Carnegie Mellon University
Software Engineering Institute

Zero Trust for DCO Data Collection

AUGUST 23, 2023

Tim Morrow, Situational Awareness Technical Manager
Phil Groce, Senior Network Defense Analyst

Document Markings

Agenda

Carnegie Mellon University Software Engineering Institute

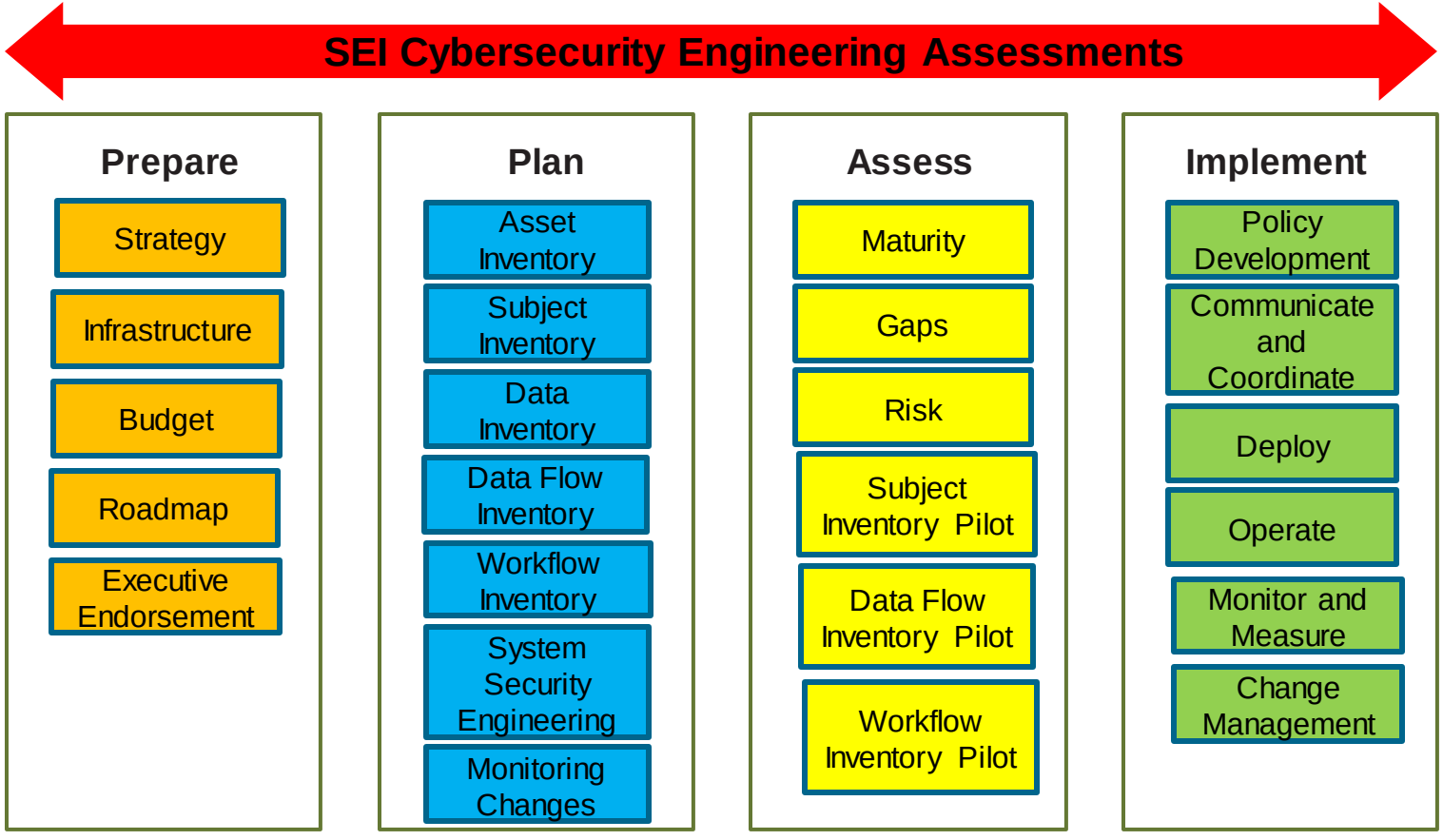
- What is Zero Trust?
  - **Zero Trust Implementation best practices**
  - **Zero Trust and mission engineering**
- How Zero Trust changes data collection for DCO-IDM
  - **What is collected**
  - **How it is collected**
- Data engineering for advanced analytics and ML

Presentation Name

Zero Trust Implementation

Carnegie Mellon University
Software Engineering Institute

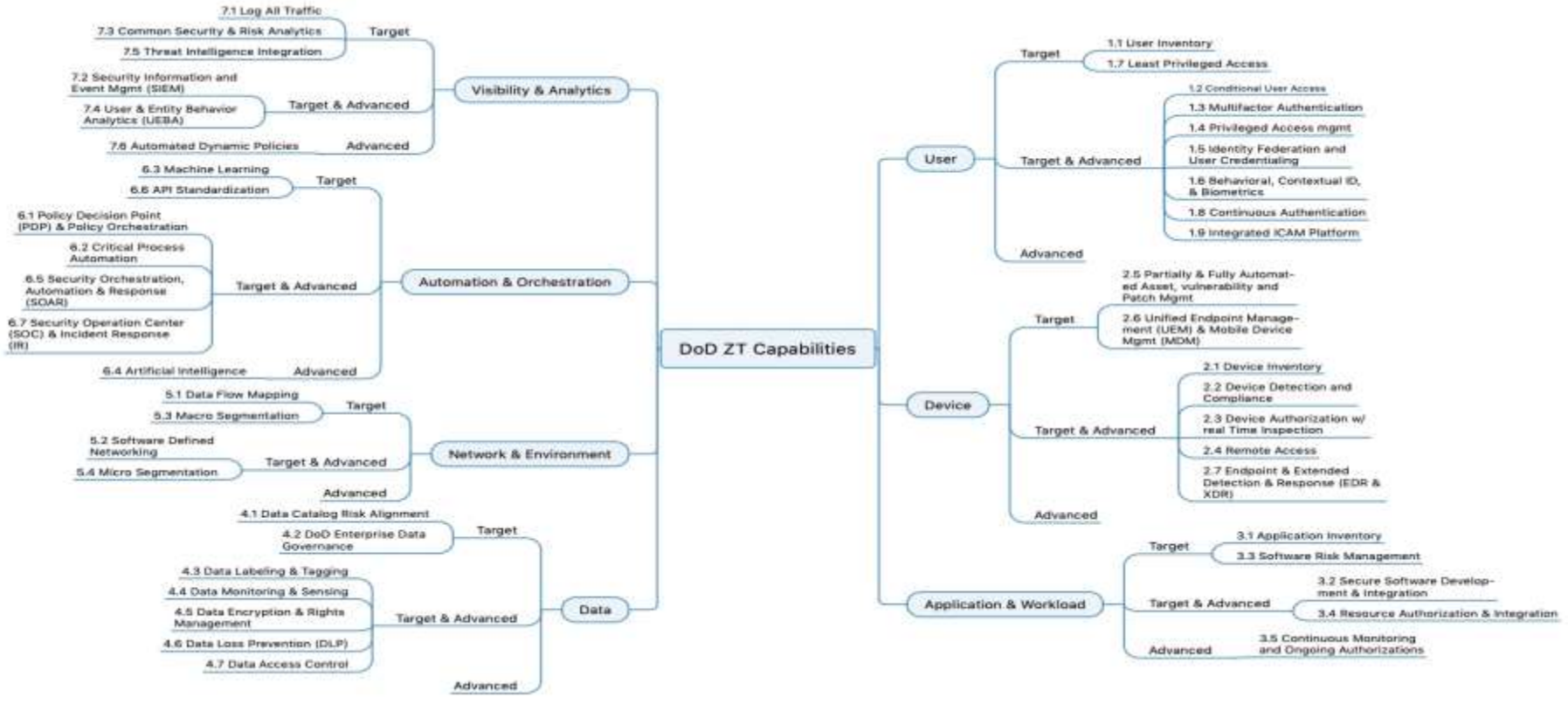
Software Engineering Institute (SEI) Zero Trust Journey



Prepare

1. Strategy
2. Infrastructure

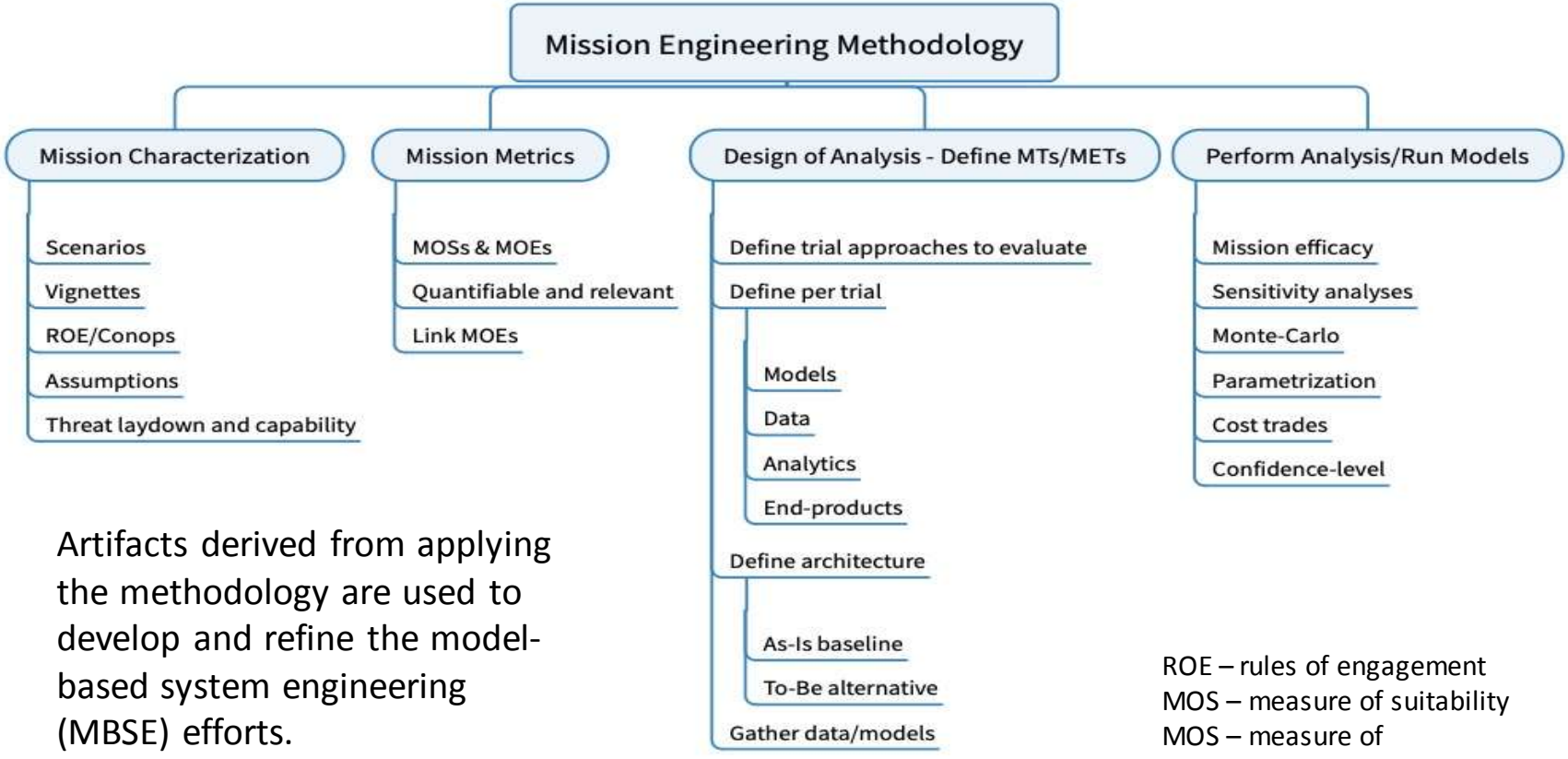
DoD Zero Trust Strategy



Plan

1. System Security Engineering
2. Acquisition

Developing a Contextual Understanding



Artifacts derived from applying the methodology are used to develop and refine the model-based system engineering (MBSE) efforts.

