INCOSE Healthcare Working Group

CPAMS

Cybersecurity Post-Market Analysis and Monitoring System

Gerald Rigdon

Fellow, SW Engineering

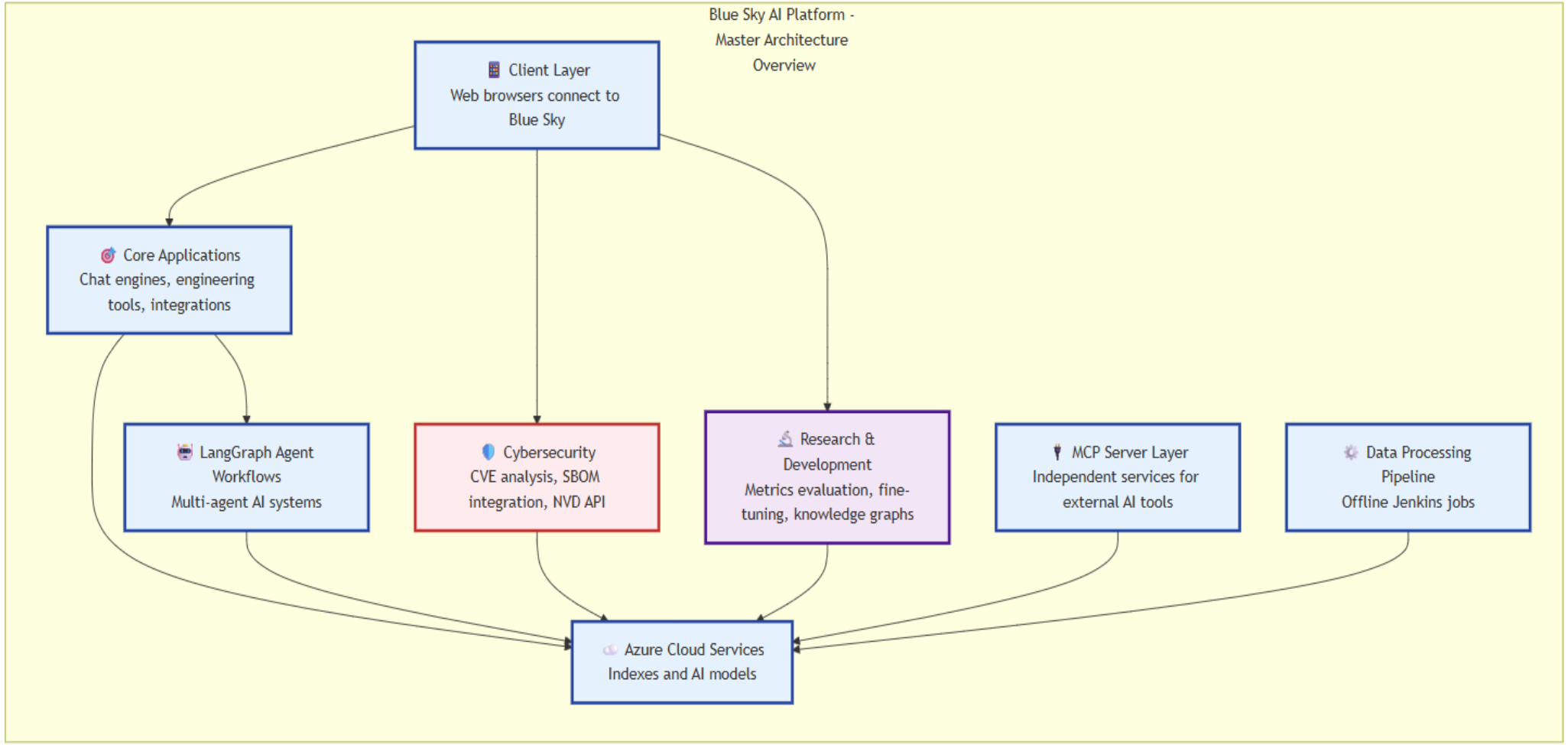
gerald.rigdon@bsci.com

INCOSE Healthcare Working Group

Project Blue Sky

INCOSE Healthcare Working Group

What is Project Blue Sky?



