black hat
MIDDLE EAST AND AFRICA

02 - 04 DECEMBER 2025
RIYADH EXHIBITION AND CONVENTION CENTER, MALHAM, SAUDI ARABIA

FalconEYE
Local LLM powered Code Review

Hardik Mehta (hardw00t)
Rajanish Pathak (h4ckologic)

ORGANISED BY:

tahaluf an informa company

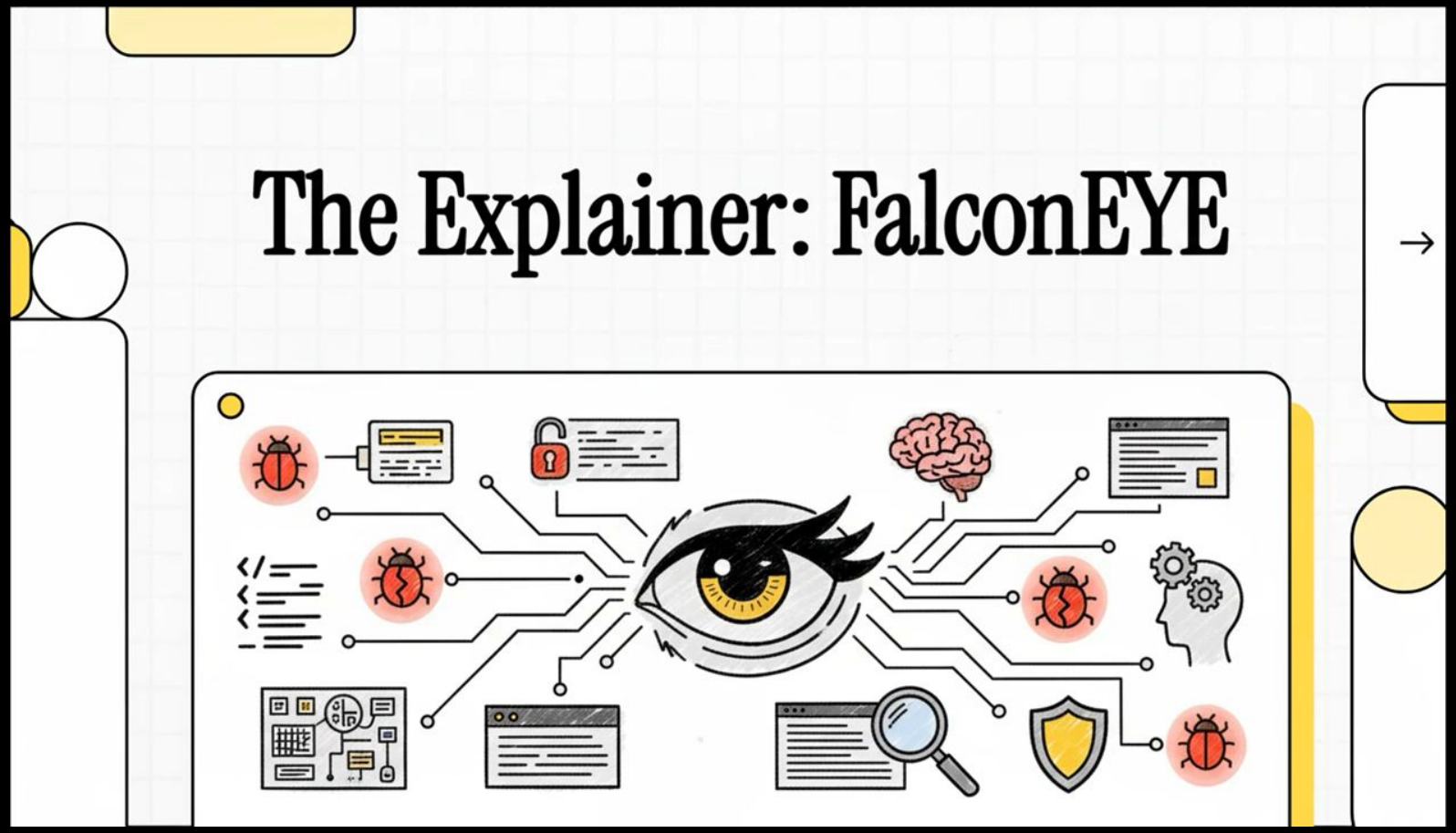
الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

IN ASSOCIATION WITH:

black hat

black hat
MIDDLE EAST AND AFRICA

FalconEYE
Local LLM powered Code Review



Why Traditional Security Scanners Fall Short

Traditional security scanners are limited by their pattern databases. They can only find what they've been programmed to look for, leaving critical gaps in your security posture.

