CISSE 2025

Towards Experiential Training Program for AI Security & Privacy Practitioners

Mohammed Abuhamad, Mujtaba Nazari, Loretta Stalans, **Eric Chan-Tin**

11/13/2025

LOYOLA UNIVERSITY CHICAGO

MOTIVATION

- Rapid adoption of Artificial Intelligence across industries
- Lack of formal security and privacy training for AI practitioners

ChatGPT

Claude

Gemini

Copilot

AI USAGE


Article
AI Research
New Tab
tobi lutke
@tobi
Reflexive AI usage is now a baseline expectation at Shopify
245
1.2K
5.9K
1.8M
Shopify internal memo that I shared here


TECH
LATEST NEWS
Meta Implements AI Usage Tracking and Gamification to Boost Employee Adoption


EA EMPLOYEES STRUGGLE WITH AI PUSH ACROSS ALL DEPARTMENTS


TICKER: $AMZN
amazon
AMAZON TO CUT ABOUT 14,000 CORPORATE JOBS IN AI PUSH
yahoo/finance


Artificial Intelligence at John Deere
JOHN DEERE
emerj

CHALLENGES

Traditional training is ineffective

Unprecedented security and privacy challenges with use of AI

Passive learning and/or rigid schedules for security/AI classes and certification programs

GOALS

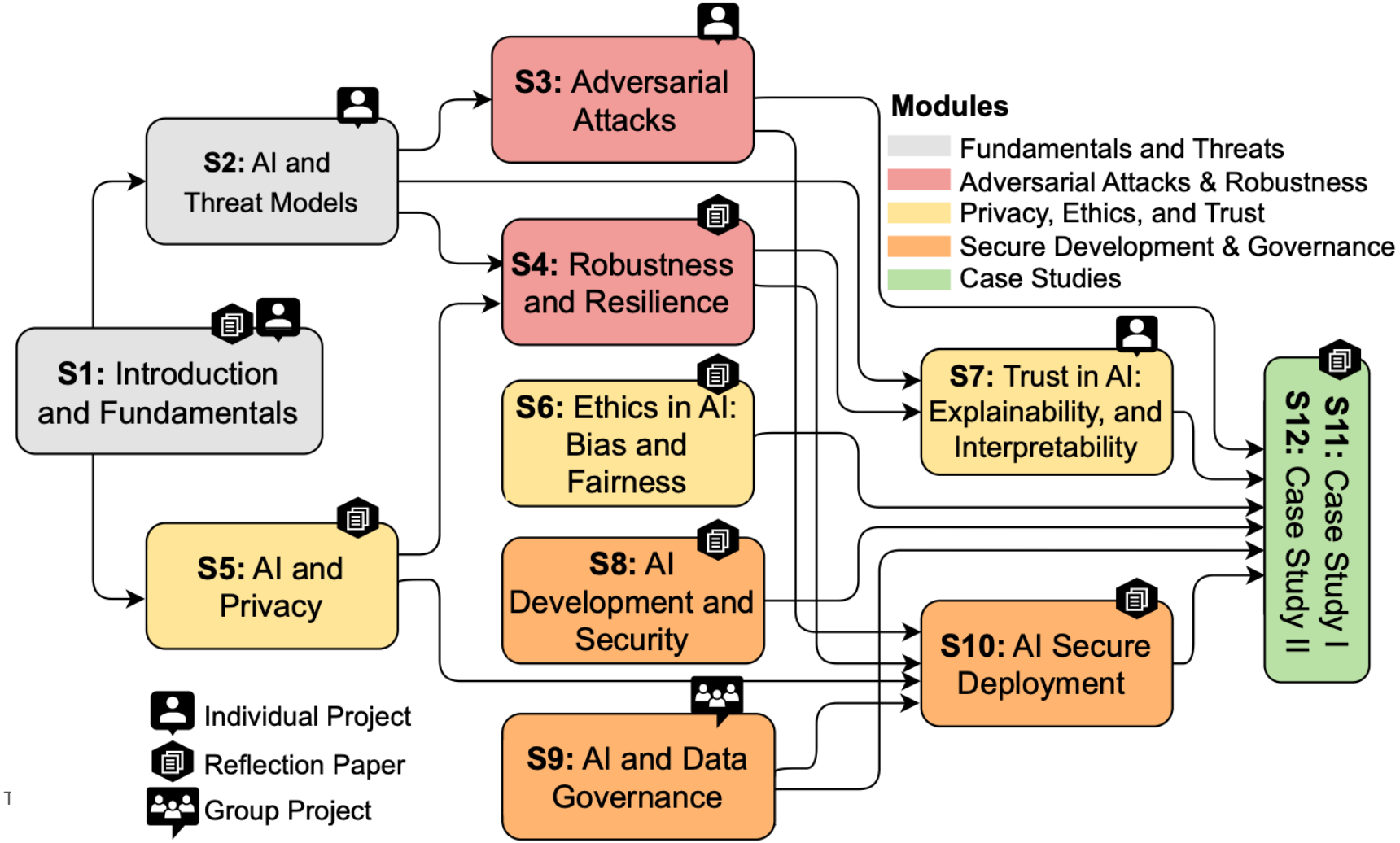
Experiential training program specifically for AI practitioners

