USC University of Southern California

Analyst, Host Security
Job Description

JOB INFORMATION

Job Code:	166049
Job Title:	Analyst, Host Security
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

The Host Security Analyst defensively monitors the university’s networks, configuring and managing anti-malware to prevent and detect threats. They will receive and analyze system alerts, identify anomalies and triage malware, determine the effects of any observed attacks. The analyst creates, defines and maintains solutions based on IT security standards, coordinates with varied system owners throughout the university, and regularly reports on the performance of the networks’ defenses.

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		3 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		Understanding of endpoint devices protection concepts, including anti-virus, configuration updates, patch management, host based firewalls, host based IDS, etc.
X		Knowledge of different operating systems, configuration standards, solutions, application of endpoint protection technologies and analysis of events and alerts.
X		Extensive experience with endpoint protection technologies.
X		Extensive experience with review/analysis of alerts and events from endpoint protection technologies.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Extensive experience with system administration for managing configuration standards.
X		Demonstrable knowledge of programming languages and operating systems, and current USC equipment and technologies in use.
X		Ability to plan, organize and document complex system design activities.
	X	Ability to configure systems to be consistent with information security policies/procedures.
		Strong ability to communicate technical/complex information, both verbally and in writing.
		One year of direct experience in host security.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Manages anti-malware technologies on systems, detects host and network-based intrusions, and analyzes network traffic to identify anomalous activity and potential threats to resources.				
Reviews performance of anti-malware technologies and reports on patterns in attacks to update signatures and install any additional security control needs.				
Updates configurations and solutions based on IT security standard requirements for prevention and detection tools.				
Defines and maintains standard configuration requirements for hosts, including various systems and software.				
Tracks and obtains approval from ITS Information Security for any exceptions of defined configuration standards.				
Defines standard patch management and security upgrade processes.				
Reviews proposed exceptions to patching through the defined risk management process.				
Coordinates with system owners to identify appropriate times to schedule patches/upgrades.				
Manage implementation of defined patch management process requirements.				
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.