MITREembed Project Plan

Objective**:**

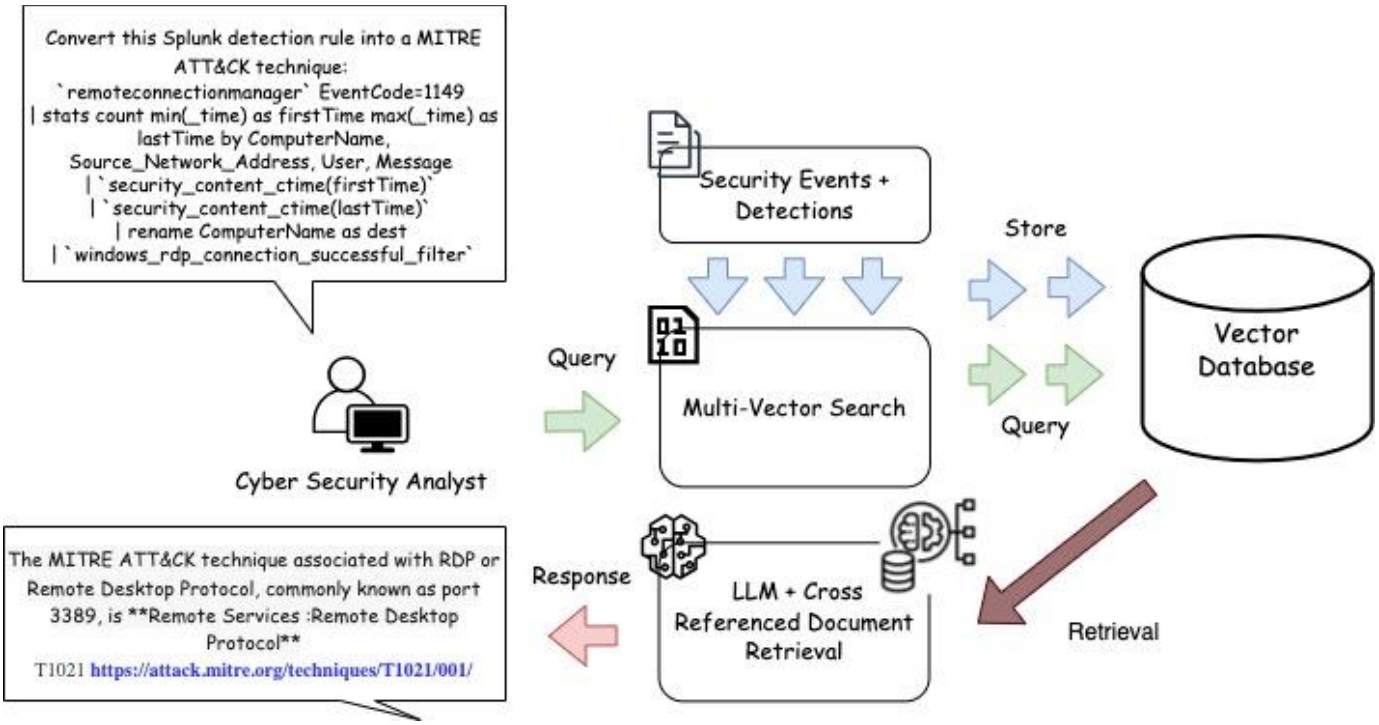
Develop an open-source platform that maps security log events and security event detection rules to MITRE ATT&CK techniques using multimodal testing and machine learning.

Target Users

Cybersecurity professionals, researchers, and organizations seeking to enhance their security monitoring capabilities through advanced data analytics and mapping techniques.

Background

MITRE ATT&CK is a comprehensive matrix of tactics and techniques employed by adversaries to compromise enterprise networks. Understanding these tactics through real-time data can significantly enhance an organization's defensive mechanisms. MITREembed aims to automate the identification of these tactics from various security logs, leveraging vector databases and large language models to provide actionable insights and facilitate a more proactive security posture.



