Boost up Your Certification Score

CyberArk
GUARD
CyberArk Guardian Exam

Exams Boost
Boost Up Your Career

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/guard

Latest Version: 6.0

Question: 1

What encryption capability is required for the HSM?

A. The HSM must support AES-192 encryption in ECB mode.
B. The HSM must support Triple Data Encryption Standard (TripleDES).
C. The HSM must support AES-256 encryption in ECB and CBC modes.
D. The HSM must support Blowfish encryption algorithm.

Answer: C

Explanation:
Hardware Security Modules (HSMs) provide protected cryptographic key storage and cryptographic operations within a dedicated security boundary.
When integrating an HSM with the CyberArk Digital Vault, the selected device and its cryptographic interface must support the algorithms and mechanisms required by the applicable Vault integration.
For the HSM requirement represented by this question, the expected capability is AES-256 encryption with support for Electronic Codebook (ECB) and Cipher Block Chaining (CBC) modes.
AES-256 uses a 256-bit encryption key and is widely implemented in enterprise cryptographic systems.
CBC and ECB are distinct block-cipher operating modes. Their inclusion in an HSM capability requirement does not mean that both should be used interchangeably for protecting arbitrary application data.
ECB is unsuitable for general-purpose bulk-data encryption because identical plaintext blocks produce identical ciphertext blocks. Its availability may nevertheless be required for a particular supported cryptographic mechanism.
TripleDES and Blowfish are not appropriate substitutes for the specified AES-256 functionality, while AES-192 alone does not satisfy the stated requirement.
Architects must additionally verify HSM compatibility, PKCS#11 integration, supported firmware, key management procedures, and recovery requirements.
[Reference:CyberArk Digital Vault — Hardware Security Module Integration, Server Key Protection, PKCS#11 Cryptographic Interface and Supported Encryption Mechanisms.]

Question: 2

How can a Secondary PTA server be promoted to a Primary PTA Server?

A. A manual procedure.
B. Automatically using the PTA Network Sensors.
C. This is not possible.
D. Automatically using a BASH script.

Answer: A

Explanation:
CyberArk Privileged Threat Analytics (PTA) provides security analytics for privileged account activity, identifying suspicious behavior, anomalous access patterns, and potential credential misuse.
In the traditional PTA disaster recovery architecture, the Primary PTA server processes incoming security events and performs the active analytics functions. A Secondary PTA server maintains replicated information and provides a recovery capability if the Primary PTA becomes unavailable.
Promoting the Secondary server requires an administrator-controlled failover procedure. The administrator must confirm the failure, assess replication consistency, activate the secondary environment according to the supported recovery procedure, and ensure that relevant integrations direct their traffic to the newly active server.
PTA Network Sensors collect network authentication information for analytics. They do not independently manage PTA server promotion or provide automatic high-availability orchestration.
Although Linux shell scripts may be involved in PTA disaster recovery configuration and recovery operations, the presence of such scripts does not mean that unattended automatic promotion is supported.
Manual promotion provides operational control over recovery and helps prevent inconsistent analytics environments or an unintended simultaneous-primary condition.
[Reference:CyberArk Privileged Threat Analytics — Disaster Recovery Architecture, Secondary PTA Server, Manual Failover and Recovery Procedures.]

Question: 3

What type of attack can CyberArk mitigate?

A. Pass-the-Hash
B. SQL Injection
C. DDOS
D. Phishing

Answer: A

Explanation:
Pass-the-Hash is an authentication attack in which an adversary obtains an NTLM password hash and uses it to authenticate without knowing the corresponding plaintext password.
The technique is particularly dangerous in Windows environments where privileged credentials or reusable authentication material are exposed across multiple systems.
CyberArk mitigates this risk through privileged credential protection, controlled session initiation, endpoint privilege management, and restrictions on local administrative privileges.
CyberArk PAM helps reduce credential exposure by rotating privileged account passwords, maintaining unique credentials where applicable, and isolating administrative sessions through Privileged Session Manager.
CyberArk Endpoint Privilege Manager complements these protections by restricting unnecessary administrative access and implementing endpoint controls designed to reduce credential-theft and lateral-movement opportunities.
These safeguards make it more difficult for attackers to obtain and reuse privileged authentication material.

