Job Details

Job Title: R&D Cybersecurity Researcher (Entry or Senior)
Location: Livermore, CA
Regular/ Temporary: Regular
Job ID: 652087
Department: 08960
Full/Part Time: Full-Time

About Sandia

Sandia National Laboratories is the nation's premier science and engineering lab for national security and technology innovation. We are a world-class team of scientists, engineers, technologists, post docs, and visiting researchers all focused on cutting-edge technology, ranging from homeland defense, global security, biotechnology, and environmental preservation to energy and combustion research, computer security, and nuclear defense.

To learn more, visit http://www.sandia.gov.

Department Description

The Information Security Sciences group (dept. 8960) includes work in advanced computer security research, operational network security, high-performance computing research, decision analysis, and information extraction research. This work is conducted for a wide range of government sponsors, including the Departments of Energy, Homeland Security, and Defense.

Our mission is to both underpin the current business areas with robust and exciting research capabilities and provide fundamental knowledge for future innovation.

This posting will be used to fill openings in both the Enterprise Cyber Security (8965) and Cyber System Assessments (8966) departments.

How to Apply

Click on the "Apply" button at the top or bottom of this screen, follow the instructions to upload a resume, and complete the submission process to indicate your interest in this position.

Job Description

R&D S&E, Cybersecurity MM

Job Summary

We have multiple openings for full-time entry-level and experienced cybersecurity researchers to participate in efforts to secure government and critical infrastructure systems in support of the Department of Homeland Security and other government Departments and Agencies. Our group is a unique team whose members develop and deploy operational cybersecurity capabilities, and also conduct cutting-edge research in advanced cybersecurity technologies. Researchers are

expected to apply research advances to challenging multi-disciplinary problems important to national security, with an emphasis on creating a strong cyber environment that can withstand multipronged, highly sophisticated attacks. Current research includes vulnerability assessments, countermeasures development and assessment, reverse engineering, malware analysis, VM introspection, intrusion detection, network and host forensics, mobile devices and networks, at-scale virtualization, and enterprise-scale emulation and analysis of cyber events. Team members are expected to conduct innovative research; to lead projects and also contribute effectively on research teams; to work with customers to understand needs and propose solutions; and to present results as appropriate at open conferences and classified meetings. Access to knowledge and data in this arena will require a security clearance. Some travel is expected to meet with sponsors and support successful execution of programs.

Primary Job Duties

Plans, conceives, conducts, or manages research and development for Sandia's customers and sponsors.
Directs systematic study toward a fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts, and discovers new approaches to achieve goals.
Creates new understandings and capabilities by using the scientific method's hypothesis, test, and evaluation techniques; critical review; or similar engineering research and development methods.
Initiates, designs, develops, executes, and evaluates new processes, products, or systems through basic and applied research.
Uses engineering principles to research, design, or develop structures, instruments, machines, experiments, processes, systems, theories, or technologies; to construct or operate the same with full cognizance of their design; or to forecast their behavior under specific operating conditions.
Undertakes development and possible technology transfer of solutions, products, principles or technology.
Undertakes creative work, making systematic use of investigation or experimentation, to discover or revise knowledge of reality, and uses this knowledge to devise new applications.

Knowledge, Skills & Abilities

Ability to conduct independent research.

Excellent written and oral communication skills.

Proficiency prioritizing work and making decisions.

Minimum Qualifications

- Master's degree in computer science, computer engineering, or a related technical discipline, with an emphasis on cybersecurity; or bachelor's degree in these disciplines with at least two years' relevant experience.
- Expertise in one or more of the following: cyber vulnerability assessment, intrusion detection systems and countermeasures, network protocols and monitoring, host forensics and memory forensics, malware analysis and triage, Android OS and mobile security, cloud security, network traffic analysis, and emulation of large-scale computer networks.
- Evidence of relevant research expertise in the form of technical publications, presentations, software, and/or knowledge of applications.
- Software development competence in at least one programming language; e.g. C/C++, Perl, Python, Ruby, Java or a related language.
- Ability to obtain and maintain a Department of Energy (DOE)-granted Q-level and SCI security clearance. In order to obtain these clearances, U.S. Citizenship and polygraphs are required.

Desired Qualifications

- Record of strong academic performance.
- Demonstrated ability to team effectively in a collaborative research environment.
- Demonstrated ability to independently bring definition to difficult ill-defined problems in order to develop workable technical approaches.
- Software engineering proficiency, particularly with respect to best practices and team development of high quality code.
- Familiarity with system level development, kernel programming, and binary reverse engineering.
- Experience with Intrusion Detection Systems (IDS) and signature development
- Hands-on network/packet level examination using tools such as tcpdump or wireshark.
- Strong understanding of inter-domain networking including BGP, layer-2 networking protocols such as OSPF, ARP, DHCP, and TCP/IP networks in general.
- Working knowledge of TCP/IP, HTTP, SSL, DNS, FTP, SSH, and other common Internet protocols as well as common client scripting languages such as Javascript and VBscript.
- Experience searching/parsing log files with command line utilities.
- Working knowledge of multiple operating systems (Windows, UNIX/BSD, Linux, OS X, etc.)
- Background in solving practical problems in science and engineering that involve encounters with real-world data.

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.

Benefits

At Sandia you will receive many benefits as a valued employee of a premier national multi-program engineering and science research laboratory. In our Total Rewards package you will enjoy competitive pay, great benefits, a stimulating, positive environment and learning opportunities that will help build your career. More information may be found on our Careers website.

EEO

Equal opportunity employer/Disability/Vet/GLBT