Blue Sky Web App Tools

- Community Blog
- Academy
- Open Chat & Personal Azure Indexing
- Repository Chat
- Deep Research Chat
- Code Review Clinic
- Documentation Generator
- Platform Integrations
- Research Center
- Cybersecurity Monitoring (CPAMS)

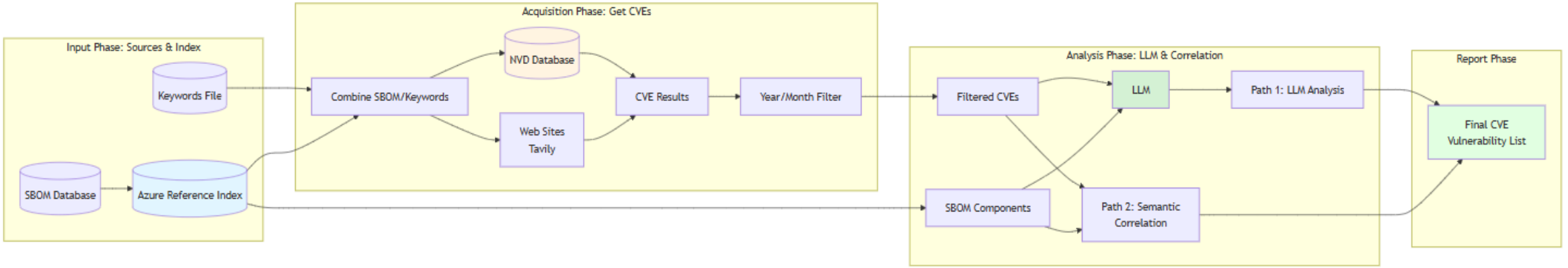
The Problem: Post-Market Cyber Risk

- **Medical devices contain third-party software components (SBOM)**
  - Bluetooth stacks, TCP/IP libraries, RTOS kernels, wireless chipsets
- **New CVEs are published daily — manual monitoring is not scalable**
  - NVD publishes 20,000+ CVEs per year
  - Relevant vulnerabilities may go undetected for months
- **Regulators require ongoing post-market surveillance**
  - Manufacturers must assess exploitability and patient risk
- **Challenge: Correlate CVEs to your specific software inventory**

CPAMS — System Overview

- **Integrated into BlueSky: an AI-augmented engineering platform**
- **Multiphase pipeline:**
  - Input → SBOM, Keywords
  - Acquire → Vulnerability search (NVD, Web, Azure Vector DB)
  - Analyze → Dual-path. AI analysis / Semantic correlation against software inventory
  - Report
- **User-configurable keywords, web domains, and SBOM index**
- **Exports: CSV, JSON, Markdown AI report**
- **Built on: Python, Streamlit, LangChain, Azure AI Search**
- **LLM: Configurable (GPT-5, Claude Sonnet 4.5, etc.)**
- **Embedding model: text-embedding-3-large**

CPAMS Architecture



Architecture & Azure Integration

- **Azure SBOM Reference Index**
  - Stores SBOM documents
- **Per-user file storage: custom keywords, domains, filter terms**
- **Embeddings**
  - CVEs from NVD
  - SBOM key terms

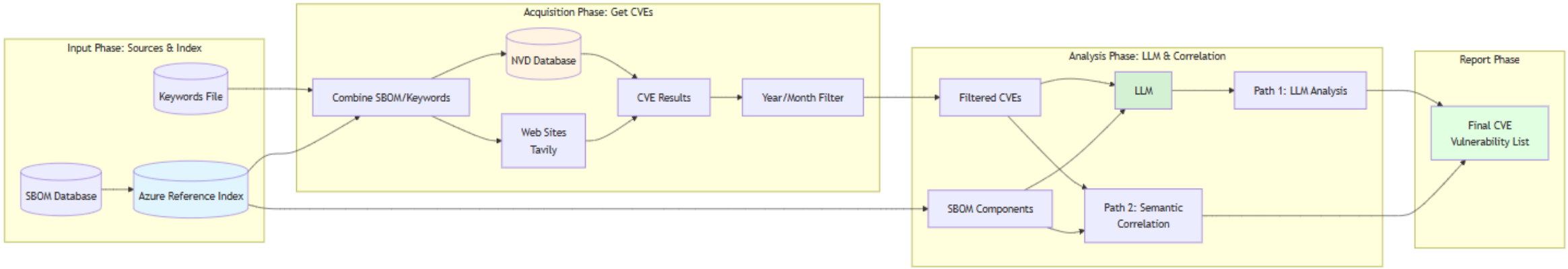
Input Phase: Multi-Source Vulnerability Search

- **SBOM-driven search: extract component names from uploaded inventory**
- **Custom keyword-driven search**
- **LLM-enhanced query expansion**
  - Automatically adds synonyms, vendor names, related technologies

Final Keyword Search List = SBOM + Custom Keywords + LLM expansion

- **Year-range and custom filter term support**
- **Search sources:**
  - NVD (NIST) — official CVE records
  - Vendor Websites — security advisories, bulletins
  - Web Search (Tavily API) — supplemental CVE advisories

CPAMS – Input Phase



Looking at CPAMS Inputs

Items included in SBOMs are:

- The software packages, libraries, and modules used (open source, commercial, or proprietary)
- Metadata such as creation date, SBOM author, and format details, etc.
- Component version numbers and supplier details

Custom Keywords File

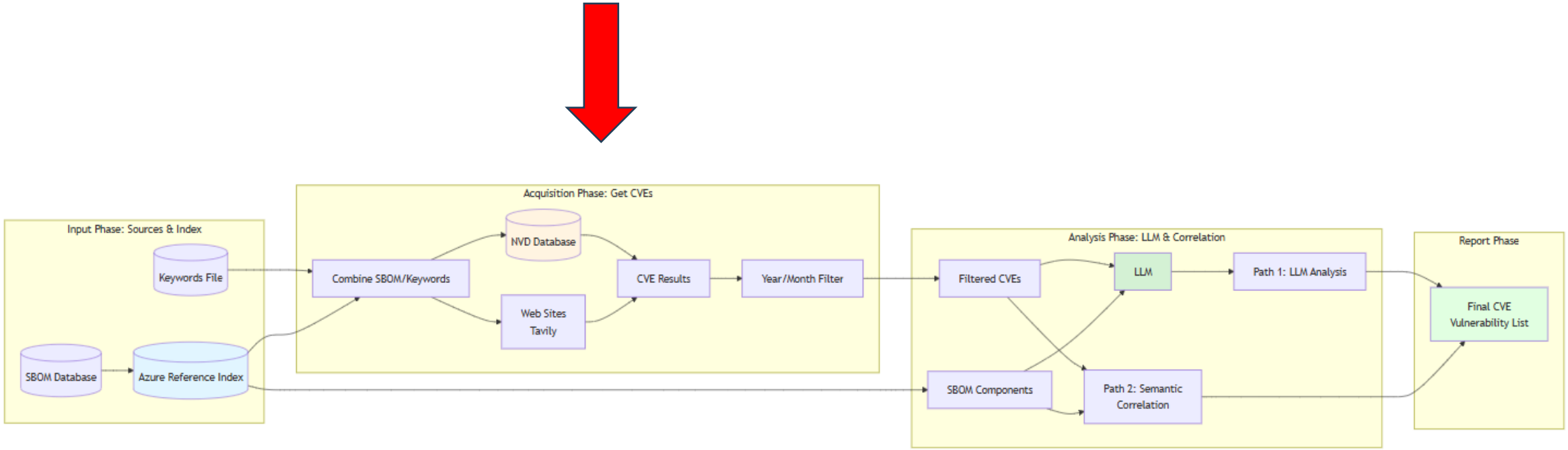
```
# Custom Keywords for Cybersecurity Search
# Add one keyword per line
# Lines starting with # are comments

# Saved keywords:
treck
bluetooth
bluetooth core
BLE
dialog
renesas
riviera
waves
CEVA
ricow
```

