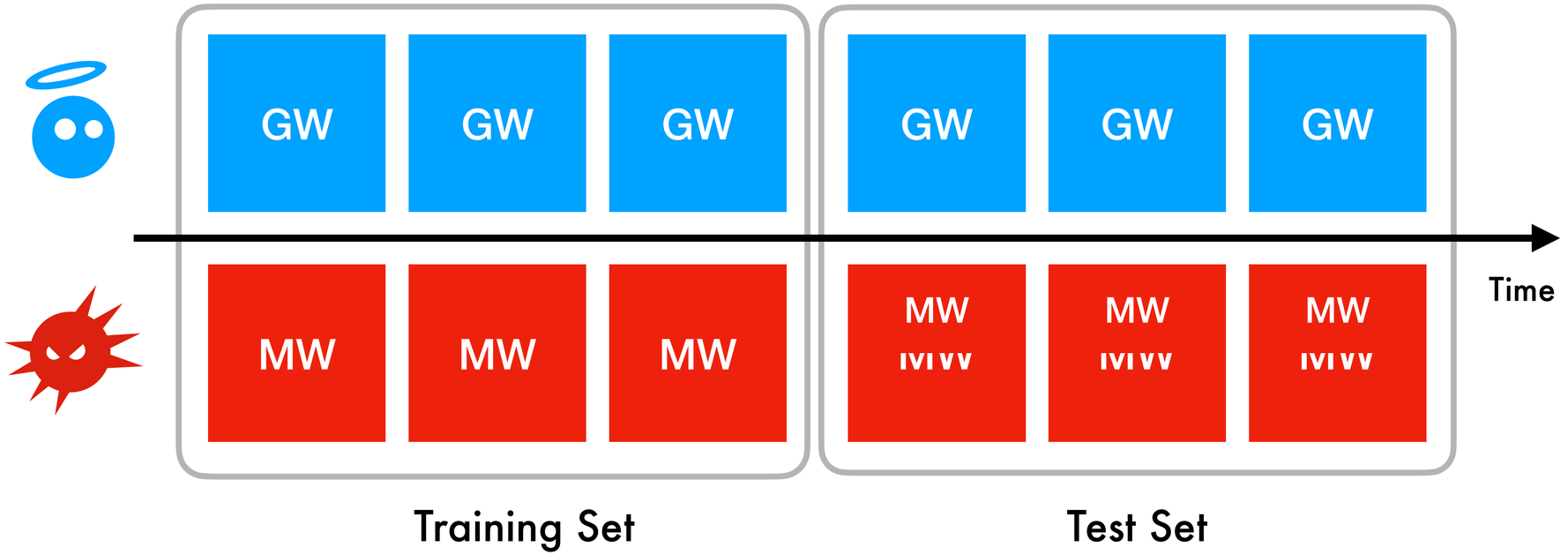
TESSERACT

TESSERACT Framework

Experimental Constraints

- **C1** Temporal training consistency
- **C2** {good|mal}ware temporal consistency
- **C3** Realistic testing classes ratio



