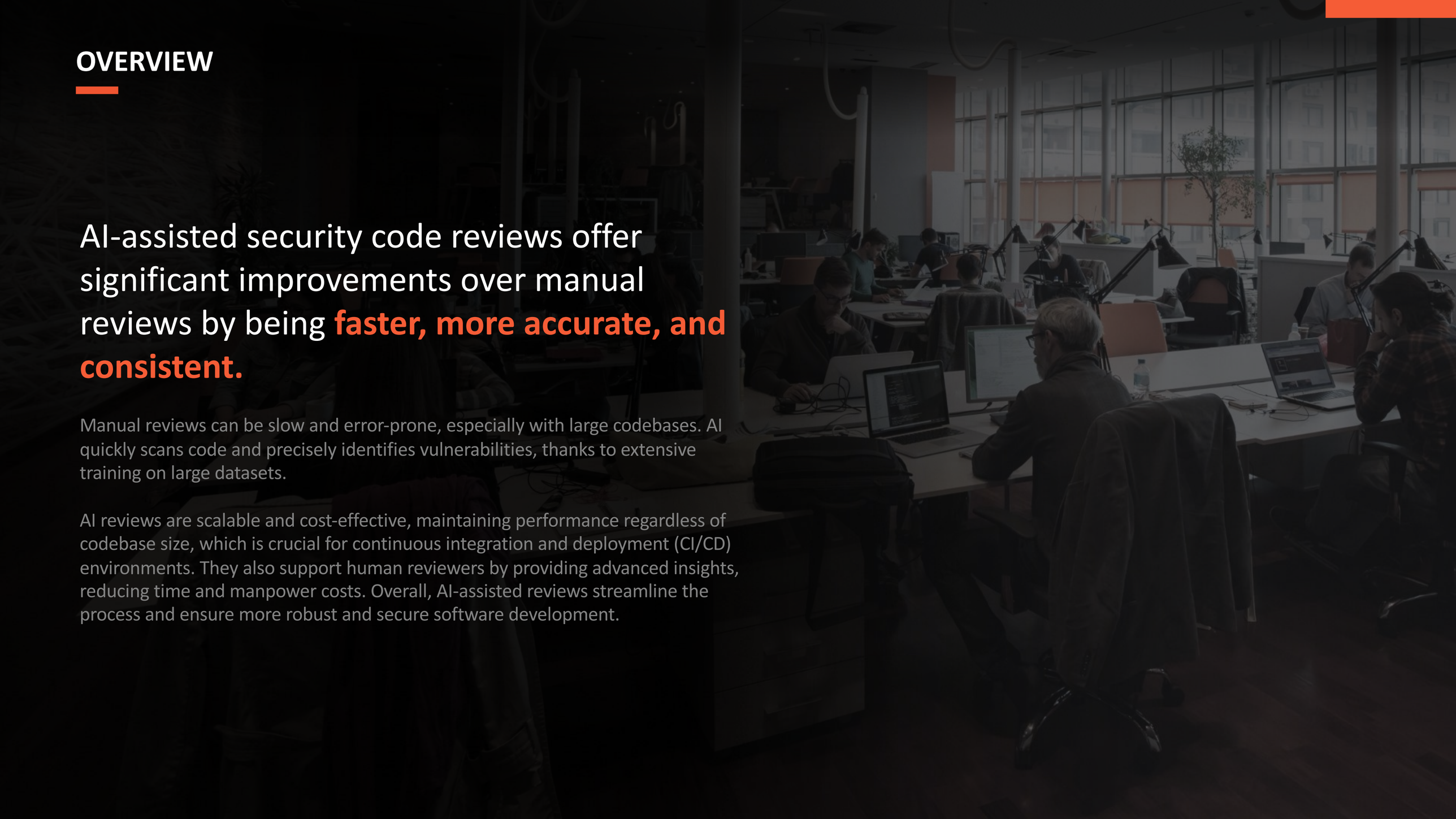
AI ASSISTED CODE REVIEW

OVERVIEW



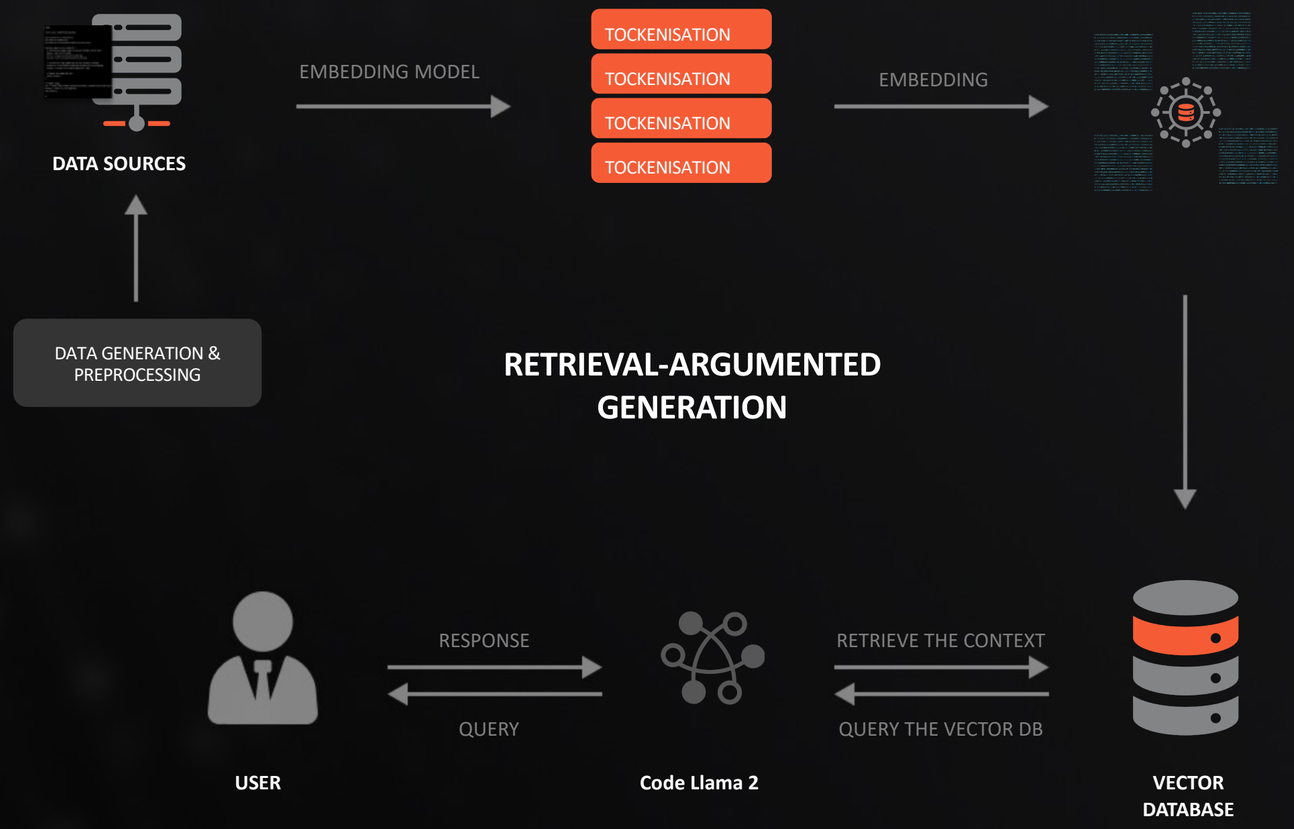
AI-assisted security code reviews offer significant improvements over manual reviews by being **faster, more accurate, and consistent.**

Manual reviews can be slow and error-prone, especially with large codebases. AI quickly scans code and precisely identifies vulnerabilities, thanks to extensive training on large datasets.

AI reviews are scalable and cost-effective, maintaining performance regardless of codebase size, which is crucial for continuous integration and deployment (CI/CD) environments. They also support human reviewers by providing advanced insights, reducing time and manpower costs. Overall, AI-assisted reviews streamline the process and ensure more robust and secure software development.

HIGH LEVEL DIAGRAM (HLD)

