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

September 7, 2023

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 (1 mins)
- Approval of Minutes from previous meeting (2 mins)
- Trusted AI Committee update (20 minutes)
- ML Security Committee update (20 minutes)
- Open Discussion

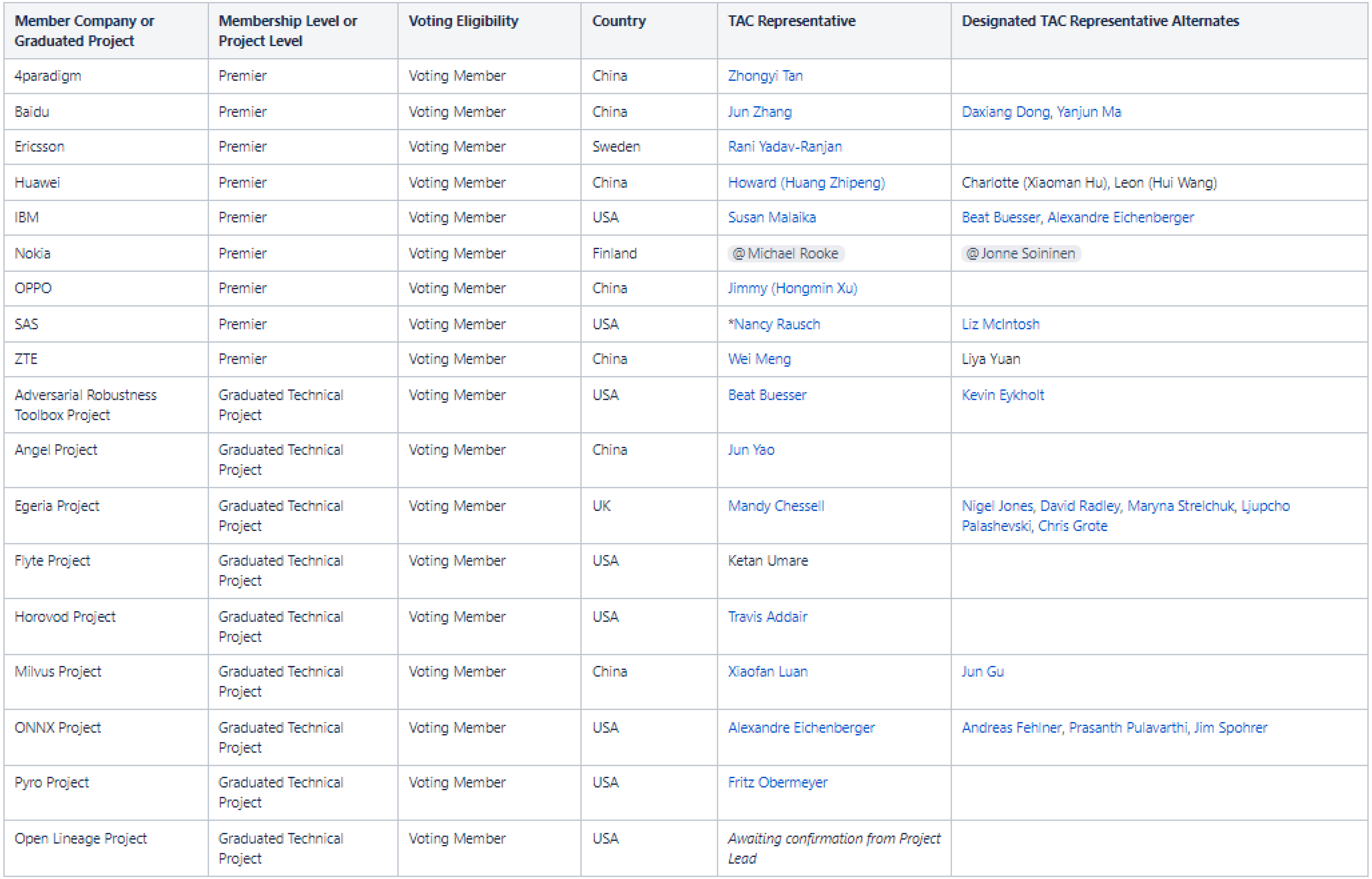
TAC Voting Members - Please note

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

TAC Voting Members

Note: we still need a few designated backups specified on wiki



Member Company or Graduated Project	Membership Level or Project Level	Voting Eligibility	Country	TAC Representative	Designated TAC Representative Alternates
4paradigm	Premier	Voting Member	China	Zhongyi Tan	
Baidu	Premier	Voting Member	China	Jun Zhang	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	Beat Buesser, Alexandre Eichenberger
Nokia	Premier	Voting Member	Finland	@Michael Rooke	@Jonne Soininen
OPPO	Premier	Voting Member	China	Jimmy (Hongmin Xu)	
SAS	Premier	Voting Member	USA	*Nancy Rausch	Liz McIntosh
ZTE	Premier	Voting Member	China	Wei Meng	Liya Yuan
Adversarial Robustness Toolbox Project	Graduated Technical Project	Voting Member	USA	Beat Buesser	Kevin Eykholt
Angel Project	Graduated Technical Project	Voting Member	China	Jun Yao	
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	Andreas Fehlner, Prasanth Pulavarthi, Jim Spohrer
Pyro Project	Graduated Technical Project	Voting Member	USA	Fritz Obermeyer	
Open Lineage Project	Graduated Technical Project	Voting Member	USA	*Awaiting confirmation from Project Lead*	

Minutes approval

LF AI & DATA

Approval of August 24, 2023 Minutes

Draft minutes from the August 24 TAC call were previously distributed to the TAC members via the mailing list

Proposed Resolution:

- That the minutes of the August 24 meeting of the Technical Advisory Council of the LF AI & Data Foundation are hereby approved.

LF AI & DATA

Trusted AI Committee

Recap & 23/24 Plan

LF AI & Data - TAC Presentation

September 7, 2023

Basic Information

Wiki	https://wiki.lfaidata.foundation/display/DL/Trusted+AI+Committee
Mailing list	
(Site)	https://lists.lfaidata.foundation/g/trustedai-committee
(Email)	trustedai-committee@lists.lfaidata.foundation
Calendar	https://lists.lfaidata.foundation/g/trustedai-committee/calendar
Repository	https://github.com/Trusted-AI

Monthly calls:
Trusted AI Committee Monthly Meeting - 4th Thursday of the month (additional meetings as needed)

Agenda

- **Activity Summary**
    - Sessions delivered
    - Blogs published
    - Connecting Trusted AI Projects to related activities
        - ONNX https://lfaidata.foundation/projects/onnx/ and Trusted AI
        - CMF https://github.com/HewlettPackard/cmf and Trusted AI
- **News from the Trusted AI open source projects** https://lfaidata.foundation/projects
    - Adversarial Robustness Toolbox - Beat Buesser https://lfaidata.foundation/projects/adversarial-robustness-toolbox/
    - AI Explainability - Vijay Arya https://lfaidata.foundation/projects/ai-explainability-360/
    - AI Fairness - Sam Hoffman https://lfaidata.foundation/projects/ai-fairness-360/
    - Intersectional Fairness https://lfaidata.foundation/projects/intersectional-fairness-isf/
- **Plans for 2023/24**
    - Trusted AI Day in 1H 2024
    - New LF Podcast → AI Horizons: Visions of Tomorrow
    - AI Software Bill of Materials (AISBOM) Project for Transparency requirements for EU AI Act and others → Focus on standard format, access to information, where to store, etc.
    - Benchmark metrics for LLM → Focus on the how, initial exploration of approaches + industry guests from Hugging Face and other orgs

