Meeting of the LF AI & Data Technical Advisory Council (TAC)

January 13, 2022

LF AI & DATA

Antitrust Policy

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Undergone LLP, which provides legal counsel to the Linux Foundation.

Recording of Calls

Reminder:

TAC calls are recorded and available for viewing on the TAC Wiki

Reminder: LF AI & Data Useful Links

- Web site: lfaidata.foundation
- Wiki: wiki.lfaidata.foundation
- GitHub: github.com/lfaidata
- Landscape: https://landscape.lfaidata.foundation or https://l.lfaidata.foundation
- Mail Lists: https://lists.lfaidata.foundation
- Slack: https://slack.lfaidata.foundation
- Youtube: https://www.youtube.com/channel/UCfasaeqXJBCAJMNO9HcHfbA
- LF AI Logos: https://github.com/lfaidata/artwork/tree/master/lfaidata
- LF AI Presentation Template: https://drive.google.com/file/d/1eiDNJvXCqSZHT4Zk_-czASlz2GTBRZk2/view?usp=sharing

- Events Page on LF AI Website: https://lfaidata.foundation/events/
- Events Calendar on LF AI Wiki (subscribe available): https://wiki.lfaidata.foundation/pages/viewpage.action?pageId=12091544
- Event Wiki Pages: https://wiki.lfaidata.foundation/display/DL/LF+AI+Data+Foundation+Events

Agenda

- Roll Call (2 mins)
- Ethics in AI for Healthcare (10 minutes)
- Google Summer of Code Mentor brief update (5 minutes)
- Graduation proposal for ART (20minutes)
- Approval of Minutes from previous meetings (2 mins)
- LF AI General Updates (2 min)
- Open Discussion (2 min)

TAC Voting Members - Please note

Please ensure that you do the following to facilitate smooth procedural quorum and voting processes:

- Change your Zoom display name to include your First/Last Name, Company/Project Represented
    - example: Nancy Rausch, SAS
- State your First/Last Name and Company/Project when submitting a motion
    - example: First motion, Nancy Rausch/SAS

Challenge with TAC Quorum

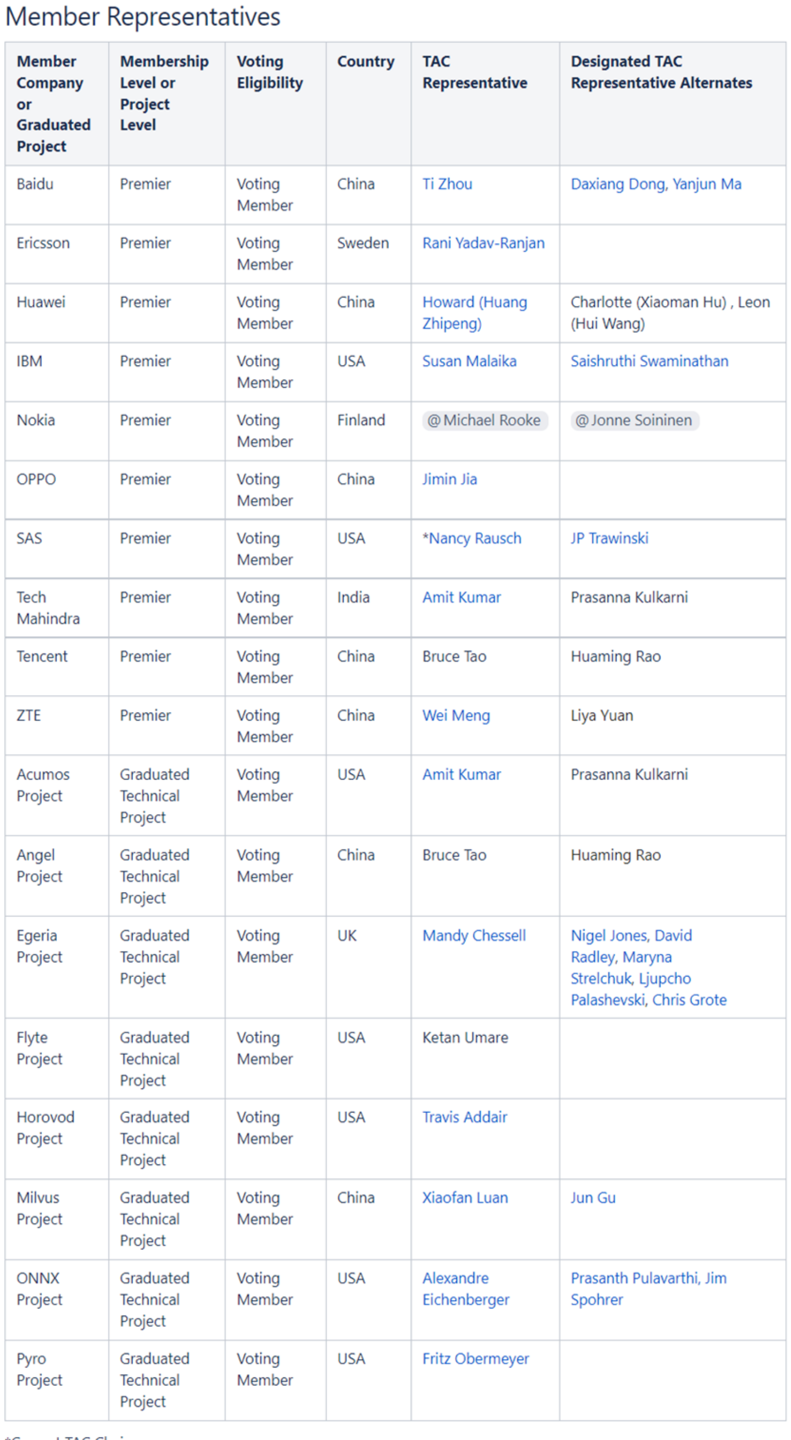
- 18 voting members requiring 10 voting members to achieve quorum

- Proposing updating charter to reflect the following changes:
  - A TAC voting member who misses 2 TAC meetings in a row will lose their voting seat until they attend twice in a row.

