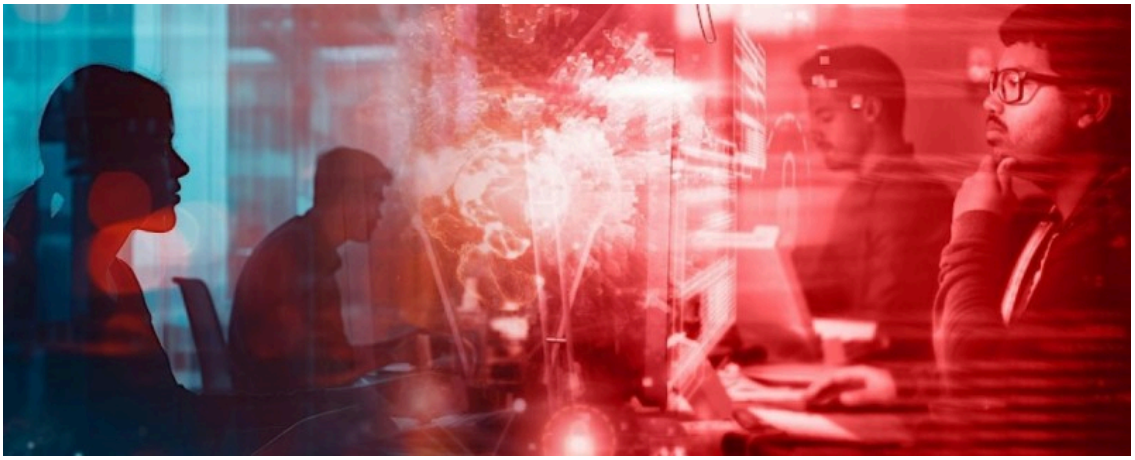
SEI Bulletin 40 years





# Generative AI Red-Teaming Can Learn Much from Cybersecurity Says SEI Study

**September 3, 2025 —** AI practitioners have been red-teaming generative AI systems, but too narrowly for robust security assessments. Established cybersecurity red-teaming methodologies can greatly enhance AI security practices, according to a recent SEI report. *What Can Generative AI Red-Teaming Learn from Cyber Red-Teaming?* analyzes the method in both domains and recommends 10 ways AI security researchers and practitioners can leverage cybersecurity best practices.

“Given the immediacy of the risks surrounding generative AI, the AI security community needs to be deliberate in its efforts to counter threats,” said Keltin Grimes, a researcher in the SEI’s AI Division and a coauthor of the report. “Leveraging insights from more established fields like cybersecurity is a common-sense way to accelerate maturity and maximize impact.”

**Read more »**

## SEI News

SEI Workshop Calls for Actions to Improve Model-Based Systems Engineering in Defense and Intelligence
Defense Department and intelligence community stakeholders met with SEI experts to discuss how software-intensive programs can better implement model-based systems engineering (MBSE).

Study Finds Key Causes of Divergence in Software Bills of Materials
Potential differences in software bills of materials (SBOMs) for an individual piece of software can undermine confidence in these key supply chain documents.

**See more news »**

## Latest Blogs

7 Recommendations to Improve SBOM Quality
There is growing interest in using software bills of materials (SBOMs) to support software supply chain risk management. This post recommends seven ways to improve SBOM accuracy.

Artificial Intelligence in National Security: Acquisition and Integration
This post details practitioner insights from the AI Acquisition workshop, including challenges in differentiating AI systems, guidance on when to use AI, and matching AI tools to mission needs.

Managing Security and Resilience Risks Across the Lifecycle
This post introduces the Security Engineering Framework, a detailed schema of software-focused engineering practices that acquisition programs can use to manage security and resilience risks across the lifecycle of software-reliant systems.

**See more blogs »**

## Latest Podcasts

Understanding Container Reproducibility Challenges: Stopping the Next Solar Winds
Kevin Pitstick and Lihan Zhan discuss Vessel, a recent SEI tool that helps developers identify the difference between two container images to help sort benign from problematic issues.

Mitigating Cyber Risk with Secure by Design
SEI CERT Division director Greg Touhill and Matt Butkovic highlight recommendations, built on prior joint efforts by the SEI and the Cybersecurity Infrastructure Security Agency, for making software secure by design.

**See more podcasts »**

## Latest Publications

History of Innovation at the SEI
This book offers snapshots of the culture of innovation at the SEI from 1988 to 2025 as our researchers and engineers have worked to advance software for national security.

Report on the First MBSynergy Workshop
MBSynergy research focuses on ways of pursuing government equities using model-based systems engineering and digital engineering in DoD and intelligence community settings. This report describes the MBSynergy team's first working session.

Software Bill of Materials (SBOM) Harmonization Plugfest 2024
This report describes how differences in SBOM generation can result in different SBOM outputs.

**See more publications »**

## Latest Videos

Quantum Computing Meets High Performance Computing Skills in the Class
The SEI's Dan Justice and NVIDIA's Monica VanDieren discuss why high-performance computing (HPC) and AI skills are no longer optional for quantum professionals and how to prepare students for the reality of accelerated quantum supercomputing.

Achieving Balance: Agility, MBSE, and Architecture
Peter Capell addresses a practical vision for meeting stakeholder expectations of Agile implementation, highlighting the value of model-based systems engineering and architecture.

Identifying AI Talent for the DoD Workforce
Eric Keylor, Intae Nam, and Dominic Ross go beyond traditional knowledge and skill assessments as they introduce prototype tools that reveal key information about evaluating talent for AI and data positions.

**See more videos »**

## Upcoming Events

Webcast - Using LLMs to Evaluate Code, October 1
Mark Sherman will summarize the results of experiments investigating whether various large language models (LLMs) could correctly identify problems with source code.

AAAI Fall Symposium: Engineering Safety-Critical AI Systems, November 6-8, Arlington, Va.
As AI is increasingly applied to new and more high-risk settings, a mature safety engineering discipline for AI becomes ever more critical. Join the SEI to advance the discipline of engineering AI for safety.

**See more events »**

## Upcoming Appearances

16th Annual Billington CyberSecurity Summit, September 9-12, Washington, D.C.
Hear the SEI's Matthew Butkovic, Christopher Cullen, Lauren McIlvenny, David Schulker, Greg Touhill, Brett Tucker, and Nathan VanHoudnos, and visit the SEI at booth 214.

AFA Air Space Cyber Conference 2025, September 22-24, National Harbor, Md.
Visit the SEI at booth 116.

**See more opportunities to engage with us »**

## Upcoming Training

Software Architecture Design and Analysis
October 14-17 (Live Online)

Risk Program Development - Governance and Appetite Workshop
October 15-16 (Arlington, Va.)

**E-learning -** CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate

**E-learning -** Introduction to Artificial Intelligence (AI) Engineering

**E-learning -** Effective Communication of Technical Concepts

**See more courses »**

## Employment Opportunities

Embedded Software Engineer - Florida
Embedded Software Engineer - Utah
Senior Real-Time Embedded Software Engineer
Embedded Software Engineer

**All current opportunities »**

Carnegie Mellon University
Software Engineering Institute