USC University of Southern California

Security Operations Director
Job Description

JOB INFORMATION

Job Code:	168037
Job Title:	Security Operations Director
FLSA Status:	Exempt
Supervisory:	Manages through subordinate supervisors.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	4 Administrator

JOB SUMMARY

Responsible for developing the strategy and vision for the security operations team, and the execution of the responsibilities within the security operations directorate. Accountable for the key security operations areas, including but not limited to, incident response, forensics, data loss prevention, security monitoring, threat management, host security and vulnerability management, while providing security support for key stakeholders across the university. Serves as the primary point of contact for relevant parties concerning required forensics issues/risks and develops programs and procedures to ensure monitoring and response to security events. Oversees the management of anti-malware technologies on systems. Directly or indirectly manages all program staff and develops and administers a budget, while maintaining up-to-date knowledge in the field of specialty.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Master'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		8 years		
X		5 years	in a management role	
	X	10 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		Understanding and technical knowledge of Security Operations concepts, including but not limited to, incident response, forensics, data loss prevention, security monitoring, threat management, host security and vulnerability management.
X		Demonstrable strong management skills, including the ability to develop, mentor and coach others.
X		Strong written and oral executive communication, including up to the C-level.
	X	Experience in the management and/or implementation of security monitoring, anti-malware, data loss prevention and vulnerability management technologies.
	X	Knowledge and experience with Qrader, SOC, MSSP.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CISSP

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Serves as a Subject Matter Expert (SME). Provides expertise and understanding of all aspects of the Security Operations landscape, working with senior leadership to mold, shape and expand the security operations footprint.				
Oversees the Incident Response (IR) program, including reviewing status provided on level 2 and 3 risks and high-level monitoring of all IR activities and alignment to the university's IR Plan.				
Defines security monitoring expectations and goals in alignment with the university's information security strategy. Develops programs to ensure successful achievement of goals.				
Participates in the development and administration of the department budget. Approves/disapproves department expenditures. Develops short and long-term budget projections and plans. Provides financial status reports as needed.				
Reviews status of security monitoring, threat management and vulnerability treatment across the university. Determines corrective course of action, if necessary, and communicates plans and relative level of security threats, if any, to senior management.				
Engages with and serves as the primary point of contact for relevant parties concerning required forensics issues/risks that span legal, compliance and regulatory requirements.				
Approves, or coordinates approval for, security monitoring policies, procedures, standards and roles and responsibilities.				
Develops programs and procedures to ensure monitoring and response to security events, alerts and reports identified via implemented security tools, such as SIEM, DLP, physical alarms, etc.				
Directly or indirectly manages program and administrative staff, usually through subordinate managers and supervisors. Recruits, screens, hires, and trains staff, as necessary. 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. Reassesses or redefines priorities as appropriate in order to achieve performance objectives. Recommends, approves and monitors professional training and development opportunities for staff.				
Identifies opportunities for enhanced coverage of threat intelligence and security monitoring. Recommends and implements solutions.				
Oversees the management of anti-malware technologies on systems including the performance of anti-malware technologies, patterns in attacks to update signatures and additional security control needs, and update of configurations based on security standard requirements.				

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Collaborates cross-functionally with other technology teams and security policy organizations. Represents the unit or university on internal and external committees, task forces, or boards, as assigned. Provides consultation across the university to stakeholders concerning security issues.				
Maintains up-to-date knowledge by researching new technologies and software products, participating in educational opportunities and conferences, and reading professional publications.				

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/	Yes

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.