



Carnegie Mellon University Software Engineering Institute CERT® Division

Build. Assure. Defend.

Firstname Lastname

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM21-0474

Carnegie Mellon Leads an Ecosystem of Innovation for Cybersecurity



- Global research university known for its world-class, interdisciplinary programs in computer science, machine learning and artificial intelligence, engineering, business, arts, policy, and science
- Ranked #1 for Computer Science, #1 for Artificial Intelligence, #4 in Engineering (*U.S. News and World Report*)
- 1,400+ total faculty and 130 research centers
- CyLab, CMU's security and privacy research institute, brings together experts from all schools across the university

CMU Software Engineering Institute (SEI)



- Founded in 1984 by the DoD as an FFRDC focused on software engineering
- Leader in software engineering, cybersecurity, and AI research
- Non-degree granting college-level unit of CMU
- Established CERT in 1988
- Critical to the DoD ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring
- CMU retains ownership of intellectual property; the U.S. government enjoys a free-to-use license

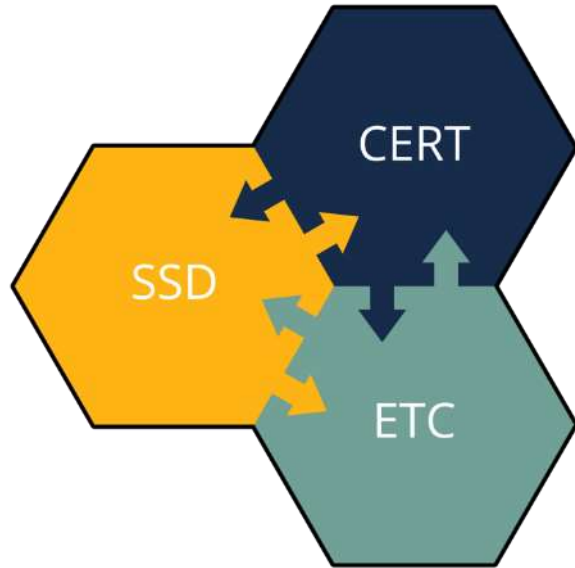
CERT Division



- Has a unique combination of experiential understanding of DoD missions, network operations, and constantly changing technology
- Applies the best science to impact operational missions, increase the trustworthiness of technology, and develop cyber talent
- Strengthens the resilience of critical national functions, increases the cybersecurity and resilience of systems and the Defense Industrial Base, and develops the cyber capacity of allies and partners

CERT Division and the SEI's Interlocking Technical Objectives

[optional non-DoD, non-USG customer slide]



CERT Division

- Build innovative technologies to defend against cyber attacks
- Assure the security and resilience of critical capabilities
- Defend against current and emerging threats

Emerging Technology Center

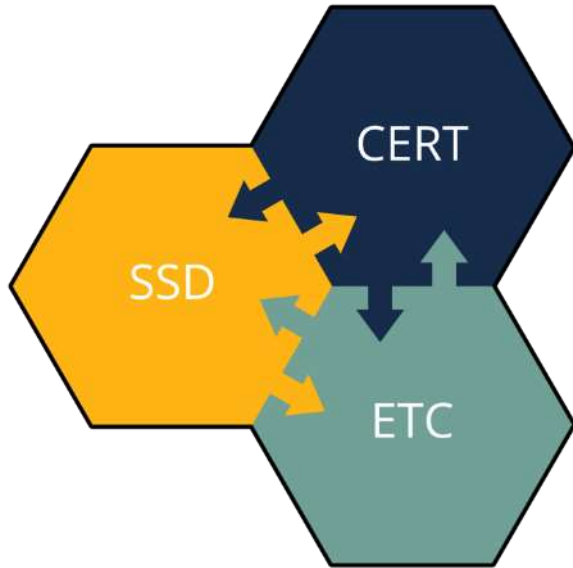
- Applied artificial intelligence and machine learning
- Advanced computing
- Human-machine interaction