- Process: Socialize with GB and TAC. Propose amendment to the Charter and have the GB vote on it.

TAC Voting Members

* = still need backup specified on wiki



Member Representatives

Member Company or Graduated Project	Membership Level or Project Level	Voting Eligibility	Country	TAC Representative	Designated TAC Representative Alternates
Baidu	Premier	Voting Member	China	Ti Zhou	Daxiang Dong, Yanjun Ma
Ericsson	Premier	Voting Member	Sweden	Rani Yadav-Ranjan	
Huawei	Premier	Voting Member	China	Howard (Huang Zhipeng)	Charlotte (Xiaoman Hu) , Leon (Hui Wang)
IBM	Premier	Voting Member	USA	Susan Malaika	Saishruthi Swaminathan
Nokia	Premier	Voting Member	Finland	@Michael Rooke	@Jonne Soininen
OPPO	Premier	Voting Member	China	Jimin Jia	
SAS	Premier	Voting Member	USA	*Nancy Rausch	JP Trawinski
Tech Mahindra	Premier	Voting Member	India	Amit Kumar	Prasanna Kulkarni
Tencent	Premier	Voting Member	China	Bruce Tao	Huaming Rao
ZTE	Premier	Voting Member	China	Wei Meng	Liya Yuan
Acumos Project	Graduated Technical Project	Voting Member	USA	Amit Kumar	Prasanna Kulkarni
Angel Project	Graduated Technical Project	Voting Member	China	Bruce Tao	Huaming Rao
Egeria Project	Graduated Technical Project	Voting Member	UK	Mandy Chessell	Nigel Jones, David Radley, Maryna Strelchuk, Ljupcho Palashevski, Chris Grote
Flyte Project	Graduated Technical Project	Voting Member	USA	Ketan Umare	
Horovod Project	Graduated Technical Project	Voting Member	USA	Travis Addair	
Milvus Project	Graduated Technical Project	Voting Member	China	Xiaofan Luan	Jun Gu
ONNX Project	Graduated Technical Project	Voting Member	USA	Alexandre Eichenberger	Prasanth Pulavarthi, Jim Spohrer
Pyro Project	Graduated Technical Project	Voting Member	USA	Fritz Obermeyer	

*Current TAC Chair

Medical Ethics in AI

Jim St.Clair
www.lfph.io
https://calendly.com/jstclair-4
13JAN2022

LF AI & DATA

Linux Foundation Public Health (LFPH)

Overview for public health authorities, prospective members, and project maintainers

www.lfph.io

LF PUBLIC HEALTH

About Linux Foundation Public Health (LFPH)

- LF Public Health's mission is to use open source software to help public health authorities (PHAs) around the world.
- Founded in summer of 2020, the initial focus of LFPH has been helping PHAs deploy an app implementing the Google Apple Exposure Notification (GAEN) system.
- LFPH brought in the Covid Credentials Initiative to take lead on creating interoperable standards for sharing pandemic-related health data.
- As the organization grows we are moving into other areas of public health that can take advantage of open source innovation.

Why AI/ML in Healthcare?

- Software as a second pair of eyes in the ICU
- Personalized Treatments
- Reduce Administrative Burden
- Mining the Data Ocean

Clinical Tools

- Predictive Analysis: *e.g.* COVID surges
- Treatment recommendations – but not just CDS – learning constantly
- Monitoring patients: hospitalized and ambulatory
- Guiding surgical care: *e.g.* Black Box project
- Population Health

Administrative Utility

- Recording digital notes *e.g.* transcription
- Operations, such as scheduling
- Automation support
- Coding and billing

