Next-Gen AI-Driven SIEM & XDR Platform

A modular, cloud-native cybersecurity platform combining real-time threat detection, forensic intelligence, and automated response -built for law enforcement agencies and enterprise SOC teams.

Key Activities

- End-to-end product leadership: discovery → delivery → PLG scaling
- User research with law enforcement, SOC teams, and CISOs
- Continuous MVP validation and feature iteration through usage analytics
- AI/ML model lifecycle orchestration (RAG, LLMs, Orchestration & Evaluation)
- Secure data ingestion pipelines (Kafka, Airbyte, Airflow, Mlflow, ELK)
- Cross-functional collaboration (engineering, design, data, compliance, GTM, CX)
- Enabling product-led growth via analyst onboarding flows, in-product tours, self-serve setup. Led market validation and iterative roadmap development.

Product Leadership Outcomes (Impact):

- 20% of annual company revenue driven by this suite
- Achieved PMF within 6 months through rapid MVP iteration and analyst-led discovery
- Annual churn drops from 18% → **6%** when NSM thresholds are consistently met
- Delivered +70 NPS and sustained user growth via intuitive analyst experience
- Scaled platform adoption across national security agencies and global enterprise security teams via product-led-growth, enabled double-digit MoM growth.

Customer Segments & User Personas:

- **Primary Segments**:
  - National law enforcement & digital forensics agencies
  - Enterprise SOC teams in BFSI, telecom, energy, and critical infrastructure
  - Managed Security Service Providers (MSSPs)
- **User Personas**:
  - SOC Analyst: Needs intuitive dashboards, automated triage, threat correlation
  - Security Investigator: Needs forensic visibility, drill-down access, case timelines
  - Platform Admin: Needs role-based access control, audit trails, and deployment tooling
  - Compliance Officer: Needs logs, retention policies, regulatory dashboards.

Problem Space (Needs & Challenges)

- Fragmented SIEM and XDR tooling with poor interconnectivity
- Long time-to-detect/respond (TTD/TTR) due to alert fatigue and lack of automation
- Limited forensic traceability and explainability in ML models
- High integration overhead with existing EDR, SOAR, and threat intel systems
- Rigid compliance environments (NIST, GDPR, SOC2, HIPAA)

Value Propositions

- Proactive threat detection using behavioural analytics and LLM-based correlation

- Forensic-grade investigations via full event replay, agent paths, and timeline reconstruction
- Automated response orchestration with RAG + agentic workflows
- Flexible integrations with EDRs, SOARs, vector DBs, and log pipelines
- Compliant by design: RBAC, audit logging, and data retention governance
- Self-serve and scalable: Built for easy onboarding, trial, and expansion

Revenue Streams

- Tiered enterprise SaaS licensing (based on volume, modules, integrations)
- Add-ons for advanced analytics, compliance packs, or model explainability tooling
- MSSP/partner licensing for white-label deployments

Strategy (Development & Go-To-Market)

- Land-and-expand with analyst-centric trials, role-based dashboards, and auto-detection templates
- Use security demos, guided walkthroughs, and in-product chat to support onboarding
- Drive PLG via free trials, SOC automation libraries, and usage-based feature unlocking
- Enable top-down sales for regulated sectors, with pilot-to-production pipelines

NSM (North Start Metrics)

Number of Active Investigations Successfully Resolved via Automated Detection & Forensic Insights per Customer per Month.

Key Resources

- AI/ML Engineers (RAG, model tuning, evaluation pipelines)
- Product & Design Team (platform UX, PLG loops, self-serve tooling)
- Infra + Security Ops (deployment, cloud security, data retention)
- Compliance & Governance Experts (NIST, SOC2, GDPR, HIPAA alignment)

Key Partners

- Vector database providers (Pinecone, Elastic)
- Security stack integrators (SOAR, EDR, threat intel feeds)
- Channel & regional MSSP partners for public sector/governments

Channels

- Direct sales for law enforcement, enterprise security, and compliance-driven verticals
- Product-led acquisition via trial, community forums, and SOC templates
- Events, security webinars, analyst briefings, and partner co-selling
- Content-driven inbound (blog tutorials, case studies, explainer videos)

Customer Relationships

- In-product support via chat, diagnostics, guided setup
- Community-driven content: analyst playbooks, threat libraries, explainability packs
- Dedicated CS & technical support for enterprise and regulated customers
- Regular feedback loops through beta programs and roadmap previews.