

Security & Identity Management Consultant

Description

The Security and Identity Management Premiere Support Consultant will support our client's effort related to security solutions integration, conversion and deployment services.

Responsibilities

- Provides IDM security direction to the client to ensure security and organizational objectives are accomplished via security best practices.
- Plan and direct the tracking, and coordinating tasks towards IDM solution implementation schedules.
- Provide implementation, deployment and maintenance support of the Secure Authentication, Access Management Systems, and Identity as a Service (IDaaS) technologies.
- Develop and/or create Enterprise Architecture integration strategies that allow secure access across programs and applications.
- Ensure that mission critical program requirements are properly addressed through provisioning of an implementation plan for estimated timeframes for the work, with approach to managing risks and dependencies.
- Establish an effective privileged account management capability.
- Strengthen the security posture of the client by protecting from cyber-attacks relating to privileged accounts.
- Implement the principle of least privilege by ensuring that privileged access is only used when required and is revoked when not required.
- Limit and control the access of privileged accounts or administrative credentials.
- Implement a full audit trail for all privileged account activities.
- Transition IDM systems to live service, implementing new working processes for impacted teams, and providing knowledge transfer to the end customer.
- Provide compliance support with all applicable State policies, particularly the California Statewide Information Management Manual (SIMM).
- Assist in the development of weekly status reports and project metrics.

Qualifications

Mandatory Qualifications

- Minimum 2 years of experience on State of California IT Security assessment project in a delivery role
- Knowledge of CyberArk Privileged Access Management, including process design, PAM strategy, roadmap, and technology implementation
- Knowledge of OKTA Identity Management, including process design, IDM strategy, roadmap, and technology implementation
- Knowledge of directory technologies including AD, LDAP, or virtual directories
- Experience preparing security analysis and remediation plans, schedules, issue and risk management response plans, budget projections and revisions, and other standard project management work products.
- Demonstrable knowledge of networking technologies (including but not limited to HTTPS, RDP, SSH)
- Demonstrable knowledge of Privileged Access Management best practice methodologies and tools

Hiring organization

Lume Consulting Group

Job Location

Sacramento

Date posted

Desirable Qualifications

- Possession of a current CyberArk certification
- At least one (1) security assessment completed in compliance with CA security standards.

Contacts

info@lumecg.com