



JOB INFORMATION

<i>Job Code:</i>	166053
<i>Job Title:</i>	Host Security Lead
<i>FLSA Status:</i>	Exempt
<i>Supervisory:</i>	May oversee student and/or temporary workers.
<i>Job Family:</i>	IT Security
<i>Job Family Group:</i>	Information Technology
<i>Management Level:</i>	7 Individual Contributor

JOB SUMMARY

The Host Security Lead ensures that all operations and tasks related to managing anti-malware technologies on systems across the university are conducted, and assists in providing technical expertise to identify, mitigate, manage, track and support processes for maintaining sound anti-malware security technologies. This position is responsible for reviewing anti-malware technologies to identify patterns and establish appropriate controls. The Host Security Lead is responsible for defining and maintaining configuration standards, and overseeing defined patch/upgrade management process requirements. This position will work closely with Governance and Risk Management function on the topic of host security.

JOB QUALIFICATIONS:

Education

<i>Req</i>	<i>Pref</i>	<i>Degree</i>	<i>Field of Study</i>
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

<i>Req</i>	<i>Pref</i>	<i>Work Experience</i>	<i>Experience Level</i>
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

<i>Req</i>	<i>Pref</i>	<i>Functional Skills</i>
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.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Extensive experience with review/analysis of alerts and events from endpoint protection technologies.
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.
X		Strong ability to communicate technical/complex information, both verbally and in writing.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
In conjunction with Governance and Risk Management function, defines new policies 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. Acts as a technical SME to the Governance and Risk Management function on the topic of host security and provide input into the reporting and metrics captured by Governance and Risk Management.				
Provides guidance and support to Host Security Analyst by translating strategic objectives into tactical activities.				
Leads efforts in management of anti-malware technologies on systems. Provides technical assistance in the selection, configuration, and maintenance of network security devices including, but not limited to, firewalls, network-based malware detection and related platforms. Serve as a technical resource in advising and assisting all departments and schools for issues relating to network security.				
Reviews performance of anti-malware technologies and patterns in attacks to update signatures and additional security control needs. Ensure appropriate security policies and controls are in place that safeguards digital files and vital electronic systems.				
Updates configurations and solutions based on IT security standard requirements for prevention and detection tools. Tests and troubleshoots information security technologies and solutions to ensure protection of ITS assets, and meet business functions and requirements.				
Oversees implementation of defined patch management process requirements. 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.				
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		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

Other Requirements

<i>Essential:</i>	<i>Emergency Response/Recovery</i>	<i>Essential:</i>	<i>Mandated Reporter</i>
	following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.		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/
<i>Campus Security Authority (CSA)</i>			<i>Essential:</i>
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.