GRAPHMIND AI: MODEL CONTEXT PROTOCOL POWERED AGENTS FOR CYBER INTELLIGENCE

Leveraging ArangoDB, LangGraph & Model Context Protocol to Predict, Visualize, and Mitigate Security Threats for Next-Gen Vulnerability Defense using Common Vulnerabilities and Exposures (CVE) Dataset

ArangoDB Hackathon - (Team GraphMind AI)

Bhanu Reddy Manikanta Revuri Raghu Ram Vadlamani

WHY WE PARTICIPATED ?

Protect Critical Infrastructure

Cybersecurity threats can disrupt essential services and systems. By leveraging the CVE dataset, we aim to develop solutions that enhance the security and resilience of critical infrastructure.

Mitigate Emerging Risks

The CVE dataset provides insights into newly discovered vulnerabilities, enabling us to proactively identify and address emerging cybersecurity risks to stay ahead of potential attacks.

Collaborative Problem-Solving

By participating in this hackathon, we applied first principle techniques by delegating the effort to solve the issues at hand, using multi agent orchestration framework and ensuring resilience into the agentic flow.

Foster Innovation

The hackathon offers a chance to develop groundbreaking solutions blending ArangoDB's multimodal capabilities, Model Context Protocol, and LangGraph to bolster cybersecurity and vulnerability management.

Participating in this hackathon aligns with our team's commitment to enhance cybersecurity and protecting critical infrastructure. We are excited to leverage the CVE dataset and cutting-edge technologies to develop innovative solution that address emerging threats and contribute to a more secure digital landscape.

PROBLEM STATEMENT

Exponential Growth of Software Vulnerabilities

The CVE dataset shows a rapidly increasing number of known software vulnerabilities, making it challenging for organizations to stay on top of the escalating cybersecurity risks.

Complexity of Vulnerability Management

The CVE data includes detailed information on each vulnerability, such as descriptions, severity scores, and affected products, requiring organizations to process large amounts of data to assess and mitigate risks.

Lack of Real-time Vulnerability Monitoring

Traditional vulnerability management often relies on periodic scans and manually curating structured data, making it difficult for organizations to gather necessary and meaningful insights from the convoluted data.

Effectively identifying, tracking, and mitigating software vulnerabilities is a critical challenge for organizations, requiring advanced data processing and analysis capabilities to stay ahead of the evolving cybersecurity landscape.

WHY CVE DATASET?

Note: The original dataset pointed all vendors to a single product. We fixed this by using the corresponding CSV files to accurately map vendors to their products.

Vast Dataset

The CVE dataset contains over 145k nodes and 316k edges, making it challenging to explore and extract meaningful insights.

Enables Vulnerability Assessment and Mitigation

By analyzing the CVE data, organizations can identify and prioritize vulnerabilities within their systems, allowing them to proactively address security risks and enhance their overall defense posture.

Supports Threat Intelligence and Risk Management

The detailed information on CVEs, including severity scores, affected products, and references, enables security teams to better understand the threat landscape and make informed decisions about resource allocation and mitigation strategies.

Facilitates Collaboration and Knowledge Sharing

The open-source nature of the CVE dataset promotes collaboration among the cybersecurity community, allowing researchers, developers, and security professionals to share insights and best practices for addressing common vulnerabilities.

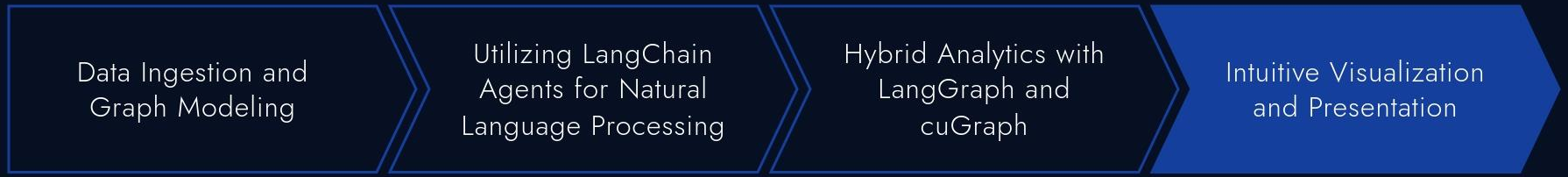
Aligns with Industry Standards and Frameworks - National Vulnerability Database (NVD)

The CVE dataset is widely recognized and integrated into various industry standards, frameworks, and tools, making it a reliable and widely-adopted resource for security management and compliance initiatives.

Comprehensive Database of Known Vulnerabilities

The CVE dataset provides a comprehensive catalog of known security vulnerabilities across a wide range of software and hardware products, making it a critical resource for cybersecurity professionals.

