

# Zero Trust Journey

Geoff Sanders  
Tim Morrow

October 7, 2021

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

**NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.**

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

DM21-0888

# Agenda

Overview

Challenges

SEI Zero Trust Journey

Next Steps

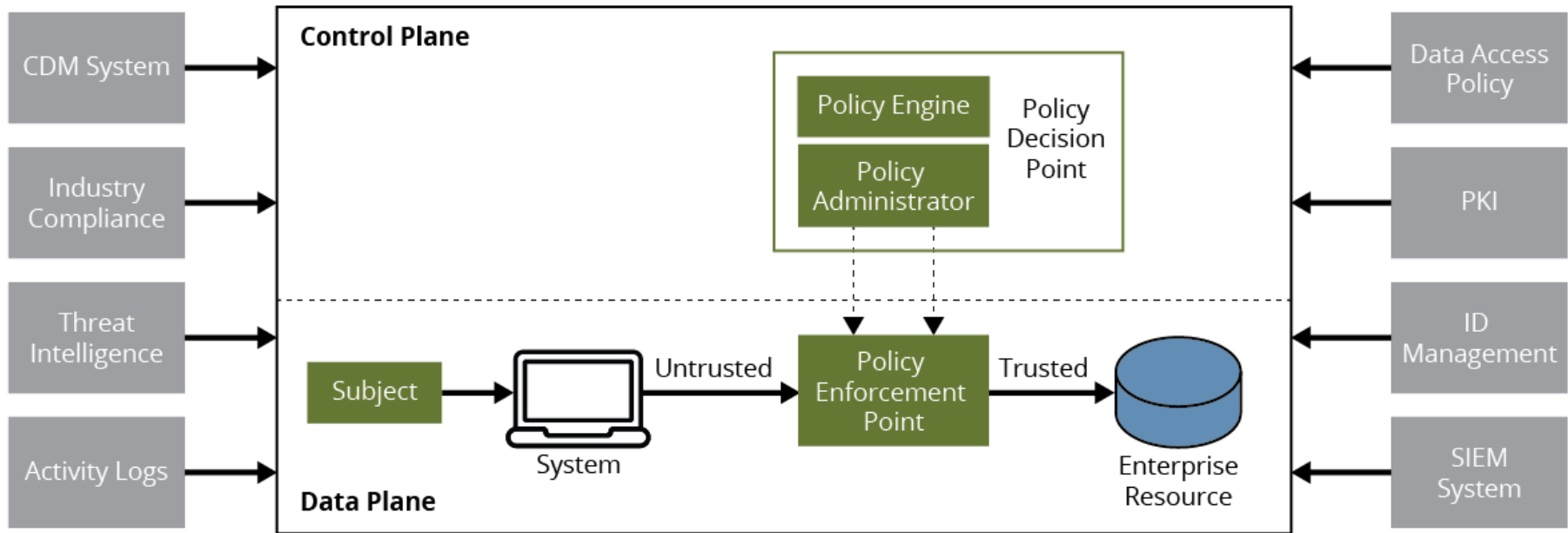
# Zero Trust Tenets

Assume attacker presence.

Remove implicit trust in design and implementation.

Move security from the network to users, applications, and workloads.

