

LÉO BOISVERT

514-971-8555 > leo.boisvert@hotmail.ca

Montreal, Canada

github: [jardinetsouffleto](https://github.com/jardinetsouffleto) > website: leo-boisvert.com

PRESENTATION

I bridge the gap between cutting-edge AI research and public understanding through a focus on technical innovation and science communication. While advancing the development of secure and robust LLM-based web agents that can safely interact with web interfaces (WorkArena++, DoomArena), I share complex scientific concepts with broader audiences through radio columns and educational talks. This allows me to not only contribute to the technical advancement of AI systems but also foster informed public discourse on their ethical implementation and societal impact.

EDUCATION

Polytechnique Montréal + MILA

2024 -

PhD in Computer Engineering

Polytechnique Montréal

2022 - 2024

M.Sc. in Computer Engineering

Université de Montréal

2016 - 2020

B.Sc. in Mathematics

EXPERIENCE

Fonds de recherche du Québec

Oct 2025 -

Member of the student intersectorial committee

- Advise the Chief Scientist of Quebec and the Quebec Research Funds board of directors on issues related to the next generation of researchers.

Radio-Canada

July 2025 -

Columnist - Moteur de Recherche

- Guest columns on the topic of AI on National public radio

Independent Consulting

January 2025 -

Self-employed

- Secured \$400,000 in R&D funding from the Quebec Ministry of Culture and Communications for L'actualité magazine by designing an integrated AI platform for editorial automation and predictive analytics.
- Built, deployed and maintained custom optimization app for various clients, including a scheduling software used by the Canadian Olympic Committee and Hockey Canada.

ServiceNow Research

March 2024 -

Visiting Researcher

- Studied and managed to break several state-of-the-art agents, highlighting security flaws
- Led development of WorkArena++, focusing on large-scale AI systems and LLM-based web agents
- Designed representative tasks for knowledge workers on web platforms

Newtrax Technologies

Jan 2021 - Jun 2022

Team Lead, Data Science

- Led data science product lifecycle from idea to production
- Established system-level reliability tests achieving 99.99% prediction accuracy
- Grew team's product line from 2 to 10 products
- Set up company's first system-level reliability tests

Newtrax Technologies

Sept 2019 - Jan 2021

Data Scientist

- Developed first activity detection products with 99% prediction accuracy
- Managed end-to-end product development including DevOps aspects
- Established coding standards and test practices for growing team

PUBLICATIONS

JOURNAL ARTICLES

The BrowserGym Ecosystem for Web Agent Research

TMLR, March 2025

Thibault Le Sellier de Chezelles, Maxime Gasse, Alexandre Lacoste, Massimo Caccia, Alexandre Drouin, **Léo Boisvert**, Megh Thakkar, Tom Marty, Rim Assouel, Sahar Omid Shayegan, Lawrence Keunho Jang, Xing Han Lù, Ori Yoran, Dehan Kong, Frank F. Xu, Siva Reddy, Graham Neubig, Quentin Cappart, Russ Salakhutdinov, Nicolas Chapados

Learning and fine-tuning a generic value-selection heuristic inside a constraint programming solver

Constraints 2024

Tom Marty*, **Léo Boisvert***, Tristan François, Pierre Tessier, Louis Gautier, Louis-Martin Rousseau, Quentin Cappart

CONFERENCE PAPERS

Malice in Agentland: Down the Rabbit Hole of Backdoors in the AI Supply Chain

ACM CAIS 2026 - 🏆 *Best Paper Award*

Léo Boisvert, Abhay Puri, Chandra Kiran Reddy Evuru, Nicolas Chapados, Quentin Cappart, Nazanin Sepahvand, Alexandre Lacoste, Krishnamurthy Dj Dvijotham, Alexandre Drouin