Expert-led panels

Practical lab sessions

Real-world case studies

Experiential Training Program Overview



EXPERIENTIAL TRAINING PROGRAM IMPLEMENTATION

- Guest Speakers
  - Industry: Paypal, Meta, YSecurity
  - Academia: Loyola University Chicago, University of Wisconsin – Madison, North Carolina State University, Sungkyunkwan University, Arizona State University, University of California – Irvine, Brown University
- 2-hour session
  - Hour 1: Lecture or panel
  - Hour 2: hands-on laboratory session
    - Access to GPU-enabled Virtual Machines using Microsoft Azure Labs and Google CoLab
- Learned: TensorFlow, PyTorch, differential privacy libraries, federated learning, etc.
  - Standard implementations used in production AI systems

Curriculum of Workshop 1

SESSION	KEY ACTIVITIES
Lab 1	Identify cybersecurity risks in AI systems Assess risk likelihood and impact Propose mitigation strategies Implement security measures
Lab 2	Define white-box threat model Implement attacks (PGD, FGSM, C&W) Evaluate attack effectiveness Implement defenses (input sanitization, adversarial training)
Lab 3	Define black-box threat model Implement attacks (SimBA, MGAattack) Implement defenses Deploy adversarial detectors
Lab 4	Implement evaluation metrics Apply denoising methods Implement domain adaptation/transfer learning Assess robustness
Lab 5	Set up federated learning environment Implement client-side training Configure model aggregation Evaluate performance and privacy
Lab 6	Identify bias in datasets Measure bias using metrics Apply bias mitigation techniques Analyze impact on model performance
Lab 7	Analyze feature importance Implement interpretable models Apply interpretation methods (e.g. GRAD & CAM)
Lab 8	Set up secure development environment Implement secure coding practices Deploy models securely Establish monitoring procedures
Lab 9	Assess data handling practices Develop data governance framework Apply compliance checklists Review industry standards
Lab 10	Containerize AI models Apply secure API design Implement access controls
Lab 11 & 12	Analyze real-world case studies Review security vulnerabilities Implement mitigation strategies Document lessons learned Final reflection

RECRUITMENT

- LinkedIn
- Computer Science Industry Advisory Board
- Center for Data Science Consulting
- Startup Incubators
- Alumni network

