AUBURN
Human Resources

Senior Cybersecurity Analyst, McCrary

Job Description

JOB INFORMATION

Job Code	JA32
Job Description Title	Senior Cybersecurity Analyst, McCrary
Pay Grade	CS04
Range Minimum	$73,560
33rd %	$93,180
Range Midpoint	$102,980
67th %	$112,790
Range Maximum	$132,410
Exemption Status	Exempt
Organizational use restricted to the following divisions	128 Samuel Ginn Col of Engineering
Approved Date:	11/5/2025 4:48:09 PM

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

The Senior Cybersecurity Analyst is a trusted operator and emerging leader within McCrary's SOC/ISAC environment. Provides advanced threat hunting, incident response, automation initiatives, and operational support for state and local partners and customers. Acts as a key integrator that bridges day-to-day security operations with applied research and field deployment teams to deliver innovative and resilient cybersecurity solutions. Blends deep technical capability with the ability to communicate complex concepts clearly to diverse audiences, including non-technical partners, executives, and critical infrastructure stakeholders..

RESPONSIBILITIES

- Directs high complexity incident response operations, leading containment, eradication, and recovery efforts while ensuring rapid, coordinated, and technically sound resolution of security events.
- Applies research driven methodologies to enhance detection, response, and post incident analysis.
- Conducts sophisticated threat hunting operations informed by emerging research, adversary tradecraft, and evolving threat landscapes.
- Develops actionable threat intelligence products tailored for state agencies, critical infrastructure operators, and mission focused partners.
- Architects, develops, and optimizes SOAR playbooks and automated workflows to improve SOC efficiency and reduce analyst workload.
- Prototypes and evaluates new automation techniques, integrating research findings into operational capabilities.
- Leads comprehensive security assessments, vulnerability research, and red/blue team aligned evaluations.
- Designs and facilitates cyber tabletop exercises that translate complex technical risks into clear operational insights for non-technical participants.
- Produces high quality technical reports, research briefs, incident summaries, and executive level presentations.
- Distills complex cybersecurity concepts into accessible explanations for non-technical customers, leadership, and cross disciplinary teams.
- Mentors students/interns, junior analysts, and early career engineers, fostering a culture of technical excellence, curiosity, and continuous learning.
- Provides expert guidance on advanced analysis techniques, research methodologies, and cybersecurity best practices.

RESPONSIBILITIES

- Supports the design, testing, and integration of lab developed cybersecurity tools, prototypes, and research outputs into operational SOC environments.
- Evaluates emerging technologies and contribute to long term capability roadmaps.
- Performs additional duties aligned with advancing the institute’s cybersecurity research mission and strengthening partner resilience.

The responsibilities listed above show the typical duties for jobs in this classification. Actual tasks may differ depending on the department's needs. Other similar duties may be assigned with discretion of the supervisor. Not every duty will apply to every position, and the amount of time spent on each task can change based on department needs.

SUPERVISORY RESPONSIBILITIES

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

MINIMUM QUALIFICATIONS

To be eligible, an individual must meet all minimum requirements which are representative of the knowledge, skills, and abilities typically expected to be successful in the role. For education and experience, minimum requirements are listed on the top row below. If substitutions are available, they will be listed on subsequent rows and may only to be utilized when the candidate does not meet the minimum requirements.

MINIMUM EDUCATION & EXPERIENCE

Education Level	Focus of Education		Years of Experience	Focus of Experience	
Bachelor's Degree	Cybersecurity, Computer Science, or IT.	and	4 years of	cybersecurity operations or incident response experience.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Effective communicator and presentation experience.	And
Customer service experience.	And
Ability to work effectively with a team.	And
Ability to explain technical problems and solutions to non-technical clientele.	And
Experience in performing incident response and security monitoring processes and tools.	And
Proficiency in scripting and programming languages.	And
Ability to analyze malware behavior and low-level code execution.	And
Fundamental understanding of ports and protocols.	And
Experience with enterprise network and security infrastructure.	And
Experience using Security Information and Event Management (SIEM) tools	And
Experience using Open Source Intelligence (OSINT) tools	And
Understanding of security policies and operational procedures.	And
Strong analytical thinking and problem-solving capabilities.	And
Project management experience.	And
Effective communication skills for technical documentation and interdisciplinary collaboration.	And
Proficiency with SIEM/EDR tools, threat hunting techniques, and security automation.	And
Strong knowledge of ICS/OT (Industrial Control Systems / Operational Technology) environments.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
Other	GCIA, GCIH, GCFE, GCFA, Security+, CCNA CyberOps, OSCP, GPEN, GWAPT, CEH, CISSP or		Desired	And

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
	other equivalent certifications			

PHYSICAL DEMANDS & WORKING CONDITIONS

Physical Demands Category:	Other

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
Standing			X			
Walking			X			
Sitting				X		
Lifting	X					
Climbing		X				
Stooping/ Kneeling/ Crouching		X				
Reaching			X			
Talking					X	
Hearing					X	
Repetitive Motions			X			
Eye/Hand/Foot Coordination			X			

WORKING ENVIRONMENT

Working Condition	Never	Rarely	Occasionally	Frequently	Constantly
Extreme cold		X			
Extreme heat		X			
Humidity		X			
Wet		X			
Noise		X			
Hazards		X			
Temperature Change		X			
Atmospheric Conditions		X			
Vibration		X			

Vision Requirements:

Ability to see information in print and/or electronically and distinguish colors.