# Components (NIST SP 800-207)



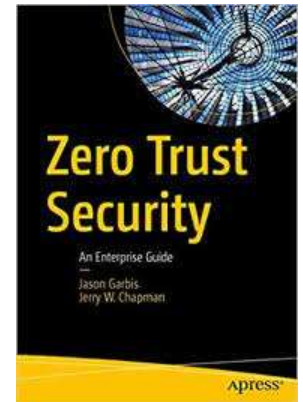
# Guidance



**NIST**



National Cyber  
Security Centre



# Common Challenges

## Governance

- Asset inventory

## Architecture

- Awareness and accuracy

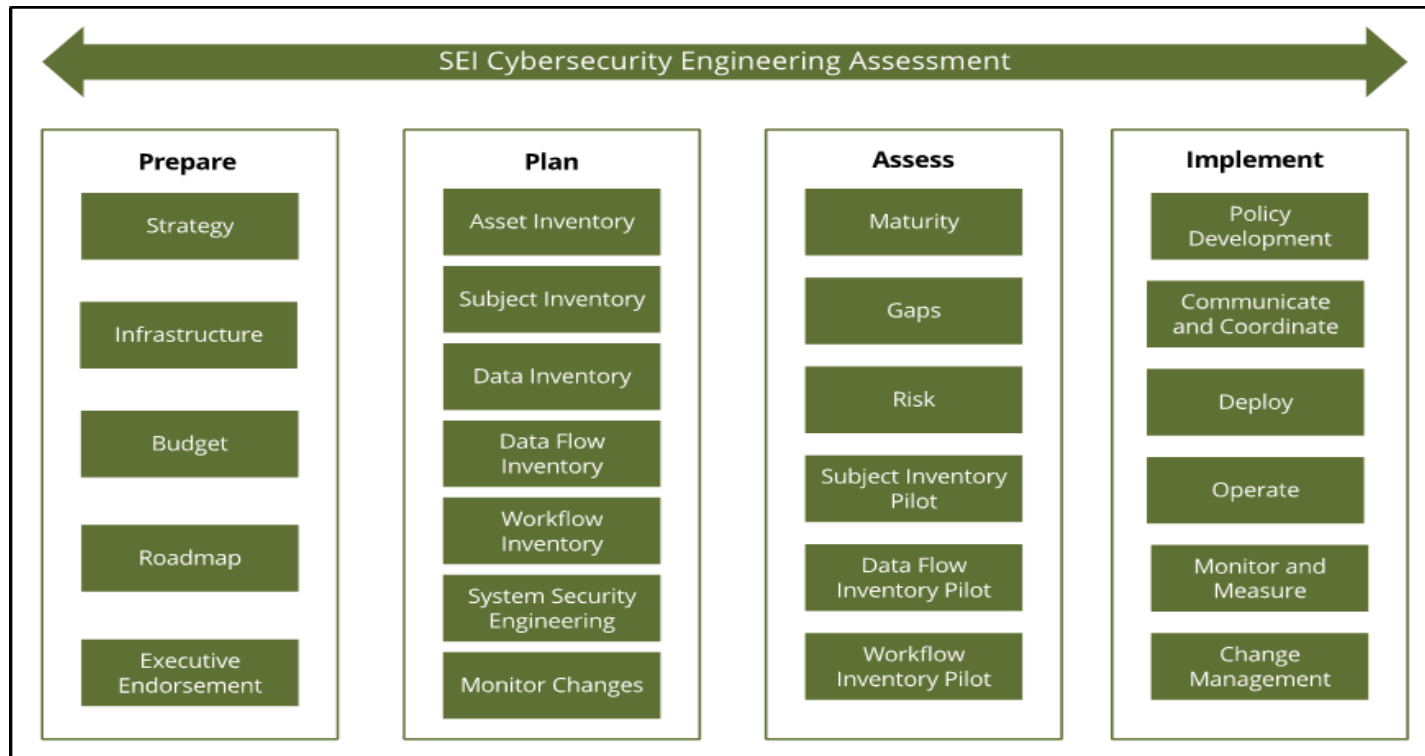
## Cost

- Adoption cost

## Measurement

- Success

# Zero Trust Journey



# Zero Trust Journey

SEI approach combines

- Mission/Business Threads
- Systems Security Engineering (SSE)
- Model-Based Systems Engineering (MBSE)
- Continuous Authorization (cATO) concepts
- Cybersecurity Engineering Assessments

# Mission/Business Threads

Development of vignettes, mission/business threads, and associated architecture documentation provide operational, lifecycle, and development context.

# Systems Security Engineering

Process to achieve identified cybersecurity goals by building security in which supports analysis efforts.

