Zero Trust Journey

Geoff Sanders
Tim Morrow

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Carnegie Mellon University
Software Engineering Institute

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

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.

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.

DM21-0888

Agenda

Overview

Challenges

SEI Zero Trust Journey

Next Steps

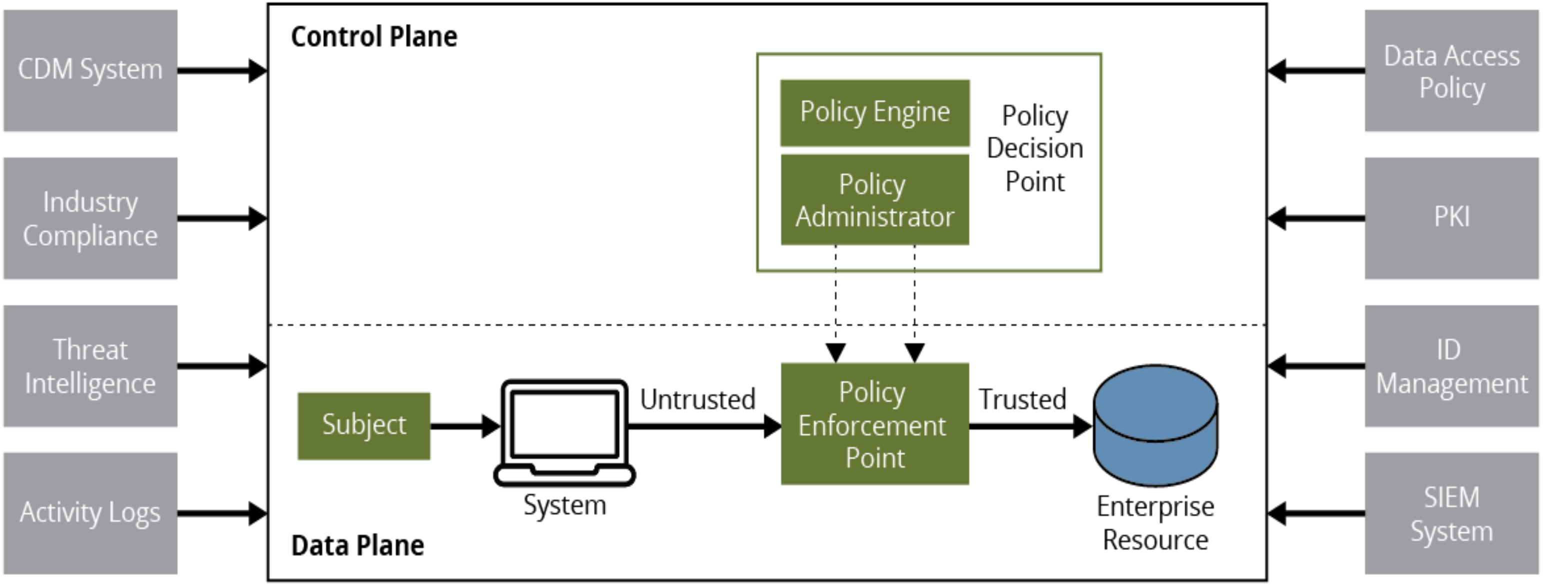
Zero Trust Tenets

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)



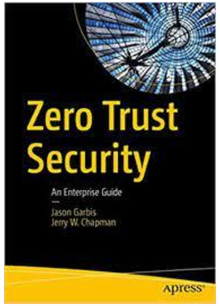
[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Guidance

