Job Title: Identity Access Management - Subject Matter Expert

Work Location – India

Mode – Remote
(You will work for BST Timings which starts in India timings from 1 pm to 09.30 pm IST)

Employment Type – 1 Yr Contract

Experience: 8+ years

Job Description

8+ Years of Technical IAM Domain experience with minimum 5 years of experience in Microsoft Azure Identity Platform.
Includes ability to delegate more routine tasks to other team members to support overall delivery, plus ability to work closely with the Business Analyst on process design.

Responsibilities:

- Design, deploy, configure, and administer Azure Active Directory services to meet the organization's requirements.
- Develop and enforce security policies, multi-factor authentication (MFA), and conditional access policies within Azure AD.
- Monitor Azure AD services, investigate and resolve any issues related to user authentication, access permissions, and directory synchronization.
- Perform regular security assessments and identifying and mitigating any vulnerabilities or risks.
- Collaborate with IT teams to integrate Azure AD with other systems, applications, and identity providers.
- Provide technical guidance and support to end-users, troubleshooting any Azure AD-related issues and incidents.
- Stay up-to-date with the latest Azure AD features, security best practices, and industry trends, and make recommendations for improvements.
- Document Azure AD configurations, processes, and procedures, ensuring that knowledge is effectively shared within the team.
- Mandatory Requirements:
- Good experience in designing, implementing, and managing Azure Active Directory services.
- Strong experience of Azure AD security features, including Conditional Access, Identity protection (User risk and sign in risk policies and investigation & remediation of risky users) and MFA(Multifactor Authentication)
- Good Understanding of Threat Handling
- Identification
  - ❖ Identify Attack Patterns
  - ❖ Identify false positives
- Prevention
  - ❖ Perform pro-active & reactive measures in response to Incidents/Threats
- Understanding of On-prem active directory

- Understanding of authentication protocols (e.g., OAuth, OpenID Connect, SAML) and knowledge across Azure AD SSO on-boarding(SAML, OAuth/OIDC)
- Understanding of Azure AD Connect and directory synchronization.
- Working experience of C#, REST API
- Knowledge of CICD pipeline and pipeline development
- Good knowledge of PowerShell scripting for Azure AD automation and management.
- Strong problem-solving skills and the ability to troubleshoot and resolve complex Azure AD issues.
- Excellent communication and collaboration skills, with the ability to work effectively in cross-functional teams.

Desirable:

- Troubleshooting and reporting via Azure AD sign in logs required. Log analytics/Azure Monitor querying experience desirable.
- Graph API basic knowledge and overview will be a bonus, experience with any similar management API could also be considered.
- Participate in deep- dive discussions/workshops with Microsoft Product Groups
- Eg. Azure Identity Protection deep-dive and feedback session

Testing

- Testing of new Microsoft features and private preview feedback when applicable
- One time passcode for B2B users
- SSPR/MFA Converged Registration Experience
- SSPR Reporting

If you are interested for above position kindly share your resume at hr@blupace.co.uk