Carnegie Mellon University
Software Engineering Institute

# TRUSTED. VALUED. RELEVANT.

The CERT Division is the birthplace of cybersecurity, strengthening the resilience of systems and networks.

**WE ARE PART OF THE SOFTWARE ENGINEERING INSTITUTE (SEI),** bringing innovation to the U.S. government. Since 1984, the SEI has been critical to the government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

We are one of three collaborative divisions researching complex software engineering, cyber operations, and artificial intelligence (AI) engineering solutions; creating and piloting innovative technologies; and transitioning maturing solutions into practice.

We are part of Carnegie Mellon University (CMU), pioneering discoveries that enrich the lives of people on a global scale. We turn disruptive ideas into successes through leading-edge research.

## 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 academia, government, and private industry

**Transitioners**
Partnering with CMU to disseminate our solutions

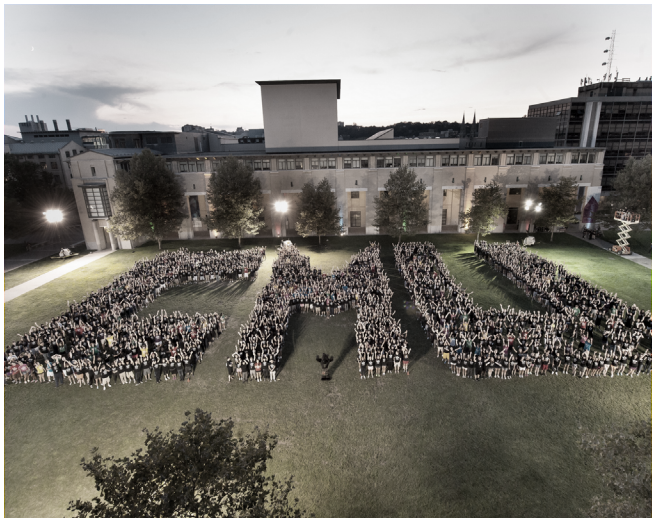
## HOW THE SEI WORKS WITH YOU

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 …

**The private sector—**Commercial organizations achieve strategic advantage by rapidly applying improved software engineering technology. We combine our expertise with yours to mature new 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.

**Government—**As a federally funded research and development center (FFRDC), we fulfill core DoD software engineering needs that are unmet by in-house and private-sector R&D centers.

**Academia—**As part of the CMU community, the SEI contributes 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.



## HOW TO ENGAGE WITH US

**Learn from our training**

Available as eLearning, live online, and in person, our cybersecurity courses and certificate programs help you tackle cybersecurity challenges in areas such as insider threat, DevOps, 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**

Our tools and methods help you conduct forensic examinations, analyze vulnerabilities, monitor large-scale networks using flow data, and more.

**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. Evaluate the C code in your software using SCALe Conformance Analysis.

**Get involved with our research**

We study and solve problems that have widespread implications for cybersecurity. You can explore opportunities to sponsor our research, collaborate with us, or join our team.

**Attend an event**

We sponsor events including FloCon, a network security conference where attendees discuss the next generation of flow-based analysis techniques; the National Insider Risk Management Symposium, which assembles information about mitigated insider risks to share successes and challenges; and NatCSIRT, where CSIRT organizations responsible for protecting the security of nations, economies, and critical infrastructures meet.

**Explore our blogs, cyber-minute videos, podcasts, and webinars**

Our researchers publish their insights on the SEI blog. Cyber minutes provide short videos on current cybersecurity topics. Our podcasts and webinars cover topics that include DevOps, insider threat, secure coding, and improving your security program.

## About the CERT Division

The CERT Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

## 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