SBOM – Example

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "components": [
    {
      "name": "library-a",
      "version": "1.2.3",
      "supplier": "vendor-x",
      "license": "Apache-2.0",
      "hashes": ["sha256..."]
    },
    {
      "name": "library-b",
      "version": "4.5.6",
      "supplier": "vendor-y",
      "license": "MIT"
    }
  ]
}
```

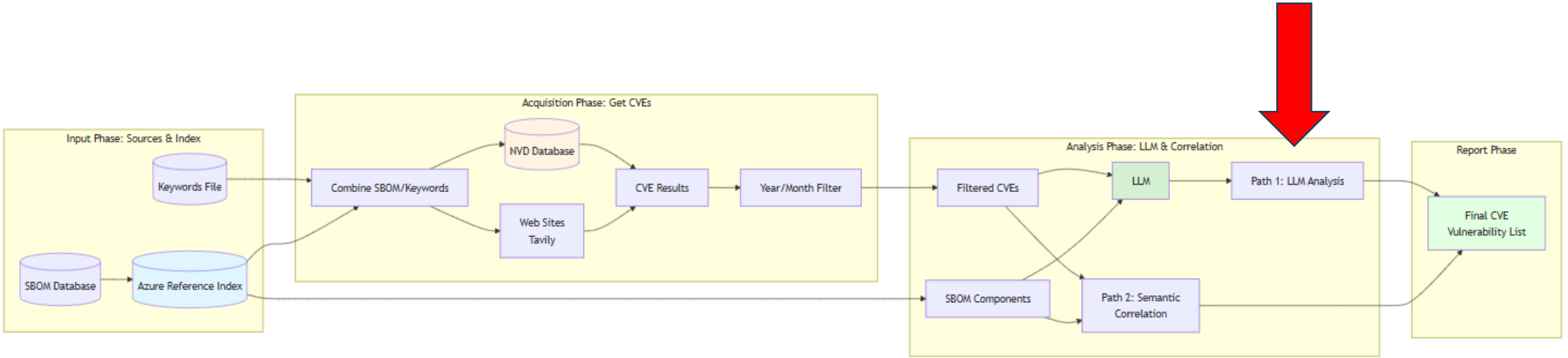
CPAMS – Acquisition Phase



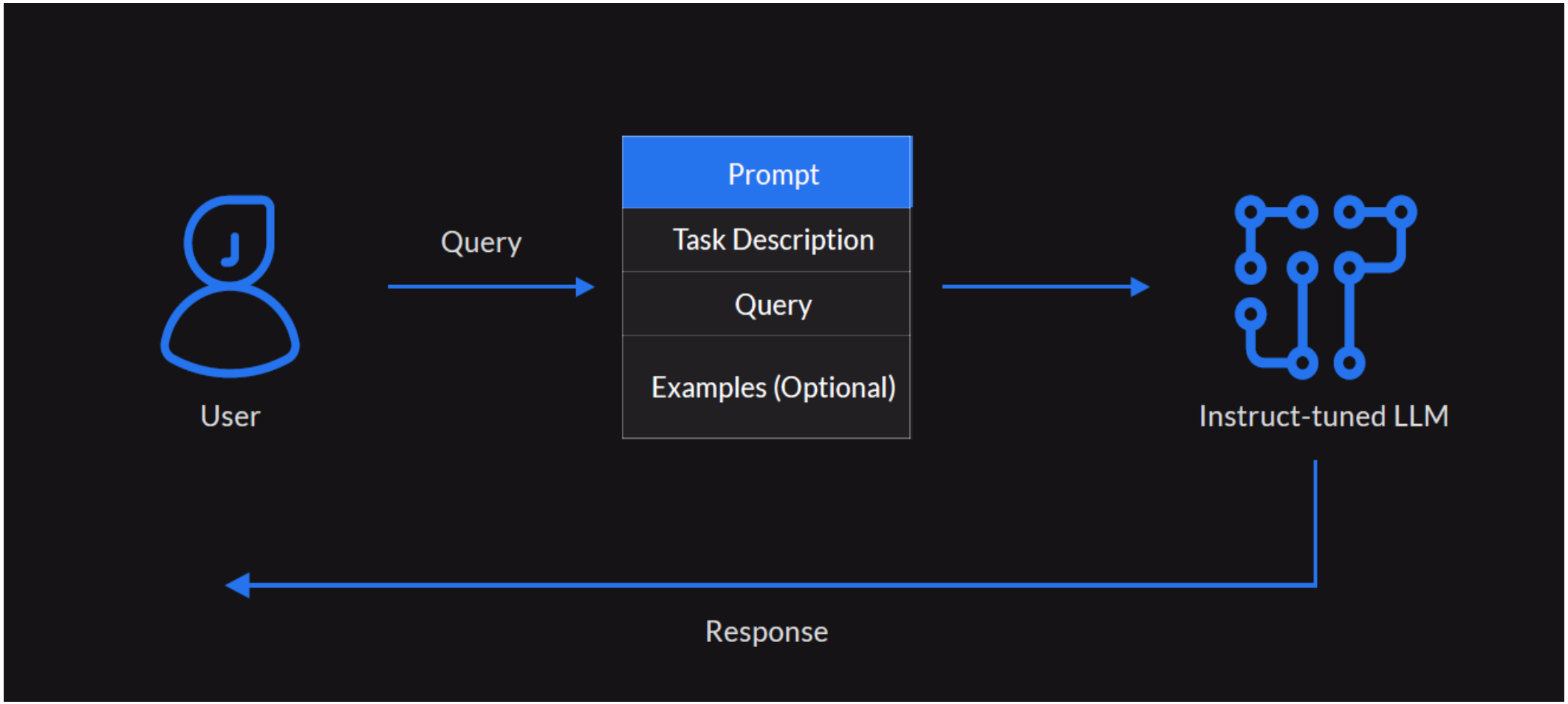
Analysis Phase: Path 1 AI Analysis

- **Analysis Path 1 — LLM Reasoning**
  - CVE descriptions + SBOM component list sent to LLM in a prompt as text
  - Natural language analysis: contextual, fast, human-readable
  - Identifies relevant CVEs with brief justification

CPAMS – Analysis Phase LLM



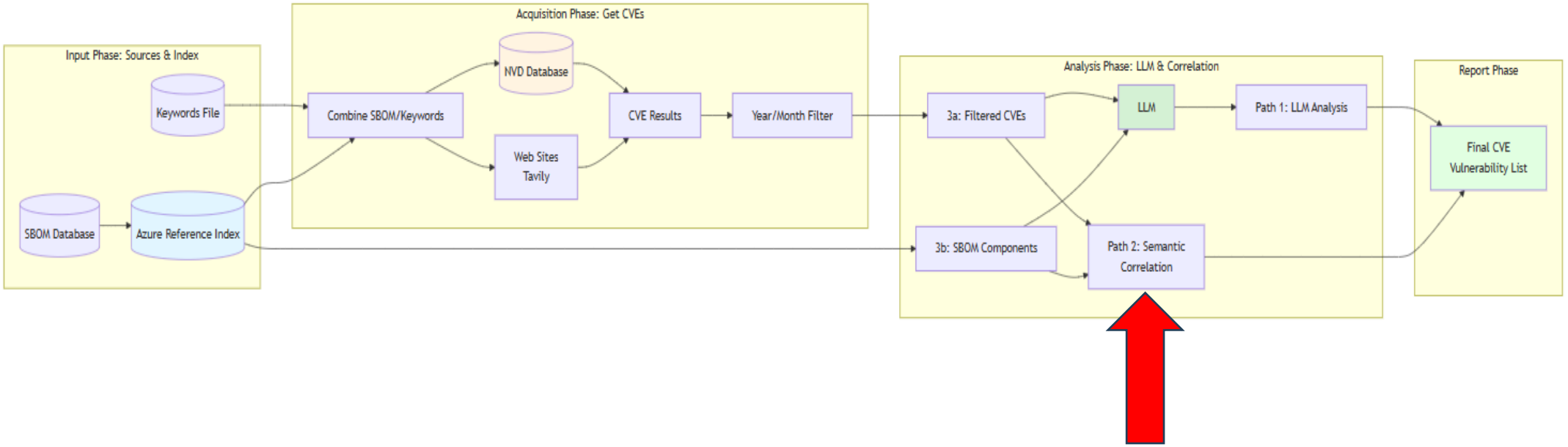
Analysis Path 1: LLM Reasoning



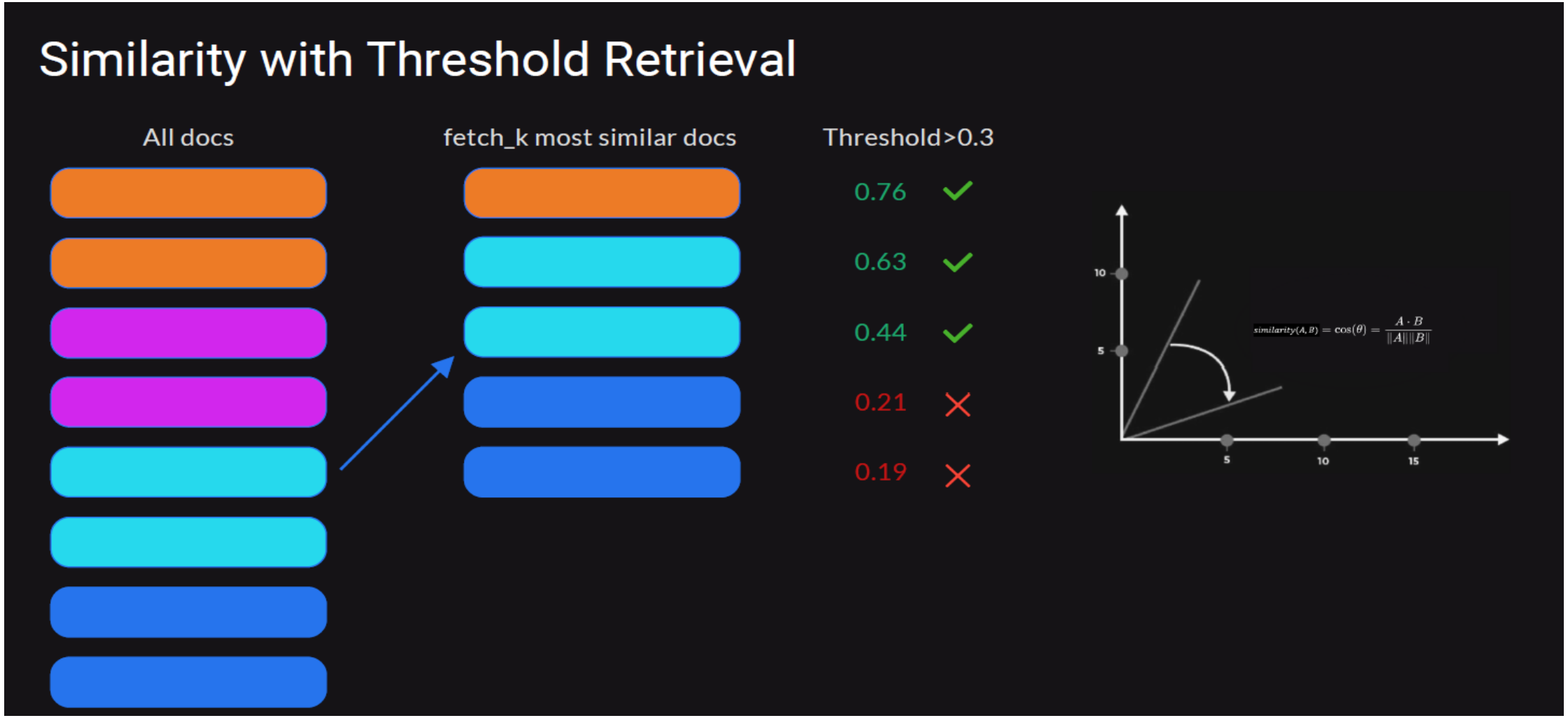
Analysis Phase: Path 2 Semantic Vector Analysis

- **Analysis Path 2 — Semantic Vector Correlation**
  - SBOM components and CVE descriptions as embeddings
  - Cosine similarity score for every SBOM × CVE component pair
  - Configurable threshold (default 0.3); outputs confidence levels

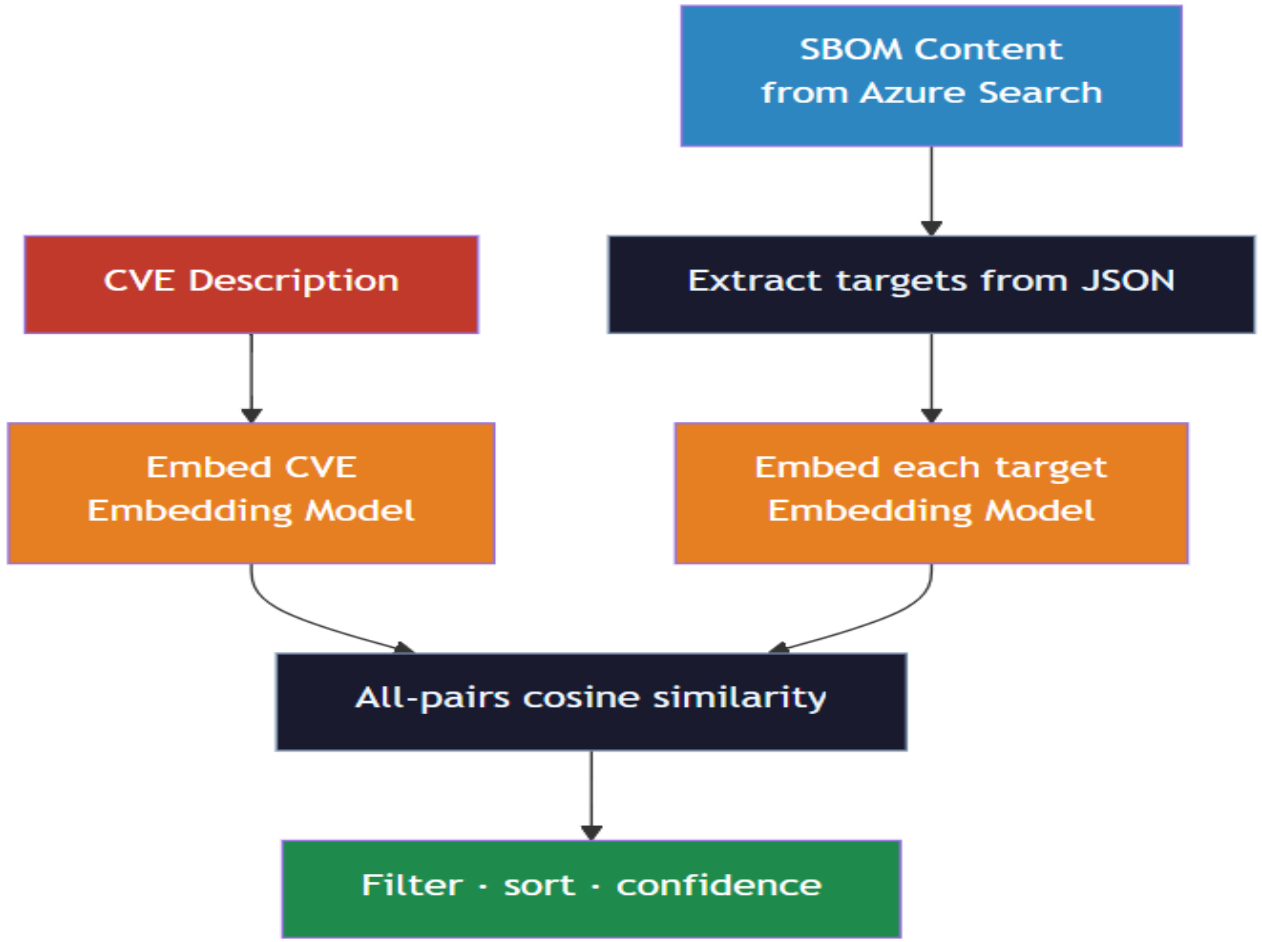
CPAMS – Analysis Phase Semantic Correlation



Semantic Vector Correlation



Analysis Path 2: Semantic Vector Correlation



The CPAMS LLM and Semantic Analyses