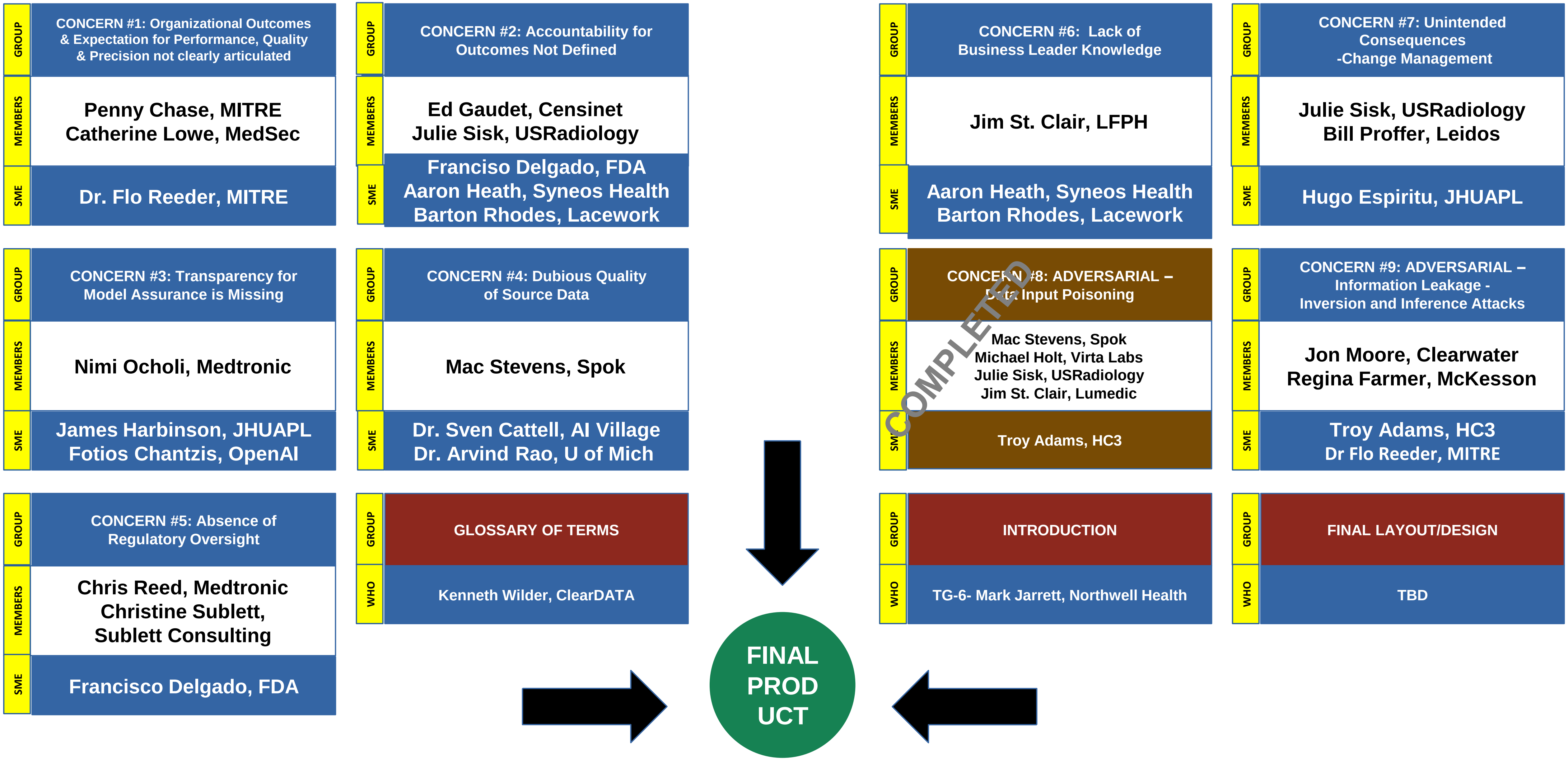
Challenges

- Data ocean pollution
- Transparency of algorithms: proprietary?
- Patient privacy
- Liability issues
- CYBERSECURITY

Healthcare & Public Health
Sector Coordinating Councils

Healthcare Tech Risk
AIML Bulletin – Sub-Group Assignments

Last Updated: 2021-07-30 REV 11



GROUP	CONCERN #1: Organizational Outcomes & Expectation for Performance, Quality & Precision not clearly articulated
MEMBERS	Penny Chase, MITRE Catherine Lowe, MedSec
SME	Dr. Flo Reeder, MITRE

GROUP	CONCERN #2: Accountability for Outcomes Not Defined
MEMBERS	Ed Gaudet, Censinet Julie Sisk, USRadiology
SME	Franciso Delgado, FDA Aaron Heath, Syneos Health Barton Rhodes, Lacework

GROUP	CONCERN #6: Lack of Business Leader Knowledge
MEMBERS	Jim St. Clair, LFPH
SME	Aaron Heath, Syneos Health Barton Rhodes, Lacework

GROUP	CONCERN #7: Unintended Consequences -Change Management
MEMBERS	Julie Sisk, USRadiology Bill Proffer, Leidos
SME	Hugo Espiritu, JHUAPL

GROUP	CONCERN #3: Transparency for Model Assurance is Missing
MEMBERS	Nimi Ocholi, Medtronic
SME	James Harbinson, JHUAPL Fotios Chantzis, OpenAI

GROUP	CONCERN #4: Dubious Quality of Source Data
MEMBERS	Mac Stevens, Spok
SME	Dr. Sven Cattell, AI Village Dr. Arvind Rao, U of Mich

COMPLETED

GROUP	CONCERN #8: ADVERSARIAL – Data Input Poisoning
MEMBERS	Mac Stevens, Spok Michael Holt, Virta Labs Julie Sisk, USRadiology Jim St. Clair, Lumedic
SME	Troy Adams, HC3

GROUP	CONCERN #9: ADVERSARIAL – Information Leakage - Inversion and Inference Attacks
MEMBERS	Jon Moore, Clearwater Regina Farmer, McKesson
SME	Troy Adams, HC3 Dr Flo Reeder, MITRE

GROUP	CONCERN #5: Absence of Regulatory Oversight
MEMBERS	Chris Reed, Medtronic Christine Sublett, Sublett Consulting
SME	Francisco Delgado, FDA

GROUP	GLOSSARY OF TERMS
WHO	Kenneth Wilder, ClearDATA

GROUP	INTRODUCTION
WHO	TG-6- Mark Jarrett, Northwell Health

GROUP	FINAL LAYOUT/DESIGN
WHO	TBD

FINAL PROD UCT

Proposed Training Plan

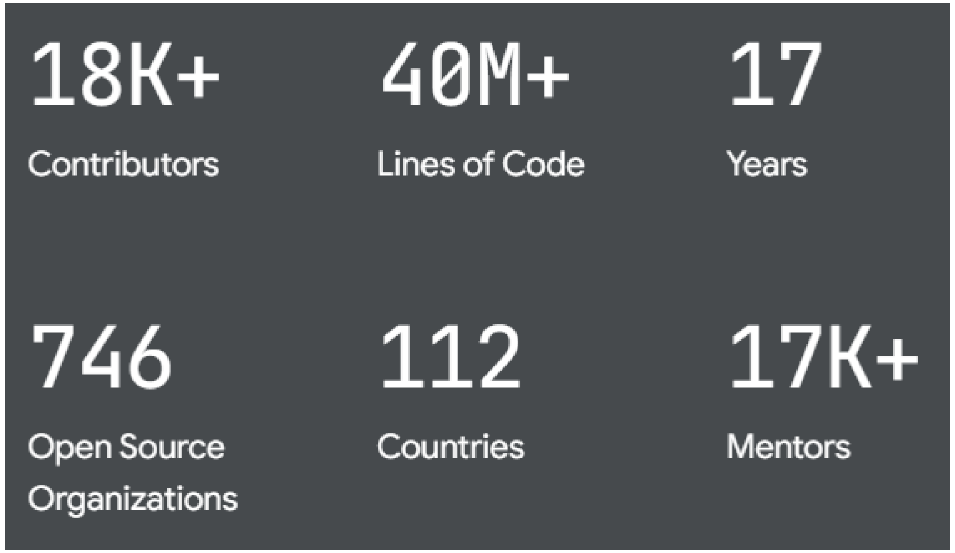
- Background of AI in Healthcare
- Concerns of AI/ML
- Example Frameworks
  - EU
  - UN
  - China
- LF AI tools

Google Summer of Code - Interest in LFAI Mentorship?

Jun Gu

Apply Google Summer of Code 2022

A global, online program focused on bringing new contributors into open source software development.



18K+
Contributors

40M+
Lines of Code

17
Years

746
Open Source Organizations

112
Countries

17K+
Mentors

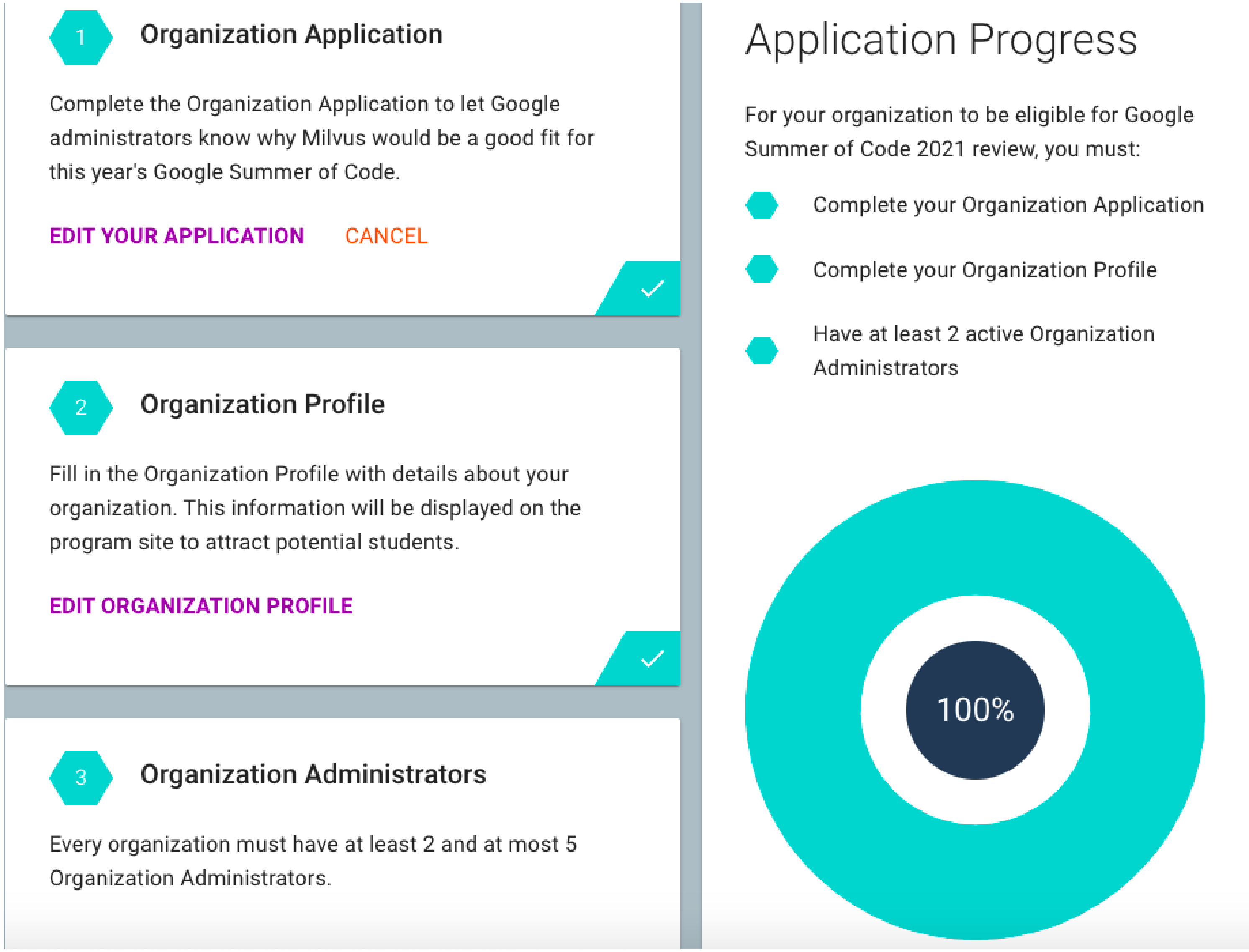
More details:
https://summerofcode.withgoogle.com/

Expanding Google Summer of Code in 2022

The organizations apply in **Feb. 2022**, what we need to do?

- Register the organization with GSoC
  - 2-5 org administrators needed
- List the program ideas/projects, e.g.,
  - The idea/project in detail
  - The mentors for the idea
  - Skills needed for the idea
  - The expected outcome of the idea

Reference from GSoC 2021: Organization Application



1 **Organization Application**

Complete the Organization Application to let Google administrators know why Milvus would be a good fit for this year's Google Summer of Code.