WORKSHOPS

RUN 1

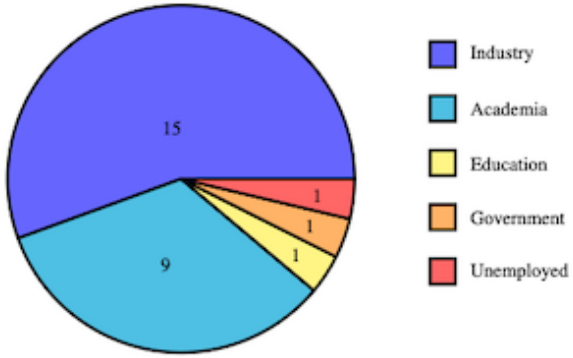
12 sessions every 2 weeks

RUN 2

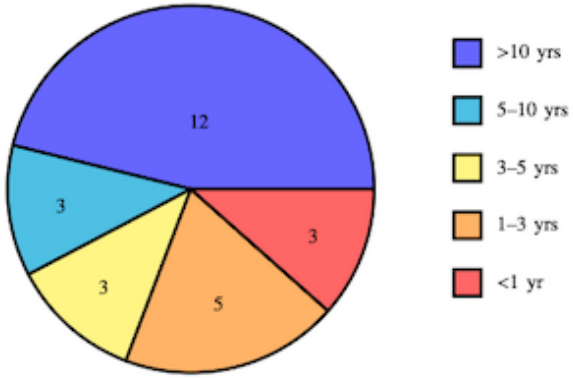
6 sessions every week

Same material

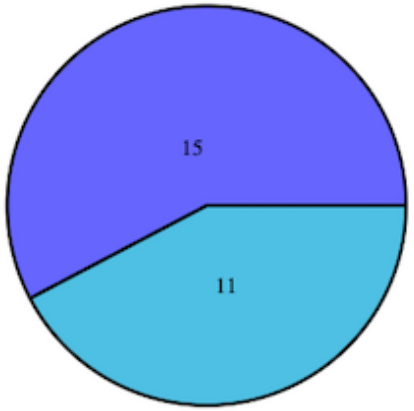
More asynchronous videos



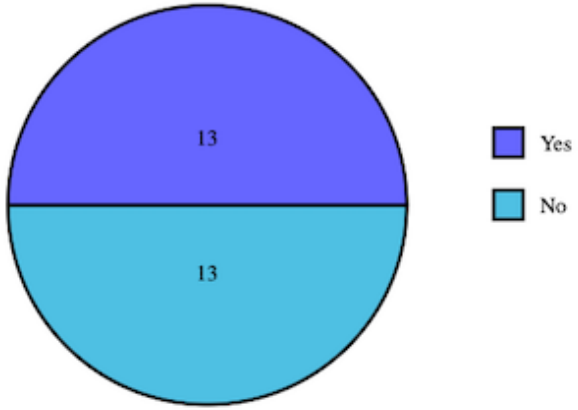
(a) Work sectors (n=26)



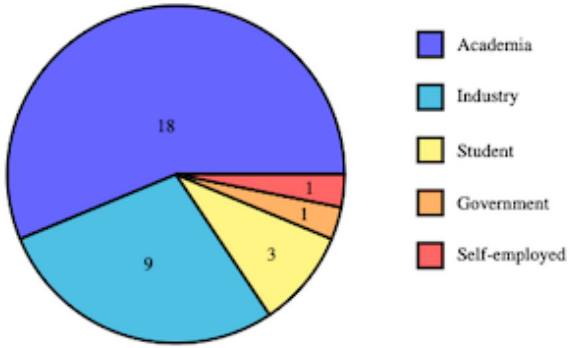
(b) Experience levels



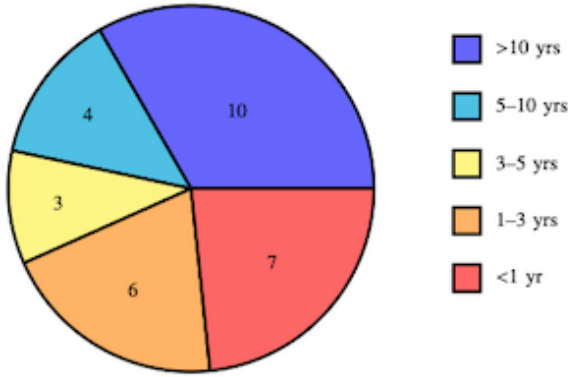
(c) Formal AI training



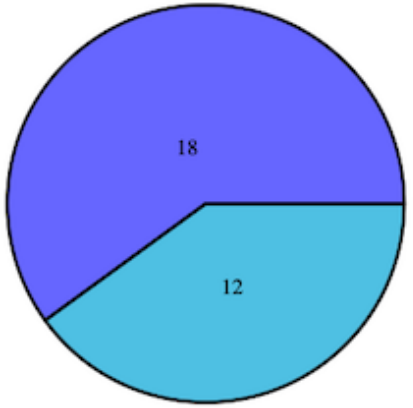
(d) Formal cybersecurity training



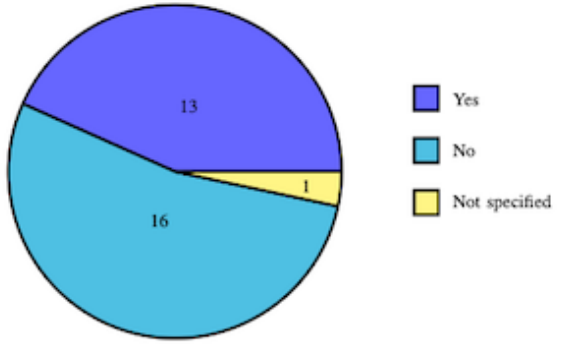
(h) Work sectors (n=30)