HARNESSING THE POWER OF NATIVE MULTI-MODEL CAPABILITIES OF ARANGODB, LANGGRAPH & MODEL CONTEXT PROTOCOL



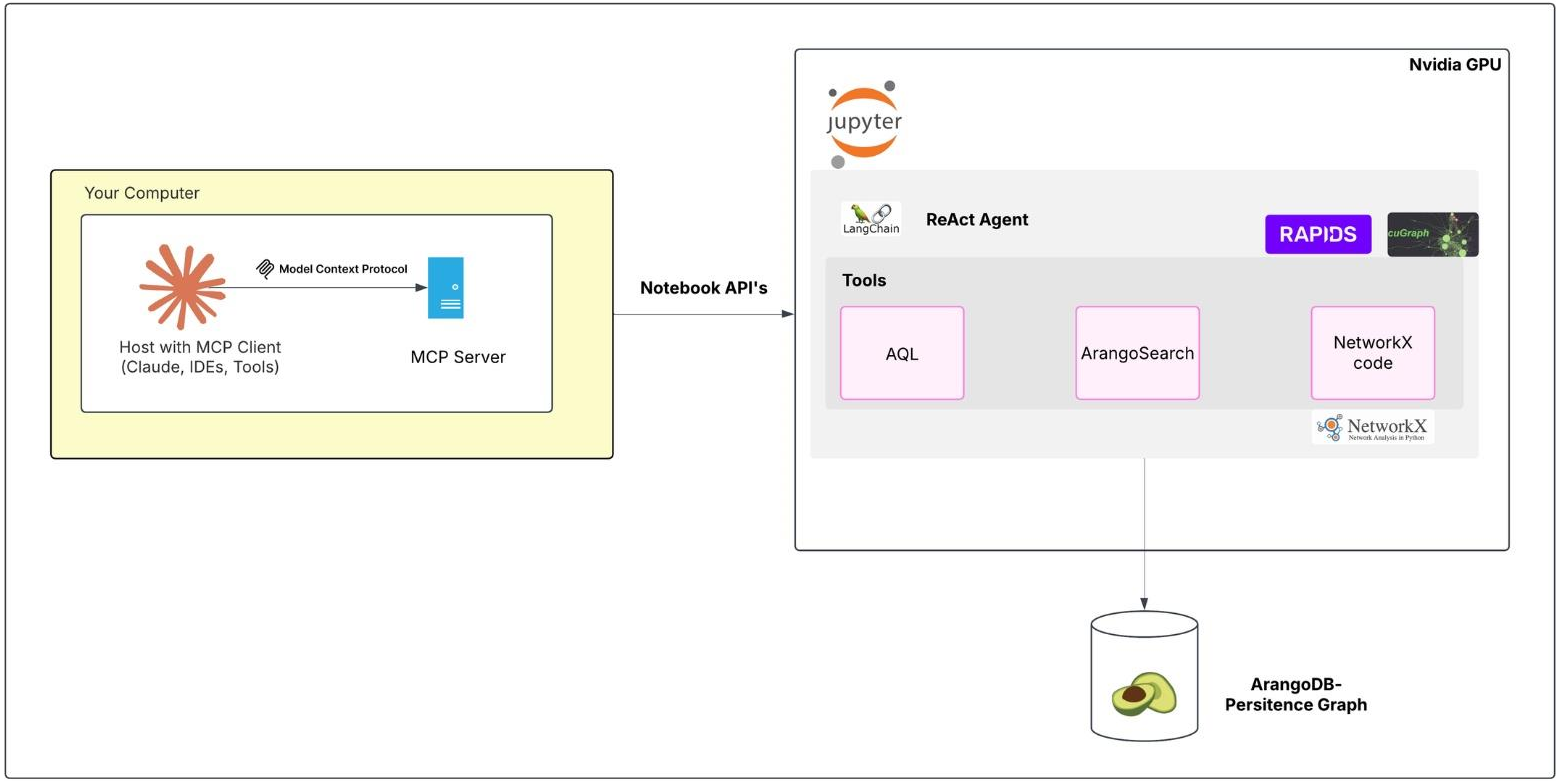
Ingested the Common Vulnerability Exposures (CVE) dataset and modeled it as a graph in ArangoDB, leveraging the ArangoDB NetworkX integration to persist and maintain the graph structure.

Utilized the LangChain agent tools to build a natural language interface that can understand user queries and dynamically generate AQL Queries, ArangoSearch and NetworkX for graph analytics.

Integrated LangGraph to enable stateful, multi-agent workflows that combine AQL queries with GPU-accelerated graph analytics using NVIDIA cuGraph for tasks like centrality analysis and community detection.

Leveraged MCP for creating an OOTB LLM powered interactive dashboard that presents the query results and analysis insights in a concise and visually appealing manner, allowing users to quickly understand and act on the vulnerability information.

HIGH-LEVEL ARCHITECTURE DIAGRAM



DEMO TIME

TEAM GRAPHMIND AI

THANK YOU

TEAM GRAPHMIND AI