AI::Sec - AppSec Engineer Replacement FAQ

1. What is AI::Sec and what problem does it solve?

AI::Sec is an AI-powered **Application Security (AppSec) Engineer** designed to replace human labor. The global cybersecurity industry faces a shortage of over 4 million professionals, and hiring AppSec engineers is expensive and slow. AI::Sec automates **90% of application security tasks**, scales instantly, and provides cost-effective security staffing on a subscription model.

Market & Problem Validation

Q1: How do you validate that companies will pay for application security talent on a subscription model?

✅ AI::Sec solves the **global AppSec talent shortage (4M unfilled jobs)** by offering scalable **AI-powered AppSec engineers on demand**.

✅ **Existing validation:** Companies spend **$520B annually** on cybersecurity salaries, taxes, and benefits, showing **clear market demand for automation**.

✅ **Competitive edge:** Unlike MSSPs, AI::Sec provides **dedicated AI security agents** that scale **instantly**, are **cheaper than human engineers**, and offer **customized security testing and compliance enforcement**.

Q2: How do you compete with existing security vendors?

✅ **Existing AI-driven cybersecurity tools** (e.g., Snyk, Veracode, Checkmarx) focus on vulnerability scanning, but lack the ability to **replace full-time AppSec engineers**.

✅ AI::Sec offers a **fully autonomous AppSec engineer**, handling **secure code reviews, compliance enforcement, and vulnerability management**—essentially replacing an entire **AppSec team** in an enterprise.

✅ **Faster ROI**: AI::Sec **costs 30-50% less than hiring AppSec engineers**, while providing **real-time, scalable security automation**.

Q3: What is your total addressable market (TAM) and near-term revenue potential?

✅ The **cybersecurity workforce market is worth $520B annually**, expanding toward **$1T+ in enterprise security**.

✅ Capturing just **1% of this labor market translates to a $5.2B ARR opportunity**.

✅ Near-term (Year 1): We aim to onboard **10 enterprise customers**, each paying **$200K annually**, leading to **$2M ARR** within 12 months.

---

2. How big is the market opportunity?

- The **cybersecurity labor market is valued at $520B annually**, with a broader expansion potential to **$1T+ in enterprise security workforce automation**.
- AI::Sec is targeting the **replacement of human AppSec engineers, which cost enterprises billions in salaries, taxes, and benefits**.
- Capturing just **1% of this labor market translates to a $5.2B ARR opportunity**.

---

3. How does AI::Sec differentiate from competitors like Snyk, Veracode, and Checkmarx?

Unlike existing **AppSec tools** that focus on scanning for vulnerabilities, AI::Sec **fully replaces human AppSec engineers** by performing **automated security code reviews, enforcing compliance policies, and integrating into DevSecOps workflows**. AI::Sec integrates **finite automata and DAG-based workflows** to provide a deterministic, structured approach to security—offering higher accuracy and eliminating AI hallucinations.

---

4. What makes AI::Sec's technology unique?

- **Patented AI Model**: AI::Sec eliminates major AI security vulnerabilities, including **prompt injection, data privacy breaches, and backdoor threats**.
- **No Hallucinations**: Proprietary mathematical updates ensure only validated, factual security actions are taken.
- **Finite Automata & DAG Architecture**: Provides structured, deterministic security processes instead of purely statistical AI decision-making.
- **Dynamic Scalability**: Instantly scales AI security agents based on demand without the need for manual configuration.

Technology & Product Validation

Q4: How does finite automata and DAG technology improve application security automation?
✅ Unlike **traditional AI models**, AI::Sec integrates **finite automata** to ensure **deterministic, repeatable security processes**, avoiding unpredictable **AI hallucinations**.
✅ **DAG-based workflows** enable **asynchronous security automation**, ensuring **faster, scalable, and parallel execution** of tasks like secure code review and threat modeling.
✅ This ensures **AI::Sec operates with zero downtime**, processes thousands of security events in **milliseconds**, and **adapts dynamically to evolving threats**.

Q5: How does AI::Sec achieve zero hallucinations?
✅ AI::Sec uses a **proprietary mathematical update** to GPT, eliminating **hallucinations and security vulnerabilities**.
✅ **Tech Differentiation:**

- Uses **post-processing validation layers** to eliminate incorrect responses.
- Integrates **secure prompt engineering** and **policy-based AI constraints** to prevent unauthorized outputs.
- Works **energy-efficiently**, dynamically adjusting resource consumption to ensure **optimized cost and security execution**.

---

5. What is AI::Sec's revenue model?

AI::Sec operates on a **SaaS subscription model**, where enterprises pay per AI AppSec agent.

- **Pricing per AI AppSec Engineer:** $80K–$120K per year per agent (40–50% cheaper than hiring human engineers).

- **Enterprise Plans:** Monthly subscription or usage-based pricing.
- **Scaling:** Each enterprise typically starts with 1-2 AI agents and expands as security needs grow.

---

6. What are the financial projections for AI::Sec?

Year 1: $10.7M ARR (with 92 AI agents sold).
Year 2: $50M ARR (with 500 AI agents sold).
Year 3: $150M ARR (with 1500 AI agents sold).
Gross Margin: 75–85% (comparable to SaaS industry benchmarks).

---

7. What is AI::Sec's go-to-market strategy?

Phase 1 (6 Months): Secure 5 pilot enterprise customers, targeting finance, healthcare, and regulated industries.
Phase 2 (Year 1): Expand through MSSP partnerships and integrations with CI/CD pipelines.
Phase 3 (Year 2+): Establish AI::Sec as the industry standard for AI-powered application security staffing.