[MEG]

ROE – rules of engagement
MOS – measure of suitability
MOS – measure of effectiveness

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems

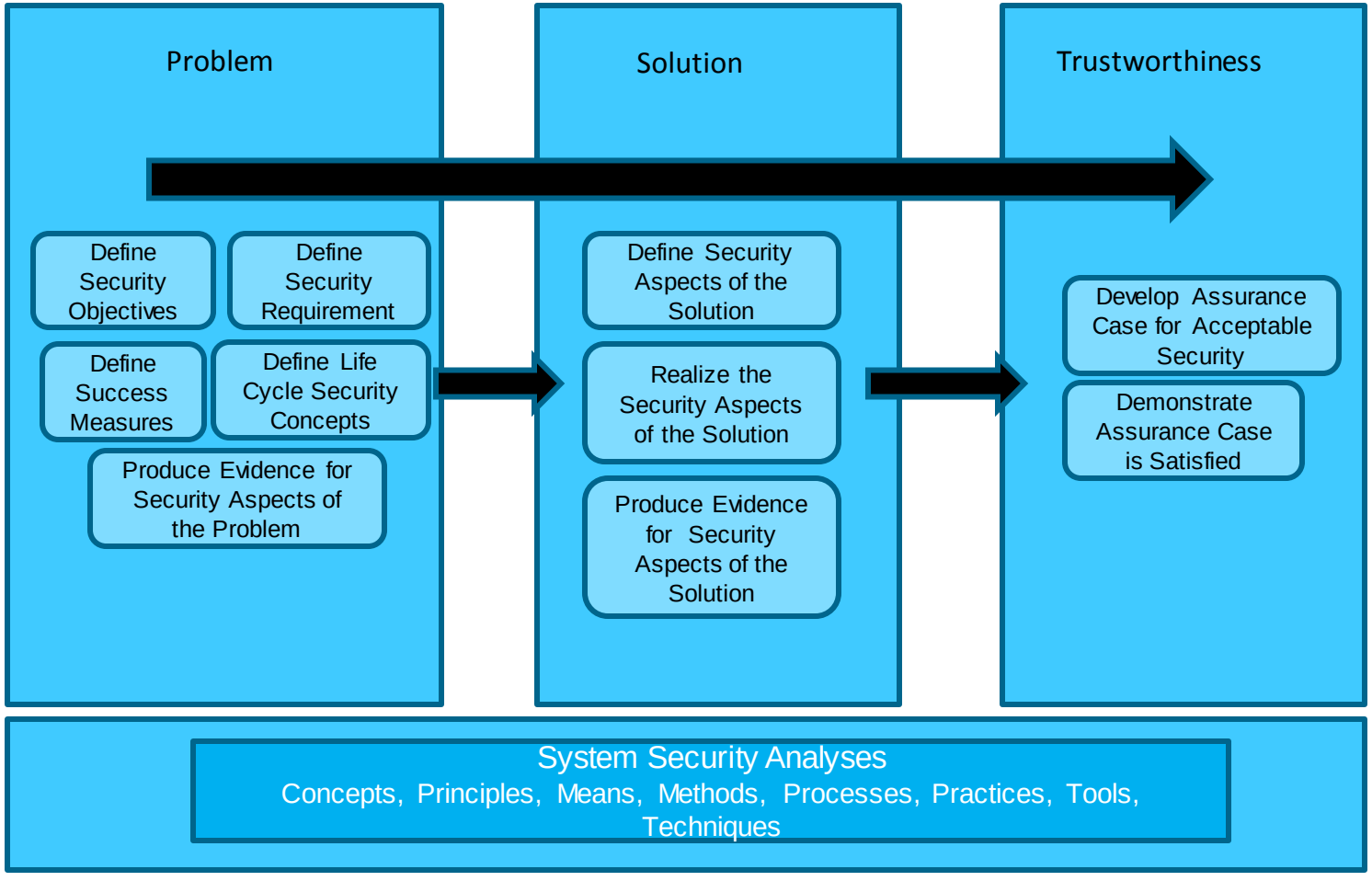


Figure 10

What is the Acquisition Security Framework (ASF)?

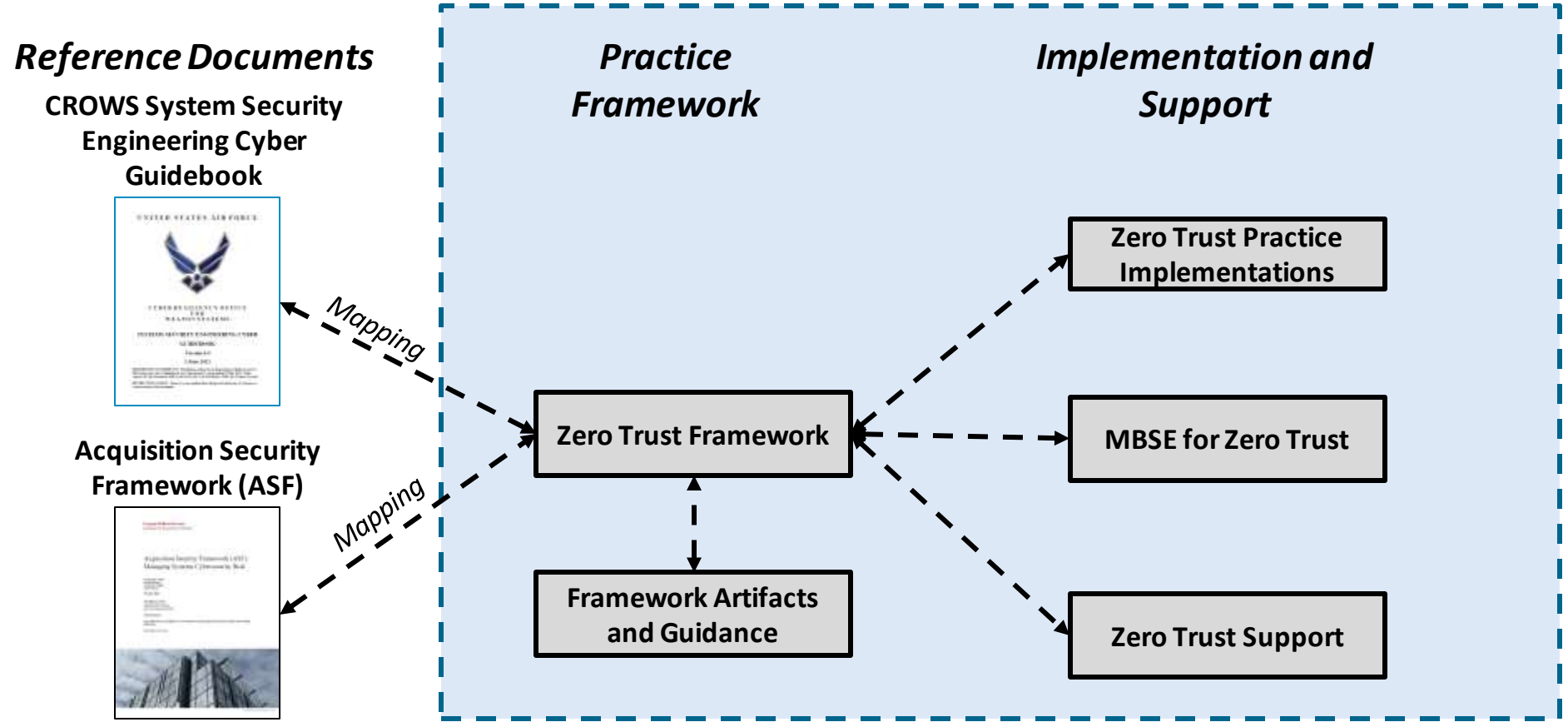
Carnegie Mellon University Software Engineering Institute

