Code: 06E5
Family: IT-Engineer
Service: Administrative
Group: Clerical, Accounting, and General Office
Series: Information Technology

CLASS TITLE: CLOUD SECURITY ENGINEER

CHARACTERISTICS OF THE CLASS

Under supervision, primarily responsible for building and maintaining a cloud environment for hosting security tools and for maintaining the cloud security tools that are used to secure cloud environments. Protects City of Chicago systems against advanced persistent threats from cyberspace by defending against hacking, malware and ransomware, and cybercrime. Also involved in tool management, scripting, log analysis, controls design, threat analysis, and incident response.

This class is assigned to the Engineer Information Technology Job Family which consists of engineers and developers that design, build, test, deploy, and support IT products and solutions.

ESSENTIAL DUTIES

- Designs, analyzes, implements, and supports secure network solutions, routers, firewalls, application development environments and operating systems specific to cloud environments
- Develops secure systems and performs assessments and penetration testing
- Manages security technology and audit/intrusion systems and develops secure network solutions to protect against persistent threats
- Provides technical support for routine security services and participates in 24/7 on-call rotations
- Implements security solutions for intrusion detection and notification, security auditing, alert and response, virus detection and removal, password complexity enforcement, and media protection
- Verifies security systems by developing and implementing test scripts and running security scans
- Validates baseline security configurations for operating systems, applications, networking, and telecommunications equipment
- Works with developers to respond to escalated problem from Technical Administrators or other Engineers
- Partners with other stakeholders to keep them informed about network security problems and resolutions
- Maintains City of Chicago's IT standards across systems security
- Administers technology used in support of cybersecurity efforts (e.g., firewalls, intrusion detection/prevention systems, endpoint detection and response solutions, web application firewalls and security and event management systems)
- Responds to cybersecurity incidents, participates in penetration and vulnerability testing, cybersecurity audits, and assists with remediation of cybersecurity vulnerabilities
- Recognizes that telemetry for security products will increasingly be curated in the cloud and be prepared to develop API endpoints and connections to collect and collate this knowledge

***NOTE**: The list of essential duties is not intended to be inclusive; there may be other duties that are essential to particular positions within the class.*

MINIMUM QUALIFICATIONS

Education, Training, and Experience

- Graduation from an accredited college or university with a Bachelor's degree, two (2) years' experience securing cloud environments, plus two (2) years of experience in computer science, cybersecurity, systems administration, networking, DBA, design and support or an equivalent combination of education, training, and experience

Licensure, Certification, or Other Qualifications

- One or more cloud certification such as: AWS Certified Solutions Architect – Associate, Microsoft Certified: Azure Solutions Architect Expert, Certified Cloud Security Professional (CCSP)
- Information Security Certifications such as: CompTIA: Security+, GIAC Certification: GCWN, GSEC, ISC2: CISSP, SSCP, CCSP, Cloud Security Alliance: CCSK

WORKING CONDITIONS

- General office environment

EQUIPMENT

- Standard office equipment (e.g., phone, printer, copier, computers, mobile devices)
- Standard productivity suites (e.g., Microsoft Office Suite, OpenOffice, Google Workspace)

PHYSICAL REQUIREMENTS

- No specific requirements

KNOWLEDGE, SKILLS, ABILITIES, AND OTHER WORK REQUIREMENTS

Knowledge

Comprehensive knowledge of:

- *information security principles and an understanding of the Cyber Kill Chain, MITRE ATT&CK, Zero Trust and other security defense and intelligence frameworks
- *IT/Security infrastructure
- *Amazon Web Services, Azure, Google Cloud Platform
- *Native and third-party cloud security tools (e.g., AWS Security Hub, Azure Security Centre)
- leading coding, networking and network security, threat modeling, and testing skills

Moderate knowledge of:

- common controls used in frameworks such as NIST CSF,NIST 800-53, NIST 800-171 and ISO 27002
- SAST/DAST and SDLC frameworks
- Identity and Access Management (IAM)

Knowledge of applicable City and department policies, procedures, rules, and regulations

Skills

- ACTIVE LEARNING - Understand the implications of new information for both current and future problem-solving and decision-making

- ACTIVE LISTENING - Give full attention to what other people are saying, take time to understand the points being made, ask questions as appropriate, and not interrupt at inappropriate times
- CRITICAL THINKING - Use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions, or approaches to problems
- COMPLEX PROBLEM SOLVING - Identify complex problems and review related information to develop and evaluate options and implement solutions
- TIME MANAGEMENT - Manage one's own time or the time of others
- COORDINATION WITH OTHERS - Adjust actions in relation to others' actions
- JUDGEMENT AND DECISION MAKING - Consider the relative costs and benefits of potential actions to choose the most appropriate one
- SYSTEMS ANALYSIS - Determine how a system should work and how changes in conditions, operations, and the environment will affect outcomes

