SEI Bulletin

New Research Supports SEI AISIRT Mission to Secure Artificial Intelligence

April 2, 2025—The general-purpose artificial intelligence (GPAI) ecosystem needs to adapt lessons from the software security domain, according to a newly released paper by representatives from academia, industry, and the SEI. Lauren McIlvenny, the technical director of threat analysis in the SEI's CERT Division, was a coauthor on the paper. McIlvenny oversees the SEI's AI Security Incident Response Team (AISIRT), which was created in 2023 to identify, analyze, and respond to AI-related incidents, flaws, and vulnerabilities, particularly in systems critical to defense and national security.

The paper *In-House Evaluation Is Not Enough: Towards Robust Third-Party Flaw Disclosure for General-Purpose AI* raises the alarm about GPAI safety and the need for coordinated vulnerability disclosure (CVD). "This paper was backed by more than 30 respected technology, policy, and security experts," McIlvenny said. "They all recognized how critical CVD for GPAI is for consumers, the commercial sector, and national security. Their

collaboration sends a signal that the community recognizes the importance of the challenge and is ready to make meaningful progress."

Read more »

SEI News

New DoD Memo Accelerates Software Acquisition Modernization
The directive signals an accelerated uptake of the Software Acquisition Pathway, which reforms software development and acquisition within the Defense Department.

See more news »

Latest Blogs

The Essential Role of AISIRT in Flaw and Vulnerability Management
The SEI established the first Artificial Intelligence Security Incident Response Team (AISIRT) in 2023. Lauren McIlvenny and Vijay Sarvepalli discuss the AISIRT's role in the coordination of flaws and vulnerabilities in AI systems.

Enhancing Machine Learning Assurance with Portend
This post introduces Portend, a new open source toolset that simulates data drift in machine learning models and identifies the proper metrics to detect drift in production environments.

Cybersecurity of Logistics Decision Models
Goods, services, and people cannot get to where they are needed without effective logistics. Clarence Worrell and Lauren Hoge focus on cyber attacks to logistics decision models.

See more blogs »

Latest Podcasts

Getting the Most Out of Your Insider Risk Data with IIDES
Insider incidents cause around 35 percent of data breaches. Austin Whisnant and Dan Costa discuss the Insider Incident Data Expression Standard (IIDES), a new schema for collecting and sharing data about insider incidents.

Grace Lewis Outlines Vision for IEEE Computer Society Presidency
The SEI's Grace Lewis was elected the 2026 president of the IEEE Computer Society, the largest community of computer scientists and engineers.

See more podcasts »

Latest Videos

Threat Hunting: What Should Keep All of Us Up at Night
Dan Ruef explains how cybersecurity professionals can stay on task to secure networks and systems even as the big promises of the latest and greatest tools and other distractions vie for their attention.

Can a Cybersecurity Parametric Cost Model be Developed?
Christopher Miller shares insights from an SEI study on cybersecurity cost estimating that can help national security organizations successfully deploy parametric cost modeling.

See more videos »

Latest Publications

AI Hygiene Starts with Models and Data Loaders
This paper places a call to action for traditional cybersecurity tools and techniques to be applied to artificial intelligence for improving the cybersecurity of AI systems.

See more publications »

Upcoming Events

Webcast - New Data Exchange Standard Eases Insider Incident Data Collection and Sharing, April 2
Austin Whisnant and Dan Costa introduce the Insider Incident Data Exchange Standard (IIDES), which enables researchers and practitioners to easily build insider threat case data and share analysis and insights.

Webcast - Malware Research: If You Cannot Replicate it, You Will Not Use It, April 23
Leigh Metcalf and Edward Schwartz recommend ways to overcome the problem of replicating and reproducing academic malware research results, so that new and needed concepts and tools can be more quickly used.

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

See more events »

Upcoming Appearances

Navy League Sea Air Space (SAS) 2025, April 7-9
Visit the SEI at booth 205.

40th Space Symposium 2025, April 7-10
Visit the SEI at booth 304.

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

See more opportunities to engage with us »

Upcoming Training

Software Architecture: Principles and Practices
April 28-May 1 (Live Online)

Foundations of Incident Management
May 13-16 (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

Accredited Network Administrator

Senior AI Security Researcher

Senior C++ Engineer

All current opportunities »