SEI Bulletin

Trouble reading this email? View in browser.

SEI CERT Division Research Supports Cybersecurity Awareness

October 9, 2024—This October, the Cybersecurity and Infrastructure Security Agency (CISA) is once again promoting cybersecurity awareness through its annual Secure Our World campaign. To support cybersecurity awareness within government, industry, and academia, the CERT Division of the SEI presents some recent releases and upcoming events.

SEI Blog Posts

- A Roadmap for Incorporating Positive Deterrence in Insider Risk Management
- 3 API Security Risks and Recommendations for Mitigation

SEI Podcasts

- 3 Key Elements for Designing Secure Systems

- Best Practices and Lessons Learned in Standing Up an AISIRT

Recent Publications

- Counter AI: What Is It and What Can You Do About It?
- Positive Deterrence for Reducing Insider Threat Collection

Upcoming Webcasts

- Cyber Challenges in Health Care: Managing for Operational Resilience

Upcoming Courses

- Insider Threat Program Manager: Implementation and Operation

Follow the CERT/CC for the latest on software vulnerabilities, and report vulnerabilities on their website. You can also report vulnerabilities in artificial intelligence systems to the CERT Division's Artificial Intelligence Security Incident Response Team (AISIRT).

Learn more about the CERT Division »

SEI News

SEI's Grace Lewis Elected IEEE Computer Society President
Lewis, an accomplished SEI researcher on the effects of emerging technology on software engineering, will serve as IEEE Computer Society president in 2026.

DevSecOps Days D.C. 2024 Presentations Now Available
Presentations from the September 18 event feature SBOMs, zero trust, open source projects, and other topics on the integration of security into DevOps.

See more news »

Latest Blogs

Evaluating Static Analysis Alerts with LLMs
Large language models offer possibilities for better vulnerability detection. William Klieber and Lori Flynn discuss initial experiments using GPT-4 to evaluate static analysis alerts.

Measuring AI Accuracy with the AI Robustness (AIR) Tool
Understanding an AI system's predictions can be challenging. SEI researchers discuss a new tool to help improve AI classifier performance.

See more blogs »

Latest Podcasts

3 Key Elements for Designing Secure Systems
To make secure software by design a reality, engineers must intentionally build security throughout the software development lifecycle. Timothy A. Chick discusses building, designing, and operating secure systems.

Using Role-Playing Scenarios to Identify Bias in LLMs
Harmful biases in large language models (LLMs) make AI less trustworthy and secure. Katie Robinson and Violet Turri discuss their recent work using role-playing game scenarios to identify biases in LLMs.

See more podcasts »

Latest Videos

Embracing AI: Unlocking Scalability and Transformation Through Generative Text, Imagery, and Synthetic Audio
Tyler Brooks, Shannon Gallagher, and Dominic Ross aim to demystify AI and illustrate its transformative power in achieving scalability, adapting to changing landscapes, and driving digital innovation.

Latest Publications

Positive Deterrence for Reducing Insider Threat Collection
This collection contains materials related to the SEI's research on organizations' use of positive deterrence to reduce the risk of insider activity.

Counter AI: What Is It and What Can You Do About It?
This paper describes counter AI and provides recommendations on what can be done to defend AI systems in the long term and near term.

See more publications »

Upcoming Events

Webcast - Independent Verification and Validation for Agile Projects, October 23
Justin Smith highlights a novel approach to providing independent verification and validation (IV&V) for projects that are using an Agile or iterative software development.

Webcast - Cyber Challenges in Health Care: Managing for Operational Resilience, October 30
Matthew Butkovic and Darrell Keeling will explore approaches to maximize return on cybersecurity investment in the health-care context.

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

TechNet Indo-Pacific 2024, October 22-24
Visit the SEI at booth 1411.

27th Annual Systems & Mission Engineering Conference, October 28-31
Visit the SEI at booth 8, and hear SEI researchers Lori Flynn, Alexander Vesey, and Jérôme Hugues.

See more opportunities to engage with us »

Upcoming Training

Risk Program Development - Governance and Appetite Workshop
November 13-14 (SEI Arlington, Va.)

Introduction to the CERT Resilience Management Model
December 3-4 (SEI Arlington, Va.)

See more courses »

Employment Opportunities

Senior Machine Learning Engineer - Secure AI Lab

Manager of Public Relations

Program Development Manager

All current opportunities »