From Knowledge to Evaluation: Modelling Cybersecurity Knowledge Graphs for Automatic Benchmark Generation

Project Description: Cybersecurity knowledge is distributed across structured and semi-structured sources such as:

- MITRE ATT&CK
- MITRE CWE
- NIST vulnerability records
- Wikipedia cybersecurity articles

This project has two tightly coupled components:

(1) Knowledge graph modelling

- Extract entities and relationships from structured (e.g., MITRE, NVD) and unstructured sources (e.g., Wikipedia articles, benchmarks)
- Design a unified cybersecurity ontology
- Construct a scalable cybersecurity knowledge graph
- Evaluate graph completeness and consistency

(2) Automatic benchmark generation

- Convert graph paths (e.g., attack chain → vulnerability → mitigation) into natural-language evaluation prompts
- Automatically derive ground-truth labels
- Generate multilingual prompts
- Evaluate generated benchmarks against existing curated datasets

The goal is a fully automated pipeline that transforms evolving threat intelligence into continuously updated evaluation benchmarks.

Deliverable: a prototype system and a full conference paper draft.

Project Type: Research + Engineering

Internship Batch: Batch 1 or Batch 2

Duties/Activities:

- Data extraction from public cybersecurity sources

- Knowledge graph design and implementation
- Prompt generation from graph traversal
- Automatic labeling and validation
- Comparative benchmark evaluation
- Conference paper drafting

Required Skills:

- Python
- Basic graph modelling (e.g., Cypher for Neo4j)
- NLP fundamentals
- Interest in cybersecurity

Preferred Intern Academic Level: Senior undergraduate or MSc

Learning Opportunities:

- Knowledge graph construction
- Automated dataset generation
- Security-oriented NLP
- Research publication process

Expected Team Size: 3 students

Mentors:

- Dr. Yazan Boshmaf (yboshmaf@hbku.edu.qa)
- Dr. Mohannad Alhanahnah (malhanahnah@hbku.edu.qa)