AI Assisted
Security Code Review
with Locally Hosted LLM

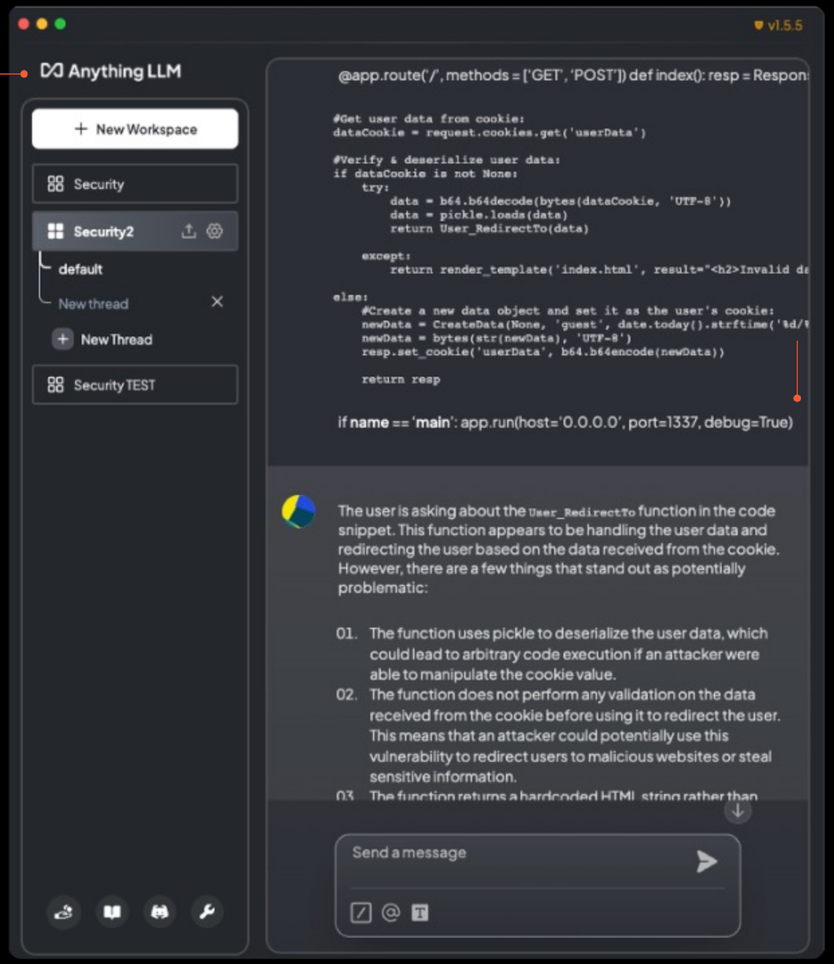


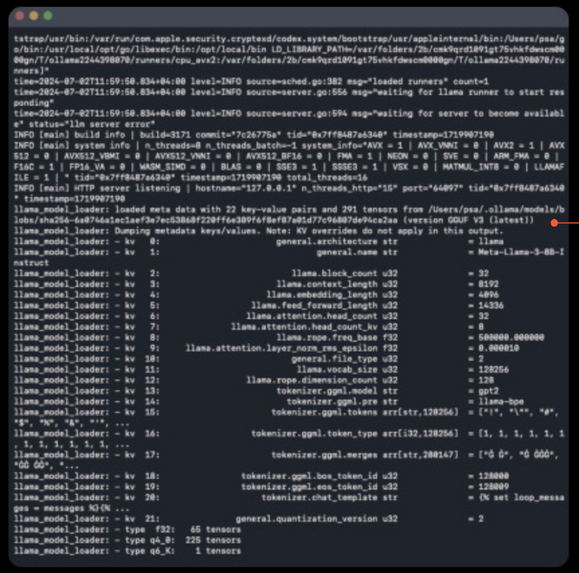
MANUAL VS AI ASSISTED CODE AUDITS

METRICS	MANUAL	AI ASSISTED (LLAMA 3)	OUTCOMES
REVIEW RATE	400 Lines of Code / Hour i.e. 2400 Lines of Code / Day	2500 Lines of code in few minutes with 32k context on high end Laptop – Can be greater depends on the underlying compute power.	e.g. 10k lines of code can be reviewed with AI Assistance in 4 hours whereas ~5 Man Days of manual effort is required for the same. **90% improvement in lead time**
TECHNOLOGY	Proficiency in 2-3 programming Languages eg Python , C/ C++ , Java	Can audit any programming language, depends on the language model trraining set.	Ensure enhanced coverage over a large number of technologies. **Reduces number of resources** required to carry out similar execution, reducing manpower cost.
SCALIBILITY	Requires additional skilled resources to accommodate large projects and frequent changes	Easily scalable to accommodate large projects and frequent code changes.	For auditing 100k lines of code, around 4 Experts are required to work ~8 Days, considering staffing a new available expert in the team takes 1-2 weeks on average. With AI Assisted reviews quick turnaround is expected similar review can be carried by an individual in ~10 days. **Saving upto 75% on Manpower Cost.**
CONSISTENCY	Potential for oversight or missed vulnerabilities due to fatigue or lack of expertise in certain areas.	Provides consistent results without the variability inherent in human reviews, ensuring a uniform level of scrutiny across the entire codebase.	**Consistent quality of work and enhanced throughput.**

