CHIDI AJAEZI

me@chidiajaezi.com | (214) 861-8023 | www.chidiajaezi.com | linkedin.com/in/chidiajaezi

Summary

IAM Engineer with 9 years of experience in healthcare, tech, and oil & gas, specializing in enterprise identity lifecycle management, SSO/Federation, PAM, and cloud IAM controls. Expertise in designing Zero Trust architectures using Okta, Entra ID, AWS IAM, and CyberArk to enable secure, compliant access at scale. Proven track record of resolving complex IAM challenges, such as access failures, privilege escalations, and audit remediation, while automating processes to streamline operations in hybrid environments.

Skills

- **Identity Lifecycle & Federation:** Joiner/Leaver/Transfer, SCIM, SSO (SAML, OIDC, OAuth2), MFA, Conditional Access
- **IAM & Access Control:** Okta (Lifecycle, Workflows, Access Gateway), Entra ID, CyberArk, AWS IAM, RBAC, PIM, PKI
- **Zero Trust Architecture:** Least Privilege, Verified Trust, Continuous Evaluation
- **Automation & Infrastructure:** Terraform, Ansible, Docker, PowerShell, Python, REST API, Git, GitHub, CI/CD
- **Security Monitoring & Frameworks:** Splunk, WIZ, Audit Logs, SOC 2, HIPAA, PCI-DSS, NIST 800-53

Experience

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

- Designed and implemented Zero Trust IAM architectures using Okta and Entra ID, enabling secure access for 500+ users across hybrid cloud environments while reducing unauthorized access incidents by almost 40%.
- Configured SAML and OIDC SSO for enterprise, incorporating adaptive MFA and conditional access to enforce least privilege principles.
- Provisioned and de-provision users via SCIM integration between Entra ID, Okta, and internal HRIS, automating lifecycle management and ensuring compliance with SOC 2 audits.
- Led PAM initiatives with CyberArk, onboarding password vaults and session monitoring for privileged accounts, mitigating escalation risks in production environments.
- Automated IAM workflows using Terraform and Python scripts, integrating Okta Workflows and API calls to onboard users across dev, test, and prod, cutting deployment time drastically.
- Supported access troubleshooting, analyzing SAML logs to resolve metadata mismatches and user authentication failures, maintaining 99.9% uptime for critical systems.
- Enforced RBAC and PIM in AWS IAM and Entra ID, conducting quarterly access reviews and remediating SoD violations to meet PCI-DSS standards.

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

- Managed IAM operations for 1,000+ users, handling onboarding, offboarding, and entitlement changes across 20+ SaaS applications with Okta and Entra ID, focusing on Zero Trust enforcement.
- Integrated applications with Okta using SAML and OIDC, collaborating with app teams to implement MFA and Conditional Access, reducing phishing-related incidents by 50%.
- Automated user provisioning with Okta Workflows and Beanshell scripts, syncing identity events in real-time and minimizing manual errors in hybrid environments.
- Resolved lockout and MFA enrollment issues using PowerShell and API tools, restoring access for critical users while analyzing logs for root causes.
- Supported LDAP integrations with CyberArk for legacy apps, implementing just-in-time privilege elevation to align with Zero Trust models.
- Developed CI/CD pipelines with GitLab and Terraform, enforcing secure IAM roles for Docker/Kubernetes deployments and rotating secrets via HashiCorp Vault.

IAM Security Engineer *April 2018—Dec 2019*
Elevance Health *Waukesha, WI*

- Created and maintained RBAC policies enforcing least privilege access for 300+ engineering users, reducing excessive permissions.
- Deployed Conditional Access policies blocking legacy authentication protocols and enforcing MFA for privileged users.
- Processed 1,000+ ServiceNow tickets for terminated employee access removal and orphaned account cleanup, maintaining HIPAA compliance.
- Supported PKI rollout for developer access to CI/CD pipelines, improving authentication security.
- Built GitHub Actions workflows for joiner/mover/leaver processes and used Splunk dashboards for IAM event monitoring and incident response.

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

- Supported identity infrastructure for global oil & gas operations across multiple countries.
- Collaborated with IT security to establish device trust policies and identity compliance for field workers accessing operational applications.
- Documented and implemented Okta SSO integrations with on-premises LDAP/Active Directory for refinery monitoring systems.
- Managed team of 8 engineers to resolve complex identity and access issues affecting critical operational systems.
- Developed identity system backup and recovery procedures ensuring business continuity for mission-critical applications.

Education

- **University of Texas**, Tyler, TX: Master of Science, Industrial Engineering Management, Dec 2012
- **University of Benin**, Edo, Nigeria: Bachelor of Science, Mechanical Engineering, July 2008

Certification

- **Amazon Web Services (AWS)**: Certified Developer Associate (DVA-C01), Aug 2022
- **Scrum.org**: Professional Scrum Master, Sep 2022

Additional Information

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