SEI Bulletin

Trouble reading this email? View in browser.

SEI Establishes AI Division, Introduces AI Engineering Pillars

July 7, 2021 — The SEI has established a new research division dedicated to artificial intelligence (AI) engineering and named Matthew Gaston as the new division's director. Gaston is currently director of the SEI's Emerging Technology Center. The new SEI AI Division will focus on research in applied artificial intelligence and the engineering questions related to the practical design and implementation of AI technologies and systems.

AI engineering is an emerging field of research and practice that combines the principles of systems engineering, software engineering, computer science, and human-centered design to create AI systems in accordance with human needs for mission outcomes. The SEI recently released white papers outlining the challenges and opportunities of three initial pillars of AI engineering: human centered, scalable, and robust and secure.

"I am very excited to lead the new SEI AI Division and to scale the SEI's AI engineering capabilities in support of defense and national security," said Gaston.

Read more about the new AI Division »

Read more about the three pillars white papers »

SEI News

Building AI Better: SEI Introduces Three Pillars of AI Engineering
New white papers explore open questions around creating and implementing human-centered, scalable, and robust and secure artificial intelligence systems.

Software Engineering Institute Announces Establishment of New AI Division, Names Director
Carnegie Mellon University's Software Engineering Institute today announced the establishment of a new research division dedicated to artificial intelligence (AI) engineering and named Matthew Gaston as the new division's director.

SEI Maps Out Cybersecurity for World Economic Forum
The interactive conceptual map connects today's top cybersecurity challenges to other critical global issues.

See more news »

Latest Blogs

The Latest Work from the SEI: Artificial Intelligence, DevSecOps, and Security Incident Response
Doug Schmidt summarizes some recently published SEI reports, podcasts, and webcasts.

Considerations for Operator-Feedback Sessions in Government Settings
Michael Szegedy and Timothy Chick describe a design approach that considers operator feedback and effectively leverages feedback sessions.

Anti-Tamper for Software Components
Scott Hissam explains how to identify system software components in

danger of being exploited that should be protected by anti-tamper practices.

See more blogs »

Latest Podcasts

Is Your Organization Ready for AI?
Rachel Dzombak and Carol Smith discuss how AI engineering can help organizations implement AI systems.

My Story in Computing with Marisa Midler
Marisa Midler discusses the career path that led to her work as a cybersecurity engineer in the SEI's CERT Division.

Managing Vulnerabilities in Machine Learning and Artificial Intelligence Systems
Allen Householder, Jonathan Spring, and Nathan VanHoudnos discuss how to manage vulnerabilities in AI/ML systems.

See more podcasts »

Latest Publications

A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)
This report discusses performance indicators that stakeholders in coordinated vulnerability disclosure (CVD) can use to measure its effectiveness.

DevSecOps Days Pittsburgh 2021 Graphic Recordings
This collection of graphic recordings is of the presentations from DevSecOps Days Pittsburgh 2021.

Pillars of AI Engineering Assets
These white papers describe the three pillars of AI engineering: scalable, robust and secure, and human-centered.

See more publications »

Latest Videos

Webcast - Software Development Open Forum: Ask Hasan Anything!
Hasan Yasar hosts a software development question and answer session.

Using Value Engineering to Propel Cyber-Physical Systems Acquisition
Nickolas Guertin and Alfred Schenker discuss adapting value engineering (VE) methods into the acquisition of software-intensive weapon systems.

Webcast - Software Supply Chain Concerns for DevSecOps Programs
Aaron Reffett and Richard Laughlin explore the important architectural aspects of DevSecOps that are impacted by the software supply chain.

Upcoming Events

Software Engineering Workshop for Educators, August 3-5
The annual Workshop for Educators will foster an ongoing exchange of ideas among educators whose curricula include the subjects of software architecture and software product lines.

AI World Government 2021, October 18-19
SEI experts will participate in this two-day forum to educate federal agency leaders on proven strategies and tactics to deploy AI and cognitive technologies.

Note: The SEI is evaluating all upcoming courses, conferences, and events case-by-case in light of COVID-19 developments. Check individual event pages for the latest information.

See more events »

Upcoming Training

Software Architecture: Principles and Practices
August 3-6, 2021 (SEI, Live Online)

Insider Threat Analyst
August 10-12, 2021 (SEI, Live Online)

Cybersecurity Oversight for the Business Executive
August 17-18, 2021 (SEI, Live Online)

Note: The SEI is evaluating all upcoming courses, conferences, and events case-by-case in light of COVID-19 developments. Check individual training pages for the latest information. You may also contact us at courseregistration@sei.cmu.edu or +1-412-268-7388.

See more courses, including live-online and eLearning offerings »

Employment Opportunities

Senior Risk Engineer

Insider Risk Researcher

All current opportunities »