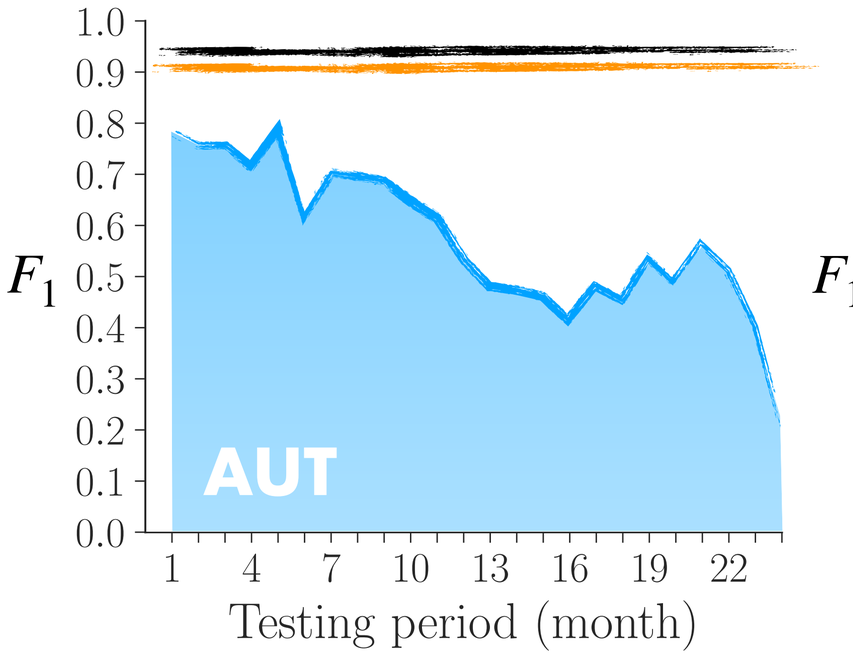
TESSERACT: Eliminating Experimental Bias in Malware Classification Across Space and Time.
Pendlebury F., Pierazzi F.,* Jordaney R., Kinder J., Cavallaro L.*
USENIX Security, 2019.

TESSERACT Framework

Experimental Constraints

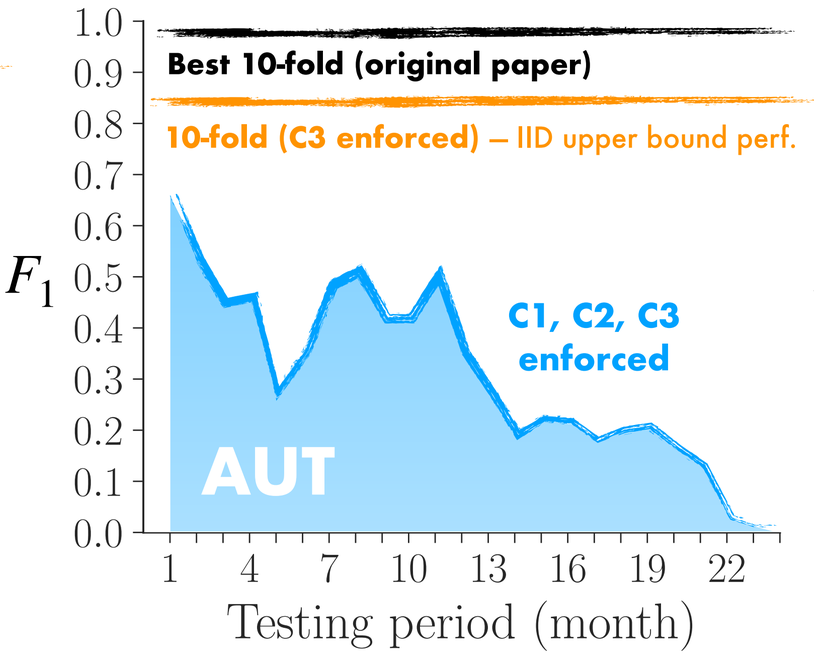
- **C1** Temporal training consistency
- **C2** {good|mal}ware temporal consistency
- **C3** Realistic testing classes ratio

