This is a starting point for you, not the final copy. Please remember to revise it as needed for your particular organization's needs! If you have feedback, please contact editor@idpro.org.

Senior IAM Developer

Performance Indicators

- System Scalability
- Increased Automation
- System Availability
- System Stability
- System Security
- Compliance
- User Satisfaction

Responsibilities

Design and Build Identity Solutions

- **Design Solutions:** collaborate with engineering, product, and other stakeholders to architect solutions and shape system design.
- **Implement Solutions**: implement in accordance with architecture, product, and design specifications, while ensuring performance, maintainability, and security of implementation.
- **Maintain Systems:** address emerging functional, security, or performance issues.

Secure Development

- **Scalable Architecture:** ensure scalability of secure development and production environments.
- **Hardening:** design and manage specifications for maintaining hardened systems and containers.
- **Automation:** design and implement robust automation strategies for maintaining hardened systems, images, implementations, releases, testing, etc.
- **Secure Environments:** collaborate with IT Operations and security teams to ensure ongoing compliance with security.

Implement and Deploy

- **CI/CD Pipeline:** utilize and assist in managing optimized CI/CD pipeline.

Incident Response

- **Incident Response**: support security incident investigations related to IAM to identify root causes and drive remediation.

Supporting Change

- **Strategy**: partner with IAM Product and Architecture teams to define and design IAM solutions that achieve business objectives.
- **Advise on Design:** provide feedback and guidance related to how IAM impacts/is impacted by organizational initiatives.

People Leadership (Optional)

- **Team Management**: Manage a team of direct reports and contract service providers.
- **Capacity Building**: implement a staffing and continuous development strategy to ensure that the team remains well-equipped to manage in the modern threat landscape.

Knowledge and Qualifications

- Authoritative knowledge of Identity and Access Management Technology or Cybersecurity
- Authoritative knowledge on secure software development, CI/CD processes, test automation, etc.
- Extensive knowledge identity proofing, identity verification, fraud prevention, and detection technologies.
- Deep familiarity with IAM protocols, such as SAML, SPML, XACML, SCIM, OpenID Connect, and OAuth 2.0
- Experience with key IAM and Cybersecurity concepts, like PAM, Directories, Single Sign-On, Multi-Factor Authentication, Delegated Administration, API Gateways, SOA Services, threat detection, etc.
- Past experience working with IAM architecture within a diverse IT environment, including Cloud, On-Premises, IaaS, and SaaS platforms
- Familiarity with key regulatory requirements and industry standards, such as NIST 800-63, GDPR, CCPA, HIPAA, and SOX
- Professional certifications, like CIDPRO, CISSP, CISM, CIAM.


IDPRO®