However, password rotation alone does not guarantee prevention of Pass-the-Hash attacks. Effective protection also depends on endpoint configuration, authentication mechanisms, credential isolation, and Windows security controls.
SQL Injection primarily concerns weaknesses in application input handling. DDoS targets service availability, while phishing involves social engineering. CyberArk offers identity-related defenses relevant to some phishing scenarios, but Pass-the-Hash is the specific attack most directly aligned with the controls tested here.
[Reference:CyberArk Identity Security — Credential Theft Prevention, Endpoint Privilege Manager, Privileged Session Isolation and Lateral Movement Protection.]

Question: 4

ClientABC is moving into the DevOps space. They currently use CCP and are considering Conjur. They have noticed there is considerable overlap.
How would you explain the difference between the two?
Choose two

A. Conjur is well suited for the velocity of the CI/CD pipeline because it includes native authentication such as API keys, 1AM, and OAuth. You store the secret at the project folder level.
B. CCP is a good choice if you're using client certificate authentication. With CCP you need to authenticate and pass an application ID and your query for your secret.
C. Conjur is best suited for static secrets. You only need to pass an API key to make the call. This is suited well for the velocity of the CI/CD pipeline because it integrates seamlessly with containers.
D. CCP is best used for ad-hoc scripts. It's a great choice because you're able to use enhanced authentication mechanisms such as 'Path' and 'Hash'.
E. When trying to decide between the two, you should generally choose CCP, as Conjur cannot be integrated with the same vault that is used for CyberArk PAM.

Answer: A, B

Explanation:
CyberArk Central Credential Provider (CCP) and Conjur both provide secure credential retrieval, but they address different application architectures and operational requirements.
CCP is an agentless credential retrieval service accessed through HTTPS. Applications authenticate using supported methods, including client certificates, and submit requests containing an authorized Application ID and criteria identifying the requested account.
This makes CCP suitable for traditional applications, automation scripts, and systems that can integrate with an HTTPS-based credential retrieval interface.
Conjur is designed primarily for cloud-native applications, containers, orchestration platforms, and CI/CD workflows.
It supports workload-oriented authentication mechanisms, including API-key authentication and integrations with cloud identity services and signed identity tokens.
Conjur also supports policy-based secrets management, allowing development teams to define application identities and authorized access through structured policies.
Option C incorrectly suggests that Conjur is limited to static secrets and that all workloads authenticate exclusively through API keys.

Option D incorrectly attributes local executable path and hash authentication mechanisms to CCP as its defining capability. Option E is incorrect because supported Conjur architectures can integrate with CyberArk PAM through synchronization mechanisms.
[Reference:CyberArk Secrets Manager (Conjur) — Workload Authentication, Policy-as-Code, CI/CD Integration, Central Credential Provider and Vault Synchronizer.]

Question: 5

A customer must retain all privileged-access records for 7 years. The environment has approximately 2000 users who create nearly 100 GB of session recordings each day.
How should CyberArk PAS be designed to meet this requirement for PSM recordings?

A. Set a low PSM Recording Retention period and use Secure Replicate to offload recordings for archival storage.
B. Connect Vault servers to SAN storage and increase disk size whenever free disk space monitoring sends an alert.
C. Connect external storage to PSM servers to more evenly distribute the storage requirements.
D. Set Audit Retention Master Policy and PSMRecording Safe object retention to 2555 days (365 days * 7 years).

Answer: A

Explanation:
CyberArk Privileged Session Manager records administrative sessions and stores completed recordings in designated Recording Safes within the Digital Vault.
At approximately 100 GB per day, retaining seven years of recordings requires substantial storage capacity.
The estimated volume is:
100 GB × 365 × 7 = 255,500 GB
This represents approximately 255.5 TB before accounting for filesystem overhead, additional metadata, growth, and redundancy.
Retaining this entire volume within the operational Digital Vault would introduce considerable storage, backup, and recovery requirements.
The more appropriate approach is to establish a shorter operational recording-retention period and use CyberArk replication or supported archival processes to transfer recordings into secure long-term storage.
Secure Replicate can support the transfer of Vault data into an external backup environment, reducing dependence on continuously expanding primary Vault storage.
However, the archival solution must independently enforce the required seven-year retention period, integrity protection, recoverability, and audit requirements. A backup copy alone does not automatically establish regulatory compliance.
Option B relies on reactive storage expansion. Option C incorrectly treats PSM servers as the permanent recording archive. Option D does not address practical capacity management and incorrectly combines different retention mechanisms.
[Reference:CyberArk Digital Vault — Secure Replicate, Vault Backup and Recovery, PSM Recording Safes, Recording Retention and Long-Term Archival Design.]

