**Senior Cyber Security Analyst**

|  |  |
| --- | --- |
| Position Number: | 000TBD Sr Cyber Security Analyst |
| Department: | SITIS |
| Campus: | University of Maine System |
| Date of Issue: | 9-21-17 |

1. Primary Purpose of Position:

The Senior Cyber­ Security Analyst is responsible for proactively defending the integrity, confidentiality and availability of information systems, data resources, and other networked assets. Primary responsibilities include leading the Information Security Office's technical team along with other University partners to prevent, detect, respond, and recover from security incidents; and to develop and operate a distributed security monitoring capability and an incident response team. This individual will be a technical lead for one of the regulatory or industry-adopted compliance programs (e.g. HIPAA, PCI, ITAR).

1. Essential Duties:
   1. Ensure reasonable security practices are employed to protect all information technology assets, including networks, computing systems, virtual/cloud infrastructure, applications, and sensitive or compliant data. Participate in the maturation of the University's information security program.
   2. Analyze business requirements and their information security implications. Work with cross-functional teams to integrate security thinking throughout project lifecycles.
   3. Perform risk, gap and vulnerability assessments of technology environments to ensure adherence to policy and standards via penetration testing, software security lifecycle assessments, and threat modeling. Work with area experts to implement remedial measures.
   4. Maintain current and informed awareness of cyber­ security compromises, their means of entry, effects on systems, and means of prevention. Prepare notices of same. Evaluate legislation, regulations and industry best practices to provide technical and project leadership to staff.
   5. Ensure the University maintains a defensible security posture by monitoring key security events of networks, operating systems, and applications.
   6. Design, implement, and maintain monitoring solutions (e.g. IDS, netflow monitoring, vulnerability scanning system, SIEM alerting) to detect attacks on networked assets.
   7. Be well-versed in incident response best-practices and lead the security incident response team. Train select University staff to act as first responders to a cyber­ security event. Use forensic and malware analysis techniques in responding to incidents. Compile lessons learned to improve security designs.
   8. Respond to alerts and notifications provided by IT and non-IT partners, including from external third-parties and law enforcement.
   9. Investigate and identify solutions to cyber­ security compromises and work with area experts to take corrective action.
2. Non­essential duties:
   1. Maintain a broad knowledge of state-of-the-art technology, equipment and/or practices.
   2. Research new technologies and commercial software/systems for possible use.
   3. Perform other related duties as assigned.
3. Supervisory Responsibilities:

May be responsible for the supervision of part-time student workers.

1. Reporting Relationships:

Reports Chief Information Security Officer

1. Knowledge, Skills, and Abilities:

This position requires some weekend and evening assignments as well as availability during off-hours for participation in schedules and unscheduled activities. The employee must respond to calls after normal hours.

Work will normally be performed at Portland campus of the University of Southern Maine, other university campuses and telecommuting. Unpredictability is inherent in this position, requiring scheduling flexibility. Occasional weekend work or overnight travel may be required.

See qualifications section for additional knowledge, skills, and abilities.

1. Qualifications:

# Required:

A Master's degree in Information Security, Computer Science, Management Information Systems, or related field or an equivalent combination of education and experience is required. In addition to any equivalent experience in lieu of education, more than seven years of professional responsibilities for network, system, or application security.

CISSP, GIAC or equivalent certification

Broad, current knowledge of internet technologies. Professional experience defending networks and managing enterprise network infrastructure. Fluency in the analysis of TCP/IP protocols. Knowledge of host-based network services and their related security risks.

Knowledge of industry standards for cyber­ security monitoring software. Professional experience designing, deploying and maintaining intrusion detection/prevention systems, network flow monitoring, vulnerability management systems, and related network or endpoint monitoring technologies.

Experience auditing or implementing information security frameworks (e.g., ISO 17799/27002, etc.) or legal or industry regulations (e.g. PCI, FERPA, HIPAA).

Knowledge of principles for risk identification and analysis of desktop, server, application, database, and network security.

Knowledge of current cyber­ security issues, and technology developments/trends; Knowledge of the nature and sources of cyber­ security threats and methodologies/technical/requirements for devising solutions.

# Demonstrated excellence in communication (oral, written, presentation), interpersonal, and consultative skills

# Preferred:

# Experience in a higher education environment.

# Knowledge of system management disciplines such as security architecture; disaster recovery and business continuity of operations.

Experience performing network and/or application penetration testing.

Experience performing digital forensics and preserving evidence according to industry best practices.

Signatures: The signatures indicate the employee and immediate supervisor have reviewed the job description and had the opportunity to edit the document.

Employee:

Date:

Immediate Supervisor:

Date:

# US:IT RESERVES THE RIGHT TO ASSIGN REASONABLY RELATED ADDITIONAL DUTIES AND CHANGE OR REASSIGN JOB DUTIES.