FireEye enables forensic dives into backups, crucial for variant attribution. CDN redundancy aids availability but not core response, while OneTrust automates compliance but is governance-oriented.

Question: 1214

How can Cohesity use custom RBAC roles to enhance security?

A. By giving all roles full access
B. By defining specific permissions aligned to organizational policies
C. By using the default roles only
D. By removing all access restrictions

Answer: B

Explanation: Custom RBAC roles allow organizations to tailor permissions precisely, ensuring users get access strictly aligned to their responsibilities.

Question: 1215

In a recent audit, it was discovered that a company's data isolation practices were inadequate, leading to unauthorized access to sensitive information. Which actions should the company take immediately?

A. Review and update access control policies
B. Increase the number of users with administrative privileges
C. Conduct a comprehensive security training for all employees
D. Implement logging and monitoring of data access

Answer: A,C,D

Explanation: Reviewing and updating access control policies is crucial to prevent unauthorized access. Comprehensive security training raises awareness among employees, while logging and monitoring help detect and respond to security incidents in real-time.

Question: 1216

Which MFA factor category does biometric authentication fall under?

A. Knowledge
B. Inherence
C. Possession
D. Location

Answer: B

Explanation: Biometrics are based on something inherent to the user, such as fingerprints or facial recognition, distinguishing them from possession (e.g., tokens) or knowledge (e.g., passwords).

Question: 1217

What is a critical advantage of using instant mass restore selectively rather than restoring full backups during security incidents?

A. It resets all user credentials
B. It disables all cluster alerts to enhance performance
C. It automatically quarantines infected backups
D. It reduces restoration time for critical workloads

Answer: D

Explanation: Instant mass restore enables rapid recovery of critical data minimizing downtime, whereas disabling alerts, quarantining backups, or resetting credentials are separate processes.

Question: 1218

During digital forensics training, a law enforcement agency assesses third-party solutions for Cohesity in evidence chain management. Which are relevant for tamper-evident integrations?

A. Forensic toolkits like EnCase for chain-of-custody verification on restored snapshots
B. Blockchain ledgers from IBM for immutable hashing of evidence backups
C. E-discovery platforms from Relativity for searchable indexing of Cohesity views

D. Access logging enhancers from Imperva for detailed provenance tracking

Answer: A, C

Explanation: For law enforcement, EnCase verifies custody on restores, ensuring evidentiary integrity. Relativity enables searchable e-discovery on views, streamlining investigations. Blockchain hashing adds immutability but duplicates Cohesity's WORM. Imperva enhances logging but isn't core to chain management.

Question: 1219

Which encryption technology is used by Cohesity to secure replicated data inflight?

A. SSL 2.0
B. TLS 1.3
C. DES
D. RC4

Answer: B

Explanation: Cohesity uses the modern TLS 1.3 protocol for securing data inflight replication, avoiding outdated and vulnerable protocols like SSL 2.0 or deprecated cyphers.

Question: 1220

A company is implementing a new security policy that requires all logs to be sent to a remote syslog server. What are the key factors they should consider in this implementation?

A. Network latency between the Cohesity system and the syslog server
B. Compatibility of syslog formats
C. Encryption of log data in transit
D. Frequency of log transmission

Answer: A,B,C,D

Explanation: Key factors to consider when implementing remote syslog servers include network latency, as delays can affect real-time monitoring capabilities. Compatibility of syslog formats is essential to ensure that logs can be properly interpreted by the receiving

server. Encrypting log data in transit is crucial for protecting sensitive information from interception. Finally, the frequency of log transmission should be determined to balance performance and the need for timely log availability.

Question: 1221

What is the main advantage of using write-once snapshots from a security perspective?

A. Faster snapshot deletions
B. Prevention of tampering and ransomware encryption
C. Lower storage costs without replication
D. Easier snapshot modifications

Answer: B

Explanation: Write-once snapshots ensure backups cannot be altered post-creation, effectively blocking ransomware from encrypting or tampering with backup data.

