UNICOM Engineering, Inc.
A Division of UNICOM Global

JOB TITLE: Cyber Security Architect

DEPARTMENT:	IT Infrastructure
REPORTS TO:	Vice President, IT Infrastructure
FLSA:	Exempt
JOB GRADE:	24
DATE:	June 2021

SUMMARY:

As a senior member of the IT Infrastructure team, a Cyber Security Architect plans and designs security solutions and capabilities that enable the organization to identify, protect, detect, respond, and recover from cyber threats and vulnerabilities. Defines and develops security requirements using risk assessments, threat modeling, testing, and analysis of existing systems. Develops security integration plans to protect existing infrastructure and to incorporate future solutions. Designs action plans for policy creation and governance, system hardening, monitoring, incident response, disaster recovery, and emerging cybersecurity threats.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

- Consult with other members of the IT team and stakeholders to encourage the adoption of security-compatible software designs and best practices
- Utilizes a variety of security information and event management (SEIM), data loss prevention (DLP), intrusion prevention systems (IPS), and other tools to analyze critical systems for vulnerabilities
- Monitors, analyzes, and alerts organization of emerging security threats and related vulnerabilities.
- Keeps abreast of the latest intelligence from law enforcement and other sources of cyber threat information
- Recommends appropriate actions, safeguards, and notifications.
- Performs risk reviews, identifies risk treatment plans, and monitors identified risks to ensure risks are properly addressed.
- Help maintain and update ISO 27001 practices and treatment plans as related to IT systems and participates in internal and external security audits.
- Provide assistance with security requirements review in contracts, RFPs, and security questionaries as related to IT systems and infrastructure
- Helps develop, implement, and update Security Awareness training for the organization, including phishing campaigns, results analysis, and recommending improvements based on results.
- Represents the Information Security Program by participating in technical advisory groups, project teams, and relevant cross functional teams.
- Provide guidance on the design, implementation, management, and maintenance of enterprise security infrastructure, including firewalls, intrusion detection and prevention systems, virtual private networks, vulnerability scanning systems, penetration testing, access control systems and forensics analysis.
- Continually researches and provides suggestions to improve security procedures and guidelines for various topics, such as data classification, system

configuration, malware protection, access control, encryption, risk assessment, and disaster recovery.
- Ensures regularly scheduled disaster recovery tests are performed and any identified gaps are appropriately addressed.
- Provides technical leadership and project management for security related projects.
- Provides leadership and guidance in security incident response activities.
- Oversees computer forensics investigations to establish timelines, determine root cause, and identify data exposures, and recommends corrective actions.
- Develops and manages written content in support of the team's documentation, communication, and education goals.
- Learns about Company's business as appropriate.
- Shows up to work on time and attends work as scheduled.
- All other duties as requested by direct manager.

COMPETENCY QUALIFICATIONS:

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. If an employee does not meet the required competency level in any area, a required development training plan will be implemented.

Job-Specific Competencies:

(Education and/or years of experience; technical and/or analytical; software or applications; department and/or position specific; internal or external certifications required)

- BS Degree, preferably in Computer Science, Engineering, or equivalent work experience.
- 7+ years of IT related experience
- 5+ years of experience in Cyber Security or related fields
- Security certification(s) such as Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM)
- Solid understanding of Hybrid Cloud enterprise environments
- Experience with multi-site network and WAN infrastructure typologies
- Experience with Microsoft Infrastructure, including Azure AD, Windows Server, Hyper-V, and Azure Cloud architecture
- Familiarity with Cisco firewall, VPN, and SD-WAN solutions a plus
- Ability to work independently and collaboratively across various functional groups.
- Strong oral and written communication skills.
- Proficiency in MS Office365.
- Ability to multi-task and to adapt to changing priorities.
- Ability to follow all applicable Business Management System (BMS) processes.

Management Competencies:

(Management experience required)

- None

Core Competencies:

(Other core requirements including communication, presentation, language, math, and reasoning skills)

- Ability to read, write and speak English;
- Ability to compose reports and correspondence.
- Ability to define problems, collect data, establish facts, and draw valid conclusions.

- Know and follow established company core values.

PHYSICAL DEMANDS:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is regularly required to use hands to finger, handle, or feel objects, tools, or controls; reach with hands and arms; to sit, stand, walk; and to talk and hear. Specific vision abilities required by this job include close vision and the ability to adjust focus.

- Lifting Requirement: 20 pounds
- Lifting Limitations: 50 pounds

WORK ENVIRONMENT:

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- The noise level in the work environment is usually moderate.