Franklin County
Data Center

Franklin County Data Center
Job Posting

$82,590-$107,397 **Excellent Benefits Package

JOB TITLE: Security Engineer

SUMMARY

The Franklin County Data Center is seeking a Senior Security Engineer which will have responsibilities in both security operations and security engineering. This position will report to the Senior Security Engineer. The Security Engineer is expected to have experience in information security and network administration, with Internet Protocol (IP), firewalls, encryption, intrusion detection systems, web filtering, authentication, and authorization methodologies. The Security Engineer will assist the Senior Security Engineer with preserving the confidentiality, integrity, availability, and non-repudiation of County information resources. The Security Engineer must demonstrate effective communication skills and be able to assist with the development of communication strategies and the execution of security strategies. Must successfully complete a 180-day probationary period.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Include the following. Other duties may be assigned.

Security Operations
This position will be the major role in the ongoing security operations and day to day security activities. The Security Engineer will also assist with the development and coordination of a dedication Security Operations Center (SOC).

Policy
Lead the effort for development of security policies and integration into ServiceNow IT GRC. Work with the Senior Security Engineer to execute on security policies and procedures. Review current policies and is responsible for the ongoing updates.

Governance and Enforcement
Assist the Senior Security Engineer in ongoing reporting and monitoring. Responsible for integration with systems and the automatic generation of reports. Responsible for the execution of the comprehensive security program.

Vulnerability Management
Responsible for the execution of the vulnerability management program. The vulnerability program will include, but is not limited to, external and internal networking, servers, pc's, and wireless devices. This position will also be responsible for ongoing security scanning and routine remediation efforts.

Incident Response
Responsibilities include the execution of the defined incident response program in conjunction with the appropriate staffing model.

Security Awareness Training
Assist the Senior Security Engineer with the security awareness training and will play a large role in the implementation of training county wide. This role may be required to assist with the development of, and execution of, a communication strategy for security awareness training.

Security Tools

Serve as subject matter expert or have base familiarity for the following security tools and security areas:

- Tenable Security Center Continuous View
- ServiceNow IT GRC
- SecureWorks IDS/IPS
- Elevated account management tools
- Firewall systems
- Web and content filtering
- Log correlation engines
- End point (anti-virus, malware, and related end point threats)
- Mobile Device Management (MDM) tools
- PHI, PII, PCI, and sensitive data

SUPERVISORY RESPONSIBILITIES

This position will be responsible for supervisory activities as assigned by the Senior Security Engineer and act as a backup when the Security Engineer is not available.

Off-hours support is expected and have the ability to respond to security events during off hours.

QUALIFICATIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily and be a reliable presence on site, maintaining appropriate business hours. 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.

- Proven working experience building and maintaining security systems.
- Excellent analytical and problem-solving skills.
- Good technical knowledge of security industry best practices and procedures.
- Experience with network technologies and with system, security, and network monitoring tools.
- Familiarity with web related technologies (Web applications, web services, service oriented architectures) and of network/web related protocols.
- Hands-on experience in security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc.
- Problem solving skills and ability to work under pressure.
- Understanding of the system hardening processes, tools, guidelines and benchmarks.
- Hands-on experience with vulnerability scanning, firewall, antivirus & malware analysis, proxy, IDS/IPS, log correlation tools, Data Privacy, SIEM, DLP, and other related tools.

EDUCATION and/or EXPERIENCE

- Bachelor's degree from four-year college or university with courses in computer science, cyber security, application programming languages, development tools, systems analysis and systems design; or equivalent combination of education and experience.
- Prior development experience is preferred.
- CISSP or CISM certification.
- Experience with and knowledge of NIST 800-53.

- 10+ years of hands on experience in IT security.
- Demonstrated proficiency in PowerShell

LANGUAGE SKILLS

- Ability to read, analyze, and interpret general business periodicals, professional journals, technical procedures, or governmental regulations.
- Ability to write reports, business correspondence, and procedure manuals.
- Ability to effectively present information and respond to questions from groups of managers, clients, customers, agencies, elected officials, and the general public.

REASONING ABILITY

- Ability to define problems, collect data, establish facts, and draw valid conclusions.
- Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

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.

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.

Data Center Benefits Summary:
Medical, Vision, Life, Mental Health, Direct Deposit, Credit Union, Deferred Comp, Retirement, Sick and Vacation Accrual, Tuition Reimbursement
EEO **No fees**