EDIT YOUR APPLICATION   CANCEL

✓

2 **Organization Profile**

Fill in the Organization Profile with details about your organization. This information will be displayed on the program site to attract potential students.

EDIT ORGANIZATION PROFILE

✓

3 **Organization Administrators**

Every organization must have at least 2 and at most 5 Organization Administrators.

Application Progress

For your organization to be eligible for Google Summer of Code 2021 review, you must:

- Complete your Organization Application
- Complete your Organization Profile
- Have at least 2 active Organization Administrators

ART Graduation Proposal

Animesh Singh
Beat Buesser
13JAN2022

LF AI & DATA

Adversarial Robustness Toolbox (ART)

Adversarial Robustness Toolbox

ART is a Python library for machine learning security

TensorFlow Keras

PYTORCH mxnet

scikit learn GPy

dmlc XGBoost LightGBM CatBoost

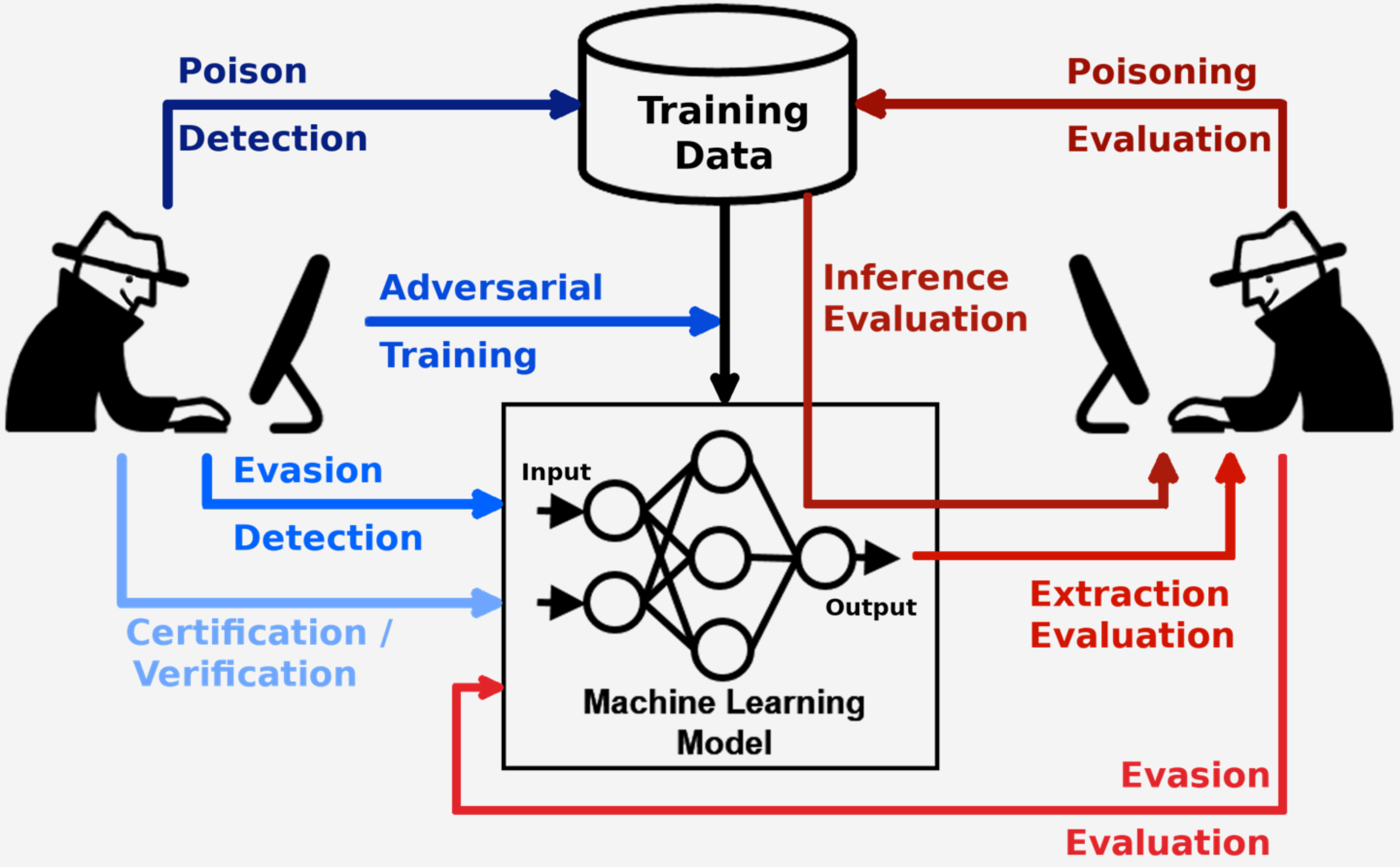
- github.com/Trusted-AI/adversarial-robustness-toolbox
- **Goal:** provide tools to developers and researcher for evaluating, defending, certifying and verifying machine learning models and applications
- **All Tasks:** Classification, Object Detection, Object Tracking, Speech Recognition, Generation, Encoding, Certification, etc.
- **All Frameworks:** TensorFlow, Keras, PyTorch, MXNet, scikit-learn, XGBoost, LightGBM, CatBoost, GPy
- **All Data Types:** images, tables, audio, video, etc.

