# Anomaly Detection in ICSs using SNN
# **MARATHON DAY**

Student: Michael Kaminer

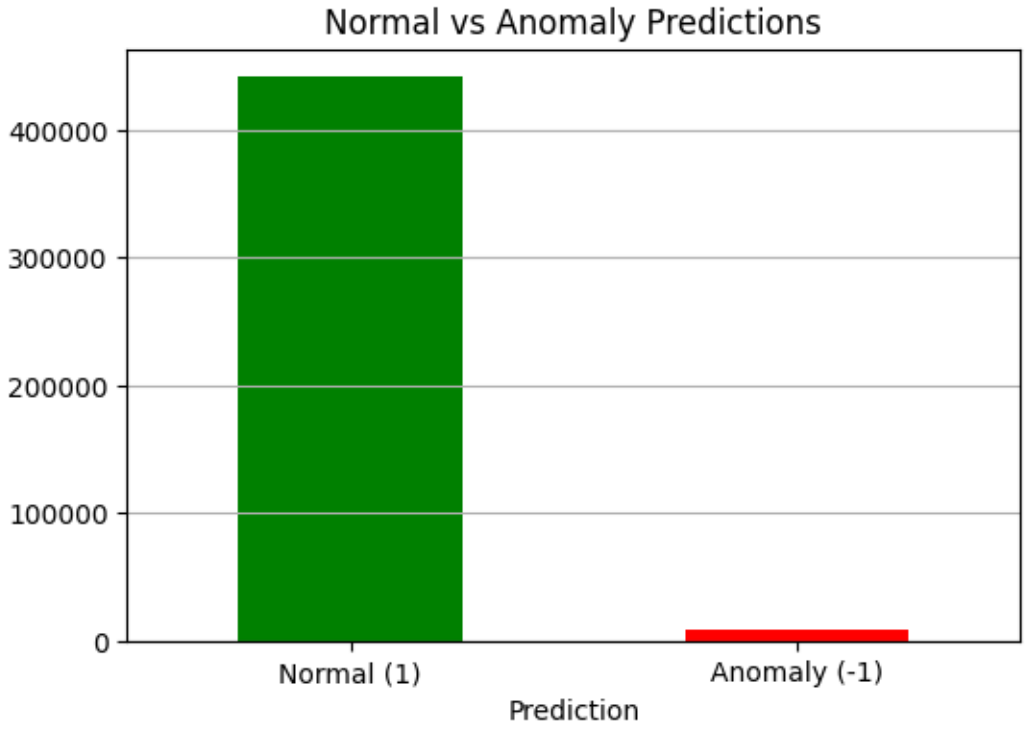
22.04.2025

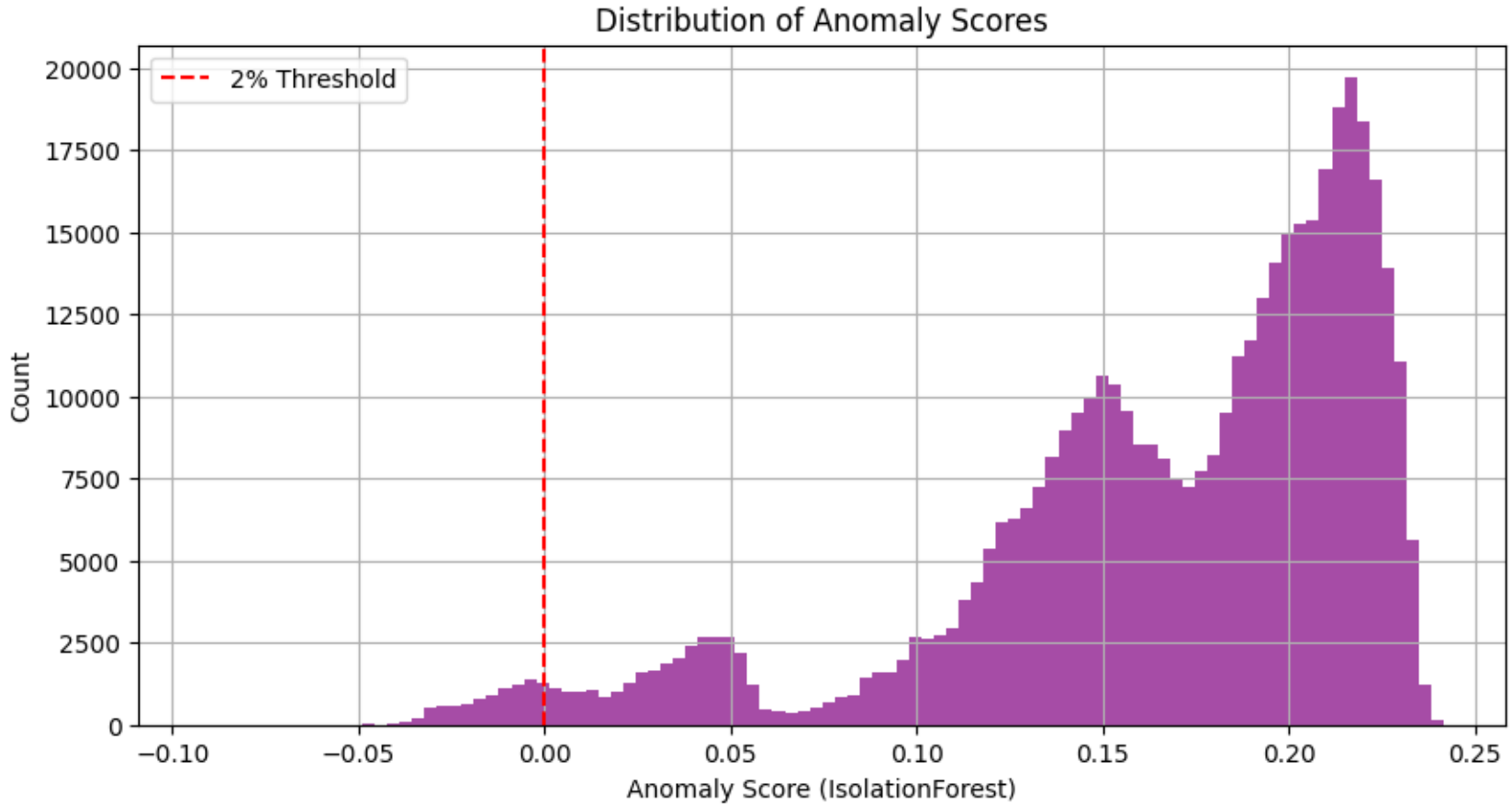
# Plans for today were:

