USC University of Southern California

Senior Incident Response Analyst
Job Description

JOB INFORMATION

Job Code:	166079
Job Title:	Senior Incident Response Analyst
FLSA Status:	Exempt
Supervisory:	May oversee staff, students, volunteers, agencies and/or resource employees.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Leads the investigation, coordination, resolution, closure and reporting on security incidents. Responsible for forensically analyzing end-user systems and servers, as well as installing, implementing, configuring and operating numerous security systems and incident response tools. Interacts with server owners, system custodians and IT contacts in pursuit of incident response activities, and consults and assesses perceived threats. Analyzes findings and develops fact-based reports, and resolves incidents by identifying root causes and solutions.

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		5 years		
	X	3 years	as an SOC analyst.	
	X	1 year	as a level-three response 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		Experience with security threats, vulnerabilities, intrusion techniques, malware capabilities and system diagnostics.
X		Experience with electronic investigation, forensic tools and methodologies, including log correlation and analysis, forensically handling electronic data, knowledge of the computer security investigative processes, and malware identification and analysis.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Understanding of legalities surrounding electronic discovery and analysis.
X		Experience with SIEM technologies.
X		Excellent analytics and reporting skills.
	X	Prior experience in managed or enterprise information security services, incident response, forensics, malware analysis, penetration testing, or network defense.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		Certified Information Systems Security Professional (CISSP)
	X		Certified Information Systems Auditor (CISA)
	X		Certified Information Security Manager (CISM)
	X		GIAC Security Essentials (GSEC)
	X		Certified in Risk and Information Systems Control (CRISC)

Other Job Factors

- Ability to work evenings, weekends and holidays as the schedule dictates.

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Leads the investigation, coordination, resolution, closure and reporting on security incidents as they are escalated or identified. Performs complex incident response technical analysis and develops technical conclusions based on analysis of evidence. Reviews analysis and conclusions of other consultants, when applicable.				
Forensically analyzes end-user systems and servers found to have possible indicators of compromise. Analyzes the artifacts collected during a security incident/forensic analysis.				
Installs, implements, configures and operates multiple security systems and incident response tools in an extended enterprise environment.				
Effectively configures and utilizes security detection systems, logs, monitoring alerts and other sources of information to identify and address security threats and events.				
Interfaces and communicates with server owners, system custodians and IT contacts to pursue security incident response activities, including obtaining access to systems, collecting digital artifacts and containing the incident or executing other remediation actions.				
Provides consultation and assessment on perceived security threats. Conducts assessments of client readiness to respond to incidents, including designing and delivering incident response exercises to test client incident response plans. Assists with the ongoing development and improvement of the enterprise incident response plan (IRP). Manages, improves and updates the information security incident response process and protocol documentation.				
Analyzes findings in investigative matters and develops fact-based reports. Regularly provides reporting and metrics to the ITS Information Security organization.				
Resolves security incidents by identifying root causes and 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/	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.