Carnegie Mellon University
Software Engineering Institute

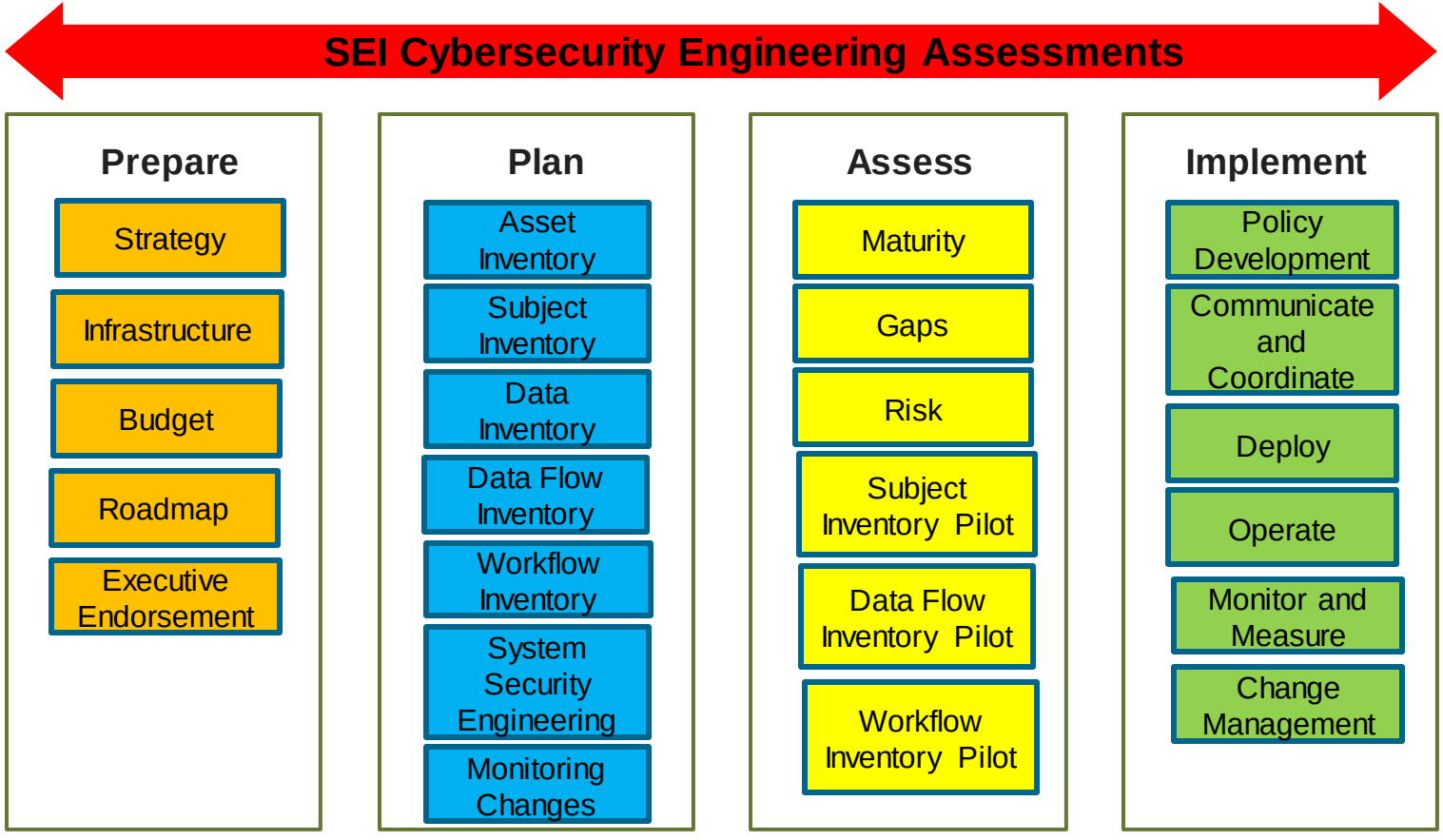
Best Practices and Results from Fall 2022 SEI Zero Trust Industry Day

APRIL 18, 2023

Tim Morrow
CMU/SEI CERT Situational Awareness Technical Manager

Document Markings

Software Engineering Institute (SEI) Zero Trust Journey



SEI Zero Trust Industry Day 2022

Carnegie Mellon University Software Engineering Institute

Goal

Collect information from those who develop solutions for implementing a zero trust architecture to help government agencies form a zero trust implementation that meets their mission goals, budget, and time frame.

