Nagaraju Teppani

[nagarajuteppani365@gmail.com](mailto:nagarajuteppani365@gmail.com)  <https://linkedin.com/in/teppani-nagaraju-001ba6216>

Senior Cybersecurity/ CyberArk Consultant in Big4 firm with close to 9 years of expertise in Identity and Access Management, I have extensive experience working in IAM activities. My background includes proficiency in implementation and support of CyberArk Privileged Access Management (PAM), CyberArk CPC, Ping Identity solutions such as PingFederate, PingOne, and PingId for single sign-on, Microsoft EntraID.

**Technical Skills**

* CyberArk PSM, CPM, PVWA, PTA, CCP, CyberArk CPC, AWS IAM Users, Roles, Groups and Policies, Azure/EntraID, PingFederate, PingDirectory, PingOne, PingID, PingAccess, OKTA IAM, Splunk, New Relic, ServiceNow, Active Directory

**Certifications**

* CyberArk Defender and Sentry Certified
* CyberArk CDE Certified
* Certified Professional - PingFederate PFP-001
* SC-300: Microsoft Certified Identity and Access Administrator Associate

**EDUCATION**

**Osmania University** | *Bachelor of Engineering, Electronics and Communication Engineering* **Professional Experience**

**EY - GE Aerospace Jul 2024 - Mar 2025**

*Senior Security Consultant - PAM and SSO Lead Evendale, Ohio, U.S- Remote*

As a leader in aviation technology, GE Aerospace continues to design, develop and manufacture jet engines, components and integrated systems for military. As part of the GEA Managed Services Operations team lead, I led both the PAM CyberArk and Ping Identity SSO teams during the initial migration and transition phases. I successfully developed appropriate migration plans and assisted the client in various aspects, including scheduling calls, facilitating knowledge transfer, creating knowledge base articles and standard operating procedures, and aligning the team. Additionally, I contributed to the implementation of monitoring tools such as New Relic and Splunk.

* Spearheaded the conceptualization and initiation of a greenfield project, defining project scope, objectives, and deliverables in alignment with business goals.
* Developed comprehensive project plans that included timelines, resource allocation, and risk management strategies.
* Led multiple technologies like CyberArk, PingFederate and My Password and Fostered a collaborative environment that encouraged innovation and agile methodology for rapid iteration and continuous improvement.
* Maintained regular communication with stakeholders to gather requirements, provide updates, and incorporate feedback into the devel- opment process.
* Successfully launched the greenfield project on schedule, meeting all key performance indicators and business objectives.
* Created extensive documentation for the project, including technical specifications, user manuals, and maintenance guides.
* Conducted training sessions for end-users and support teams to ensure a smooth transition and adoption of the new system.
* Involved in almost all the transition and KT calls from client side.
* Prepared 50 + SOP documents, Operation Manual and RACI to ensure smooth operational activities.

**EY - GE Aerospace Jul 2024 - Mar 2025**

*CyberArk Lead Role Evendale, Ohio, U.S- Remote*

* Has experience in performing major version upgrades, minor version upgrades.
* Has experience in configuring CPM, PSM, secure tunnel, identity connector components for CyberArk privileged cloud.
* Has experience in SAN storage migration activity, troubleshooting HA cluster vaults, DR drill activities, component connectivity related issues.
* Experience in performing POCs with CyberArk CEM, PTA, Sphere technologies.
* Hands on experience in conducting audit meetings, engaging and gathering requirements from clients, stakeholders, and multiple teams.
* Has good knowledge on SailPoint, active directory, Service Now workflows, incident management, change management, developing SOPs, developing RCA.
* Implemented security enhancements and best practices to safeguard privileged accounts and sensitive data, reducing the risk of unautho- rized access.
* Experienced in performing integrations on SIEM and SNMP and PTA(POC).
* Knowledgeable in using Rest API scripts and experienced in automating accounts life cycle management, safe management, finding disabled EPV users in CyberArk etc.
* Experienced in SailPoint IIQ for role and entitlement creation, terminations, and managing accounts and security groups in AD via PowerShell Rest APIs.
* Conducted POCs to identify critical alerts through CyberArk PTA integration and onboard/manage cloud subscriptions with CyberArk Cloud Entitlement Manager.
* Managed and updated SOPs, Confluence, and JIRA dashboards.
* Skilled in gathering and managing weekly, monthly, quarterly, and annual reports.
* Has hands on experience in deploying CPM, PSM, Identity Connector, and Secure Tunnel in CyberArk privileged cloud.
* Has hands on experience in troubleshooting issues and executing test cases in CPC.

