Manager, Security Operations Center
Job Description

JOB INFORMATION

Job Code:	166108
Job Title:	Manager, Security Operations Center
FLSA Status:	Exempt
Supervisory:	May supervise student, temporary and/or resource workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	5 Manager

JOB SUMMARY

Leads internal investigations of security violations, responding to information security events and ensuring service level agreements and standard operating procedures are defined, tracked and met. Holds in-depth knowledge of common attack vectors, security exploits and countermeasures, and is responsible for driving execution of regular metrics for statistical threats. Responsible for driving incident response while evaluating the efficacy of the security operations and incident response processes. Works to maintain any required certifications and knowledge of current changes within legal, regulatory and technology environments that might affect the university.

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		Excellent people management skills.
X		Good technical and troubleshooting ability.
X		Ability to work in a high-stress environment.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Ability to interact with a broad spectrum of stakeholders and business partners on a technical and professional level.
X		A thorough understanding of customer service performance metrics.
X		Experience in crisis management.
	X	Extensive experience in a security operations environment for a large, research university.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
X			CISSP certification.
X			ITIL Certified.
X			Security management certification (e.g., ISSMP, CRISC, CISM).
	X		One of more relevant GIAC certifications (e.g., Security Essentials [GSEC], Certified Perimeter Protection Analyst (GPPA), Certified Enterprise Defender [GCED]).

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Holds overall responsibility for the day-to-day functions of the university's Security Operations Center (SOC), maintaining and creating operational processes that support overall security strategies. Ensures operational procedures and Service Level agreements are defined, tracked and met. Manages incident response efforts by maintaining strong partnerships with internal and external business leaders to support and drive effective incident resolutions. Ensures operational relationships with other units (e.g., threat intelligence, endpoint security, vulnerability assessment) are maintained and developed.				
Leads and supports the Security Operations Center team, effectively driving team strategy, goals and performance objectives. Establishes team and individual goals to support overall objectives. Coaches, mentors, and provides career development guidance. Recruits, screens, hires, trains and directly supervises all assigned subordinate staff. Evaluates employee performance and provides guidance and feedback. Counsels, disciplines and/or terminates employees, as required. Recommends departmental goals and objectives, including workforce planning and compensation recommendations.				
Supports and manages the systems and programs that monitor the university's assets, network and data, ensuring the prevention of events that negatively impact confidentiality, availability and integrity. Supports the development of strategic plans and projects to meet security goals and objectives. Identifies new technologies, processes and procedures to streamline the security incident response program.				
Establishes daily operations, regular communications, and resource planning, providing guidance, relaying leadership expectations, and leading team initiatives and activities. Authors and coordinates security status reports to provide system status, report potential and actual security violations, and provide procedural recommendations. Responsible for driving execution of daily, weekly and monthly metrics for statistical threats and key performance indicators (KPIs).				
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 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/	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.