Sr Cybersecurity Eng-Central

Job Description

JOB INFORMATION

Job Title:	Sr Cybersecurity Eng-Central
Auburn Title:	Sr Cybersecurity Engineer - Central
Job Code:	MA41
FLSA Classification:	Exempt
Salary Grade:	CS06 $79,800 - $151,600
Organizational use restricted to the following divisions:	*155 - Office of Info Technology*

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

Family Description

This job family manages or performs work associated with analysis, design, implementation, operation, deployment, and support of the organization's information technology resources (including computer hardware, operating systems, communications, software applications, data processing and security), telecommunication systems, and software/database products by internal staff, outsourcing staff, or consultants. Activities include developing information technology strategies, polices and plans; maintenance and use of information technology resources; training and supporting technology users; telecommunications network planning, operations and site acquisition; programming software/database products for sale to external customers; developing PC, online, and mobile games; and internet product management & operations.

Function Description

JOB SUMMARY

Under minimal supervision, serves as technical lead for information technology (IT) security analysis projects and services. Responsible for overseeing and improving the function of the suite of IT security tools utilized by the University to protect the institution's informational assets. Participates in active troubleshooting of data flows as well as evaluates and collaborates on the implementation of new security tools. Functions as the technical and engineering subject matter expert for specific cybersecurity technology areas and is a primary interface to the University's IT community. (Employee must work in central IT unit. Exceptions require CIO prior approval.)

KEY RESPONSIBILITIES

		% TIME
•	Serves as the subject matter expert in operating systems, network devices and protocols, security technologies, cloud technologies, and security data sharing work flows. Leads small projects when necessary.	10%
•	Assists and, at times, leads efforts for incident response activities. Works with vendors to define mitigation strategies when incidents are identified and responded to.	10%
•	Validates and tests information security architecture and design solutions to produce detailed engineering specifications with recommended vendor technologies. Integrates large amounts of intelligence information on threats into context in order to draw insights about the possible implications.	10%
•	Compiles relevant data and integrates data into a coherent whole. Considers the information's reliability, validity, relevance, and time sensitivity.	10%

•	Works with stakeholders to identify strategies to mitigate and remediate vulnerabilities as they are identified.	10%
•	Provides peer level review to work performed by other team members in order to mentor and elevate the team's overall effectiveness.	10%
•	Aides in identifying and evaluating assets, trends, and patterns of threat actors. Performs tailored analysis to develop comprehensive target definition for far-reaching strategic threats to support operational planning and to identify opportunities for neutralizing or degrading activities of threat actors.	10%
•	Trains other team members on new information security solutions and transitions ownership, where possible, upon successful implementation.	10%
•	May serve as a lead within the team, coordinating the work of others and serving as the primary contact.	10%
•	Performs other related duties as assigned by the supervisor.	10%

The above key responsibilities are representative of major duties of positions in this job classification. Specific duties and responsibilities may vary based upon departmental needs. Other duties may be assigned similar to the above consistent with the knowledge, skills and abilities required for the job. Not all of the duties may be assigned to a position and the percent of time spent on each duty varies based on department needs.

MINIMUM QUALIFICATIONS

To perform this job successfully, an individual must be able to perform the minimum requirements listed below. The requirements listed below are representative of the skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the key responisibilities.

Minimum Education and Experience

Education Level	*Field of Study*		*Years of Experience*	*Area of Experience*	
Bachelor's Degree	No specified discipline. Degree in IT or related field suggested. Master's degree in related field preferred.	And	8	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber-attacks.	

Minimum Skills and Abilities

Description	*Proficiency*	
In-depth knowledge of IT architecture, project management, basic vendor relations, proposal writing, business acumen, and quality assurance methodologies.	Advanced	And
Must have team leadership skills, negotiation skills, and advanced client relation skills.	Advanced	And
Ability to remain up-to-date with privacy and security regulations.	Advanced	And
Ability to recognize, analyze, and solve a variety of problems.	Advanced	And
Ability to effectively communicate technical concepts to a non-technical audience.	Advanced	

Minimum Technology

Technology	*Technology Details*	
Strong technical aptitude and computer skills.		

Minimum Licenses and Certifications

Licenses/Certifications	*Licenses/Certification Details*	*Time Frame*	
Certified Information Systems Security Professional (CISSP) Certification required.		Upon Hire	

Approved Date: 11/10/2019