SEI Bulletin

Trouble reading this email? View in browser.

New SEI Tool Enhances Machine Learning Model Test and Evaluation

October 23, 2024—Machine learning (ML) models are frequently developed in isolation, making it impossible to test and evaluate them against system and operational requirements. The SEI recently released a tool to help teams developing ML-enabled software systems mitigate this problem. Machine Learning Test and Evaluation (MLTE), available from GitHub, is a semi-automated process and infrastructure for testing ML models based on stakeholder-generated quality attribute requirements.

“Many models fail in production because they are not tested properly,” said Grace Lewis, a principal researcher at the SEI and lead of its Tactical and AI-Enabled Systems Initiative. “MLTE provides system and operational context for ML model developers to make informed decisions about design and development. Other stakeholders can better understand whether the requirements for models are realistic so that problems can be detected and fixed early in the process, not discovered in operational tests or production.”

Read more »

Download MLTE »

SEI News

New SEI Tool Enhances Machine Learning Model Test and Evaluation
Machine Learning Test and Evaluation version 1.0 applies software engineering best practices to ensure ML model development results in production-ready ML models.

FloCon 2025 Opens Call for Participation
The annual conference on data-driven security is seeking abstracts on situational awareness beyond the network by December 20.

See more news »

Latest Blogs

An Introduction to Model-Based Systems Engineering (MBSE)
Revisit our most read post over the last four years. Nataliya Shevchenko introduces model-based systems engineering, a methodology to support the requirements, design, analysis, verification, and validation associated with the development of complex systems.

Challenges to Assuring Large-Scale Systems
National defense efforts have shifted from defeating terrorism to accelerating innovation, with a priority of delivering capability at speed and scale. SEI experts outline a model problem for assurance of large-scale systems and six challenges to assuring systems at the speed DoD needs now.

See more blogs »

Latest Podcasts

Cybersecurity Metrics: Protecting Data and Understanding Threats
Scoping down objectives and determining what kinds of data to gather are persistent challenges in cybersecurity. Bill Nichols explores cyber metrics in our latest podcast.

3 Key Elements for Designing Secure Systems
To make secure software by design a reality, engineers must intentionally build security throughout the software development lifecycle. Timothy A. Chick discusses building, designing, and operating secure systems.

See more podcasts »

Latest Videos

From Chaos to Clarity: Conceptual Modeling for Complex Systems
Wolfgang Maass, Hyoil Han, and Hasan Yasar discuss key principles of conceptual modeling and explore its significance in various domains and its role in driving successful system design.

Redemption Tool Demo Video: Separate Environments for Code Compilation and Code Repair
David Svoboda shows the manual review of the code repairs done by Redemption in a terminal.

See more videos »

Latest Publications

Positive Deterrence for Reducing Insider Threat Collection
This collection contains materials related to the SEI's research on organizations' use of positive deterrence to reduce the risk of insider activity.

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.

See more publications »

Upcoming Events

Webcast - Cyber Challenges in Health Care: Managing for Operational Resilience, October 30
Matthew Butkovic and Darrell Keeling will explore approaches to maximize return on cybersecurity investment in the health-care context.

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 at booth 8, and hear SEI researchers Lori Flynn, Alexander Vesey, and Jérôme Hugues.

See more opportunities to engage with us »

Upcoming Training

Introduction to the CERT Resilience Management Model
December 3-4 (SEI Arlington, Va.)

Insider Threat Analyst
December 10-12 (SEI Live Online)

See more courses »

Employment Opportunities

Software Acquisition Specialist

Security Researcher

Senior AI Engineer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute

Copyright © 2024 Carnegie Mellon University Software Engineering Institute, All rights reserved.

Want to subscribe or change how you receive these emails?
You can subscribe, update your preferences or unsubscribe from this list.