SEI Bulletin

Trouble reading this email? View in browser.

SEI Support for President's Cup Leaves Lasting Legacy

January 22, 2025—Each year the President's Cup Cybersecurity Competition identifies and rewards the best cyber professionals in the federal, executive-branch workforce. Since the first event in 2019, the SEI CERT Division has helped the Cybersecurity and Infrastructure Security Agency (CISA) create and update the competition's platform, challenges, and infrastructure.

The conclusion of the fifth competition in April 2024 marked the beginning of the transition of President's Cup support from the SEI to CISA. The agency's new vendor will take over after the SEI runs the first round of the sixth event, which started on January 7. At this moment of change, the SEI looks back on more than five years of collaboration and innovation that created a unique cyber workforce development capability. Many of the President's Cup assets are available in a new collection of the SEI's cyber workforce exercises.

Read more »

SEI News

2024 SEI Research Review Materials Now Available
The event's videos, presentation slides, and posters showcase SEI methods, prototypes, and tools that address the nation's software challenges.

Portend Toolset Creates Guardrails for Machine Learning Data Drift
The SEI's new, open source toolset provides an end-to-end machine-learning assurance solution for simulating drift, detecting it in operation, and generating alerts.

See more news »

Latest Blogs

13 Cybersecurity Predictions for 2025
CERT Division director Greg Touhill presents 13 cyber predictions for 2025.

The Myth of Machine Learning Non-Reproducibility and Randomness for Acquisitions and Testing, Evaluation, Verification, and Validation
A reproducibility challenge faces machine learning (ML) systems today. This post explores configurations that increase reproducibility and provides recommendations for these challenges.

See more blogs »

Latest Podcasts

Securing Docker Containers: Techniques, Challenges, and Tools
Sasank Venkata Vishnubhatla and Maxwell Trdina sit down with Tim Chick to explore issues surrounding containerization, including recent vulnerabilities.

An Introduction to Software Cost Estimation
Software cost estimation is an important first step when beginning a

project. Anandi Hira discusses various metrics, best practices, and common challenges.

See more podcasts »

Latest Videos

Understanding the Need for Cyber Resilience
Matthew Butkovic, Greg Crabb, and Ray Umerley explore how to plan for maintaining operational resilience when a ransomware incident occurs.

See more videos »

Latest Publications

Addressing Today's Software Risks Requires an Assurance-Educated Workforce
Carol Woody summarizes gaps in workforce knowledge, skills, and support resources based on recent publications and panel discussions held by the Software Assurance Supply Chain forum.

Portend
This open source toolset provides an end-to-end machine-learning assurance solution for simulating drift, detecting it in operation, and generating alerts.

Vessel
These open source tools help software developers identify the cause of discrepancies between container builds.

Security Engineering Framework (SEF): Managing Security and Resilience Risks Across the Systems Lifecycle
The SEF is a collection of software-focused engineering practices organized into a hierarchy of goals and domains and includes in-depth guidance.

See more publications »

Upcoming Events

Probing the Limits: A Workshop on Red-Teaming AI Systems, January 28
Participants in this free, hybrid workshop will help identify best practices for red-teaming generative AI systems to extend existing guidance on cyber red teaming.

FloCon 2025, March 4
FloCon is the SEI's annual conference on data-driven security.

See more events »

Upcoming Appearances

AFCEA West 2025, January 28-30
Visit the SEI at booth 3233.

AFCEA Rocky Mountain CyberSpace Symposium 2025, February 10-13
Visit the SEI at booth 335.

See more opportunities to engage with us »

Upcoming Training

Software Architecture Design and Analysis
February 11-14 (SEI Live Online)

Creating a Computer Security Incident Response Team
March 25 (SEI Live Online)

Managing Computer Security Incident Response Teams
March 26-28 (SEI Live Online)

See more courses »

Employment Opportunities

Senior Research Scientist - Advanced Computing Lab

Senior Portfolio Development Manager

Senior Data Engineer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute