GRID SIEM SDMAY29

Trent Bickford, Westin Chamberlain, Daniel Ocampo, Ella Cook

Work Done

- Figures and information for the paper were finished
- Addressed the feedback given to us in the peer review
- Started work on the poster - Final Poster.pptx

Security Onion

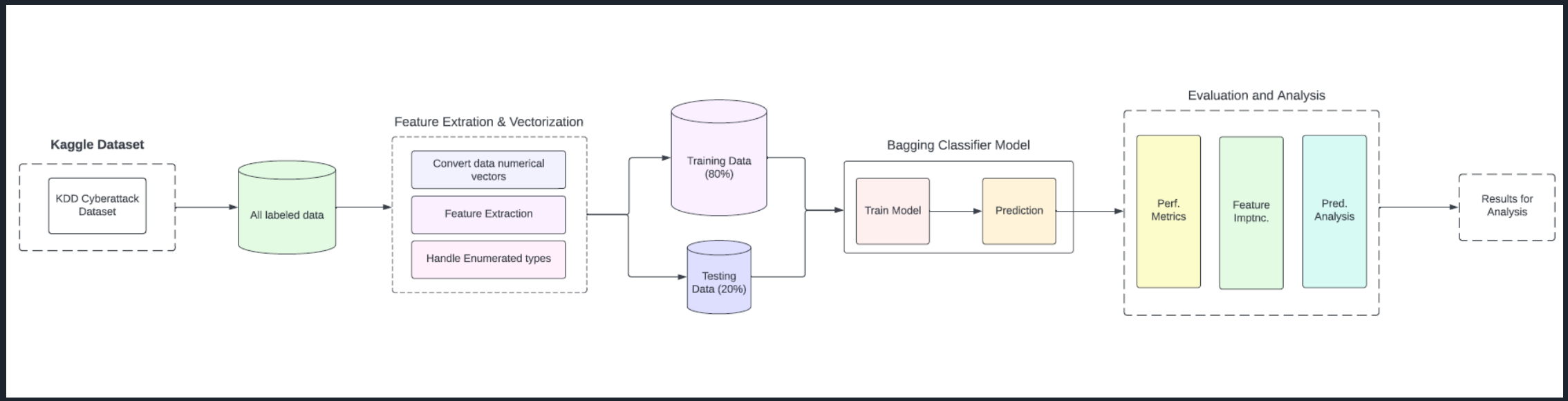
- Having difficulty picking up alerts
- Changed Zeek Home_Net to include public IPs of the zones
- Need to attempt to change sensors 2 and 3 and investigate why sensor 1 changed

Plan for Attack data on Poster

- Potentially doesn't have its own section
  - Might be best to support other sections with the data from attacking
  - Include how we would be able to interpret the data packets produced during an attack, either though Kibana or other means.
  - Describe attack mitigation/remediation procedure.
- Caldera Section
  - Explain how it was supposed to be used in our project
  - Outline why it was selected to test the security of our ICS systems.
  - Similar to section in IEEE paper

Machine Learning

- Changed the main model used for the KDD Cyberattack dataset was overfitting with Random Forest
  - Likely because the KDD dataset was purposefully chosen because it was smaller and easier to process but that means it is imbalanced with some of the least occurring features only having a count of 2
- Chose Bagging classifier because it is known to help reduce overfitting
  - Similar to RF because RF is also a specific type of bagging classifier
  - It generates multiple subsets of data from the training set, trains a model on each subset, then combines predictions for result



Work To Be Done

- Review the presentation with peer feedback
- Finish the final document
- Finish the poster – would it be okay to include the paper?
- Change some of the project diagrams
- Update team website with most recent work.
- Attend one of the presentation practice sessions on 4/18 or 4/25
  - Receive feedback from faculty and peers.