Method 2



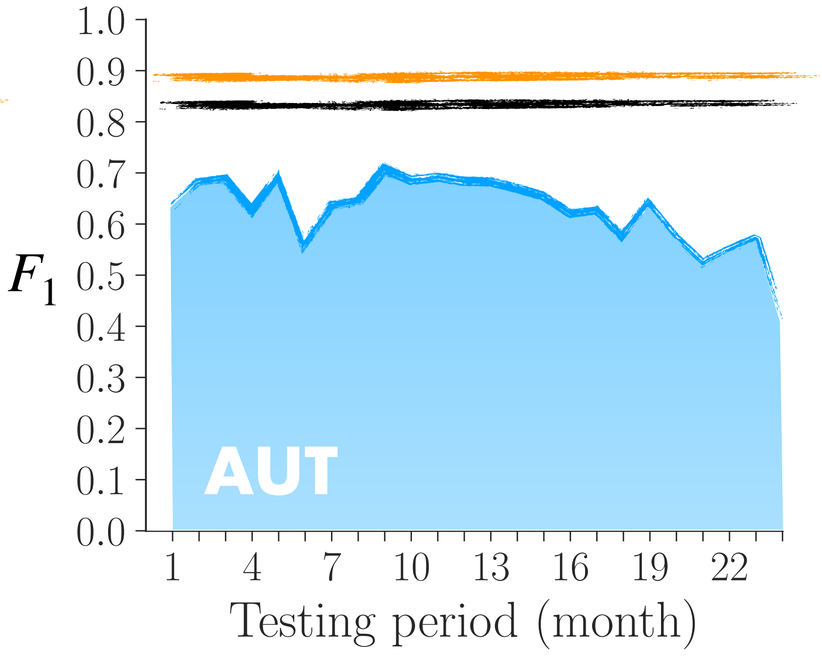
$AUT(F_1,24,m) = 0.58$

Method 1



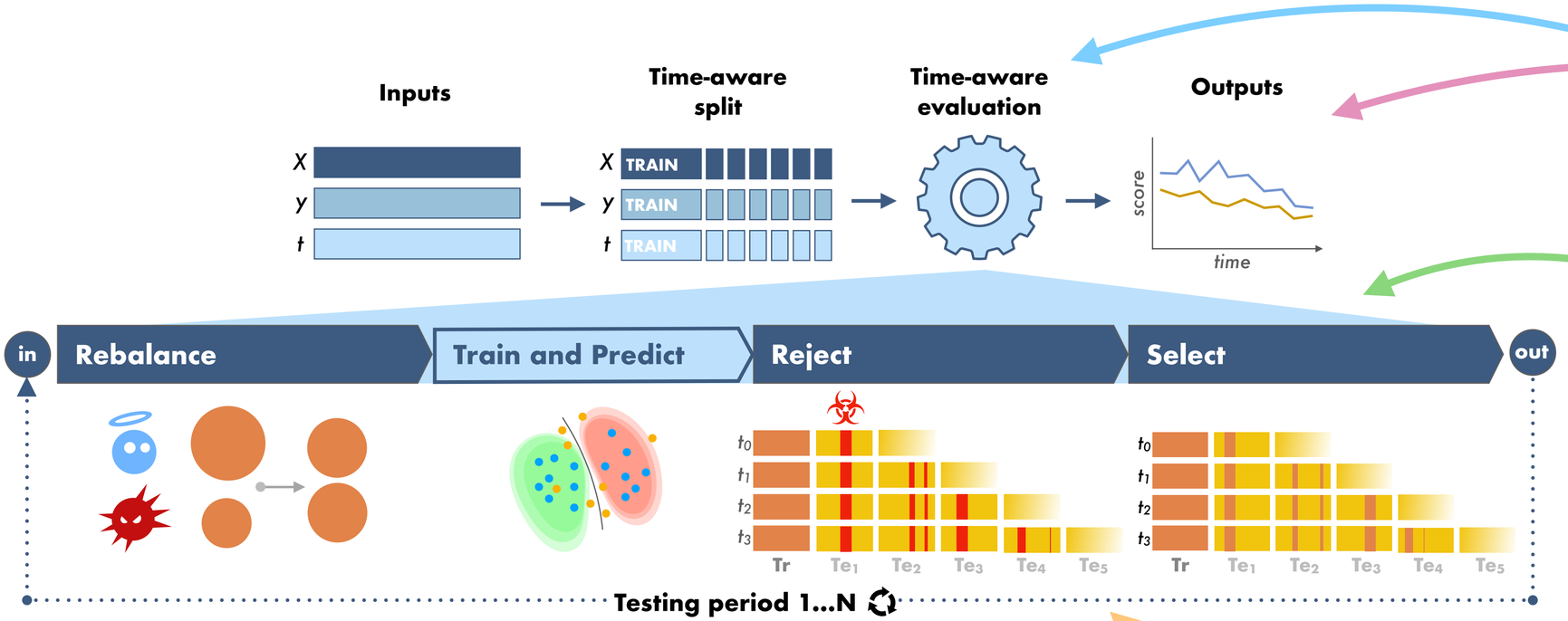
$AUT(F_1,24,m) = 0.32$

Method 3



$AUT(F_1,24,m) = 0.64$

Artifact Design

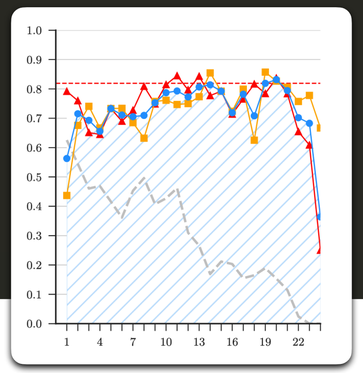


- Compatible with sklearn and pyplot
- Modular, designed to be extended
- Supports drift mitigations strategies

https://github.com/s2labres/tesseract-ml-release

Artifact: How easy is it to use?

```python
from sklearn.svm import SVC
from tesseract import evaluation, temporal, spatial, temporal, loader, metrics, viz

def main():
    # Load features, labels and timestamps
    X, y, t = loader.load_features('dataset_fname')

    # Partition dataset
    splits = temporal.time_aware_train_test_split(
        X, y, t, train_size=12, test_size=1, granularity='month')

    X_train, X_tests, y_train, y_tests, t_train, t_tests = splits

    # Enforce spatio-temporal constraints
    for y_test, t_test in zip(y_tests, t_tests):
        temporal.assert_positive_negative_temporal_consistency(y_test, t_test)
        temporal.assert_train_test_temporal_consistency(t_train, t_test)