The ASF is a collection of leading practices for building and operating secure and resilient software-reliant systems.

The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

- Provides a roadmap for building security and resilience into a system rather than "bolting it on" after deployment
- Facilitates efficient and predictable systems environments and more manageable delivery and risk outcomes

Notional ZT Framework Application



Assess

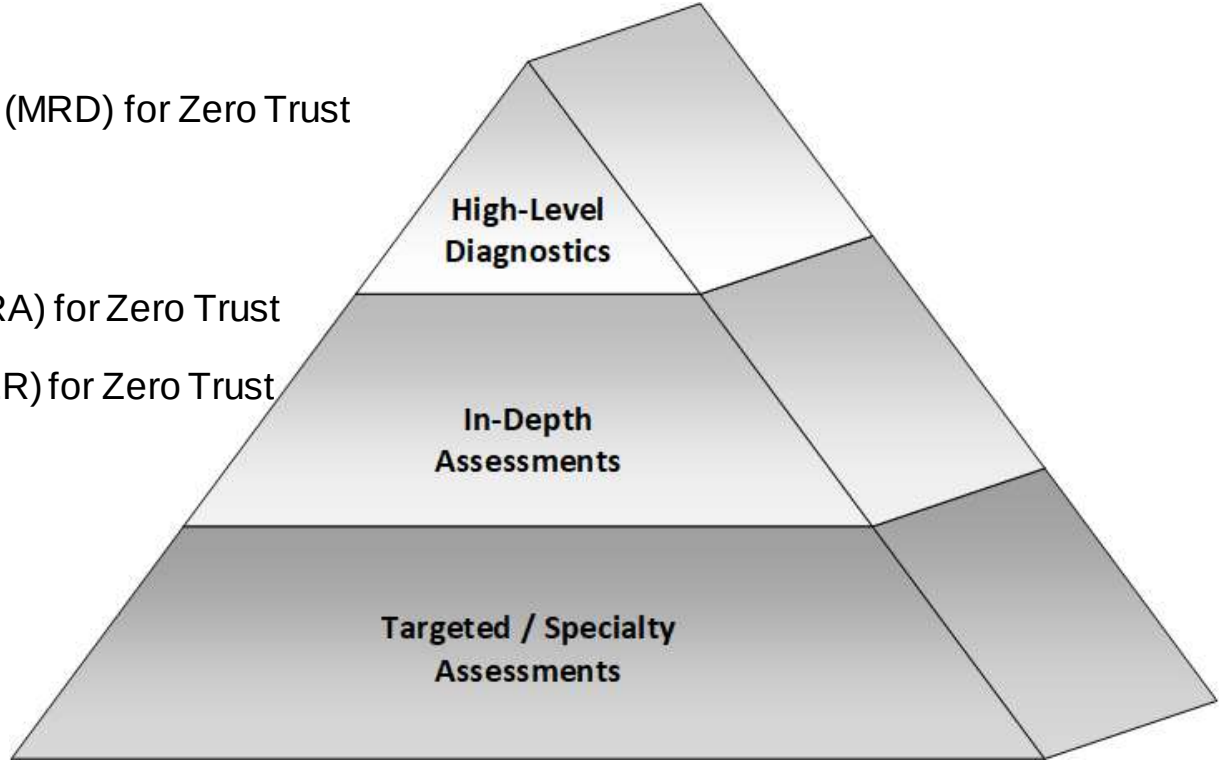
1. Zero trust assessments

Proposed Zero Trust Assessments

Mission Risk Diagnostic (MRD) for Zero Trust

Security Engineering Risk Analysis (SERA) for Zero Trust

Cybersecurity Engineering Review (CSER) for Zero Trust



Implement

1. Policies
2. Operate

What Was Missed or Needs Beefed Up in SEI ZT Journey?

1. API inventory
2. Developing contextual awareness
3. Visibility of data to support continuous monitoring and logging
4. Focus on automation activities
5. Identification of competencies to enable/support zero trust implementation
6. Goals for policy decision point analytics for organizations

Presentation Name

How Zero Trust Changes Data Collection for DCO-IDM

Carnegie Mellon University
Software Engineering Institute

Zero Trust in the Simplest Terms

Carnegie Mellon University Software Engineering Institute

NIST 1800-35 Executive Summary:

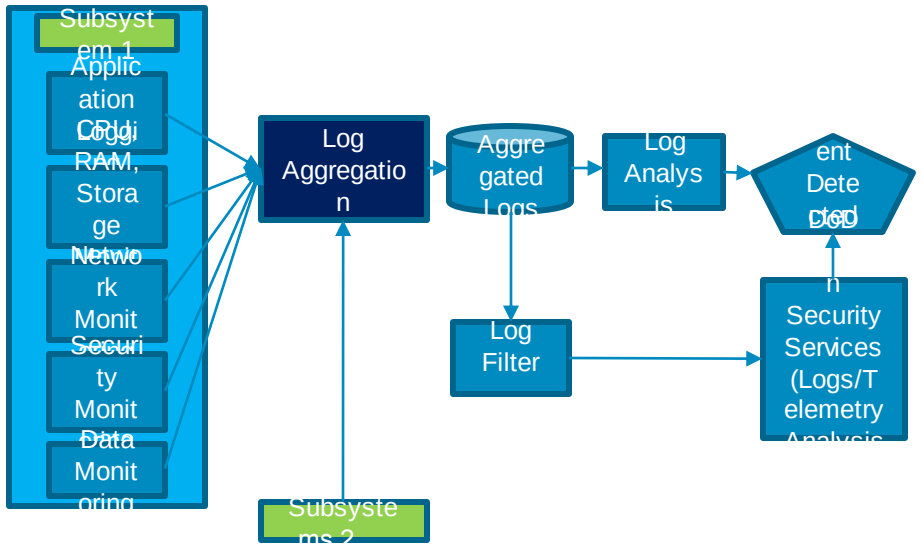
A zero-trust architecture (ZTA) enables secure ***authorized*** *access to…machines, applications and services running on them, and associated data and* ***resources****…****For each access request****, ZTA explicitly verifies the context available at access time…. If the* ***defined policy*** *is met, a secure session is created….A* real-time*, risk-based assessment of resource access…[is] performed to establish and maintain the access.*

Zero Trust is about *defining* and *enforcing* policies at the same conceptual level.