Abilities

- COMPREHEND ORAL INFORMATION - Listen to and understand information and ideas presented through spoken words and sentences
- SPEAK - Communicate information and ideas in speaking so others will understand
- COMPREHEND WRITTEN INFORMATION - Read and understand information and ideas presented in writing
- WRITE - Communicate information and ideas in writing so others will understand
- CONCENTRATE - Concentrate on a task over a period of time without being distracted
- RECOGNIZE PROBLEMS - Tell when something is wrong or is likely to go wrong
- REASON TO SOLVE PROBLEMS - Apply general rules to specific problems to produce answers that make sense
- COME UP WITH IDEAS - Come up with a number of ideas about a topic
- MAKE SENSE OF INFORMATION - Quickly make sense of, combine, and organize information into meaningful patterns
- REACH CONCLUSIONS - Combine pieces of information to form general rules or conclusions (includes finding a relationship among seemingly unrelated events)

Additional Competency Requirements

- COMMUNICATION FOR RESULTS – Writes, speaks and presents effectively. Explains the immediate context of the situation, asks questions with follow-ups and solicits advice prior to taking action. Develops presentations to influence others by using graphics, visuals or slides that display information clearly. Listens and asks questions to understand other people’s viewpoints.
- GROWTH MINDSET – Takes ownership of personal growth. Identifies knowledge gaps. Asks questions of subject matter experts and seeks help when needed. Keeps abreast of information, developments and best practices within a field of expertise (e.g., by reading, interacting with others or attending learning events).
- INITIATIVE – Volunteers to undertake tasks that stretch his or her capability. Identifies who can provide support and procures their input. Identifies problems and acts to prevent and solve them.

- OWNERSHIP AND COMMITMENT – Volunteers to undertake tasks that stretch his or her capability. Checks the scope of responsibilities of self and others. Monitors day-to-day performance and takes corrective action when needed to ensure desired performance is achieved. Identifies problems and acts to prevent and solve them. Identifies who can provide support and procures their input.
- NETWORK TECHNOLOGY KNOWLEDGE – Applies and interprets the fundamental principles of network technology. Solves day-to-day networking problems. Undertakes routine preventive maintenance and troubleshooting on components used in voice and data networking. Reports on problems and may recommend appropriate remedial action.
- ANALYTICAL THINKING – Gathers and links data. Breaks down tasks and problems into manageable components. Reviews for nonconformity and gathers further information in response to routine problems. Solicits guidance as needed to assess importance and urgency.
- CUSTOMER PARTNERSHIP – In response to requests for new types of assistance, refers representatives of the customer to the appropriate IT contact. Gathers information about customers' business and technology products and services. Solicits customer recommendations for improved day-to-day functionality and translates simpler recommendations into technical business requirements.
- INFORMATION SEEKING – Gathers and analyzes information or data on current and future trends of best practice. Uses appropriate tools, techniques and sources to gather, update and monitor information. Checks for accuracy of interpretation. Seeks out the appropriate people for guidance when needed, depending on the type of issue.
- OUTCOME DRIVEN – Responds quickly and effectively to instructions and requests. Seeks guidance on priorities and goals. Applies effort that is commensurate with the outcome.
- PROCESS ORIENTATION – Understands key work processes within own functional area. Follows defined processes as required to accomplish assigned work. Identifies opportunities for process improvement and modifies own work style and approach to incorporate changes.
- SYSTEMS THINKING – Investigates the critical relationships between primary business, technology and system platforms. Devises approaches that recognize the interdependencies of key system components.
- THOROUGHNESS – Performs tasks according to quality and output standards. Takes initiative to ensure that outcomes meet internal and external customer requirements. Solicits feedback on performance of new tasks. Measures accuracy using performance metrics. Sets improvement standards to reduce errors, omissions and oversights.

Other competencies as required for successful performance in the lower-level series.

All employees of the City of Chicago must demonstrate commitment to and compliance with applicable state and federal laws, and City ordinances and rules; the City’s Ethics standards; and other City policies and procedures.

The City of Chicago will consider equivalent foreign degrees, accreditations, and credentials in evaluating qualifications.

* May be required at entry.

City of Chicago
Department of Human Resources
March 2023