DON Implement Zero Trust Blueprint

David L. Voelker, DON CIO ZT Implementation Lead

January 2025

Controlled by: Department of the Navy
Controlled by: DON CIO/CTO
CUI Categories: N/A
Distribution/Dissemination Control: DISTRO A
POC: david.l.voelker.civ@us.navy.mil

Agenda

- DON ZT Implementation Plan Phases
- Standards Based ZT Architecture
- Design Patterns and Approaches
- Resources
- Q&A

DON ZT Implementation Plan Phases

DON ZT Implementation Plan

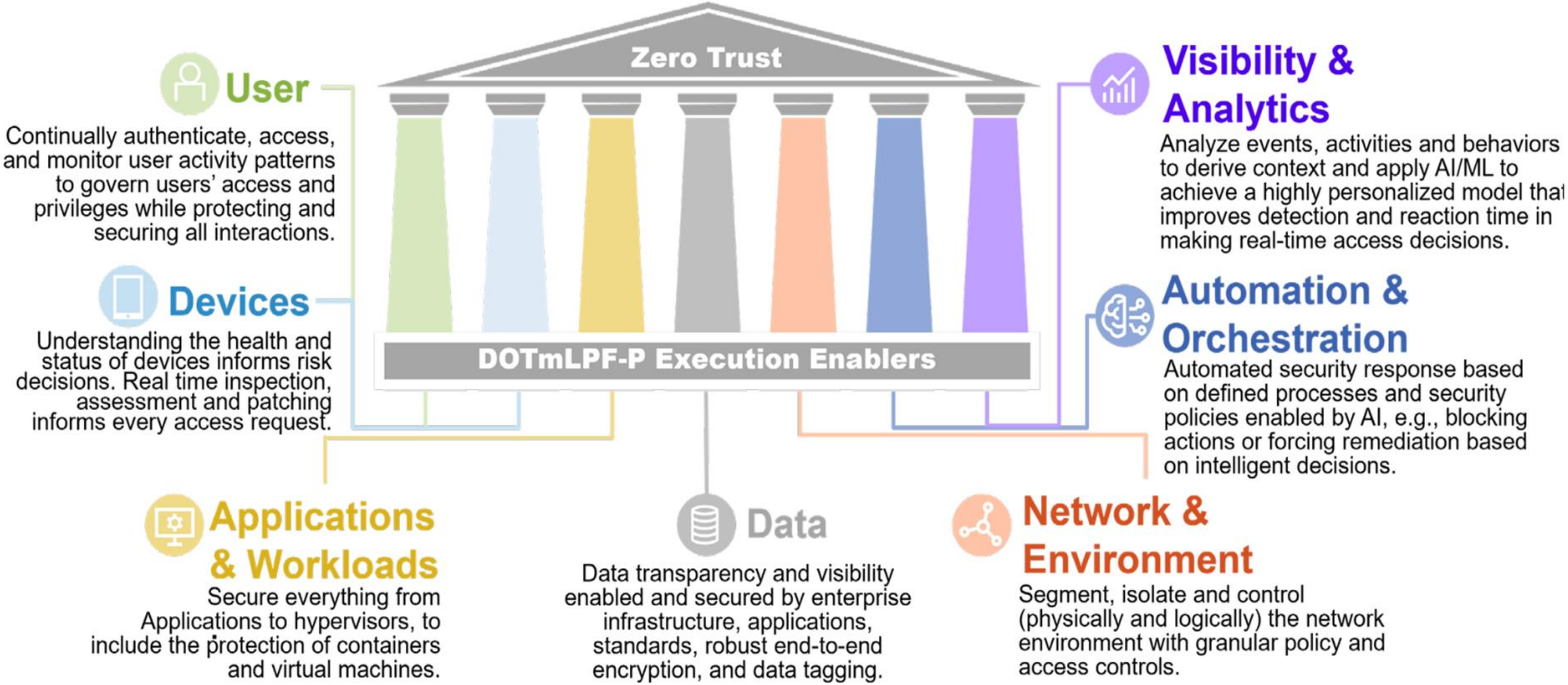
- **Phase One: Integrate Cyber Ready and ZT in Project and Program Modernization Acquisition Strategies; Implementation and Execution Plan completed by the end of FY 2025**
  - All DON acquisition programs will ensure both new and existing IT supports the DoD ZT framework and DON technology direction
  - ZT-enabled DON enterprise services will be leveraged to reduce costs, increase delivery speed, and maintain strategic alignment with ZT principles
  - Perform DOTmLF analysis
  - Programs will identify Program Objective Memorandum (POM) 27 Future Years Defense Program (FYDP) ZT investments needed to achieve Target Level ZT status by FY 2027

- **Phase Two: ZT Target Level Authentication, Authorization, Identity-Aware and Controlled Data Pathways, Applications, and Workloads completed by FY 2027**
  - Desired outcome: ZT Activities are deeply integrated in controlling data pathways (deny/permit) between all connected hosts on the network, enabling Mutual TLS (mTLS) authentication between devices and full implementation of target level 'Visibility & Analytics' and 'Automation & Orchestration' by the end of FY2027

- **Phase Three: Complete Remaining Target Level ZT Activities completed by FY 2029**

- **Phase Four: Implement Applicable Advanced Level Activities completed by FY 2030**

DON is a Zero Trust aligned organization at all levels by the end of FY2030



User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Standards Based ZT Architecture

Standards Based ZT Architecture

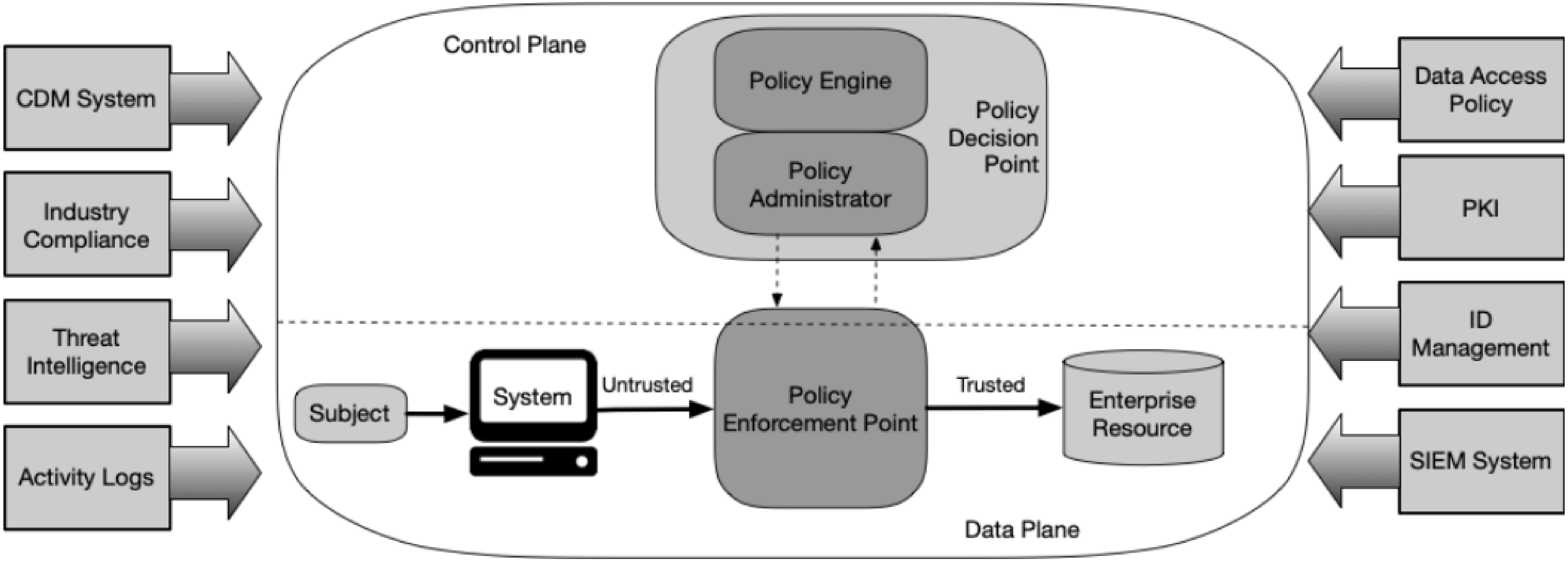
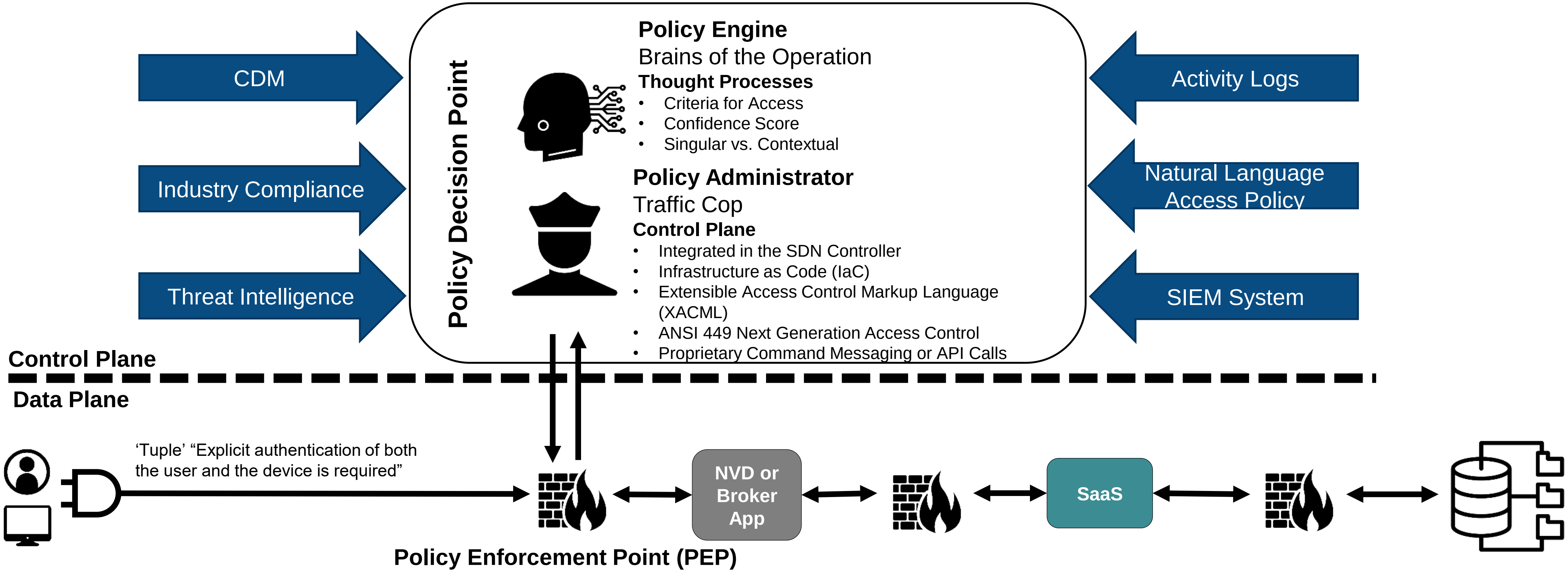