Software Solutions Division

- Engineering intelligent software systems
- Software innovation for mission capability
- Software policy and practice to accelerate acquisition

CERT Division and the SEI's Interlocking Technical Objectives

[optional DoD customer slide]



CERT Division

- Build secure and resilient operational capabilities
- Assure operational resilience and readiness to defend
- Defend against threats with advanced technologies

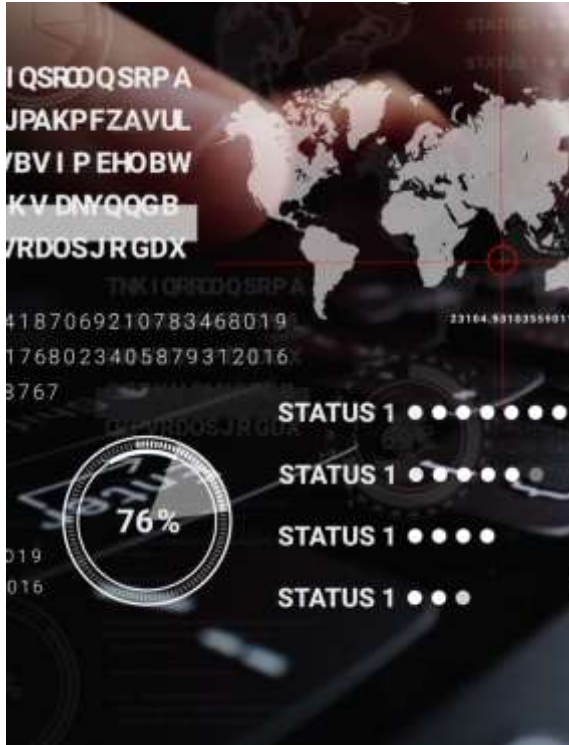
Emerging Technology Center

- Applied artificial intelligence and machine learning
- Advanced computing
- Human-machine interaction

Software Solutions Division

- Engineering intelligent software systems
- Software innovation for mission capability
- Software policy and practice to accelerate acquisition

CERT Division – Conducting Cybersecurity R&D



Engineering for cybersecurity

Security and resiliency engineering, software security assurance, prototype tools for emerging challenges

Improving enterprise cyber resilience

Risk management, assessment, security operations, insider threat, network situational awareness

Understanding and countering threat

Malware analysis, vulnerability analysis, platform evaluation

Developing the cyber workforce

Rapid cyber skills acquisition, modeling and simulation

Strengthening the foundations of cybersecurity

Data analytics, AI, formal methods

Engineering for Cybersecurity



Security and resiliency engineering

- Apply security engineering risk analysis, expose and mitigate cyber risk, and reduce cost
- Increase confidence in resilience against cyber attack by designing in cyber defense mechanisms

Software security assurance

- Apply software assurance methods and tools to define, validate, and verify software security requirements
- Develop robust, attack-resistant code using secure coding standards
- Identify and mitigate risks to the software supply chain

Prototype tools for emerging challenges

- Validate design assumptions with operational prototypes

Improving Enterprise Cyber Resilience



Risk management

- Ensure that processes and frameworks measurably increase confidence in risk management for operational readiness

Assessment

- Build automated diagnostic tools that provide verifiable confidence in the effectiveness and resilience of cyber-dependent missions

Security operations

- Enable organizations to respond to cyber threats
- Improve cybersecurity capacity building

Insider threat

- Reduce the impact and likelihood of insider attacks

Network situational awareness

- Quickly detect and respond to system and network security risks with state-of-the-art processes and tools

Understanding and Countering Threat



Malware analysis

- Develop tools that analyze malware
- Curate collections of malware, attacker tools, and exploits
- Enable development of survivable computing and survivable systems