Visit us at: https://www.examsboost.com/test/guard

Question: 6

Which risk should be considered before enabling OLAC (Object Level Access Control)?

A. OLAC can significantly impact Vault performance.
B. OLAC can increase in complexity for user access workflows.
C. OLAC prevents the use of PSM session isolation and recording.
D. OLAC automatically grants 'Use' and 'Retrieve" authorizations to any new safe owner.

Answer: A

Explanation:
CyberArk Object Level Access Control (OLAC) enables administrators to assign permissions to individual objects stored within a Safe rather than relying exclusively on Safe-level authorizations.
This capability is useful when different privileged accounts within the same Safe require distinct access restrictions.
However, enabling OLAC introduces additional authorization-processing requirements.
Without OLAC, the Vault can determine access primarily through Safe-level membership and authorization settings.
When OLAC is enabled, the Vault must also evaluate object-specific permissions for relevant access operations.
As the number of objects, users, groups, and authorization relationships grows, this additional processing can increase administrative overhead and negatively affect Vault performance.
The performance implications are particularly important in large enterprise deployments containing substantial numbers of privileged accounts and frequent credential-access requests.
CyberArk therefore recommends using granular object-level authorization selectively, according to documented business requirements.
An additional limitation is that enabling OLAC for a Safe is not a temporary configuration decision; it cannot subsequently be disabled through the supported configuration mechanism.
Option B identifies a possible operational consequence, but option A represents the specific performance risk emphasized by the source.
Options C and D incorrectly describe PSM functionality and permission inheritance.
[Reference:CyberArk PAM Self-Hosted — Object Level Access Control, Safe Authorization Model, Vault Performance Considerations and OLAC Configuration Limitations.]

Question: 7

In the customer’s current environment, Administrators use shared Admin accounts. The account passwords are configured never to expire and are stored in an Excel sheet that each Administrator keeps locally on their system.
How can the customer use CyberArk to secure the shared Admin accounts?

A. Vault the shared accounts and allow the Administrators access to the accounts via CyberArk and enable one-time passwords and exclusive accounts.

B. Vault the shared accounts in CyberArk and enable one-time passwords and exclusive accounts. Create new shared accounts for the Administrators to use outside of CyberArk.
C. Vault the shared accounts and do not allow the Administrators to use the accounts in CyberArk.
D. Vault the shared accounts and allow the Administrators access to the accounts via CyberArk and enable manual password change.

Answer: A

Explanation:
Shared administrative accounts present significant security risks when their credentials are distributed among multiple users and stored in uncontrolled locations.
In the described environment, administrators maintain local Excel files containing passwords that never expire. These credentials can be copied, disclosed, reused, or compromised without effective centralized oversight.
CyberArk Privileged Access Manager mitigates these risks by storing privileged credentials in the Digital Vault and enforcing controlled access through PVWA and supported session-management components.
Enabling one-time password access causes CyberArk to change the managed password after use, according to the configured password-management workflow.
This reduces the time during which a previously retrieved password remains valid.
Exclusive check-in/check-out controls restrict concurrent checkout of a shared privileged account, reducing overlapping administrative access and improving accountability.
Administrators can continue performing authorized work while CyberArk records credential access and associated privileged-session activity.
Option B undermines the solution by introducing additional unmanaged shared accounts. Option C prevents legitimate administrative use. Option D relies on manual password changes and does not adequately address the risks associated with static shared credentials.
[Reference:CyberArk PAM — Digital Vault, Shared Privileged Accounts, One-Time Password Access, Exclusive Check-In/Check-Out and Privileged Session Management.]

Question: 8

Where should the Master Private Key be stored?

A. A physical safe or similar solution.
B. USB drive.
C. On the Vault server.
D. In a Safe in the Vault.

Answer: A

Explanation:
The CyberArk Digital Vault uses cryptographic key material to protect sensitive information stored within its secure repository.
The Master Private Key is a highly sensitive recovery asset associated with emergency access and cryptographic recovery operations.