Zero Trust (in the network) = reliance on the application layer

Challenges and Opportunities

- Shift from network vantage to endpoint vantage
- More dimensions
- Higher volumes
- Reliability of application-layer reporting
- Importance of identification/authorization/access decisions
- Understanding why something happened relies on reconstructing context



Identity management

- Identity is part of every Zero-Trust policy decision
- A single user may have different accounts/roles
- Accounts may cross multiple domains; accounts/roles change over time
- When do operators need to know about identity?
  - Reachability/damage assessment in incident response
  - DCO of ICAM/verification of trust decisions

Use case: Identity compromise

An end-user endpoint is compromised; anomalous access to multiple systems is detected as logged-in user

Which other systems might have been accessed?

- Query: systems for which user is authorized, across all ICAM systems in which user is registered

Data requirements

- ICAM user information for protected services

Use case: Event Reconstruction

New CVE: Authentication service bypass

Was this vulnerability exploited?

- Query: All access authorization events by users where user was not authorized at time of access

Data Requirements

- Historical access events
- Historical ICAM state

Data Engineering for Advanced Analytics and ML

Carnegie Mellon University
Software Engineering Institute

Advanced Analytics

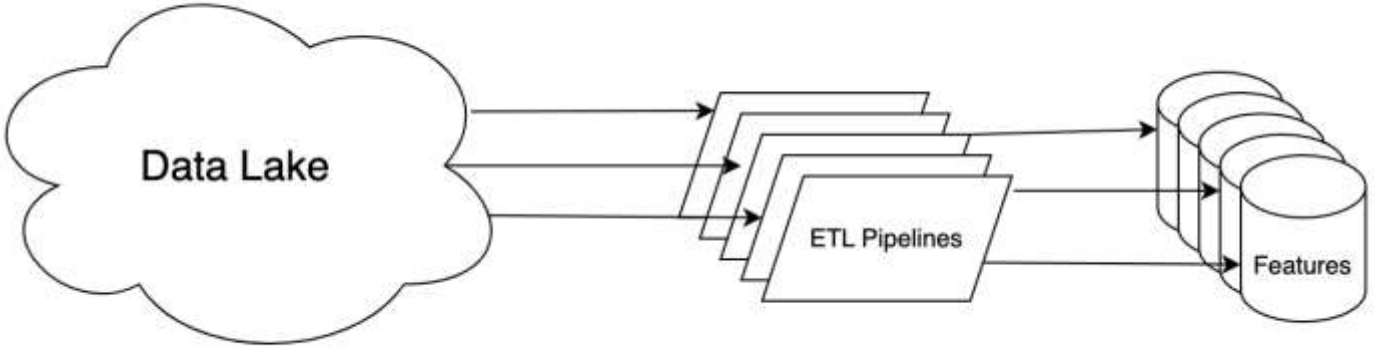
Zero Trust: More data, more analytic problems:

- How can I maximize insight into security-relevant behaviors?
- How can I make my data collection more efficient? What amount of data is *necessary* and *sufficient* for required insight?
- How much trust can I put in my data?

Supporting advanced analytics

- Identifying best practices
- Architecting data to maximize effectiveness
- Taking advantage of feedback loops, even between application tiers

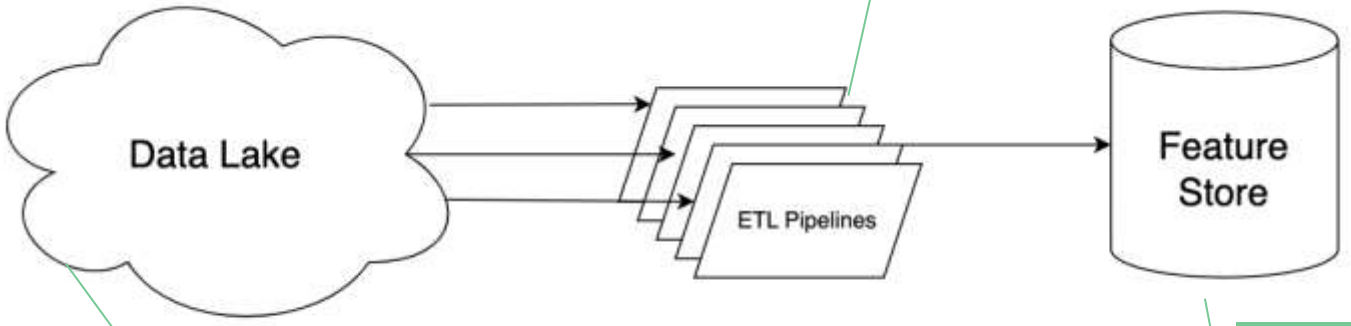
Data Utility



- In current practice, for each modeling activity, data is pulled from the data lake, a new ETL pipeline is generated and new features are extracted.
- This results in duplicated effort and unnecessary re-engineering of data transformation and extraction.
- Reduces utility of data because every new analytic development is starting from data of record.

