USC University of Southern California

Cyber Threat Intelligence Analyst
Job Description

JOB INFORMATION

Job Code:	166089
Job Title:	Cyber Threat Intelligence Analyst
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

The Cyber Threat Intelligence Analyst identifies, prioritizes and tracks cyber threat intelligence requirements, probes for signs of compromise, and provides initial analyses. Develops models to determine incident-type activities, organizes and contextualizes intel, and communicates the nature, impact and mitigations for applicable security vulnerabilities. Parses large technical data sets, integrates output of technical research, and shares and escalates severe findings to team and management. The analyst takes an active part in the gathering, evaluation and study of multiple intelligence reports, digs for intrusion patterns, and manages documentation and tracking of relevant threats. Collaborate with other analysts, ensuring that individual and team goals are met.

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		1 year		
	X	2 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		Strong analytical and problem solving skills.
X		Knowledge of security intelligence threats and threat actors.
X		Knowledge of packet capture and analysis.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Experience with log management or security information management tools.
X		Experience with security assessment tools (e.g., NMAP, Nessus, Metasploit, Netcat).
X		Ability to make information security risk determinations based on threat intelligence analysis.
X		Effective verbal and written communication skills.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CEH certification.
	X		Intrusion Detection In Depth - SEC503.
	X		Hacker Guard:Security Baseline Training - SEC464. Security Essentials - SEC501.
	X		Hacker Techniques, Exploits & Incident Handling - SEC504.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Identifies, prioritizes and tracks cyber threat intelligence requirements utilizing both technical and actor information across domains (e.g., crime, espionage, hacktivism); formulate and prioritize intelligence requirements according to established risk management framework.				
Hunts for indicators of compromise using various toolsets, and provides initial analysis of security intelligence feeds relative to network traffic analysis, intrusion detection, offensive security, data science and predictive analytics.				
Develops models for identifying incident-type activity, of malware or bad actors, using statistical/advanced analytic tools; shares indicators of compromise (IOC) models with trusted parties for validation and collaboration; synthesizes and places intelligence information into context; communicates the nature, impact and mitigations for applicable security vulnerabilities.				
Sifts through large technical data sets, and identifies intelligence collection requirements that can be met through automated and human collection methodologies.				
Integrates output of technical research, e.g., network forensics and reverse engineering, into intelligence products; communicates and escalates severe intelligence findings to team members and management.				
Collects, assesses and analyzes intelligence reports from multiple sources and disciplines; reviews incident logs/records mining for intrusion patterns; manages documentation and tracking of relevant threats.				
Collaborates with other cyber intelligence analysts to ensure individual and team goals are met; maintain understanding of unit, department, and university regulations, policies, and procedures.				
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		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,

Other Requirements

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