By OnlineInterviewQuestions.com

CyberArk is a company providing information security to organizations. The company offers Security to Privileged Accounts to many sectors which includes healthcare, government markets, and many other sectors. Viewfinity is used by CyberArk to enhance the measures of security. It lets the unrecognized applications to function in a safe mode so that it stays secure and protected from being infiltrated through malignant applications. One of the elements of the CyberArk's security solutions is CyberArk's primary function of privileged accounts. It uses PIM (Privileged Identity Management) for security purposes and to monitor the accounts of superusers in the CyberArk. It keeps an eye on whether a superuser account is safe or is it being used incorrectly by intruders and takes care of the account's security.

While preparing for an interview, you will have to be thorough with various **CyberArk Interview Questions** that an interviewer may throw to you instantly and you are supposed to answer on the spot quickly. Do prepare these answers sincerely in order to achieve success in CyberArk Interview. Some important CyberArk Interview Questions have been gathered in order to help you succeed in the interview with CyberArk. These questions have been hand-picked so that they help you to get through the CyberArk Interview. So you do not want to miss any of these questions of the CyberArk interview.

Q1. What do you understand by CyberArk?

CyberArk is a company that provides information security. It has more than half of fortune 500 in its customer's list. The headquarter of CyberArk is in Petah Tikva, Israel and headquarter of US is situated in Newton, Massachusetts. The company offers Privileged Account Security to various sectors including healthcare, energy sector, retail services, and government markets sector.

Q2. Explain the working of CyberArk Security?

For the highest security of the content, many encryption layers are issued to each safe by CyberArk Digital Vault. This is also referred to as EPV (Enterprise Password Vault). These keys which are safely encrypted are then kept in the vault for storage. These are encrypted again with some other vault encryption key that too be unique. A person with proper rights to access is given all these keys. A supervisor is appointed by the administrator for safety and the supervisor is the person whom the user has to manually confirm for accessing the safe and to the content of the safe.

Q3. . What is Privileged Session Manager?

Privileged Session Manager, also usually known by its abbreviation form PSM is CyberArk's key module. Privileged Session Manager (PSM) is responsible for the security of the access of all privileged users and its activities at database and OS platforms. Also, take note of the privileged users' access to the mainframe sites. Private Session Manager allows an only single point of control to access. It counts each keystroke and also does

count each mouse click and take high notice to not let any malware to access entry to the target system.

Q4. What is CyberArk Viewfinity?

Viewfinity is the EPM (Endpoint Privilege Manager) of CyberArk having enhanced safety measures. CyberArk Viewfinity allows the institution to enforce the least policies of privilege for the administrators of the system and business, elevating the privileges for running the authorized applications. This helps the servers to get prevented from accidental damages and also reduces the segregate duties of administrative on servers. The environment gets secured from being infiltrated through malignant applications by letting unrecognized application to function separately in safe mode.

Q5. What does a privileged user mean?

A privileged user has few better benefits over other uses. Any system's privileged user has significantly more potential in that system and these potentials are larger than those allotted to most of the other users. This privileged user's accounts are more prone to be hacked. Their accounts are slightly overlooked which expose them to big risks. It’s very simple for hackers to access these attack points for intensifying privileged access into the institution. System administrator itself uses the account of privilege to make changes with different other applications and databases. These accounts are also used to correspond with other services of the web and are at risk of being manipulated by the intruders.

Q6. Tell something about Identity and Privilege management?

Privileged Identity Management is often known by PIM which is its abbreviated form. It is used for the protection of accounts of super users. It supervises these accounts from an IT perspective. PIM keeps track that these accounts’ ability to access does not get used incorrectly. It uses the power of supervising to ensure that intruders don’t misuse or abuse the accessibility of the super user’s account.

Q7. What is meant by PrivateArk Client?

PrivateArk client is an application of Windows. It is a standard application used for the solution of PAS as the administrative client. The client can enter to the Enterprise Password Vault through internet by deploying the client to many remote computers. Safes are created using this interface and users also define a hierarchy of vault. A user should be validated from Digital vault in order to access the Enterprise Password Vault using PrivateArk client.

Q8. What do you understand by CPM?

The CPM is the abbreviation to the term ' Central Policy Manager '. Central Policy Manager enforces the

security policies without the need for human interaction. It does so by changing the remote machine's password and then stores the fresh password code in EPV (Enterprise Password Vault) under root 3 basis. The master policy of the institution confirms the password created by the CPM. Open the password is going to be expired or if the password has expired, then administrators are informed through PVWA. CPM is capable of creating new passwords on remote machines aimlessly and then the new password gets saved on the Enterprise Password Vault by replacing old password by this new one.

Q9. What are CyberArk's primary functions?

CyberArk EPV, also known as CyberArk Enterprise Password Vault is developed for controlling very secret passwords which are used for accessing the system throughout the institution in its environment of IT. CyberArk's primary function is structured by CyberArk EPV. It is one of the elements of the CyberArk's security solution of the privileged account.

Q10. What do you know about BYOC?

BYOC is an abbreviation to the term ' Bring Your Own Computer '. This term is used in the gaming culture by gamers during a gaming event involving multiple players. Players are needed to bring the computer of their own in order to take part in that event of gaming and then gamers hook their computing device to the network for participating. If PSM it is enabled then any client can be used for accessing the target system. This concept is also used in the corporates where employees are given permission to bring their own personal devices of computing at the workplace and use it for performing some tasks of their job. BYOC is helpful as it has the potential to eliminate the requirement of in-office computing devices hence helping to decrease the expense of any institution.

Q11. What do you understand by CyberArk endpoint Privilege Manager?

The Endpoint privilege manager of CyberArk helps to protect the institution by preventing the attacks that occur at the endpoint. This decreases the threat of stealing the content in any manner. CyberArk hosts this manager and also aids to remove the obstructions to enforce the least privilege.

Q12. What is PIM?

PIM is the abbreviated version for 'Privileged Identity Management'. It is used for the security and to monitor the superuser accounts in the CyberArk. PIM is used to analyze that the superuser accounts does not get misused. It is very important to supervise the accounts so that intruders are unable to use these accounts for ill purposes.

Some steps have to be followed in order to implement the Privileged Identity Management (PIM).

- First, a policy needs to be created to specify the management of the accounts of superusers. Along with this, it should be made specified the controls that account holder should have access and those controls which they won't be able to access.
- Second, a management model needs to be developed in order to make sure that the policies are followed by identifying an accountable party.
- Third, the extensiveness of the population and their identification to be identified by Inventory privileged accounts.
- Fourth and last but equally important step is to invent the tools and processes for managing the accounts.

PIM is important because the superuser accounts that are unmanaged are prone to losses and have a threat to the theft of sensitive information.

Q13. What factors need to be enabled for the policy of auto password reconciliation?

Password reconciliation for a specific or particular policy should be enabled in CyberArk for the auto password reconciliation policy. Along with this the automatic password verification also needs to be enabled. The additional account also is enabled having the required right on the target server. When the password gets unsynchronized then password reconciliation to be enabled.

Q14. What do you understand by the web form capability of CyberArk PSM?

The webform capability of CyberArk PSM means that web-based apps integrated the PSM connector in itself. The integration happens with a bunch of conditions. Web capability of PSM includes the login to HTML page using the form id along with the input form that is used for the password.

Q15. What steps have to be followed for registering a privileged account with help of PVWA to CyberArk PISM?

The following steps need to be followed for the purpose of registration to a privileged account :

Steps	What to do
Initiate a safe	Create a safe and define the holder of the safe
Generate a PIN	Generate a PIM policy
Generate policy	Now,generate the policy of CPM and PSM.
Add your Account	The finally aad the account with the properties such as its password,username and password

Q16. What do you mean by identity and access management?

Identity management or what is called identity and access management is responsible for maintaining the system that the right person gets the correct approach to right technology's resource for a specific correct reason at the particular correct time. Identity management is the discipline of protection and business in the security of

the computer system.

Q17. How many numbers of times can we access the count of the wrong password at the highest?

Not more than 99 times.

Q18. Can the password be changed in a text file in CyberArk?

Yes. If the password is the plaintext or is encrypted, then with the help of the encrypted algorithm the password may be changed.

Q19. What is the full form of OPM with reference to CyberArk?

OPM is an abbreviation and its full form is 'On-Demand Privileges Manager'. CyberArk On-Demand Privileges Manager is available for both Unix/Linux as well as for the Windows. Users are allowed to be limited to commands with access that is transparent from the definitions of the flexible policy of On-Demand Privileges Manager.

Q20. Which user directories does the CyberArk support?

Active Directory and IBM Tivoli DS are the user directories that are supported by the CyberArk. Other user directories supported by CyberArk include the Oracle Internet Directory and Novell eDirectory is also supported by CyberArk.