

JOB OPENING ANNOUNCEMENT

Apply On-line at <https://www.samtrans.com/jobs>

Employment Hotline 650-508-6308

March 1, 2024

TITLE: Cybersecurity Analyst
EMPLOYMENT TYPE: Exempt (Full-Time)
DIVISION: Innovation & Technology
APPLICATION DEADLINE: Sunday, May 5th, 2024 (1st cutoff Sunday April 21st)
PAY RANGE: \$1,913.67 - \$2,870.51 weekly (\$99,511.00 - \$149,267.00 estimated annual)
WORK LOCATION: San Carlos, CA

JOB SUMMARY: The Cybersecurity Analyst will report to the Manager of IT Infrastructure & Cybersecurity and will be responsible for supporting the implementation, monitoring, and response activities of the District's Cybersecurity Program. The District's Cybersecurity Program is the implementation of information security governance and controls for the San Mateo County Transit District (SamTrans), the Peninsula Corridor Joint Powers Board (Caltrain), and the San Mateo County Transportation Authority (TA).

EXAMPLES OF ESSENTIAL FUNCTIONS:

- Act as a resident subject matter expert in information security, including strategies to secure multiple cloud-based tenants, on-premises virtual infrastructure, computer systems, networks, telecommunications, and applications.
- Coordinate and act as a technical resource for the district's information security activities and programs and participate in the district's interdepartmental cybersecurity committee.
- Implement and then perform ongoing monitoring and analysis of information security measures and controls related to the district's computer networks and other technology systems. Align information security activities with business risk priorities through prioritization of security risk and mitigation activities.
- Improve data security through the mitigation of cybersecurity risks and safeguarding the district's computer networks and related systems against security intrusions.
- Investigate and perform response activity for observed or reported data security incidents.
- 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-a-service (SaaS) services.
- Collaborate with internal and external stakeholders in implementing and supporting technical projects, and for operational support of production platforms.
- Assist in the evaluation of security solutions, contractors, and consultants.

EXAMPLES OF DUTIES:

- Implement and monitor the District's Cybersecurity Program to protect the confidentiality, integrity, availability, privacy, and recoverability of information assets owned, controlled, or/and processed by the district.
- Review metrics and reports that measure the efficiency and effectiveness of the District's Cybersecurity Program, provide analysis of the metrics and recommend improvements, and report on the effectiveness of the program.
- Identify, evaluate, and report on cybersecurity risk related to assets. Recommend, and upon approval implement, measures to address identified risks in line with the district's goals for risk management.
- Monitor organizational compliance with the district's information security policies, standards, and procedures; responsible for maintaining an exception process that authorizes and documents all exceptions; and maintain a repository of all exceptions.

San Mateo County Transit District, 1250 San Carlos Ave., San Carlos, CA 94070-1306

- Act in a leadership role for all information security related audit work (internal & external). Coordinate with auditors and other IT and non-IT personnel in the execution of audits.
- Participate as a cybersecurity subject matter expert for all projects, including the evaluation and recommendation of technical controls, and reviewing and recommending security protections to be included in contracts and other agreements.
- Monitor the external threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action.
- Conduct cybersecurity vulnerability testing and risk analysis.
- Maintain relationships with local, state, and federal law enforcement and other related government agencies to ensure that the organization is prepared for effective incident response.
- 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 of IT Infrastructure & Cybersecurity, who establishes goals and objectives and evaluates performance.

MINIMUM QUALIFICATIONS: Sufficient experience, training and/or education to demonstrate the knowledge and ability to successfully perform the essential functions of the position. In lieu of a degree, work-related experience that demonstrates the skills and experience necessary to perform this role will be accepted. Development of the required knowledge and abilities is typically obtained through but not limited to:

- Bachelor's degree in information security, management information systems, information technology, or a closely related field.
- Three (3) years of experience in a cybersecurity role contributing to information security programs and initiatives.

PREFERRED QUALIFICATIONS:

- Certified CISSP, CISM, GSE, or other relevant security certifications.
- Experience monitoring compliance with information security standards, such as NIST Cybersecurity Framework, CIS Critical Security Controls, PCI-DSS, or ISO 27000.
- 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 centralized policies.
- Strong knowledge in the following areas: Cloud Security, Identity and Access Management, Application Whitelisting, Threat and Vulnerability Management, Data Loss Prevention, and operating systems security for Windows and Linux environments.
- Expert level 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.
- 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.
- Two (2) or more years of project management experience with technology projects.
- 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.

CURRENT EMPLOYMENT BENEFITS AT SAMTRANS:

For additional information on SamTrans benefits, please visit, <https://www.samtrans.com/jobs>

Holidays:	Seven (7) paid holidays, plus up to four (4) floating holidays per year
Paid Time Off:	Up to 26 days per year
Cafeteria Plans:	Medical, dental, vision care, group life insurance and more
Transportation:	Free Bus Transportation for employees and qualified dependents
Work Location:	Select positions are eligible to work remote up to 50% of the time
Pension:	Social Security and California Public Employees Retirement Systems (CalPERS) <ul style="list-style-type: none">• 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.samtrans.com/jobs>. Complete an online employment application **11:59 p.m. on Sunday, April 21, 2024, for first cutoff and May 5, 2024 for final cutoff**. A resume will not be accepted in lieu of the application. Incomplete applications 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 recruitment@samtrans.com.
- SamTrans 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.