* Experienced in executing major version upgrade from V12.2 to V14.0, including high availability cluster vaults, standalone environments for CPM, PSM, PVWA.
* Has hands on experience in performing SAN storage migration.
* Has hands on experience in SCIM integration i.e., integrating CyberArk with IGA based solution using CyberArk identity administration as SCIM server.
* Extensive experience with numerous instances of conducting Disaster Recovery (DR) drills during maintenance activities.
* Provided technical support and troubleshooting high availability cluster vaults during outages, vault unavailability, node failures, PVWA unavailability, replication issues.
* Conducted periodic audits and assessments to ensure compliance with organizational security policies and standards, addressing any discrepancies promptly.

**EY - ASIAN DEVELOPMENT BANK Dec 2021 - Jul 2024**

*Security Consultant Metro Manila - Remote*

The Asian Development Bank (ADB) is a regional development bank to promote social and economic development in Asia. The bank is headquartered in Metro Manila, Philippines and maintains 31 field offices around the world. As a Security Consultant, I serve as the sole resource for clients in onboarding various user accounts, including Linux, Windows, and network accounts. My responsibilities include generating daily inventory reports and troubleshooting issues by analyzing error codes from these reports. I have developed connectors using AutoIT scripts and web form fields, as well as numerous Microsoft connectors. Additionally, I have been involved in the successful patching and upgrades of all components, such as PSM, PVWA, and CPM. I also performed vault failover as part of functional testing and created several standard operating procedures (SOPs) and knowledge base (KB) articles addressing the issues encountered.

* Creating and managing of Safes, Platforms and Applications.
* Creating custom connectors and web connection components.
* Involved in CyberArk PAM components (CPM, PSM, PVWA and Vaults) upgradation from one version to other versions.
* Worked on DR failover issues and vault clustering.
* Preparing the progress documents for each procedure and related to any new error and procedures.
* Enrolling and Unenrolling the network devices, operating system accounts in PVWA.
* Generating failed account report from PVWA daily and processing the report.
* Checking the system health and updating it to client.
* Checking the replication of DR servers daily.
* Involved in monthly patching activities for all the PAM components.
* Providing 24/7 support as per the company requirements.
* Experience in troubleshooting CyberArk vaulting and password rotation issues.
* Excellent troubleshooting skill on PVWA, Vault, CPM, PSM, and user suspend issues, account lock issues, Network & Authentication issues.
* Processing Service now requests for User Administration.
* Managing day to day Security Operation task, CPM Plugin issues, troubleshooting and resolving the user issues.
* Working with direct CyberArk Engineers for challenging issues within the environment.
* Removing the decommissioned server related accounts from CyberArk.

**EY- KENVUE Nov 2021 - Jul 2024**

*Senior Security Consultant New Jersey, USA- Remote*

Kenvue Inc. is an American consumer health company. Formerly the Consumer Healthcare division of Johnson & Johnson. As part of the Cyber Managed Services Team, I participated in the migration team responsible for transitioning from Ping Identity to Microsoft Entra. We successfully categorized and migrated numerous applications that were onboarded in Ping Identity to the Entra platform. I was involved in the onboarding of end-user applications to PingFederate by gathering the necessary metadata and implementing them initially in the test, QA, and production environments following successful testing. These applications utilize SAML and OAuth protocols for integration. After the onboarding process, I addressed issues arising from Snow tasks and incidents, employing tools such as SAML Tracer, logging, and Postman for troubleshooting. Additionally, I upgraded the PingFederate instance.

* Configure and manage SSO integrations with various applications using Microsoft Entra Identity and Ping Identity.
* Set up and maintain trust relationships between the identity provider (IdP) and service providers (SPs).
* Implement and maintain authentication policies and methods, such as multi-factor authentication (MFA) to enhance security.
* Troubleshoot authentication issues and provide timely resolutions to ensure minimal disruption to users.
* Define and enforce access control policies to ensure that users have appropriate access to resources.
* Manage group memberships, roles, and permissions within Microsoft Entra Identity.
* Oversee the synchronization of user accounts and groups between on-premises directories (like Active Directory) and Microsoft Entra Identity.
* Monitor synchronization logs and resolve any synchronization conflicts or errors.
* Work with application teams to onboard new applications to the SSO ecosystem.
* Ensure that application integrations comply with security standards and best practices.
* Automate and manage user lifecycle processes, including provisioning, updates, and deprovisioning of user accounts.
* Monitor for and respond to security incidents related to SSO and identity management.
* Ensure compliance with regulatory requirements and internal policies regarding identity and access management.
* Generate reports on SSO usage, access reviews, and compliance audits.
* Conduct regular access reviews and recertification campaigns to maintain the principle of least privilege.
* Provide support to end-users experiencing issues with SSO and access to applications.
* Stay up to date with the latest Microsoft Entra Identity features and updates.
* Connecting with third-party vendors and service providers to resolve any SSO-related issues.
* Maintain detailed documentation of the SSO configurations, policies, and procedures.
* Document any changes to the SSO environment in a change management system.