Need for Better Data Abstractions

A common pattern is for multiple ETL pipelines to push features to a single common feature store

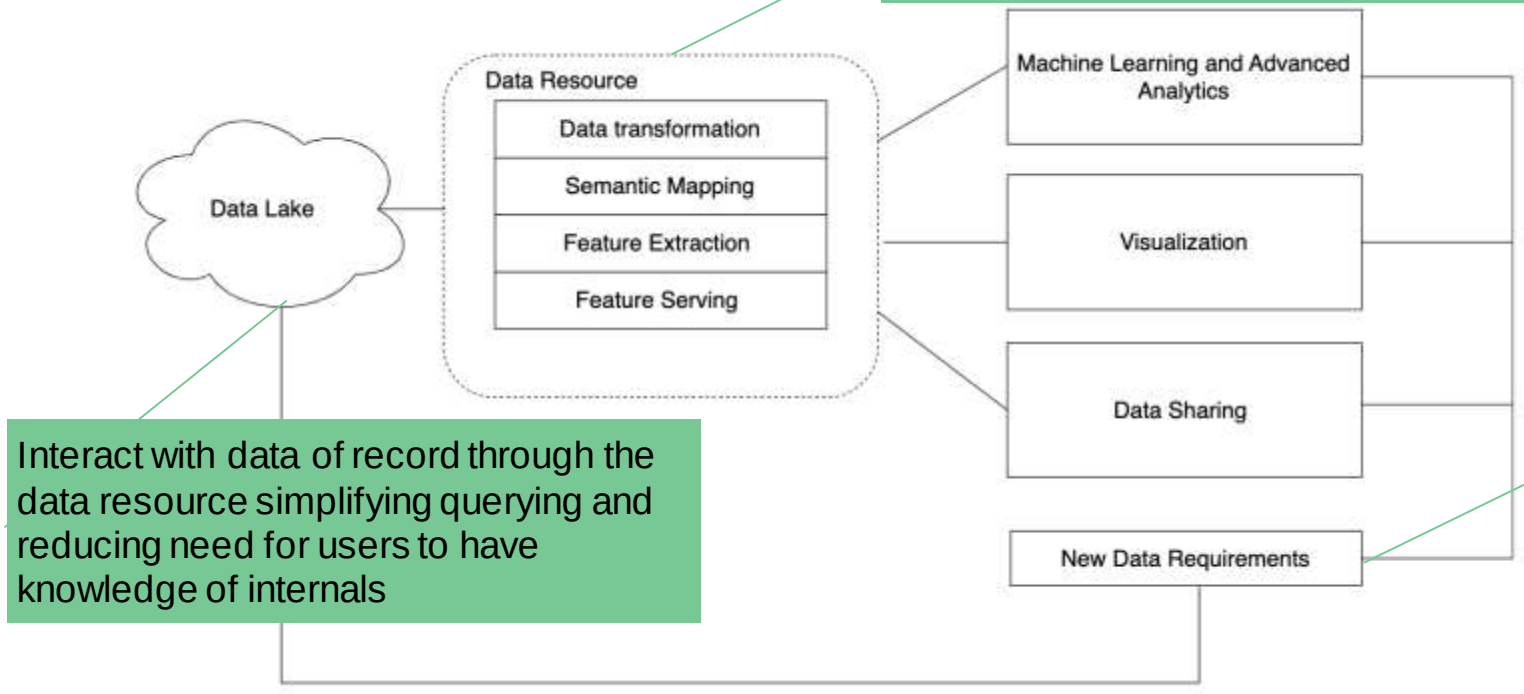


Without a semantic mapping, in order to provide traceability back to data of record requires explicit knowledge and mapping from feature store to data lake (hidden dependency)

The feature store alone cannot natively control duplication, can quickly become unmanageable and hard to integrate new data sources

Achieving Data Flexibility and Extensibility

Abstract data transformation and feature extraction to support multiple activities at once



Interact with data of record through the data resource simplifying querying and reducing need for users to have knowledge of internals

Enable consumers to reuse and augment data elements and features and push requirements from modeling activities back into data resource

Thank you for your time!

Tim Morrow tbm@sei.cmu.edu
Phil Groce pgroce@sei.cmu.edu

Additional Slides

Department of Defense References

[DoD 2019]
Department of Defense (DoD). *DoD Enterprise DevSecOps Reference Design, Version 1.0*. August 2019.
https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

[MEG]

DoD. *Mission Engineering Guide*, November 2020.

https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

ASF Information

Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889215

Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887698

Acquisition Security Framework (ASF)

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889453

Addressing Supply Chain Risk and Resilience for Software-Reliant Systems

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974293

Asking the Right Questions to Coordinate Security in the Supply Chain

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974136

ASF Engineering Lifecycle: Domains and Goals

Domain	Goal Name
Domain 1—Engineering Infrastructure	Infrastructure Development
	Infrastructure Operation
Domain 2—Engineering Management	Technical Activity Management
	Product Risk Management
Domain 3—Engineering Activities	Requirements
	Architecture
	Third-Party Components
	Implementation
	Test and Evaluation
	Transition Artifacts
	Deployment
	Secure Product Operation

Our initial development is focused on Engineering Activities (Domain 3).

Mission Risk Diagnostic (MRD)

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Security Engineering Risk Analysis (SERA)

Carnegie Mellon University Software Engineering Institute

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

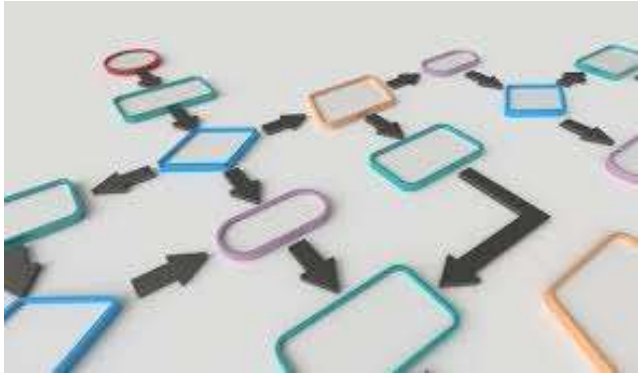
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Cybersecurity Engineering Review (CSER)

Carnegie Mellon University Software Engineering Institute

What

- Evaluates an acquisition program's security practices for conformance to accepted CSE practices



