UNIVERSITY OF SOUTHERN CALIFORNIA

Analyst, Identity Access Management

Job Code: 166011

OT Eligible: No
Comp Approval: 9/22/2017

JOB SUMMARY:
The IAM Analyst is responsible for identifying and troubleshooting security access to systems and accounts; determines defects and assesses impact of current or potential identity access issues. Responsibilities include monitoring the health of security systems, and troubleshooting and resolving threat incidences, applying patches, and resolving system incidents. This position works with IT internal support teams as well as external clients within the university to provide the highest standards of support relative to identity access management practices. Other responsibilities include creating or maintaining documentation tools and applications to support access and identity management practices, developing solutions to integrate users and tools in a secure manner, and analyzing data to establish solutions to deployment, adoption, and maintenance of new and legacy systems.

JOB ACCOUNTABILITIES:

*E/M/NA % TIME

Troubleshoots, manages, and solves issues related identities, systems, access, accounts, authentication, authorization, entitlements, and permissions. Determines and recommends the most appropriate response to identified more complex problems, issues and/or defects by assessing impact and prioritization.

Maintains, patches, operates, and monitors the health of Identity and Access Management (IAM) systems. Troubleshoots, supports and resolves system incidents, problems and changes, as required.

Provides analysis, development, testing, training, communication, deployment, adoption, and maintenance of new and legacy IAM systems. Leverages problem solving and data analysis skills to ensure projects deliver on time.

Develops, implements, and maintains documentation of processes, procedures, standards, and guideline relating to Information Security. Executes standard operating procedures (SOPs) and work instructions to meet established service level agreements (SLAs). Determines best practices and suggests how to improve current practices.

Collaborates, gathers information, and acts as a resource to internal stakeholders on the identification of access management requirements. Analyzes, recommends, implements and manages information security solutions in accordance with requirements.

Maintains awareness and knowledge of current changes within legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.

Performs other related duties as assigned or requested. The university reserves the right to add or change duties at any time.
*Select E (ESSENTIAL), M (MARGINAL) or NA (NON-APPLICABLE) to denote importance of each job function to position.

**EMERGENCY RESPONSE/RECOVERY:**

- **Essential:** No
- **Yes** In the event of an emergency, the employee holding this position is required to "report to duty" in accordance with the university's Emergency Operations Plan and/or the employee's department's emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.

**JOB QUALIFICATIONS:**

**Minimum Education:**
- Bachelor's degree
- Combined experience/education as substitute for minimum education

**Minimum Experience:**
- 2 years

**Minimum Field of Expertise:**
- Technical experience in IT operations or systems administration supporting identity and access management (IAM) solutions (such as BeyondTrust, CyberArk, Duo, Fischer International, ForgeRock, Grouper, ISIM, OIM, OUD/OVD, Ping Identity, RadiantLogic, SailPoint, Saviynt, Shibboleth, Thycotic).

**Preferred Education:**
- Bachelor's degree

**Preferred Field of Expertise:**
- Expertise in financial services, healthcare, or other regulated industries. CISSP certification.

**Skills: Administrative:**
- Communicate with others to gather information
- Customer service
- Research information
- Understand and apply policies and procedures

**Skills: Other:**
- Analysis
- Assessment/evaluation
- Consulting
- Organization
- Problem identification and resolution
- Teaching/training

**Skills: Technology:**
- Configuration management
- Database administration and management
- Database and application security
Groupware applications
Incident/problem management
Network administration
Network administration reporting
Network communications technologies
Network security access, management and testing
Network systems/data backup, storage and recovery
Server security policies and procedures, access management
Technical documentation
Technical training and instructional design
Troubleshooting

Skills: Machine/Equipment:
- Computer network (department or school)
- Computer network (university)
- Computer peripheral equipment

Supervises: Level:
- May oversee student and/or temporary workers.

Comments:
- Ability to work evenings, weekends and holidays as the schedule dictates.

SIGNATURES:

Employee: ________________________________ Date: ______________________________
Supervisor: ______________________________ Date: ______________________________

The above statements are intended to describe the general nature and level of work being performed. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified.

The University of Southern California is an Equal Opportunity Employer