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.

Zero Trust Industry Day: Request for Information (RFI)

Carnegie Mellon University Software Engineering Institute

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.

Link to "SEI Zero Trust Industry Day: Request for Information (RFI)

https://resources.sei.cmu.edu/asset_files/Brochure/2022_015_001_886713.pdf

Ten Organizations Were Selected

Requested to:

- Develop a proposal that meets the requirement specifically selected from the two OMB memoranda.
- Ensure that the proposal stays within the budget provided.
- Create a set of artifacts that support your proposal. (list of artifacts on next slide).
- Create a 30-minute presentation that describes your proposal.
- Participate in a panel discussion

Industry Best Practices for Zero Trust Architecture Themes

1. Inventories
   - Develop and maintain comprehensive inventories that include data, applications, assets (emphasizing high-value assets), services, and workflows.

1. Auditing/Logging
   - Auditing and logging are critical, considering the dynamic nature of ZT.

1. Governance and Risk
   - ZT is a complex paradigm with a relatively long jouney from introduction to maturity. Organizations should leverage governance and risk management to help plan, implement, and support the ZT Journey.

Industry Best Practices for Zero Trust Architecture Themes

Carnegie Mellon University Software Engineering Institute

4. Cloud and Virtual Solutions
   - Leverage cloud and virtual solutions when they reasonably fit into an organization's ZT journey to decrease overall risk.

4. Automation, Orchestration, and API
   - Use automation, orchestration, and API to optimize maturity

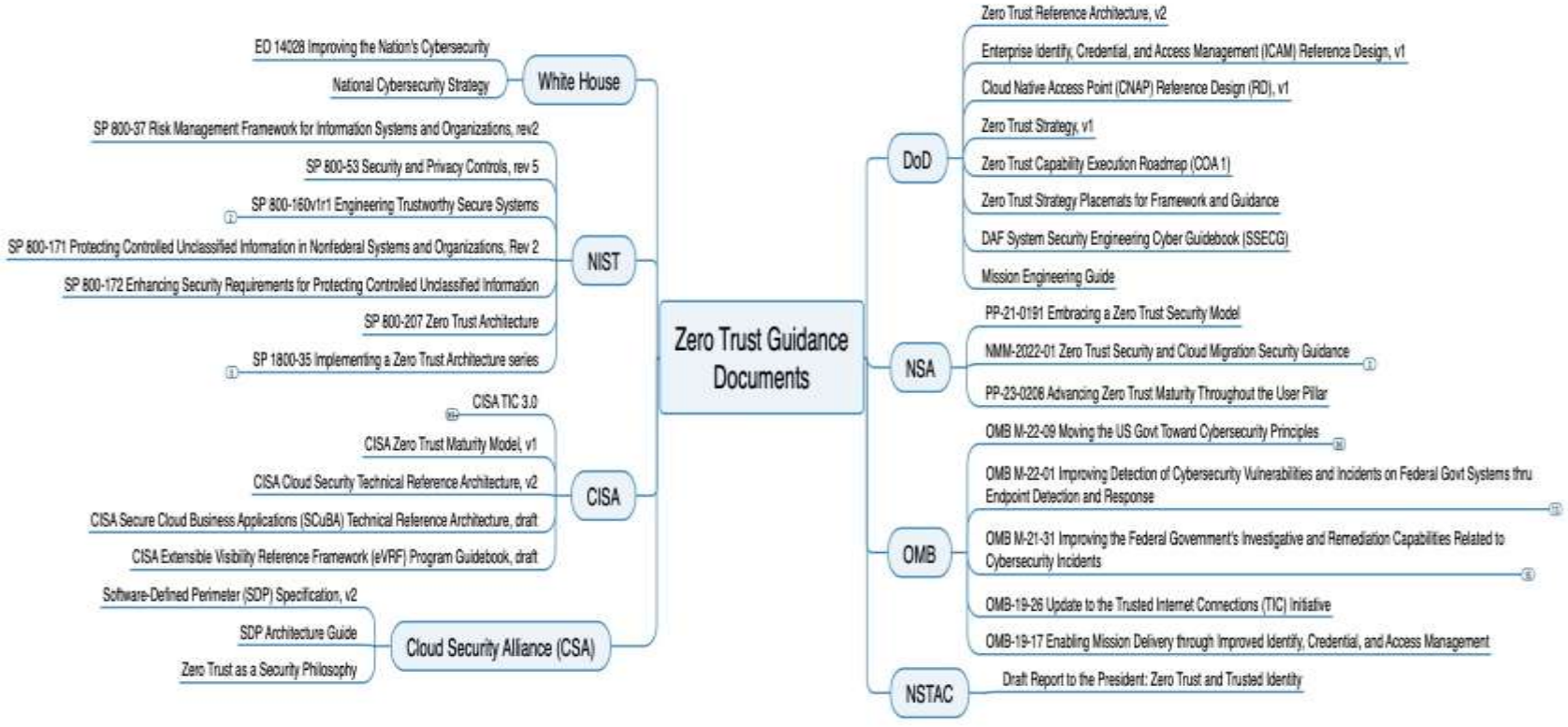
Panel Question - What areas dealing with ZT need further research?