Vulnerability analysis

- Develop technologies and practices to identify, analyze, and remove code that causes unintended effects in software systems
- Curate collections of vulnerabilities
- Coordinate vulnerability disclosure and response

Platform evaluation

- Analyze commercial technology
- Develop tooling to examine technology platforms
- Help organizations understand the relevance and behavior of current technology platforms

Developing the Cyber Workforce



Rapid cyber skills acquisition

- Build and improve the cybersecurity workforce
- Rapidly accelerate acquisition of cyber knowledge, skills, and experience
- Develop learning methods and analytics to assess capacity, capability, and effectiveness
- Validate methods of effective learning for cyber

Modeling and simulation

- Develop cutting-edge open-source tools and methodologies
- Create and test realistic simulations for operational test and rehearsal
- Create learning content that interweaves multimedia information with realistic, scenario-based simulations
- Enable operational tests and rehearsals with reusable infrastructure and scenario-event designs

Strengthening the Foundations of Cybersecurity



Data analytics

- Leverage growing data sets and rapidly evolving technologies including social media, live streaming, real-time analytics, and machine learning
- Use AI to detect malicious activity and automate cyber threat analysis

AI

- Evaluate and advance AI-based capabilities for network defense
- Develop verification and validation for ML components used in behavioral analysis

Formal methods

- Develop metrics and measurement methods
- Support evidence-based policy making

Example Work Products



Technical and Process-Driven Solutions: Novel solutions that include prototype software, proprietary risk and resiliency methodologies, and evaluative frameworks for assessing commercial technologies



Training and Exercises: A wide array of cybersecurity-focused workforce development offerings such as gap-area technical training content, in-person and distance delivery options, and extensive modeling and simulation capabilities to test organizational readiness



Analysis and Recommendations: Written artifacts detailing original SEI research, independent analysis, and findings at varying levels of technical depth answering organizations' questions and addressing organizations' challenges

Engage with Us

[optional STE customer slide]



- SEI is managed by CMU as an FFRDC under Air Force Contract Number FA8702-15-D-0002
- Contract is a cost-reimbursement, no-fee instrument with Federal Acquisition Regulation clauses and provisions appropriate for research and development work
- Air Force agencies fund via AF Form 9 or AFMC Form 36; other DoD agencies fund via DD Form 448, Military Interdepartmental Purchase Request
- Congressionally allocated STE (Staff years of Technical Effort) limits the amount of DoD work undertaken

Engage with Us

[optional non-DOD customer slide]



- SEI is managed by CMU as an FFRDC under Air Force Contract Number FA8702-15-D-0002
- Contract is a cost-reimbursement, no-fee instrument with Federal Acquisition Regulation clauses and provisions appropriate for research and development work
- Non-DoD agencies fund via an Inter-Agency Agreement using FS Form 7600A and 7600B (U.S. Treasury forms)
- Non-DoD agencies must complete a Non-DoD Agency Review (NDAR) form to address issues related to human-subject research, export control, conflicts of interest, and privacy review before beginning work

Engage with Us

[optional non-USG customer slide]



- SEI is managed by CMU as an FFRDC sponsored by the U.S. Department of Defense
- The SEI DoD sponsor reviews all prospective work to ensure that it is consistent with the SEI charter as an R&D-focused FFRDC
- The SEI often collaborates with commercial organizations to help them apply improved software engineering technology
- The U.S. government has a royalty-free government-purpose license to use, duplicate, or disclose works authored by the SEI and permit others to do so
- SEI technologies may be licensed for commercial use

Engage with Us



Download [software and tools](#)

Participate in [education](#) offerings

Attend an [event](#)


Search the [digital library](#)

Read the [SEI Year in Review](#)

Explore our [research and capabilities](#)

[Collaborate](#) with the SEI on a new project

Contact Us



Presenter
Photo

Presenter Name

Carnegie Mellon University
Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213

888-201-4479

info@sei.cmu.edu

www.sei.cmu.edu