UNIVERSITY OF SOUTHERN CALIFORNIA

Analyst, Host Security

Job Code: 166049

OT Eligible: **No**

Comp Approval: **1/9/2018**

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 ACCOUNTABILITIES:

*E/M/NA	% TIME	
_____	_____	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.
		Performs other related duties as assigned or requested. The university reserves the right to add or change duties at any time.

***Select E (ESSENTIAL), M (MARGINAL) or NA (NON-APPLICABLE) to denote importance of each job function to position.**

EMERGENCY RESPONSE/RECOVERY:

Essential: ☐ No

☐ Yes 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.

JOB QUALIFICATIONS:

Minimum Education:

Bachelor's degree

Combined experience/education as substitute for minimum education

Minimum Experience:

3 years

Minimum Field of Expertise:

Understanding of endpoint devices protection concepts, including anti-virus, configuration updates, patch management, host based firewalls, host based IDS, etc. Knowledge of different operating systems, configuration standards, solutions, application of endpoint protection technologies and analysis of events and alerts. Extensive experience with endpoint protection technologies. Extensive experience with review/analysis of alerts and events from endpoint protection technologies. Extensive experience with system administration for managing configuration standards. Demonstrable knowledge of programming languages and operating systems, and current USC equipment and technologies in use. Ability to plan, organize and document complex system design activities. Ability to configure systems to be consistent with information security policies/procedures. Strong ability to communicate technical/complex information, both verbally and in writing.

Preferred Field of Expertise:

One year of direct experience in host security.

Skills: Other:

Analysis

Assessment/evaluation

Communication -- written and oral skills

Interpretation of policies/analyses/trends/etc.

Problem identification and resolution

Research

Skills: Technology:

Configuration management

Database administration and management

Database and application security

Groupware applications

Incident/problem management

Network administration reporting

Network communications technologies
Network security access, management and testing
Network systems/data backup, storage and recovery
Server security policies and procedures, access management
Technical documentation
Technical training and instructional design
Troubleshooting

Comments:

Ability to work evenings, weekends and holidays as the schedule dictates.

SIGNATURES:

Employee: _____ **Date:**_____

Supervisor: _____ **Date:**_____

The above statements are intended to describe the general nature and level of work being performed. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified.

The University of Southern California is an Equal Opportunity Employer