Zero Trust Journey

Geoff Sanders
Tim Morrow

October 7, 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM21-0888

Agenda

Overview

Challenges

SEI Zero Trust Journey

Next Steps

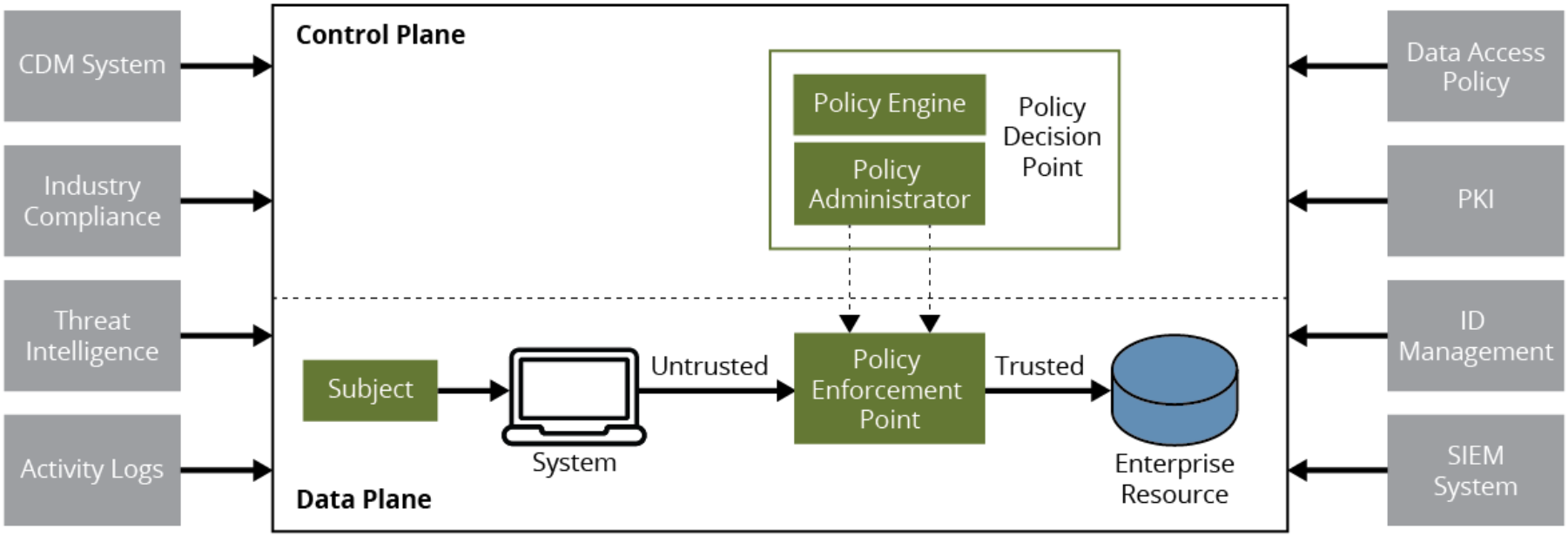
Zero Trust Tenets

Assume attacker presence.

Remove implicit trust in design and implementation.

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

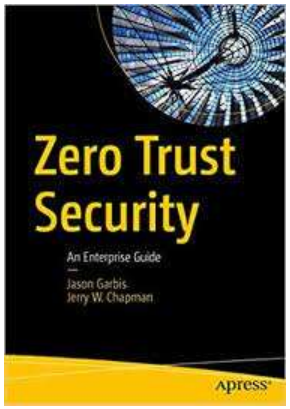
Components (NIST SP 800-207)



