Cyber Defense Infrastructure Engineer

MONTGOMERY COLLEGE

	Cyber Defense Infras Engineer I	Cyber Defense Infras Engineer II
Grade	31	33
Job Class Level	This is developmental level work, responsible for less complex assignments of testing, implementing, deploying, maintaining, and administering security infrastructure hardware and software	This is senior level work, responsible for testing, implementing, deploying, maintaining, and administering security infrastructure hardware and software.
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 with course work in cybersecurity and computer science 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: installing and maintaining commercial software products, and incident handling/response. • Experience and/or training in use of enterprise level networking equipment (switches, routers, etc.).	• 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: installing and maintaining commercial software products; incident handling/response, and disaster recovery planning. •Experience and/or training in use of the networking equipment (switches, routers, etc.) used at the College.
Certifications (Required)	None	Professional certification in information security - GSEC, CISSP, CISA, etc.
Training (Required)	None	None
Knowledge (Required)	• Knowledge of network security architecture concepts including topology, protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)), components, and principles. • Knowledge of Microsoft, Novell, and/or UNIX platforms and TCP/IP networking. Familiarity with packet-level analysis; risk management processes (e.g., methods for assessing and mitigating risk). • Knowledge of cybersecurity principles, cyber threats and vulnerabilities, host/network access control mechanisms (e.g., access control list). • Familiarity with Virtual Private Network (VPN) security. • Knowledge of basic system, network, and OS hardening techniques. • Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications, incident response, handling methodologies, event logging, and Security Incident and Event Management (SIEM) systems.	• Strong knowledge of network security architecture concepts including topology, protocols, directory services, components, and principles. • Strong knowledge of Microsoft, Novell, and/or UNIX platforms and TCP/IP networking. • Strong knowledge of packet-level analysis; risk management processes. • Thorough knowledge of cybersecurity principles, cyber threats and vulnerabilities. • Strong knowledge of host/network access control mechanisms, Virtual Private Network (VPN) security. • Thorough knowledge of basic system, network, and OS hardening techniques. • Strong knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. • Strong knowledge of incident response and handling methodologies, event logging, and Security Incident and Event Management (SIEM) systems.
Role Summary	• Performs basic testing, implementing, deploying, maintaining, and administering the security infrastructure hardware and software. • Assignments of greater complexity are performed as an incumbent gains knowledge and experience. • Responds to and investigates security incidents, including external/internal attacks and internal violations of policy	• Tests, implements, deploys, maintains, and administers the security infrastructure hardware and software. • Responds to and investigates security incidents, including external/internal attacks and internal violations of policy, and promotes security awareness via seminars, written materials and other media.
Level of Autonomy	Under moderate supervision	Under general supervision
Core Functions	• Assists with identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources. • Assists with assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure. • Administers test bed(s), tests and evaluates applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). • Coordinates with other IT security personnel to manage and administer the updating of rules and signatures (e.g., firewalls, intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications. • Performs system administration on specialized cyber defense applications and systems (e.g., anti-virus, audit and remediation) Virtual Private Network (VPN) devices and load balancers, to include installation, configuration, maintenance, backup and restoration.	• Coordinates with other IT security personnel to manage and administer the updating of rules and signatures (e.g., firewalls, intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications. • Performs system administration on specialized cyber defense applications and systems (e.g., anti-virus, audit and remediation) Virtual Private Network (VPN) devices and load balancers • Identifies prioritizes, and coordinates the protection of critical cyber defense infrastructure and key resources. • Builds, installs, configures, and tests dedicated cyber defense hardware. • Configures cyber defense tools to provide appropriate logging of events to a central logging server or Security Incident and Event Management (SIEM) system.

Cyber Defense Infrastructure Engineer

MONTGOMERY COLLEGE

	Cyber Defense Infras Engineer I	Cyber Defense Infras Engineer II
Grade	**31**	**33**
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