

ML Security Committee

Overview

You can find the official ML Security Committee site in the LF AI & Data website at <https://lfaidata.foundation/projects/ml-security-committee/>

Attending Meetings

The current meetings take place monthly. The meetings take place on the second Thursday of the month.

Please contact Alejandro Saucedo a@ethical.institute if you would like to join the meetings and contribute to the LF AI ML Security Committee.

You can also join the slack: LF AI & Data Foundation - [#lfaifoundation.slack.com](https://lfaifoundation.slack.com) - #ml-security channel if you would like to engage in discussion about machine learning security.

You can find the mailing lists and monthly meetings at <https://lists.lfaidata.foundation/g/mlsecurity-committee>

Committee Members

For any required communication please contact the chairperson members:

- [Alejandro Saucedo](#) (ML Security Committee Chair) - Chief Scientist, The Institute for Ethical AI [a@ethical.institute]

Committee members from [LF AI & Data Foundation member organisations](#):

First Name	Last Name	Company	Position	Email Address
Beat	Buesser	IBM Research	Research Staff Member	beat.buesser@ie.ibm.com
Matthieu	Maitre	Microsoft	Principal Software Developer	mmaitre@microsoft.com
Aankur	Bhatia	IBM	Chief Data Scientist, IBM Security	abhatia@us.ibm.com
Anna	Jung	VMware	Engineer	antheaj@vmware.com
Teodora	Sechkova	VMware	Open Source Software Engineer	tsechkova@vmware.com
Diana	Atanasova	VMware	Open Source Software Engineer	dianaa@vmware.com
Saurabh	Tangri	Intel Corporation	Principal Engineer	tangri@berkeley.edu

OpenSSF Committee Members as per [LF AI & Data Cross-Foundation Collaboration structure](#):

First Name	Last Name	Company	Position	Email Address
Jay	White	Microsoft	Senior Principal	jaywhite@microsoft.com
Christine	Abernathy	F5	Senior Director Open Source	c.abernathy@f5.com
Sal	Kimmich	EscherCloud	Director	

LF AI & Data Committee Participants (updated based on 6-month activity):

First Name	Last Name	Company	Position	Email Address
Karen	Bennet	Quality Craft	VP	bennetkl@yahoo.com
Hyrum	Anderson	Robust Intelligence	Distinguished Engineer	hyrum@robustintelligence.com
Jacob	Bond	General Motors	Senior Researcher	jacob.bond@gm.com
James	Stewart	TrojAI Inc.	CEO	james.stewart@troj.ai
Arun	Prabhakar	Boston Consulting Group	Security Architect	arun.p1405@gmail.com
Phil	Munz	TrojAI	Director of Data Science	phil.munz@troj.ai
Jim	St.Clair	Interoperability Institute	Advisor	jim.stclair@interoperabilityinstitute.org
Kara	de la Marck	Linux Foundation / Continuous Delivery Foundation	Senior Ecosystem Advocate	kdelamarck@linuxfoundation.org

Hasan	Yasar	Software Engineering Institute Carnegie Mellon University	Technical Director, Teaching Professor	hyasar@cmu.edu
-------	-------	---	--	--

Meetings Overview

Date	Agenda
September, 2022	• Introduction to Committee group goals • Outline initial milestones • Brainstorming and discussion
October, 2022	• Update on workign group milestones • Presentation by ◦ Arun Prabhakar - Senior Security Architect, Boston Consulting Group Recording link
November, 2022	• Update on workign group milestones • Presentation by ◦ Mitre ATLAS team ◦ Daniel Huynh - CEO, Mithril Security Recording link
December, 2022	• Intros from new members • Overview and Updates on Initiative ◦ LF AI & Data Website ◦ ML Security rename ◦ ML Security Groups.io Mailing List • Presentation from Adrin Jalali, Sklearn Core Developer & HuggingFace MLE (10-20 mins) • AOB
February, 2023	• Intros from new members • Overview and Updates on Initiative • Presentation from Adrian Gonzalez-Martin, Seldon Technologies • AOB
March, 2023	N/A
April, 2023	• Intros from new members • Overview and Updates on Initiative • Updat of ML Security Ecosystem • AOB
May, 2023	• Intros from new members • Overview and Updates on Initiative • Ibrahim Haddad, Executive Director at Linux Foundation - Ecosystem Overview • AOB
June, 2023	• Intros from new members • Overview and Updates on Initiative • Ibrahim Haddad, Executive Director at Linux Foundation - Ecosystem Overview • AOB

July, 2023	• Intros from new members • Overview and Updates on Initiative • Arun Prabhakar, Senior Manager at BCG • AOB
August, 2023	• Intros from new members • Overview and Updates on Initiative • OpenSSF Collaboration • AOB
September, 2023	• Intros from new members • Overview and Updates on Initiative • TBC • AOB
October, 2023	• Intros from new members • Overview and Updates on Initiative • TBC • AOB