
Auburn University Job Description

Job Title: **Sr Cybersecurity Eng-Central**

Job Family: No Family

Job Code: **MA41**

CS04: \$85,400 - \$136,600

FLSA status: Exempt

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.)

Essential Functions

1. 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.
2. Assists and, at times, leads efforts for incident response activities. Works with vendors to define mitigation strategies when incidents are identified and responded to.
3. 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.
4. Compiles relevant data and integrates data into a coherent whole. Considers the information's reliability, validity, relevance, and time sensitivity.
5. Works with stakeholders to identify strategies to mitigate and remediate vulnerabilities as they are identified.
6. Provides peer level review to work performed by other team members in order to mentor and elevate the team's overall effectiveness.
7. 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.
8. Trains other team members on new information security solutions and transitions ownership, where possible, upon successful implementation.
9. 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.

Supervisory Responsibility

May be responsible for training, assisting or assigning tasks to others. May provide input to performance reviews of other employees.

Auburn University Job Description

The above essential functions 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.



Auburn University Job Description

Minimum Required Education and Experience

	<u>Minimum</u>	<u>Focus of Education/Experience</u>
Education	Four-year college degree	No specified discipline. Degree in IT or related field suggested. Master's degree in related field preferred.
Experience (yrs.)	8	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber-attacks.

Substitutions allowed for Education:

Indicated education is required; no substitutions allowed.

Substitutions allowed for Experience:

Indicated experience is required; no substitutions allowed.

Minimum Required Knowledge

In-depth knowledge of IT architecture, project management, basic vendor relations, proposal writing, business acumen, and quality assurance methodologies.

Must have team leadership skills, negotiation skills, and advanced client relation skills.

Ability to remain up-to-date with privacy and security regulations.

Ability to recognize, analyze, and solve a variety of problems.

Ability to effectively communicate technical concepts to a non-technical audience.

Certification or Licensure Requirements

Certified Information Systems Security Professional (CISSP) Certification required.

Physical Requirements/ADA

No unusual physical requirements. Requires no heavy lifting, and nearly all work is performed in a comfortable indoor facility.

Routine deadlines; usually sufficient lead time; variance in work volume seasonal and predictable; priorities can be anticipated; some interruptions are present; involves occasional exposure to demands and pressures from persons other than immediate supervisor.

Job frequently requires sitting, talking, hearing, .

Job occasionally requires standing, walking, reaching, handling objects with hands, and lifting up to 50 pounds.

Vision requirements: Ability to see information in print and/or electronically, ability to distinguish colors.

Date: 11/1/2020