**CapGemini - CSL Behring Aug 2018 - Nov 2021**

*Security Consultant Pennsylvania, USA*

CSL Behring is a biopharmaceutical company, manufacturing plasma-derived and recombinant therapeutic products. As a Security consul- tant, I was involved in the onboarding of end-user applications to PingFederate by gathering the necessary metadata and implementing them initially in the test, QA, and production environments following successful testing. These applications utilize SAML and OAuth protocols for integration. After the onboarding process, I addressed issues arising from Snow tasks and incidents, employing tools such as SAML Tracer, logging, and Postman for troubleshooting. Additionally, I upgraded the PingFederate instance from version 9 to version 10.

* Designing and implementing applications integration with Ping Federate/ PingOne in both Non-Production and Production. Working with application's business and technical teams to gather requirement to integrate application with Ping Federate/ PingOne for Single Sign On.
* Exporting Metadata, creating Adapters, Service Provider connections, Identity Provider connections, replicating configuration archive, importing and exporting SSL certificates using Ping Federate.
* Onboarded Applications on Ping Federate, PingOne and Microsoft Entra using SAML, Oauth and OIDC protocols.
* Troubleshooting all the Ping ID related issues such as device mapping in PingOne, MFA.
* Ability to adapt the different environments.
* Supported development with integration of Mobile Apps using OAuth/SAML in Ping Federate.
* Excellent communication skills and working on with SAML Tracer, Server log files for trouble shooting the error from client end.
* Modifying existing integrations as per the request from application teams.
* Implemented open ID and OAuth solutions using Ping Federate.
* Handled certificate deployment (renewal) for around 100 applications which are already on boarded in Ping Federate.
* Upgraded PingFederate version from 10. To 11. Version in Linux environment.
* Created SOP for upgrade activities and many other operational activities.
* Provide L2/L3 Support and meeting SLA for the Federation issues reported by Application team and customers.
* Co-ordination with Ping Federate vendor if any software related issues.
* Maintained both Test and Production servers for Ping Federate along with the cluster management and timely Replications to deploy changes to servers.
* Responsible for preparing documentation for each application and providing the Run Book to the Operations team to troubleshoot issues.
* Was an integral part of the 24/7 On-call team for troubleshooting outages/ issues.
* Strong analytical, problem solving and communication skills.

**CapGemini - Smith & Nephew (SNI) Nov 2016 - Aug 2018**

*Staff Security Consultant Watford, England*

Smith & Nephew plc, also known as Smith+Nephew, is a British multinational medical equipment manufacturing company headquartered in Watford, England. As a Staff Security Consultant, I was involved in the manual and automated onboarding and offboarding of users, utilizing PowerShell scripts. This included the creation of shared mailboxes, managing access to security groups, and generating email accounts through the Exchange server. Additionally, I established security groups and distribution lists, while also managing access permissions and restrictions at the group level.

* Creation, modification, deletion of user accounts in active directory.
* Granting permission and managing access through security groups to support the business.
* Creation, modification and deletion of Generic mailbox, Generic id's, Distribution list.
* Granting permissions to folders, mailboxes and distribution lists.
* User Management in Active Directory (Account unlocking, password resets).
* Administration of user accounts and groups on AD.
* Assignment of work to team and sending daily report to Management.
* Managing Active Directory on Windows Server 2008/2012.
* Managing a complete Service Now (SNOW) queue where a ticket is raised in case the request raised has not fixed the issue.
* Working on Tasks and Incidents on Daily IAM Activities on ID creation, modification and deletion.
* Managing complete Remedy queue where a BMC remedy ticket is raised in case the request raised has not fixed the issue.
* Creation, amendment of the accounts with the specific accesses as per the security guidelines suggested on Active Directory.
* Creating and deleting IDs in AD. Maintaining user accounts in AD.
* Amendment with group policies and user management.
* Mailbox/distribution list creation, deletion on Exchange Server.
* Granting shared drive access.
* Provide 24\*7 supports.
* Troubleshooting user problems using remote administering/viewing tools.
* Creating and Managing Organizational Units within AD.
* Working on daily incidents based on monitoring and access related issues.