Code: 06K2
Family: IT-Engineer
Service: Administrative
Group: Clerical, Accounting, and General Office
Series: Information Technology

CLASS TITLE: SENIOR 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 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
- Verifies security systems by developing and implementing test scripts and running security scans
- Validates baseline security configurations for cloud environments
- Works with developers to respond to escalated problems from Technical Administrators or other Engineers
- Partners with stakeholders to keep them informed about security problems and resolutions
- Maintains City of Chicago's IT standards across systems security
- 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
- Assess and propose solutions regarding cloud security to Information Security Office leadership
- Perform architectural and design reviews through the security lens leveraging policy and best practices providing timely, actionable requirements and recommendations
- Remain current on cloud technologies and best practices to secure them

***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 in Computer Science, Cybersecurity, Information Systems or a directly related field, plus four (4) years experience securing cloud environments, 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) or Google Professional Cloud Security Engineer
- One or more 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

Considerable 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 27001 / 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.
- BUSINESS FUNCTION KNOWLEDGE – Involves the key players in identifying operating needs, issues and solutions. Proposes technical plans that are aligned with business objectives

and technical requirements. Takes and leads actions to enhance business function standards and performance with the participation of business and technical partners.

- ANALYTICAL THINKING – Undertakes a process of information and data collection and analysis for integration purposes. Identifies and makes sets of information and determines their relationships. Makes logical deductions from data. Identifies a solution for resolving the problem.
- CONSULTING – Shares information and reports on the immediate situation. Provides feedback and advice as appropriate in relation to procedures and routine activities. Asks questions that raise awareness and demonstrate insight.
- INFORMATION SEEKING – Utilizes a variety of information and data sources pertaining to organizational and professional trends. Checks the source for omission and accuracy. Identifies the sources that are appropriate for specific types of information. Checks for bias and omission. Seeks out the appropriate people to approach for guidance either formally or informally depending on the type of issue. Links information in a lateral as well as linear manner. Finds hidden data. Relates and manipulates data from various sources to create a fuller picture. Investigates and uncovers root causes of a problem or issue.
- INFORMATION SYSTEMS KNOWLEDGE – Possesses a basic understanding of the strategy, structures, processes and procedures of the enterprise in its relationship with the business and its activities. Troubleshoots in response to requests for technical support. Identifies problems and needs. Escalates problems to appropriate technical experts.
- OUTCOME DRIVEN – Establishes specific performance standards and measures for own work. Assesses performance against metrics, deadlines and quality. Ensures that personal performance meets the standards and expectations of internal and external customers, as well as the organization.
- RISK MANAGEMENT – Uses a risk analysis as a way to understand the organization's environment and his or her own work, and adjusts accordingly. Assesses risk and applies risk management strategies to mitigate it.

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