Defending and Evaluating with ART

Adversarial Robustness Toolbox

ART's Blue Team tools (selection)

ART's Red Team tools

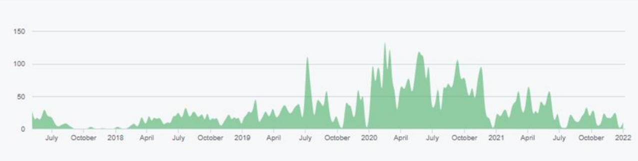


The Graduation Requirements – Summary

- Have a healthy number of code contributions coming from at least five organizations.
  - https://github.com/Trusted-AI/adversarial-robustness-toolbox/blob/main/AUTHORS
  - IBM, Two Six Technologies, Kyushu University, Intel, University of Chicago, MITRE, General Motors, AGH University of Science and Technology, Rensselaer Polytechnic Institute (RPI), IMT Atlantique, Johns Hopkins University, Troj.AI
- Have reached a minimum of 1000 stars on GitHub.
  - 2711 Stars
- Have achieved and maintained a Core Infrastructure Initiative Best Practices Gold Badge.

cii best practices gold

- Have demonstrated a substantial ongoing flow of commits and merged contributions for the past 12 months.



- Have completed at least one collaboration with another LF AI & Data hosted project.

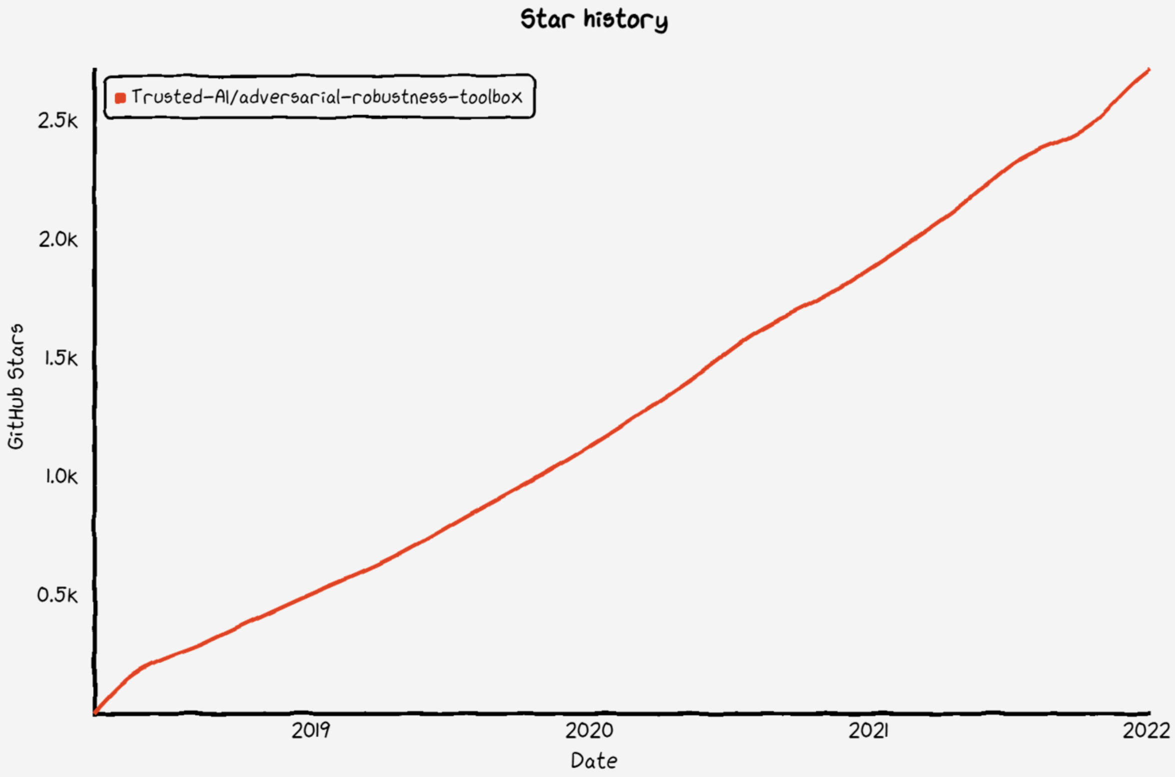
AI Fairness 360

- Have a technical lead appointed for the representation of the project on the LF AI & Data Technical Advisory Council
  - Beat Buesser (IBM)

