USC University of Southern California

Lead Analyst, Incident Response
Job Description

JOB INFORMATION

Job Code:	166077
Job Title:	Lead Analyst, Incident Response
FLSA Status:	Exempt
Supervisory:	Supervises employees and/or student workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Serving as a subject-matter expert in incident response and forensic investigations, the Lead Analyst, Incident Response, independently decides on and defines approaches for complex cases. The position leads the investigation, coordination, resolution, closure and reporting on security incidents as they are escalated or identified, and forensically analyzes systems, servers and artifacts. The lead analyst mentors other team members in security operations, assists in formulating best practices for incident response and forensic investigations, and manages, improves and updates processes and protocol documentation.

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		2 years		
	X	5 years	in information security experience.	
	X	3 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.
X		Knowledge of packet capture and analysis.
X		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.
X		Effective verbal and written communication skills.
X		High level of critical thinking to filter case data.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X	Cisco Certified Network Associate (CCNA)	
	X		GIAC Security Essentials (GSEC)

Other Job Factors

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

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Serves as an Incident Response and Forensic Investigation subject-matter expert (SME). Along with the Security Operations Manager, helps design, build and implement best practices. Independently decides on and defines approaches for complex forensic investigations and analysis.				
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 conclusions based on evidence. Reviews analysis and conclusions of other consultants, when applicable.				
Forensically analyzes end-user systems and servers found to have possible indicators of compromise, as well as the artifacts collected during a security incident to gather information pertaining to current investigations.				
Provides consultation and assessment on perceived security threats and conducts assessments of client readiness to respond to incidents. Designs and delivers incident response exercises to test client incident response plans (IRP), and assists with the ongoing development and improvement of the enterprise incident response plan. Works with the Office of Compliance and General Counsel to build forensic case documentation, including chain-of-custody information, data categorization and investigatory results.				
Serves as a liaison to other business units during incidents, and as a communication lead for the Security Operations team for details concerning current investigations. Provide executive communication, finished incident reports and forensics data, as appropriate, advising management on business decisions that may significantly affect University-wide or departmental operations, policies or procedures.				
Mentors team members in security operations, forensic analysis, e-discovery and IT operations, helping define their investigative processes.				
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.