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NIST



Zero Trust Security

An Enterprise Guide

Jason Garbis
Jerry W. Chapman

Apress

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

DIEU ET MON DROIT

National Cyber
Security Centre

Common Challenges

Governance

- Asset inventory

Architecture

- Awareness and accuracy

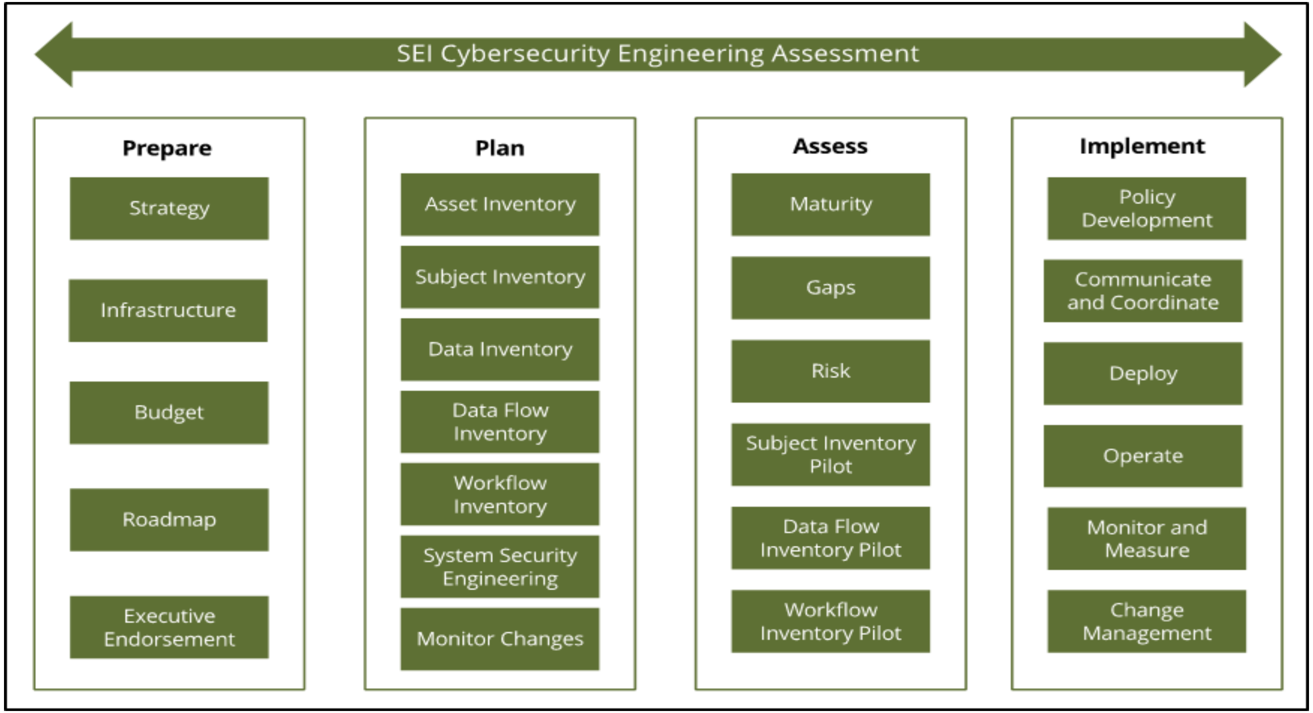
Cost

- Adoption cost

Measurement

- Success

Zero Trust Journey



[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

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 that provide operational, lifecycle, and development context.

