JOB OPENING ANNOUNCEMENT

Apply On-line at https://www.caltrain.com/about/Jobs.html

Employment Hotline (650) 508-6308

May 20, 2022

TITLE:	**Cyber Security Analyst**
EMPLOYMENT TYPE:	**Exempt (Full-Time)**
DIVISION:	**Rail Development (Network Engineering)**
APPLICATION DEADLINE:	**Continuous Recruitment (Open until filled)**
PAY RANGE:	**$1,914 - $2,871 per week ($99,511 to $149,267 est. annual)**
WORK LOCATION:	**San Carlos, California**
WORK SCHEDULE:	**Hybrid Work Schedule**

JOB SUMMARY: The Cybersecurity Analyst reports to the Manager, Network Engineering, and is responsible for the oversight and implementation of the Districts rail network infrastructure and provides technical and engineering design support for complex cross-functional network and cybersecurity projects within the District. Manages and develops connectivity solutions utilizing the district's fiber optic infrastructure; develops and implements standards and procedures for the District's PTC, PCEP, and other rail network systems; develops security policy, compliance and design strategy for the security of the District's enterprise network and systems; works to improve the security posture of district owned sites & facilities, as well as develop threat modeling, coordination of application security requirements, and strategic application security remediation using a wide variety of hardware and software tools.

EXAMPLES OF ESSENTIAL FUNCTIONS:

- Lead the security compliance efforts and conduct periodic audits, regular penetration testing, and remediation in accordance with TSA, DHS, and CISA requirements. Take charge ensuring data security, mitigating cyber security risks, and safeguarding SMCTD's computer networks, Operations (Train) Network and related systems against security intrusions. Responsible for coordinating and managing SMCTD's cyber security activities, upgrade cyber security measures and controls and actively combat security intrusions.
- Plans, analyzes, and implements system security measures and controls related to SMCTD's computer networks and other technology systems. Aligns information security activities with business risk priorities through prioritization of security risk and mitigation activities.
- Research and resolve sensitive and confidential data security issues and provide leadership or technical assistance in projects involving protection of confidential data against unauthorized access.
- Provide hands-on support for a broad spectrum of technologies, including security software running on Windows and Linux systems, network devices, virtual machines, Cloud Infrastructure as well as software-as-service (SaaS) services.
- Collaborate with internal and external stakeholders in implementing and supporting technical projects, and for operational support of production platforms. Researches and evaluates new technologies and cybersecurity management tools; develop and deliver training materials such as online OT cybersecurity awareness training and provide accurate and prompt status reports as required.

EXAMPLES OF DUTIES:

- Develops, implements, and monitors a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy, and recovery of information assets owned, controlled, or/and processed by the organization.
- Identifies, evaluates, and reports on cybersecurity risk related to assets. Performs an inventory of information assets, maintains the asset repository; manages the data classification project.
- Ensures organizational compliance in accordance with agency information security policies, standards, and procedures; responsible for the exception process, authorizes and documents all exceptions, and maintains a repository of all exceptions.
- Manages systems and network security and remote access methodologies such as Firewalls, IDS/IPS, VPN, and MFA. Perform packet analysis using tools such as NMAP, Ethereal a Wireshark; review device logs, provide event correlation, and forensic analysis; conducts regular vulnerability scanning and recommends remediation steps.

- Reviews annually and coordinates any changes to the Incident Response Plan and the overall IT Security Policies/Standards. Responsible for oversight compliance with PCI Compliance and regulations. (Includes conduct annual PCI compliance exercise, security patching process and validation). Acts as a Focal point for all information security related audit work (internal & external). Coordinates with auditors in the execution of audits. Develops a strategy for handling audits and external assessment processes for relevant regulations.
- Maintain relationships with local, state, and federal law enforcement and other related government agencies to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies.
- Provides support and consulting to the Executive Officer, IT while staying current on relevant security regulations, laws, and technologies. Monitor the external threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action.
- Perform all job duties and responsibilities in a safe manner to protect oneself, fellow employees, and the public from injury or harm. Promote safety awareness and follow safety procedures to reduce or eliminate accidents.
- Provide 24/7 on-call construction and maintenance support.
- Perform all job duties and responsibilities in a safe manner to protect one's self, fellow employees and the public from injury or harm. Promote safety awareness and follow safety procedures in an effort to reduce or eliminate accidents.
- Perform other duties as assigned.

