Postdoctoral Researcher Position in Cybersecurity and Machine Learning

Location: Tecnológico de Monterrey University - Guadalajara, Mexico.
Duration: Six months with possibility to renew every six months up to two years.
Start Date: As soon as possible

We are seeking a highly motivated Postdoctoral Researcher to join a project focused on the development of advanced IA models(machine learning, deep learning and generative IA) for cybersecurity threats detection such as malware, network intrusion detection, disinformation detection, etc. The project aims to design, implement, and validate intelligent cybersecurity solutions capable of operating in realistic environments, with the goal of achieving a working prototype.

Key Responsibilities

- Design and develop machine learning and deep learning models for detecting cybersecurity threats such as network attacks, ransomware, botnets, etc.
- Work with structured and unstructured network data (e.g., NetFlow, pcaps packet captures, logs).
- Implement data preprocessing pipelines, feature engineering, and model evaluation frameworks
- Build and validate a functional prototype in an operational environment.
- Collaborate with multidisciplinary teams, including cybersecurity and machine learning experts
- Publish research findings in several papers of high-impact journals and conferences

Required Qualifications and Skills

- PhD in Computer Science, Cybersecurity, Data Science, or a closely related field
- Strong background in machine learning (including deep learning), particularly supervised and unsupervised methods
- Proven experience with Python and ML frameworks (e.g., scikit-learn, TensorFlow, PyTorch)
- Ideally, the candidate should have experience working in cybersecurity fields, developing AI models for attack identification and mitigation in simulated networks and real environments.
- Familiarity with network security, monitoring, Datasets and security tools (e.g., Zeek, Caldera, Suricata, Snort, Wireshark) and their integration into ML pipelines.
- Solid understanding of cybersecurity concepts (e.g., intrusion detection systems, threat models, attack vectors)
- Ability to develop functional prototypes and deploy ML models in realistic environments
- Strong scientific writing and publication record
- Strong written and reading English skills

Preferred (Optional) Skills

- Experience with real-time or streaming data processing (e.g., Apache Kafka, Spark)
- Knowledge of cloud platforms (AWS, Azure, GCP) and containerization (Docker, Kubernetes)
- Experience deploying systems in virtualized or emulated environments (e.g., virtual labs, cyber ranges, or network simulators such as Mininet)
- Experience with SIEM systems or integration with operational cybersecurity tools
- Experience with LLMs and Agents
- Knowledge of graph models and NLP.

Expected Outcomes

- Development of a validated AI-based cybersecurity Framework
- Deployment of a test environment where the Framework is tested reporting metrics and benchmarks of performance of the framework.
- Demonstrated performance on benchmark and real-world datasets
- Publications in leading cybersecurity and machine learning venues
- Documented code, technical and user manuals

What We Offer

- Opportunity to work on cutting-edge cybersecurity challenges
- Collaborative and interdisciplinary research environment
- Support for conference travel and publications

Application Process

Applicants should submit (in the same PDF):

- Cover letter describing relevant experience and research interests
- Curriculum Vitae (CV)
- List of publications
- Contact information of 2–3 references

Submit your application to enrique.gc (at) tec.mx