Blind to Context

They match patterns but don't understand *intent*. They can't see how different parts of your code interact, missing vulnerabilities that span multiple files or depend on business logic.

Noise & False Positives

Limited by rigid rules, they generate a flood of alerts. Critical vulnerabilities get buried in the noise from pattern-based false alarms.

One Step Behind

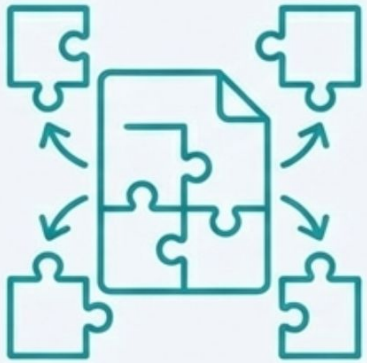
They are fundamentally reactive. They can only find *known* vulnerability patterns and miss novel, complex, or application-specific flaws unique to your codebase.

A Paradigm Shift: Reasoning, Not Pattern Matching

FalconEYE represents a new approach to static code analysis. Instead of relying on predefined patterns, it leverages large language models to reason about your code the same way a security expert would—understanding context, intent, and subtle security implications.

Semantic Reasoning

Uses pure AI to understand your code's logic and data flow, not just its syntax.



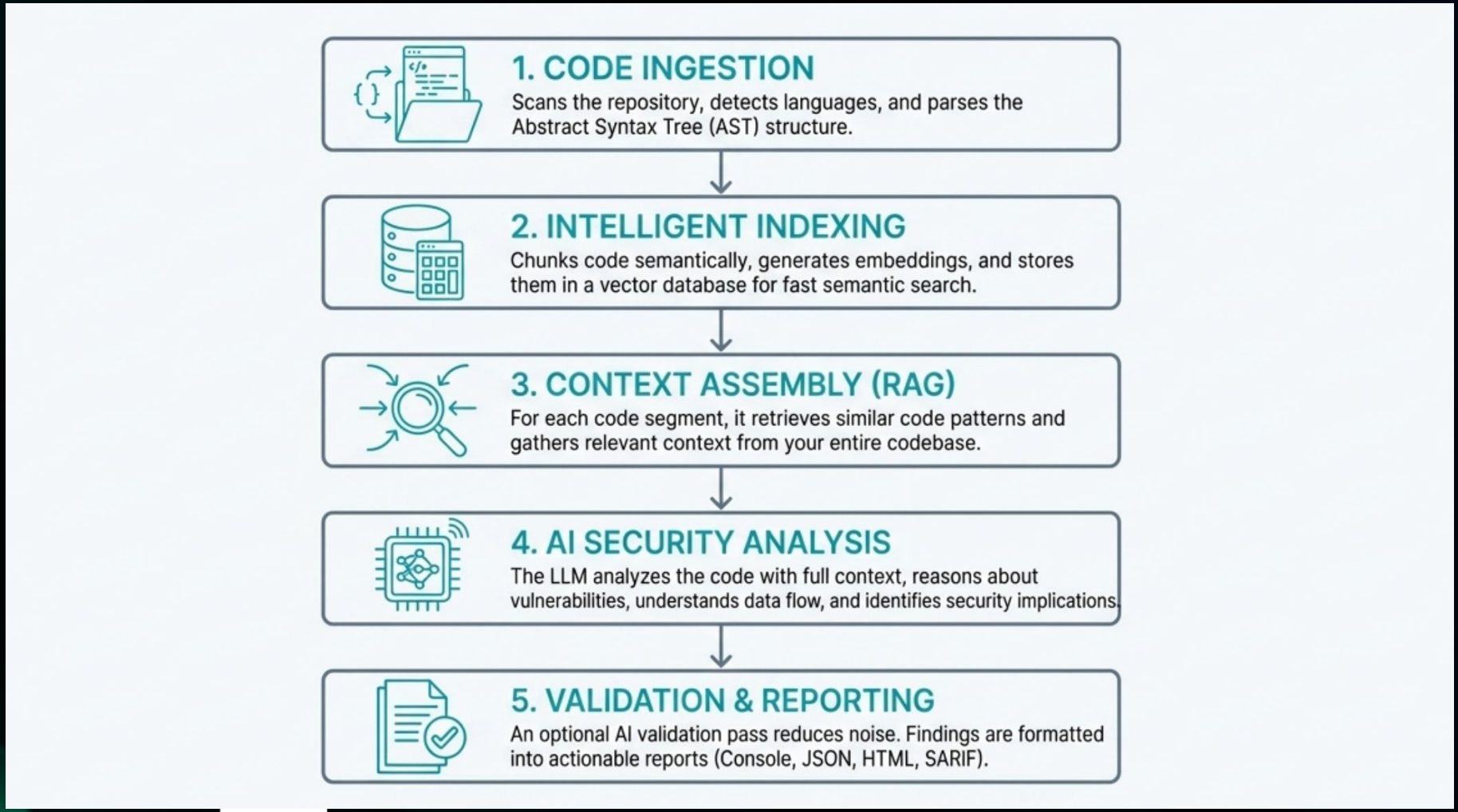
Context-Aware Analysis

Retrieval-Augmented Generation (RAG) provides relevant code context from your entire repository for deeper, more accurate insights.

Privacy-First by Design

Runs entirely locally with Ollama. Your code never leaves your machine. Period.

From Code to Insight: The 5-Step Analysis Pipeline



Deeper Insights, Higher Confidence

RAG-Enhanced Context

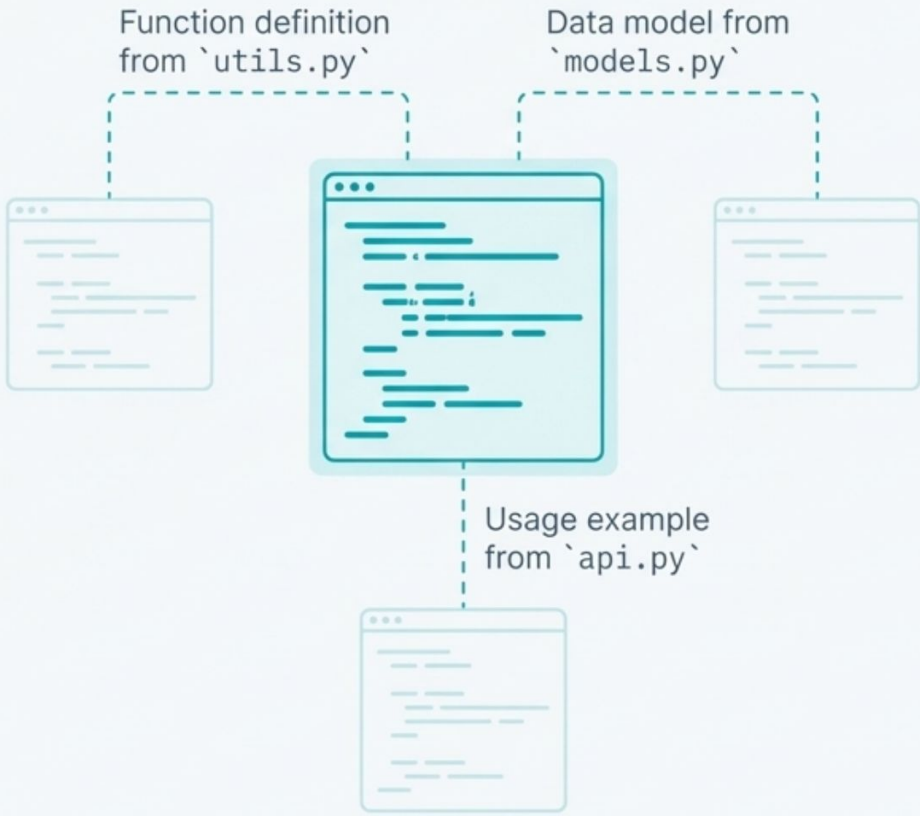
Finds complex issues that span multiple files by understanding how functions are actually used across your application, what data they handle, and their potential security implications.

Confidence Scoring & CWE Mapping

The AI doesn't just find issues; it rates its confidence in each finding and maps vulnerabilities to the industry-standard Common Weakness Enumeration (CWE) for easier triage and remediation.

