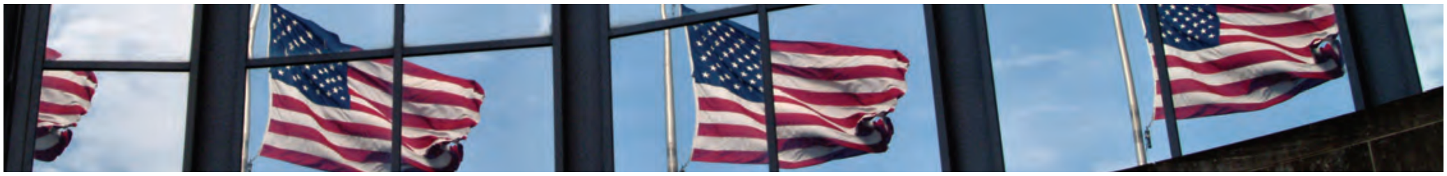
The SEI's CERT Division: Leaders in Cybersecurity

Knowledge, Experience, Impact

CERT | Software Engineering Institute | Carnegie Mellon University



Overview

At the CERT Division of Carnegie Mellon's Software Engineering Institute (SEI), we research and analyze cybersecurity in its many forms. We discover and address software vulnerabilities, develop approaches that measure and mitigate risk, and research how cyber attackers behave. We also research ways to improve incident response practices, investigate ways to identify and mitigate cyber threats from insiders, improve data monitoring for measuring adversary activity, and devise strategies for developing and maintaining a prepared cyber workforce.

We help organizations determine how effective their security-related practices are. To help others benefit from our work, we develop tools, products, methods, and training to help organizations conduct forensic examinations, analyze vulnerabilities, and monitor large-scale networks.

The Value of Knowledge and Experience

Our researchers, software engineers, security analysts, and other cybersecurity experts rely on theoretical and empirical knowledge to understand security problems. As part of our scientific research, we collect real-world data to gain insight into today's pressing problems.

Our connection to the internationally known Carnegie Mellon University creates multi-disciplinary collaboration opportunities and strengthens our research focus. We are also part of the SEI, a federally funded research and development center, and thereby contribute to national security efforts, including research and development for our sponsor, the Department of Defense.

We work with many other organizations as well, including the U.S. Department of Homeland Security; federal, state, and local governments; multiple levels of law enforcement; the intelligence community; operators of critical infrastructures; and many industry organizations.

Our Work

Security-Aware Acquisition. Address vulnerabilities and plan for threats earlier and more effectively in the acquisition lifecycle

Secure Development. Assess platforms through the analysis of source code to assure they adhere to security best practices

System and Platform Evaluation. Assess software, devices, systems, and platforms of unknown design or origin to find vulnerabilities and strategies for defending against possible attacks

Threat-Aware Sustainment. Reduce exposure to known vulnerabilities in systems

Enterprise Risk Management. Develop measurable practices and frameworks that enable organizations to measure and mitigate risks

Network Situational Awareness. Analyze the cyber terrain as it evolves to characterize assets at risk, measure adversary activity, and prioritize responses to threat

Cyber Intelligence. Study and describe the behaviors and capabilities of cyber attackers and identify the properties of their methods

Digital Forensics. Enable and improve incident response and analysis practices used by organizations as the technology landscape and sophistication of adversaries evolve

Insider Threat. Detect and mitigate the impact of insider threats and reduce their occurrence in organizations

Cyber Operator Development. Develop and maintain a well-equipped cyber workforce that is immediately able to support the cybersecurity needs of organizations

Cyber Center Development. Develop measurable and repeatable practices to prepare CSIRTS and other operational security organizations

Our Mission

We support the nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

Our Experience and Collaborations

Cyber Lightning Exercise Helps Reserve Units Learn and Test Skills

Cyber Lightning, a three-day training exercise designed and directed by CERT experts, provides innovative cyber defense training to Air Force Reservists and Guardsmen from Pennsylvania and Ohio.

In this low-cost exercise, participants learn and test their new cybersecurity skills in an environment that simulates real DoD networks. Cyber Lightning helps the Air Force and Air National Guard develop a capable, well-prepared cyber workforce.