ART Community

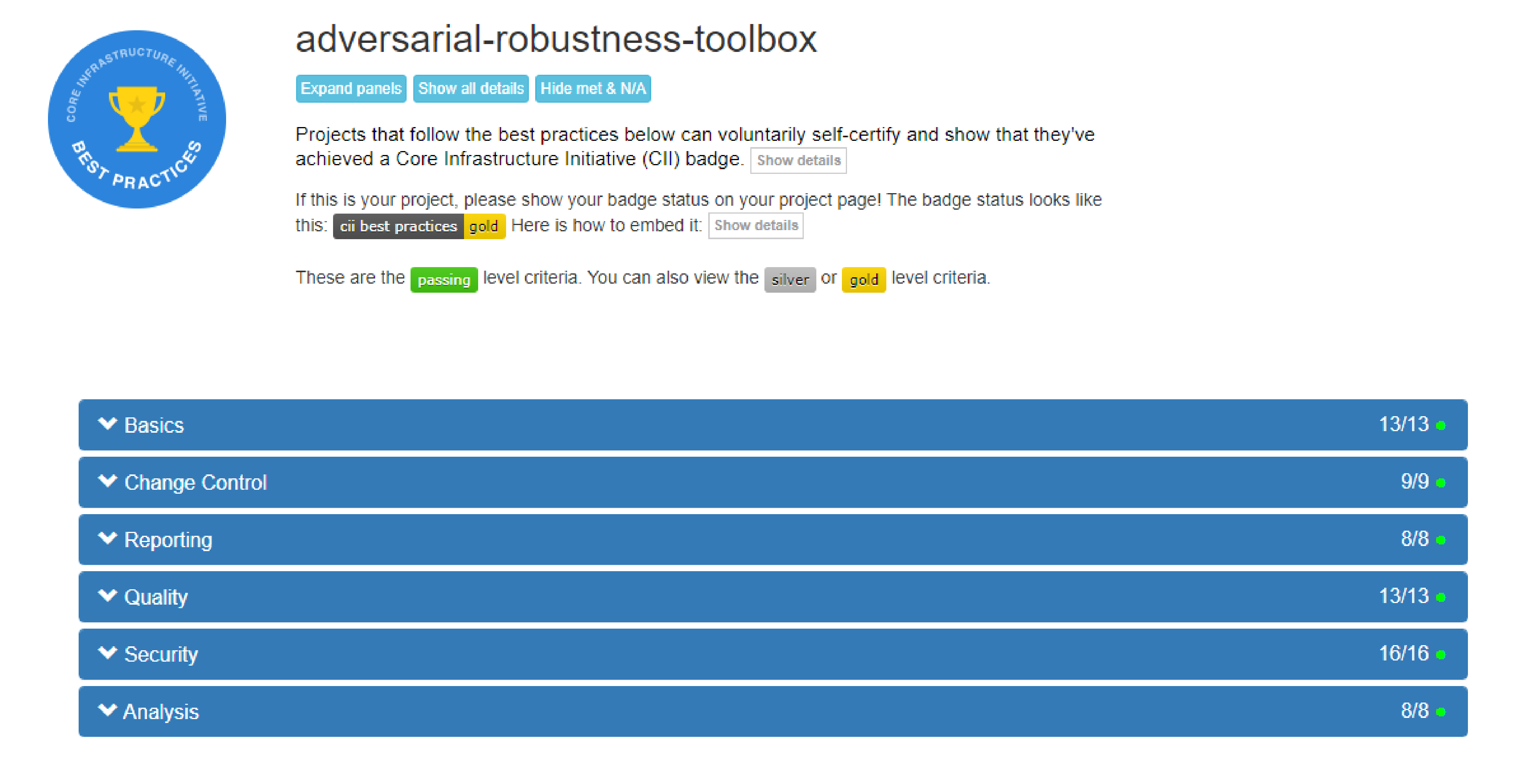
Adversarial Robustness Toolbox

- Contributors: 70
- Authors:
  - IBM, Two Six Technologies, Kyushu University, Intel, University of Chicago, MITRE, General Motors, AGH University of Science and Technology, Rensselaer Polytechnic Institute (RPI), IMT Atlantique, Johns Hopkins University, Troj.AI
- GitHub Stars: 2711
- GitHub Forks: 758
- Slack workspace members: 336



Best Practices Badge

Adversarial Robustness Toolbox



adversarial-robustness-toolbox

Expand panels | Show all details | Hide met & N/A

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved a Core Infrastructure Initiative (CII) badge. Show details

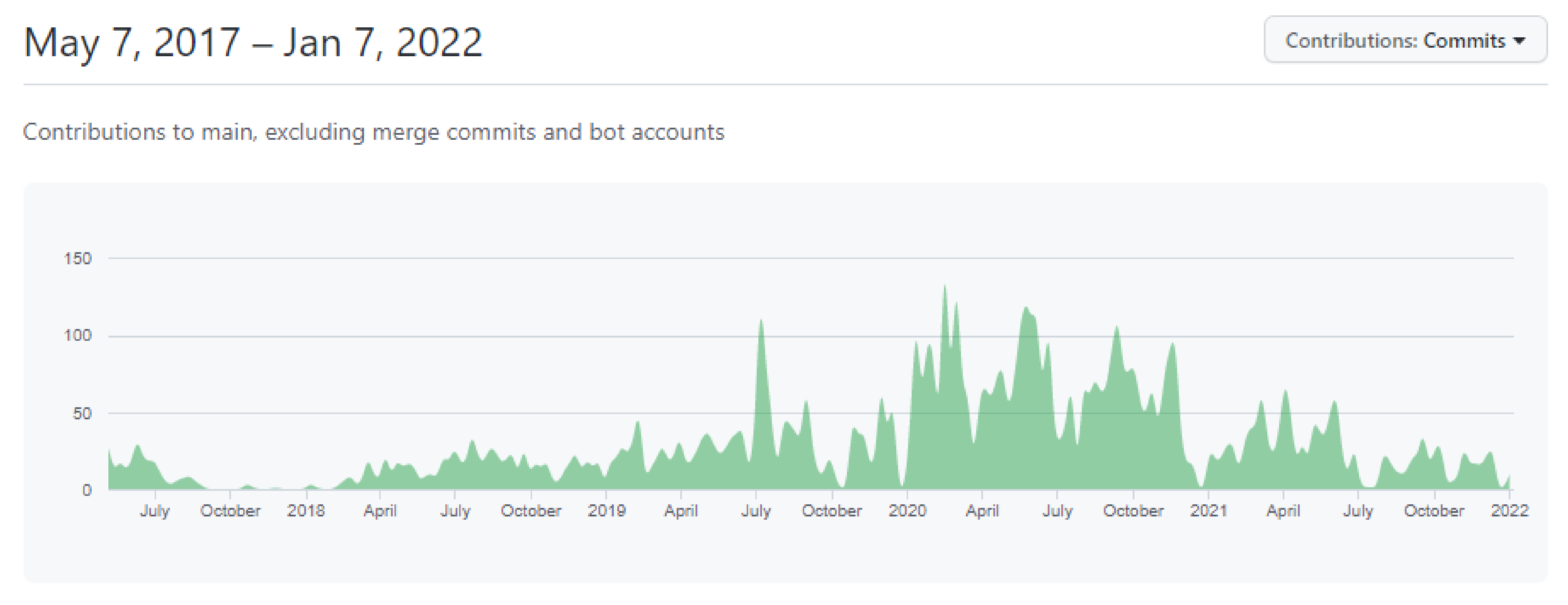
If this is your project, please show your badge status on your project page! The badge status looks like this: cii best practices gold Here is how to embed it: Show details

These are the passing level criteria. You can also view the silver or gold level criteria.