Figure 2: Core Zero Trust Logical Components

Standards Based ZT Architecture



CDM

Industry Compliance

Threat Intelligence

Activity Logs

Natural Language Access Policy

SIEM System

Policy Decision Point

Policy Engine

Brains of the Operation

Thought Processes

- Criteria for Access
- Confidence Score
- Singular vs. Contextual

Policy Administrator

Traffic Cop

Control Plane

- Integrated in the SDN Controller
- Infrastructure as Code (IaC)
- Extensible Access Control Markup Language (XACML)
- ANSI 449 Next Generation Access Control
- Proprietary Command Messaging or API Calls

Control Plane

Data Plane

'Tuple' "Explicit authentication of both the user and the device is required"

NVD or Broker App

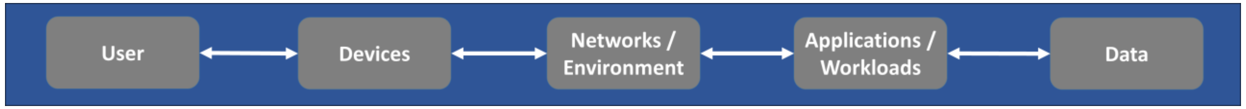
SaaS

Policy Enforcement Point (PEP)

Design Patterns and Approaches

Audit the Technical Baseline

- Identify HW/SW Reconfiguration or Replacement Options and Requirements
  - Schedule Autonomous Penetration testing before and after reconfigurations
- Types of Users and Locations
  - Onsite / Offsite
  - CONUS/OCONUS
- Devices
  - Networking Equipment
  - End Points
- Data Pathways
- Applications
- Data Stores



Identify applicable ZT activities; create an initial mapping of ZT requirements to functions in the technical baseline

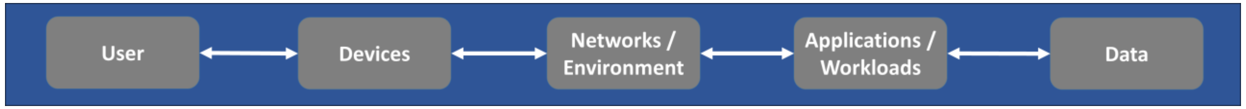
Prioritize ZT implementation based on Target Network, Devices, User, Visibility and Analytics, Automation and Orchestration requirements

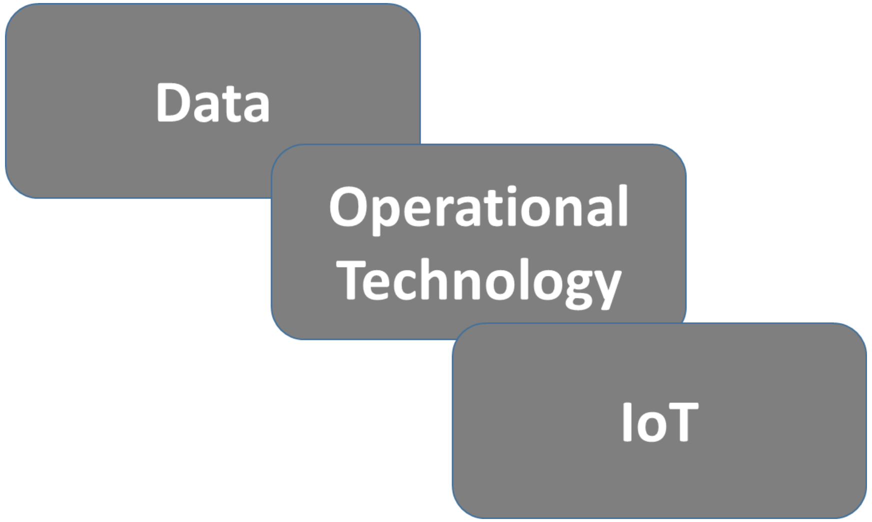
Followed by remaining Target Level ZT activities, ensuring full alignment with ZT requirements and security controls up the OSI and Cloud Hosting Stack

Apply applicable advanced ZT activities

Identify what you want to protect

- The next step in designing a ZTA is identifying the critical assets that need protection
- This includes data, applications, systems, and network resources
- Understanding what needs to be protected helps prioritize security efforts and allocate resources effectively


User ⟷ Devices ⟷ Networks / Environment ⟷ Applications / Workloads ⟷ Data

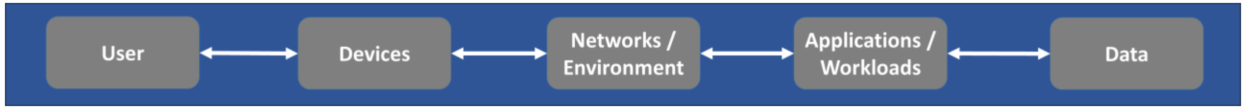

Data

Operational Technology

IoT

Define Mission Outcomes

- Define mission outcomes that account for continuous operation and resilience in the face of potential breaches

