Project Title: *Cross-Matching Threat Knowledge among Incident Response Reports*

Project Description: This summer project aims at improving language understanding capabilities from cybersecurity text in view of recent advances in NLP and machine learning. As a first step towards this goal, we investigate the problem of automatic annotation of incident response reports to identify trends and patterns in the way APT attacks are carried out. This task is currently performed manually by analysts. Our approach aims at mapping the findings of a security report to the relevant *tactics* and *techniques* used by cyber attackers. The intern will help us in cross-matching the findings of different reports describing the same phenomena. We will deploy a semantic text-matching approach.

Project Type: Research

Internship Batch: Batch 1 from May 7 to June 29

Duties/Activities: Students are expected to learn basic text-retrieval techniques and get involved in daily discussions. They will also run experiments in alignment with the goals of the project.

Required Skills: Basic knowledge in systems and algorithms. Comfort in programming Python or other prominent programming languages.

Preferred Intern Academic Level: Project is open to students at all levels. Preference will be given to students at the junior & senior levels.

Learning Opportunities: This project is an extension of ongoing research work. Student(s) will work as part of the team.

Expected Team Size: *This project is an extension of ongoing research work. Student(s) will work as part of the team.*

Mentors

Husrev Taha Sencar (hsencar@hbku.edu.qa)