AI Security Researcher

highheredjobs.com/search/details.cfm

Type: Full-Time
Posted: 5 days ago
Category: Software Engineer/Programmer
Military

Carnegie Mellon University

Are you a cybersecurity and/or AI researcher who enjoys a challenge? Are you excited about pioneering new research areas that will impact academia, industry, and national security? If so, we want you for our team, where you'll collaborate to deliver high-quality results in the emerging area of AI security.

The CERT Division of the Software Engineering Institute (SEI) is seeking applicants for the AI Security Researcher role. Originally created in response to one of the first computer viruses -- the Morris worm - in 1988, CERT has remained a leader in cybersecurity research, improving the robustness of software systems, and in responding to sophisticated cybersecurity threats. Ensuring the robustness and security of AI systems is the next big challenge on the horizon, and we are seeking life-long learners in the fields of cybersecurity, AI/ML, or related areas, who are willing to cross-train to address AI Security.

As part of the Threat Analysis Directorate, you will join a group of security experts focused on advancing the state of the art in AI security at a national and global scale. Our tasks include vulnerability discovery and assessments for AI systems, evaluation of the effectiveness and robustness of defenses and mitigations for AI systems, reverse engineering AI systems and models, and identifying new areas where security research is needed. We participate in communities of network defenders, software developers and vendors, security researchers, AI practitioners, and policymakers. You'll get a chance to

work with elite AI and cybersecurity professionals, university faculty, and government representatives to build new methodologies and technologies that will influence national AI security strategy for decades to come.

You will co-author research proposals, execute studies, and present findings and recommendations to our DoW sponsors, decision makers within government and industry, and at academic conferences. The SEI is a non-profit, federally funded research and development center (FFRDC) at Carnegie Mellon University.

What you'll do:

- Develop state of the art approaches for analyzing robustness of AI systems.
- Apply these approaches to understanding vulnerabilities in AI systems and how attackers adapt their tradecraft to exploit those vulnerabilities.
- Reverse engineer malicious code in support of high-impact customers, design and develop new analysis methods and tools, work to identify and address emerging and complex threats to AI systems and effectively participate in the broader security community.
- Study and influence the AI security and vulnerability disclosure ecosystems.
- Evaluate the effectiveness of tools, techniques and processes developed by industry and the AI security research community.
- Uncover and shape some of the fundamental assumptions underlying current best practice in AI security.
- Develop thought models, tools and data sets that can be used to characterize the threats to, and vulnerabilities in, AI systems, and publish those results. You will also use these results to aid in the testing, evaluation and transition of technologies developed by government-funded research programs.
- Identify opportunities to apply AI to improve existing cybersecurity research.

Who you are:

- You have BS in machine learning, cybersecurity, statistics, or related discipline with eight (8) years of experience; OR MS in the same fields with five (5) years of experience; OR PhD in the same fields with two (2) years of experience.

- You have a deep interest in AI/ML and cybersecurity with a penchant for intellectual curiosity and a desire to make an impact beyond your organization.
- You have practical experience with applying cybersecurity knowledge toward vulnerability research, analysis, disclosure, or mitigation.
- You have experience with advising on a range of security topics based on research and expert opinion.
- You have familiarity with implementing and applying AI/ML techniques to solving practical problems.
- You have familiarity with common AI/ML software packages and tools (e.g., Numpy, Pytorch, Tensorflow, ART).
- You have knowledge or familiarity with reverse engineering tools (e.g. NSA Ghidra, IDA Pro)
- You have experience with Python, C/C++, or low-level programming.
- You have experience developing frameworks, methodologies, or assessments to evaluate effectiveness and robustness of technologies.
- You have excellent communication skills (oral and written), particularly regarding technical communications with non-experts.
- You enjoy mentoring and cross-training others and sharing knowledge within the broader community.
- Candidates with strong technical proficiency in either AI/ML or cybersecurity are welcome to apply, provided a demonstrated intellectual agility and commitment required for accelerated learning within the role.

You are able to:

- Travel to various locations to support the SEI's overall mission. This includes within the SEI and CMU community, sponsor sites, conferences, and offsite meetings on occasion (5%).
- You will be subject to a background check and will need to obtain and maintain a Department of War (DoW) security clearance.

Why work here?

- Join a world-class organization that continues to have a significant impact on software.
- Work with cutting-edge technologies and dedicated experts to solve tough problems for the government and the nation.
- Be surrounded by friendly and knowledgeable staff with broad expertise across AI/ML, cybersecurity, software engineering, risk management, and policy creation.
- Get 8% monthly contribution for your retirement, without having to contribute yourself.
- Get tuition benefits to CMU and other institutions for you and your dependent children.
- Enjoy a healthy work/life balance with flexible work arrangements and paid parental and military leave.
- Enjoy annual professional development opportunities; attend conferences and training or obtain a certification and get reimbursed for membership in professional societies.
- Qualify for relocation assistance and so much more.

Joining the CMU team opens the door to an array of exceptional benefits.

Benefits eligible employees enjoy a wide array of benefits including comprehensive medical, prescription, dental, and vision insurance as well as a generous retirement savings program with employer contributions. Unlock your potential with tuition benefits, take well-deserved breaks with ample paid time off and observed holidays, and rest easy with life and accidental death and disability insurance.

Additional perks include a free Pittsburgh Regional Transit bus pass, access to our Family Concierge Team to help navigate childcare needs, fitness center access, and much more!

For a comprehensive overview of the benefits available, explore our Benefits page.

At Carnegie Mellon, we value the whole package when extending offers of employment. Beyond credentials, we evaluate the role and responsibilities, your valuable work experience, and the knowledge gained through education and training. We appreciate your unique skills and the perspective you bring. Your journey with us is about more than just a job; it's about finding the perfect fit for your professional growth and personal aspirations.

Are you interested in an exciting opportunity with an exceptional organization?! Apply today!

Location

Pittsburgh, PA

Job Function

Software/Applications Development/Engineering

Position Type

Staff - Regular

Full Time/Part time

Full time

Pay Basis

Salary

More Information:

- Please visit **"Why Carnegie Mellon"** to learn more about becoming part of an institution inspiring innovations that change the world.
- Click here to view a listing of employee benefits
- **Carnegie Mellon University is an Equal Opportunity Employer/Disability/Veteran**.
- **Statement of Assurance**

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

Related Searches:

- Software Engineer/Programmer
- Military-Friendly