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 - #ml-security channel if you would like to engage in discussion about machine learning security.

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]

Below are a list of core committee members - all affiliations listed for identification purposes only:

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
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
Anna	Jung	VMware	Engineer	antheaj@vmware.com
Teodora	Sechkova	VMware	Open Source Software Engineer	tsechkova@vmware.com
Phil	Munz	TrojAI	Director of Data Science	phil.munz@troj.ai
Jim	St.Clair	Linux Foundation Public Health	ED	Jstclair@linuxfoundation.org
Kara	de la Marck	Linux Foundation / Continuous Delivery Foundation	Senior Ecosystem Advocate	kdelamarck@linuxfoundation.org
Diana	Atanasova	VMWare	Open Source Software Engineer	dianaa@vmware.com

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

January, 2023	• Intros from new members • Overview and Updates on Initiative • Presentation from Adrian Gonzalez-Martin, Seldon Technologies • AOB
February, 2023	• Intros from new members • Overview and Updates on Initiative • Luc Georges - ML & Software Engineer, HuggingFace • AOB