Senior Software Engineer – EL1 equivalent

Description

Software Engineers have experience overseeing software development projects, writing optimised code, and provide technical leadership to a team of software engineers. They are responsible for the quality and functionality of the software produced by their team. The Senior Identity and Access Management (IAM) Software Engineer is a key technical role responsible for the design, development, and ongoing support of enterprise identity and access management solutions built on Microsoft technologies.

This position requires deep expertise in Active Directory, Active Directory Federation Services (ADFS), Microsoft Entra ID (formerly Azure AD), and custom IAM solutions developed using Microsoft .NET. The engineer will contribute to the secure management of identities, authentication, authorization, and access governance across a hybrid environment.

They will work closely with architecture, security, infrastructure, and application development teams to ensure secure and efficient access to corporate systems and data.

Responsibilities

• Design and implement scalable IAM solutions leveraging Microsoft Entra ID, Active Directory, and Microsoft Identity Manager (MIM).
• Develop custom IAM components and workflows using the Microsoft .NET framework and libraries (C#, ASP.NET, OWIN).
• Integrate authentication and authorization mechanisms into enterprise and web applications using protocols such as OAuth2, OpenID Connect, and SAML.
• Implement and maintain identity lifecycle processes, including provisioning, deprovisioning, and access reviews.
• Automate identity tasks using PowerShell and Azure-based tools, ensuring repeatability and compliance.
• Collaborate with cross-functional teams to align IAM solutions with business and security requirements.
• Troubleshoot complex identity issues and lead resolution activities across cloud and on-prem environments.
• Contribute to documentation, standards, and continuous improvement of IAM practices and toolsets.
• Provide technical mentoring to junior team members and contribute to IAM capability uplift.

LH-02946

Qualifications

Australian Citizen able to obtain NV1 clearance

Experience

Essential criteria

1. Demonstrated experience designing and implementing enterprise IAM solutions using Active Directory, and Active Directory Federation Services (ADFS) and Microsoft Entra ID (Azure AD).
2. Proven knowledge and practical implementation of authentication and authorization protocols such as SAML, OAuth2, and OpenID Connect.
3. Experience automating IAM processes using PowerShell and integrating with

Hiring organization
Services Australia

Employment Type
Contractor

Beginning of employment
01 July 2025

Duration of employment
Initial contract of 12 months with possible two extnsions of 12 months each.

Job Location
Remote work possible

Valid through
13.05.2025

Microsoft cloud and on-premises platforms.
4. Ability to lead the technical architecture and delivery of IAM solutions, with a strong focus on documentation, integration, and compliance.

Desirable criteria

1. Experience working in hybrid identity environments, integrating on-prem Active Directory with cloud-based identity services (e.g., Azure AD Connect).
2. Strong .NET development experience (C#, ASP.NET Core) focused on building custom identity and access management workflows and services.
3. Familiarity with advanced Entra features such as Conditional Access, Identity Governance, and B2B/B2C user flows.
4. Relevant qualifications or certifications in Microsoft identity and security technologies 5. Experience mentoring junior engineers and contributing to IAM knowledge-sharing and capability development.