Based on the following artifacts

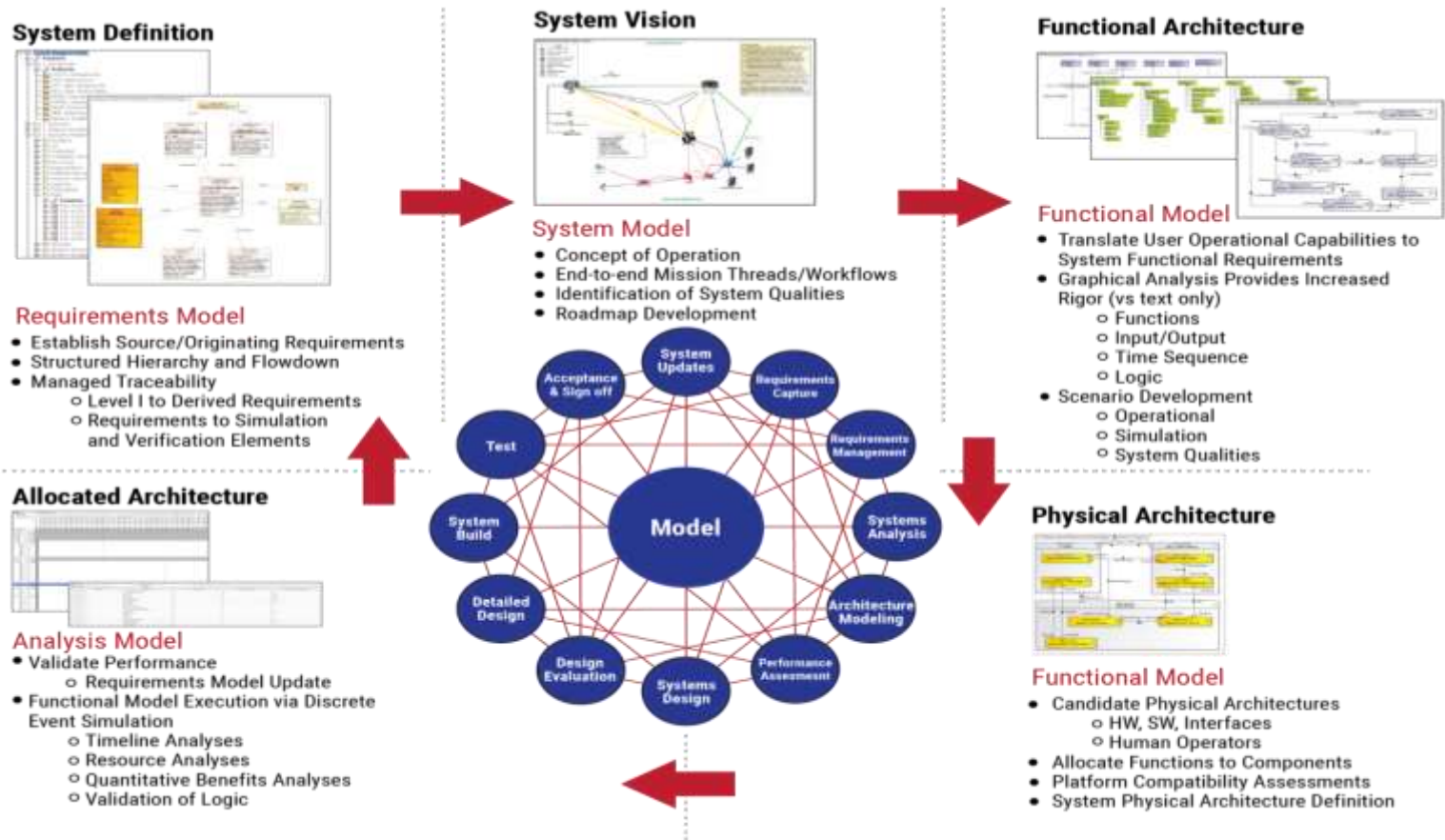
ISO/IEC/IEEE 15288:2015

NIST Special Publication 800-160, Volume 1

NIST Special Publication 800-160, Volume 2

NIST Special Publication 800-37

# Model Based Systems Engineering (MBSE)



# Continuous Authorization to Operate (cATO)

Incorporates the NIST Risk Management Framework (RMF) and continuous monitoring with software engineering activities that leverage cloud computing and cyber-resilient systems engineering.

## Key Conditions

1. Adoption and deliberate use of a secure software supply chain.
2. Complete understanding of activities inside system boundaries including robust continuous monitoring.
3. Ability to conduct active cyber defense in order to respond to cyber threats in real-time.