Guidance

NIST

National Cyber Security Centre



Common Challenges

Governance

- Asset inventory

Architecture

- Awareness and accuracy

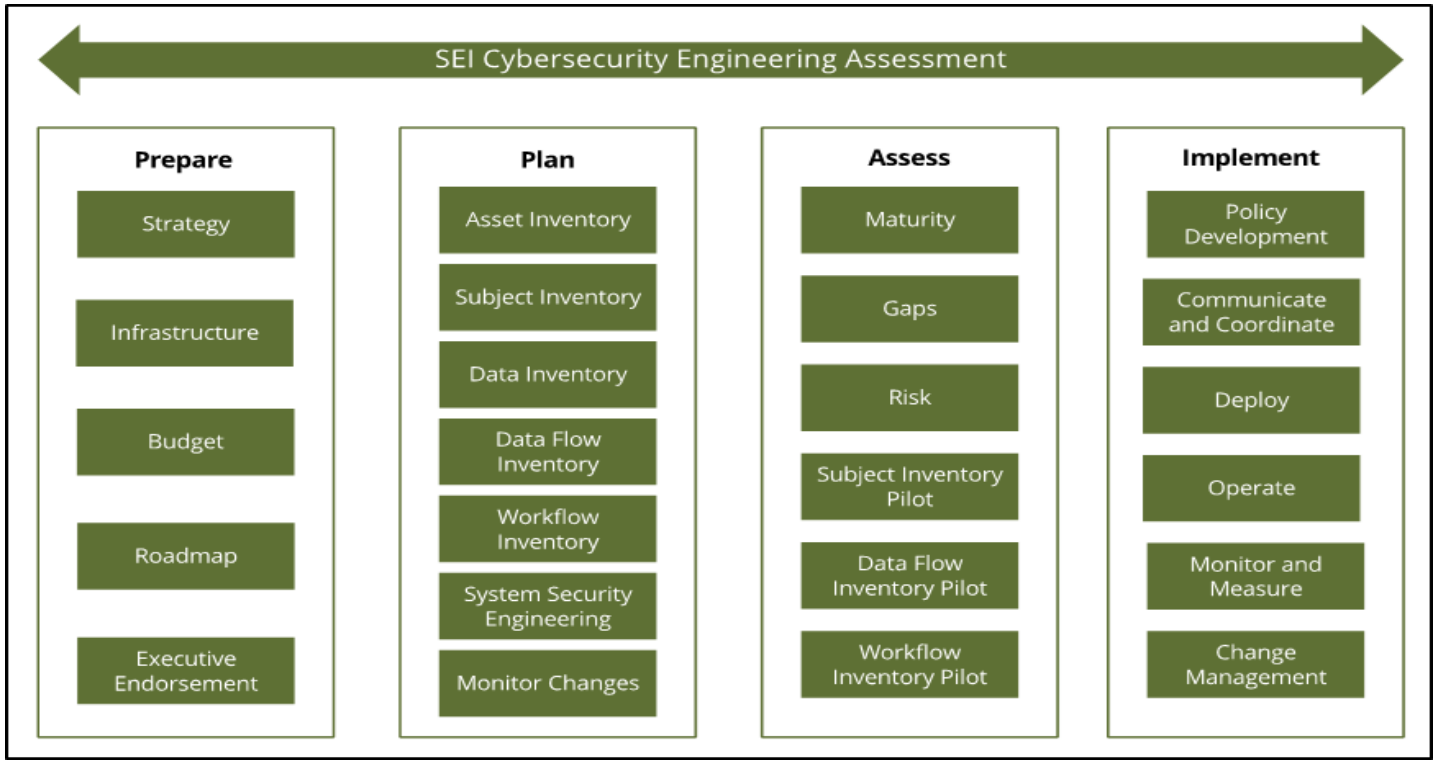
Cost

- 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