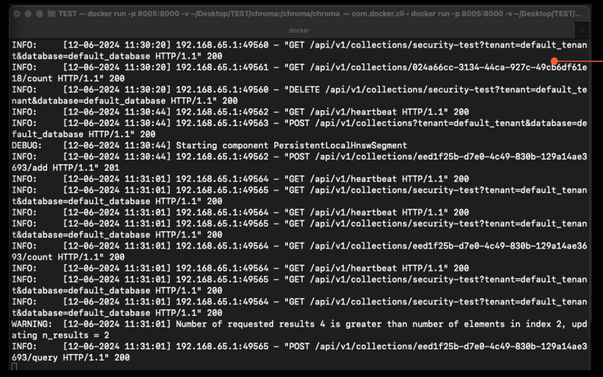
AI ASSISTED SECURITY CODE REVIEW IN ACTION

INTERACTIVE INTERFACE



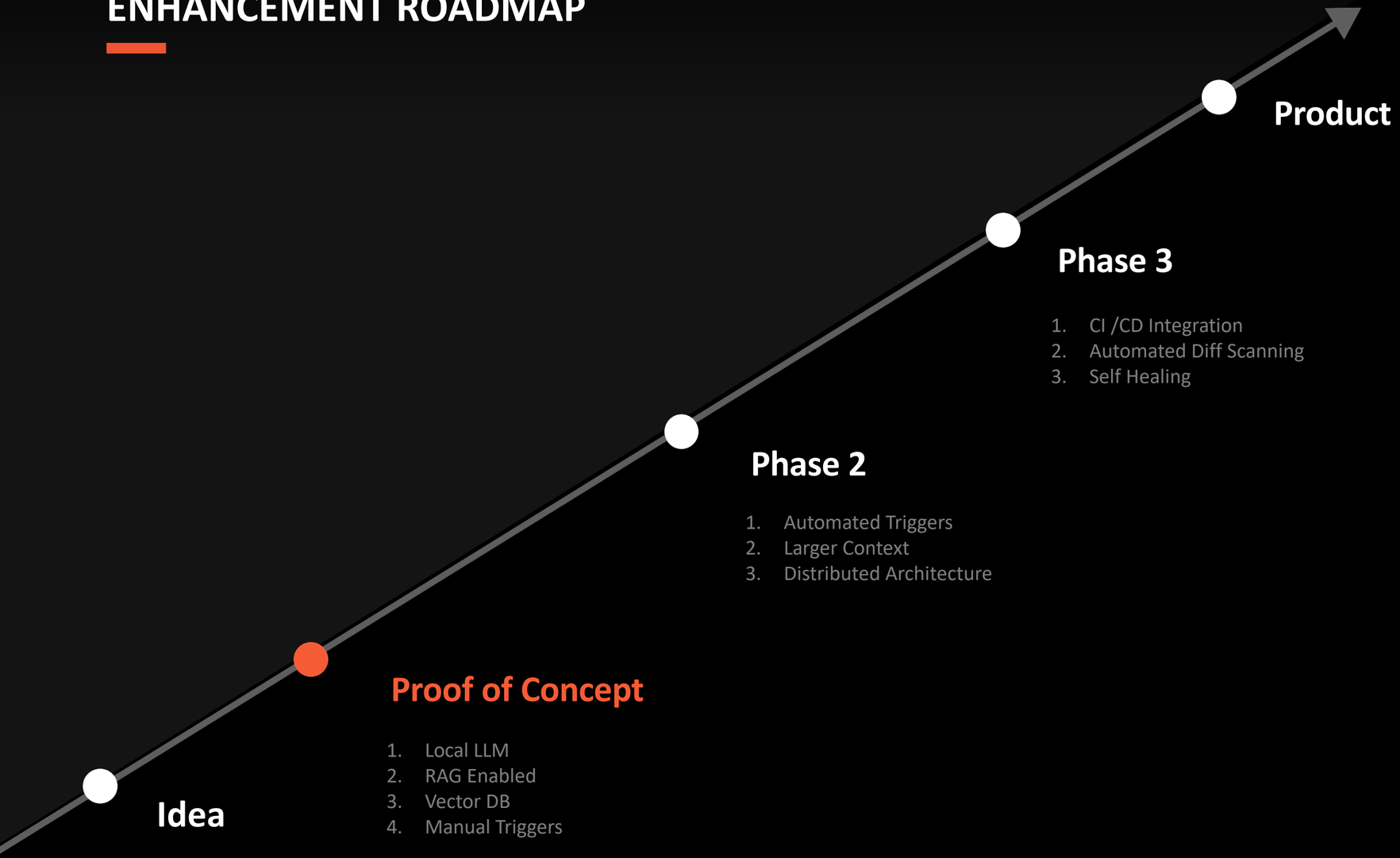


LOCAL LLM



VECTOR DB

ENHANCEMENT ROADMAP



Idea

Proof of Concept

1. Local LLM
2. RAG Enabled
3. Vector DB
4. Manual Triggers

Phase 2

1. Automated Triggers
2. Larger Context
3. Distributed Architecture

Phase 3

1. CI /CD Integration
2. Automated Diff Scanning
3. Self Healing

Product

THANK YOU.