*\* CrossTalk August 2021, “Exploring the Ingredients of a Continuous Authorization to Operate”, Weiss, J. and Gesling, T.*

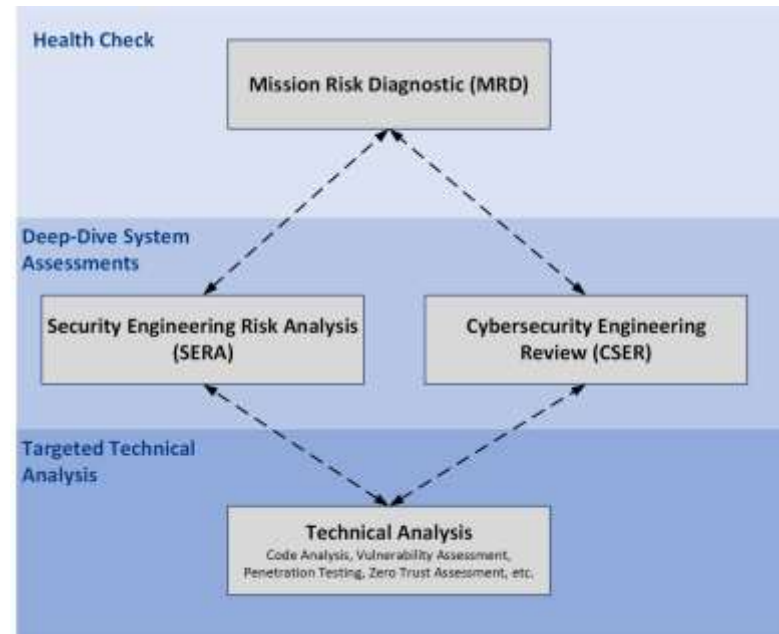
# Cybersecurity Engineering Assessments

SEI is developing an integrated approach for assessing and managing security across the system lifecycle and supply chain.

Health check

Deep-dive system assessments

Targeted technical analysis



# MRD Method

## MRD Platform



## Risk Factors



## Risk Factor Evaluation

**Driver 4: Security Process**

**Driver Question**  
Does the process being used to develop and deploy the system sufficiently address security?

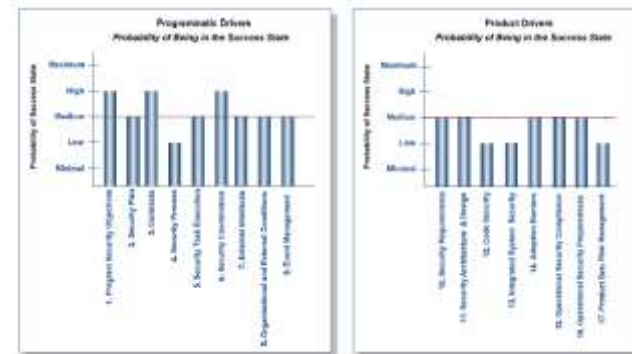
**Considerations:**

- Security-related tasks and activities in the program workflow
- Conformance to security process models
- Measurements and controls for security-related tasks and activities
- Process efficiency and effectiveness
- Software security development life cycle
- Security-related training
- Compliance with security policies, laws, and regulations
- Security of all product-related information

**Response**

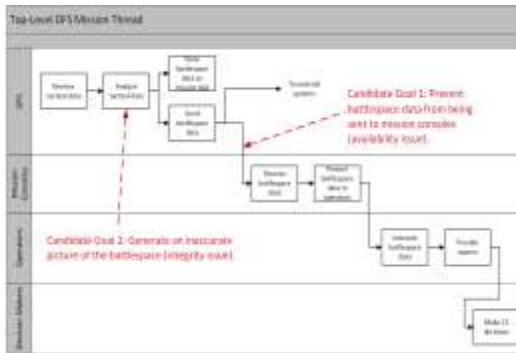
- Yes
- Likely Yes
- Equally Likely
- Likely No
- No
- Don't Know

