Carnegie Mellon University
Software Engineering Institute

SEI Zero Trust Industry Days 2024

MAY 14–15, 2024 | SOFTWARE ENGINEERING INSTITUTE, PITTSBURGH, PENNSYLVANIA AND VIRTUAL

Join Us to Share Your Zero Trust Solutions

CARNEGIE MELLON UNIVERSITY'S (CMU'S) SOFTWARE ENGINEERING INSTITUTE (SEI) IS HOSTING ITS ANNUAL ZERO TRUST INDUSTRY DAYS to collect information from those who develop solutions for implementing a zero trust (ZT) architecture. Contribute your ideas, solutions, and experiences to help organizations form a ZT implementation that meets their mission goals, budgets, and time frame.

Ideas We're Looking for

SEI Zero Trust Industry Days 2024 will be a request for information (RFI) that focuses on addressing the following six guidance documents:

- **OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles**[1]
- **OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents**[2]
- **CISA Zero Trust Maturity Model, Version 2.0**[3]
- **National Cybersecurity Strategy**[4]
- **DoD Zero Trust Strategy**[5]
- **CISA Zero Trust Implementation Strategy**[6]

Presenters We're Looking for

We need participants from established providers of ZT solutions—vendor organizations, Federally Funded Research and Development Centers (FFRDCs), other research organizations, and other solution providers—to apply to present at SEI Zero Trust Industry Days 2024. Twelve accepted presenters will develop and propose a solution for a scenario we provide. This scenario involves a chip manufacturing company starting its ZT journey on an island, where there may be loss of connectivity and cloud services for short or extended periods of time.

Format

During the two-day hybrid event, individuals from 12 organizations will present their proposals and participate in one of two panel discussions. A keynote presentation will start each day, and a wrap-up session will end each day.

For more information about the SEI, scan the QR code using your smartphone camera or point your web browser to **sei.cmu.edu**.

How to Participate

Upload your information using **Sessionize**[7] to request to be a presenter and explain how you can contribute to the ZT conversation. Once we vet and approve your request, we will notify you and ask you to complete the following activities within 30 days:

1. Develop a proposal that meets the requirements specifically selected from the five guidance documents listed earlier.
2. Address common budget concerns when implementing ZT solutions.
3. Create a set of artifacts that support your proposal. (See the list of recommended artifacts in the next section.)
4. Create a 60-minute presentation that describes your proposal.

Artifacts Supporting Your Proposal

We suggest that you develop the following artifacts as part of your ZT implementation to support your presentation:

- a ZT cybersecurity architecture strategy
- ZT roadmaps, one for near term (0-2 years) and another for long term (3-5 years) that address the five guidance documents listed earlier
- a ZT implementation plan that addresses the following:
  - Internet of Things (IoT) and Industrial IoT (IIoT) in ZT—What considerations do industrial technologies bring, and how are they relevant in the implementation of ZT?
  - Legacy Systems—What concerns do legacy systems bring, and how might the ZT implementation address those concerns?
  - Smart City—How does a ZT implementation mitigate threats and vulnerabilities in highly connected systems, such as smart cities?
  - Connected Services—How are identity, credential, and access management (ICAM) service capabilities managed when there is a disruption to cloud-hosted services?
  - Manufacturing Concerns—What considerations must be in place for ZT implementations in manufacturing environments concerning the accessibility and availability of the facility generally and in a disaster?
- impact on the organization's training needs to implement your proposal
- total cost of operation, including anticipated costs, potential cost savings, and ongoing support and maintenance costs
- the effect on users (e.g., how they log in, the work flows they follow, the types of information that will be logged and monitored)

1 **https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf**

2 **https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf**

3 **https://www.cisa.gov/zero-trust-maturity-model**

4 **https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**

5 **https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf**

6 **https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf**

7 **https://sessionize.com/application-deadline-for-sei-zero-trust-2024/**

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

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