JBM Recruitment

Senior Identity Access Management Engineer

CLIENT OVERVIEW

The mission of this financial organization is to partner with member shareholders in the region to provide competitively priced funding, a reasonable return on investment, and support for community investment activities to promote home ownership.

POSITION OVERVIEW

The Senior Identity Access Management Engineer will perform and improve Identity Access Management (IAM) within and for the organization.

ESSENTIAL DUTIES AND RESPONSIBILITIES

- Apply knowledge and understanding of the key principles of Identity Access Management
- Use knowledge of access controls (i.e. RBAC, DAC, MAC) and least privilege
- Subject matter expert on security design and solution development related to Identity Lifecycle management
- Identify areas of improvement within Identity & Access Management and initiate through to resolution
- Use ability "Script" in languages SQL, PowerShell, Python
- Develop Python and shell scripts for automation
- Use DevOps tools and mindset to promote a culture of automation
- Develops and/or supports the introduction of new and improved methods, products, procedures, or technologies
- Apply knowledge of AWS IAM roles, groups and policy creation
- Assist existing AWS deployments and identify security improvements and create proof-of-concepts in AWS
- Ensure team knowledge and experience with AWS services remains current
- Perform CyberArk administration, configuration, implementations, designs, and troubleshooting
- Maintain CyberArk on a daily basis from a tier 3-4 standpoint
- Ensure CyberArk resolution of tier 2/3 trouble tickets including password rotations, password malfunctions, account creations, account changes, scheduling.
- Cross-train and develop peers on CyberArk suite of products
- Perform PAM Operational tasks - Defining Access Control, User Entitlements, Manage Applications Credentials, User Access Policy Management.
- Track and complete IAM-related requests/issues via ticketing system. Ensure that appropriate approvals are in place, and provide guidance to approvers as needed, prior to taking action on tickets.
- Enforce compliance with IAM principles including: least privilege and password management.
- Create, maintain, and adhere to policies and procedures to ensure accurate provisioning and de-provisioning of all user accounts and permissions for employees, contractors, interns, and vendors.
- Perform Periodic Access Reviews as identified by need and work with auditors to provide verifiable evidence of compliance.
- Adhere to established SLAs, established processes, security controls and corporate policies;
- Perform system user provisioning maintenance for new employees, transfers, name changes, authority changes and terminations as they apply to core, networking, and Audit standards;
- All other duties as assigned (note: essential functions and responsibilities may change or new ones may be assigned at any time with or without notice).

REQUIREMENTS

- 4 year college degree in information technology or equivalent experience.
- 4-6 years of Identity & Access Management experience. 6+ years of experience necessary without a degree.
- Security certification is highly preferred.
- AWS certifications is a must (solution architect certification in AWS - highly preferred)
    - AWS knowledge must include identity and access management, and automation
    - Minimum of 2 - 3 years' experience supporting AWS Cloud Applications with sound working knowledge of IAM, S3, CloudWatch, CloudTrail, Lambda Serverless Redshift Spectrum IAM EC2 VPC RDS.
- Azure based certifications and O365 experience
    - Must have strong, demonstrated experience with Azure AD design, implementation and management.
    - Experience in deploying and/or migrating multiple environments to Azure

SKILLS

- Strong proactive communication skills
- Customer focused with effective multitasking skills and an excellent team player
- Must have good communication (verbal, written, and listening) skills and ability to manage customer expectations
- Advanced knowledge of IT security controls and Identity & Access Management
- Works well within a team setting
- Ability to work in agile delivery environment
- Skilled in Active Directory concepts, including users, security groups, policies
- Experience supporting Banking or Financial applications and ability to quickly adapt to fast paced business technology landscape is a plus