## Mission Assurance Profile

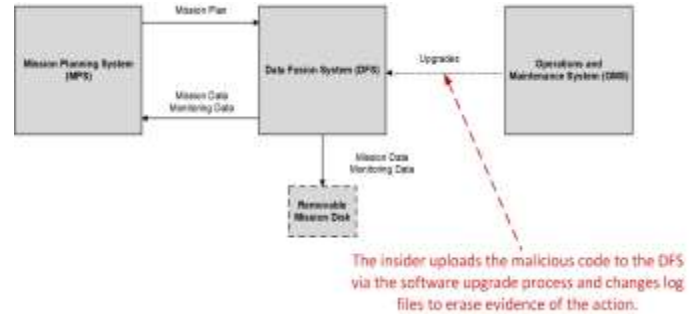


# SERA Method: *Example*

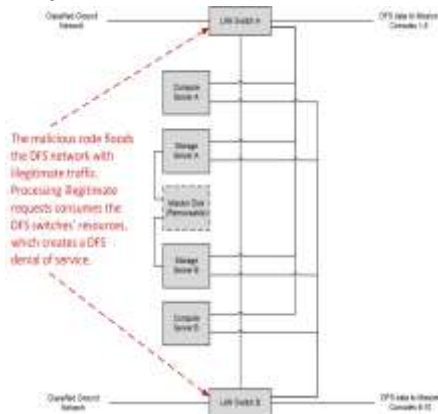
## Mission Thread



## System Interfaces



## System Architecture



## Threat Profile

Step	Knowledge	Candidate Control	NET Mapping
1. An insider with technical skills and administrative access to the Data Fusion Systems (DFS) harvests diagnostic information passed over for a processor and not verifying a return.	Insufficient feedback about employee performance.	The organization's managers are trained to provide concrete, actionable feedback on performance issues.	NET CSP: PS-IP-11 NET 001-03, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-11
2. The insider begins to behave aggressively and stealthily toward coworkers.	Collusion for inappropriate employee behavior.	The organization's managers investigate inappropriate behavior when it occurs and respond appropriately.	NET CSP: PR-IP-10 NET 001-03, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
3. After a while, the insider decides to execute a cyber attack on the DFS. The primary goal is to disrupt or destroy a data-in-transit (DIT) attack on DFS systems.	No simulation to understand employee intent.	The organization's managers investigate an employee's escalating frustration and proactively work to diffuse the situation.	NET CSP: PR-IP-11 NET 001-03, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
4. The insider uses their access to the DFS engineering resources (including their sufficient access control mechanisms) to alter engineering resources. The insider uses physical access to the DFS engineering organization's work space to alter conventional hard copies of DFS engineering documents.	Insufficient access control for administrative and resources (physical and cyber).  Insufficient monitoring of the organizational environment for abnormal activity (physical and cyber).	Physical access to information and resources is managed and protected.  Access permissions and authorizations to computing resources are managed.  The organization monitors the physical environment for abnormal activity.	NET CSP: PS-AC-2 NET 001-03, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-8  NET CSP: PR-AC-9 NET 001-03, AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11  NET CSP: IS-0202 NET 001-03, CA-7, PS-3, PS-8, PS-9
		The organization monitors systems and networks for abnormal activity.	NET CSP: DE-08-1 NET 001-03, AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11
		The organization performs targeted monitoring of individuals with suspected behavioral issues.	NET CSP: IS-0203 NET 001-03, AC-1, AC-2, AC-3, AC-4, CA-1, CA-2, CA-3, CA-4, CA-5, CA-6, CA-7, CA-8, CA-9, CA-10, CA-11
		The organization responds appropriately when abnormal activity is detected.	NET CSP: PS-AB-1, PS-AB-2 NET 001-03, PS-4

# CSE Lifecycle Roadmap

A collection of cybersecurity engineering practices and competencies that can be applied across a system lifecycle.

1. Security risk assessment
2. Requirements
3. Architecture and design
4. Implementation
5. Developmental test and evaluation (DT&E)
6. Operational test and evaluation (OT&E)
7. Operations and sustainment (O&S)

Each area includes

- *Practices*
- *Evidence*
- *Competencies*

# Next Steps

Pilots

ZT Journey paper

Document CSE assessment application.

Example enterprise ZT Journey.

# Contact Information

Geoff Sanders

CERT Division

Senior Network Defense Analyst

[gtsanders@cert.org](mailto:gtsanders@cert.org)

703.247.1393

Tim Morrow

CERT Division

Situational Awareness Technical Manager

[tbm@sei.cmu.edu](mailto:tbm@sei.cmu.edu)

412.268.4792