| | | | |
|---|---|---|---|
| Job Title: | CyberArk Privileged Access Management (PAM) Resource | Years of Experience: | 4-5 Year |
| Department | Technical | Position Type: | Full Time |
| Location: | Mumbai | | |
| Package: | 6-7LPA | | |

Job Description

**Position Overview**

We are seeking a skilled CyberArk Privileged Access Management (PAM) Resource to join our team. As a PAM Resource, you will be responsible for implementing, managing, and maintaining CyberArk's suite of PAM solutions within our organization. Your primary focus will be on safeguarding privileged accounts and credentials, ensuring the security and integrity of our critical assets.

**Responsibilities:**

1. **Implementation:** Deploy and configure CyberArk PAM solutions based on best practices and organizational requirements.
2. **Administration:** Manage and maintain CyberArk components, including the Vault, Central Policy Manager, Privileged Session Manager, and others.
3. **Policy Management:** Define and enforce policies for privileged account access, password rotation, and session monitoring.
4. **Integration:** Integrate CyberArk with existing IT infrastructure and security tools, such as SIEM, IAM, and ticketing systems.
5. **User Training:** Provide training and support to system administrators and end-users on CyberArk functionalities and best practices.
6. **Incident Response:** Assist in investigating and responding to security incidents related to privileged accounts and access.
7. **Documentation:** Maintain detailed documentation of configurations, procedures, and troubleshooting steps.
8. **Compliance:** Ensure compliance with relevant regulatory requirements and industry standards (e.g., PCI DSS, HIPAA, GDPR) related to privileged access management.
9. **Continuous Improvement:** Stay updated on the latest CyberArk features, patches, and security advisories. Implement improvements and optimizations to

enhance the effectiveness of PAM controls.

**Requirements:**

1. **Certification:** CyberArk Certified Defender (CCD) or CyberArk Certified Sentry (CCS) certification preferred.
2. **Technical Skills:**
    - Proficiency in deploying, configuring, and troubleshooting CyberArk components.
    - Solid understanding of privileged access management concepts and best practices.
    - Familiarity with LDAP, Active Directory, and other directory services.
    - Experience with scripting languages (e.g., PowerShell, Python) for automation tasks.
    - Knowledge of network protocols and security technologies (e.g., SSL/TLS, firewalls, IDS/IPS).
3. **Communication:** Excellent verbal and written communication skills, with the ability to explain technical concepts to non-technical stakeholders.
4. **Team Player:** Ability to collaborate effectively with cross-functional teams and adapt to changing priorities.
5. **Problem-Solving:** Strong analytical and troubleshooting skills, with a proactive approach to identifying and resolving issues.
6. **Additional:** Privileged Standard User SaaS Credential Protection, Session Isolation, Recording; Just in Time Access, Remote Access, Adaptive MFA, Adaptive SSO, Identity Security Intelligence
7. **Attention to Detail:** Meticulous attention to detail and adherence to security best practices.

**How to apply-**

Interested candidates are invited to submit their resume along with a cover letter detailing their relevant experience and motivation to **contact@pmspl.net**