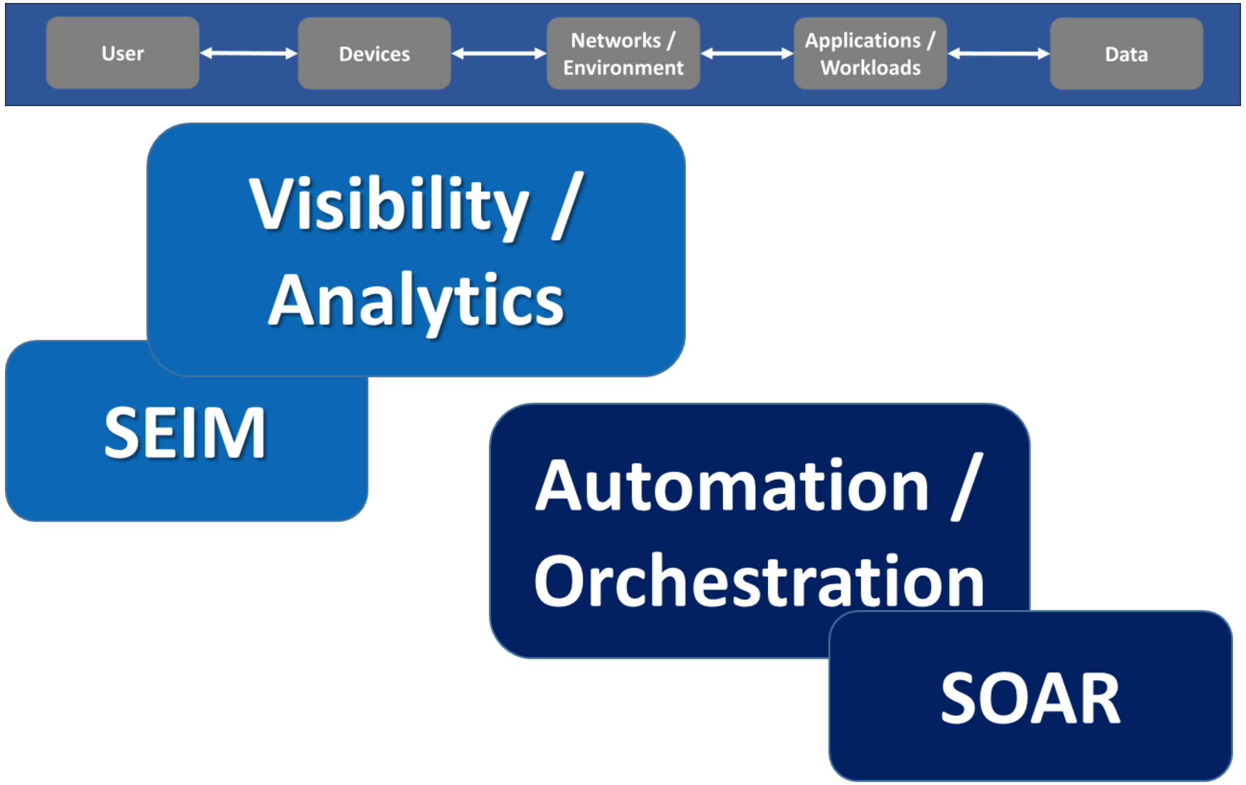


- Assume that adversaries are already inside the network

- This mindset ensures that security measures are proactive rather than reactive

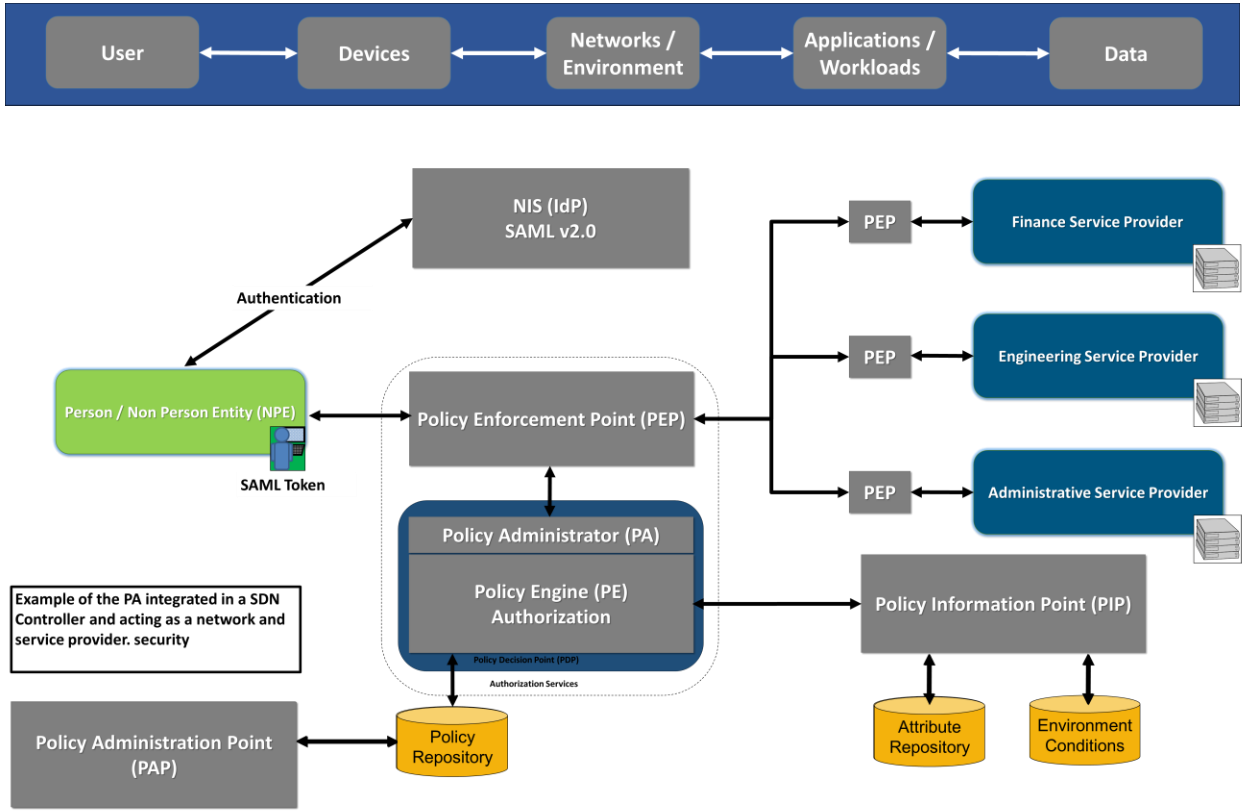
Map Transaction Flows

- Understand how data and processes flow within the network is essential
- Identify data pathways between users, applications, and systems
- Analyze the interactions and dependencies among network components
- Recognize potential points of vulnerability and interception
- Ensure that all transaction flows are secured and monitored



