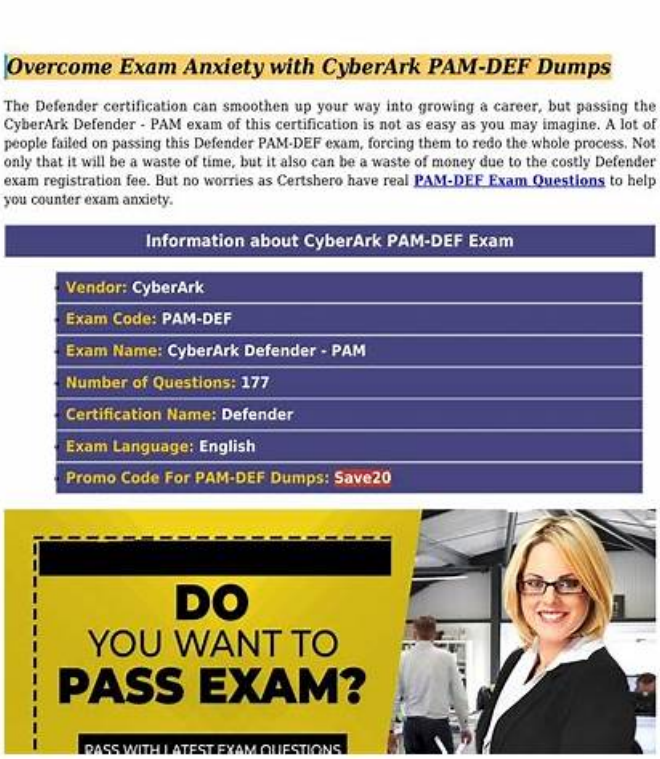
PAM-DEF Dumps und Test Überprüfungen sind die beste Wahl für Ihre CyberArk PAM-DEF Testvorbereitung



P.S. Kostenlose und neue PAM-DEF Prüfungsfragen sind auf Google Drive freigegeben von It-Pruefung verfügbar: https://drive.google.com/open?id=1-1itIBrPxz5PXzsiVvUuwecUK5zfbBB6

It-Pruefung bietet Ihnen die neuesten Schulungsunterlagen zur CyberArk PAM-DEF Zertifizierungsprüfung. Die fleißigen IT-Experten von It-Pruefung aktualisieren ständig Schulungsunterlagen durch ihre eigene Kompetenz und Erfahrung, so dass die IT-Fachleute die Prüfung mühlos bestehen können. Das CyberArk PAM-DEF Zertifikat stellt eine immer wichtigere Stelle in der IT-Branche dar. Und immer mehr Leute haben sich an dieser Prüfung beteiligt. Und viele davon benutzen unsere Produkte von It-Pruefung und haben die CyberArk PAM-DEF Zertifizierungsprüfung bestanden. Die Feedbacks von diesen Leute haben bewiesen, dass unsere Produkte von It-Pruefung eher zuverlässig sind.

Cyberark PAM -Def (Cyberark Defender - PAM) Zertifizierungsprüfung ist ein Zertifizierungsprogramm, das von Cyberark für Fachleute im Bereich Cybersicherheit entworfen wurde. Diese Zertifizierung soll die Fähigkeiten und Kenntnisse von Fachleuten validieren, die für die Sicherung privilegierter Konten verantwortlich sind und Cyber -Angriffe auf diesen Konten verhindern. Die Cyberark PAM-Def-Zertifizierungsprüfung soll die Kenntnisse der Fachleute bei der Verwendung von Cyberarks Privilegge Access Management (PAM) -Lösungen (Cyberark) bewerten.

>> PAM-DEF Examsfragen <<

Die anspruchsvolle PAM-DEF echte Prüfungsfragen von uns garantiert Ihre bessere Berufsaussichten!

Wenn Sie noch zögern, ob Sie It-Pruefung wählen, können Sie kostenlos einen Teil der CyberArk PAM-DEF Fragen und Antworten in It-Pruefung Website herunterladen, um unsere Zuverlässigkeit zu testen. Wenn Sie alle unsere Prüfungsfragen und Antworten herunterladen, geben wir Ihnen eine 100%-Pass-Garantie, dass Sie die CyberArk PAM-DEF Zertifizierungsprüfung einmalig mit einer hohen Note bestehen können.

Die Cyberark PAM -Def (Cyberark Defender - PAM) Prüfung ist ein Zertifizierungsprogramm, mit dem die Fähigkeiten und

Kenntnisse von Fachleuten im Bereich Privilegge Access Management (PAM) validiert werden sollen. Cyberark ist ein führender Anbieter von PAM -Lösungen und hat dieses Zertifizierungsprogramm entwickelt, um sicherzustellen, dass Einzelpersonen über die erforderlichen Fähigkeiten verfügen, um privilegierte Konten und Zugang effektiv zu verwalten.

Um die CyberArk PAM-DEF Zertifizierung zu erhalten, müssen Kandidaten eine rigorose Prüfung bestehen, die ihr Verständnis von CyberArks PAM-Lösungen und ihre Fähigkeit, diese Lösungen effektiv zu implementieren und zu verwalten, misst. Die Prüfung ist darauf ausgelegt, das Wissen der Kandidaten über CyberArks Kern-PAM-Komponenten, wie die Privileged Access Security (PAS) Suite, den Enterprise Password Vault (EPV) und den Privileged Session Manager (PSM), sowie ihre Fähigkeit zu testen, diese Komponenten in verschiedenen IT-Umgebungen zu implementieren und zu konfigurieren.

CyberArk Defender - PAM PAM-DEF Prüfungsfragen mit Lösungen (Q68-Q73):

68. Frage
What is the purpose of the HeadStartInterval setting m a platform?

- A. It determines how far in advance audit data is collected tor reports
- B. It instructs the CPM to initiate the password change process X number of days before expiration.
- C. It instructs the AIM Provider to 'skip the cache' during the defined time period
- D. It alerts users of upcoming password changes x number of days before expiration.

Antwort: B

Begründung:
Explanation
The purpose of the HeadStartInterval setting in a platform is to instruct the CPM to initiate the password change process X number of days before expiration. This setting is used when the platform has the One Time Password feature enabled, which means that the passwords are changed every time they are retrieved by a user. The HeadStartInterval setting defines the number of days before the password expires (according to the ExpirationPeriod parameter) that the CPM will start the password change process. This gives the CPM enough time to change the password before it becomes invalid, and ensures that the user will always receive a valid password when they request it1. The HeadStartInterval setting can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 0, which means that the CPM will start the password change process on the same day as the password expiration date1.
The other options are not the purpose of the HeadStartInterval setting in a platform:
* A. It determines how far in advance audit data is collected for reports. This option is not related to the HeadStartInterval setting, which does not affect the audit data collection or reporting. The audit data is collected by the Vault server and stored in the Audit database, and the reports are generated by the PVWA or the PrivateArk Client based on the audit data2.
* C. It instructs the AIM Provider to 'skip the cache' during the defined time period. This option is not related to the HeadStartInterval setting, which does not affect the AIM Provider or the cache mechanism. The AIM Provider is a component that enables applications to securely retrieve credentials from the Vault without requiring human intervention. The cache mechanism is a feature that allows the AIM Provider to store credentials locally for a limited time, in case of a temporary network failure or Vault unavailability3.
* D. It alerts users of upcoming password changes x number of days before expiration. This option is not related to the HeadStartInterval setting, which does not alert users of anything. The HeadStartInterval setting only instructs the CPM to initiate the password change process, not to notify the users. The users
* do not need to be aware of the password changes, as they are performed automatically by the CPM and do not affect the user experience1. References:
* 1: Privileged Account Management, Min Validity Period subsection
* 2: Reports and Audits
* 3: Application Identity Manager

69. Frage
A password compliance audit found:
1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.
What should you do to address these findings?

- A. Edit safe properties and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".

- B. Edit the Master Policy and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
- C. Edit CPM Settings and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
- D. Contact the Windows Administrators and request them to add two policy exceptions at Active Directory Level: enable "Enforce one-time password access", enable "Record and save session activity".

Antwort: B

Begründung:
Explanation
To address the findings of the password compliance audit, you should edit the Master Policy in CyberArk Privileged Access Manager. The Master Policy is where you can enforce one-time password access and record session activity. One-time password access ensures that each password is used only once and then changed, which is a security measure to prevent unauthorized reuse of passwords1. Recording session activity is a feature of the Privileged Session Manager (PSM) that allows all activities during a session to be recorded for auditing purposes2. By enabling these settings in the Master Policy, you ensure that the domain accounts have one-time password access enforced and that all sessions connecting to domain controllers are recorded by CyberArk PSM.
References:
* CyberArk Docs: One-time passwords and exclusive accounts1

70. Frage
Your organization has a requirement to allow users to "check out passwords" and connect to targets with the same account through the PSM.
What needs to be configured in the Master policy to ensure this will happen?

- A. Enforce check-in/check-out exclusive access = inactive; Record and save session activity = active
- B. Enforce check-in/check-out exclusive access = active; Record and save session activity = inactive
- C. Enforce check-in/check-out exclusive access = active; Require privileged session monitoring and isolation = active
- D. Enforce check-in/check-out exclusive access = inactive; Require privileged session monitoring and isolation = inactive

Antwort: A

71. Frage
When running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

- A. List Accounts, Access Safe without confirmation
- B. List Accounts, View Safe Members
- C. Manage Safe Owners
- D. Manage Safe, View Audit

Antwort: B

Begründung:
Explanation
The Privileged Accounts Inventory Report provides information about all the privileged accounts in the system, based on different filters, such as safe, platform, policy, and owner. To run this report through the Reports page in PVWA on a specific safe, the user needs to have the following permissions on that safe:
* List Accounts: This permission allows the user to view the accounts in the safe and their properties, such as name, address, platform, and policy.
* View Safe Members: This permission allows the user to view the members of the safe and their authorizations, such as owners, users, and groups.
These permissions are required to show complete account inventory information for the specific safe. Other permissions, such as Manage Safe Owners, Access Safe without confirmation, Manage Safe, and View Audit, are not relevant for this report.
References: Reports and Audits - CyberArk, Safe Member Authorizations

72. Frage

You want to create a new onboarding rule.
Where do you accomplish this?

- A. In PVWA, click Reports > Unmanaged Accounts > Rules
- B. In PVWA, click Options > Platform Management > Onboarding Rules
- C. In PrivateArk, click Tools > Onboarding Rules
- D. In PVWA, click Accounts > Onboarding Rules

Antwort: D

73. Frage
.....