SOLOMON AJAEZI

me@solomonajaezi.com | (214) 861-8023 | Houston, TX

Summary

Senior IAM Engineer with 8+ years of experience in healthcare, tech, and oil & gas, specializing in identity lifecycle management, SSO/Federation, PAM, IGA tools, and cloud IAM controls (AWS, Azure, GCP). Proven ability to resolve real-world IAM issues such as access failures, privilege escalations, joiner/leaver processes, and audit remediation. Hands-on expertise with Okta, SailPoint, ForgeRock, CyberArk, Azure AD, LDAP, SCIM, SAML, and OAuth2. Combines IAM expertise with security operations, DevOps automation mindset, and engineering mindset.

Skills

- **Identity Lifecycle & Federation:** Joiner/Leaver/Transfer, SCIM, SSO (SAML, OIDC, OAuth2), MFA, Conditional Access
- **IAM & Access Control:** Azure AD, Okta, ForgeRock, SailPoint IIQ, Auth0, RBAC, PIM, PKI
- **Privileged Access & PAM**: CyberArk, Delinea, Just-in-Time Access, Session Monitoring
- **Cloud & Directory Services:** AWS IAM, Azure IAM, GCP IAM, Active Directory, LDAP
- **Infrastructure & Automation:** Terraform, Ansible, PowerShell, Azure CLI, AWS CLI, Okta Workflows
- **DevOps & Secrets Management:** Git, GitLab CI/CD, Jenkins, Docker, Kubernetes, HashiCorp Vault
- **Security Monitoring & Frameworks:** Splunk, ServiceNow, Audit Logs, Zero Trust Architecture (ZTA)

Experience

Cloud IAM Engineer ***July 2022—Present***
Luxer One ***Sacramento, CA***

- Provision and de-provision users across hybrid environment using SCIM between Azure AD, Okta, and internal HRIS.
- Configure and manage SAML SSO integrations for enterprise apps including Salesforce, Workday, and Jira.
- Enforced RBAC via Azure AD and Conditional Access; handled MFA rollout including FIDO2 device testing.
- Responded to access issues (user unable to authenticate via Okta), reviewed SAML assertion logs, and worked with app owners to resolve metadata mismatches.
- Conducted access reviews and user certification campaigns through SailPoint and submitted SoD exceptions for review.
- Supported PAM workflows in CyberArk: password vault onboarding, privileged session monitoring, and break-glass account access.
- Automated provisioning pipelines using Terraform to define IAM roles and policies across dev, test, and prod environments.
- Leveraged Ansible for role-based configuration enforcement and repeatable deployment of access policies.

IAM Engineer ***Dec 2019—July 2022***
Cisco ***Austin, TX***

- Managed IAM tickets related to on-boarding, off-boarding, and entitlement changes across 20+ SaaS applications.
- Integrated 10+ applications with Okta using SAML and OIDC protocols, working closely with application teams.
- Automated user access provisioning using Okta Workflows and integrated SCIM connectors.
- Participated in LDAP integration between ForgeRock and backend databases to support internal legacy apps.
- Resolved user lockout incidents, MFA enrollment issues, and stale account discovery with PowerShell scripts.
- Used Docker and Kubernetes RBAC to control IAM roles for internal services and API interactions.
- Integrated GitLab CI with IAM systems to enforce secure deployment pipelines and rotate secrets via environment variables.
- Managed IAM scripting tasks using AWS CLI and Azure CLI to validate access rights, rotate credentials, and pull audit reports.
- Designed and enforced Conditional Access and MFA policies in Azure AD and Okta, aligned with Zero Trust Architecture principles (least privilege, verified trust, and continuous evaluation.)
- Partnered with audit/compliance teams to support quarterly access certifications and remediation via SailPoint.

Cloud Security Engineer (IAM Focus) ***April 2018—Dec 2019***
Elevance Health ***Waukesha, WI***

- Worked across DevSecOps and IAM to harden identity security posture within Azure and AWS environments.
- Created and maintained RBAC policies in Azure AD to enforce least privilege access across engineering teams.
- Deployed Conditional Access policies blocking legacy protocols and enforcing MFA for privileged users.
- Supported PAM deployments using Delinea Secret Server; managed onboarding of local/admin accounts.
- Handled high-volume ServiceNow tickets related to terminated employees with lingering access or orphaned accounts.
- Assisted in PKI rollout to enforce certificate-based authentication for developers accessing CI/CD pipelines.
- Contributed to access automation using GitHub Actions for joiner/mover/leaver workflows and service account governance.
- Leveraged Splunk dashboards to audit IAM events (login failures, PIM activations, access reviews) and respond to ServiceNow security tickets in compliance with SLA timelines.

Reliability Engineer *Sep 2013—Aug 2017*
Shell Oil *Abu Dhabi, UAE*

- Led disaster recovery strategy development and implemented resilient cloud backup workflows.
- Partnered with cross-functional teams to define secure provisioning patterns for oilfield tech infrastructure.
- Introduced incident response SOPs and root-cause tracking for field equipment anomalies.
- Acted as liaison between field users and IT security to triage mobile access issues, helping align device access trust policies and identity compliance requirements for secure operational app access.
- Collaborated with IT to document authentication flows for refinery monitoring systems, mapping Okta SSO integrations with on-prem LDAP and Active Directory for seamless access control.
- Managed a cross-functional team of 8 to solve complex reliability issues, utilizing strong leadership and communication skills to drive problem-solving across departments

Education & Certification

- **Amazon Web Services (AWS)**: Certified Developer Associate (DVA-C01), Aug 2022
- **Scrum.org**: Professional Scrum Master, Sep 2022
- **University of Texas**, Tyler, TX: Master of Science, Industrial Engineering Management, Dec 2012

Additional Information

- U.S. Citizen, eligible for Public Trust & Secret Clearance
- Proficient in ITIL processes and Lean Six Sigma Methodologies