A Web Application for Automated STIX Reports Generation from Cyber Threat Intelligence

Project Description: The goal of this project is to build a web application for automated STIX reports generation from cyber threat intelligence using large language models. During this internship, the intern will interact with multiple components such as graph databases, malware analysis reports, and large language models. In addition, he/she will work on production-level application with established CI/CD pipelines to make software engineering skills into practice.

Project Type: Engineering

Internship Batch:
- **Batch 1:** May 12 to July 12, suitable for Education City students, i.e., CMUQ, TAMUQ and HBKU students
- **Batch 2:** May 26 to July 25, suitable for QU university students

Duties/Activities:

- Designing a web UI for a command line tool that extracts STIX reports from cyber threat intelligence.
- Building the web UI using one of the frontend frameworks (React, Vue, Flutter, etc.).
- Building a query engine using Neo4j graph database.
- Building a backend a simple API that interacts with our core tool.

Required Skills:

- Familiarity with one of the frontend frameworks (React, Vue, Flutter, etc.).
- Familiarity with how web applications work.
- Some knowledge on systems' design.
- Familiarity with web sockets, concurrency, and blocking/non-blocking behaviors.
- Experience with Neo4j and Flask is a plus.

Preferred Intern Academic Level: Senior

Learning Opportunities:

- Implementing a system design for a production-level web application that has multiple heavy load tasks.
- Learning how to interact with Continuous Integration and Continuous Deployment (CI/CD) pipeline.
- Learning git for production.

Expected Team Size: *3*

Mentors

Name: Dr. Ahmed Lekssays   email: alekssays@hbku.edu.qa

Name: Dr. Husrev Taha Sencar   email: hsencar@hbku.edu.qa