

Cyber Research for a Secure Tomorrow

CERT—dedicated to cyber research and response

WE ARE THE SOFTWARE ENGINEERING INSTITUTE (SEI), advancing software for national security and critical to the ability of the Department of Defense (DoD) to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

We are one of three collaborative divisions objectively researching complex software engineering, cyber operations, and artificial intelligence (AI); maturing solutions; and facilitating their transition into practice.

We are part of Carnegie Mellon University (CMU), conducting research that moves the world forward.



OUR WORK

Once a Computer Emergency Response Team formed in 1988 in response to the Morris Worm, today the CERT Division leads as a Cybersecurity Engineering and Resilience Team conducting collaborative and innovative evidence-based research to fortify the cyber ecosystem and protect national security and prosperity.

OUR GOALS

- **Advancing Cybersecurity by Design**—Develop and transition evidence-based solutions addressing foundational and enduring challenges
- **Enhancing Cybersecurity Resilience**—Discover and prototype methods to build resilience into existing and future critical infrastructure
- **Influencing the Cybersecurity Marketplace**—Promote more effective, efficient, and resilient methodologies and principles
- **Shaping the Future**—Inform stakeholders of technical priorities and emerging research challenges in partnership with the community

OUR PEOPLE

Researchers

Maturing the disciplines of engineering and secure software systems

Innovators

Creating and prototyping technologies that enable the cyber mission

Collaborators

Applying our expertise with the DoD, government, academia, and private industry

Transitioners

Partnering with CMU, the DoD, and other federal organizations to disseminate our solutions



For more information about the Software Engineering Institute, scan the QR code using your smartphone camera or point your web browser at sei.cmu.edu.

HOW THE SEI WORKS WITH YOU

The SEI takes innovation from concept through research and development and into application. Although we are an R&D center, our contribution doesn't end there; we also make things that software and cybersecurity professionals can use—prototypes, tools, methods, curricula, and more. We research, develop, and apply our work with organizations in...

DoD and government—We fulfill core DoD software engineering needs as a federally funded research and development center (FFRDC). Our research addresses areas that are unmet by in-house and private-sector R&D centers.

The private sector—We combine our expertise with commercial organization expertise, allowing the private sector to achieve strategic advantage by maturing new technology and rapidly applying improved software engineering technology. While all of industry benefits, our commercial R&D sponsors enjoy early access to results they can use to improve development, streamline operations, and gain an edge.

Academia—We leverage our relationship with CMU by contributing to the intellectual capital of the university through research, collaboration, and teaching. Our technical staff maintain close relationships with top researchers and faculty in cybersecurity and software engineering at CMU, and we frequently collaborate with other universities as well. SEI staff publish dozens of papers in academic journals and frequently speak at top conferences in the field.



About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute conducts valued, relevant, and trusted evidence-based research that fortifies the cyber ecosystem and protects national security and prosperity.

HOW TO ENGAGE WITH US

Learn from our training

Attend our eLearning, live online, and in person courses and certificate programs and tackle your cybersecurity challenges in areas such as applied data science, insider risk and threat, secure software by design, and software assurance.

Report a vulnerability

Report security vulnerabilities when a vendor has not responded to your direct contact with them. We work with affected vendors to resolve vulnerabilities in these types of cases.

Use our tools

Conduct forensic examinations, analyze vulnerabilities, monitor large-scale networks using flow data, and more using our tools and methods.

Request an assessment

Gauge your exposure to insider threat with CERT Insider Threat Vulnerability Assessments. Evaluate your organization's operational resilience using the CERT-RMM Capability Appraisal assessment. Analyze the C code in your software using SCALe Conformance Analysis.

Get involved with our research

Explore our research, collaborate with us, or join our team to study and solve problems that have widespread implications for cybersecurity.

Attend an event

Participate in our events including the Insider Risk Management Symposium, which shares successes and challenges of mitigating insider risks; Secure Software by Design, which promotes all aspects of secure software systems development; and NatCSIRT, which convenes CSIRT organizations responsible for protecting the security of nations, economies, and critical infrastructures.

Explore our blogs, videos, podcasts, and webinars.

Subscribe to the SEI Bulletin to get SEI news, events, and research in your inbox and the SEI Blog to read our researchers' latest insights on cyber. Our SoundBytes provide short videos on current cyber topics. Our podcasts and webinars cover topics that include DevOps, insider threat, secure coding, and improving your security program.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu