# ATARC Zero Trust Lab: Phase 3 Zero Trust Artificial Intelligence AI Track

https://atarc.org/zt-lab-phase-3_ai-track/

Dr. Amy Hamilton, Leadership Chair, Department of Energy, National Defense University, College of Information & Cyber Space
Mun-Wai Hon, Government Vice Chair - AI, FAA
Matt Henson, Industry Chair - AI, TC Engine
Elizabeth Wyckoff, Associate Director, Working Groups
Amy Karpowicz, Working Groups Associate

Members: Lara George, Walacor; Kamil Kolodziejski, STRUCTURA.IO; James Carnall, Red River; Conrad Bovell, HHS; Tim Howard, NSF; Brian Vu, GSA; Norman Wong, Palo Alto Networks; Austin Boone, Red River; Craig Nickel, Alethia Labs

# ATARC AI Zero Trust Use Cases

## Introduction

The ATARC Zero Trust Working Group AI Track aims to explore how AI, including automation and generative AI, can enhance cybersecurity from an explicit trust versus implicit trust perspective. The initiative seeks to answer the following:

1. How can AI benefit Zero Trust?
2. How can Zero Trust benefit AI?

AI fundamentally changes the way users interact with and generate information. This lab seeks to elevate innovative application of AI for data governance and compliance use cases. Use cases must be directly applicable to the capabilities articulated in ATARC's Zero Trust Architecture Capability Maturity Model.

## Lab Deliverables

Each lab should address the following:

1. ZT Capabilities Scope - identify the ZT capabilities targeted and describe how they are addressed in the lab
2. Use Case(s) - articulate the use case(s) addressed
3. Tech Stack - provide an overview of the tech stack used in the demo
4. Architecture Overview - provide and explain architectural diagram, being sure to note SaaS vs localized/isolated model
5. Current Security and Compliance Posture - describe how you address security and compliance within the lab
6. Data Connection - identify the source system connectors demonstrated in the lab and/or available in the tech stack
7. Data Ingestion - demonstrate ingestion of information relevant to the use case(s)
8. Data Transformation - demonstrate data attribution and classification
9. Metadata Tagging - demonstrate embedding of data transformation outputs in records and files
10. Search and Chat - demonstrate search and chat on ingested and tagged information
11. Analytics - demonstrate analytics and explain the insights gained
12. Human-in-the-Loop - demonstrate UI/UX for human intervention

## Use Cases

Any use case that deploys AI to enhance one or more capabilities in the Zero Trust Capabilities matrix is eligible for consideration. The below examples include those use cases most frequently discussed and acknowledged as priorities by working group members.

Classification

1. As a Data Governance Stakeholder, I want AI to automatically classify data, so that I can enable Fine-Grained Authorization Controls (FGAC)
2. As a Data Governance Stakeholder, I want AI to automatically classify data, so I don't have to rely on personnel to correctly identify and classify data.

3. As a Data Governance Stakeholder, I want AI to automatically classify data, so that my IT Asset Management, Security Incident Event Management (SIEM), vulnerability scans, compliance scans, etc. are data aware and use data classification as a prioritization variable.
4. As a Data Governance Stakeholder, I want AI to automatically classify data, so that my user provisioning processes are data aware and can use data classification as an authorization decision input.
5. As a Data Governance Stakeholder, I want AI to automatically classify data, so that data-level transactions (e.g., read, download, etc.) are data aware and can use data classification as an authorization decision input.

### Authorization

1. As a Data Governance Stakeholder, I want AI to automatically decompose data transaction authorities (e.g., NDAs, Contracts, Export Authorizations, Authorities to Operate, etc.) into machine-actionable attributes, so that I can deliver file, table, row, and cell-level Fine-Grained Access Controls (FGAC) against discrete authorizations.

### Policy-to-Code, Code-to-Policy

1. As a Data Governance Stakeholder, I want AI to automatically convert my written, human-readable, natural language policies, processes, and procedures (rules) into machine-actionable policy (e.g., XACML, ALFA, OPA/REGO, etc.), so that I can automate data-level Fine-Grained Authorization Controls (FGAC).
2. As a Data Governance Stakeholder, I want AI to automatically convert my electronic policies into human-readable, natural language, so that key stakeholders can understand and validate electronic policy rules and logic.

### Vulnerabilities & Incident Management

1. As a Data Governance Stakeholder, I want AI to automatically analyze and prioritize signals intelligence, so that I can most effectively allocate remediation resources.
2. As a Data Governance Stakeholder, I want AI to automatically determine the most effective remediation and to automatically cut a service ticket, so my resources can spend more time remediating and less time researching and documenting.

### Ecosystem Governance and Compliance

1. As a Data Governance Stakeholder, I want AI to automatically analyze my ecosystem against technical controls in security control frameworks, so that I can understand my compliance posture in near-real-time.
2. As a Data Governance Stakeholder, I want AI to automatically analyze my Command Media against the non-technical controls in security control frameworks, so that I can understand my compliance posture in near-real-time.
3. As a Data Governance Stakeholder, I want AI to automatically analyze and prioritize signals intelligence, so that I can most effectively allocate remediation resources.
4. As a Data Governance Stakeholder, I want AI to automatically determine the most effective remediation and to automatically cut a service ticket, so my resources can spend more time remediating and less time researching and documenting.

Software Governance & Compliance

1. As a Data Governance Stakeholder, I want AI to automatically generate a SBOM for internally developed software, so that I can analyze it for known vulnerabilities.
2. As a Data Governance Stakeholder, I want AI to automatically analyze my software for known vulnerabilities, so that I can understand the risks and mitigations.
3. As a Data Governance Stakeholder, I want AI to automatically prioritize SBOM vulnerabilities, risks, and mitigations, so that I can allocate resources to mitigation.
4. As a Data Governance Stakeholder, I want AI to automatically determine the most effective remediation and to automatically cut a service ticket, so my resources can spend more time remediating and less time researching and documenting.