SEI Bulletin

Delivering Next Generation Cyber Capabilities to the Warfighter

April 16, 2025—In a new SEI podcast, Gregory Touhill, director of the SEI CERT Division, discusses ways CERT researchers and technologists are working to deliver rapid capability to warfighters in the Department of Defense (DoD), from cyber best practices to artificial intelligence and protecting critical infrastructure.

One of these capabilities was telemetry for optimizing cloud environments, which Touhill said CERT researchers shared with the Department of Homeland Security and the DoD. "[These] capabilities and improvements…helped save taxpayers money because it reduces waste, but it also provides greater insights for the operators there," Touhill said in the podcast Delivering Next Generation Cyber Capabilities to the Warfighter. "As a military professional, I want to be able to outthink, outsmart, and out act our adversaries. With those types of improvements that our researchers are able to provide, we maintain a competitive advantage not only on the military standpoint, but conveying that to our

industry partners, we maintain a competitive advantage in the marketplace as well."

Watch the podcast »

SEI News

New Research Supports SEI AISIRT Mission to Secure Artificial Intelligence
Academia, industry, and the SEI collaborated to illuminate the need for coordinated disclosure of AI vulnerabilities and propose solutions.

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

Radio Frequency 101: Can You Really Hack a Radio Signal?
Recent reports indicate the DoD is susceptible to radio frequency (RF) attacks. Roxxanne White and Michael Bragg discuss common RF tools and ways malicious actors can attack systems.

Evaluating LLMs for Text Summarization: An Introduction
Deploying LLMs without human supervision and evaluation can lead to significant errors. Shannon Gallagher, Swati Rallapalli, and Tyler Brooks outline the fundamentals of LLM evaluation for text summarization in high-stakes applications.

See more blogs »

Latest Podcasts

Delivering Next Generation Cyber Capabilities to the Warfighter
Greg Touhill, director of the SEI CERT Division, discusses ways CERT researchers and technologists are working to deliver rapid capability to warfighters in the Department of Defense.

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.

See more podcasts »

Latest Videos

New Data Exchange Standard Eases Insider Incident Data Collection and Sharing
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.

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.

See more videos »

Latest Publications

Kubernetes (k8s) in the Air Gap
This paper explains how the act of mirroring the required container images

for a k8s deployment in the air gap has become increasingly simplified in the past few years.

Center for Calibrated Trust Measurement and Evaluation (CaTE)—Guidebook for the Development and TEVV of LAWS to Promote Trustworthiness
This guidebook supports personnel in the development and testing of autonomous weapon systems that employ ML, focusing on system reliability and operator trust.

Reference Architecture for Assuring Ethical Conduct in LAWS
This reference architecture provides guidance to reason about designing and developing ML-enabled autonomous systems that have the capability to use lethal force.

Key Takeaways from Zero Trust Industry Day 2024
This paper describes key takeaways from Zero Trust Industry Day 2024, which gathered vendors and partners to propose solutions for implementing zero trust practices in an information technology (IT) and operational technology (OT) systems environment.

See more publications »

Upcoming Events

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."

International Workshop on Envisioning the AI-Augmented Software Development Life Cycle, June 26
This workshop seeks to explore how AI might transform end-to-end software systems development workflows and emphasizes the need to

collect relevant data now to assess the long-term effects of AI throughout the software development life cycle.

Secure Software by Design 2025, August 19-20
Join thought leaders in secure software by design for presentations and discussions on all aspects of secure software systems development.

See more events »

Upcoming Appearances

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.

AFCEA TechNet Augusta 2025, August 18-21
Visit the SEI at booth T825.

See more opportunities to engage with us »

Upcoming Training

Foundations of Incident Management
May 13-16 (Live Online)

Software Architecture Design and Analysis
June 10-13 (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

All current opportunities »

Carnegie Mellon University
Software Engineering Institute