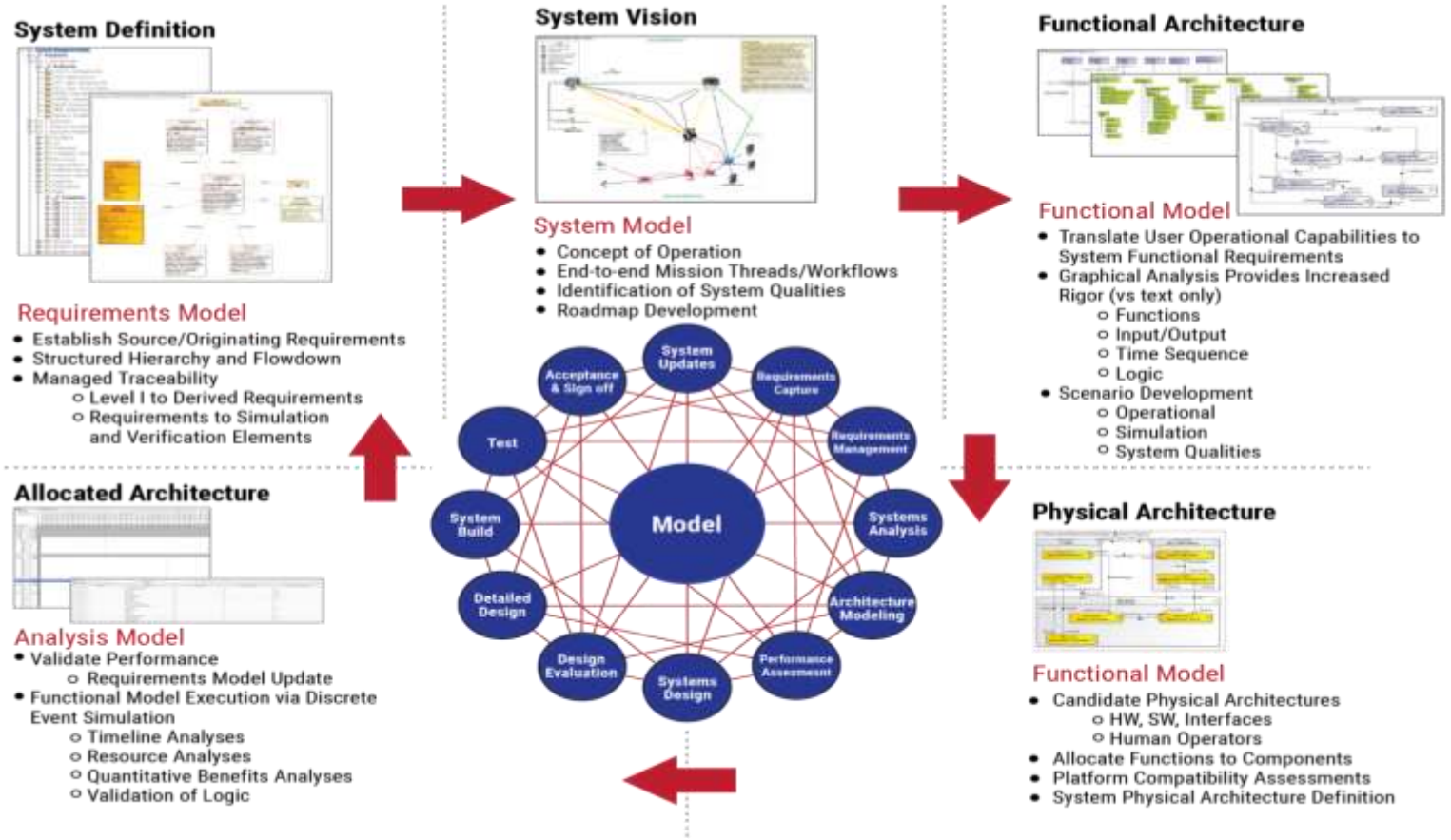
ISO/IEC/IEEE 15288:2015

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.*

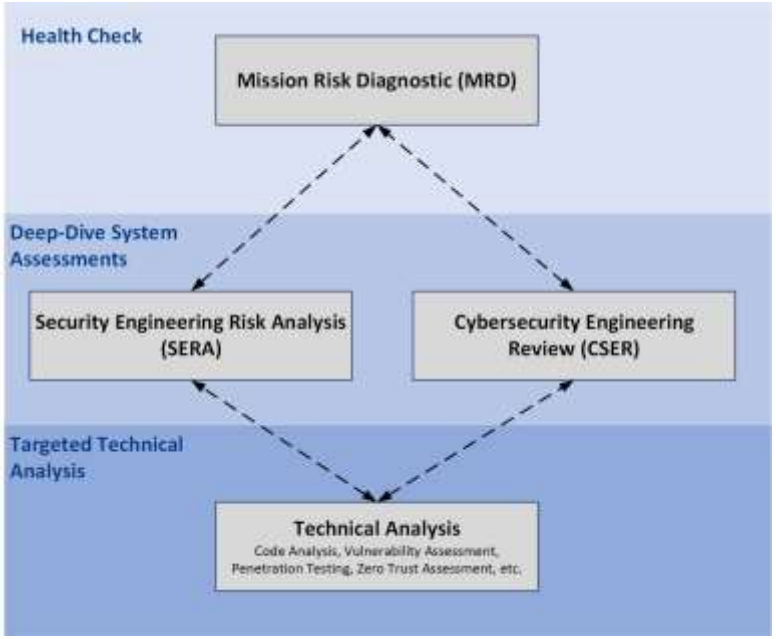
Cybersecurity Engineering Assessments

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

Health check

