الكلية العالمية للهندسة والتكنولوجيا
GLOBAL COLLEGE OF ENGINEERING AND TECHNOLOGY

Part Time Research Assistant in Cybersecurity & AI – Zero Trust

Specification	Essential	Desirable
Knowledge and Qualifications	1. B.Ss or Msc in Cybersecurity, Computer Science, Information Security, Artificial Intelligence Data Science, Or in relevant field from a reputable university. 2. Strong foundational knowledge of: Network security principles, Intrusion Detection Systems (IDS), Zero Trust Architecture (ZTA), Machine learning fundamentals	
Experience	Experience in as many of the following areas as possible: ● Data collection and preprocessing for cybersecurity datasets ● Machine learning model development (supervised, unsupervised, semi-supervised) ● Working with cybersecurity datasets (e.g., CICIDS, UNSW-NB15, NSL-KDD) ● Feature engineering and anomaly detection ● Python programming (scikit-learn, TensorFlow, PyTorch) ● Data visualization and reporting ● Technical report writing ● Basic knowledge of Explainable AI (SHAP, LIME) ● Familiarity with SOC environments or enterprise network monitoring (desirable)	
Interpersonal Skills	● Strong analytical and problem-solving skills ● Ability to work independently and within a research team ● Flexible and able to meet research deadlines ● Strong written and verbal communication skills ● Enthusiastic about cybersecurity research and innovation	
Research	● Experience conducting applied or experimental research in: ● Cybersecurity ● AI-based threat detection ● Behavioral anomaly detection ● Familiarity with research methodology and academic writing	

الكلية العالمية للهندسة والتكنولوجيا
GLOBAL COLLEGE OF ENGINEERING AND TECHNOLOGY

JOB DESCRIPTION

Research Assistant-Part time

Grade: Research Assistant-Part time

Reporting to: PI/Co-PI block funding research

Post Holder: Research Assistant on block funded TRC project

Salary and Benefits: As per contract

Effective Start Date: 1st August 2026

Description

The Part-Time Research Assistant will support the implementation of a research project focused on developing a machine learning–based threat detection framework aligned with Zero Trust Architecture (ZTA) principles.

The role involves:

- Assisting in data preprocessing and feature engineering
- Developing and evaluating machine learning models for anomaly detection
- Supporting integration of Explainable AI (XAI) tools
- Conducting experimental validation and performance benchmarking

The Research Assistant will contribute to the development of a modular, scalable, and interpretable AI-driven cybersecurity system designed for enterprise environments.

Duties and Responsibilities

1. Assist in designing and implementing a modular, Zero Trust–aligned AI threat detection framework using Python and machine learning libraries.
2. Prepare and preprocess publicly available cybersecurity datasets, including data cleaning, normalization, and transformation into structured model inputs.
3. Perform behavioural and contextual feature engineering (e.g., session duration, access frequency, protocol usage) and apply feature selection or dimensionality reduction techniques.
4. Develop, train, and optimize unsupervised and semi-supervised models (e.g., Isolation Forest, One-Class SVM, Autoencoders) for anomaly detection.

5. Integrate Explainable AI techniques (SHAP, LIME) to enhance model interpretability and support reduction of false positives.
6. Evaluate system performance using metrics such as accuracy, F1-score, AUC, and false positive rate, and assist in benchmarking experiments.
7. Maintain proper documentation of experiments, datasets, and results, and assist in preparing technical reports and research publications.

Apply Now