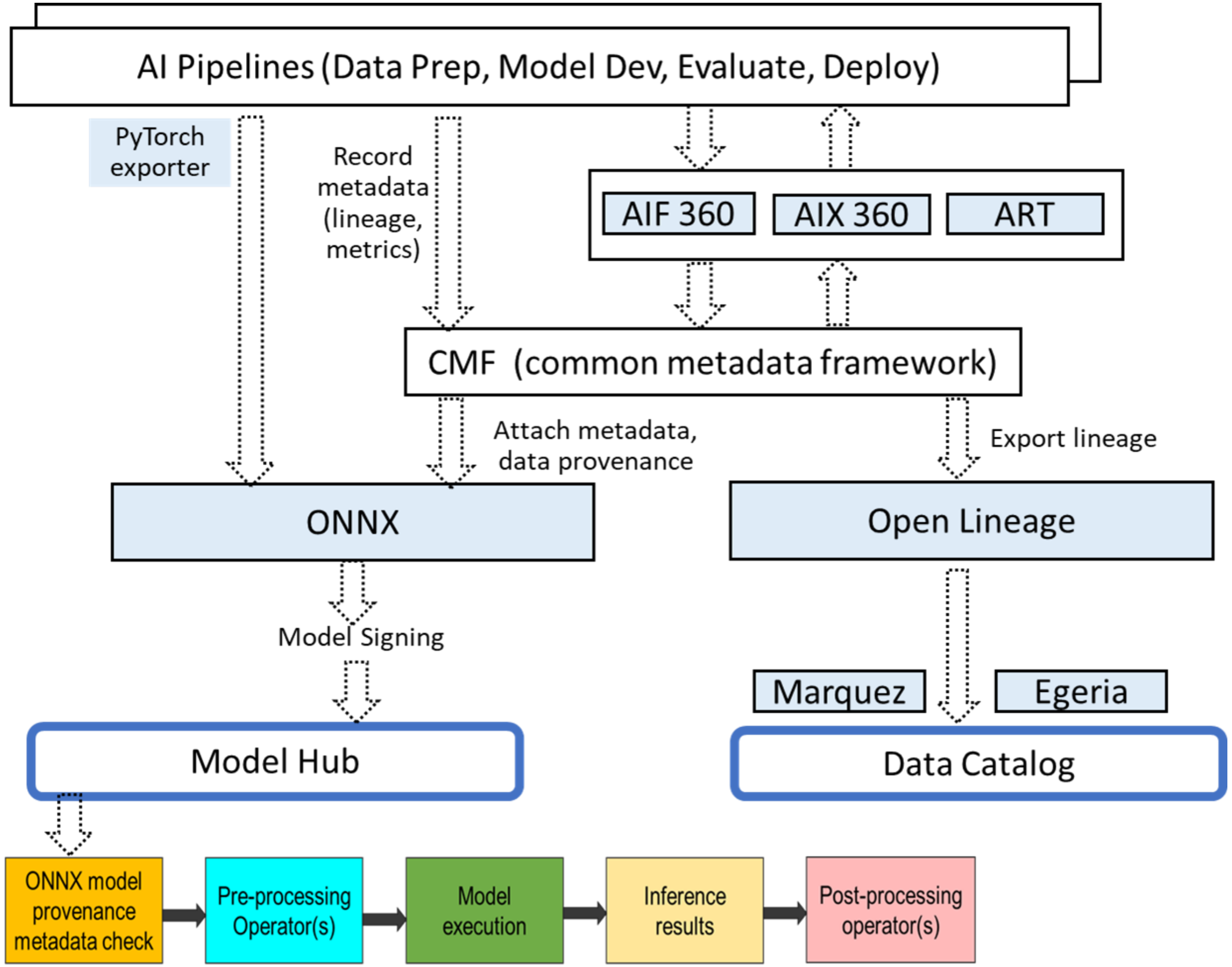
Consideration: Emerging Generative AI Committee

Join us

Trusted AI Activity Summary

Items	Contact	When	Information	Comments
Blog Articles	Ofer Hermoni & Adrián González Sánchez	July 17	2023: The Time for Accountable AI is NOW	Article for current status of international AI regulations and initiatives + open source considerations. Potential follow-up for diversity topics, suggested by Phaedra Boinodiris
	Nora Anwar	Through 2023	More blogs e.g., - *The role of transparency and ontologies* - *AIF 360 at Grace Hopper Open Source Day* *https://ghc.anitab.org/awards-programs/open-source-day/* - *Connecting Trusted AI Projects*	Publicize the ability to publish blogs on the LF-AI website Proposed Blog authors: *-Ali Hashmi and Aalap Tripathi ;* *-Anupama Murthi , Sam Hoffman, and Karthi Ramamurthy* *- Suparna Bhattacharya*
Topic Presentations	Adrián González Sánchez	April 6 & 27	AI Act Overview and updates	The Trusted AI Committee grew as a result of this session
	Suparna Bhattacharya	May 25, Jun 22	Common Metadata Framework (CMF) and Data Centric Foundation for Trustworthy AI	
	Suparna Bhattacharya, Vijay Arya, Ann Maty Roy , Rodolfo (Gabe) Esteves, Soumi Das	Jun 8, July 13	Responsible AI at ONNX, Metadata, Model Cards, Provenance at 31 minutes for 30 minutes AI Explainability and Metadata	
Presentations from companies or/and LF projects	Andreas Fehlner, Martin Nocker,	July 27	HE-MAN – Homomorphically Encrypted MAchine learning with oNnx models.	
	Lucy Hyde, John Tine, Oita Coleman	June 8	Open Voice Network,	New connections were made
Presentations at other venues	Andreas Fehlner	June 28	Onnx Community Meetup 2023 Roundtable Discussion on Trusted AI	This activity provided publicity for the Trusted AI Committee

Activity in 2023:
Connecting Trusted AI related Projects


AI Pipelines (Data Prep, Model Dev, Evaluate, Deploy)
PyTorch exporter
Record metadata (lineage, metrics)
AIF 360
AIX 360
ART
CMF (common metadata framework)
Attach metadata, data provenance
Export lineage
ONNX
Open Lineage
Model Signing
Marquez
Egeria
Model Hub
Data Catalog
ONNX model provenance metadata check
Pre-processing Operator(s)
Model execution
Inference results
Post-processing operator(s)

News from the Trusted AI Projects

Project	Contact	News in 2023	Generative AI Considerations
Adversarial Robustness Toolbox https://lfaidata.foundation/projects/adversarial-robustness-toolbox/	Beat Buesser beat.buesser@ibm.com	Reached 3.9k GitHub Stars and growth remains steady and linear with time Published 4 releases in the past 12 months with ART 1.16 planned for September 15, 2023 New features for evaluation of object detection and tracking models including support for Yolo models and support for evasion and poisoning attacks	Work is in progress to provide an initial version of an ART Estimators that facilitates the connection of HuggingFace vision transformer models with ART's attacks to evaluate the robustness against evasion and safety of models used for generative AI in the image and video domain.
AI Explainability 360 https://lfaidata.foundation/projects/ai-explainability-360/	Vijay Arya vijay.arya@in.ibm.com	1.4k stars AI Explainability Toolkit v0.3.0 released with new explainability algorithms and time series support.	Planning to integrate algorithms that support Generative-AI use cases (e.g. new version of SHAP, etc.)
AI Fairness 360 https://lfaidata.foundation/projects/ai-fairness-360/	Sam Hoffman shoffman@ibm.com	2.1k stars currently 12 first-time committers in the last year 2 new collaborations with Horizon Europe projects — AutoFair and MAMMOth The AIF360 project is part of the Grace Hopper 2023 Open Source Day	Working towards fully integrating inFairness https://ibm.github.io/inFairness which supports group and individual fairness for language models
Intersectional Fairness https://lfaidata.foundation/projects/intersectional-fairness-isf/	Koji Yamamoto yamamoto.kouji@fujitsu.com	Joined as a sandbox project to LF AI & Data (Approved in June 2023; to be announced at LF Open Source Summit Europe in September 2023). After the announcement, plan to start discussions with the AIF360 team for integration or collaboration with AIF360.	No plan for it yet.

Proposed Workstreams for 2023/24

LF AI & DATA

Workstream	Contact	Description	Comments
Events Trusted AI Day	Susan Malaika malaika@us.ibm.com	Conduct an 2-3 hour event "Trusted AI Day" in 1Q2024 perhaps focusing on: - Part 1 - Using the Trusted AI tools - Part 2 - A synopsis of the latest regulations - Part 3 - Trusted AI and Generative AI Activities	If a Generative AI Day is considered more suitable, the Trusted AI Committee can support that If there is an LF event in 1Q, the Trusted AI Day can happen there
Outreach and Education Podcast → AI Horizons: Visions of Tomorrow Blogs	Adrian Gonzalez Sanchez adrian.gonzalez-sanchez@hec.ca adriango@microsoft.com	- New LF Podcast, similar to old ones such as The Untold Stories of Open Source - The idea behind it is to use this podcast as a neutral space for divergent opinions, views, predictions, etc. - Focus on AI topics, including Responsible AI, Generative AI, regulations, news, etc.	Working with Nora to set technical tools, podcast branding, etc. Preparing calendar and guests, WIP + Engagement metrics TBD
Regulation AI-SBOM for Transparency Requirements	Adrian Gonzalez Sanchez adrian.gonzalez-sanchez@hec.ca adriango@microsoft.com	- AI Software Bill of Materials kind of specification for transparency requirements, including EU AI Act and other regulations - Including Generative AI requirements - Focus on standard format, access to information, where to store, etc. - Possibility to move repo to LF AI & Data? - Andreas - SPDX? open SSF - Susan - Relationship with modelcards and factsheets?	The initial outcome will be a JSON specification with required parameters. Initial focus on EU AI Act (because of Adrian's involvement with the Spanish AI Sandbox for the transparency article and guidelines). Existing discussions with other European network of AI regulations experts + initial collaboration with AI Verify (Singapore) to incorporate the AI-SBOM.
Technical FM/LLM Evaluation Techniques Analysis, along dimensions of trust	Suparna Bhattacharya suparna.bhattacharya@hpe.com	- Focus on the how: approaches and metrics - Initial exploration of evaluation and benchmarking approaches, looking for some convergence - Industry guests from different organizations working on evaluation/benchmark	This is a new workstream, complements prior work to expand metadata and lineage in ONNX further to Gen AI/Foundation models ecosystem

