USC University of Southern California

Senior Cyber Threat Intelligence Analyst

Job Description

JOB INFORMATION

Job Code:	166088
Job Title:	Senior Cyber Threat Intelligence Analyst
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Ensures identification, prioritization and tracking of cyber threat intelligence requirements, probing for signs of compromise and providing analyses. Leads development of threat models to determine incident-type activities, organizes and contextualizes intel, and communicates the nature, impact and mitigations for applicable security vulnerabilities. Provides offensive security and intelligence support to other Security Operations functions in support of established objectives. Parses large technical data sets, integrates output of technical research, and shares and escalates severe findings to team and management. Gathers, evaluates and studies multiple intelligence reports, digs for intrusion patterns, and manages documentation and tracking of relevant threats. Collaborates with other analysts, ensuring that individual and team goals are met.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	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.

X	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	*Pref*	*Functional Skills*
X		Strong analytical and problem-solving skills.

Knowledge, Skills and Abilities

Req	*Pref*	*Functional Skills*
X		Knowledge of a wide variety of technologies, platforms, threats, and threat actors.
X		Experience with packet capture and analysis.
X		Experience with security assessment tools (e.g., NMAP, Nessus, Metasploit, Netcat).
X		Understanding of network interoperability and current best practices in cyber security (e.g., relevant laws, regulations, standards).
X		Experience conducting analytical studies and communicating technical information to non-technical audiences.
X		Ability to make information security risk determinations based on threat intelligence analysis.
X		Effective verbal and written communication skills.
	X	Bachelor’s degree in information technology, computer science, or a related field.
	X	One of more relevant certifications (e.g., OSCP, GCTI, GCIH etc.).
	X	Experience with multiple programming languages (e.g., Python, C#, Java).

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Develops threat models to facilitate a threat intelligence-informed prioritization of Security Operations and Information Technology activities in order to mitigate cyberattacks and security risks across business and technology environments. Supports security leadership to instill cybersecurity policies and practices throughout business units to address security operations, incident response, application security and infrastructure.				
Coordinates closely with other Security Operations functions in order to analyze threat actor activity, identify intrusions, and develop detections. Analyzes data feeds for relevance and potential impact to the university to enhance security monitoring, provide contextual information to enable alert handling, response, and preventative control configuration.				
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.				
Designs and conducts proof-of-concept tests to replicate third-party findings and propose solutions to resolve discovered security issues. Prepares detailed reports on findings while working closely with internal and external groups to develop appropriate security controls. Conducts tactical assessments involving social engineering, application security (web and mobile), physical methods, lateral movement, threat analysis, internal and external network architecture and a wide array of commercial and bring-your-own (BYO) products.				
Actively hunts for threat exposure and identifies incidents warranting action to disrupt and remediate threats. Documents threats into contextual reports outlining severity, urgency and impact, and ensures they can be understood by both management and technical teams. Maintains currency with industry best practices. Assesses and recommends additional tools and technologies as needed, and performs research activities to investigate technologies which may impact the university and present findings to appropriate leadership.				
Influences departmental goals and objectives (e.g., workforce planning, compensation). Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics. Establishes and maintains appropriate network of professional contacts and memberships in professional organizations. Attends meetings, seminars and conferences, and maintains required/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/	

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.