Lead Engineer, Information Security
Job Description

JOB INFORMATION

Job Code:	166109
Job Title:	Lead Engineer, Information Security
FLSA Status:	Exempt
Supervisory:	May oversee staff, students and/or resource employees
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Leads the deployment and day-to-day operations of security engineering solutions (e.g., endpoint, email, cloud security tools) across the university, ensuring they meet policies and standards. Works closely with security architecture, governance and risk management, and other central/local IT departments. Responsible for leading the deployment of technologies protecting systems from security threats, data exfiltration, and other risks.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Bachelor's degree	Information Science	Or
	X	Bachelor's degree	Computer Science	

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		6 years	deploying security engineering technologies and solutions (e.g., EDR/XDR, Cloud security tools, file integrity monitoring, information security configuration, data security platforms, CASB, DLP, IDS/IPS, firewalls).	
	X	7 years		

Additional Work Experience

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

X	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Excellent understanding of information security engineering processes, from acquisition and design to build and operation.
X		Excellent understanding of security controls frameworks (e.g., CIS Top20, NIST CSF, 800-53).
X		Extensive experience defining and deploying security hardening guidelines.
X		Proven subject matter expertise in the different technology stack from OS, system, network, application, etc.
X		Excellent leadership and people management skills. Proven understanding of CIS benchmarks and customer service metrics.
X		Experience managing different operating systems and configuration standards.
X		Ability to plan, organize and document complex system design activities.
X		Excellent written and oral communication skills, able to interact with a broad spectrum of people on a technical and professional level to share complex information.
X		Proven analytical, consulting and problem-solving skills, with exceptional attention to detail.
X		Excellent organizational skills and proven ability to manage multiple projects and priorities simultaneously.
X		Ability to manage, teach and train others.
X		Experience with database administration, access management and systems/data backup, storage and recovery.
	X	Extensive experience in endpoint security operations at large research universities.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		Certified Information Systems Security Professional (CISSP)
	X		Red Hat Certified Systems Administrator (RHCSA)
	X		Linux Foundation Certified Systems Administrator (LFCSA)

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Leads security deployment projects across the university (e.g., scope development, vendor selection, product testing), working with relevant stakeholders to gather requirements. Ensures projects are aligned to the security engineering lifecycle, designing, building, deploying, and managing enterprise infrastructure and solutions to enable compliance with university policies and standards. Maintains and operates security operations' infrastructure, supporting day-to-day work. Ensures performance impact is monitored and that tools are always available with applicable patches and updates. Leads efforts to implement technology/process improvements.				
Oversees the security hardening process with the schools/units, ensuring compliance to configuration baselines providing guidance on how systems are managed and hardened against security threats and vulnerabilities. Serves as subject-matter expert for security enginnering functions, maintaining and creating operational processes supporting overall security strategies, as well as providing technical/granular recommendations for the development of policies and standards.				
Leads efforts managing and deploying analytical, endpoint security and data loss prevention technologies on systems. Provides technical recommendations in security device selection, configuration and maintenance (e.g., network access control, data loss prevention). Leads the work with internal/external stakeholders to ensure the enterprise security infrastructure is effective in deterring, detecting, and containing security threats and incidents. Leads customer meetings, gathering requirements for enhancing security solution designs.				
Ensures procedures and service level agreements are defined, tracked and met. Provides input on the reporting and metrics captured by governance and risk management. Presents reports to leadership on system security status and potential/actual violations with procedural recommendations provided. Reports				

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
daily, weekly and monthly metrics for statistical threats and key performance indicators.				
Serves as escalation point for daily security engineering functions and related platforms, maintaining and creating operational processes supporting overall security strategies. Responsible for daily information security operations and resource planning, providing guidance and regular communication. Influences departmental goals and objectives, relaying leadership expectations and leading team initiatives and activities.				
Stays current with proven/emerging technologies that could strengthen security posture, as well as with any changes in legal, regulatory, and technology environments which may affect operations. Develops and maintains internal/external partnerships with relevant stakeholders to drive effective incident resolutions and the deployment of new security solutions. Ensures senior management and staff are informed of any changes and updates in a timely manner.				
Coaches and mentors junior staff. Recruits, hires, trains and directly supervises all assigned staff. Evaluates performance and provides feedback. Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics. Establishes and maintains appropriate network of professional contacts and memberships in professional organizations. Attends meetings, seminars and conferences, and maintains required/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 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.		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 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/	

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.