1) The minimum amount of information that must be understood about a piece of malware to isolate and block it.
2) Adding security into technology as it is being developed.
3) Defining and standardizing the meaning of a session, per request access, and per request logging.
4) Defining the vocabulary, protocol, and event model for ZT.
5) Defining the minimum requirements for an effective security strategy for a ZT system in production.
6) Security frameworks that account for application and data moving from a central location to being closer to the user.

Panel Question - Given SEI's role is to be an honest broker, what one suggestion would you offer to the SEI in its pursuit to helping improve your work in in ZT?

1) Provide guidance to the commercial and public sector on how to measure progress during ZT implementation.
2) Provide a framework to induce commercial entities to move towards ZT.
3) Provide details on how to construct a timeline to achieve an organization's ZT goals.
4) Publish use cases illustrating government success in implementing ZT principles.
5) Provide research on what an organization's ZT investment cycle should look like and what the return on investment (ROI) is for different things.

Guidance Documents When Considering a Zero Trust Implementation



What's Mission Engineering and it's Objectives?

Carnegie Mellon University Software Engineering Institute

Mission Engineering (ME) is the planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.

Five Objectives

1. Enable mission-focused, threat-informed analysis.
2. Identify and address mission gaps.
3. Develop Government Reference Architectures (GRA) to guide development and prototypes.
4. Inform stakeholders how the architecture is envisioned to address/support the missions.
5. Generate and capture scenarios, assumptions, constraints, system attributes, and data for use during analysis.