🤖 Analysis 1 (Path 1): LLM Analysis with SBOM Components

Method: Traditional LLM reasoning approach **Process**:

1. **Input**: CVE descriptions + SBOM component list (targetname, targetgroup, targetversion)
2. **Analysis**: LLM uses built-in knowledge to match CVE descriptions to software components
3. **Output**: Numbered list of relevant CVEs with brief descriptions and hyperlinks

Strengths:

- ✅ **Fast execution** - single LLM call
- ✅ **Contextual reasoning** - understands complex relationships
- ✅ **Domain knowledge** - leverages LLM's cybersecurity training
- ✅ **Human-readable explanations** - natural language analysis

Limitations:

- ❌ **Subjective** - depends on LLM's interpretation
- ❌ **No quantitative scoring** - binary relevant/not relevant
- ❌ **Limited by training data** - may miss newer vulnerabilities

🧠 Analysis 2 (Path 2): Semantic Correlation Analysis

Method: Vector embedding similarity approach **Process**:

1. **Input**: CVE descriptions + SBOM components
2. **Embedding Conversion**: Converts both to vector representations
3. **Similarity Calculation**: Mathematical cosine similarity between vectors
4. **Threshold Filtering**: Only shows matches above configured similarity threshold
5. **Output**: CVEs with similarity scores, ranked by relevance

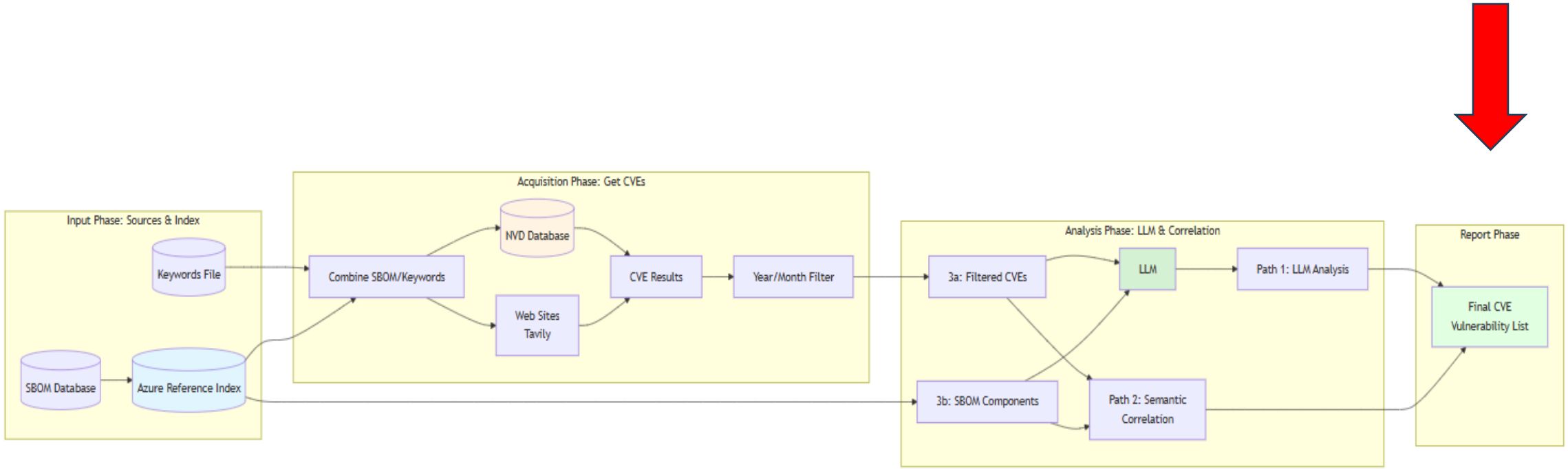
Strengths:

- ✅ **Quantitative scoring** - precise similarity percentages
- ✅ **Objective measurements** - mathematical rather than subjective
- ✅ **Semantic understanding** - finds conceptually related items with different wording
- ✅ **Configurable threshold** - adjustable precision/recall balance
- ✅ **Confidence levels** - high/medium/low confidence indicators

Limitations:

- ❌ **Requires embeddings** - needs vector database setup
- ❌ **Slower execution** - multiple embedding calculations
- ❌ **Threshold dependent** - results vary with similarity threshold

CPAMS – Report Phase



Key Capabilities & Results

- **Automated monitoring reduces manual triage from hours/days to minutes**
- **SBOM-driven and keyword search filters irrelevant CVEs**
- **Dual-path analysis provides independent corroboration**
  - LLM path: fast contextual reasoning
  - Semantic path: objective similarity scores (0.0 – 1.0)
- **Export package: Markdown report + relevant CVE CSV + JSON**
- **Configurable for any medical device product line**
  - Swap SBOM, keywords, and domains per product

Original Case Study

CyberMonitor_Rigdon.pdf

Note: final implementation in slides is different

CPAMS: A Cybersecurity Post-Market Analysis Monitoring System

Gerald Rigdon
Fellow, Software Engineering
Boston Scientific Corporation
St. Paul, USA
gerald.rigdon@bsci.com