Determine Means of User, Device, and Network Access

- Access control is a cornerstone of ZT
- Apply network segmentation to isolate sensitive data and systems

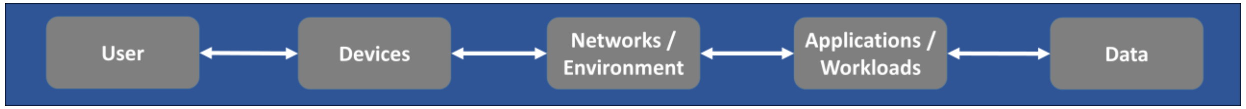


Example of the PA integrated in a SDN Controller and acting as a network and service provider. security

Zero Trust Architecture NIST SP 800-207 / Attribute Based Access Control (ABAC) NIST SP 800-162 Composite Diagram

Design the Architecture

- Start by securing core data and systems; implement micro segmentation using PEPs to the Macro Boundary
- Determine Access Criteria
- Develop Access Policies
- Design Thinking Activities
  - Tabletop Mission Cyber Risk Assessments (TMCRAs)
- Implement a Metamorphic Cyber Landscape to confuse adversary surveillance techniques
  - Deploy active and changing cyber safeguards, deception and decoy strategies and technologies

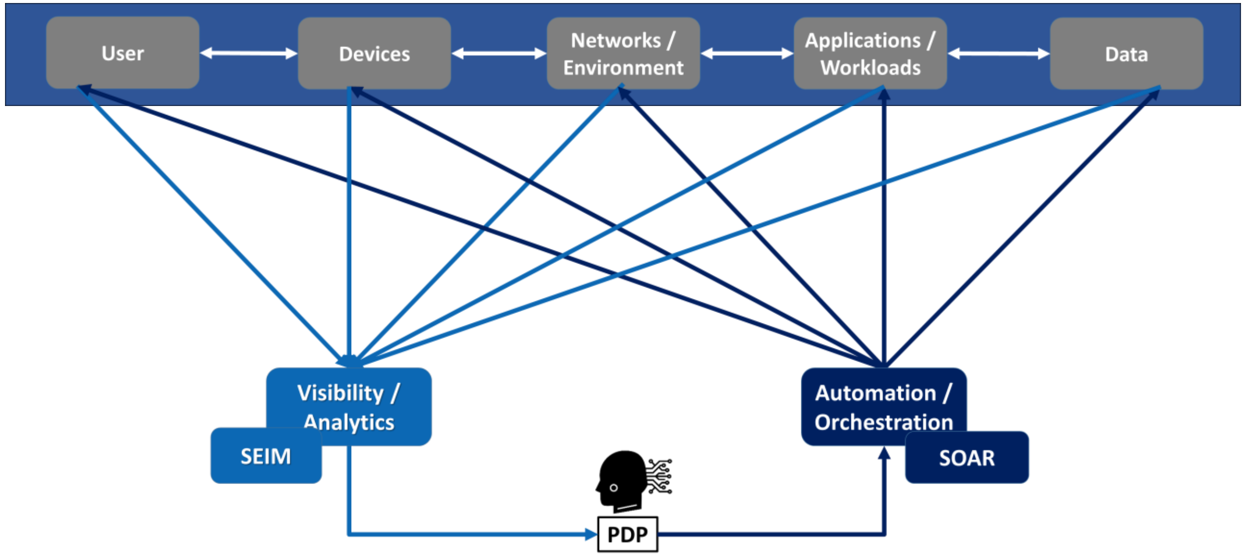


“**User and Entity Behavioral Analytics (UEBA)** enhances security by analyzing the behavior of users and entities to identify anomalies that could indicate potential threats”

Consult **Naval Network Warfare Command (NAVNETWARCOM)** on technical baseline design options that enhance current technology detection strengths

