Carnegie Mellon University
Software Engineering Institute

SEI Zero Trust Industry Days 2023

OCTOBER 25-26, 2023 | 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 architecture. Contribute your ideas, solutions, and experiences to help organizations form a zero trust implementation that meets their mission goals, budgets, and time frame.

Ideas We're Looking for

Zero Trust Industry Days 2023 will be a request for information (RFI) that focuses on addressing the following five 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]

Presenters We're Looking for

We need 12 volunteers from established providers of zero trust 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 2023. Accepted presenters will develop and propose a solution for a scenario we provide. This scenario involves a company setting up a chip manufacturing facility on an island, where there may be loss of connectivity and cloud services for short or extended periods of time.

Format of Zero Trust Industry Days 2023

During the two-day hybrid event, volunteers 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 CMU SEI, scan the QR code using your smartphone camera or point your web browser to **sei.cmu.edu**

How to Volunteer

Upload your information using **Sessionize**[6] to request to be a presenter and explain how you can contribute to the zero trust 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 four guidance documents listed earlier.
2. Ensure that the proposal stays within the budget provided in the scenario.
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 recommend that you develop the following artifacts as part of your zero trust solution:

- a cybersecurity architecture strategy
- zero trust roadmaps, one for near term (0-2 years) and another for long term (3-5 years) that address the four guidance documents listed earlier
- a zero trust implementation plan that
  - –identifies, prioritizes, and addresses the risks the organization will face as it implements its strategy and roadmap
  - – identifies possible implementation alternatives with their advantages and disadvantages
- 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://sessionize.com/application-deadline-for-sei-zero-trust-2023/**

About the CERT Division

The CERT® Division of Carnegie Mellon University’s Software Engineering Institute conducts valued, relevant, and trusted evidence-based research that fortifies the cyber ecosystem and protects national security and prosperity.

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