Because compromise of this key could undermine the security of protected Vault information, its storage requires controls substantially stronger than those applied to ordinary operational files.
The recommended approach is to maintain the Master Private Key offline, protected by strict physical access controls.
A physical safe or equivalent secure custody solution provides protection against remote compromise and reduces the likelihood that an attacker who gains access to an operational system can also obtain the recovery key.
Organizations should establish formal procedures governing key custody, authorized access, recovery operations, and access auditing.
Depending on organizational requirements, additional safeguards may include dual-person authorization, controlled key backups, tamper-evident storage, and geographically separated recovery materials.
A USB drive alone does not provide adequate protection unless incorporated into an appropriately controlled custody process.
Storing the Master Private Key on the Vault server or within the same Vault it protects would introduce unnecessary security dependencies.
The selected storage arrangement must support both strong confidentiality and reliable recovery during a major infrastructure failure.
[Reference:CyberArk Digital Vault — Master Key Management, Master Private Key, Emergency Recovery, Cryptographic Key Custody and Disaster Recovery Security.]

Question: 9

At which stage is it appropriate to incorporate the C3 Alliance integrations?

A. Since we already have integrations available and little development is required, they should all be completed in Stage 1.
B. Integrate the security tools in Stage 1 and other tools such as RPA in Stage 2.
C. They are less of a risk, so we should leave them until Stage 3 and focus on other privileged accounts first.
D. They should all be integrated prior to the actual ’go-live' of CyberArk PAM.

Answer: B

Explanation:
The CyberArk Blueprint establishes a risk-based, phased approach to implementing privileged access management and identity security controls. C3 Alliance integrations should be introduced according to their contribution to risk reduction, security operations, and organizational readiness.
Stage 1 prioritizes foundational security controls and integrations with third-party security tools. These may include vulnerability management, security monitoring, and discovery solutions that rely on highly privileged credentials. Securing these integrations early reduces the exposure of powerful service accounts and improves the organization's ability to monitor privileged activity.
Stage 2 extends the program to commonly deployed technologies and third-party business applications. Robotic Process Automation platforms, such as UiPath and Automation Anywhere, frequently use service accounts to interact with enterprise systems. Integrating these applications with CyberArk enables centralized credential management and reduces dependence on embedded or hard-coded credentials.

Implementing every integration in Stage 1 would unnecessarily increase deployment complexity and potentially delay foundational security improvements. Conversely, deferring essential security integrations until Stage 3 would postpone meaningful risk reduction.
The appropriate implementation sequence balances security impact, operational dependencies, and deployment effort.
[Reference:CyberArk Blueprint — Stage 1: Highest Privilege Identities; Stage 2: Common Technology Platforms; C3 Alliance Integrations.]

Question: 10

What are the three Guiding Principles of the CyberArk Blueprint?

A. Credential Theft, Lateral and Vertical Movement, Privilege Escalation and Abuse.
B. Identity Security, Credential Theft, Lateral and Vertical Movement.
C. Attack and Defend capability, Credential Theft, Least Privilege.
D. Quick return on investment, Password Management, Credential Theft.

Answer: A

Explanation:
The CyberArk Blueprint is based on three security principles designed to interrupt the identity attack chain used by malicious actors to compromise enterprise systems.
The first principle is preventing credential theft . Attackers frequently obtain passwords, authentication tokens, SSH keys, and other privileged credentials through phishing, malware, exposed configuration files, or credential repositories. CyberArk mitigates these risks through secure credential storage, controlled retrieval, password rotation, and session isolation.
The second principle is stopping lateral and vertical movement . After obtaining initial access, attackers attempt to move between systems or cross security boundaries to reach more valuable resources. Unique privileged credentials, segmentation, and controlled privileged sessions reduce opportunities for such movement.
The third principle is limiting privilege escalation and abuse . Attackers may attempt to elevate compromised identities into administrative roles or misuse existing privileges. Least-privilege controls, session monitoring, application control, and just-in-time access help restrict these activities.
Together, these principles support the Blueprint's phased implementation methodology. Organizations can prioritize security controls according to their ability to reduce identity-related attack risk.
Option A correctly identifies all three areas, although CyberArk commonly presents them as preventative actions rather than simply naming the attack techniques.
[Reference:CyberArk Blueprint — Three Guiding Principles: Prevent Credential Theft, Stop Lateral and Vertical Movement, Limit Privilege Escalation and Abuse.]

Visit us at: https://www.examsboost.com/test/guard

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

