SOV SAM

(240)764-9619 • SovSam@outlook.com • Linkedin.com/in/SovSam

PROFESSIONAL SUMMARY

IAM/ICAM professional with 4+ years supporting Department of Veterans Affairs (VA) and enterprise environments. Experienced in identity lifecycle management, provisioning, access governance, RBAC, MFA, SAML/OIDC SSO, REST APIs, enterprise integrations, and IAM troubleshooting. Hands-on experience with Saviynt, Active Directory, Okta, PingID, and ServiceNow, with familiarity in NIST RMF and Zero Trust principles. Security+ certified (DoD 8140 IAT Level II) with an active Tier 4 Public Trust.

CORE SKILLS:

Identity Lifecycle & Governance: Provisioning/deprovisioning, access governance, joiner-mover-leaver workflows, access request and approval workflows, RBAC concepts
Integration & Federation: Enterprise application onboarding and integration, VA MPI integrations, REST API, SAML/OIDC SSO (supported configuration and testing), requirements gathering with application owners
Directory & Authentication: Active Directory, authentication/authorization concepts, MFA, access controls
Operations & Troubleshooting: Tier 1-3 incident triage and resolution, identity-related incident troubleshooting
Documentation & Testing: SOPs, escalation procedures, integration design documentation (ISDD), test plans, manual test case creation/execution, audit-ready documentation
Tools & Platforms: Saviynt IGA, Active Directory, Okta, PingID, ServiceNow, Jira, Splunk, Microsoft 365

PROFESSIONAL EXPERIENCE

IAM Engineer - Full Time 08/2025 – Present
Hybrid Enterprises | U.S. Department of Veterans Affairs

- Triage and resolve IAM requests in the ServiceNow ticket queue, prioritizing by impact and urgency and escalating as needed.
- Assist with user provisioning, access modifications, and deprovisioning across Enterprise applications, supporting least-privilege and Zero Trust principles
- Partner with governance, application owners, and delivery teams to support secure IAM and SSO integrations using SAML and OIDC
- Build and maintain ServiceNow dashboards to track SSO ticket trends, SLA performance, and operational metrics.
- Configure and test Saviynt IGA workflows, access requests, approval rules, and REST APIs supporting identity governance.
- Develop and maintain IAM procedures and workflow documentation to support operational consistency and audit readiness.
- Create and execute manual test cases for the VA provisioning/deprovisioning tool, validating development items through the SDLC.

IT/Cybersecurity Analyst - Contract 12/2024 – 02/2025
Software Resources | Florida Government

- Supported enterprise IAM operations using Active Directory by provisioning identities, modifying access, processing password resets.
- Processed onboarding and offboarding requests while enforcing least-privilege access and security policy.
- Responded to security incidents by implementing mitigation actions and documenting remediation efforts.
- Used Splunk SIEM to analyze security logs, investigate suspicious activity, and support security incident triage and escalation.
- Conducted phishing email investigations, analyzing headers, links, and attachments to identify malicious indicators and support remediation.

MDM Administrator - Full Time 05/2021 – 12/2024
Iron Bow Technologies | U.S. Department of Veterans Affairs

- Provided technical support to Veterans and VA healthcare providers, troubleshooting device, connectivity, and application issues.
- Assigned user profiles, applied security policies, and ensured devices met federal compliance standards.
- Executed user onboarding, offboarding, provisioning, device enrollment, and PingID MFA setup.
- Executed remote wipes and asset recovery procedures for lost or stolen devices in alignment with federal guidelines.

CERTIFICATIONS & CLEARANCE

Certifications: CompTIA Security+ CE, Saviynt ISAA
Clearance: Public Trust Tier 4