USC University of Southern California

Analyst, Vulnerability Management
Job Description

JOB INFORMATION

Job Code:	166071
Job Title:	Analyst, Vulnerability Management
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

This position provides on-going analysis of scans and maintenance of tools for assessments of the security environment; reviews and mitigates penetration tests, and recommends fixes and security patches required in the event of security breaches. This role is also responsible for security analysis and producing monthly exception and management reports that lead to the implementation and remediation required by audits; The Analyst, Vulnerability Assessment, is responsible for developing program quality metrics, and reviewing findings to eliminate risks. The analyst analyzes and monitors the security practices of vendors and third parties, and provides reporting for governance of vulnerability impact.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
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		2 years		
	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		Ability to perform vulnerability assessments and penetration testing using manual testing techniques, scripts, commercial and open source tools.
X		Knowledge with prioritizing remediation activities with operational teams through risk ratings of vulnerabilities and assets.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Ability to read, write and modify scripts for automation of vulnerability management tasks.
X		Working experience with industry frameworks (CSF, ISO, COBIT, etc.).
X		Experience in deploying and operating vulnerability scanning infrastructure and services.
X		Strong knowledge of industry standards regarding vulnerability management, including Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS) and Open Web Application Security Project (OWASP).
X		Strong knowledge of technology and security topics including network security, wireless security, application security, infrastructure hardening, security baselines, and web server and database security.
	X	Knowledge of computer networking concepts, protocols and network security methodologies.
	X	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
	X	Knowledge of specific operational impacts of cybersecurity lapses.
	X	Knowledge of host network access control mechanisms (e.g., access control list, capabilities lists).
	X	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
	X	Knowledge of systems diagnostic tools and fault identification techniques.
	X	Knowledge of system administration, network and operating system hardening techniques.
	X	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
	X	Knowledge of penetration testing principles, tools and techniques.
	X	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
	X	Skill in performing impact/risk assessments.
	X	Skill in the use of penetration testing tools and techniques.
	X	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Reviews and mitigate penetration tests and vulnerability assessments on information systems and infrastructure. Provides input to assist with the analysis, development and advancement of key risk indicator. Reviews penetration test findings with system owners and works to eliminate or remediate risks associated with the findings.				
Monitors security vulnerability information from vendors and third parties; incorporates findings and insights of complex issues into objective security intelligence assessments that comply with internal governance practices and requirements.				
Performs asset and network discovery reviews, helping to ensure full coverage of vulnerability management environment. Conducts system and application vulnerability testing; analyze and verify information obtained from reviews.				
Leverages asset inventory and patch management systems to provide reporting and governance for vulnerability impact and remediation progress.				
Maintains tools used for conducting vulnerability scanning. Collates and analyzes security incident and event data to produce monthly exception and management reports; prepares audit reports that identify technical and procedural findings, and provide recommended remediation solutions.				
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.