NoSec — Business Plan Subtitle: Investor-ready plan for securing cloud-native, AI, and Web3 systems.

Date: October 25, 2025

Executive Summary

- Company: NoSec — cybersecurity consultancy & managed services for cloud-native, AI, and Web3 systems.
- Mission: Help organizations design, build, and operate secure, resilient systems for modern stacks.
- Offerings: Assessments, pentests/red-team, secure architecture & DevSecOps enablement, MDR, incident response, supply-chain/SBOM services, productized automation/playbooks.
- Target market: Mid-market & enterprise technology companies (SaaS, fintech, healthcare, Web3, AI platforms) in North America & EMEA.
- Financial snapshot (high-level): Year1 revenue $1.2M (projects-heavy), Year2 $3.6M (managed expansion), Year3 $8.0M (productization + scale). Break-even in Year2 under base case.
- Ask / Next steps: Hire initial team, launch MDR offering, productize 3 playbooks, engage 3–5 pilot customers.

Company Overview

- Legal: NoSec (private). Headquarters: assumed North America (adjustable).
- Core competencies: cloud-native security, application security, DevSecOps, AI/ML pipeline security, Web3 smart contract security, incident response, security automation.
- Value proposition: Deep technical expertise + automation/productization to reduce remediation time and scale delivery.

Market Analysis

- Market drivers:

    - Rapid cloud & AI adoption across industries.
    - Increased software supply-chain and third-party risks.
    - Regulatory and compliance pressures driving security investments.
    - Rise of automated attacks and AI-assisted threat activity.

- Market size: Multi-billion-dollar global security services market; high growth in segments focused on modern stacks (cloud-native, AI, Web3).

- Initial focus (SOM): Mid-market and enterprise customers in North America & EMEA within SaaS, fintech, healthcare, blockchain infrastructure, and AI platforms.

- Customer pain points:
    - Lack of internal expertise for emergent stack security (AI pipelines, smart contracts).
    - Manual or inconsistent CI/CD and supply-chain controls.
    - Long mean-time-to-detect (MTTD) and mean-time-to-remediate (MTTR).
    - Compliance and auditability gaps.

Competitive Landscape

- Competitors:
    - Boutique security consultancies (broad consulting).
    - Specialized Web3/smart contract security firms.
    - Large MSSPs/MDR providers.

- NoSec differentiators:
    - Specialization in modern technology stacks (AI, Web3, cloud-native).
    - Productized automation playbooks to scale delivery and margins.
    - Engineering-first delivery model emphasizing embedding security into pipelines.
    - Measurable outcomes (MTTD/MTTR improvements).

Value Proposition & Service Lines

- Consulting & Assessments: architecture reviews, threat modeling, SBOM and supply-chain analysis.

- Offensive & Defensive Exercises: penetration tests, red-team, purple-team, tabletop exercises.

- Managed Services: MDR, SOC-as-a-service, continuous DevSecOps enablement and monitoring.

- Incident Response & Forensics: retained IR, on-call response, forensic investigations.

- Productized Automation: IaC/CI/CD scanning templates, remediation playbooks, integration modules, reporting dashboards.

Integrated Delivery Model (Overview)

- Engagement types:
    - Fixed-fee projects (assessments).
    - Time & Materials (incident response).
    - Subscription (MDR/managed services).
    - Productized one-time + integration (automation modules).
- Typical delivery flow:
    - Discovery → Assessment/Workshop → Remediation Sprints → Handoff to Managed Services → Continuous Improvement.
- Example SLAs:
    - MDR onboarding: ≤ 30 days.
    - Critical alert triage: initial response ≤ 1 hour.
    - Remediation guidance: within 48 hours for prioritized issues.
- High-level unit economics:
    - Project gross margin ~50%.
    - Managed & licensing gross margin ~70%.
    - Target blended gross margin >60% by Year 3.
- Utilization targets:
    - Billable utilization 60–70% for delivery engineers at scale.