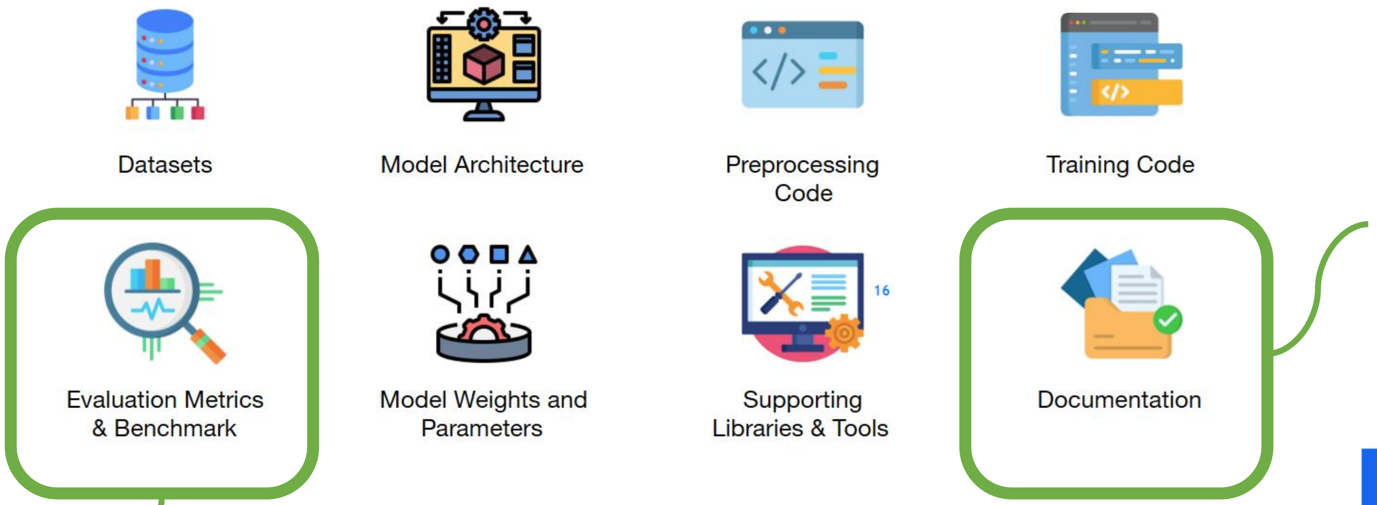
More on Podcast →
AI Horizons: Visions of Tomorrow

- Goal and Objectives
  - Raise AI awareness by providing educational content
  - Provide a neutral platform for diverse opinions
  - Connect LF projects & committees

- Target Audience
  - AI practitioners of all levels

- Format and Structure
  - Solo, co-hosted, interview, panels
  - Video podcast format
  - Episode duration: 20-40 mins

Consideration: Convergence areas with Generative AI Committee



Datasets

Model Architecture

Preprocessing Code

Training Code

Evaluation Metrics & Benchmark

Model Weights and Parameters

Supporting Libraries & Tools

Documentation

Trusted AI focus → Transparency requirements for AI, including Generative AI and High Risk applications. Initially for EU AI Act, potential expansion to other future regulations.

Input for Generative AI Committee's documentation workstream.

Complementary workstreams:

- **Trusted AI focus** → Understanding the different benchmark and best practices for comparison between Generative AI models.
- **Generative AI Committee focus** → Analyzing metrics and benchmark for a specific Generative AI model, to evaluate its level of openness.

Level 01	BRONZE Basic Open Source	Model architecture **Documentation** Supporting libraries and tools
Level 02	SILVER Enhanced Open Source	Preprocessing code Training code Model weights and parameters
Level 03	GOLD Extended Open Source	**Evaluation metrics and benchmarks**
Level 04	Platinum Advanced Open Source	Datasets

Opportunities & Challenges

- Opportunities
  - Perfect timing for parallel work streams with Trusted AI and Generative AI Committees
  - Internal traction to get a good set of volunteers
  - Available marketing resources to increase awareness and showcase progress

- Challenges
  - Disparate / ongoing evolution of benchmarking and evaluation models - e.g.
    - Holistic Evaluation of Language Models (HELM) (stanford.edu)
    - Chat with Open Large Language Models (lmsys.org)
    - Open LLM Leaderboard - a Hugging Face Space by HuggingFaceH4
    - MMLU Benchmark (Multi-task Language Understanding) | Papers With Code
    - MTEB Leaderboard - a Hugging Face Space by mteb
    - LLM Evaluation Metrics (mosaicml.com)
    - Alpaca Eval Leaderboard (tatsu-lab.github.io)
    - GitHub - google/BIG-bench
    - GitHub - EleutherAI/lm-evaluation-harness

Mechanisms for running the committee: Slack is convenient BUT :

currently we lose notes after 3 months on slack - creating this presentation was difficult

Call to Action

Join us:

- Open Source Projects- Contacts;
  - Adversarial Robustness Toolbox: Beat Buesser beat.buesser@ibm.com
  - AI Explainability 360: Vijay Arya vijay.arya@in.ibm.com
  - AI Fairness 360: Sam Hoffman shoffman@ibm.com
  - Intersectional Fairness:
- Event Planning : Trusted AI Day in 2024
  - Contact: Susan Malaika malaika@us.ibm.com
- Outreach and Education : blogs, podcasts etc
  - Adrian Gonzalez Sanchez adrian.gonzalez-sanchez@hec.ca ; adriango@microsoft.com
  - Nora Anwar nanwar@linuxfoundation.org
- Regulation: AI SBOM
  - Contact: Adrian Gonzalez Sanchez adrian.gonzalez-sanchez@hec.ca ; adriango@microsoft.com
- Technical: Foundation Models and LLM Evaluation
  - Contact: Suparna Bhattacharya, suparna.bhattacharya@hpe.com

Collaboration with Generative AI Committee likely in late 2023 and 2024

Backup

Podcast →
AI Horizons: Visions of Tomorrow

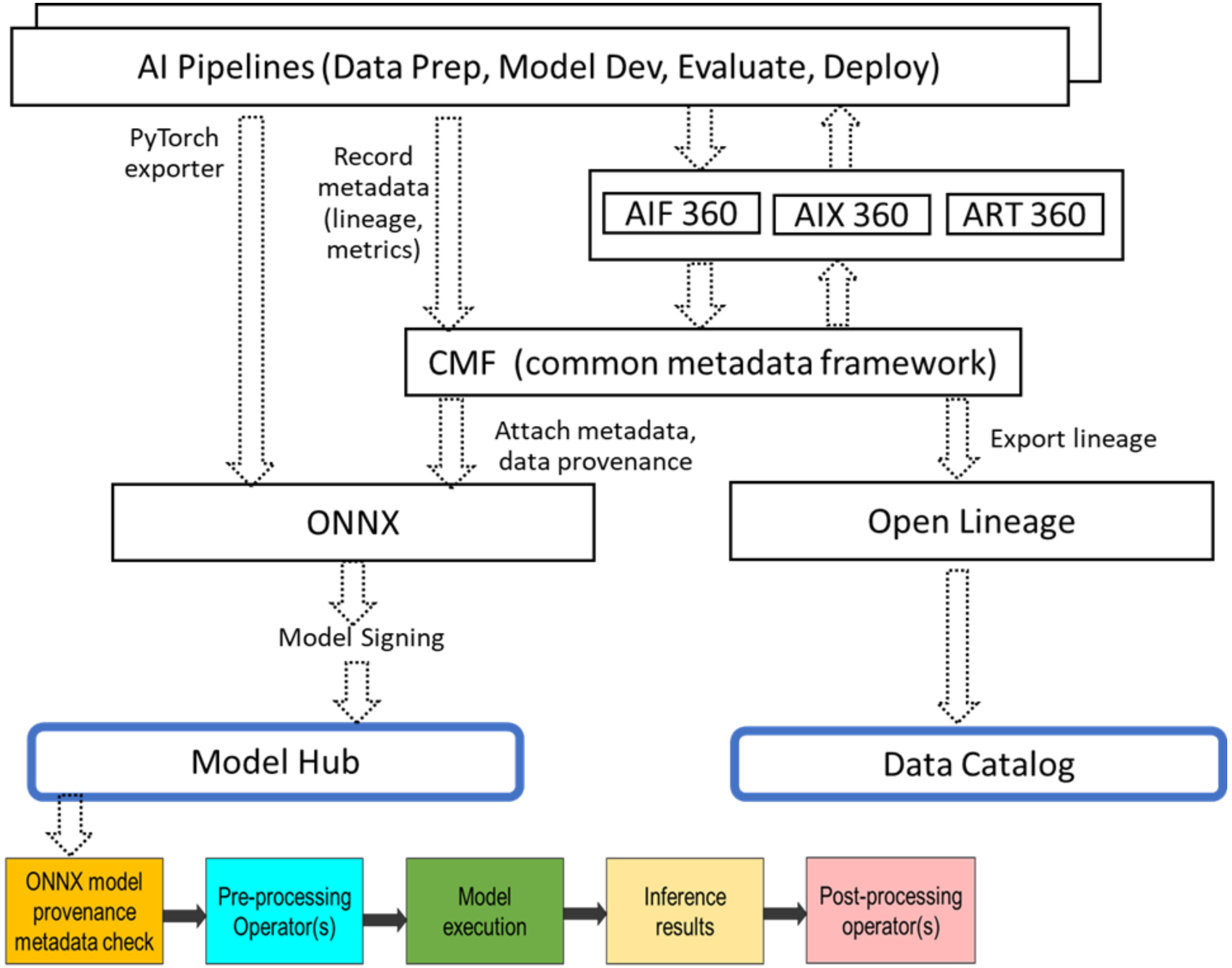
- Content Strategy
  - Release Cadence
    - Bi-weekly starting late Sep/early Oct
  - Calendar
    - Launch 1st Season 1 episode Q4 (Late Sep/Early Oct)
    - 6 episodes in initial phase, wrap by EOY
  - Promotion Strategy
    - LF AI & Data level - Social media, email
    - Linux Foundation level - Monthly newsletter
    - Derived Content - Summary articles linking to podcasts, Insights report using surveys & contributions.

