

SAMPLE

AI Startup Security Hiring Kit

The opening of security-hiring-kit.docx, one of 4 files in the kit. <https://solasai.net/products/ai-security-hiring/>

AI Startup Security Hiring Kit

Solas AI | AI Startup Security Hiring Kit solasai.net

Job descriptions, interview questions, and evaluation rubrics for the first security hire at an AI startup.

When to Hire (And What to Hire)

Company Stage	Headcount	Revenue	Security Need	Recommended Hire
Pre-seed / Seed	5-15	<\$1M ARR	Basic hygiene, first enterprise deal	Fractional CISO (\$3-5K/mo) — not a full-time hire
Series A	15-40	\$1-5M ARR	SOC 2, first security policies, enterprise sales pipeline	Security Engineer / First Security Hire (this kit)
Series B	40-100	\$5-20M ARR	Scaling the program, team building	Head of Security / CISO + Security Engineer
Series C+	100+	\$20M+ ARR	Full security org	Security team with specialized roles

The "first security hire" sweet spot is **Series A**. Before that, a fractional CISO handles it. After that, you need a team. This kit focuses on the first full-time hire.

Job Description: First Security Hire (Security Engineer / Head of Security)

Customize the title based on your company's level and the candidate's experience.

{{COMPANY_NAME}} — **{{TITLE: Security Engineer / Head of Security}}**

Location: {{LOCATION / Remote}} **Reports to:** {{CTO / CEO / VP Engineering}} **Compensation:** \${{RANGE}} + equity

About {{COMPANY_NAME}}

{{2-3 sentences about your company and product. Include that you use AI — this attracts candidates who want AI security experience.}}

About the Role

You will be our first dedicated security hire. This is a builder role, not an inheritor — you will design and implement our security program from the ground up, not maintain someone else's work.

You will own everything from policies to pen tests, SOC 2 to AI-specific controls. You will work directly with engineering to embed security into our AI product architecture. You will interface with enterprise customers on security reviews and questionnaires. You will report directly to {{REPORTING_LINE}}.

This is for someone who wants to build, not babysit. If you thrive on greenfield security work and want to shape how an AI company does security, this is the role.

What You'll Do

First 90 days:

- Conduct a security assessment and build a prioritized roadmap
- Deploy foundational security policies (information security, access control, incident response, AI acceptable use)
- Enforce MFA and SSO across all systems
- Implement vulnerability scanning and dependency management
- Begin SOC 2 preparation (if applicable)

First year:

- Build and maintain the security program aligned with SOC 2 Trust Services Criteria
- Implement AI-specific controls: model access management, training data governance, prompt logging, output monitoring, tenant isolation
- Lead the SOC 2 Type II audit process
- Respond to enterprise security questionnaires
- Conduct or coordinate annual penetration testing
- Build security awareness training program
- Establish vendor risk management (especially for AI model providers)
- Serve as the incident response lead

Ongoing:

- Own the security roadmap and present quarterly to leadership
- Be the security voice in product and architecture decisions

- Manage compliance obligations and regulatory monitoring
- Build relationships with enterprise customers' security teams

The sample ends here. The full document runs about 1,573 words; the kit holds 4 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/ai-security-hiring/>, 14-day refund for any reason.