CERT Contributes to Crisis Simulation Exercise

CERT researchers developed a cybersecurity exercise that uses video, live action, fictional websites, and a fully functional simulated Internet environment on the Simulation, Training, and Exercise Platform (STEPfwd).

The exercise was presented at an event that brought together organizations in the government, military, and industry sectors. Participants were given a simulated threat and tasked with assessing it and putting it into context for decision makers. For the exercise, CERT researchers created large, simulated networks for participants to explore and authored custom malware for the "threat actors" to use. CERT researchers also contributed a flow data analysis component as part of the exercise.

CERT Data Characterizes the Insider Threat Problem

Much of CERT insider threat research builds on the CERT insider threat database, which documents thousands of facts about insider threat cases. CERT researchers use modeling to characterize the insider threat problem, explore indicators of insider threat risk, and identify and experiment with controls for mitigating insider threat. At the CERT insider threat lab, researchers identify, tune, and package technical controls as an extension of their modeling efforts. CERT researchers use this same data to help organizations identify their technical and nontechnical vulnerabilities to insider threats.

Our Collaborations Benefit Government and Private Sector Organizations

In other work with government and private-sector organizations, CERT researchers provided new malware analysis capabilities to aid these organizations in defending themselves against malware attacks.

Researchers also performed high-value assessments and provided remediation recommendations to address a large data breach affecting personally identifiable information. Other CERT researchers developed next-generation cyber attack forecasting techniques. Still others provided critical support to help organizations meet the software assurance needs of their cybersecurity programs.

USPS Improves Its Cybersecurity and Resilience

CERT researchers worked with the CISO of the United States Postal Service (USPS) on two projects that helped the USPS improve its cybersecurity and resilience. The first was a cybersecurity strategy that integrated recommendations into strategic improvement initiatives. Using the CERT Resilience Management Model (CERT-RMM), CERT researchers developed metrics to track progress, an essential element in executing the USPS strategy.

The second project prepared USPS employees for cybersecurity issues. CERT and the USPS collaborated to form the CISO Academy, a new cybersecurity workforce training program. Its curriculum includes tracks for program managers and technical staff. Courses are delivered through CERT's STEPfwd and the Federal Virtual Training Environment (FedVTE). CERT researchers are continuing their cyber workforce development research by investigating and measuring the impact of how other organizations strengthen their cybersecurity teams and culture.

Engage with Us

Learn from our training. Available online and in person, our cybersecurity courses and certificate programs help you tackle cybersecurity challenges in areas such as insider threats, DevOps, and software assurance.

Report a vulnerability. Report security vulnerabilities when the 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 threats with CERT's 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 Analyses.

Attend an event. We sponsor FloCon, a network security conference where attendees discuss the next generation of flow-based analysis techniques; the Insider Threat Symposium, an event that assembles those mitigating insider threats to share their successes and challenges; NatCSIRT, where CSIRT organizations responsible for protecting the security of nations, economies, and critical infrastructures meet to discuss their unique issues; and the Secure Coding Symposium, where attendees discuss software assurance and secure coding.

Explore our blogs, cyber minute videos, podcasts, and webinars. Our researchers publish their insights on the CERT/CC, DevOps, and Insider Threat blogs. 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.

Join the CERT Secure Coding wiki. Read and contribute to our CERT secure coding wiki, where you can work with CERT researchers to develop new standards. Learn to develop more secure code using our coding standards for C, C++, Java, and Perl.

Benefit from CERT-developed curricula and course materials. CERT experts research how to address security and survivability by developing curricula and educational materials. Recognized by the IEEE Computer Society and ACM, these assets are used by educational institutions in their degree programs and by commercial and government institutions in their employee training programs.

Get involved with our research. We study and solve problems that have widespread implications for cybersecurity. There are plenty of opportunities to sponsor our research or collaborate with us.

Join our team. Your top-notch skills and knowledge can help us make a difference in our nation's cybersecurity.

To learn about these opportunities and CERT research, visit our website at www.cert.org.

Our collaborative work environment enables our staff to participate in cross-functional teams in the CERT Division, the SEI, other Carnegie Mellon departments, and across the global community.

About Us

For nearly 30 years, the CERT Division of the SEI at Carnegie Mellon University has been a leader in cybersecurity. Originally focused on incident response, we have expanded into cybersecurity areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threats, digital investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu