Job Title: Security Research Engineer

USD $160,000.00/Yr. - USD $230,000.00/Yr

(Remote / U.S-Based)

About Us

AI Security Assurance is a new, remote‑first startup building **AI‑Storm**, an AI‑powered platform that bridges high‑level systems‑theoretic security analysis with actual source code to reveal design flaws that traditional tools miss. Our mission is to help engineers design and verify secure systems across software, cyber‑physical, and organizational domains. Transparency is one of our core values: we operate as a distributed team across the United States and we're open about our progress and challenges. To learn more about the platform's capabilities please see our product page at aisecurityassurance.com/products.

As an early employee, you'll wear multiple hats typical of a startup. You'll help build our core AI-powered analysis engine that ingests code in multiple languages, extracts structural and semantic information, and ties it back to system‑level security analysis. Working closely with our STPA‑Sec/verification experts and threat‑modelling SME, you'll work with team members to design and implement the ingestion engine, knowledge graph, pattern‑matching and data‑flow analysis, and dataset collection and evaluation. If you thrive in a transparent, fast‑moving environment where your contributions shape the product, we'd love to hear from you.

The Role

As our Security Engineer Specialist, you will:

- Build and extend the AI-powered Ingestion Engine: work with our team members to develop a multi‑language ingestion pipeline that generates syntactic, semantic, focus and hierarchical labels.
- Integrate hierarchical abstraction and data‑flow: extend the engine with data‑flow extraction, a pattern‑matching library for scenario mitigations, and attack‑tree structures.
- Expose backend APIs to the web UI: collaborate with the front‑end specialist to ensure the pipeline's outputs are accessible in both cloud and on‑prem deployments.
- Support evaluation and dataset creation: help collect test data, generate multi‑level datasets and contribute to our LLM‑as‑a‑judge evaluation metrics.
- Collaborate across the stack: work with our STPA‑Sec and formal‑verification leads to integrate mitigation constraints, proofs, and assurance evidence into the backend.

What We’re Looking For

Must‑haves:

- Bachelor’s degree or higher in Computer Science or a related technical discipline.
- 4+ years of professional experience in security engineering, static/dynamic analysis, threat modeling, or related roles with a demonstrated ability to deliver.
- Experience designing and implementing backend services or pipelines and exposing APIs for other components.
- Familiarity with threat‑modelling frameworks and vulnerability databases (e.g., CWE/CVE) and the ability to map findings back to code.
- Strong critical thinking about trade‑offs in performance, accuracy and scalability in security tooling.
- Ability to work independently, collaborate with domain experts, and wear multiple hats in a fast‑moving environment.
- Ability to work with complex datasets, such as natural language and knowledge graphs, and develop robust evaluation metrics.
- Ability to work in the US without sponsorship. Future work may require ability to obtain a U.S. security clearance.

Nice‑to‑haves:

- Experience with STPA‑Sec or formal methods (e.g., theorem provers, formal verification frameworks).
- Knowledge of graph‑based representations of code (Code Property Graphs), knowledge graphs, and pattern‑matching techniques.
- Contributions to open‑source security tools or static/dynamic analysis projects.
- Familiarity with cloud/on‑prem deployment, DevOps practices and database technologies (e.g., PostgreSQL).
- Publications, conference presentations, or blog posts in the area of software or systems security or related areas.
- Preference for East Coast residents who can travel to the D.C./Virginia area for occasional meetings.

What We Offer

- Remote-first organization
- Health / Dental / Vision benefits / etc.
- Life Insurance, Short-Term and Long-Term Disability coverage.
- 401(k) retirement plan.
- Occasional travel.

How to Apply

If you're excited about taking on this challenge and helping re-imagine how advanced analysis tools are used, please submit your resume (careers@aisecurityassurance.com) and a short cover letter describing why you will be successful in this position, highlighting previous projects (links to code is highly recommended.)

Transparency Note: This role is contingent on the company securing funding for the pending contract. If funding is awarded, the position will begin once the contract starts and will be fixed-term for the duration of that contract (currently projected to be less than two years). Should the company secure additional funding and the selected candidate demonstrate strong performance, there may be an opportunity to extend the role beyond the initial term. We're looking for colleagues who are motivated to contribute to our collective success and help us achieve the milestones necessary for future growth.

EEO:Equal opportunity employer, including disability and protected veterans, or other characteristics protected by law. AI Security Assurance operates a drug free workplace.