Carnegie Mellon University
Software Engineering Institute

SEI Zero Trust Industry Day

Join Us to Share Your Zero Trust Solutions

THE SOFTWARE ENGINEERING INSTITUTE (SEI) IS HOSTING THIS ZERO TRUST INDUSTRY DAY to collect information from those who develop solutions for implementing a zero trust architecture. Contribute your ideas, solutions, and experiences to help government agencies form a zero trust implementation that meets their mission goals, budget, and time frame.

The SEI Zero Trust Industry Day is a request for information (RFI) exercise. This two-day exercise will be held in a hybrid environment at the SEI in August 2022. It will focus on how agencies can comply with the guidance in the following Office of Management and Budget (OMB) memoranda:

- **M-22-09—Moving the U.S. Government Toward Zero Trust Cybersecurity Principles**
- **M-21-31—Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents**

Interested in Presenting?

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. If you choose to volunteer, you will present a proposal in response to this scenario: *A federal agency with finite labor resources, time, and budget must plan for and implement a zero trust architecture. The agency's operating environment includes and requires protection of government-owned on-premises information technology (IT), operational technology (OT), industrial control systems (ICS), and Internet of Things (IoT) equipment; data in hybrid cloud environments (including software-as-a-service [SaaS] platforms); a heterogenous endpoint environment; and a distributed, remote workforce.* You may also be asked to participate in one of four panel discussions. The industry day will also include two keynote presentations and a wrap-up session.

How to Volunteer

Upload your information using **Sessionize** to request to be a presenter and explain how you can contribute to the zero trust conversation. Once we vet and approve your request, you will be notified, given more details about the scenario, and asked to complete the following activities across a 30-day period:

- Develop a proposal that meets the requirements specifically selected from the two OMB memoranda listed above.
- Ensure that the proposal stays within the budget provided.
- Create a set of artifacts that support your proposal. (See the list of recommended artifacts in the next section.)
- Create a 30-minute presentation that describes your proposal.

Artifacts Supporting Your Proposal

To support your proposal, you must develop artifacts. Consider selecting from the following artifacts, which are particularly valuable to government agencies implementing a zero trust architecture:

- a cybersecurity architecture strategy
- near-term (0-2 year) and long-term (3-5 year) zero trust roadmaps that address the following guidance:
  - **OMB M-22-09**
  - **OMB M-21-31**
  - **CISA Maturity Model**
  - **CISA TIC 3.0 Guidance**
  - **CISA Cloud Security Technical Reference Architecture**
- a list of potential risks the organization might face when moving to a zero trust environment
- an implementation plan that addresses and prioritizes those risks
- projected training needs for both end users and supporting technical staff members
- projected total cost of operation, including anticipated costs, the potential for cost savings, and ongoing support/maintenance costs
- the effect on users (e.g., how they log in, the workflows they follow, the types of information that will be logged and monitored)

More Information

If you have questions or need more information about being a presenter or about the Zero Trust Industry Day itself, send email to **info@sei.cmu.edu**.

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