SHIELDY

THE AI SECURITY ASSISTANT

By Ismael Gonzalez

AIE8 - AI Makers Space

PROBLEM STATEMENT.

Small and medium businesses struggle to implement basic security practices due to overwhelming, expensive, and generic guidance that doesn't fit their limited budgets and IT resources.

WHY IS THIS A PROBLEM?

60% of small businesses close within 6 months of a cyber attack

- **Overwhelming**: Security standards contain hundreds of controls—where do you start with 2 IT staff and no security expertise?
- **Expensive**: Security consultancy is very expensive, just for an assessment, and putting proper guidance
- **Generic**: ChatGPT and online guides give one-size-fits-all advice that doesn't consider your reality

SOLUTION OVERVIEW.

OVERVIEW

Shieldy is an AI-powered security assistant that transforms overwhelming security frameworks into personalized, actionable guidance for small-medium businesses.

SOLUTION

Users interact through a clean web interface where they can either:

- request a security assessment in minutes and get a report with prioritized recommendations
- search for implementation help and receive step-by-step guides

USER EXPERIENCE

The experience feels like having a knowledgeable security consultant on-demand—fast, specific, and practical, without having to read 500-page standards

THE TECH STACK

LLM
gpt-4o-mini

EMBEDDINGS
text-embedding-3-small

ORCHESTRATION
LangGraph

VECTOR DB
Qdrant

MONITORING
LangSmith

EVALUATION
RAGAS

FRONTEND
React + Vite + Tailwind

BACKEND
FastAPI

THE DATA SOURCE

AWS SECURITY CONFIGURATION GUIDANCE

CIS Amazon Web Services Foundations Benchmark v6.0.0

Type: PDF

WEB APPLICATION SECURITY REQUIREMENTS

OWASP ASVS 5.0

Type: PDF

REAL TIME WEB SEARCH

Tavily Search API

Type: REST API

Chunking Strategy:

RecursiveCharacterTextSplitter (1500 tokens, 200 overlap)

THE GOLDEN TEST DATA SET

- 2 Personas:
  - Cloud Engineer
  - Security Engineer
- 60 synthetic questions about security frameworks
- Query Distribution:
  - SingleHopSpecificQuery (50%)
  - MultiHopSpecificQuery (50%)

ADVANCED RETRIEVAL

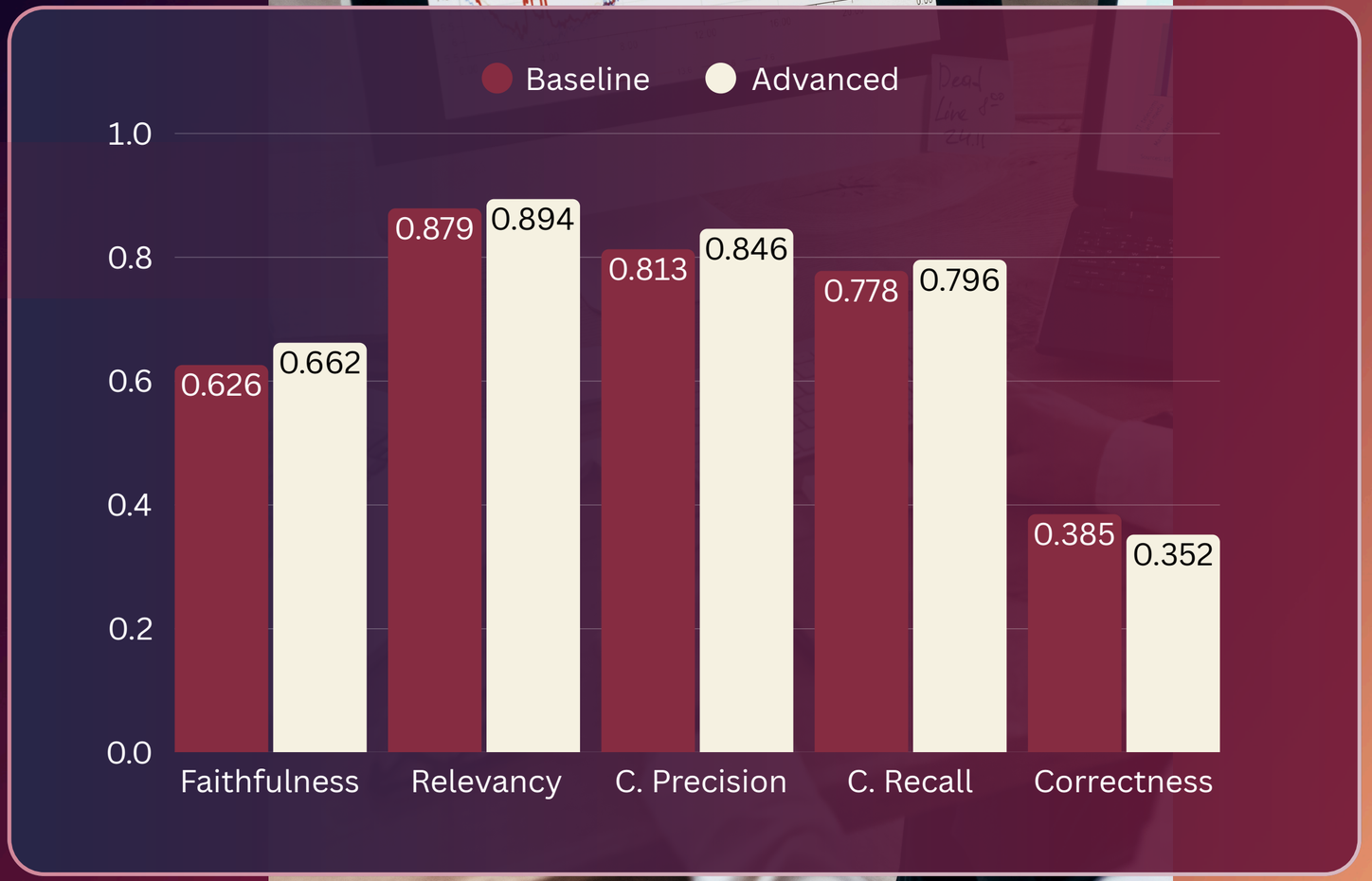
ENSEMBLE RETRIEVAL

Vector Search (Semantic)
BM25 Retriever
Contextual Compression (Reranking)

Gets best of both worlds—catches exact terms AND conceptual relationships

ASSESSING PERFORMANCE

- Ensemble retrieval (Vector + BM25 + Cohere) measurably improves the system.
- Cost is minimal (+$0.01/query, +200ms latency), quality gains are real.
- NOTE: Factual correctness decreased because our prompt encourages detailed



LET'S DEMO IT!

SHIELDY

click here!