        spatial.assert_class_distribution(y_test, positive_rate=0.1, variance=0.05)

    # Perform a timeline evaluation
    clf = SVC(kernel='linear', probability=True)
    results = evaluation.fit_predict_update(clf, *splits)

    # View results
    metrics.print_metrics(results)
    # View AUT(F1, 24 months) as a measure of robustness over time
    print(metrics.aut(results, 'f1'))

    # Generate plot
    plt = viz.plot_decay(results)
    plt.show()


if __name__ == '__main__':
    main()
```



← Imports

← Load timestamped datasets with helpers

← Split datasets by time in one line

← Assert each constraint to catch accidental bias or when analyzing existing datasets

← Run the evaluation, compatible with *sklearn* classifiers

← View key metrics such as AUT

← Generate and display *pyplot*-compatible charts

Key Influenced Work

Within our team...

- DroidEvolver++ (AISec '21)
- Transcendent (IEEE S&P '22)
- Drift Forensics (AISec '23)
- Tesseract (S&P-Magazine '23)

Best Runner-Up Paper Award

- RPAL (ARTMAN '24)

Through collaboration...

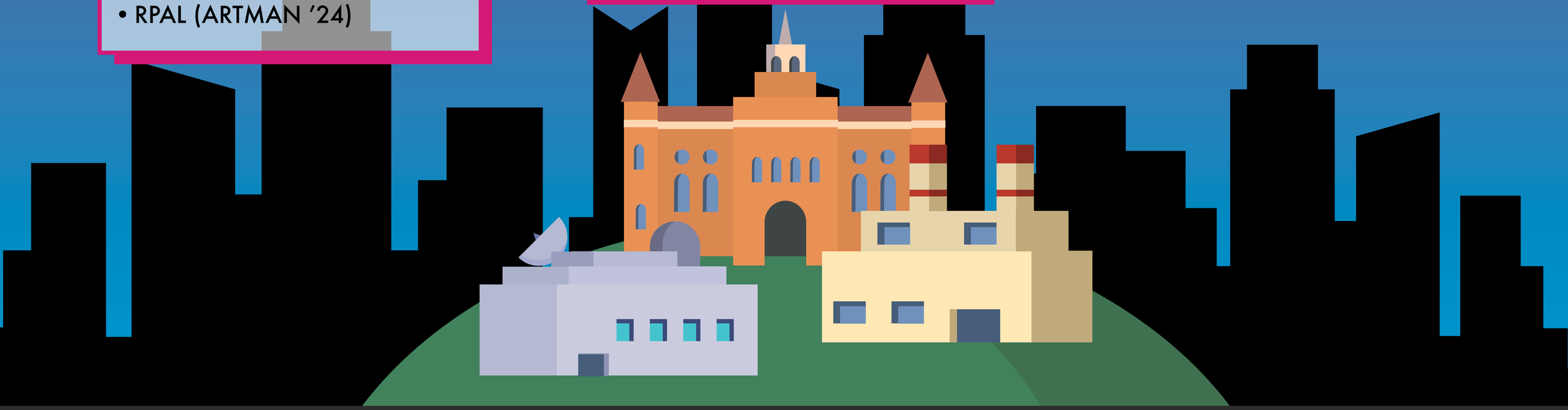
- Insomnia (AISec '21)
- Do's and Don'ts (USENIX Sec '22)