DoomArena: A framework for Testing AI Agents Against Evolving Security Threats

COLM 2025

Leo Boisvert, Chandrakiran Reddy Evuru, Abhay Puri, Mihir Bansal, Gabriel Huang, Alexandre Drouin, Alexandre Lacoste, Avinandan Bose, Krishnamurthy Dvijotham

WorkArena++: Towards Compositional Planning and Reasoning-based Common Knowledge Work Tasks

NeurIPS 2024

Léo Boisvert, Megh Thakkar, Maxime Gasse, Massimo Caccia, Thibault Le Sellier De Chezelles, Quentin Cappart, Nicolas Chapados, Alexandre Lacoste, Alexandre Drouin

Towards a Generic Representation of Combinatorial Problems for Learning-Based Approaches

CPAIOR 2024

Léo Boisvert, Hélène Verhaeghe, Quentin Cappart

REFEREED WORKSHOP PAPERS

FocusAgent: Simple Yet Effective Ways of Trimming the Large Context of Web Agents

ICLR Lifelong Learning Agents 2026

Imene Kerboua, Sahar Omid Shayegan, Xing Han Lù, **Léo Boisvert**, Megh Thakkar, Massimo Caccia, Jérémy Espinas, Alex Aussem, Véronique Eglin, Alexandre Lacoste

DoomArena: A framework for Testing AI Agents Against Evolving Security Threats

ICML Computer Use Agent Workshop 2025

Leo Boisvert, Chandrakiran Reddy Evuru, Abhay Puri, Mihir Bansal, Gabriel Huang, Alexandre Drouin, Alexandre Lacoste, Avinandan Bose, Krishnamurthy Dvijotham

Silent Sabotage: Injecting Backdoors into AI Agents Through Fine-Tuning

ICML Computer Use Agent Workshop 2025

Leo Boisvert, Abhay Puri, Chandra Kiran Reddy Evuru, Joshua Kazdan, Avinandan Bose, Quentin Cappart, Maryam Fazel, Sai Rajeswar, Jason Stanley, Nicolas Chapados, Alexandre Drouin, Krishnamurthy Dvijotham

AgentMerge: Enhancing Generalization in Fine-Tuned LLM Agents

NeurIPS Workshop on Adaptive Foundation Models 2024

Megh Thakkar, **Léo Boisvert**, Thibault Le Sellier De Chezelles, Alexandre Piché, Maxime Gasse, Alexandre Lacoste, Massimo Caccia

Fine-Tuning Web Agents: It Works, But It's Trickier Than You Think

NeurIPS Workshop on Open-World Agents 2024

Massimo Caccia, Megh Thakkar, **Léo Boisvert**, Thibault Le Sellier De Chezelles, Alexandre Piché, Nicolas Chapados, Alexandre Drouin, Maxime Gasse, Alexandre Lacoste

WorkArena: How Capable are Web Agents at Solving Common Knowledge Work Tasks?

ICLR Workshop on LLM Agents 2024

Alexandre Drouin, Maxime Gasse, Massimo Caccia, Issam H. Laradji, Manuel Del Verme, Tom Marty, **Léo Boisvert**, Megh Thakkar, Quentin Cappart, David Vazquez, Nicolas Chapados, Alexandre Lacoste

MEDIA

L'IA n'est plus un simple générateur de texte

University Affairs

Article explaining recent progress in the use of AI for science

BLOG POSTS

Malice in AgentLand

ServiceNow AI Research blog post

Leo Boisvert, Abhay Puri, Alexandre Drouin

OFFICIAL REPORTS

AI in education report

Report and recommendations on AI use for students. Presented to the Quebec Chief Scientist

TALKS

WORKSHOP ORGANIZATION

CSPC 2026 - Organizer of panel on the future of training and skills in the AI era. *November 2026*
Ottawa, Canada

CONFERENCE PRESENTATIONS

Digital Research Alliance of Canada - AI Agent security testing *October 2025*
[Talk available here](#)

