SEI Bulletin 40 years

Machine Learning Test and Evaluation Tool and Process Adds Features

May 28, 2025 — Machine learning (ML) models integrated into a larger software system are frequently developed in isolation, making testing and evaluation (T&E) against system and operational requirements impossible. This limitation can lead to failures in production, putting at risk warfighters who depend on ML-enabled capabilities, such as situational awareness and threat recognition enabled by computer vision models.

The SEI created the Machine Learning Test and Evaluation (MLTE) process and tool to help ensure ML models are production ready. Earlier this month, the SEI released version 2.0.0 of MLTE. It creates stronger links between ML model requirements, derived from the larger system, and requirement satisfaction testing. This kind of context-aware T&E prevents the lengthy rework that follows ML model failure during operational tests or in production, so ML capabilities are deployed faster to the warfighter.

Read more »

SEI News

SEI Study on Defense Department DevSecOps Finds Excellence and Opportunities
The study, released by the DoD Chief Information Officer, found the department should scale up its pockets of DevSecOps success.

2024 Year in Review Showcases SEI's Impact on National Security
This annual publication highlights the research and development in software engineering, cybersecurity, and artificial intelligence that enhanced warfighter capabilities and national defense in fiscal year 2024.

See more news »

Latest Blogs

A 5-Stage Process for Automated Testing and Delivery of Complex Software Systems
Caden Milne and Lyndsi Hughes describe how managing and maintaining deployments of complex software present engineers with a multitude of challenges, including security vulnerabilities.

Stop Imagining Threats, Start Mitigating Them: A Practical Guide to Threat Modeling
Alex Vesey describes a method for developing a cyber threat model when building a software-intensive system.

See more blogs »

Latest Podcasts

The Best and the Brightest: 6 Years of Supporting the President's Cup Cybersecurity Competition

The SEI team that supported the President's Cup Cybersecurity Competition details their challenges, successes, and lessons learned.

Updating Risk Assessment in the CERT Secure Coding Standard
Joe Sible, David Svoboda, and Robert Schiela explore proposed risk assessment updates to the CERT Secure Coding Standard.

See more podcasts »

Latest Publications

Practical Supervised Machine Learning Classification of Highly Imbalanced Text
Austin Whisnant describes a machine learning model used to build a corpus of insider threat data to support insider threat research.

2024 SEI Year in Review
The 2024 SEI Year in Review highlights the work of the institute undertaken during the fiscal year spanning October 1, 2023, to September 30, 2024.

See more publications »

Latest Videos

The State of DevSecOps in the DoD: Where We Are, and What's Next
The SEI's Brigid O'Hearn and Eileen Wrubel and George Lamb, the Department of Defense (DoD) director of cloud and software modernization, discuss how key findings of *The State of DevSecOps in the DoD* study will help the DoD ensure an effective, scalable, and adaptable software ecosystem.

I Spy with My Hacker Eye: How Hackers Use Public Info to Crack Your Creds
Destiney Plaza reveals five ways to protect yourself from getting your password cracked.

See more videos »

Upcoming Events

Demystifying Operational Resilience, June 4, webcast
Alexander Petrilli and Matthew Butkovic explain why operational resilience is important and discuss best practices to carry out mission priorities when core operational capacities are affected.

Insider Risk Management Symposium 2025, June 12, Arlington, Va.
The theme of this year's event is "Technology-Driven Changes to the Insider Risk Landscape."

International Workshop on Envisioning the AI-Augmented Software Development Life Cycle, June 26, Trondheim, Norway
This workshop seeks to explore how AI might transform end-to-end software systems development workflows and emphasizes the need to collect relevant data now to assess the long-term effects of AI throughout the software development life cycle.

Secure Software by Design 2025, August 19-20, Arlington, Va.
Join thought leaders in secure software by design for presentations and discussions on all aspects of secure software systems development.

Model-Based Systems Engineering (MBSE) in Practice 2025, August 21, Arlington, Va.
Join us to gain practical insights from seasoned MBSE adopters, discover innovative solutions to common challenges, and shape the future of systems engineering in an increasingly complex world.

See more events »

Upcoming Appearances

Ash Carter Exchange on Innovation and National Security and A+ Expo 2025, June 2-4, Washington, D.C.
Visit the SEI and Carnegie Mellon University at booth 627.

AFCEA TechNet Augusta 2025, August 18-21, Augusta, Ga.
Visit the SEI at booth T825.

See more opportunities to engage with us »

Upcoming Training

Cybersecurity Oversight for the Business Executive
July 29-30 (Live Online)

Documenting Software Architectures
August 4-7 (Live Online)

E-learning - CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate

E-learning - Introduction to Artificial Intelligence (AI) Engineering

See more courses »

Employment Opportunities

Technical Lead

Senior Embedded Software Engineer - Utah

All current opportunities »