Carnegie Mellon University Software Engineering Institute CERT® Division

Build. Assure. Defend.

Jamie Lord, Technical Manager, Security Operations
Mark Sherman, Technical Director, Cybersecurity Foundations
Matthew Butkovic, Technical Director, Risk and Resilience

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM21-0531

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 in Cybersecurity, #1 in Artificial Intelligence, #1 in Software Engineering, #1 in Computer Engineering, #2 in Computer Science and #3 in Data Analytics/Science (*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

Customers

CERT Division supports improving security for

- US Department of Defense
- US Department of Homeland Security – Cyber and Infrastructure Security Agency
- US Department of Energy
- US Department of State
- National CERT teams worldwide
- Industrial consortia in the United State and Internationally
- Private industry

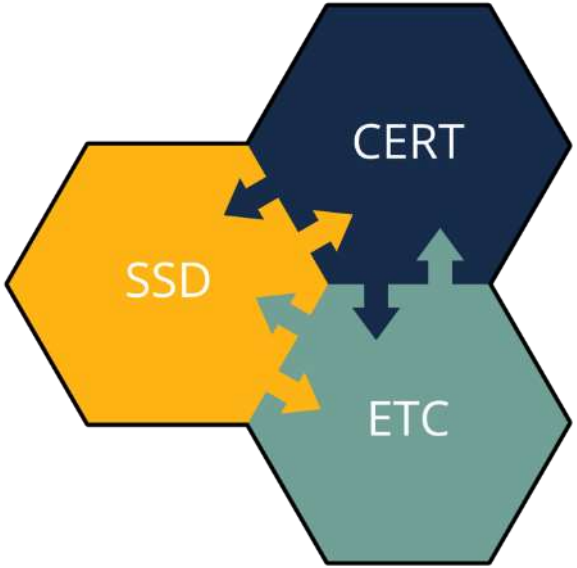
Engagements in Eastern Europe

- Moldova (CERT-GOV-MD)
- Albania (AKCESK, formerly ALCIRT)
- Serbia (SRB-CERT)
- Kosovo (KOS-CERT)
- Ukraine (Ukrainian National Bank (NBU))
- Republic of North Macedonia (MKD-CIRT)
- Western Balkans Working Group
- Bank for International Settlements

The Caucasus

- Georgia (CERT-GOV-GE)
- Armenia (CERT.AM)

CERT Division and the SEI's Interlocking Technical Objectives



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 – Conducting Cybersecurity R&D

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

Strengthening the foundations of cybersecurity
Data analytics, AI, formal methods

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

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

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

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

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

Jamie Lord, Technical Manager, Security Operations
Mark Sherman, Technical Director, Cybersecurity Foundations
Matthew Butkovic, Technical Director, Cyber Risk and Resilience

Carnegie Mellon University

Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213

888-201-4479

info@sei.cmu.edu

www.sei.cmu.edu