NoSec — Delivery Model Subtitle: Operational playbook for scalable delivery of consultancy, managed services, and productized automation.

Date: October 25, 2025

Purpose:

Provide the operational blueprint for delivering NoSec services reliably and at scale across projects, managed services, and product offerings.

Scope:

Organizational structure, staffing plan, engagement templates (SOWs), SLAs, tooling, runbooks, unit economics, quality controls, scaling playbooks.

Org Chart & Role Descriptions

- Leadership:
  - Head of Delivery: accountable for delivery quality, SLAs, staffing strategy, hiring.
  - Head of Product: owns productized automation modules and integration roadmap.
  - Head of Sales: responsible for revenue targets, GTM, partnerships.
- Delivery Team:
  - Senior Security Engineer (x2): lead engagements, architecture reviews, remediation design.
  - Pentester / Red-Team Lead: plan and execute offensive testing.
  - MDR Analysts (L1/L2): alert triage, investigation, remediation guidance.
  - Incident Response Lead: manage IR engagements; on-call rotation owner.
  - Solutions Engineer: presales demos and integration planning.
- Product & Automation:
  - Automation Engineer: build playbooks, CI/CD integrations, SOAR workflows.
  - SRE/DevOps: support managed-service infra and multi-tenant ingestion.
- Customer Success & Sales Ops:
  - CSM: onboarding, reporting, renewals.
  - Sales Lead: enterprise outreach, partner ops.
- Finance/Legal:
  - Finance: billing, forecasting.
  - Legal: SOWs, MSAs, data processing agreements.

Hiring Plan & Timeline (First 12 Months)

- Month 0–3:
    - Hire Head of Delivery (if not in-place), 2 Senior Security Engineers, Sales Lead, Solutions Engineer, CSM.
- Month 4–8:
    - Hire 2 MDR Analysts, 1 Automation Engineer, 1 Pentester.
- Month 9–12:
    - Add 2 consultants, expand MDR bench, hire Partnerships Manager.

Engagement Types & Standard Templates

- Assessment SOW (fixed-fee):
    - Elements: scope, objectives, systems in-scope, timeline, deliverables (executive summary, technical findings, remediation roadmap), acceptance criteria, fees.
    - Typical duration: 2–6 weeks.
- MDR Retainer SOW (subscription):
    - Elements: service description (monitoring, detection, triage), onboarding tasks, access requirements, reporting cadence, SLAs, fees, renewal terms.
    - Onboarding duration: up to 30 days.
- Incident Response Engagement:
    - Activation: retainer or T&M; phases: triage, containment, eradication, recovery, lessons learned; deliverables: incident report and forensic artifacts.
    - SLAs: immediate notification; reporting within 24 hours of engagement.

Onboarding Checklist (MDR example)

- Contract & Kickoff meeting.
- Identify data sources and provide connector access (logs, cloud, endpoints).
- Configure IAM for NoSec service accounts with least privilege.
- Establish baseline & tuning period (14 days).
- Define alerting & escalation contacts.
- Share runbooks & playbooks.
- Schedule weekly CSM check-ins for first 90 days.

SLAs & KPIs

- Example SLAs:
    - Critical incident triage response: ≤ 1 hour.
    - High incident triage: ≤ 4 hours.

    - Medium/Low triage: ≤ 24–48 hours.
    - MDR onboarding: ≤ 30 days.
- Operational KPIs:
    - Mean Time to Detect (MTTD).
    - Mean Time to Remediate (MTTR).
    - SLA compliance rate.
    - Ticket backlog and age.
    - Billable utilization.
    - Customer churn and NPS.

Tooling & Tech Stack (Recommended)

- Detection & logging: SIEM/XDR (customer-selected), standardized log schema.
- Automation & orchestration: SOAR for automated playbooks and incident handling.
- Static/Infrastructure scanning: tfsec, checkov, SCA tools, Trivy for image scanning.
- Collaboration & ticketing: Jira/ServiceNow; documentation in Confluence.
- Reporting: Looker, Metabase, or BI tool for dashboards.
- Repos & CI/CD: GitHub/GitLab, CI runners, IaC templates.
- Managed infra: cloud accounts with least-privilege roles; multi-tenant ingestion pipeline.

Pricing & Unit Economics

- Assumptions:
    - Senior engineer fully-loaded cost: $180k–$220k/year.
    - MDR analyst fully-loaded cost: $120k–$160k/year.
    - Target billable hourly rate: $150–$300/hr depending on role and geography.
    - Utilization: ramp from 50–60% → 65–70% by Year 2.
- Example unit economics:
    - MDR client at $15k/month → Annual revenue $180k; gross margin ~70% → gross profit ~$126k; supports ~1 FTE MDR analyst capacity and shared overhead.

Runbooks (Summaries)

- Incident Response Runbook:
    - Steps: detection → triage → containment → eradication → recovery → post-incident review.

        - Include: roles & responsibilities, escalation matrix, evidence collection checklist, communication templates.
- Onboarding Runbook (MDR):
    - Steps: kick-off → access provisioning → log mapping → baseline tuning → production monitoring → handoff to CSM.
- Vulnerability Remediation Runbook:
    - Steps: discovery → risk scoring → owner assignment → remediation window → verification → closure.

Quality Controls & Continuous Improvement

- Deliverable peer reviews (second engineer sign-off).
- Post-engagement retros and NPS surveys.
- Quarterly playbook and detection rule reviews.
- Internal knowledge base; monthly training sessions.
- Maintain contractor bench for surge capacity.

Scaling Playbooks

- Productize assessment outputs into remediation modules and automation.
- Convert recurring remediation tasks into MDR subscriptions.
- Build low-touch self-service product modules for mid-market customers.
- Partner scaling:
    - Partner onboarding kit.
    - Co-sell playbook and partner revenue-share model.
- Automation investments:
    - SOAR and integration work to reduce manual triage and per-incident cost.

Templates & Artifacts (Outlines)

- Assessment SOW Outline:
    - Title, Parties, Scope, Objectives, Deliverables, Timeline, Fees, Acceptance Criteria, Confidentiality, Terms & Conditions.
- MDR SOW Outline:
    - Service Description, Onboarding Tasks, Data & Access Requirements, Monitoring Scope, Reporting Cadence, SLAs, Fee Schedule, Renewal/Termination.
- IR Activation Checklist:

        - Contact list, notification flow, evidence preservation steps, legal hold guidance, communications plan.
- Onboarding Checklist: see Section 5.

Metrics Dashboard & Reporting

- Dashboard fields to track:
    - ARR by offering (projects vs. managed vs. product).
    - Number of managed customers.
    - Average ARR per managed customer.
    - Monthly churn percentage.
    - New bookings and pipeline value.
    - Billable utilization percentage.
    - Conversion rate: assessment → retainer.
    - MTTD and MTTR metrics.

Appendix — Sample Operational Flows (Concise)

- Assessment → Managed Conversion:
    1. Deliver 4-week assessment with prioritized remediation roadmap.
    2. Propose 6–12 month MDR retainer to address top 3 priorities.
    3. Use productized playbooks to accelerate onboarding and demonstrate ROI.
- Incident Response Engagement:
    1. Activation (retainer or T&M) → immediate triage & containment.
    2. Forensics & eradication sprints; daily update cadence.
    3. Post-incident report and remediation roadmap; follow-up remediation sprints as needed.