Basics	13/13 ●
Change Control	9/9 ●
Reporting	8/8 ●
Quality	13/13 ●
Security	16/16 ●
Analysis	8/8 ●

Commit History

Adversarial Robustness Toolbox



May 7, 2017 – Jan 7, 2022

Contributions: Commits ▾

Contributions to main, excluding merge commits and bot accounts

Governance and Procedures

Adversarial Robustness Toolbox

- **Contributors Guide**
  - https://github.com/Trusted-AI/adversarial-robustness-toolbox/blob/main/CONTRIBUTING.md

- **Governance Information**
  - https://github.com/Trusted-AI/adversarial-robustness-toolbox/blob/main/CODE_OF_CONDUCT.md
  - https://github.com/Trusted-AI/adversarial-robustness-toolbox/blob/main/SECURITY.md
  - https://github.com/Trusted-AI/adversarial-robustness-toolbox/wiki/Code-Reviews

ART Project Leader

Beat Buesser, Dr. sc. ETH Zurich

Research Staff Member at IBM Research in the AI Security and Privacy group at the Dublin Research Laboratory, Ireland and co-lead of AI Security research and development at IBM Research.

He is maintainer and leading the core-development team of the Adversarial Robustness Toolbox (ART) as open-source project of the LF AI & Data Foundation.

Before joining IBM, he graduated from ETH Zurich and worked at the Massachusetts Institute of Technology (MIT).

Collaboration with LF AI & Data Projects and Members

Adversarial Robustness Toolbox

- Integrated **Adversarial Robustness Toolbox (ART)** classification model abstractions into LFAI’s **AI Fairness (AIF) 360** as Transformer serving as abstraction for any process which acts on an AIF’s Dataset and returns a new, modified Dataset encompassing pre-processing, in-processing, and post-processing algorithms for fairness evaluations.

AI Fairness 360

12 Months Roadmap

Adversarial Robustness Toolbox

- **ART 1.9 (December 15, 2021)**
  - Adversarial Textures attack on object tracking models
  - Support for JAX models
  - Shadow model training for membership inference attacks
  - Modified adversarial training as poisoning defense
  - Ensemble defense against poisoning
  - Hidden Trigger Backdoor poisoning attack
  - Poison Frogs poisoning attack
  - Adversarial Laser Pointer attack
  - Etc.
- **ART 1.10 (March 15, 2022)**
  - Sleeper Agent poisoning attack
  - Expand robustness certification tools
  - Query-efficient black-box evasion attacks: Sign-Opt, SurFree, etc.
  - Etc.
- **ART 1.11 (June 15, 2022)**
  - Redesign notebook examples and presentation on Binder
  - Etc.
- **ART 1.12 (September 15, 2022)**

Thank you

Beat Buesser
Maintainer of ART
Research Staff Member
IBM Research
—
beat.buesser@ie.ibm.com

TAC Vote on ART Graduation Proposal

Proposed Resolution:

The TAC approves the ART proposal as a graduation project of the LF AI & Data Foundation

Minutes approval

LF AI & DATA

Approval of December 2nd, 2021 Minutes

Draft minutes from the December 2nd TAC call were previously distributed to the TAC members via the mailing list

Proposed Resolution:

- That the minutes of the December 2nd meeting of the Technical Advisory Council of the LF AI & Data Foundation are hereby approved.

Approval of December 16th, 2021 Minutes

Draft minutes from the December 16 TAC call were previously distributed to the TAC members via the mailing list

Proposed Resolution:

- That the minutes of the December 16 meeting of the Technical Advisory Council of the LF AI & Data Foundation are hereby approved.

Upcoming TAC Meetings

LF AI & DATA

Upcoming TAC Meetings

- January 27, 2021: Artigraph – Incubation proposal
- February 10, 2022: Kompute moving from Sandbox to Incubation

Please send agenda topic requests to tac-general@lists.lfaidata.foundation

Open Discussion

TAC Meeting Details

- To subscribe to the TAC Group Calendar, visit the wiki: https://wiki.lfaidata.foundation/x/cQB2 ______
- Join from PC, Mac, Linux, iOS or Android: https://zoom.us/j/430697670
- Or iPhone one-tap:
  - US: +16465588656,,430697670# or +16699006833,,430697670#
- Or Telephone:
  - Dial(for higher quality, dial a number based on your current location):
  - US: +1 646 558 8656 or +1 669 900 6833 or +1 855 880 1246 (Toll Free) or +1 877 369 0926 (Toll Free)
- Meeting ID: 430 697 670
- International numbers available: https://zoom.us/u/achYtcw7uN

Legal Notice

- The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation's Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.
- Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute's trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.
- Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.
- TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.
- Facebook and the "f" logo are trademarks of Facebook or its affiliates.
- LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.
- YouTube and the YouTube icon are trademarks of YouTube or its affiliates.
- All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.
- The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy. each as may be modified from time to time. More information about The Linux Foundation's policies is available at https://www.linuxfoundation.org.
- Please email legal@linuxfoundation.org with any questions about The Linux Foundation's policies or the notices set forth on this slide.

LF AI & DATA