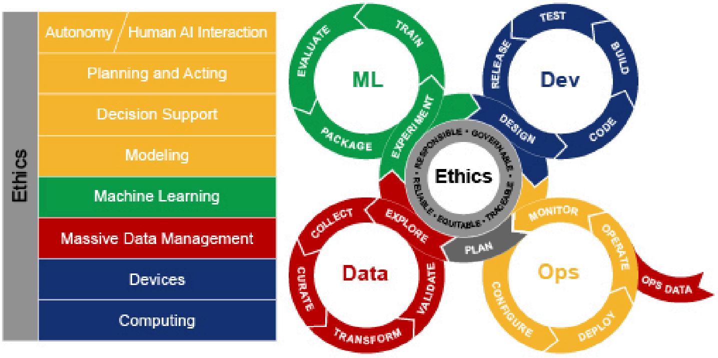
SEI Bulletin

Trouble reading this email? View in browser.



Counter AI: What Is It and What Can You Do About It?

September 11, 2024—As the strategic importance of AI systems increases, so too does the importance of defending them from AI offense, or counter AI. A new paper from the SEI describes the AI technology stack, the machine learning operations (MLOps) lifecycle and the threat models throughout it, and counter-AI attacks. The paper also gives long-term and near-term recommendations for preventing and mitigating counter-AI attacks.

“The existence of a Future Capability threat model underscores the fundamental insecurity of AI systems at our current level of AI maturity,” write the authors of *Counter AI: What Is It and What Can You Do About It?* The paper recommends a near-term approach similar to traditional cybersecurity: “Develop the processes necessary to respond to counter-AI attacks quickly and efficiently. Then, take what we learn from the AI incident response to inform the field of study, identify vulnerabilities, and establish best practices.”

Read more »

SEI News

DevSecOps Days D.C. Announces Agenda and Keynote Speaker
Lt. Col. Christopher Hocking will talk about why DevOps matters to the warfighter.

SEI Launches Course on Developing a National or Government Computer Security Incident Response Team
The new course is intended to help nations develop robust cybersecurity capabilities.

See more news »

Latest Blogs

Generative AI and Software Engineering Education
Educators have had to adapt to rapid developments in generative AI to provide a realistic perspective to their students. Ipek Ozkaya, Doug Schmidt, and Michael Hilton discuss generative AI and software engineering education.

Acquisition Archetypes Seen in the Wild, DevSecOps Edition: Cross-Program Dependencies
Shared capabilities can help manage costs and complexities but can also result in cross-program dependencies. William Novak examines this phenomenon in a DevSecOps context.

See more blogs »

Latest Podcasts

3 API Security Risks (and How to Protect Against Them)
McKinley Sconiers-Hasan discusses three API risks and how to address them through the lens of zero trust.

Evaluating Large Language Models for Cybersecurity Tasks: Challenges and Best Practices
Jeff Gennari and Sam Perl discuss applications for LLMs in cybersecurity, potential challenges, and recommendations for evaluating LLMs.

See more podcasts »

Latest Videos

Embracing AI: Unlocking Scalability and Transformation Through Generative Text, Imagery, and Synthetic Audio
Tyler Brooks, Shannon Gallagher, and Dominic Ross aim to demystify AI and illustrate its transformative power in achieving scalability, adapting to changing landscapes, and driving digital innovation.

Generative AI and Software Engineering Education
SEI experts in software engineering discuss how generative AI is influencing software engineering education.

Latest Publications

Counter AI: What Is It and What Can You Do About It?
This paper describes counter AI and provides recommendations on what can be done to defend AI systems in the long term and near term.

Using Quality Attribute Scenarios for ML Model Test Case Generation
This conference paper presents an approach based on quality attribute (QA) scenarios to elicit and define system- and model-relevant test cases for machine learning models.

See more publications »

Upcoming Events

DevSecOps Days Washington D.C. 2024, September 18
This free, in-person event in Arlington, Virginia, will teach how to integrate security into DevOps practices and transform DevSecOps journeys.

International Conference on Conceptual Modeling (ER 2024), October 28-31
The SEI will host the main international forum for discussing the state of the art, emerging issues, and future challenges in research and practice on conceptual modeling.

See more events »

Upcoming Appearances

TechNet Indo-Pacific 2024, October 22-24
Visit the SEI at booth 1411.

27th Annual Systems & Mission Engineering Conference, October 28-31
Visit the SEI booth at this event.

See more opportunities to engage with us »

Upcoming Training

Insider Risk Management: Measures of Effectiveness
October 29-31 (SEI Live Online)

Risk Program Development - Governance and Appetite Workshop
November 13-14 (SEI Arlington, Va.)

See more courses »

Employment Opportunities

Senior AI Security Researcher

Information System Security Manager

Program Development Manager

All current opportunities »

Carnegie Mellon University
Software Engineering Institute