Podcast →
AI Horizons: Visions of Tomorrow

- Success Metrics
  - General analytics (Spotify, social, YouTube)
  - LF awareness impact

- Format and Structure
  - Solo, co-hosted, interview, panels
  - Video podcast format
  - Episode duration: 20-40 mins

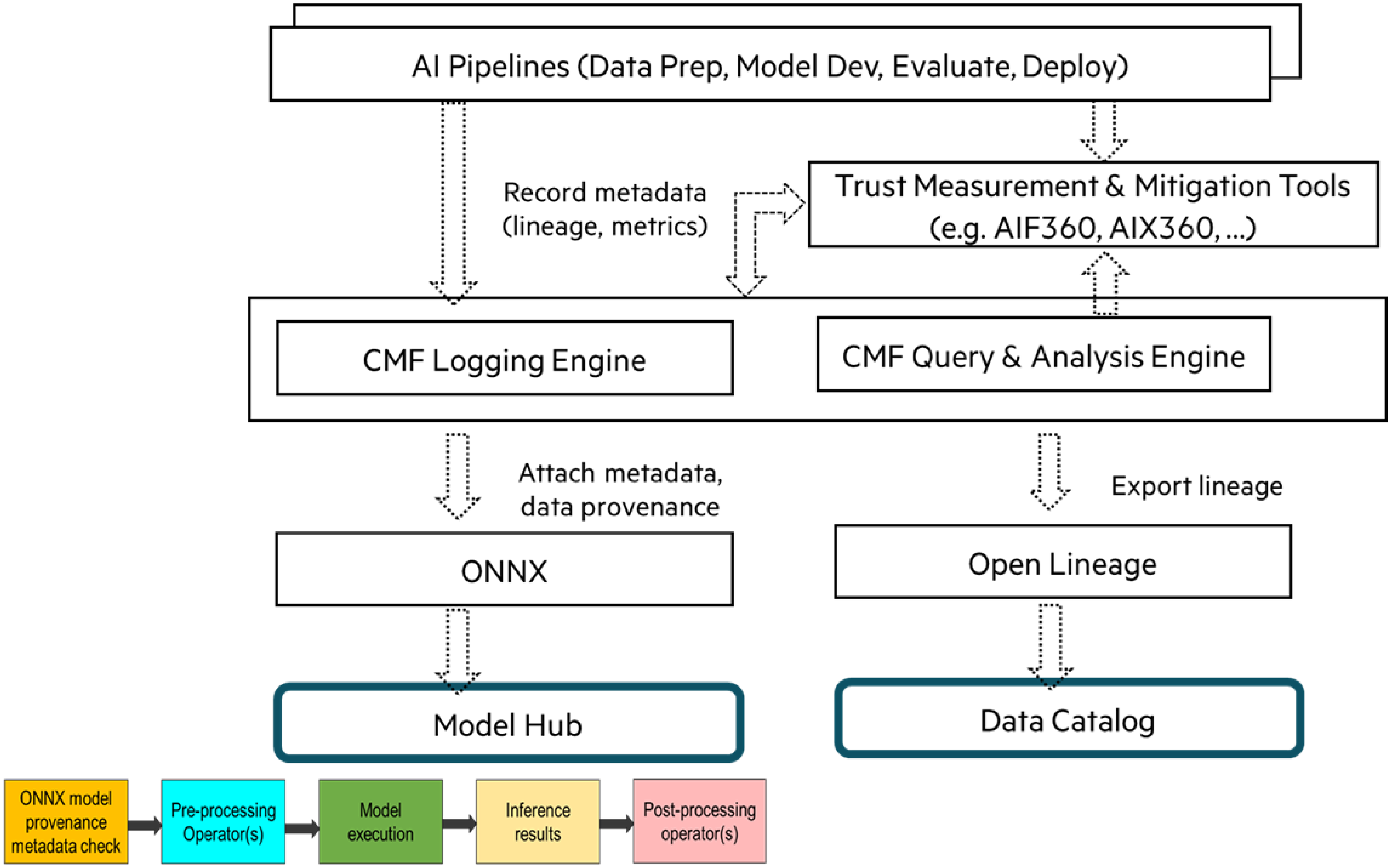
Activity in 2023: Connecting Trusted AI related Projects


AI Pipelines (Data Prep, Model Dev, Evaluate, Deploy)
PyTorch exporter
Record metadata (lineage, metrics)
AIF 360
AIX 360
ART 360
CMF (common metadata framework)
Attach metadata, data provenance
Export lineage
ONNX
Open Lineage
Model Signing
Model Hub
Data Catalog
ONNX model provenance metadata check
Pre-processing Operator(s)
Model execution
Inference results
Post-processing operator(s)

Trusted AI Projects - Mitigation Techniques - Lineage - Metadata (Old version)

Add Model Signing

PyTorch Exporter work underway to add more metadata


AI Pipelines (Data Prep, Model Dev, Evaluate, Deploy)
Record metadata (lineage, metrics)
Trust Measurement & Mitigation Tools (e.g. AIF360, AIX360, ...)
CMF Logging Engine
CMF Query & Analysis Engine
Attach metadata, data provenance
Export lineage
ONNX
Open Lineage
Model Hub
Data Catalog
ONNX model provenance metadata check
Pre-processing Operator(s)
Model execution
Inference results
Post-processing operator(s)