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems

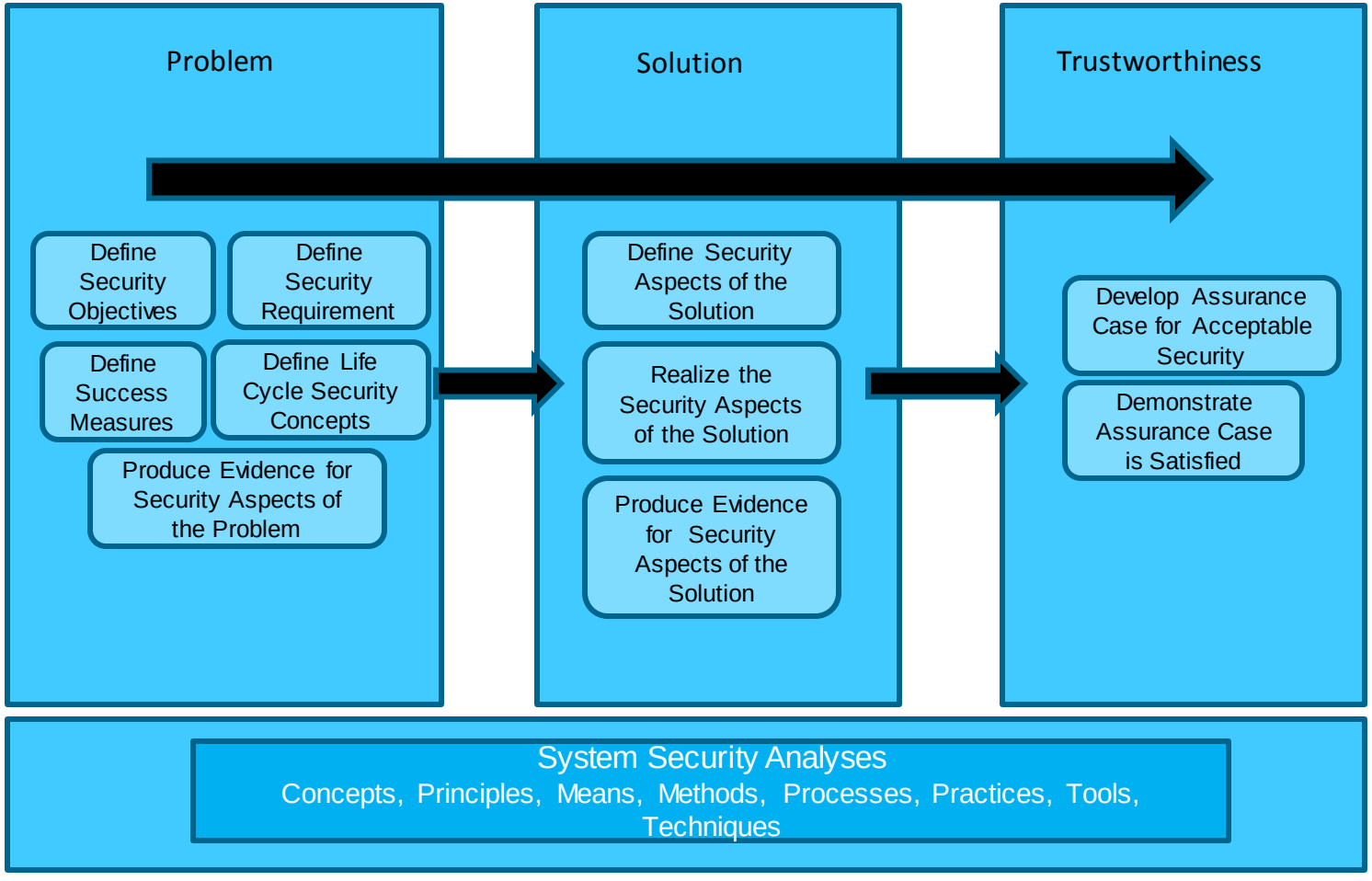


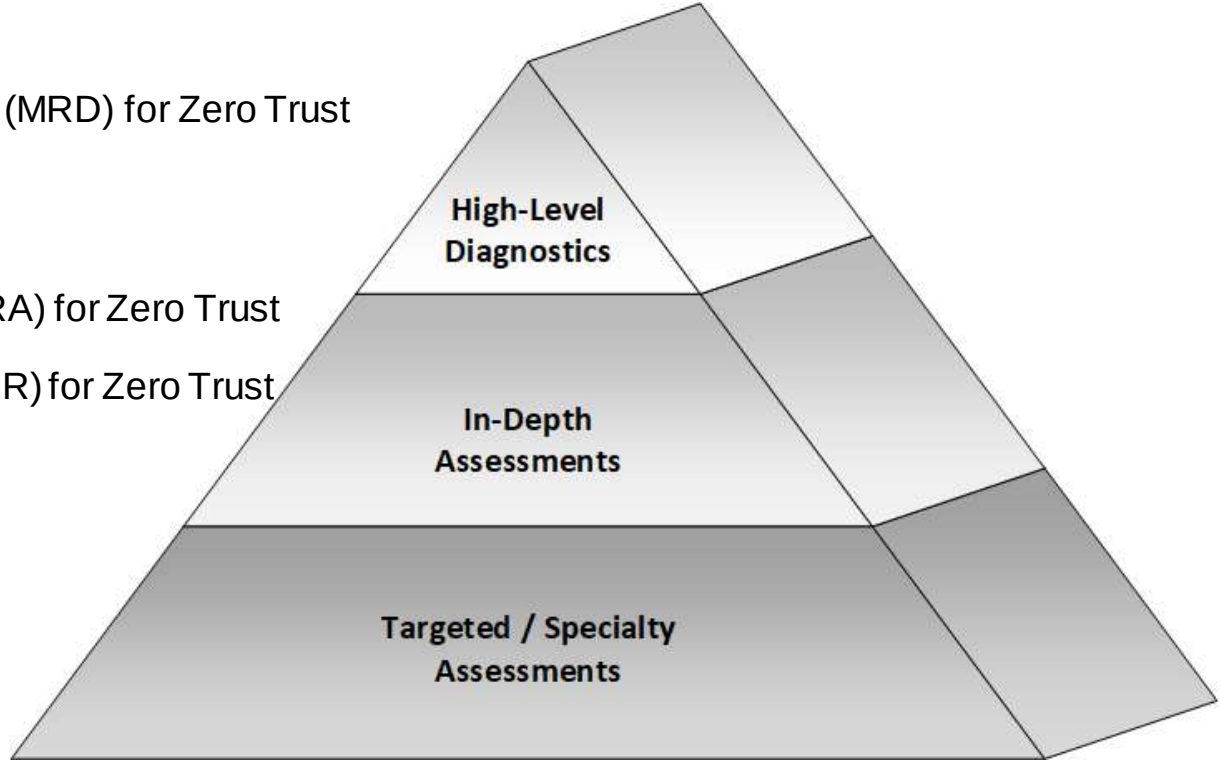
Figure 10

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



What is the Acquisition Security Framework (ASF)?

