SEI Bulletin

Trouble reading this email? View in browser.

# Portend Toolset Creates Guardrails for Machine Learning Data Drift

**January 8, 2025—**Machine learning (ML) models are powerful but brittle. If the input data from the deployment environment drifts away from the training data—for example, when flooding changes the landmarks in satellite images guiding an unmanned aerial vehicle—the model can produce incorrect outputs. The SEI recently released an open source toolset called Portend that model developers can use to simulate ML data drift, set guardrails, and give an alert when model data drifts too far, enhancing ML assurance.

While drift detection algorithms exist, Portend is an end-to-end solution. It begins by using libraries of known types of data drift to induce artificial drift in an ML model. “Now you have ground truth on what data is and isn’t drifted, and you can see the difference in the model’s behavior,” said Jeffery Hansen, a senior ML research scientist at the SEI and Portend’s principal investigator. Users can then configure alerts for behavior in operation that signals drift.

Better ML assurance makes ML system operators aware of drift's effect on the mission, tells developers when to retrain the model, and gives decision makers more data on how to budget ML training resources.

**Read more »**

---

## SEI News

SEI Releases Security Engineering Framework
The new framework compiles an actionable hierarchy of the key leading practices for building secure and resilient software-reliant systems.

AI Red-Teaming Workshop Will Explore Best Practices
The free, hybrid workshop will gather artificial intelligence and cybersecurity experts to explore effective red-teaming for generative AI systems.

Carleton Named SEI Fellow
The honor recognizes Carleton's outstanding contributions to the software community and expected future advancement of the SEI's mission.

**See more news »**

---

## Latest Blogs

The Top 10 Blog Posts of 2024
This post presents the top 10 most-visited posts of 2024, highlighting our work in software acquisition, artificial intelligence, large language models, secure coding, and more.

The Latest Work from the SEI: Insider Risk, Bias in LLMs, Secure Coding, and Designing Secure Systems
The latest work from SEI technologists encompasses insider risk, large language models, secure coding and static analysis, cybersecurity metrics, and more.

Beyond Capable: Accuracy, Calibration, and Robustness in Large Language Models

For any organization seeking to responsibly harness the potential of large language models, Matthew Walsh, David Schulker, and Shing-hon Lau describe a holistic approach to LLM evaluation that goes beyond accuracy.

**See more blogs »**

## Latest Podcasts

Securing Docker Containers: Techniques, Challenges, and Tools

Sasank Venkata Vishnubhatla and Maxwell Trdina sit down with Tim Chick to explore issues surrounding containerization, including recent vulnerabilities.

An Introduction to Software Cost Estimation

Software cost estimation is an important first step when beginning a project. Anandi Hira discusses various metrics, best practices, and common challenges.

**See more podcasts »**

## Latest Videos

Understanding the Need for Cyber Resilience

Matthew Butkovic, Greg Crabb, and Ray Umerley explore how to plan for maintaining operational resilience when a ransomware incident occurs.

**See more videos »**

## Latest Publications

Addressing Today's Software Risks Requires an Assurance-Educated Workforce
Carol Woody summarizes gaps in workforce knowledge, skills, and support resources based on recent publications and panel discussions held by the Software Assurance Supply Chain forum.

Portend
This open source toolset provides an end-to-end machine-learning assurance solution for simulating drift, detecting it in operation, and generating alerts.

Vessel
These open source tools help software developers identify the cause of discrepancies between container builds.

Security Engineering Framework (SEF): Managing Security and Resilience Risks Across the Systems Lifecycle
The SEF is a collection of software-focused engineering practices organized into a hierarchy of goals and domains and includes in-depth guidance.

**See more publications »**

## Upcoming Events

Probing the Limits: A Workshop on Red-Teaming AI Systems, January 28
Participants in this free, hybrid workshop will help identify best practices for red-teaming generative AI systems to extend existing guidance on cyber red teaming.

FloCon 2025, March 4
FloCon is the SEI's annual conference on data-driven security.

**See more events »**

## Upcoming Appearances

AIAA SciTech Forum 2025, January 6-10
Visit the SEI at booth 106.

AFCEA West 2025, January 28-30
Visit the SEI at booth 3233.

**See more opportunities to engage with us »**

## Upcoming Training

Software Architecture Design and Analysis
February 11-14 (SEI Live Online)

Insider Risk Management Measures of Effectiveness
February 19-21 (SEI Live Online)

**See more courses »**

## Employment Opportunities

Senior Software Engineer

Assistant AI Software Engineer

Program Development Manager

**All current opportunities »**

*Copyright © 2025 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.