Reduced False Positives

An optional AI validation pass acts as a second opinion on initial findings. This dramatically reduces noise and allows your team to focus on real, verifiable threats.



black hat MIDDLE EAST AND AFRICA

Powerful, Performant, and Private by Design

Smart & Fast

Incremental analysis is a game-changer. After the initial scan, FalconEYE tracks file changes and only re-analyzes what's new or modified, making subsequent scans dramatically faster.

Privacy-First

Runs 100% locally with Ollama. No exceptions. Your intellectual property and sensitive code never leave your environment.

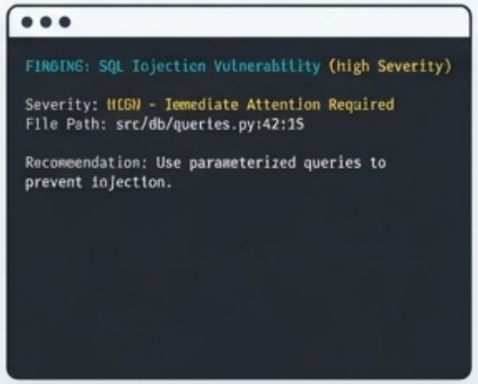
Robust Processing

Built for real-world codebases with parallel processing, smart caching, and graceful degradation, ensuring a smooth and reliable analysis even when individual files fail to parse.

Production-Ready Architecture

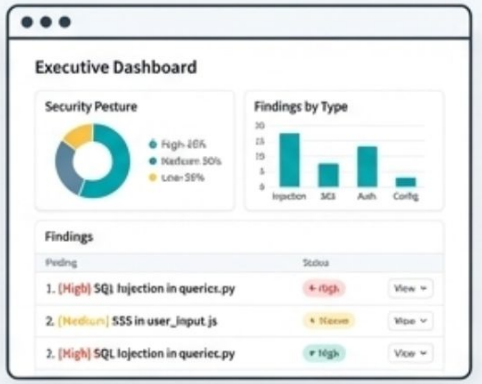
Includes circuit breakers, exponential backoff retries, and structured JSON logging for enterprise-grade reliability.

Your Findings, Your Format



Console

Rich, color-coded terminal output with clear severity levels and recommendations for immediate feedback during development.



HTML

Auto-generated interactive reports with executive dashboards and statistics, perfect for sharing with management and tracking progress.

JSON

A clean, machine-readable format for custom integrations, scripting, and programmatic processing of findings.

SARIF

The industry-standard format for seamless integration with CI/CD and DevSecOps platforms like GitHub Advanced Security and GitLab.

Security Analysis Across Your Entire Stack

Python • JavaScript • TypeScript • Go • Rust • C/C++ • Java • Dart • PHP

Extensible by Design: Our plugin system allows you or the community to add new languages and implement tailored, language-specific security prompts.

Your First Scan is Three Commands Away

Prerequisites:

- Python 3.12+ installed
- Ollama running locally

1. Pull Required AI Models

```
ollama pull qwen3-coder:30b
ollama pull embeddinggemma:300m
```

2. Install FalconEYE

```
pip install -e .
```

3. Run Your Scan

```
falconeye scan /path/to/your/project
```

black hat
MIDDLE EAST AND AFRICA

Stop Matching. Start Understanding.

Find What Others Miss

Detects novel, context-dependent, and business logic vulnerabilities that pattern-based scanners are blind to.

Eliminate Alert Fatigue

Drastically reduces false positives through AI-powered reasoning and an optional validation pass.

Own Your Security & Your Code

100% local and private analysis ensures your most valuable assets never leave your control.

Integrate Seamlessly

Built for modern CI/CD and developer workflows with industry-standard SARIF output and a powerful CLI.

Built for security engineers who demand more than pattern matching.

Contribute to the Future of Code Security

FalconEYE is an open-source project, and we welcome contributions from the community to make it even more powerful.

- **Language Support:**
  Add support for new programming languages via the plugin system.

- **Performance:**
  Help optimize analysis speed and memory usage.

- **Integrations:**
  Build integrations with more security platforms and developer tools.

- **Output Formats:**
  Implement new report formats like PDF or CSV.

Fork the repository, submit pull requests, and help shape the next generation of security analysis.

github.com/FalconEYE-ai/FalconEYE