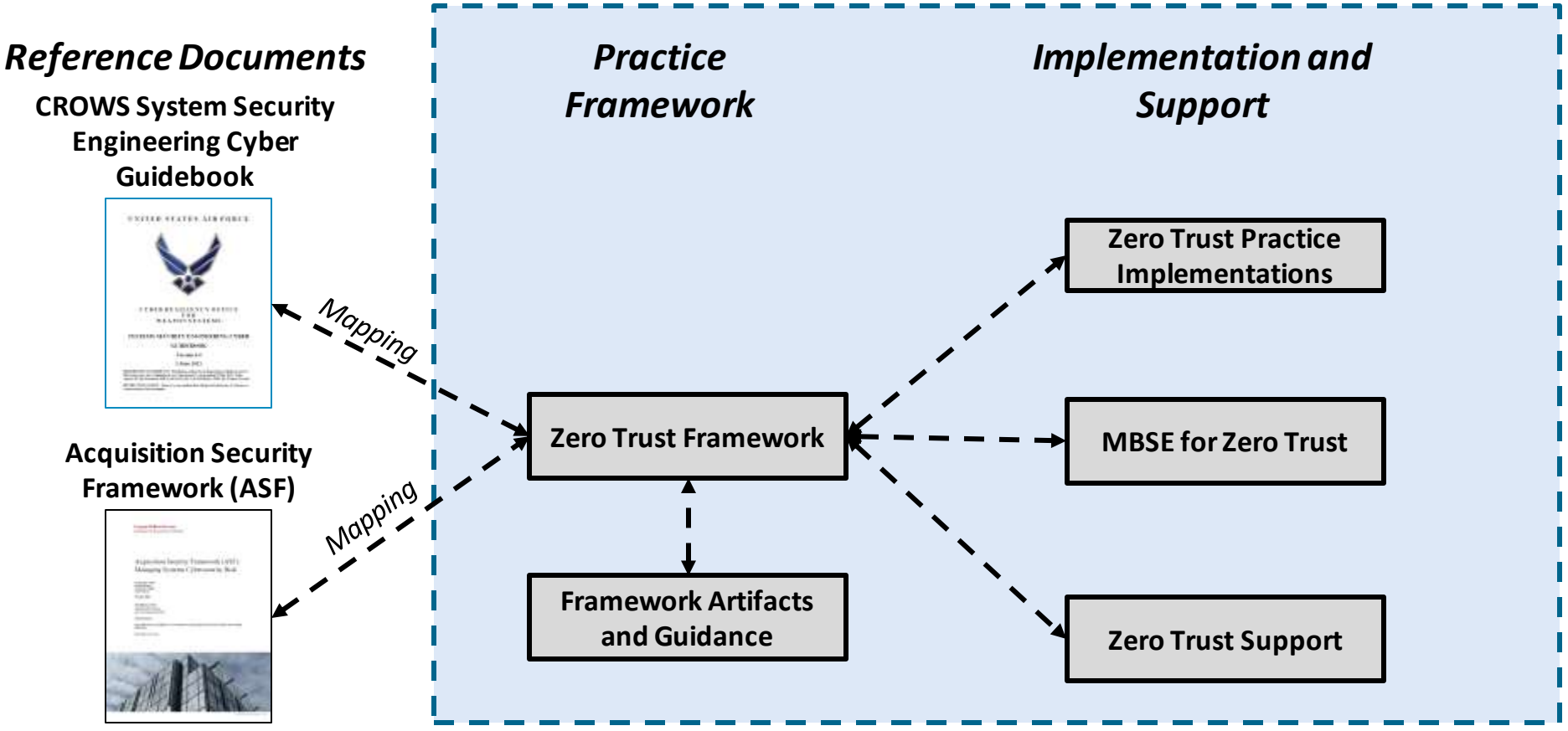
Carnegie Mellon University Software Engineering Institute

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



Focus Areas

Developing context using mission engineering approach enables security architectures to reason about zero trust strategy, design, and possible implementations for weapon systems, as well as enterprises.

Set of zero trust assessments need to be developed to support the life cycle of weapon system/enterprise.

Need to use an approach like ASF to build in security and resilience into weapon systems/enterprise in support of efforts like CROWS SSECG to provide the artifacts to enable zero trust assessments

Backup

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

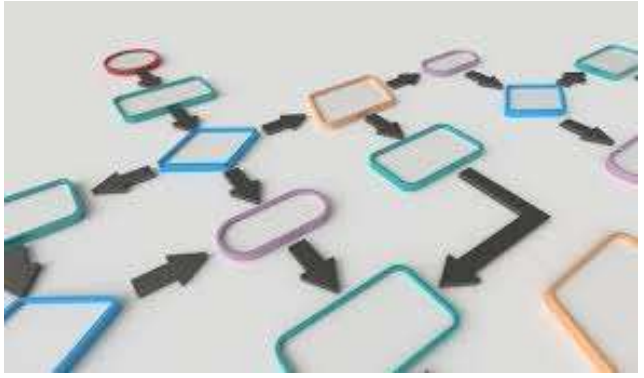
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

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

Links

SEI Zero Trust Industry Day

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=885624

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

Links

Acquisition Security Framework (ASF)

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