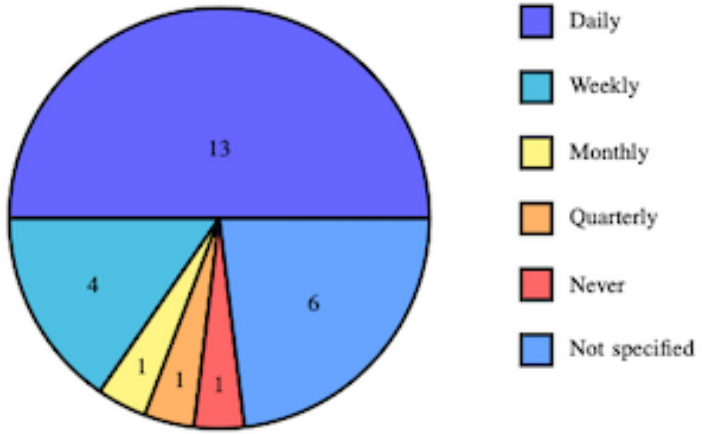
(i) Experience levels

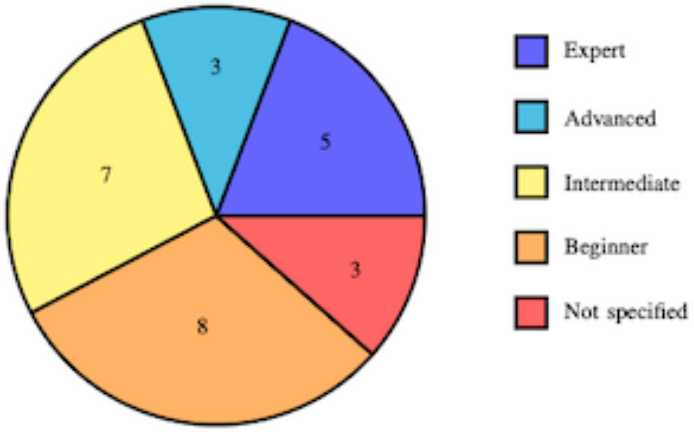


(j) Formal AI training



(k) Formal cybersecurity training

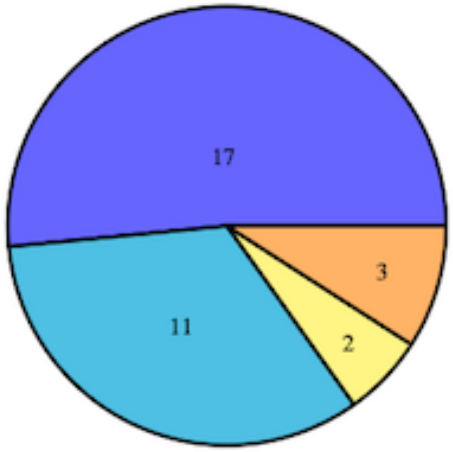




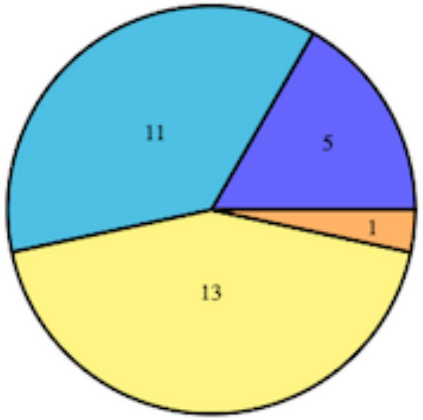
(e) AI tool usage frequency

(f) AI expertise ratings

(g) Cybersecurity knowledge ratings



(l) AI tool usage frequency



(m) AI expertise ratings

(n) Cybersecurity knowledge ratings

EVALUATION

- Institutional Review Board (IRB) approval
- External evaluator, different from instruction team

Program Surveys

PRE

Baseline knowledge in

- AI concepts
- Cybersecurity principles

POST

Measured knowledge in

- AI concepts
- Cybersecurity principles
- Skill development

Qualitative evaluation during workshop sessions

Compensation of participants to incentivize completion of post-program survey

RESULTS

TYPES OF KNOWLEDGE	Pre-Program Survey			Post-Program Survey		
	Mean	Median	# of Items	Mean	Median	# of Items
About Basic Cybersecurity	73%	87%	15	85%	86%	7
About Artificial Intelligence	20%	13%	15	56%	47%	15

CHALLENGES

- **Wide range of audience and skills**
  - E.g. some participants didn’t know how to unzip a file
  - E.g. some participants didn’t know basic command line arguments
- **Selective Interest in certain topics**
  - Participants were less interested in the topic of ethics and fairness
- **Competing demands on professionals who work 40 hours a week**
  - Only about half of the interested professionals completed the first two workshops

LIMITATIONS of EVALUATION

FUTURE WORK

- Optimal combinations of synchronous and asynchronous learning components
- Long term retention
- Career impact assessment

CONCLUSION

- Targeted, hands-on education can help with the AI Cybersecurity gap

This material is based upon work supported by the National Science Foundation under Grant No. DGE 2335700

LOYOLA UNIVERSITY CHICAGO

Thank you!

Any questions? Contact dchantin@luc.edu

LOYOLA UNIVERSITY CHICAGO