

Job Title: **Cybersecurity Analyst (Experienced)**

Job ID: **653464**

Location: **Livermore, CA**

What Your Job Will Be Like

We are seeking cybersecurity analysis experts to join our multidisciplinary team of systems analysts, whose studies provide decision insight to customers in ill-defined or complex multi-domain problem areas. Apply critical thinking using a diversity of technical skills and expertise, and effectively communicate options, insights, and trade-offs to customers in a concise way that enables action. Provide technical depth and insight in particular to analysis problems in the cyber domain, to enable connectivity between the analysis team and Sandia's broad and deep cybersecurity operations and R&D teams, and also contribute to multidisciplinary systems analysis teams addressing other domains of national security. Formally define problems, formulate requirements, develop technical approaches, gather information from a variety of sources, and apply analytical and modeling methods to design and objectively evaluate proposed solutions. Familiarity with relevant analysis and/or mod-sim tools would be beneficial, e.g., development and use of cyber risk management approaches, scalable data analytics, or at-scale virtual environments (e.g., Sandia's opensource minimega). Access to knowledge and data in this arena will require a security clearance. Travel is expected to meet with sponsors and to support successful execution of programs.

On any given day, you may be called on to:

- Conduct innovative research;
- Lead projects and also contribute effectively on research teams;
- Work with customers to understand needs and propose solutions; and
- Present results as appropriate at open conferences and classified meetings.

Qualifications We Require

- Masters in computer science, computer engineering, or a related technical discipline, with at least five years' relevant experience; or Ph.D. in these disciplines with at least three years' relevant experience; or bachelor's degree in these disciplines with at least eight years' relevant experience; and a strong record of academic performance.
- Expertise in one or more of the following: cyber risk management, cyber vulnerability assessment, secure software and hardware design, cyber system modeling and simulation, emulation of large-scale computer networks, big data analytics, machine learning, vm introspection, SDN (Software Defined Networking), Android OS and mobile security, cloud security, cryptography, intrusion detection systems and countermeasures, network monitoring and traffic analysis, host or memory forensics, malware analysis and triage.
- Software development competence in at least one programming language; e.g. Go, C/C++, Perl, Python, Ruby, Java or a related language.
- Evidence of relevant research expertise in the form of technical publications, presentations, software, and/or knowledge of applications

- Ability to obtain and maintain a Department of Energy (DOE)-granted Q-level and SCI security clearances.

Qualifications We Desire

The following would be beneficial but are not required:

- Evidence of professional service to the community, such as service on program committees, workshop organization, and/or editorial or review work.
- A proven ability to frame and tackle complex and/or ill-defined multidisciplinary problems
- Background in solving practical problems in science and engineering that involve encounters with real-world data, especially large data sets.
- Working knowledge of TCP/IP, HTTP, SSL, DNS, FTP, SSH, and other common Internet protocols
- Software engineering proficiency, particularly with respect to best practices and team development of high quality code.
- Familiarity with system level development and kernel programming
- Working knowledge of multiple operating systems (Windows, UNIX/BSD, Linux, OS X, etc.)

About Our Team

Department 8116 is part of a five department System Analysis and Engineering Group (8110) in the Homeland Security and Defense Systems Center. Work in 8110 is focused on a broad range of topics in national security including nuclear weapons, homeland security, and transportation energy. Nuclear weapons work includes stockpile studies, surety systems analysis, cost estimation, and future stockpile planning. Homeland security work includes analyses, simulations, and prototype technology deployments which address defense against biological, nuclear, chemical, and radiological terrorism; planning and training for disaster management; and emerging cybersecurity threats. Transportation energy analyses enable technology, policy and regulatory decisions focused on vehicle fleet composition and fuel alternatives. In these complex problem areas, staff in 8100 combine technical depth, cross-domain breadth, and multiple analytic disciplines to deliver products that inform decision makers and facilitate evaluation of options and tradeoffs.

About Sandia

Sandia National Laboratories is the nation's premier science and engineering lab for national security and technology innovation, with teams of specialists focused on cutting-edge work in a broad array of areas. Some of the main reasons we love our jobs:

- Challenging work with amazing impact that contributes to security, peace, and freedom worldwide
- Extraordinary co-workers
- Some of the best tools, equipment, and research facilities in the world
- Career advancement and enrichment opportunities

- Flexible schedules, generous vacations, strong medical and other benefits, competitive 401k, learning opportunities, relocation assistance and amenities aimed at creating a solid work/life balance*

World-changing technologies. Life-changing careers. Learn more about Sandia at:

<http://www.sandia.gov>

*These benefits vary by job classification.

Security Clearance

Position requires a Department of Energy (DOE) granted Q-level security clearance.

Sandia is required by DOE directive to conduct a pre-employment background review that includes personal reference checks, law enforcement record and credit checks, and employment and education verifications. Applicants for employment must be able to obtain and maintain a DOE Q-level security clearance, which requires U.S. citizenship.

Applicants offered employment with Sandia are subject to a federal background investigation to meet the requirements for access to classified information or matter if the duties of the position require a DOE security clearance. Substance abuse or illegal drug use, falsification of information, criminal activity, serious misconduct or other indicators of untrustworthiness can cause a clearance to be denied or terminated by the DOE, rendering the inability to perform the duties assigned and resulting in termination of employment.

EEO

Equal opportunity employer/Disability/Vet/GLBT

To Apply:

https://cg.sandia.gov/psp/applicant/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_APP_SCHJOB.GBL?Page=HRS_APP_JBPST&Action=U&FOCUS=Applicant&SiteId=1&JobOpeningId=653464&PostingSeq=1