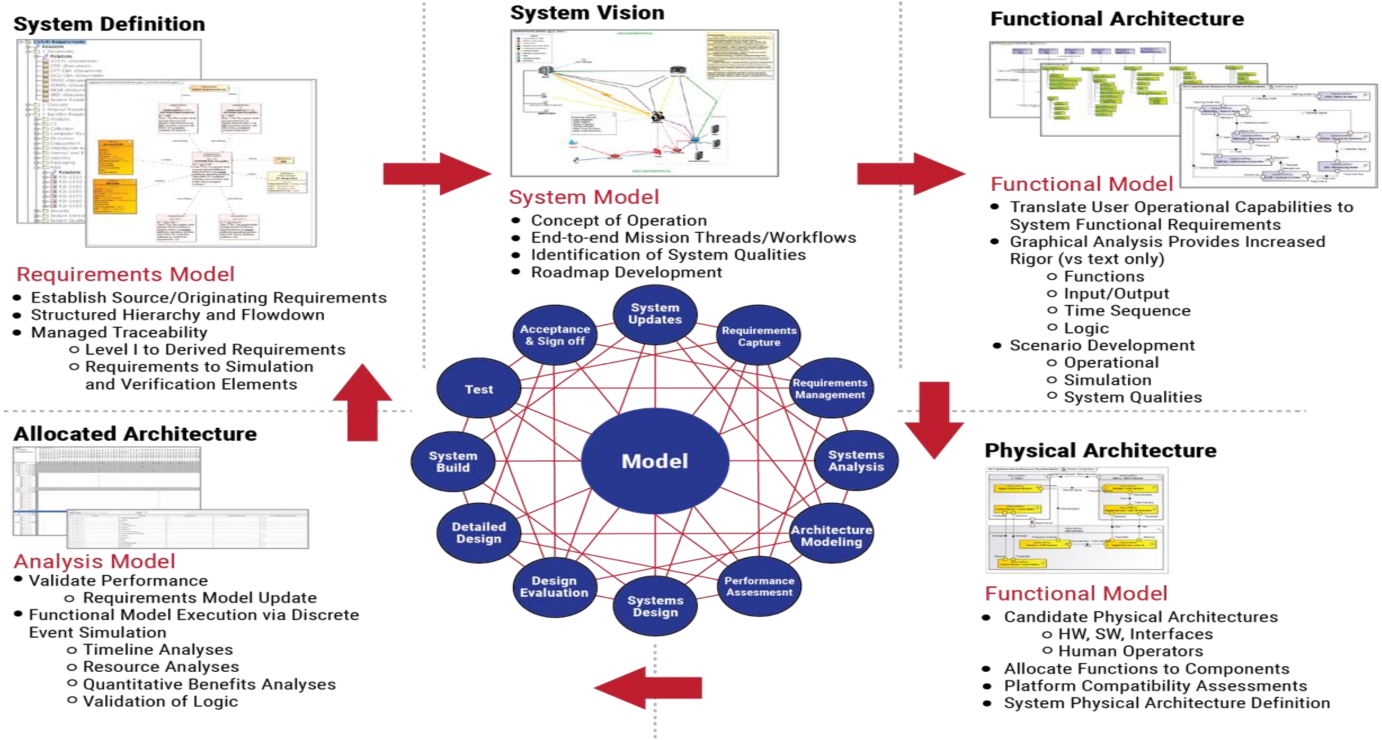
Systems Security Engineering

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)



System Definition

Requirements Model

- Establish Source/Originating Requirements
- Structured Hierarchy and Flowdown
- Managed Traceability
  - Level I to Derived Requirements
  - Requirements to Simulation and Verification Elements

System Vision

System Model

- Concept of Operation
- End-to-end Mission Threads/Workflows
- Identification of System Qualities
- Roadmap Development

Functional Architecture

Functional Model

- Translate User Operational Capabilities to System Functional Requirements
- Graphical Analysis Provides Increased Rigor (vs text only)
  - Functions
  - Input/Output
  - Time Sequence
  - Logic
- Scenario Development
  - Operational
  - Simulation
  - System Qualities

Physical Architecture

Functional Model

- Candidate Physical Architectures
  - HW, SW, Interfaces
  - Human Operators
- Allocate Functions to Components
- Platform Compatibility Assessments
- System Physical Architecture Definition

Allocated Architecture

Analysis Model

- Validate Performance
  - Requirements Model Update
- Functional Model Execution via Discrete Event Simulation
  - Timeline Analyses
  - Resource Analyses
  - Quantitative Benefits Analyses
  - Validation of Logic

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.*

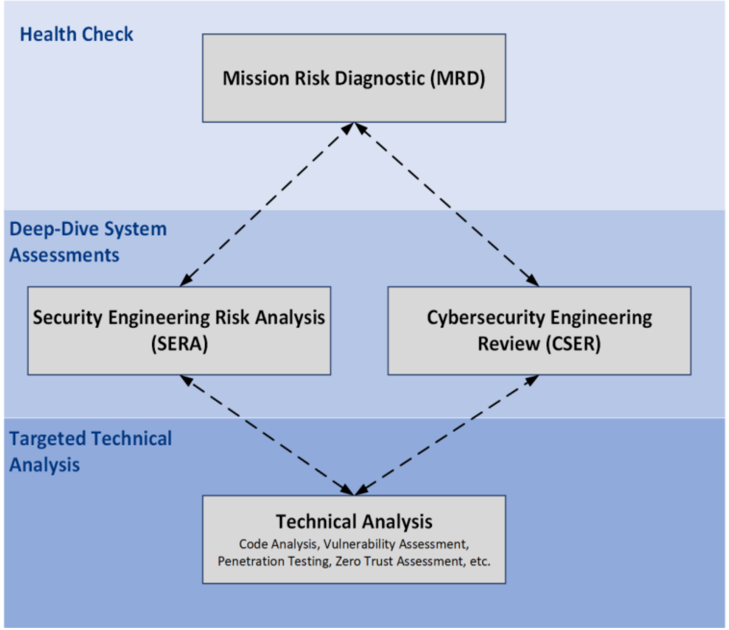
Cybersecurity Engineering Assessments

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

Health check.

