UNIVERSITY OF SOUTHERN CALIFORNIA

Security Operations Director

Job Code: 168037

OT Eligible: No
Comp Approval: 4/28/2017

JOB SUMMARY:
This position is responsible for developing the strategy and vision for the security operations team, and the execution of the responsibilities within the security operations directorate. The Security Operations Director is accountable for the key security operations areas, including but not limited to, incident response, forensics, data loss prevention, security monitoring, threat management, host security and vulnerability management, while providing security support for key stakeholders across the university. This position also serves as the primary point of contact for relevant parties concerning required forensics issues/risks and develops programs and procedures to ensure monitoring and response to security events. The Security Operations Director also oversees the management of anti-malware technologies on systems. This position directly or indirectly manages all program staff and develops and administers a budget, while maintaining up-to-date knowledge in the field of specialty.

JOB ACCOUNTABILITIES:

**E/M/NA % TIME**

---

Serves as a Subject Matter Expert (SME). Provides expertise and understanding of all aspects of the Security Operations landscape, working with senior leadership to mold, shape and expand the security operations footprint.

---

Oversees the Incident Response (IR) program, including reviewing status provided on level 2 and 3 risks and high-level monitoring of all IR activities and alignment to the university’s IR Plan.

---

Defines security monitoring expectations and goals in alignment with the university’s information security strategy. Develops programs to ensure successful achievement of goals.

---

Participates in the development and administration of the department budget. Approves/disapproves department expenditures. Develops short and long-term budget projections and plans. Provides financial status reports as needed.

---

Reviews status of security monitoring, threat management and vulnerability treatment across the university. Determines corrective course of action, if necessary, and communicates plans and relative level of security threats, if any, to senior management.

---

Engages with and serves as the primary point of contact for relevant parties concerning required forensics issues/risks that span legal, compliance and regulatory requirements.

---

Approves, or coordinates approval for, security monitoring policies, procedures, standards and roles and responsibilities.

---

Develops programs and procedures to ensure monitoring and response to security events, alerts and reports identified via implemented security tools, such as SIEM, DLP, physical alarms, etc.
Directly or indirectly manages program and administrative staff, usually through subordinate managers and supervisors. Recruits, screens, hires, and trains staff, as necessary. Evaluates employee performance and provides guidance and feedback. Counsels, disciplines and/or terminates employees as required. Recommends departmental goals and objectives, including workforce planning and compensation recommendations. Reassesses or redefines priorities as appropriate in order to achieve performance objectives. Recommends, approves and monitors professional training and development opportunities for staff.

Identifies opportunities for enhanced coverage of threat intelligence and security monitoring. Recommends and implements solutions.

Oversees the management of anti-malware technologies on systems including the performance of anti-malware technologies, patterns in attacks to update signatures and additional security control needs, and update of configurations based on security standard requirements.

Collaborates cross-functionally with other technology teams and security policy organizations. Represents the unit or university on internal and external committees, task forces, or boards, as assigned. Provides consultation across the university to stakeholders concerning security issues.

Maintains up-to-date knowledge by researching new technologies and software products, participating in educational opportunities and conferences, and reading professional publications.

Develops and implements security related procedures such as office opening and closing routines, recognition of duress signals and key controls. Coordinates security activities with Department of Public Safety. Promotes and maintains standards for security conscious awareness and behavior. Maintains knowledge of University's crime prevention and suppression programs and services. Ensures dissemination of security related information to staff.

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:**

8 years
Minimum Field of Expertise:

Understanding and technical knowledge of Security Operations concepts, including but not limited to, incident response, forensics, data loss prevention, security monitoring, threat management, host security and vulnerability management. Demonstrable strong management skills, including the ability to develop, mentor and coach others. Strong written and oral executive communication, including up to the C-level. 5 years of management experience.

Preferred Education:

Master's degree

Preferred Experience:

10 years

Preferred Field of Expertise:

Experience in the management and/or implementation of security monitoring, anti-malware, data loss prevention and vulnerability management technologies. Knowledge and experience with Qrader, SOC, MSSP. CISSP preferred.

Skills: Other:

Analysis
Assessment/evaluation
Budget control
Budget development
Coaching
Communication -- written and oral skills
Conceptualization and design
Conflict resolution
Consulting
Counseling
Customer service
Human resource process and employment knowledge
Interpretation of policies/analyses/trends/etc.
Interviewing
Knowledge of applicable laws/policies/principles/etc.
Lead/guidance skills
Managerial skills
Negotiation
Networking
Organization
Planning
Problem identification and resolution
Project management
Public speaking/presentations
Research
Scheduling
Staff development
Statistical analysis
Teaching/training

Skills: Technology:
- Applications/systems development methodologies
- Change management
- Configuration management
- Database design tools and techniques
- Enterprise/information architecture
- Incident/problem management
- Network communications technologies
- Network design, connectivity and capacity configuration
- Operating systems
- Project management tools and techniques
- Release management
- Server applications and hardware
- Technical documentation

Skills: Machine/Equipment:
- Calculator
- Computer network (department or school)
- Computer network (university)
- Fax
- Personal computer
- Photocopier

Supervises: Level:
Manages through subordinate supervisors.

Supervises: Nature of Work:
- Administrative
- Professional/Paraprofessional
- Technical

Comments:
Evening or weekend work may be necessary to meet deadlines or solve specific problems. On call 24/7 to manage problems.

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