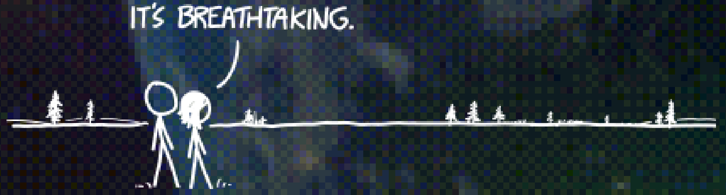
a@ethical.institute

LF AI & Data

ML Security Committee

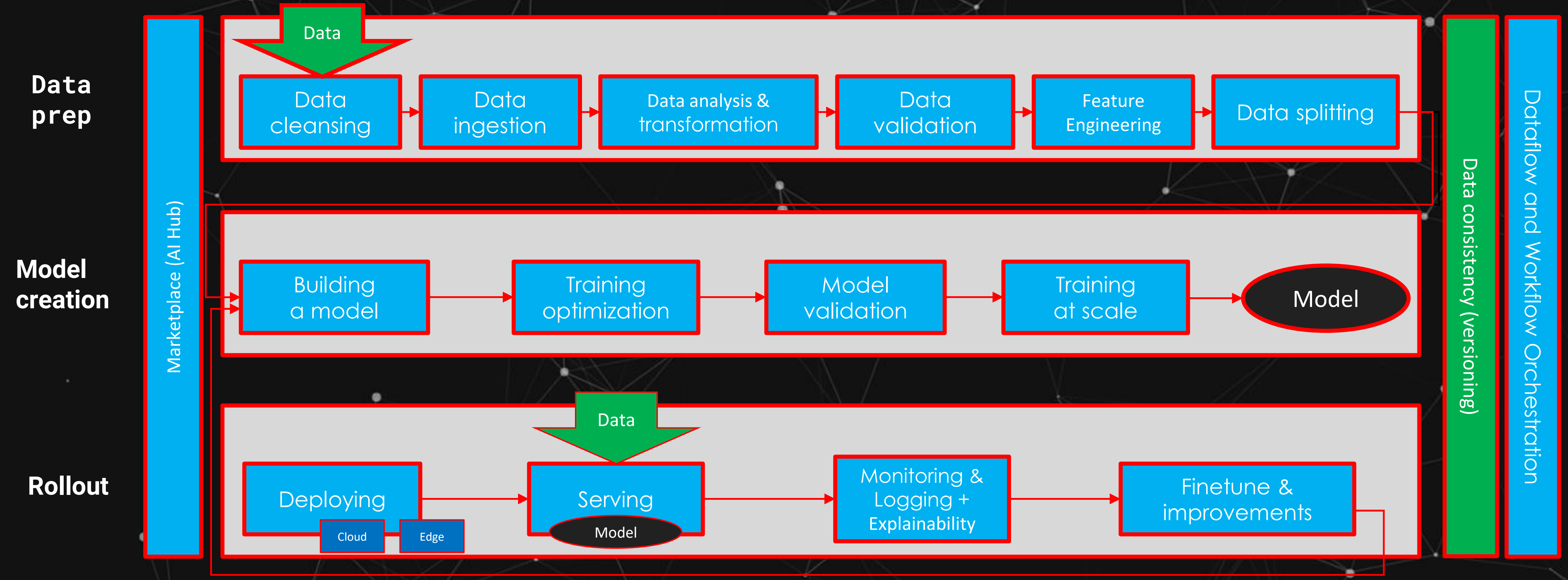
https://wiki.lfaidata.foundation/display/DL/ML+Security+Committee

TAC - August 2023



ML Security Committee

WG defining security best practices for the e2e ML lifecycle.

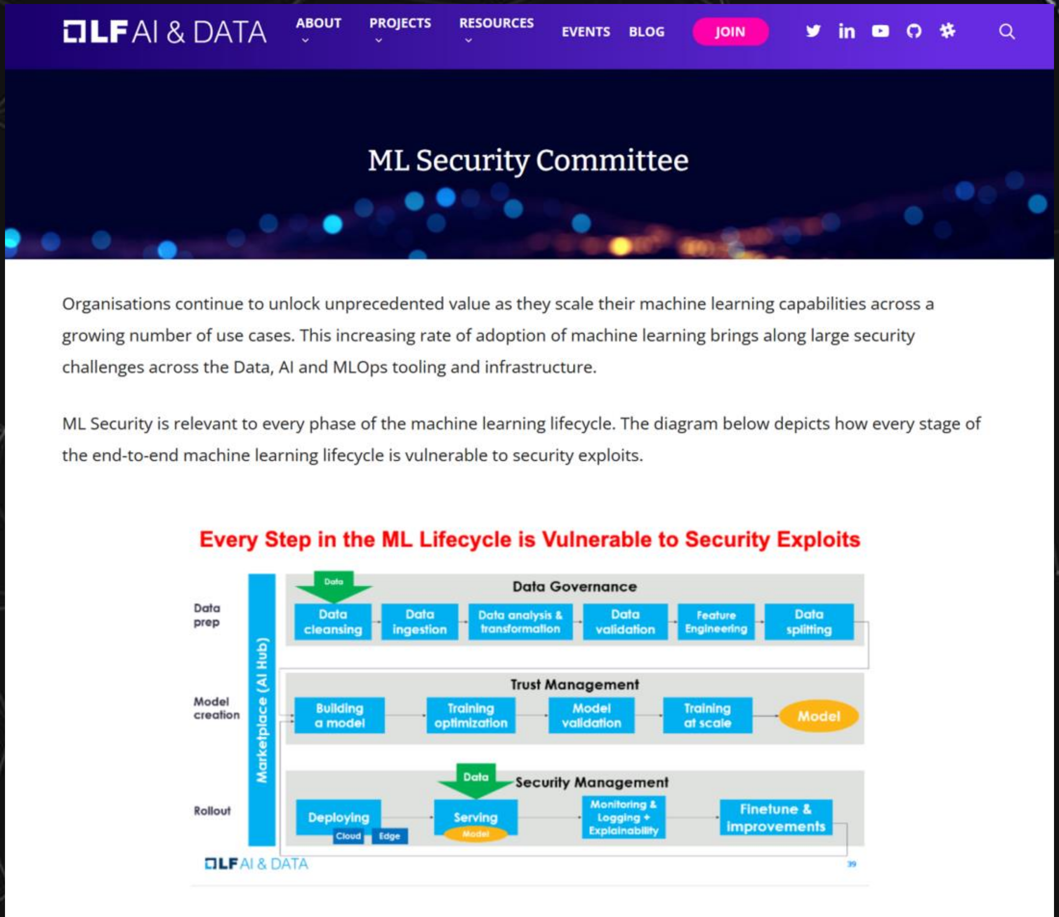


Monthly ML Security Committee Meeting

https://lfaidata.foundation/projects/ml-security-committee/

Key Priorities

- Publish Resources
- Drive ML Security Standards
- Best Practices and Examples of Secure ML



ML Security Committee

Organisations continue to unlock unprecedented value as they scale their machine learning capabilities across a growing number of use cases. This increasing rate of adoption of machine learning brings along large security challenges across the Data, AI and MLOps tooling and infrastructure.

ML Security is relevant to every phase of the machine learning lifecycle. The diagram below depicts how every stage of the end-to-end machine learning lifecycle is vulnerable to security exploits.