***Abstract*—The Cybersecurity Post-Market Analysis Monitoring System (CPAMS) represents a composite approach to cybersecurity vulnerability monitoring and research, combining artificial intelligence and multi-source data integration to deliver threat intelligence. This paper presents a detailed analysis of the system's architecture, methodology, and capabilities, with particular emphasis on its application to medical device cybersecurity post-market surveillance. CPAMS integrates data from the National Vulnerability Database (NVD) and Tavily web-based search, generates an Azure index, and utilizes both Embedding Models and Large Language Models (LLMs) for vulnerability discovery and identification.**

***Index Terms*—Cybersecurity, Vulnerability Analysis, Medical Device Security, Post-Market Surveillance**

I. Introduction

In the prior research discussed in [1], a custom software application named CyberVulModelEval was designed to test the viability of LLMs for cybersecurity monitoring based primarily on Retrieval Augmented Generation (RAG) strategies. CyberVulModelEval was presented as a RAG-Blend Framework, leveraging concepts from ReAct [2], Reflection [3], Fusion [4], and Correction [5]. That research acknowledged the vast landscape of possible future research directions, either separate or derivative of CyberVulModelEval. In summary, that research recommended caution and careful deliberation when considering RAG pipelines as the primary mechanism for cybersecurity vulnerability discovery.

LLM semantic algorithms in data correlation? (2) Can LLMs improve the True Positive signal to noise ratio in correlating SBOM descriptive elements with CVE descriptive elements while diminishing False Positives that result from missing real signals.

In concert with CyberVulModelEval [1], the goal of CPAMS is to present further research on the use of AI, particularly LLMs, to help assess the effectiveness and practical use of these technologies within a cybersecurity post-market vulnerability monitoring framework.

II. Literature Review

Although the comprehensive review of over 300 papers encompassing 25 different LLMs presented in [9] was a valuable resource, the composite CPAMS approach emerged from the knowledge gained during the CyberVulModelEval study [1] where the literature review was more detailed.

III. Research Methodology Approach

The CPAMS process is captured in a series of steps as presented in Fig. 1 and further described in phases.

Input Phase: Per [Step 1] as depicted in Fig. 1, this phase involves the input of SBOM information (saved in JSON format) and additional keyword terms to be used during the CVE Acquisition Phase as follows:

INCOSE Healthcare Working Group

Thank you for attending!

Share your experiences at #HWGSEC