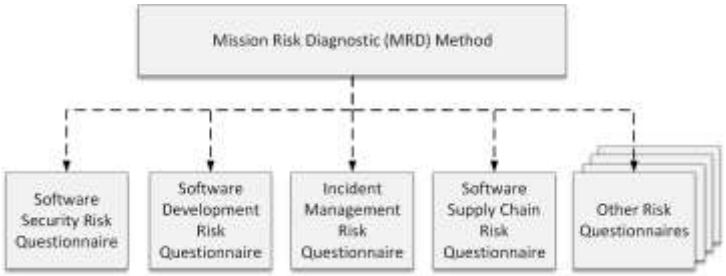
Deep-dive system assessments

Targeted technical analysis

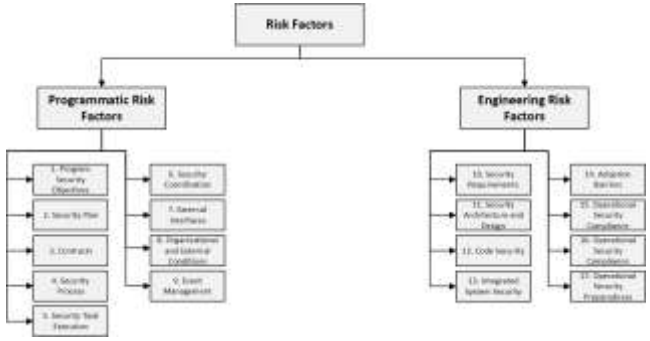


MRD Method

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?

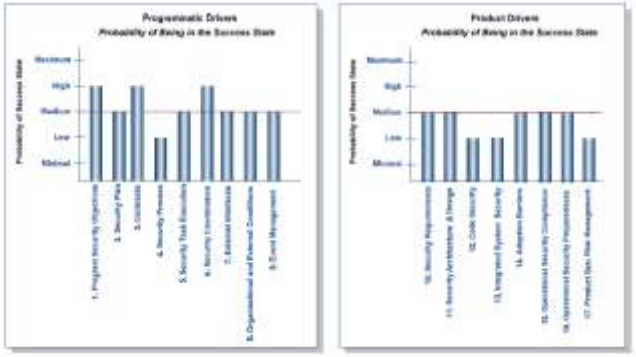
Considerations:

