**Roadmap**

**Current Version: v0.x (Initial Release)**

The AI Scraping Defense Stack is in its early stages, providing a containerized anti-scraping defense system with real-time filtering, tarpitting, behavioral analysis, and AI-driven threat assessment.

**Short-Term Goals (Next 3-6 Months)**

These features and enhancements are prioritized for near-term development:

* **Expanded ML Heuristics** – Improve the trained **Random Forest model** for better bot detection accuracy.
* **Adaptive Rate-Limiting** – Implement dynamic rate limits based on historical request patterns.
* **Improved Admin UI** – Expand dashboard analytics for better visibility into bot trends and blocked traffic.
* **Better IP Reputation Handling** – Enhance integrations with public/community blocklists for real-time threat assessment.
* **Automated Testing Suite** – Develop a suite of test cases to validate detection mechanisms and tarpitting responses.
* **Refined Markov Chain Tarpit** – Optimize PostgreSQL-backed deterministic content generation for better bot engagement.

**Mid-Term Goals (6-12 Months)**

Expanding feature sets and refining system efficiency:

* **Multi-Tenant Support** – Enable easier deployment for multiple websites and organizations.
* **Kubernetes Scaling Enhancements** – Improve Helm charts and autoscaling options for large-scale deployments.
* **Plugin API for Custom Rules** – Allow user-defined filtering rules for specialized site protection needs.
* **Expanded Honeypots** – Introduce more deceptive mechanisms like **auto-generated bad API endpoints**.
* **Anomaly Detection via AI** – Move beyond heuristics and integrate **anomaly detection models** for more adaptive security.
* **Public Community Blocklist** – Optional contributor-driven IP reputation database.

**Long-Term Vision (Beyond 12 Months)**

Larger-scale improvements and broader adoption:

* **Federated Model for Threat Intelligence Sharing** – Establish **peer-to-peer collaboration between deployments** to exchange bot intelligence.
* **Cloud-Based Management Dashboard** – Provide **hosted real-time monitoring** for multiple installations.
* **Industry Partnerships** – Integrate with cybersecurity initiatives and FOSS security groups for wider adoption.
* **Automated Configuration Recommendations** – AI-driven suggestions for optimal firewall/tarpit settings based on incoming traffic patterns.

**How to Contribute**

If you're interested in contributing to one of these features, check out the open **Issues** on GitHub and follow the guidelines in CONTRIBUTING.md.