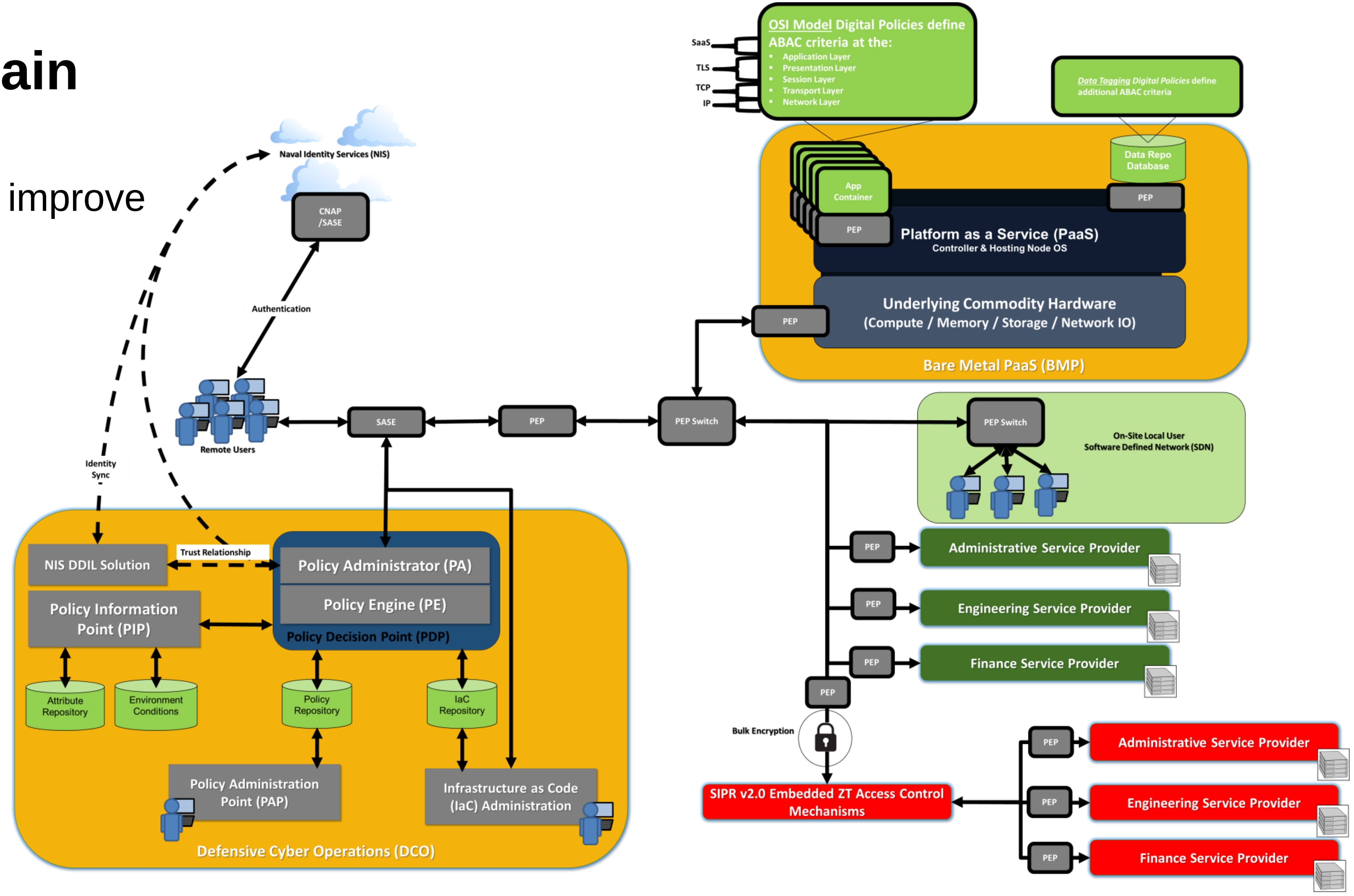
Prototype and Test

- **Verify** that all ZT **requirements** have been implemented
- **Validate** each ZT activity can demonstrate the desired outcome reaching the specified **success criteria**
- Determine how much Visibility is required to detect threat
- Determine how much Command and Control is required to enforce permit / deny access decisions
- Ensure the ZT implementation enables an Active Cyber Defense
- Simplify the design as much as possible



Monitor and Maintain

- Look for opportunities to improve the design


SaaS
TLS
TCP
IP
OSI Model Digital Policies define ABAC criteria at the:
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Tagging Digital Policies define additional ABAC criteria
Data Repo Database
PEP
App Container
PEP
Platform as a Service (PaaS)
Controller & Hosting Node OS
PEP
Underlying Commodity Hardware
(Compute / Memory / Storage / Network IO)
Bare Metal PaaS (BMP)
Naval Identity Services (NIS)
CNAP /SASE
Authentication
Remote Users
SASE
PEP
PEP Switch
PEP Switch
On-Site Local User Software Defined Network (SDN)
Identity Sync
PEP
Administrative Service Provider
PEP
Engineering Service Provider
PEP
Finance Service Provider
PEP
Bulk Encryption
SIPR v2.0 Embedded ZT Access Control Mechanisms
PEP
Administrative Service Provider
PEP
Engineering Service Provider
PEP
Finance Service Provider
NIS DDIL Solution
Trust Relationship
Policy Administrator (PA)
Policy Engine (PE)
Policy Decision Point (PDP)
Policy Information Point (PIP)
Attribute Repository
Environment Conditions
Policy Repository
IaC Repository
Policy Administration Point (PAP)
Infrastructure as Code (IaC) Administration
Defensive Cyber Operations (DCO)