J2R 2025 - Findings of the FRQ student consultations on AI *October 2025*
Rimouski, Canada

JFPC 2025 - Learning and Fine-tuning Value-selection for Constraint Programming *July 2025*
Lyon, France

SEMLA 2025 - DoomArena framework for AI agent security *June 2025*
Montréal, Canada

JOPT 2025 - Learning heuristics with Reinforcement Learning *May 2025*
HEC Montréal, Canada

PolyconGRÉ - WorkArena++ (selected as oral) *March 2025*
Internal research conference at Polytechnique Montréal

CPAIOR 2024 - Generic representation of combinatorial problems *May 2024*
Uppsala, Sweden

JOPT 2024 - Generic representation of CP problems *May 2024*
HEC Montréal, Canada

JOPT 2023 - End-to-end learning in CP problems using GNNs *May 2023*
HEC Montréal, Canada

CIM 2022 - Data science for underground mining *May 2022*
Vancouver, Canada

Québec Mines et Énergie 2021 - Production tracking software for UG mining *November 2021*
Québec, Canada

INVITED TALKS

- Georgian AI Lab** *July 2026*
Backdoors in AI Agents
Toronto, Canada
- Town of Racine, Qc** *June 2026*
Training session on AI use, trends and possible futures in the municipal context
Racine, Québec, Canada
- FTQ (Fédération des travailleurs du Québec)** *April 2026*
3h training session on AI use, trends and possible futures for the largest labour central in Quebec
Montréal, Canada
- ServiceNow AI Research Bites** - Malice in AgentLand: Backdoors in agents *December 2025*
[Remote talk](#)
- Jinesis Lab** - Malice in AgentLand; Backdoors in Agents *Nov 2025*
[Remote talk](#)
- ServiceNow AI Research Bites** - The DoomArena Framework for security testing *August 2025*
[Remote talk](#)
- MLCommons Agentic AI meeting** - DoomArena: Securing Agents *July 2025*
[Remote talk](#)
- SOCAN General Assembly of Members** - State and near future of Gen AI *May 2025*
Toronto, Canada - Talk to the general assembly of SOCAN (185,000 members)
- AI Alliance Trust & Safety meeting** - DoomArena: Securing Agents *May 2025*
[Remote talk](#)
- AAAI Web Agent Revolution Workshop** - AI Agents for Enterprise Workflows *March 2025*
Philadelphia, USA
- Association for Constraint Programming** - Learning and fine-tuning a generic value-selection heuristic *March 2025*
[Remote talk](#)
- Capital One** - WorkArena and Web Agents *February 2025*
[Remote talk](#)
- ML4CP Summer School** - Learning optimization heuristics with SeaPearl.jl *July 2023*
Leuven, Belgium

PANEL APPEARANCES

- AI × Professional Services** - Technical and operational challenges of deploying AI in high-stakes environments. *February 2026*
Hosted by Material and Brightspark Ventures at Mila, Montréal, Canada
- AAAI Web Agent Revolution Workshop** - State of the art and future of agents *March 2025*
Philadelphia, USA

SCIENCE POPULARIZATION & MEDIA

- Moteur de Recherche (Radio-Canada)** *June 2026*
[AI and CAPTCHAs](#) - On French-language Canadian public radio
Montreal, Canada
- Moteur en herbe (Radio-Canada)** *April 2026*
[Difference between traditional and AI datacenter](#) - On French-language Canadian public radio
Montreal, Canada
- Moteur de Recherche (Ici Explora)** *March 2026*
[Can LLMs help anyone create cyber-attacks](#) - TV
Montreal, Canada

