AIMailAnalyzer

AIMailAnalyzer is a cortex analyzer that inputs a .tar email archive from the Minio email-feeder.
Here is an exemple of the output:


```
{
  "summary": {
    "classification": "DANGEROUS",
    "malscore": "9.98",
    "confidence": "0.996555507183075"
  },
  "full": {
    "malscore": "9.98",
    "classification": "DANGEROUS",
    "confidence": "0.996555507183075",
    "classification_probabilities": "[5.932090e-04 2.851292e-03 9.965555e-01]",
    "sub_classification": "CLASSIC_PHISHING",
    "sub_classification_confidence": "0.9964059591293335",
    "sub_classification_probabilities": "[4.5969387e-05 5.4723962e-04 2.8482832e-
03 3.0089416e-06 9.9640596e-01\n 3.2628275e-05 1.2385264e-07 1.1671616e-04]",
    "report": {
      "mail_file_name": "noname.ext",
      "mail_file_path": "/job/input/attachment8450828744160402788",
      "classification_probabilities": "[5.932090e-04 2.851292e-03 9.965555e-01]",
      "analyzed_mail_content": "Bonjour, ...",
      "analyzed_mail_headers": "defaultdict(<class 'list'>, {'Received': ['from
THS...'], 'MIME-Version': ['1.0']})",
      "email_embedding": "[0.07140572369098663, 0.14632089944359303, ...,
-0.04556916654109955]"
    }
  },
  "success": true,
  "artifacts": [],
  "operations": []
}
```


Setup

- Use the `train_models.ipynb` notebook to train the models from a `.csv` dataset that you can build with the `mailbox_to_csv.ipynb` notebook.
- Place the output models in the `models` folder.
- Install the analyzer in your Cortex instance.

Models used

The Analyzer uses 5 ResNet models to classify the submitted emails according to the classes chosen by the Tha-CERT, you can of course modify the classes and retrain the models with your own classes. The models are used like so: