Lead Cyber Threat Intelligence Analyst
Job Description

JOB INFORMATION

Job Code:	166087
Job Title:	Lead Cyber Threat Intelligence Analyst
FLSA Status:	Exempt
Supervisory:	May supervise staff, student, temporary or resource workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Leads the identification and tracking of cyber threat intelligence requirements, probing for signs of compromise and providing analyses. Manages and develops extensive models to determine nature of intelligence-related incidents and activities. Organizes and contextualizes intelligence and communicates the nature and impact of applicable security threats, risks, and vulnerabilities. Oversees the parsing of large technical data sets, integrating output of technical research and sharing and escalating findings to team and management as appropriate. Defines the requirements for gathering, evaluating, and studying multiple intelligence reports, identifying intrusion patterns and managing tracking of relevant threats.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Bachelor's degree	International Relations	Or
	X	Bachelor's degree	Political Science	Or
	X	Bachelor's degree	Cyber Security	Or
	X	Bachelor's degree	Computer Science	Or
	X	Bachelor's degree	in related field(s)	

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		4 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		Extensive experience in a cyber threat intelligence environment.
X		Comprehensive knowledge of potential cyber threats and prevention methods.
X		Experience with one or more relevant programming language (e.g., SQL).
X		Proven experience analyzing large data sets with the ability to recognize and articulate relevant patterns.
X		Experience with log management and security information management tools.
X		Strong attention to detail.
X		Excellent written and oral communication skills.
	X	Experience with the cyber threat intelligence landscape of a university environment.
	X	Familiarity with international intelligence environments.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CEH and other relevant certifications (e.g., Intrusion Detection In Depth – SEC503 [GCIA certification], Security Essentials – SEC501 [GCED certification], Hacker Techniques, Exploits & Incident Handling – SEC504 [GCIH certification]).

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Defines standards, processes, and tools to identify, prioritize, and track cyber threat intelligence research findings. Utilizes high-level technical and threat actor information to correlate intelligence findings across domains (e.g., crime, espionage, hacktivism). Serves as threat intelligence subject matter expert, formulating and prioritizing intelligence requirements according to established risk management framework.				
Identifies and analyzes indicators of compromise (IOCs) using various toolsets and data provided by other analysts. Performs advanced threat analysis of security intelligence feeds relative to network traffic analysis, intrusion detection, offensive security, data science, and predictive analytics. Communicates IOC models to trusted parties for validation and collaboration. Synthesizes and places intelligence information into context, communicating the nature and impact of applicable security vulnerabilities.				
Manages documentation and tracking of relevant threats. Develops intelligence library and technical expertise on threat actors, attack trends, and attack tactics, techniques, and procedures (TTPs). Collects and analyzes intelligence reports from multiple sources and disciplines. Reviews incident logs and records, mining for intrusion patterns. Analyzes threat intelligence feeds to create actionable results. Integrates output of technical research (e.g., network forensics and reverse engineering, information intelligence products), communicating and escalating intelligence findings to management as appropriate.				
Collaborates with other cyber intelligence analysts to ensure individual and team goals are met. Maintains understanding of unit, department, and university regulations, policies, and procedures. Builds and maintains strong relationships with customers, partners, and stakeholders by participating in governance boards, councils, and meetings to understand current and future business needs and ensure consistent, reliable service.				

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		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

Other Requirements

Essential:	*Emergency Response/Recovery*	*Essential:*	*Mandated Reporter*
	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.		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/	

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.