Why

- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Assessment Information

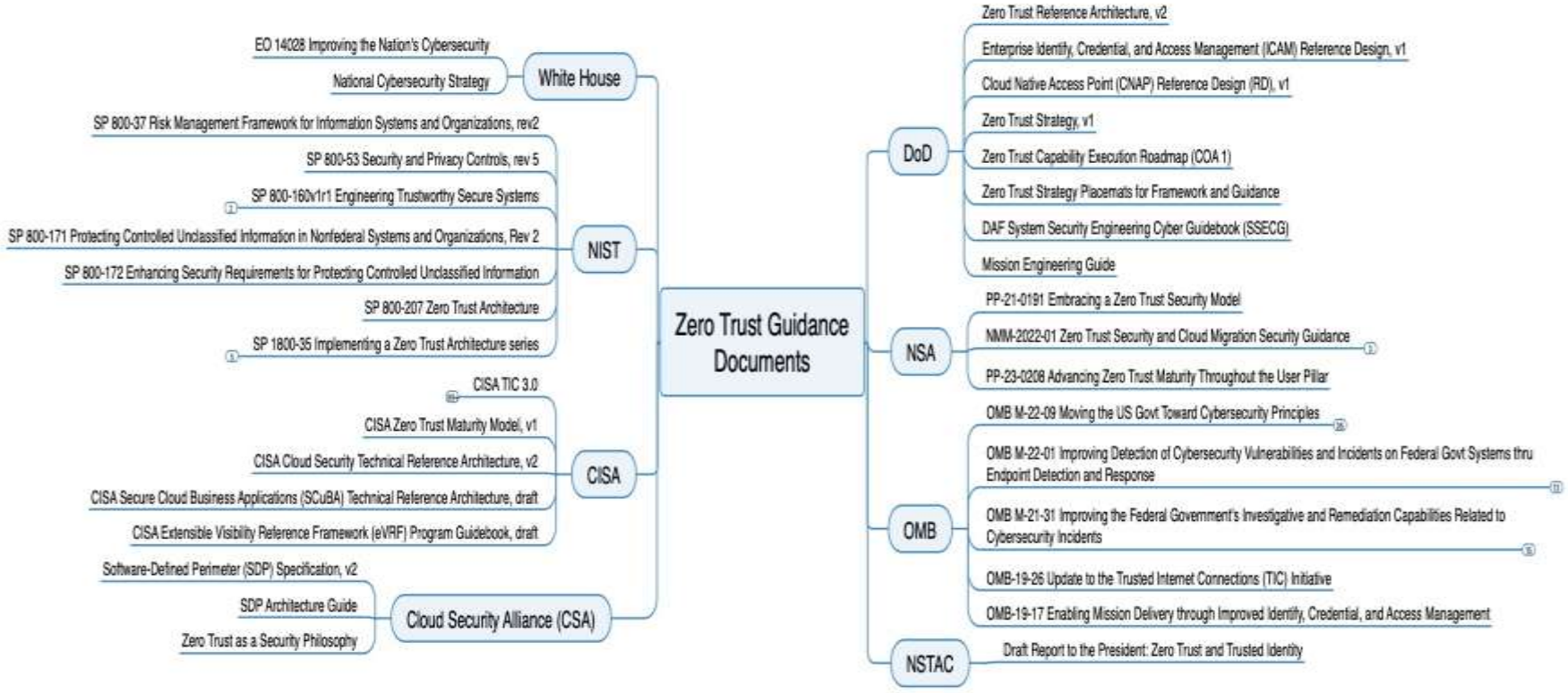
Mission Risk Diagnostic (MRD) Method Description

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

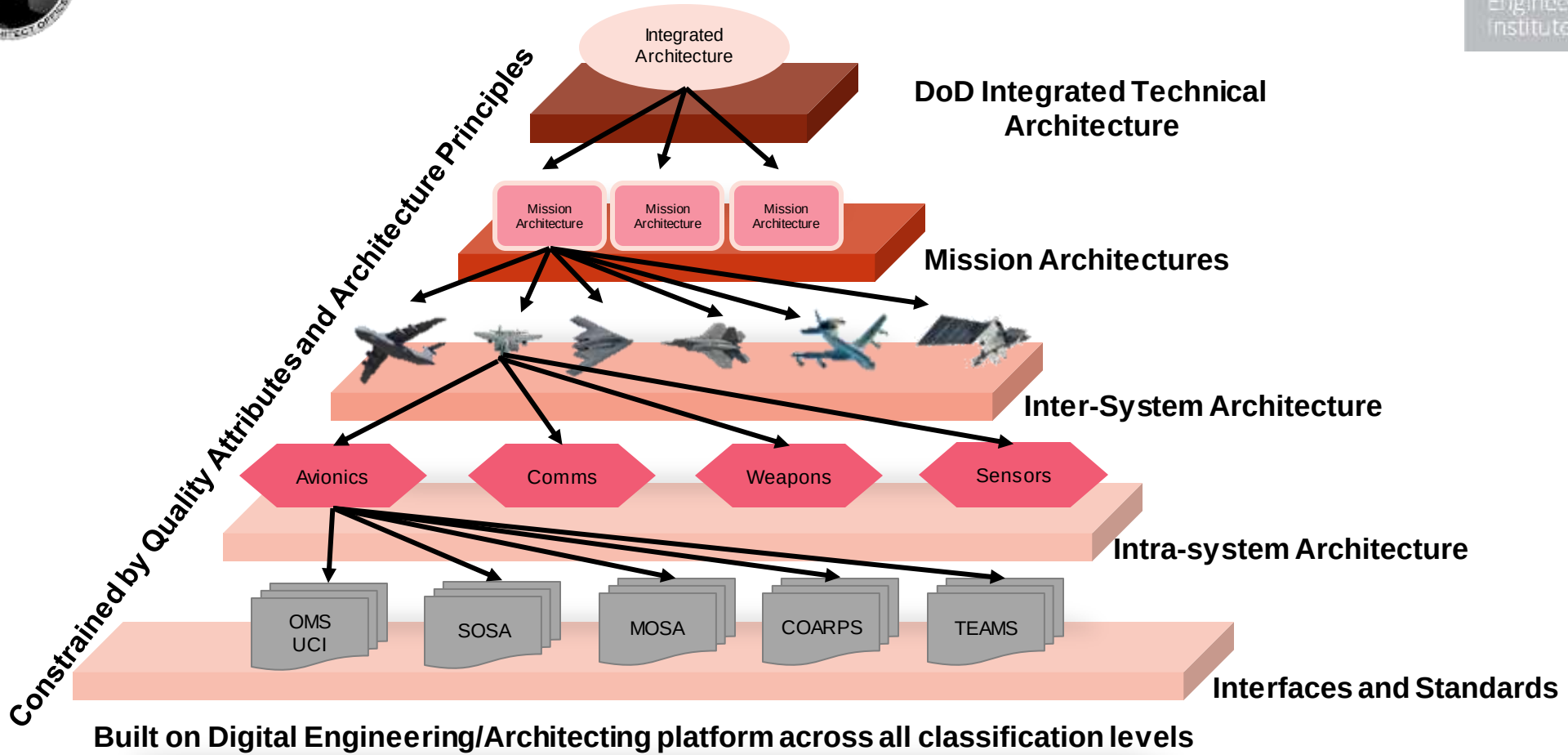
Security Engineering Risk Analysis (SERA) Collection

