UNIVERSITY OF SOUTHERN CALIFORNIA

Lead Analyst, Identity Access Management

Job Code: 166015

OT Eligible: No

Comp Approval: 9/22/2017

JOB SUMMARY:

This position acts as the lead analyst in troubleshooting security access to systems and accounts; determines and recommends defects and assesses impact of current or potential identity access issues. Responsibilities include leading efforts in monitoring the health of security systems, and troubleshooting and resolving threat incidences, applying patches, and resolving system incidents. The IAM Lead Analyst works with IT internal support teams and external clients to provide the highest standards of support and guidance relative to identity access management practices. Other responsibilities include ensuring that service level agreements are met, and creating documentation, tools and applications to support access and identity management practices. The IAM Lead Analyst participates in developing solutions to integrate users and tools in a secure manner, and leads the analyses of data to establish solutions to deployment, adoption, and maintenance of new and legacy systems.

JOB ACCOUNTABILITIES:

*E/M/NA  % TIME

_____ _____ Leads and participates in the troubleshooting, management, and resolution of 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.

_____ _____ Leads the maintenance, patching, operations, and monitoring of Identity and Access Management (IAM) systems. Troubleshoots, supports and resolves system incidents, problems and changes, as required.

_____ _____ Ensures service level agreements (SLAs) are met for daily operations of IAM systems. Leads troubleshooting, support and resolution of production incidents. Determines best practices and suggests how to improve current practices.

_____ _____ Provides evaluation, 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.

_____ _____ Leads the development, implementation, and documentation maintenance 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 with technology, functional, and business partners to improve communication, ensure alignment, and achieve shared objectives. Serves as a point of contact for information security.

_____ _____ Mentors other team members in systems administration and IT operations.
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:**

<table>
<thead>
<tr>
<th>Essential</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| 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). Experience with Linux/Unix, Windows, scripting (with programming languages such as Bash, PowerShell, Perl, or Bash), SQL, LDAP, and web services.

**Preferred Education:**

Bachelor's degree

**Preferred Field of Expertise:**

Experience leading technical teams in IT operations or systems administration. 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: 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