Introduction

all my experience is in cyber security, Identity, and access management domain. As part of my experience, I have worked on different subdomains; I have worked on different access management tools like Ping Federate, Okta implementing single sign On and multifactor authentication.

Then I have experience working on protocols like SAML, OAuth and OpenID.

I have also worked on Ping One Risk that takes authentication and authorization

decisions based on context. I have also worked on FIDO for password less authentication.

Further I have experience in privileged access management as well, where I have worked with products like Thycotic Secret Server and CyberArk. So over here, I've done discovery and governance of privileged accounts, endpoint security, password rotation capabilities, session management, implementation of vault and Privileged threat Analytics.

As part of my CyberArk Experience. I have worked on components like Digital Vault, PVWA, Central Policy Manager, Privileged Session Manager, and Privileged Session Manager for SSH. On-Demand Privileges Manager and Privileged Threat Analytics.

The mainstay of my profile is Identity Governance and administration IGA,

where primarily I have worked with SailPoint identity IQ. So, coming to identity IQ, I have worked on different versions starting with 6.4, 7.0 and 8.0 series as well. Currently I am working on version 8.3. I've worked on installation of the product into client environments, worked on upgrade projects, and upgraded SailPoint from 8.1 to 8.3. I have experience with patching identity IQ solutions; I have been part of migration projects as well, migrating from a different tool to SailPoint identity IQ.

Further I have experience working on application onboarding. Have worked on different types of applications like HR Applications PeopleSoft/Workday, delimited file, JDBC, Directories like LDAP Active Directory, Azure AD, SAP, and Oracle connectors. I have also experience with Webservices and SCIM integration with CyberArk.

Further I have also worked on Compliance modules like Policy where I’ve worked on Compliance standards like SOX, HIPAA, and GDPR.

So, implementation of separation of duties policies for identifying toxic combinations at role and entitlement level. I have worked on implementation of risk framework,

identity level risk and application-level risk. Idea was to divide identities into risk bands and move from Traditional to risk-based certifications.

I also Worked on the certification framework. So, a lot of access in the enterprise was controlled through Active Directory groups. So, I have worked on certifying their membership and composition,

working on application owner, manager, and Entitlement owner access reviews.

Further I have experience working on roles implementing role-based access control, designing the two-tier role model,

wherein we have business roles, IT roles and Entitlement analysis. So, I was working on a mining framework business role mining IT role mining and entitlement analysis.

Further, I have worked on lifecycle events like Joiner Mover Leaver framework automaton.

Experience working on LCM workflows, custom workflows, birthright provisioning using roles, hybrid provisioning.

So, this briefly covers my overall experience on identity and access management.