- 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

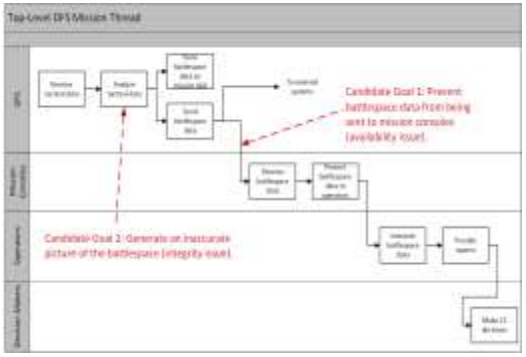
- ❑ Yes
- ❑ Likely Yes
- ❑ Equally Likely
- ❑ Likely No
- ❑ No
- ❑ Don't Know

Mission Assurance Profile

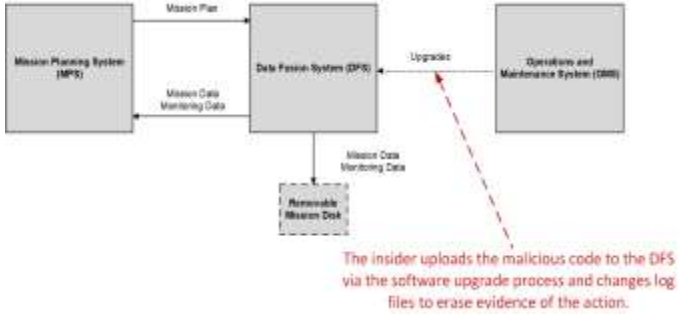


SERA Method: *Example*

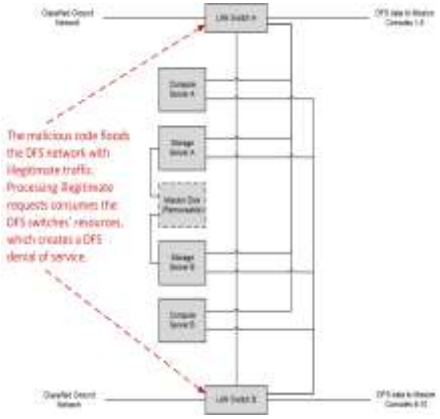
Mission Thread



System Interfaces



System Architecture



Threat Profile

Step	Enabler	Candidate Control	NIST Mapping
1	Insufficient feedback about employee performance	The organization's managers are trained to provide constructive feedback on performance issues.	NIST CSF: PR.IP-11 NIST 800-53: PS-1, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
2	Tolerance for inappropriate employee behavior	The organization's managers recognize inappropriate behavior when it occurs and respond appropriately.	NIST CSF: PR.IP-11 NIST 800-53: PS-1, PS-2, PS-3, PS-4, PS-6, PS-8, PS-7, PS-8, SA-21
3	No escalation to underlying employee issue	The organization's managers recognize an employee's escalating frustration and proactively work to diffuse the situation.	NIST CSF: PR.IP-11 NIST 800-53: PS-1, PS-2, PS-3, PS-4, PS-6, PS-8, PS-7, PS-8, SA-21
4	Insufficient access control for information and resources (physical and cyber)	Physical access to information and resources is managed and protected.	NIST CSF: PR.AC-2 NIST 800-53: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		Access permissions and authorizations for computing resources are managed.	NIST CSF: PR.AC-4 NIST 800-53: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
	Insufficient monitoring of the organizational environment for abnormal activity (physical and cyber)	The organization monitors the physical environment for abnormal activity.	NIST CSF: DE.CM-2 NIST 800-53: CA-7, PE-3, PE-6, PE-20
		The organization monitors systems and networks for abnormal activity.	NIST CSF: DE.CM-1 NIST 800-53: AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		The organization performs targeted monitoring of individuals with suspected behavioral issues.	NIST CSF: DE.CM-3 NIST 800-53: AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		The organization responds appropriately when abnormal activity is detected.	NIST CSF: RS.RP-1, RS.AN-2 NIST 800-53: IR-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

703.247.1393

Tim Morrow

CERT Division

Situational Awareness Technical Manager

tbm@sei.cmu.edu

412.268.4792