SEI Bulletin



# AI Trust and Autonomy Labs Fill the Gap Between AI Breakthroughs and DoD Deployment

**June 5, 2024—**The Department of Defense has recognized the potential benefits of using AI and machine learning (ML) systems. At the same time, recent government guidance urges responsibility with this rapidly changing technology. To help agencies and the defense industrial base meet the government's AI needs, the SEI has recently formalized two laboratories in key areas: AI trust and AI autonomy.

The two new labs join the AI Division's Adversarial ML Lab and Advanced Computing Lab. "With the addition of the Autonomy and Trust labs, the AI Division adds two key focus areas that enhance our work in promoting and advancing the art and practice of AI engineering," said Eric Heim, the SEI AI Division's chief scientist. "We strive towards making AI more robust, secure, scalable, and human-centered, all key attributes in ensuring that DoD missions can use AI successfully and responsibly."

Read more »

*Photo: Patrick Hunter*

## SEI News

Nominations for Humphrey Software Quality Award Open Through September 1
The award recognizes improvement in an organization's ability to create and evolve high-quality software-dependent systems.

New SEI Tool Brings Visibility to DevSecOps Pipelines
The Polar tool gives a comprehensive visualization of the complete DevSecOps pipeline.

**See more news »**

## Latest Blogs

The Threat of Deprecated BGP Attributes
Leigh Metcalf and Timur Snoke examine how a small issue with Border Gateway Protocol routing, a deprecated path attribute, can cause a major interruption to Internet traffic.

Versioning with Git Tags and Conventional Commits
Alex Vesey explores extending the conventional commit paradigm to enable automatic semantic versioning with git tags to streamline the development and deployment of software.

**See more blogs »**

## Latest Podcasts

Automated Repair of Static Analysis Alerts
David Svoboda discusses Redemption, a new open source tool that automatically repairs common errors in C/C++ code generated from static analysis alerts.

Cyber Career Pathways and Opportunities
Randy Trzeciak discusses his career journey, resources for pursuing a career in cybersecurity, and the importance of building a diverse workforce.

**See more podcasts »**

## Latest Videos

Can You Rely on Your AI? Applying the AIR Tool to Improve Classifier Performance
SEI researchers discuss a new AI Robustness (AIR) tool that allows users to gauge AI and ML classifier performance with confidence.

## Latest Publications

Using LLMs to Automate Static-Analysis Adjudication and Rationales
This article by Lori Flynn and William Klieber discusses a model for using large language models (LLMs) to handle static analysis output.

Redemption: Automated Repair of Static Analysis Alerts
The Redemption tool makes automated repairs to C and C++ source code based on defect alerts produced by static-analysis tools.

**See more publications »**

## Upcoming Events

Webcast - Secure Systems Don't Happen by Accident, June 12
Tim Chick will discuss how security is an integral aspect of the entire software lifecycle.

DevSecOps Days Pittsburgh 2024, July 9
Learn from fellow DevSecOps practitioners, discover how to integrate security into your teams, and gain insight on automating security in the developer and production pipeline.

Secure Software by Design, August 6-7
Collaborate on improving software security with two on-site days of panel discussions and presentations plus two optional on-site days of training.

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

Emerging Technologies for Defense Conference & Exhibition 2024, August 7-9
Visit the SEI at booth 316.

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

Cybersecurity Oversight for the Business Executive
July 30-31 (SEI Live Online)

Developing a National or Government CSIRT
October 8-9 (SEI Live Online)

**See more courses »**

## Employment Opportunities

Technical Lead

Senior Team Lead - Applied Network Defense

Senior Cyber Risk Engineer

**All current opportunities »**

Carnegie Mellon University
Software Engineering Institute