Business Model & Pricing

- Revenue streams:
    - Consulting project fees (fixed).
    - Managed subscriptions (recurring).
    - Product licensing and one-time integration fees.
    - Incident response (T&M and retainers).
- Pricing templates (guidance):
    - Security assessment: $30,000 – $120,000.
    - Penetration test / red-team: $40,000 – $200,000.
    - Managed Detection & Response (MDR): $5,000 – $30,000 per month.

        - Automation module: $10,000 – $50,000 one-time + integration.
- Sales motion:
    - Short-cycle assessments and workshops to establish credibility.
    - Land-and-expand: convert assessments into managed retainers, then sell automation modules.

Go-to-Market

- Target segments: mid-market & enterprise SaaS, fintech, healthcare, Web3 infra, AI/ML platforms.
- Channels:
    - Direct enterprise sales & account-based marketing (ABM).
    - Partnerships: cloud providers, DevOps tooling vendors, systems integrators.
    - Developer & security communities: GitHub, writeups, open-source playbooks.
    - Events & thought leadership: conferences, workshops.
- Key KPIs:
    - Lead velocity, pipeline conversion rate, conversion (assessment → retainer), ARR from managed services, customer churn, CAC, LTV.

Operations & Team

- Core functions:
    - Delivery: security engineers, pentesters, IR analysts.
    - Product: automation engineers and SRE support.
    - Sales & Partnerships: enterprise sellers and channel leads.
    - Customer Success: onboarding, renewals, SLAs.
    - Finance & Legal: billing, SOWs, MSAs.
- Year 1 hiring snapshot:
    - 2 Senior Security Engineers.
    - 1 Sales Lead.
    - 1 Solutions Engineer.
    - 1 Customer Success Manager.
- Key operational assets:
    - Standardized engagement templates (SOW/SLA).
    - Runbooks: onboarding, incident response, remediation.
    - Playbooks: automation modules for IaC, CI/CD, runtime.

Financial Summary (High Level)

- Assumptions:
    - Year 1 (projects-heavy small base).
    - Year 2: conversions to managed services and early product sales.
    - Year 3: scale via managed recurring revenue and productization.
- Summary projections:
    - Year 1: Revenue $1.2M — Gross Profit ~$720k — Opex ~$900k — Net loss ~$180k.
    - Year 2: Revenue $3.6M — Gross Profit ~$2.52M — Opex ~$1.8M — Net profit ~$720k.
    - Year 3: Revenue $8.0M — Gross Profit ~$5.6M — Opex ~$3.2M — Net profit ~$2.4M.
- Financial targets:
    - 50% ARR from managed services by Year 3.
    - CAC payback <12 months by Year 3.
    - Blended gross margin >60% by Year 3.

Risks & Mitigations

- Sales concentration and long sales cycles:
    - Mitigation: diversify verticals, add channel partners, productize lower-touch offerings.
- Talent shortages and competition for skilled engineers:
    - Mitigation: competitive compensation, equity, contractor bench, training programs.
- Rapidly changing threat landscape:
    - Mitigation: continuous R&D, automation, and knowledge-sharing processes.
- Pricing pressure from competitors:
    - Mitigation: emphasize specialized expertise, measurable ROI, and automation-driven efficiency.

Milestones (First 12 Months)

- Months 0–3:
    - Hire core team: 2 senior engineers, sales lead, solutions engineer, CSM.
    - Develop 3 productized playbooks for IaC, CI/CD, and runtime scanning.

        - Create sales collateral and case study templates.
- Months 3–6:
    - Close 3 paid assessments.
    - Convert 1–2 clients to managed services.
    - Establish MDR onboarding playbook and tech stack.
- Months 6–12:
    - Launch 1 paid productized offering.
    - Secure 5 managed customers.
    - Target ARR ~$100k (monthly MRR ~$8–10k).
- End of Year 1:
    - Finalize SOW/MSA templates and onboarding automation for scale.

Appendix / Next Steps

- Available deliverables: full business plan (this), detailed delivery model document, 10–12 slide pitch deck (prepared).

- Immediate actions recommended:
    - Approve hires and initial budget.
    - Develop pilot engagement offers and partner outreach list.
    - Run 3 pilot assessments with conversion targets to managed services.