USC University of Southern California

Incident Response Analyst
Job Description

JOB INFORMATION

Job Code:	166085
Job Title:	Incident Response Analyst
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Serves as the second level of inquiry of security events, communicating directly with data asset owners and business response plan owners and escalating throughout incidents. Hunts for suspicious activity, reviews the Security Operations Center team's work and false positives, and provides feedback to improve alert accuracy. Analyzes log files and takes an active part in containing issues, even after escalating when necessary.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Associate's degree	Cyber Security	

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		3 years		
	X	3 years	in information security	
	X	2 years	as an SOC analyst	
	X	1 year	as a level-two investigation analyst	

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		Knowledge of network security zones, firewalls, and IDS.
X		Knowledge of log formats for syslog, http logs, DB logs and how to gather forensics for traceability back to event.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Knowledge of packet capture and analysis. Experience with log management or security information management tools.
X		Experience with Security Assessment tools (NMAP, Nessus, Metasploit, Netcat).
X		Ability to make information security risk determinations. Effective verbal and written communication skills.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CCNA certification. Security Essentials – SEC401 (optional GSEC certification).

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Provides second level of investigation of security events, producing vulnerability, configuration and coverage metrics.				
Communicates directly with data asset owners and business response plan owners throughout incidents and high-security events, per the IR guidelines, escalating issues when necessary and protecting the confidentiality, integrity and information owned or entrusted by the university.				
Hunts for suspicious, anomalous activity based on data alerts and outputs from various toolsets, and reports and summarizes findings to facilitate remediation tasks.				
Reviews and takes a proactive approach to false positives, and works with the various SOC teams to tune and provide feedback to improve accuracy of the alerts.				
Analyzes log files and, working with SOC teams, investigates, compiles relevant technical and background information, and performs forensics and post-mortem analysis of information security and incidents.				
Takes an active part in the containment of events of interest, even after escalations.				
Prepares reports and conducts briefings on significant investigations.				
Applies critical thinking and risk analysis methodologies when considering evaluating impact of vulnerabilities, relative risks, and any possible 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		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

Other Requirements

Essential:	*Emergency Response/Recovery*	*Essential:*	*Mandated Reporter*
	efforts, and mobilize other staff members if needed.		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.