Question: 1222

In Cohesity, what is the impact of using certificate pinning on HTTPS connections for backup data?

A. Allows anonymous access
B. Speeds up handshake process
C. Disables encryption
D. Prevents man-in-the-middle attacks

Answer: D

Explanation: Certificate pinning ties connections to specific public keys, preventing attackers from using rogue certificates, thus helping prevent man-in-the-middle attacks during backup data transmission.

Question: 1223

A pharmaceutical R&D firm with Cohesity protecting genomic sequencing data in S3 detects insider threat via anomalous access patterns in Elasticsearch indices. Clean room

assessment must support eDiscovery and recovery of 900TB while complying with GxP. Which requirements should be prioritized?

A. Integration of Cohesity with Relativity for chain-of-custody in genomic data forensics
B. Validation of data lineage graphs for sequencing pipelines in isolated clean room views
C. Deployment of air-gapped Cohesity nodes with quantum-resistant encryption for long-term retention
D. Automated redaction tools for PII scrubbing during clean room scanning workflows

Answer: B, D

Explanation: Data lineage graphs trace modifications in sequencing pipelines, enabling identification of insider alterations without production impact, essential for GxP audit trails in clean room isolation. Automated redaction ensures PII compliance during scans, preventing exposure of sensitive genomic data and supporting eDiscovery requirements. Relativity aids legal but is not core to technical assessment; quantum-resistant crypto is forward-looking but not immediate for insider threats.

Question: 1224

A fintech's Cohesity for transaction logs uses FIX protocol on TCP 7511, exposed to sequence number replays. Which controls secure FIX access?

A. Mandate FIX 5.0 SP2 with TLS 1.3 and session recovery tags.
B. Configure possessor replay detection with GapFill rejectors.
C. Apply FIX edge proxies with certificate-bound sender compIDs.
D. Enforce heartbeat intervals under 20 seconds with test requests.

Answer: A, C

Explanation: FIX 5.0 with TLS secures transport and recovery. Proxies with compID certs prevent impersonation. Gaps detect replays; heartbeats ensure liveness.

Question: 1225

A Cohesity cluster administrator is preparing for an upcoming security audit. Which monitoring practices should they ensure are in place?

A. Regular reviews of alert notification settings
B. Continuous monitoring of user access to sensitive data
C. Implementation of a centralized logging system for all alerts

D. Annual training sessions on security policies for all staff

Answer: A,B,C

Explanation: Ensuring regular reviews of alert notification settings is crucial for maintaining effective monitoring capabilities. Continuous monitoring of user access to sensitive data helps detect unauthorized access in real-time. Implementing a centralized logging system for all alerts allows for better analysis and correlation of events. While annual training sessions on security policies for all staff are important for overall security awareness, they are not a direct monitoring practice.

Question: 1226

An automotive supplier's Cohesity setup is hit by a ransomware variant targeting CAD backups via engineer laptops, using USB vectors. The Security Assessment uncovers endpoint gaps. Which features extend protection to endpoints?

A. Agentless backup with endpoint EDR hooks for USB malware scanning pre-transfer
B. Behavioral endpoint monitoring alerting on CAD file encryption patterns
C. Immutable USB airlock protocols delaying transfers until integrity verification
D. Federated endpoint policies syncing with Cohesity for unified ransomware response

Answer: A, B, D

Explanation: Agentless backup leverages EDR integrations to scan USB payloads for malware before CAD data transfer, blocking variants at the endpoint and preventing ingress into the Cohesity cluster, crucial for IP protection in automotive design chains. Behavioral endpoint monitoring tracks file mutation rates on laptops, alerting on ransomware-like entropy increases in CAD files and triggering remote wipes if thresholds breach. Federated endpoint policies propagate Cohesity immutability rules to endpoints, enabling coordinated isolation and recovery across the supplier ecosystem.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, 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.

Exam Questions:

Killexams.com provides 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 questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

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

Practice Test:

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

Guaranteed Success:

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

Updated Contents:

Killexams.com regularly updates its question bank of MCQs 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.