Every Step in the ML Lifecycle is Vulnerable to Security Exploits

a@ethical.institute

ML Security Founding Members

IBM

vmware®

MITRE

Hugging Face

SELDON

TROJ.AI

MITHRIL SECURITY

ETHICAL ML INSTITUTE

ROBUST INTELLIGENCE

Achievements & Contributions

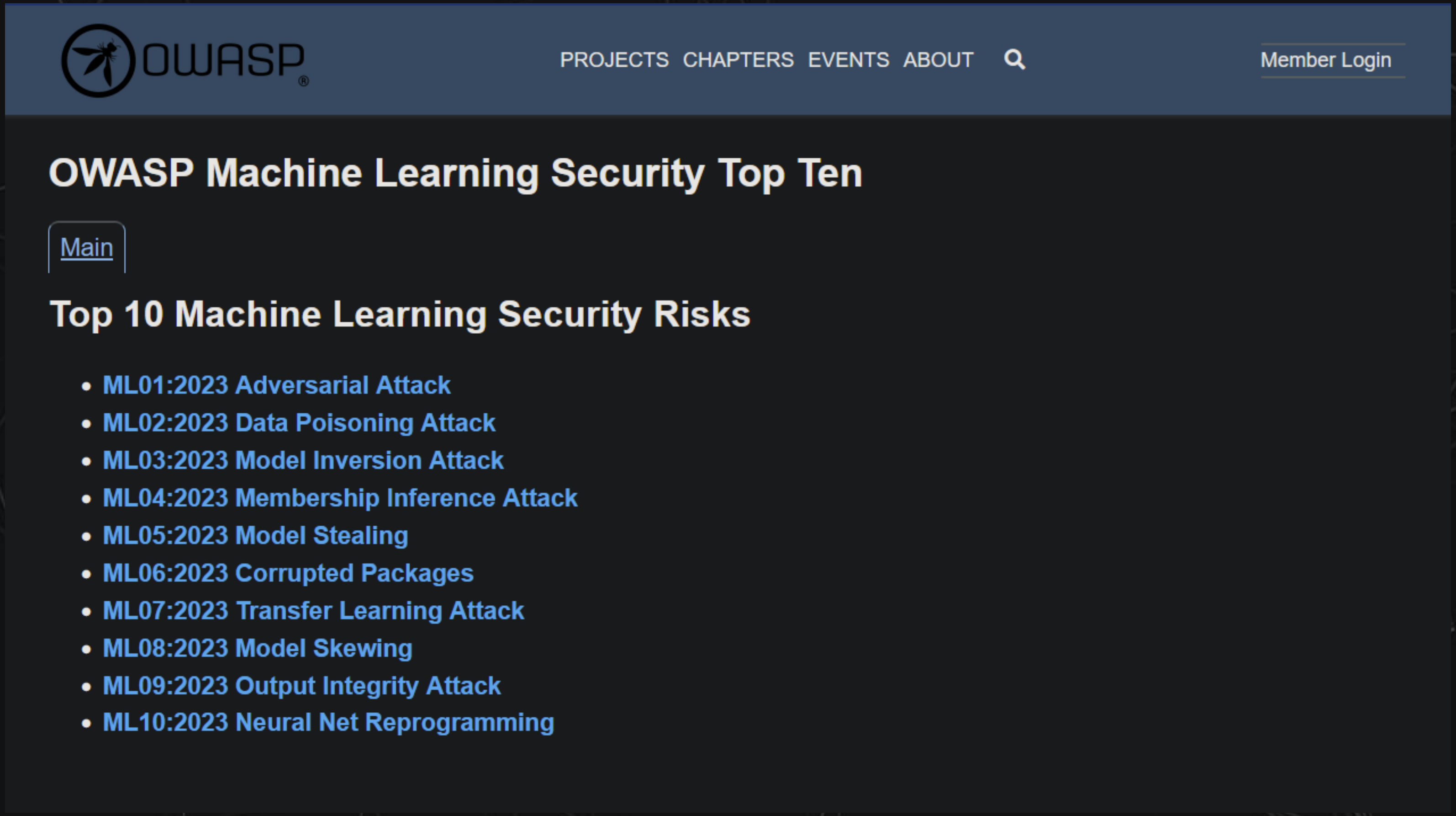
MLSecOps Top 10 - Released 2021 🚀

a@ethical.institute

#	OWASP Standard	MLSecOps Equivalent
1	Broken Access Control	Unrestricted Model Endpoints
2	Cryptographic failures	Access to Model Artifacts
3	Injection	Artifact Exploit Injection
4	Insecure Design	Insecure ML Systems/Pipeline Design
5	Security Misconfigurations	Data & Infra Misconfigurations
6	Vulnerable & Outdated Components	Supply Chain Vulnerabilities in ML Code
7	Identification and Auth Failures	IAM & RBAC Failures for ML Services
8	Software and Data Integrity Failures	ML Infra / ETL / CI / CD Integrity Failures
9	Security Logging and Monitoring Failures	Observability, Reproducibility & Lineage
10	Server-Side Request Forgery	ML-Server Side Request Forgery

https://ethical.institute/security.html

Contributions to MLSecOps Ecosystem



OWASP Machine Learning Security Top Ten

Top 10 Machine Learning Security Risks

- ML01:2023 Adversarial Attack
- ML02:2023 Data Poisoning Attack
- ML03:2023 Model Inversion Attack
- ML04:2023 Membership Inference Attack
- ML05:2023 Model Stealing
- ML06:2023 Corrupted Packages
- ML07:2023 Transfer Learning Attack
- ML08:2023 Model Skewing
- ML09:2023 Output Integrity Attack
- ML10:2023 Neural Net Reprogramming

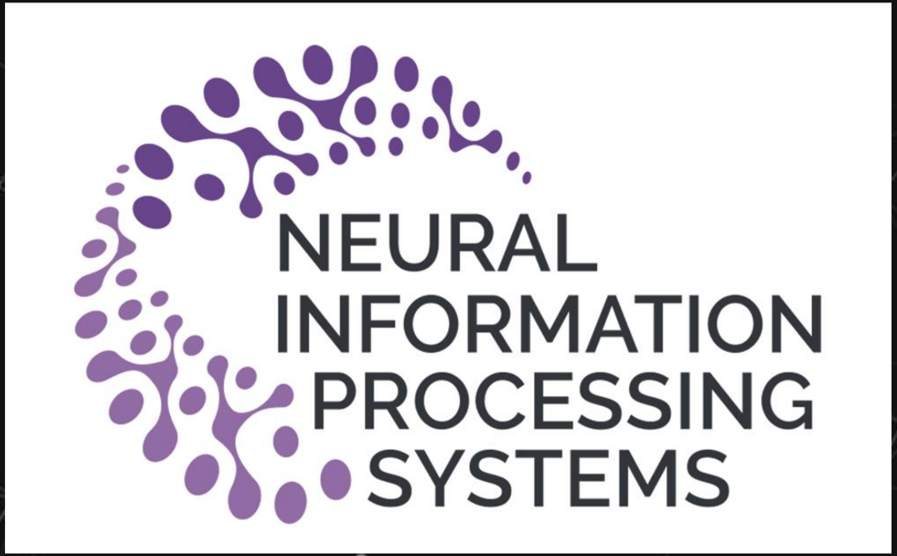
OWASP MLSec Top 10

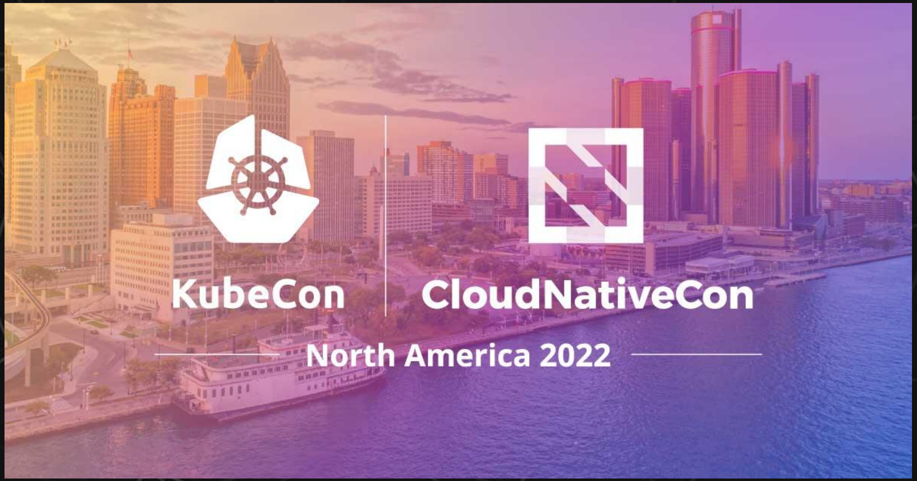
https://owasp.org/Top10/

Events & Keynotes

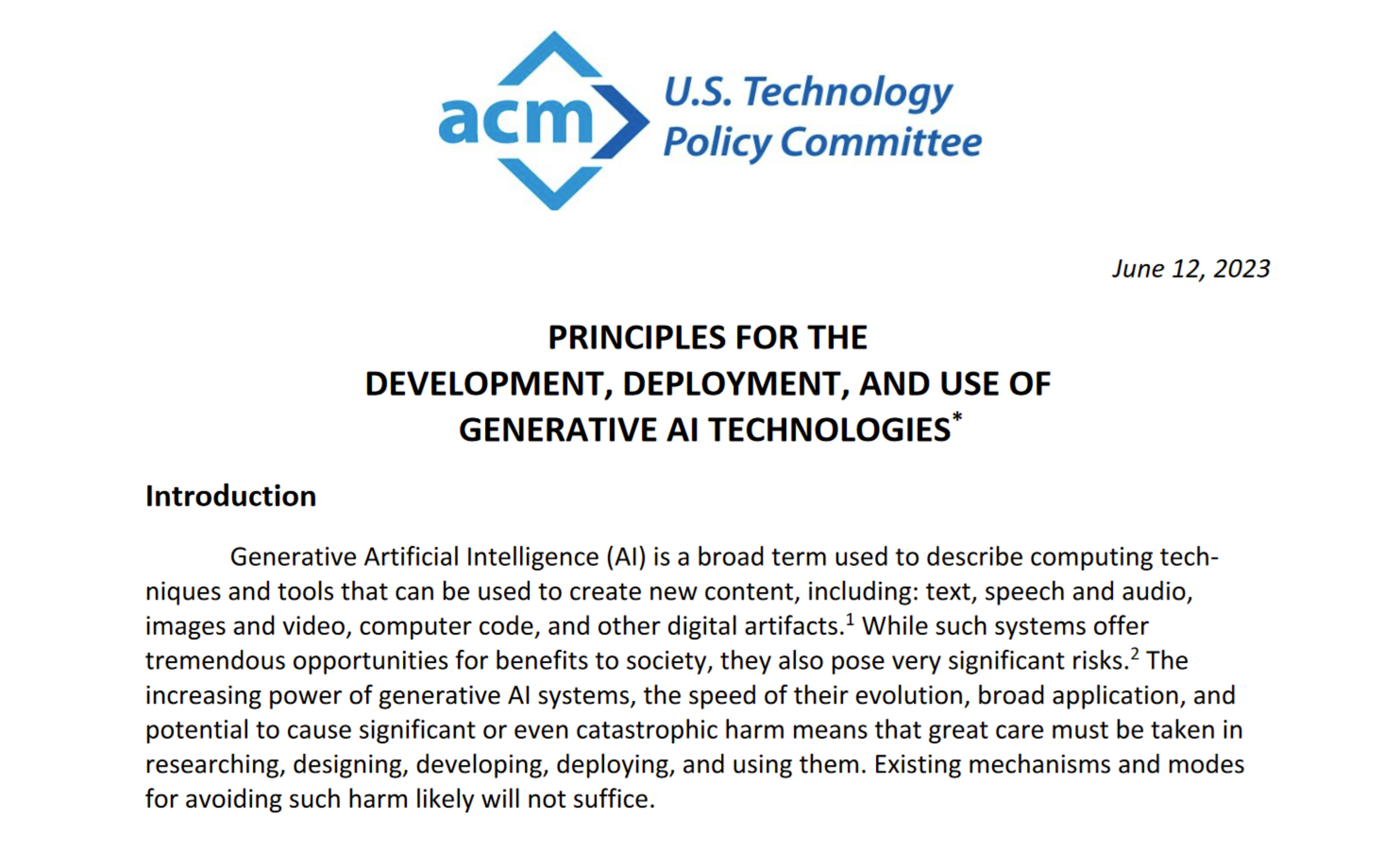
Conferences:

