SEI Bulletin

Trouble reading this email? View in browser.

SEI Establishes AI Security Incident Response Team

December 6, 2023—The SEI recently announced the formation of the Artificial Intelligence Security Incident Response Team (AISIRT) to help ensure the safe and effective development and use of AI. AISIRT will analyze and respond to threats and security incidents emerging from advances in AI and machine learning (ML). The team will also lead research efforts in incident analysis and response and vulnerability mitigation involving AI and ML systems.

"AI and cybersecurity experts at the SEI are currently at work on AI- and ML-related vulnerabilities that, if left unaddressed, may be exploited by adversaries against national assets with potentially disastrous consequences," said SEI Director and CEO Paul Nielsen. "Our research in this rapidly emerging discipline reinforces the need for a coordination center in the AI ecosystem to help engender trust and to support advancing the safe and responsible development and adoption of AI."

Read more »

SEI News

FloCon 2024 Announces Full Program and Continuing Education Units
Registration is open for the January conference on using data to defend networks.

See more news »

Latest Blogs

Creating a Large Language Model Application Using Gradio
Tyler Brooks explains how to build a large language model across three primary use cases: basic question-and-answer, question-and-answer over documents, and document summarization.

Don’t Wait for ROI on Model-Based Analysis for Embedded Computing Resources
Alfred Schenker and Jerome Hugues examine the design and implementation of embedded computing resources for cyber-physical systems, the complexities of which drive the need for model building.

See more blogs »

Latest Podcasts

The Cybersecurity of Quantum Computing: 6 Areas of Research
Thomas Scanlon discusses how to create the discipline of cyber protection of quantum computing and outlines six areas of future research in the field.

User-Centric Metrics for Agile
Will Hayes, Patrick Place, and Suzanne Miller discuss the importance of user stories in Agile metrics.

See more podcasts »

Latest Publications

Assessing Opportunities for LLMs in Software Engineering and Acquisition
This white paper examines how decision makers can assess the fitness of large language models (LLMs) to address software engineering and acquisition needs.

Mixed-Trust Computing for Real-Time Systems
This paper proposes a real-time mixed-trust computing framework that combines verification and protection.

See more publications »

Latest Videos

Connecting Stakeholders for DoD Software Systems
Hasan Yasar highlights how the upcoming DoD Weapon Systems Software Summit will play a pivotal role in creating effective solutions for securely delivering robust software capabilities on time and on budget.

Cyber Supply Chain Risk Management: No Silver Bullet
Brett Tucker emphasizes using robust enterprise risk management to achieve operational resilience in the cyber supply chain.

Upcoming Events

FloCon 2024, January 9-11, 2024
FloCon centers on improving network security by analyzing a variety of data supported by innovative machine learning, hardware, and network storage.

How Do You Know When You Need a Systems Engineer? January 10, 2024
In this webcast, Suz Miller, Jeannine Siviy, and John Wood will discuss when

and how to introduce fit-for-use systems engineering capability to ensure project success and business value.

Supply Chain Risk Management Symposium 2024, February 28, 2024
Hear about the latest challenges and best practices in SCRM from recognized leaders in SCRM research, as well as leading-edge practitioners from government and industry.

See more events »

Upcoming Training

Cybersecurity Oversight for the Business Executive
January 17-18, 2024 (SEI Live Online)

Insider Risk Management: Measures of Effectiveness
February 20-22, 2024 (SEI Arlington, Va.)

See more courses »

Employment Opportunities

Senior Software Engineer

Cyber Readiness Infrastructure Engineer

Senior Technical Writer & Content Strategist

All current opportunities »

Copyright © 2023 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.