Cyber Defense Analyst

MONTGOMERY COLLEGE

	Cyber Defense Analyst I	Cyber Defense Analyst II
Grade	**31**	**33**
Job Class Level	This is developmental level work, responsible for less complex assignments of assessments of systems and networks against vulnerabilities; using data collected from cyber defense tools to analyze events; and investigating, analyzing, and responding to cyber incidents within the College environment.	This is senior level work, responsible for performing assessments of systems and networks against vulnerabilities; using data collected from cyber defense tools to analyze events; and investigating, analyzing, and responding to cyber incidents within the College environment.
Education (Minimum)	Associate's degree with course work in cybersecurity, computer science or a related field, and/or any combination of education, training and experince.	Bachelor's degree course work in cyber security and information technology or a related field.
Yrs. of Experience (Minimum)	• 1 year of work experience in cybersecurity as an analyst or engineer. • Experience in various aspects of information technology as an analyst/programmer or similar professional level • Experience in incident handling/response and disaster recovery planning. • Experience in system, network, and OS hardening.	• 3 years of work experience in various aspects of information technology as an analyst/programmer or similar professional level, including systems administration, networking and/or application development. • 3 years of work experience in cybersecurity as an analyst or engineer. • Experience in incident handling/response and disaster recovery planning. • Experience in system, network, and OS hardening.
Certifications (Required)	None	None
Training (Required)	None	None
Knowledge (Required)	• Knowledge of network protocols and directory services. • Basic knowledge of how to use network analysis tools to identify vulnerabilities. • Knowledge of Microsoft and/or UNIX platforms and TCP/IP networking. • Basic knowledge of: penetration testing principles, tools, and techniques; risk management processes (e.g., methods for assessing and mitigating risk); cybersecurity principles, cyber threats and vulnerabilities; information classification program and procedures of information compromise; computer-based training and e-learning systems; and organizational training systems.	• Strong knowledge of network protocols and directory services. • Knowledge in the use of network analysis tools to identify vulnerabilities. • Strong knowledge of Microsoft, and/or UNIX platforms and TCP/IP networking. • Knowledge of: penetration testing principles, tools, and techniques; risk management processes. • Thorough knowledge of cybersecurity principles, cyber threats and vulnerabilities; information classification program and procedures of information compromise; computer-based training and e-learning systems; and organizational training systems. • Thorough knowledge of basic system, network, and OS hardening techniques.
Role Summary	• Performs basic assessments of systems and networks within the College environment and identifying where those systems/networks deviate from acceptable configurations or College policy. • Assignments of greater complexity are performed as an incumbent gains knowledge and experience. • Participates in measuring the effectiveness of defense-in-depth architecture against known vulnerabilities and uses data collected from cyber defense tools to analyze events and mitigate threats. • Participates in investigating, analyzing, and responding to cyber incidents.	• Performs assessments of systems and networks within the College environment and identifying where systems/networks deviate from acceptable configurations or College policy. • Measures the effectiveness of defense-in-depth architecture against known vulnerabilities and uses data collected from cyber defense tools to analyze events and mitigate threats. • Investigates, analyzes, and responds to cyber incidents.
Level of Autonomy	Under moderate supervision	Under general supervision
Core Functions	• Assist with security reviews and identifying security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy. • Participate in planning and recommending modifications or adjustments based on exercise results or system environment. • Participate on the Incident Response Team; coordinate with cyber defense staff to validate network alerts; document and escalate incidents • Examine network topologies to understand data flows through the network. • Conduct vulnerability scanning activities on systems across the enterprise. Recommend computing environment vulnerability corrections. • Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. • Assess adequate access controls based on principles of least privilege and need-to-know.	• Ensures cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. • Performs security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy. • Plans and recommends modifications or adjustments based on exercise results or system environment. • Conducts vulnerability scanning activities on systems across the enterprise. • Recommends computing environment vulnerability corrections. • Validates intrusion detection system (IDS) alerts against network traffic using packet analysis tools. • Monitors external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
Core Skills	• Service orientation • Proactive • Planning / coordination / organization • Time management • Verbal and written communication • Technology literacy: office suite software, ERP software, social media • Problem Solving • Strives to Learn • Cooperation	• Service orientation • Proactive • Planning / coordination / organization • Time management • Verbal and written communication • Technology literacy: office suite software, ERP software, social media • Cooperation • Analytical Thinking • Coordination • Guidance • Mentoring
Core Competencies (Proposed)	• Accuracy and thoroughness • Collaboration • Adaptable • Innovative • Integrity • Initiative • Critical thinking • Decision making / problem solving • Strive to learn • Communication • Service orientation • Anticipate stakeholders needs and take appropriate action • Leadership	• Accuracy and thoroughness • Collaboration • Adaptable • Innovative • Integrity • Initiative • Critical thinking • Decision making / problem solving • Strive to learn • Communication • Service orientation • Anticipate stakeholders needs and take appropriate action • Leadership

HRSTM-Nov-2019