AI::Sec - Enterprise Sales FAQ

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

AI::Sec is an **AI-powered Application Security (AppSec) automation solution** designed for enterprises, MSSPs, and regulated industries. It **automates 90% of AppSec tasks**, including vulnerability management, compliance enforcement, and secure development, reducing security costs while improving efficiency.

🔹 **Problem:** Growing security demands, talent shortage (4M+ unfilled cybersecurity jobs), and high costs of manual security reviews.
🔹 **Solution:** AI::Sec **replaces manual security processes with AI-driven automation**, reducing reliance on human AppSec engineers.
🔹 **Outcome:** Faster product releases, lower operational costs, and stronger security.

💡 *"Think of AI::Sec as your **automated AppSec engineer**, working 24/7 to secure your applications at scale."*

---

2. How does AI::Sec validate market demand?

✅ **Growing demand for automated security solutions:** Enterprises **spend over $520B annually** on cybersecurity salaries, proving the market need for automation.
✅ **Competitive edge:** Unlike traditional tools (Snyk, Veracode, Checkmarx), AI::Sec **automates the full AppSec workflow**, not just vulnerability scanning.
✅ **Proven business model:** Companies are willing to pay for **AI-powered security engineers via subscription**, as AI::Sec costs **$80K–$120K per year**, compared to **$150K–$250K per human engineer**.

💡 *"AI::Sec enables enterprises to scale security without increasing headcount."*

---

3. How does AI::Sec outperform ASOC, Snyk, and other automated AppSec tools?

1. AI::Sec Goes Beyond Traditional ASOC & SCA Solutions

🔹 **Traditional AppSec tools (Snyk, Veracode, Checkmarx, ASOC solutions)** focus **only on specific parts** of the security lifecycle (e.g., static/dynamic analysis, dependency scanning).
🔹 AI::Sec **automates the entire AppSec workflow**, from **secure code review, compliance enforcement, vulnerability management, and DevSecOps automation**—not just detection but **actual remediation** and **risk-based prioritization.**

💡 *Think of AI::Sec as replacing manual AppSec engineers, not just enhancing existing tools.*

2. AI::Sec Eliminates AI Hallucinations with Deterministic Security Automation

🔹 **Existing LLM-based tools (GitHub Copilot, CodeQL, etc.) are unreliable in security-critical environments** because they generate **hallucinated responses** and lack validation mechanisms.

🔷 AI::Sec uses a **finite automata (FA) and directed acyclic graph (DAG)-based architecture** to ensure predictable, structured, and **deterministic** security automation.
🔷 This means **zero false positives**, **zero AI hallucinations**, and **fully auditable security actions.**

💡 *Most security AI solutions are statistical. AI::Sec is deterministic—ensuring security decisions are always valid and repeatable.*

3. AI::Sec Runs AI Inference Efficiently On-Prem Without High Costs

🔷 Most commercial AI models (GPT-based security tools) are **cloud-only** due to licensing restrictions and high computational costs for on-prem AI inference.
🔷 AI::Sec provides a **commercially licensed LLM** optimized for **on-prem deployment**, reducing **GPU and RAM requirements by 70% compared to traditional AI models**.
🔷 This allows **regulated industries (finance, healthcare, defense, critical infrastructure)** to **use AI-powered AppSec without compliance risks** from cloud-based AI.

💡 *Most AI-driven security solutions are not optimized for on-prem. AI::Sec delivers enterprise-ready AI with cost-efficient local deployment.*

4. AI::Sec Provides a Fully Automated Security Engineer – Not Just a Scanning Tool

🔷 **Snyk, Veracode, and Checkmarx** help identify vulnerabilities, but **humans still have to review, triage, and fix them**.
🔷 AI::Sec **automates not just detection, but also remediation recommendations, compliance enforcement, and risk-based prioritization**—making it a true **replacement for an AppSec engineer**, not just a tool for them.
🔷 **Seamless ASOC Integration** – Works directly with **Application Security Orchestration & Correlation (ASOC) platforms (ArmorCode, ZeroNorth)** to automate security workflows, enforce compliance, and optimize DevSecOps security testing.

💡 *Traditional AppSec tools require human intervention. AI::Sec replaces manual processes entirely.*

---

4. What is AI::Sec's business model?

📌 **Subscription-based AI-powered AppSec Engineer.**
📌 **Cost:** $80K–$120K per year per AI agent (vs. $150K–$250K per human engineer).
📌 **Deployment:** Fully managed SaaS or on-prem integration.
📌 **Scalability:** Enterprises start with **1 AI agent**, expanding to **5+ within a year** based on security needs.

💡 *"AI::Sec reduces security costs while ensuring continuous protection."*

---

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

Phase 1: Early Adopter Sales (First 6 Months)

🎯 **Target Market:** Enterprises with mature software development & compliance needs (finance, healthcare, SaaS).
🎯 **Sales Motion:** Direct sales to CISOs, DevSecOps leaders, and engineering executives.

🎯 **Key Tactic: Offer AI-powered AppSec pilot programs to demonstrate automated security validation ROI.**

🔷 **Goal:** Secure **5–10 enterprise pilots, reaching $2M ARR.**

Phase 2: Scale Through Partnerships (Year 1–2)

📌 **Strategic Partnerships:** Work with **cloud security providers (AWS, Azure, Google Cloud).**
📌 **ASOC Integration:** Seamless compatibility with **Application Security Orchestration & Correlation (ASOC) platforms like ArmorCode, ZeroNorth**.
📌 **DevSecOps Expansion:** Expand into **MSSPs, CI/CD security tooling, and compliance automation.**

🔷 **Goal:** Reach **50 enterprise customers, $10M+ ARR.**

---

6. What are AI::Sec's financial projections?

📌 **Year 1:** 10 enterprise customers → $2M ARR.
📌 **Year 2:** 50 enterprise customers → $10M ARR.
📌 **Year 3:** 150 enterprise customers → $50M ARR.
📌 **Exit:** IPO or acquisition by **Palo Alto, CrowdStrike, Wiz** within 5 years.

💰 **Current funding round:** Raising **$250K SAFE @ $4M post-money valuation.**

💡 *"Investors gain early-stage equity in AI::Sec with a projected path to $150M+ ARR."*