Moteur en herbe (Radio-Canada) How do letters get from the keyboard to the computer monitor - On French-language Canadian public radio Montreal, Canada	<i>March 2026</i>
Baie d'Urfé Citizens Association AI in 2026: How we got here and where we're headed Baie d'Urfé, Canada	<i>March 2026</i>
Moteur de Recherche (Radio-Canada) Can we trust zoom meeting AI summaries - On French-language Canadian public radio Montreal, Canada	<i>February 2026</i>
Moteur de Recherche (Radio-Canada) Can LLMs help anyone create cyber-attacks - On French-language Canadian public radio Montreal, Canada	<i>January 2026</i>
Noovo Info AI Year in Review - On French-language TV Montreal, Canada	<i>December 2025</i>
Moteur de Recherche (Radio-Canada) Can LLMs develop mental illness - On French-language Canadian public radio Montreal, Canada	<i>November 2025</i>
Moteur de Recherche (Radio-Canada) LLMs' personalities - On French-language Canadian public radio Montreal, Canada	<i>October 2025</i>
Moteur de Recherche (Radio-Canada) AI for scientific discovery - On French-language Canadian public radio Montreal, Canada	<i>July 2025</i>
Moteur de Recherche (Radio-Canada) How AI guardrails work - On French-language Canadian public radio Montreal, Canada	<i>July 2025</i>
Moteur de Recherche (Radio-Canada) AI and Existential Risks Interview - On French-language Canadian public radio Montreal, Canada	<i>June 2025</i>
Montreal Public Libraries - Ethics of AI How LLMs work and are aligned -in French Montreal, Canada	<i>March 2025</i>
Montreal Public Libraries - L'IA de l'antiquité à chatGPT Intro to AI lecture + tutorial -in French Montreal, Canada	<i>February 2025</i>
Jimmy et Neutron (Scientific Radio show) - Aligning LLMs Invited for 2 columns; I explained how LLMs work and are aligned with human values. Montreal, Canada	<i>July 2023</i>
University of Montréal - Math Career Day - Data science for math alumni Talk about my work as a data scientist for the career fair day of the math program Montreal, Canada	<i>Jan 2021</i>

ACADEMIC SERVICE

REVIEWS

ACM CAIS	<i>2026</i>
ICLR	<i>2026</i>
TMLR	<i>2025-</i>
AAAI Workshop: Agentic AI Benchmarks and Applications for Enterprise Tasks	<i>2026</i>
AAAI	<i>2025, 2026, 2027</i>
NeurIPS Workshop: Differentiable Learning of Combinatorial Algorithms	<i>2025</i>
Chen Institute Symposium for AI-Accelerated Science	<i>2025</i>

ACM Transactions on Intelligent Systems and Technology	2025
ICML Workshop: Computer Use Agents	2025
COLM	2025, 2026
NeurIPS	2025, 2026
LION Conference	2025
ACL Workshop: Research on Agent Language Models	2025

TEACHING

Teaching Assistant - INF 8215: Intro to AI Polytechnique Montréal Tutorial sessions + grading for graduate-level Intro to AI course	<i>Fall 2025</i>
Teaching Assistant - INF 6102: Metaheuristics Polytechnique Montréal Developed course materials and led tutorial sessions for graduate-level optimization course	<i>Winter 2023</i>

HONORS, GRANTS AND SCHOLARSHIPS

ACM CAIS Best Paper Award	2026
Arbour Doctoral Scholarship - 30,000\$ for 1 year	2025
PolyconGRÉ, 2nd place in AI presentations competition in the university	2025
IVADO travel grant - 3,000\$ to attend Simons Institute workshop	2025
MITACS PhD Fellowship - 160,000\$ over 4 years	2024 - 2028
MITACS Accelerate Fellowship - 30,000\$ for 8 months	2024
MT180, 3rd place - Scientific communication competition	2023
NSERC Experience Award - 4,500\$ Summer research scholarship	2018
FRQNT - 2,000\$ NSERC Supplement	2018

EVENT HOSTING

Rock-Paper-Scissors Tournament Mila Organized the first 64-participant Rock-Paper-Scissors tournament in Mila history.	<i>November 2025</i>
---	----------------------