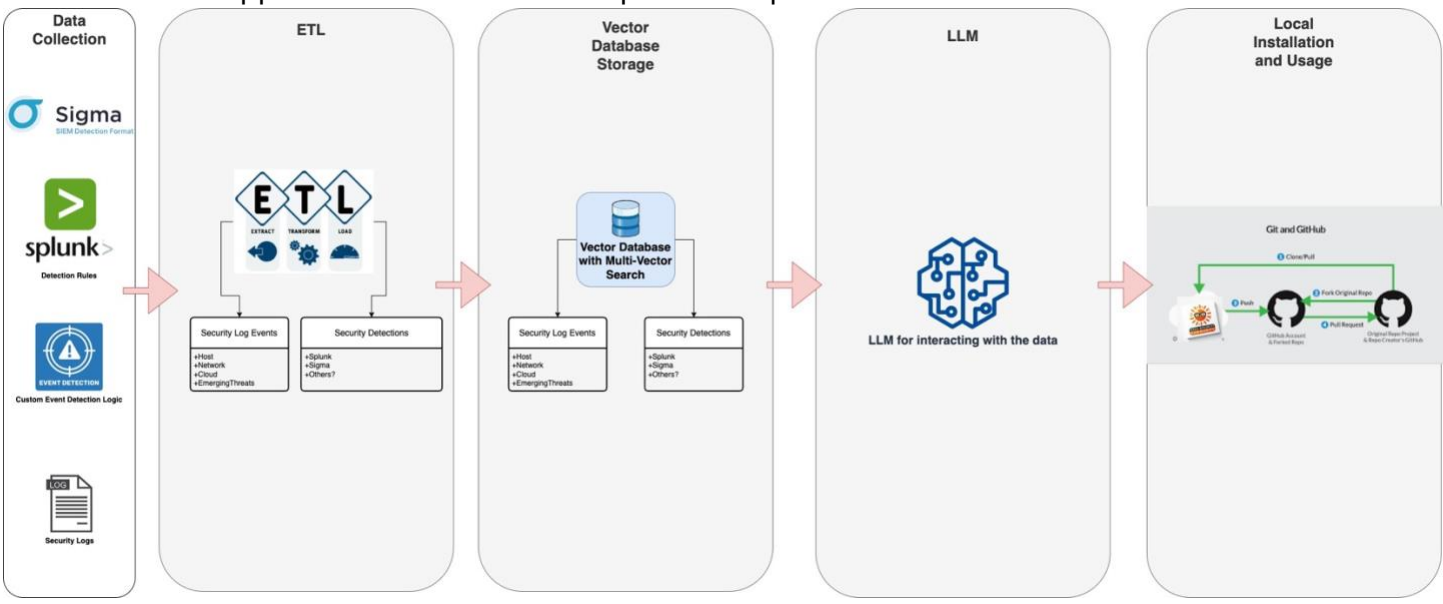
OPEN SECURITY AND DATA COMMUNITY

Project Scope

1. Data Collection and Conversion to CSV
    a. Collect complete Sigma detections and incomplete Splunk detections.
    b. Convert diverse event logs (network, host, antivirus, cloud, etc.) into CSV format for processing.
        i. Github Awesome ML For CyberSecurity
2. Multimodal Testing on Vector Databases
    a. Utilize Milvus, a vector database, for storing domain-specific data. This will allow efficient querying and mapping back to MITRE Attack Techniques.
    b. Milvus Quickstart Guide
    c. Use Multi-Vector Search

3. Large Language Model (LLM) Integration
    a. Integrate a LLM to interpret and interface with the structured data, facilitating an intuitive query mechanism for users to map log events to MITRE techniques dynamically.
4. Local Installation and Usage

    a. Ensure the tool is easy to install and run locally for users.
    b. Provide functionality for users to upload their security logs and receive mapped MITRE ATT&CK techniques as output.



Key Deliverables

1. Software Requirements Specification (SRS)
    a. Detailed documentation outlining the functional and non-functional requirements of the project.
2. Architecture Design
    a. Diagrams and descriptions detailing the software architecture, including data flow and module interactions.
3. Implementation Plan
    a. A timeline of development phases, including initial setup, core functionality development, LLM integration, and final testing.
4. Testing Strategy
    a. Description of testing methodologies to be used, including unit testing, integration testing, and system testing.
5. Documentation and Training Materials
    a. Comprehensive user guides, API documentation, and training materials for community engagement and user support.
6. Community Engagement Plan
    a. Strategies for building and maintaining an active user and contributor community, including regular updates, open forums for discussion, and transparent development processes.

Milestones and Timeline

1. Q1 2024
    a. Project kickoff, team setup, initial requirements gathering.
    b. Start of data collection module development.
2. Q2 2024
    a. Completion of data collection and CSV conversion modules.
    b. Begin development of vector database integration.
    c. Submit Abstract to DefCon 2024
3. Q3 2024
    a. Integration of LLM and testing of interaction interfaces.
    b. Start of local installation module development.
    c. Official release at Defcon 2024 and community launch event.
4. Q4 2024
    a. Final integration and testing phase.
    b. Preparation of documentation and training materials.

Budget

- Development Costs
  - Estimated based on team size, required software licenses, and infrastructure costs.
- Marketing and Community Engagement
  - Budget for promotional activities, community events, and engagement initiatives.
- Ongoing Support and Maintenance
  - Annual budget allocation for updates, patches, and community support.

Risk Management

- Technology Risks
  - Address potential issues with integrating new technologies like vector databases and LLMs.
- Data Privacy and Security
  - Implement robust security measures to protect sensitive data during collection and processing.
- Community Adoption
  - Develop strategies to ensure active community participation and feedback.

MITREembed is poised to bridge the gap between theoretical cyber defense frameworks and practical, actionable intelligence. By automating the mapping of log events to MITRE ATT&CK techniques, the project will empower cybersecurity professionals to preemptively counteract adversary tactics and enhance their security posture significantly.