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485410

Guidance Documents When Considering a Zero Trust Implementation



DoD Architecture Layers



DAF System Security Engineering Cyber Guidebook (SSECG) - Cyber Survivability Attributes

CSA	Pillar	Cyber Survivability Attribute (CSA)
CSA-01	Prevent	Control Access
CSA-02	Prevent	Reduce System's Cyber Detectability
CSA-03	Prevent	Secure Transmissions and Communications
CSA-04	Prevent	Protect System's Information from Exploitation
CSA-05	Prevent	Partition and Ensure Critical Functions at Mission Completion Performance Levels
CSA-06	Prevent	Minimize and Harden Cyber Attack Surfaces
CSA-07	Mitigate	Baseline & Monitor Systems, & Detect Anomalies
CSA-08	Mitigate	Manage System Performance if Degraded by Cyber Events
CSA-09	Recover	Recover System Capabilities; Actively manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds
CSA-10	Adapt	Achieve & Manage System's an operationally relevant Cyber Survivability Risk Posture (CSRP) and to counter risk changes in adversary's capabilities

System Survivability Key Performance Parameter

Envisioned Zero Trust Framework: Guidance

Goal-Level Guidance

- Description and Context
- Competencies

Practice-Level Guidance

- Question Intent
- Typical Work Products
- Criteria for “Yes” Response
- Criteria for “Incomplete” Response

Mission Risk Diagnostic (MRD)

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Security Engineering Risk Analysis (SERA)

Carnegie Mellon University Software Engineering Institute

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

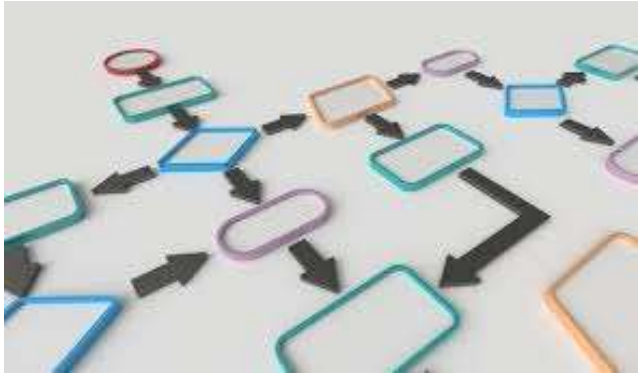
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Cybersecurity Engineering Review (CSER)

Carnegie Mellon University Software Engineering Institute

What

- Evaluates an acquisition program's security practices for conformance to accepted CSE practices



Why

- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Assessment Information

Mission Risk Diagnostic (MRD) Method Description

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

Security Engineering Risk Analysis (SERA) Collection

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485410

ASF Information

Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889215

Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887698

Acquisition Security Framework (ASF)

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889453

Addressing Supply Chain Risk and Resilience for Software-Reliant Systems

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974293

Asking the Right Questions to Coordinate Security in the Supply Chain

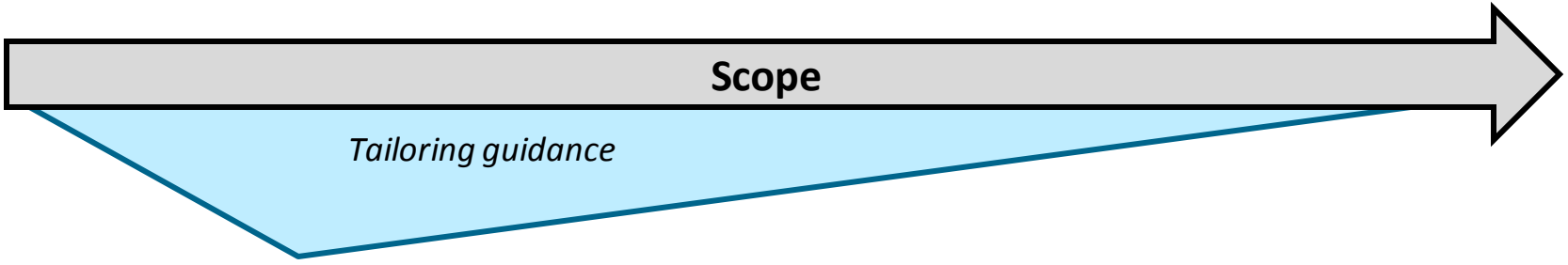
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974136

ASF Engineering Lifecycle: Domains and Goals

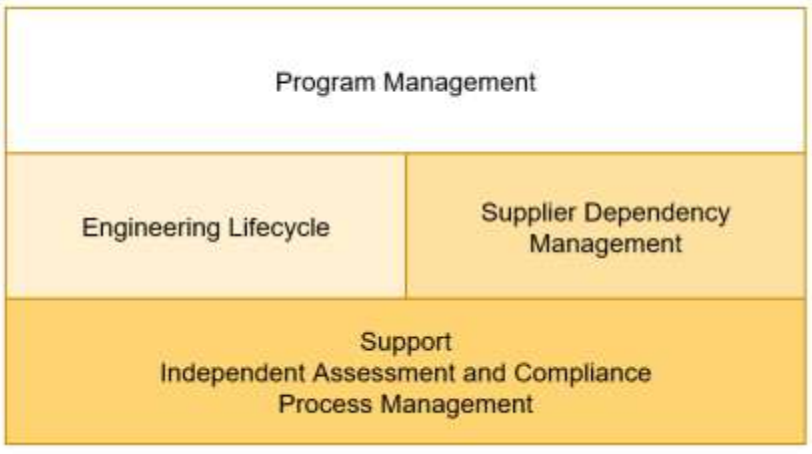
Domain	Goal Name
Domain 1—Engineering Infrastructure	Infrastructure Development
	Infrastructure Operation
Domain 2—Engineering Management	Technical Activity Management
	Product Risk Management
Domain 3—Engineering Activities	Requirements
	Architecture
	Third-Party Components
	Implementation
	Test and Evaluation
	Transition Artifacts
	Deployment
	Secure Product Operation

Our initial development is focused on Engineering Activities (Domain 3).

Creating Tailored Risk Frameworks



ASF Principles and Concepts



Tailored Framework