- **NeurIPS 2022**
  - https://www.youtube.com/watch?v=7XSy5aw8oU8
- **Kubecon North America**
  - https://www.youtube.com/watch?v=XaA6DvkhPlM
- **Open Source Summit**





Contributions on Policy & Governance



acm U.S. Technology Policy Committee

June 12, 2023

PRINCIPLES FOR THE DEVELOPMENT, DEPLOYMENT, AND USE OF GENERATIVE AI TECHNOLOGIES[*]

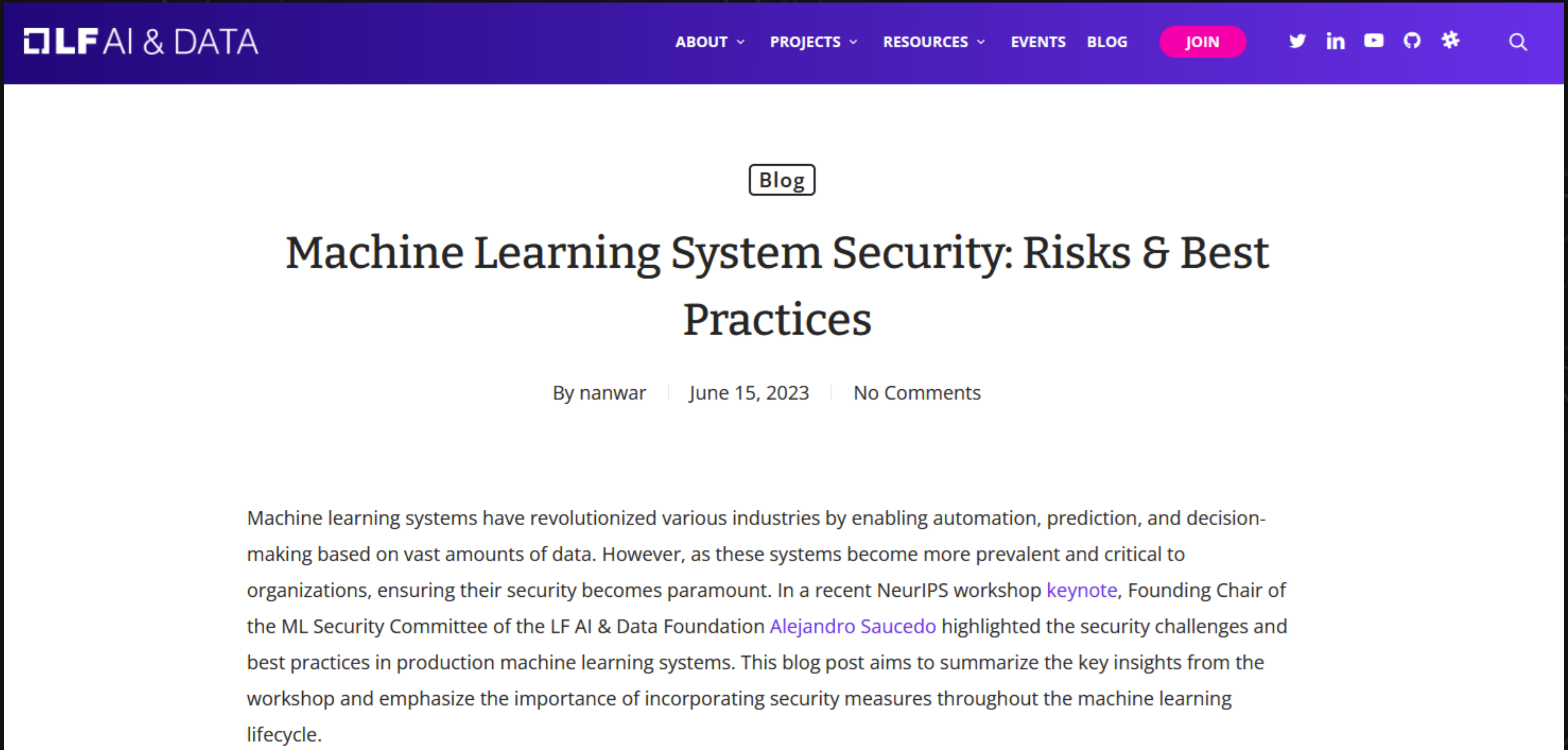
Introduction

Generative Artificial Intelligence (AI) is a broad term used to describe computing techniques and tools that can be used to create new content, including: text, speech and audio, images and video, computer code, and other digital artifacts.[1] While such systems offer tremendous opportunities for benefits to society, they also pose very significant risks.[2] The increasing power of generative AI systems, the speed of their evolution, broad application, and potential to cause significant or even catastrophic harm means that great care must be taken in researching, designing, developing, deploying, and using them. Existing mechanisms and modes for avoiding such harm likely will not suffice.

Principles for Generative AI

https://www.acm.org/binaries/content/assets/public-policy/ustpc-approved-generative-ai-principles

Updates on MLSecOps Ecosystem Blog Posts



Blog

Machine Learning System Security: Risks & Best Practices

By nanwar | June 15, 2023 | No Comments

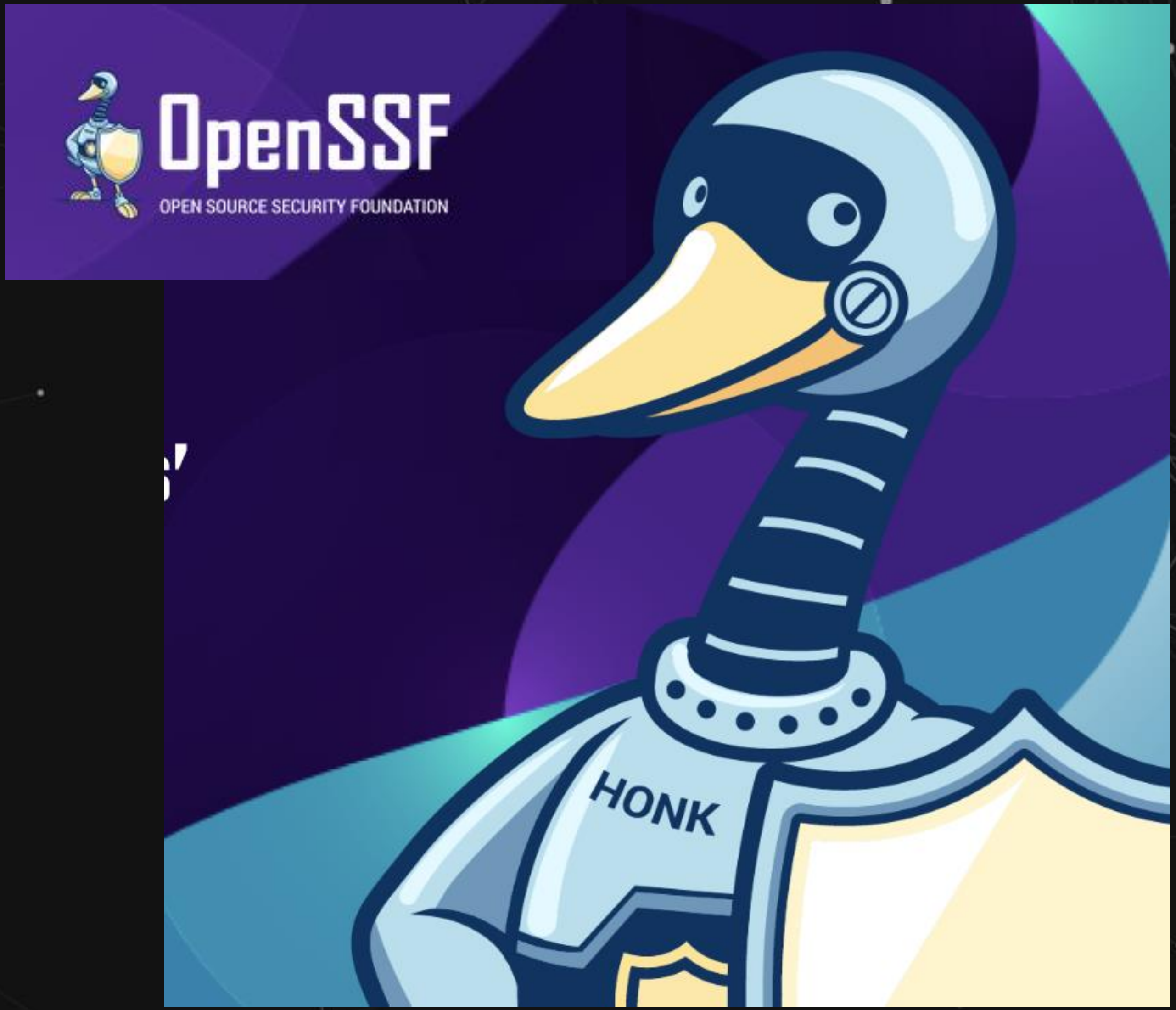
Machine learning systems have revolutionized various industries by enabling automation, prediction, and decision-making based on vast amounts of data. However, as these systems become more prevalent and critical to organizations, ensuring their security becomes paramount. In a recent NeurIPS workshop keynote, Founding Chair of the ML Security Committee of the LF AI & Data Foundation Alejandro Saucedo highlighted the security challenges and best practices in production machine learning systems. This blog post aims to summarize the key insights from the workshop and emphasize the importance of incorporating security measures throughout the machine learning lifecycle.