Distinguished Paper Award

- Is it Overkill? (DLS '23)

And beyond us...

- APIGraph (ACM CCS '20)
- Continuous Learning (USENIX Sec '23)
- Mateen (RAID '24)
- ... and more!



Academic Impact

450+ citations overall, incl:

- 41 PhD theses
- 12 MSc theses
- 38 Surveys and SoKs

Keynotes at:

- DLS 2023
- RAID 2024

Artifact shared with **100+** academic institutions across **27** countries, including:

Carnegie Mellon University
Columbia University
NYU
Princeton University
Northeastern University
Northwestern University
Rochester Institute of Technology
University of Toronto
Georgia Tech
CISPA Helmholtz Center for Information Security
TU Berlin
Technische Universität München
Notre Dame
Duke University
Tsinghua University
University of Science and Technology of China
Chinese Academy of Sciences
Universitas Studiorum Mediolanensis
Universidad Carlos III de Madrid
Rice
Technische Universität Darmstadt
Huazhong University of Science and Technology
Northwest University Xi'an China
Peking University
Indian Institute of Technology Kanpur
Indian Institute of Technology Madras
NUS National University of Singapore
King's College London
Brunel University London
Queen's University Belfast
Nanjing University
University of Cagliari
Politechnika Wrocławska
CTU Czech Technical University in Prague
UBC
大阪大学 Osaka University
The Alan Turing Institute
Université du Luxembourg
Technische Universität Braunschweig
UCL
UNSW Sydney

Industrial Impact

Artifact shared with **10+** industry and government institutions:

Meta

VISA Research

SAMSUNG

MITRE

TOSHIBA

EST SECURITY

Agence nationale de la sécurité des systèmes d'information — ANSSI

CapitalOne

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

iovation

Presented at industry-focused events:

