Job Title: Human-AI Collaboration Specialist

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 research how users currently perform security analysis with existing tools, transform those insights into requirements, design and build a web-based UI that works for both cloud and on-premises deployments, and test it with real analysts to incorporate feedback. You will also help set up our cloud/on-prem services, collect usage data, and evaluate how well the agents and models are performing. 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 Human-AI Collaboration Specialist, you will lead the design and implementation of our web-based user interface for both cloud and on-premises deployments. You will:

- Research how analysts currently perform work (via STAMPP, threat modeling, and other tools) to uncover workflows, pain points and opportunities.
- Translate research findings into user requirements, wireframes/prototypes, and collaborate with backend engineers to deliver.
- Build and iterate a data-intensive, agent-driven UI, balancing performance, clarity, usability, and design trade-offs.
- Set up and maintain both cloud-based and on-premises service delivery paths.
- Collect usage/data metrics, run human-in-the-loop tests, incorporate user feedback, evaluate model/agent performance (precision, recall, LLM-as-judge) and refine the system.
- Actively think through frontend design, optimization, UX, and how the UI interacts with complex agents and models.

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 software engineering, frontend development, or a related technical role with demonstrated ability to deliver.
- Proven experience building frontend applications that are complex, data-intensive, and agentic (or feature multi‑agent / model‑driven flows) for both cloud and on-premises contexts.
- Strong critical thinking about trade-offs in frontend design (usability vs. performance vs. scalability) and designing optimal user experiences.
- Demonstrated experience researching user workflows, collecting requirements, working with backend teams, and driving a product from concept through delivery.
- Experience handling and evaluating complex datasets and model/agent-performance metrics (e.g., precision, recall, LLM-as-judge frameworks).
- 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, threat modeling, Secure by Design Principles, etc.
- Experience integrating chat-based agents or conversational UIs into web frontends.
- Familiarity with database technologies (e.g., PostgreSQL) and cloud/edge service deployment.
- Experience in on-premises deployment scenarios (enterprise/secure environments).
- Publications, conference presentations, or blog posts in the area of software or systems security, UX and AI design, 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
- 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.) Note: Position availability is pending funding–anticipated notice is end of 2025.

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.