Latest ML Security Blog Post

https://lfaidata.foundation/blog/2023/06/15/machine-learning-system-security-risks-best-practices/

OpenSSF Collaboration

Motivation: The OpenSSF and ML Security

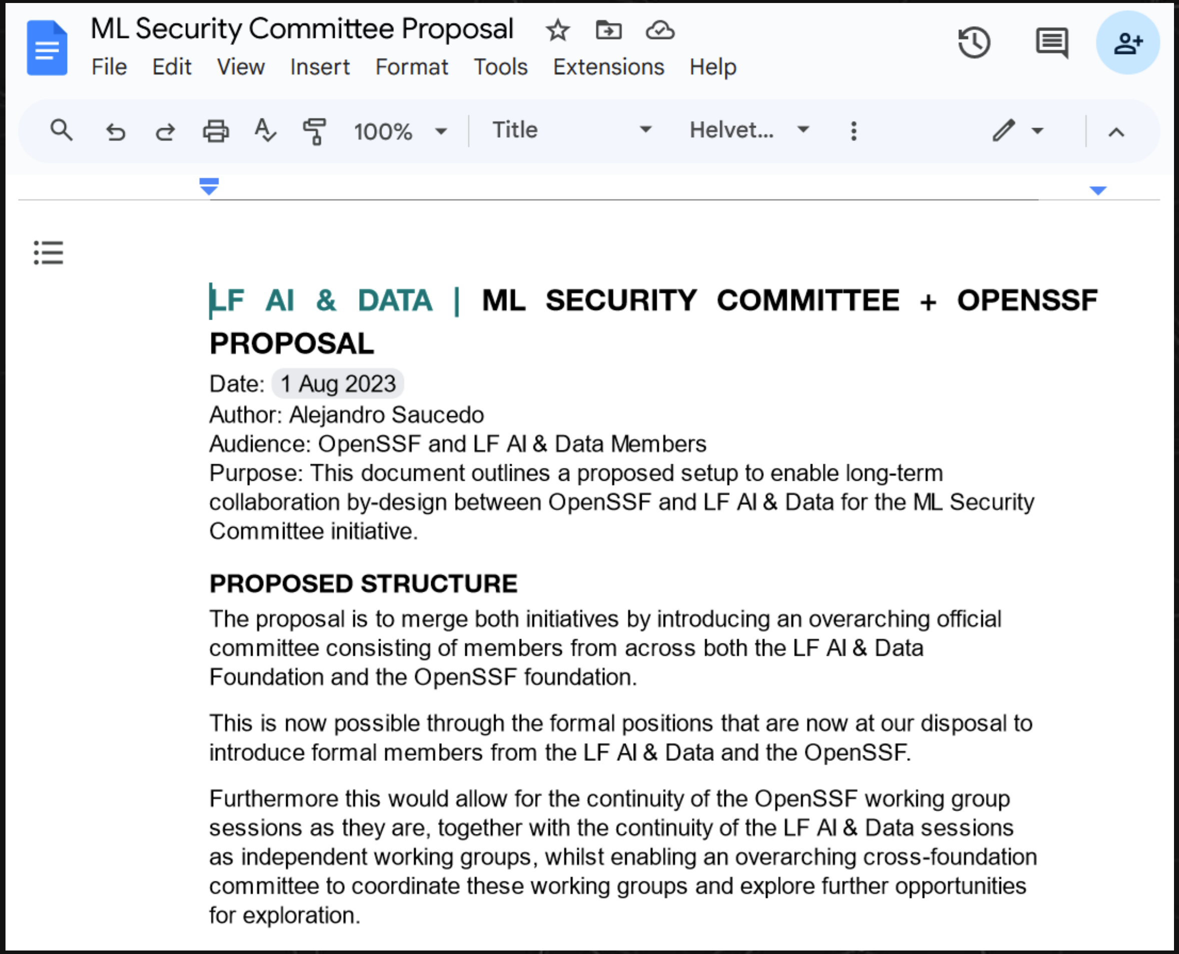


Open Software Security Foundation

- “committed to collaboration and working [with] communities to advance open source security for all.”
- ML Momentum in OpenSSF

OpenSSF + LF AI & Data Collaboration Overview

a@ethical.institute


ML Security Committee Proposal
File Edit View Insert Format Tools Extensions Help
100%
Title
Helvet...

LF AI & DATA | ML SECURITY COMMITTEE + OPENSSF PROPOSAL

Date: 1 Aug 2023
Author: Alejandro Saucedo
Audience: OpenSSF and LF AI & Data Members
Purpose: This document outlines a proposed setup to enable long-term collaboration by-design between OpenSSF and LF AI & Data for the ML Security Committee initiative.

PROPOSED STRUCTURE

The proposal is to merge both initiatives by introducing an overarching official committee consisting of members from across both the LF AI & Data Foundation and the OpenSSF foundation.

This is now possible through the formal positions that are now at our disposal to introduce formal members from the LF AI & Data and the OpenSSF.

Furthermore this would allow for the continuity of the OpenSSF working group sessions as they are, together with the continuity of the LF AI & Data sessions as independent working groups, whilst enabling an overarching cross-foundation committee to coordinate these working groups and explore further opportunities for exploration.

https://docs.google.com/document/d/1eMp5jksdNxWDtg_aQ2yoc6jYUAczhx_KPPuDrCiS8lQ/edit

Collaboration by design

- Integrating both initiatives
- Continuity on efforts
- Formal representation

OpenSSF + LF AI & Data Collaboration Overview

a@ethical.institute

Formalising OpenSSF Reps

- 3 OpenSSF Rep Positions
    - Thanks to the LF AI Leadership!
- Jay White, Microsoft
- Christine Abernathy, F5
- Sal Kimmich, Sonatype

+ Further participation from OpenSSF members!

Business as usual with more of what works!

- Encouraging cross-participation across foundations
  - Adding sessions to the calendars across both
- Continuation of existing cadences
  - + introduction to other existing committees
- Defined opportunities for contribution
  - Domain Experts for Project incubation
  - Co-publish thought leadership resources

Broader Foundation Collab

Encouraging broader cross-foundation collab!

We are keen to explore further collaborations

- Introduce members from LF AI & Data to other areas
  - Collaboration through ML Security domain
  - Opportunities to get involved through the security topic
- Invite members from other foundations to contribute to LF AI
  - Learn about the multiple SIGs, Committees and Working Groups
  - Get involved with active projects, initiatives or working sessions

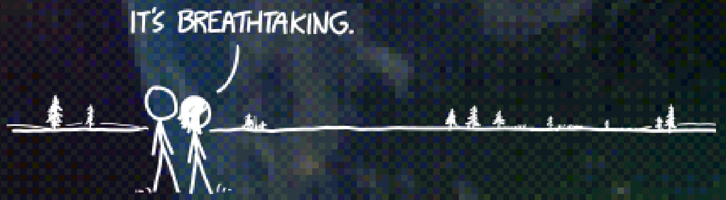
a@ethical.institute

LF AI & Data

ML Security Committee

https://wiki.lfaidata.foundation/display/DL/ML+Security+Committee

TAC - August 2023



Upcoming TAC Meetings

LF AI & DATA

Upcoming TAC Meetings

- September 21 – Marquez graduation request; AIDA, a new project requesting Sandbox Incubation
- LMSYS project review, Open slot

Please note we are always open to special topics as well.

If you have a topic idea or agenda item, please send agenda topic requests to tac-general@lists.lfaidata.foundation

Upcoming Events of Interest

- 2023 AICON Middle East Summit - October 8th to 9th in Riyadh https://lfaidata.foundation/blog/2023/07/18/2023-aicon-middle-east-summit-call-for-topics-from-around-the-world/
- Open Source Summit Europe in Bilbao, Spain, September 19-21 – LF AI&Data will have a booth https://events.linuxfoundation.org/open-source-summit-europe/

Open Discussion

LF AI & DATA

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

24AUG2023