USC University of Southern California

Lead Analyst, Identity Access Management
Job Description

JOB INFORMATION

Job Code:	166015
Job Title:	Lead Analyst, Identity Access Management
FLSA Status:	Exempt
Supervisory:	May oversee student and/or temporary workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

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. Leads efforts in monitoring the health of security systems, and troubleshoots and resolves threat incidences, applying patches and resolving system incidents. Works with IT internal support teams and external clients to provide the highest standards of support and guidance relative to identity access management practices. Ensures that service level agreements are met, and creates documentation, tools and applications to support access and identity management practices. 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 QUALIFICATIONS:

Education

Req	Pref	Degree	Field of Study	
X		Bachelor's degree		
	X	Bachelor's degree		

Additional Education

Check here if experience may substitute for some of the above education.

X	Combined experience/education as substitute for minimum education

Work Experience

Req	Pref	Work Experience	Experience Level	
X		5 years		

Additional Work Experience

Check here if education may substitute for some of the above work experience.

	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Technical experience in IT operations or systems administration supporting identity and access management (IAM) solutions (e.g., BeyondTrust, CyberArk, Duo, Fischer International, ForgeRock, Grouper, ISIM, OIM, OUD/OVD, Ping Identity, RadiantLogic, SailPoint, Saviynt, Shibboleth, Thycotic).

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Experience with Linux/Unix, Windows, scripting (with programming languages such as Bash, PowerShell, Perl, or Bash), SQL, LDAP, and web services.
	X	Experience leading technical teams in IT operations or systems administration.
	X	Expertise in financial services, healthcare, or other regulated industries.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CISSP certification.

Other Job Factors

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

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
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.				

Other Requirements

Essential:	Emergency Response/Recovery	Essential:	Mandated Reporter
	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		A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by

Other Requirements

Essential:	Emergency Response/Recovery	Essential:	Mandated Reporter
	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.		telephone or in writing within 36 hours. By virtue of the associated job duties, this position qualifies as a mandated reporter as required by state law and USC's policy at: https://policy.usc.edu/mandated-reporters/

Campus Security Authority (CSA)		Essential:
By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC's policy at: https://dps.usc.edu/alerts/clery/		No

ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

_____   _____   _____
Print Employee Name   Signature   Date

_____   _____   _____
Print Manager Name   Signature   Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills,
duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.