SkyScan - Launch Plan & Adoption Strategy

Overview

SkyScan is the first product under the BlueSky Consulting brand - a one-click threat intelligence dashboard that scans cloud assets (public IPs) against known threat intelligence feeds. The goal is to deliver immediate value, foster organic adoption, and build a strong base of early users.

Week 1 - Foundations & Threat Intel Setup

- Day 1: Finalize product name, branding, and create GitHub repo.

- Day 2: Set up FastAPI backend skeleton + SQLite or JSON for data.

- Day 3: Identify and test 3-5 threat intelligence feeds (e.g., CISA KEV, URLHaus).

- Day 4: Build feed ingestion scripts (basic normalization).

- Day 5: Write IP input handling (manual CIDRs/IPs).

- Day 6: Draft initial matcher logic (IP comparison, feed scanning).

- Day 7: Create UI wireframe + README with vision, use cases, and setup instructions.

Week 2 - Backend + Core Matching Logic

- Day 8: Improve feed normalization + standard schema.

- Day 9: Build IP/domain matcher with support for CIDRs.

- Day 10: Build and test REST API endpoints for scan initiation and result fetching.

- Day 11: Create minimal frontend HTML page (manual input + results).

- Day 12: Create test cases and mock scan data.

- Day 13: Add scan timestamping and local storage in DB.

- Day 14: Refactor and clean code, prepare for frontend integration.

Week 3 - Frontend + Share Features

- Day 15: Build out UI components for results table, search, and filtering.

- Day 16: Add CSV/JSON export buttons.

- Day 17: Create unique shareable scan links (base64 encoded or UUID).

- Day 18: Implement simple scan history view (local).

- Day 19: Add error handling, loading states, and UX polish.

SkyScan - Launch Plan & Adoption Strategy

- Day 20: Write blog-style documentation for usage and examples.

- Day 21: Build landing page copy, CTA sections, email opt-in setup.

Week 4 - Polish, Publish, Promote

- Day 22: Dockerize the app, ensure it runs locally and on cloud.

- Day 23: Deploy frontend + backend using Vercel, Render, or Fly.io.

- Day 24: Test the full flow with external IPs and live threat feeds.

- Day 25: Prepare launch post drafts for Reddit, Twitter, and LinkedIn.

- Day 26: Post on GitHub with project tags and SEO keywords.

- Day 27: Share to Discord groups, subreddits, and relevant newsletters.

- Day 28: Launch on Product Hunt and track early user feedback.

Adoption & Marketing Strategy

Target Users:
- Cloud Engineers and DevSecOps: looking for fast visibility.
- Security Analysts: need real-time external threat awareness.
- MSSPs & Freelancers: need tools for multi-client threat scans.
- Small startups: can't afford expensive cloud security platforms.

Adoption Strategy:
- Zero-friction use: No signup, no install, instant scan.
- Shareable results: Users can post their scans or send to others.
- Organic traffic: Use SEO on landing page (e.g., "CISA threat scanner for AWS").
- Community launch: Post to Reddit (/r/sysadmin, /r/netsec), Hacker News, DevSecOps Discords.
- Social content: Launch thread on Twitter/X with visuals.
- Early access list: Email opt-in for alerts or team features.

Monetization Hooks (Optional):
- Alerts via webhook or email (free tier + premium).
- Scan history and analytics dashboard.
- White-labeled PDF reports for auditors.
- Team plans with shared results and settings.

Pitch-Readiness:
Once 100+ users and positive engagement are secured, the product is ready to pitch for:
- Web3 or cybersecurity grants
- VC pre-seed investments
- Strategic partnerships in the Blue Team space