SUPERVISION: Works under the general supervision of the Manager, Network Engineering who establishes goals and objectives and evaluates performance.

MINIMUM QUALIFICATIONS: Sufficient education, training and experience to demonstrate the knowledge and ability to successfully perform the essential functions of the position. Development of the required knowledge and abilities is typically obtained through but not limited to:

- Bachelor's degree in computer science, management information systems, information technology, or a closely related field
- Three (3) years of experience managing cyber security programs and initiatives.
- Knowledge of information system architecture and security controls, such as Firewall ACL's and border router configurations, operating systems configurations, wireless architectures, databases, specialized appliances, and information security policies and procedures

PREFERRED QUALIFICATIONS:

- CISSP certification
- Experience managing information security control standards, including SOC2, PCI- DSS, NIST CSF, ISO 27000, or COBIT.
- Deep technical and operational understanding of TCP/IP and security protocols, network defense, and security related technologies including encryption, VPNs, firewalls, proxy services, and IDS/IPS, Windows Active Directory, VMware.
- Knowledge of Cisco switch, routing, firewalls, wireless, and access/identity.
- Knowledge of Security Awareness Training and Phishing Campaign applications.
- Hands-on experience installing and administering security systems and tools, including firewalls, IDS/IPS, SIEM, manage antivirus/antimalware, patch management, log analyzers, network tracers, vulnerability scanners, and Group Policy.
- Strong knowledge in the following areas: IAM, system virtualization, Windows and Unix Security, Cloud Security, Application Whitelisting, Vulnerability Management, endpoint security controls.
- Strong working understanding and knowledge of Windows and Linux Operating Systems.
- Knowledge and depth and/or breadth of expertise in informational technology disciplines e.g., network operations, databases, software application and interfaces, computer operations, production control, quality assurance and systems management.
  Excellent verbal, written, organizational, presentation, and interpersonal communications skills.

SELECTION PROCESS MAY INCLUDE: The process will include a panel interview and may include written and skills test assessments or supplemental questions. Only those candidates who are the most qualified will continue in the selection process. Meeting the minimum qualifications does not guarantee an invitation to continue in the process. Selected candidate must successfully complete a background investigation.

CURRENT EMPLOYMENT BENEFITS:

For further benefit details please go to: https://www.smctd.com/SMCTD_Employment.html#benefits

Holidays:	Seven (7) paid holidays, plus up to four (4) floating holidays per year
Time Off:	Paid Time Off: 26 days per year
Cafeteria Plans:	Medical, dental, vision care, group life insurance, and more
Transportation:	Free bus transportation for employees and qualified dependents
Retirement:	Social Security and California Public Employees Retirement Systems (CalPERS)

- Classic Members – 2% @ 60 benefit formula, 3 year average of highest compensation
- New Members – 2% @ 62 benefit formula, 3 year average of highest compensation

HOW TO APPLY:

- To apply, please visit the https://www.caltrain.com/about/Jobs.html. Complete an online employment application and supplemental questionnaire. This is a continuous recruitment until filled. A resume will not be accepted in lieu of the application and supplemental questionnaire. Incomplete application will not be considered.
- The Human Resources Department will make reasonable efforts in the recruitment/examination process to accommodate applicants with disabilities upon request. If you have a need for an accommodation, please contact the Human Resources Department at (650) 508-6308 or email written request to hr@samtrans.com.
- Caltrain celebrates diversity and is committed to creating an inclusive and welcoming workplace environment. We are an Affirmative Action/Equal Opportunity Employer. Minorities, Women, Persons with Disabilities and Veterans are encouraged to apply.