UNIVERSITY OF SOUTHERN CALIFORNIA

Senior Engineer, Information Security

Job Code: 166110

OT Eligible: **No**

Comp Approval: **1/28/2022**

JOB SUMMARY:

Deploys, operates, and maintains 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 deploying technology protecting systems from security threats, data exfiltration, and other risks.

JOB ACCOUNTABILITIES:

*E/M/NA	% TIME	
_____	_____	Gathers requirements supporting security engineering projects and engages in those that actively evaluate existing solutions, looking for areas of improvement. Contributes to the design and deployment of security solutions, ensuring efficacy in threat protection for university endpoints and data assets. Maintains security operations' infrastructure to support day-to-day work, ensuring performance impact is monitored and that tools are always available with applicable patches and updates.
_____	_____	Creates configuration baselines to provide guidance on how systems are managed and hardened against security threats and vulnerabilities. Builds security test plans to ensure successful implemenation of new/existing solutions. Serves as the technical point of contact to schools/units to implement baselines across different operating systems. Supports the security engineering lifecycle to design, build, deploy, and manage enterprise infrastructure and solutions to enable compliance with university policies and standards.
_____	_____	Manages and deploys endpoint security, data loss prevention, and analytical technologies on systems. Provides input on the development of information security policies and standards. Provides technical recommendations in security device selection, configuration and maintenance (e.g., network access control, data loss prevention). Works with internal/external stakeholders to ensure that enterprise security infrastructure is effective in deterring, detecting, and containing security threats and incidents. Provides support at 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. Creates reports on system security status and potential/actual violations with procedural recommendations provided. Contributes to the implementation of daily, weekly and monthly metrics for statistical threats and key performance indicators.

_____ _____ 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.

_____ _____ Influences departmental goals and objectives (e.g., workforce planning, compensation). 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.

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:

4 years

Combined education/experience as substitute for minimum experience

Minimum Field of Expertise:

Four years' hands-on experience with 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). Excellent understanding of information security engineering process from acquisition, design, build, and operation. Excellent understanding of security controls frameworks (e.g., CIS Top20, NIST CSF, 800-53). Experience defining and deploying security hardening guidelines. Excellent understanding of the technology stack from OS, system, network and applications. Proven understanding of CIS benchmarks and customer service metrics. Experience managing different operating systems and configuration standards. Ability to plan, organize and document complex system design activities. 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. Proven analytical, consulting and problem-solving skills, with

exceptional attention to detail. Excellent organizational skills and proven ability to manage multiple projects and priorities simultaneously. Ability to teach/train others. Experience with database administration, access management and systems/data backup, storage and recovery.

Preferred Education:

Bachelor's degree

Preferred Experience:

6 years

Preferred Field of Expertise:

Bachelor’s degree in information technology, computer science, or a related field. Extensive experience in information security operations at large research universities. Certifications as a Certified Information Systems Security Professional (CISSP), Red Hat Certified Systems Administrator (RHCSA) and/or Linux Foundation Certified Systems Administrator (LFCSA).

Comments:

May require work and travel on weekends, evenings and/or holidays, based on business necessity.

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