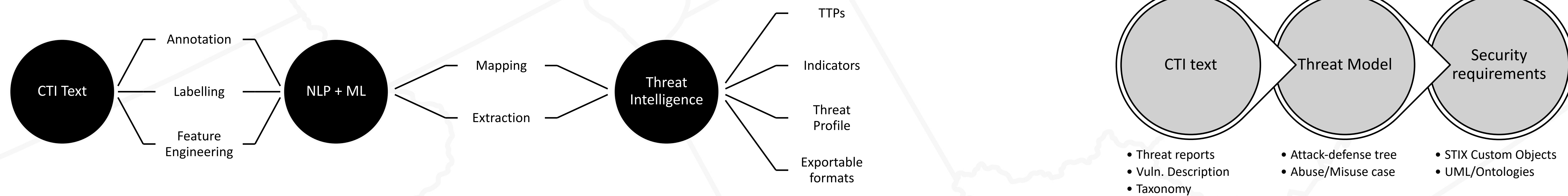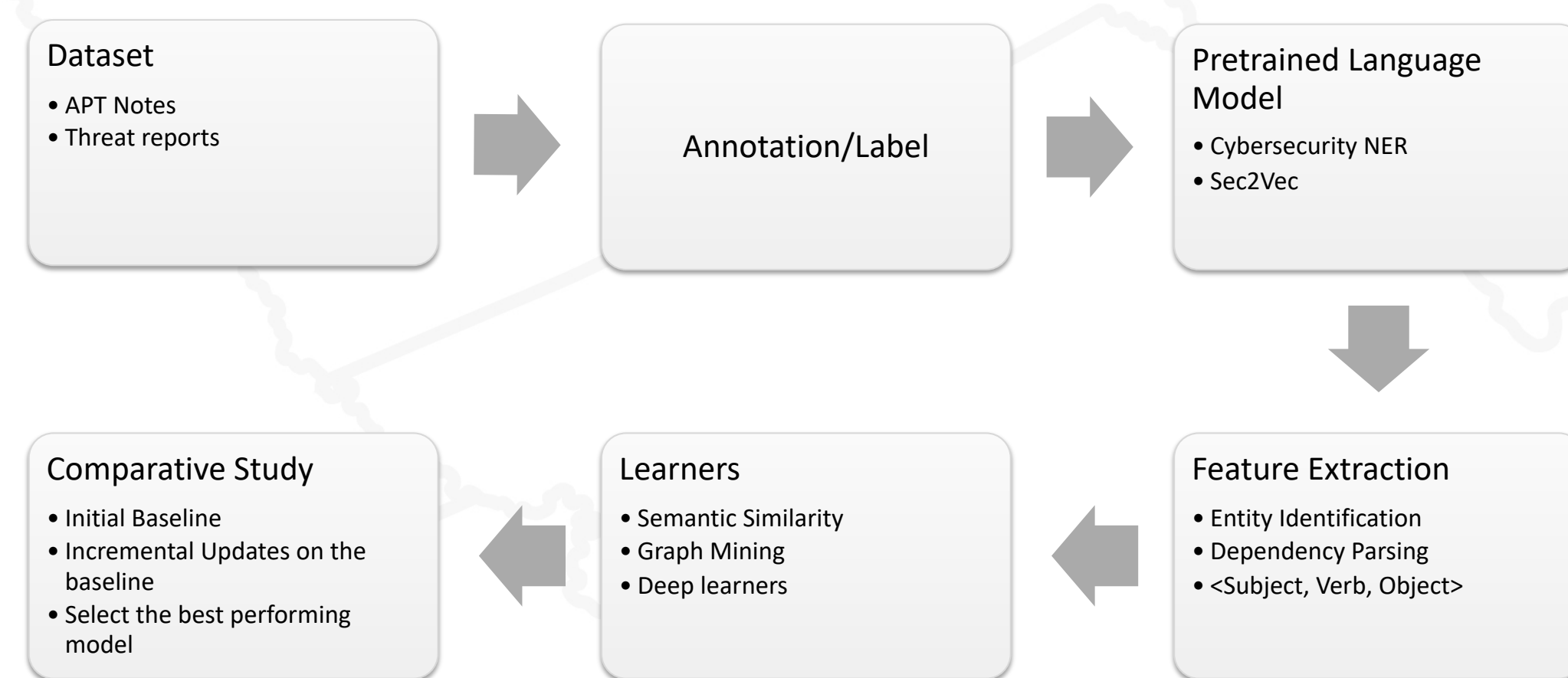# Generating Security Requirements from Threat Reports

Md Rayhanur Rahman, Laurie Williams

North Carolina State University, Raleigh, North Carolina, United States

Background and motivation

CTI Text — Annotation — Labelling — Feature Engineering → NLP + ML — Mapping — Extraction → Threat Intelligence → TTPs, Indicators, Threat Profile, Exportable formats

CTI text → Threat Model → Security requirements

- Threat reports
- Vuln. Description
- Taxonomy

- Attack-defense tree
- Abuse/Misuse case

- STIX Custom Objects
- UML/Ontologies

Workflow

Dataset
- APT Notes
- Threat reports
→ Annotation/Label → Pretrained Language Model
- Cybersecurity NER
- Sec2Vec
↓
Comparative Study
- Initial Baseline
- Incremental Updates on the baseline
- Select the best performing model
← Learners
- Semantic Similarity
- Graph Mining
- Deep learners
← Feature Extraction
- Entity Identification
- Dependency Parsing
- <Subject, Verb, Object>

• Application

– Detection and response

– Threat and mitigation profile

– Based on past evidence, strategic mitigation planning in he future

– Incorporation with SDLC

• Challenges

– Obtaining dataset and labelling

– Change in attack patterns

– No benchmarks

• Feedbacks?

– mail: mrahman@ncsu.edu

– Profile: rayhanur-rahman.github.io

– Our research group: realsearchgroup.github.io