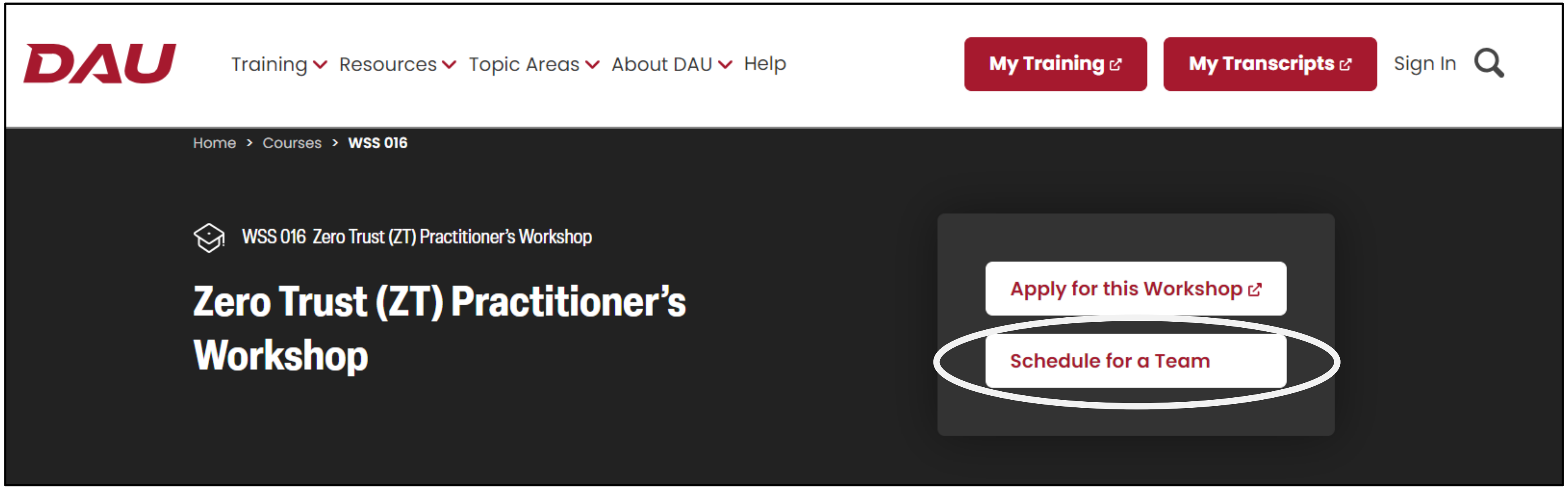
Resources

Resources

- DoD CIO Library
  - DoD Zero Trust Strategy
  - DoD Zero Trust Reference Architecture
  - Zero Trust Capabilities and Activities
  - Zero Trust Capability Execution Roadmap
  - Zero Trust Overlays

- DON CIO ZT Program
  - DON ZT Implementation Plan v2.0 (CAC Required)
  - DON ZT Major Design Concept
  - Draft DON ZT Blueprint (CAC Required / Planned release March-2025)

Zero Trust (ZT) Practitioner’s Workshop



Home > Courses > WSS 016

WSS 016 Zero Trust (ZT) Practitioner’s Workshop

Zero Trust (ZT) Practitioner’s Workshop

- https://www.dau.edu/courses/wss-016
  - The purpose of the workshop is to provide clarity on the Department of Defense (DoD)’s Zero Trust implementation requirements. This strategy supports DoD’s overarching efforts toward Digital Modernization. In this workshop, we will review DoD's information technology strategic initiatives, cybersecurity reference architectures, relevant laws, regulations, policies, and standards related to ZT. Participants will exercise their knowledge, skills, and abilities (KSAs) on project management principles, system design analysis, and assessment and reporting methodologies. Participants will assess cybersecurity ZT trade-space and tradeoffs based on the People, Processes, and Technology relating to having adequate security controls, Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) and risk management framework (RMF) principles.

Q & A