- Explore and test multiple anomaly detection algorithms (in addition to SNN)
- Apply these algorithms on different preprocessed datasets
- Compare the performance of traditional anomaly detectors to SNN on the same datasets

# Achieved Goals:

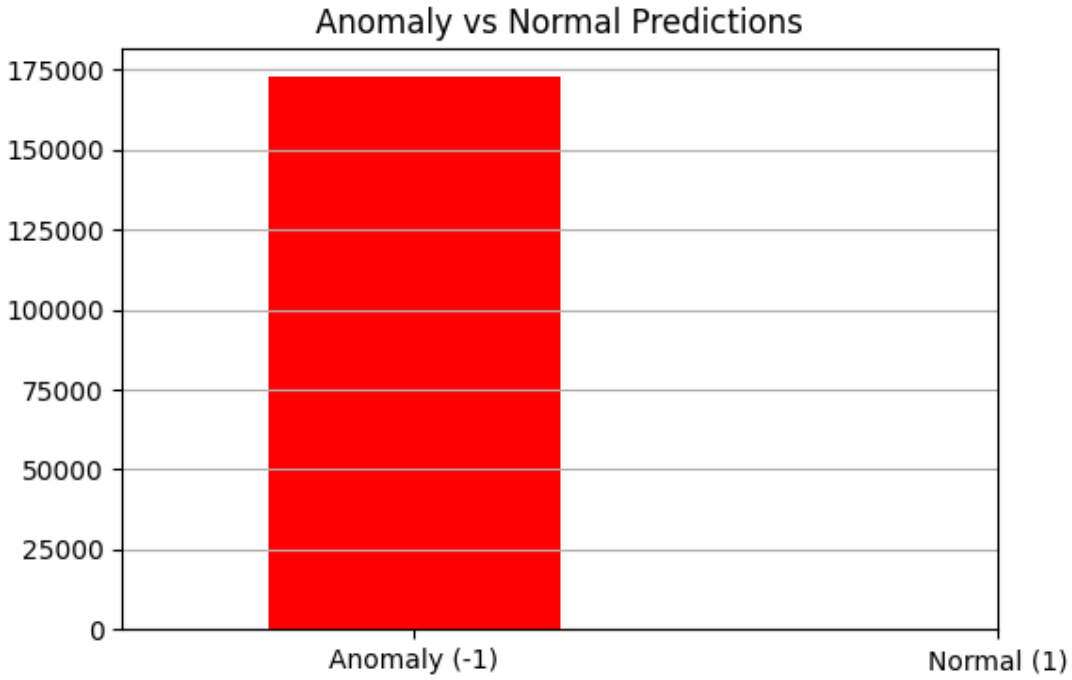
- Trained an **Isolation Forest** model on the **SWaT** dataset
- Trained a **One-Class SVM** model on the **WADI** dataset
- Observed **overfitting** in the One-Class SVM model




Distribution of Anomaly Scores
2% Threshold
Count
20000
17500
15000
12500
10000
7500
5000
2500
0
−0.10
−0.05
0.00
0.05
0.10
0.15
0.20
0.25
Anomaly Score (IsolationForest)

# Reasons for overfitting:

- Very high dimensionality of the WADI dataset
- Presence of redundant or non-informative features
- Imbalanced dataset with very few anomalies in the training data
- Sensitivity of One-Class SVM to hyperparameters like nu and gamma



# Next Steps:

- Test the **Tennessee** dataset as well
- All three datasets (SWaT, WADI, Tennessee) will be evaluated using multiple anomaly detection methods
- This will allow a thorough comparison with the **Self-Normalizing Neural Network (SNN)** later on
- Today, we built two essential frameworks — the base structures for **Isolation Forest** and **One-Class SVM**
  These will significantly speed up future experimentation
- Final evaluation will include running the datasets through the **SNN architecture**

- **Estimated project progress so far:** ~35–40%

Thank you!