**1. Pre-Installation Preparation:**

* **Assessment**: Conduct a thorough assessment of your organization's IT infrastructure to understand the scope and requirements for device discovery and account onboarding.
* **Hardware and Software Requirements**: Ensure that your infrastructure meets the hardware and software prerequisites for CyberArk.

**2. Installation of CyberArk Components:**

* **Install CyberArk Privileged Access Security Solution**: Deploy the necessary CyberArk components, including the Vault Server, Central Policy Manager, and components for Device Discovery and Account Onboarding.

**3. Device Discovery Configuration:**

* **Discoverable Assets Identification**: Identify the assets (devices) that need to be discovered, including servers, endpoints, network devices, and cloud resources.
* **Configure Device Discovery Jobs**: Set up scheduled scans or continuous monitoring to discover devices. Configure parameters such as IP ranges, SNMP settings, WMI settings, and cloud service integration.
* **Integrate with Existing Data Sources**: Configure integration with data sources like Active Directory, network logs, and cloud service logs to enhance device discovery accuracy.
* **Alerting and Remediation**: Configure alerts for newly discovered devices and set up remediation workflows for any security issues identified during device discovery.

**4. Account Onboarding Configuration:**

* **Account Identification**: Identify the privileged accounts that need to be onboarded into CyberArk, including local accounts, service accounts, and domain accounts.
* **Configure Account Discovery Jobs**: Set up automated processes for discovering accounts on devices. This may involve credential scanning, integration with endpoint logs, and application logs.
* **Credential Rotation**: Implement automatic password rotation for onboarded accounts to enhance security.
* **Integration with SIEM**: Integrate account onboarding with your SIEM solution for real-time monitoring and alerting.
* **Account Usage and Access Reports**: Configure reports that provide insights into account usage and access patterns for compliance and security auditing.

**5. Testing and Validation:**

* **Testing**: Conduct thorough testing of the device discovery and account onboarding processes to ensure they work as expected.
* **Validation**: Validate the accuracy of discovered devices and onboarded accounts against your initial requirements.

**6. User Training and Documentation:**

* **Training**: Provide training to relevant personnel on how to use CyberArk for device discovery and account onboarding.
* **Documentation**: Prepare comprehensive documentation that includes installation guides, configuration guides, and troubleshooting procedures.

**7. Post-Installation Maintenance:**

* **Regular Updates**: Keep CyberArk components up to date with the latest patches and updates.
* **Ongoing Monitoring**: Continuously monitor the device discovery and account onboarding processes for any anomalies or issues.
* **Incident Response**: Develop an incident response plan in case of security incidents related to discovered devices or onboarded accounts.

**8. Compliance and Reporting:**

* **Generate Reports**: Regularly generate compliance reports to demonstrate adherence to regulatory requirements.
* **Audit Trails**: Maintain detailed audit trails of all activities related to device discovery and account onboarding.

**9. Review and Optimization:**

* **Periodic Reviews**: Conduct periodic reviews of the device discovery and account onboarding processes to optimize performance and security.

By following this approach and documenting each step thoroughly in your proposal document, you can provide a clear and comprehensive plan for implementing device discovery and account onboarding using CyberArk in your organization.

* Benefits of device discovery and account discovery:
  + Identify all the devices and accounts in the environment that need to be protected by CyberArk.
  + Identify all the accounts in the environment that need to be managed by CyberArk.
  + Generate reports on the security posture of the environment.
  + Categorize accounts based on their privileges and risks.
  + Help to ensure that all the devices and accounts in the environment are properly managed and protected.
  + Provide visibility into the security posture of the environment.
  + Help to identify and mitigate security risks.
* Approach to device discovery:
  + Use a variety of methods to discover devices, such as scanning network ranges, querying Active Directory, and polling asset management systems.
  + Run the discovery process on a regular basis, such as daily or weekly, to ensure that the inventory of devices is always up-to-date.
  + Review the results of the discovery process to identify any missing or misconfigured devices.
  + Take action to address any missing or misconfigured devices, such as adding them to the CyberArk vault or updating their configurations.
* Approach to account discovery:
  + Use a variety of methods to discover accounts, such as scanning for password files, querying databases, and monitoring privileged activity.
  + Run the discovery process on a regular basis, such as daily or weekly, to ensure that the inventory of accounts is always up-to-date.
  + Review the results of the discovery process to identify any missing or misconfigured accounts.
  + Take action to address any missing or misconfigured accounts, such as adding them to the CyberArk vault or updating their configurations.

Here are some additional considerations that may need to be taken into account when planning the device discovery and account discovery process:

* The size and complexity of the environment.
* The specific requirements for the discovery process.
* The availability of resources, such as time and personnel.
* The budget for the project.

It is important to carefully consider all of these factors when planning the device discovery and account discovery process in order to ensure a successful implementation.

I hope this helps! Let me know if you have any other questions.

| **Aspect** | **Device Discovery** | **Account Discovery** |
| --- | --- | --- |
| **Objective** | Identify and inventory all networked devices | Discover and onboard privileged accounts |
| **Step 1: Assessment** | Evaluate existing infrastructure and asset lists | Identify critical accounts and systems |
| **Step 2: Planning** | Define scope, goals, and desired outcomes | Determine discovery methods and frequency |
| **Step 3: Installation** | Deploy CyberArk components for device discovery | Set up account discovery mechanisms |
| **Step 4: Configuration** | Configure device scanning parameters | Define account discovery rules and policies |
| **Step 5: Integration** | Integrate with existing asset management systems | Integrate with directories, databases, and apps |
| **Step 6: Automation** | Schedule periodic device scans and updates | Automate account discovery and onboarding tasks |
| **Step 7: Monitoring** | Implement alerting for new or unauthorized devices | Monitor account usage and access patterns |
| **Step 8: Remediation** | Set up remediation workflows for security issues | Implement automatic password rotation |
| **Step 9: Reporting** | Generate device inventory reports | Create reports on account usage and compliance |
| **Step 10: Compliance** | Ensure compliance with regulatory requirements | Verify compliance with relevant standards |
| **Step 11: Training** | Provide training for staff on device discovery | Educate teams on account management best practices |
| **Step 12: Documentation** | Prepare documentation for device discovery | Document account discovery and onboarding processes |
| **Step 13: Testing** | Conduct testing and validation of device discovery | Validate account onboarding accuracy |
| **Step 14: Maintenance** | Maintain and update device discovery components | Regularly review and update account configurations |
| **Step 15: Optimization** | Optimize device discovery for efficiency and accuracy | Optimize account discovery for security and efficiency |
| **Step 16: Review** | Periodically review and adjust device discovery | Review account discovery processes and policies |