



Advanced Technology Academic Research Center

WASHINGTON, D.C. – The Advanced Technology Academic Research Center (ATARC) is thrilled to announce the official launch of the Training Track and Use Cases as part of ATARC's Zero Trust Lab Phase 3 initiative. This latest milestone underscores ATARC's commitment to driving innovation in cybersecurity and equipping professionals with the knowledge and tools needed to implement robust Zero Trust principles effectively.

In Phases 1 and 2, ATARC established a collaborative platform where vendors, integrators, and teams demonstrated solutions to real-time challenges across **eight** key technology tracks: **Artificial Intelligence (AI), DevSecOps, Metrics, Mobility, Multi-Cloud, Operational Technology, Quantum, and Training**. These efforts addressed critical gaps in Zero Trust implementation, paving the way for Phase 3's focus on specialty areas.

Phase 3 not only expands on this foundation but also introduces a groundbreaking people-centric approach to cybersecurity. It acknowledges the necessity of an empowered workforce in a Zero Trust Architecture and prioritizes training as an essential pillar of modern data protection strategies.

Objectives of the Zero Trust Lab Phase 3

The lab's objectives include:

- Educating government and industry teams on transitioning to a data-centric security model.
- Highlighting strategies for mitigating threats such as credential theft and data compromise by adversarial actors.
- Providing training insights that address the confidentiality, integrity, and availability of organizational data.
- Supporting operational technology systems to protect control data that could have physical impacts.

A Shift to People-Centric Cybersecurity

Twenty-five years ago, Bruce Schneier emphasized the importance of People, Process, and Technology (PPT) in securing a connected world. While the first two phases of ATARC's Zero Trust Labs focused on technological advancements, Phase 3 shifts the spotlight to the workforce—addressing the need to train and empower individuals to play an active role in data security.

This new approach transitions from a network-focused model, where cybersecurity teams serve as gatekeepers, to one where every individual within an organization helps protect valuable data at appropriate levels.

Why This Matters Now

“At a time when adversaries are increasingly targeting U.S. government, industry, and partner networks, it is vital to equip our workforce with the skills and mindset to secure data,” said Dr. Amy Hamilton, Faculty Chair, National Defense University and Government Chair, ATARC’s Zero Trust Lab. “This lab provides actionable insights into workforce training opportunities that align with a zero-trust approach, emphasizing the role of people in safeguarding data.”

As cyberattacks increasingly target U.S. government, industry, and partner networks, the Zero Trust Lab Phase 3 provides actionable insights and training opportunities to align workforce practices with zero-trust principles. This initiative underscores the urgency of strengthening cybersecurity through education and collaboration.

Join the Movement

ATARC invites agencies and organizations to invest in their workforce’s ability to secure data across complex environments. Under the guidance of **Dr. Amy Hamilton**, the Government Chair for this training track, participants will gain valuable insights and expertise to strengthen their cybersecurity posture. Join the conversation on advancing cybersecurity by participating in the Zero Trust Working Group and contributing to the future of secure digital transformation.

Email us at workinggroups@atarc.org or visit <https://atarc.org/working-groups/zerotrustworkinggroup/>.

Training Track Use Cases

As part of the Zero Trust Lab Phase 3, the Training Track focuses on delivering practical, actionable frameworks for workforce development:

Use Case 1: Zero Trust Computer-Based Training (CBT) for Distributed Employees

A training officer must deliver on-demand Zero Trust CBT to employees across various locations, both domestic and international. The training should cater to senior leadership, program management, and tactical operational staff, be accessible via a web-based Learning Management System (LMS), and comply with accessibility standards.

Use Case 2: Remote Zero Trust Training for Dispersed Employees

The training officer is tasked with providing remote Zero Trust training to employees located across the U.S. and abroad. Training sessions must accommodate participants in multiple locations, offer materials in advance due to potential access limitations, and ensure attendance tracking. Access via phone and online platforms is essential.

Use Case 3: In-Person Zero Trust Training Facilitation

Facilitating in-person Zero Trust training requires the training organization to prepare sessions for all staff levels in both secure and non-secure environments. Presentation materials may need prior security reviews before distribution in secure facilities.

Use Case 4: Hybrid Zero Trust Training Delivery

The training officer must conduct hybrid Zero Trust training sessions with some staff attending onsite and others remotely. Materials should be accessible to all attendees, regardless of technical access or location, with provisions for those without live internet access, potentially requiring physical training packets distributed in advance.

These use cases guide training organizations in developing adaptable Zero Trust curricula for diverse organizational roles and training formats. For more information on the Training Track or to access the published use cases, visit: [ATARC Zero Trust Lab Phase 3 – Training Track Use Cases](#)

Media Contact:

Maddy Mitschke

Associate Director, Marketing and Media

mmitschke@atarc.org