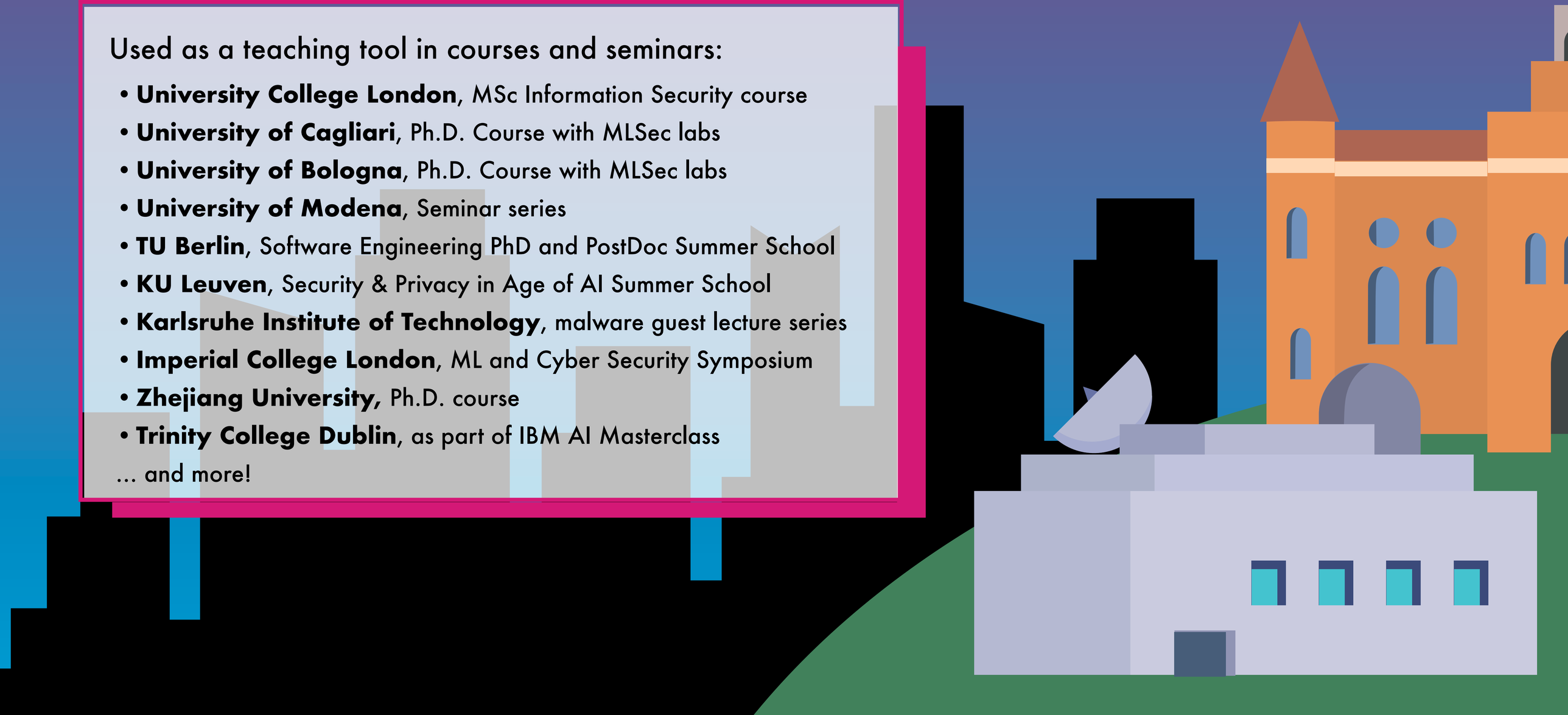
- USENIX ENIGMA, 2019
- Avast CyberSec&AI Connected, 2019
- IBM AI Masterclass, 2024

Educational Impact

Used as a teaching tool in courses and seminars:

- **University College London**, MSc Information Security course
- **University of Cagliari**, Ph.D. Course with MLSec labs
- **University of Bologna**, Ph.D. Course with MLSec labs
- **University of Modena**, Seminar series
- **TU Berlin**, Software Engineering PhD and PostDoc Summer School
- **KU Leuven**, Security & Privacy in Age of AI Summer School
- **Karlsruhe Institute of Technology**, malware guest lecture series
- **Imperial College London**, ML and Cyber Security Symposium
- **Zhejiang University,** Ph.D. course
- **Trinity College Dublin**, as part of IBM AI Masterclass

... and more!



Community Influence

From cited works:

- 34 explicitly avoided temporal bias
- 17 explicitly avoided spatial bias
- 27 explicitly avoided both
- And 10 of the above used AUT as a main metric

Shaping future research…

- Track 3 of the ELSA EU benchmark competition for cybersecurity uses Tesseract
- As does the Robust Android Malware Detection Competition at SatML

SYSTEMS SECURITY RESEARCH LAB

https://github.com/s2labres/tesseract-ml-release

"...and releasing the artifact on Github for everyone to use!"

SYSTEMS SECURITY RESEARCH LAB

From cited works:

- 34 explicitly avoided temporal bias
- 17 explicitly avoided spatial bias
- 27 explicitly avoided both
- And 10 of the above used AUT as a main metric

- 110+ research teams from 27+ countries
- 75+ papers integrated it in their methodology
- Foundational for future research

https://github.com/s2labres/tesseract-ml-release