Deep-dive system assessments.

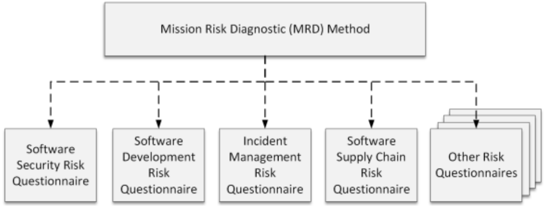
Targeted technical analysis.


Health Check
Mission Risk Diagnostic (MRD)
Deep-Dive System Assessments
Security Engineering Risk Analysis (SERA)
Cybersecurity Engineering Review (CSER)
Targeted Technical Analysis
Technical Analysis
Code Analysis, Vulnerability Assessment, Penetration Testing, Zero Trust Assessment, etc.

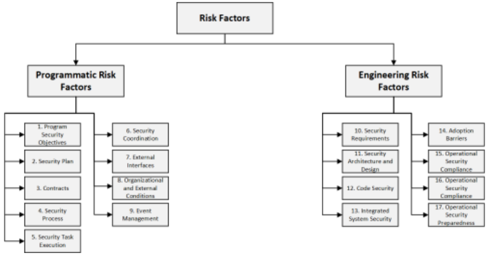
[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

MRD Method

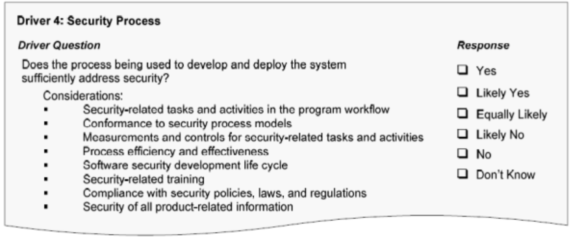
MRD Platform


Mission Risk Diagnostic (MRD) Method
Software Security Risk Questionnaire
Software Development Risk Questionnaire
Incident Management Risk Questionnaire
Software Supply Chain Risk Questionnaire
Other Risk Questionnaires

Risk Factors


Risk Factors
Programmatic Risk Factors
Engineering Risk Factors
1. Program Security Objectives
2. Security Plan
3. Contracts
4. Security Process
5. Security Task Execution
6. Security Coordination
7. External Interfaces
8. Organizational and External Conditions
9. Event Management
10. Security Requirements
11. Security Architecture and Design
12. Code Security
13. Integrated System Security
14. Adoption Barriers
15. Operational Security Compliance
16. Operational Security Compliance
17. Operational Security Preparedness

Risk Factor Evaluation



Driver 4: Security Process

Driver Question

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

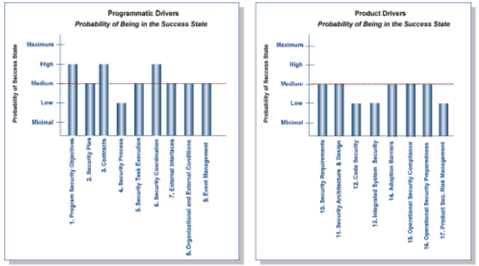
Considerations:

- 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

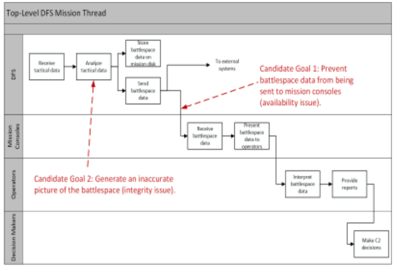
❑ Yes
❑ Likely Yes
❑ Equally Likely
❑ Likely No
❑ No
❑ Don't Know

Mission Assurance Profile



SERA Method: *Example*

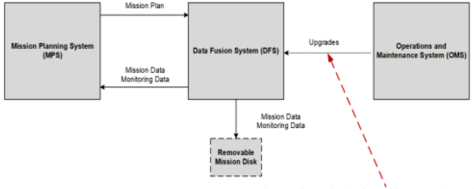
Mission Thread



Candidate Goal 1: Prevent battlespace data from being sent to mission consoles (availability issue).

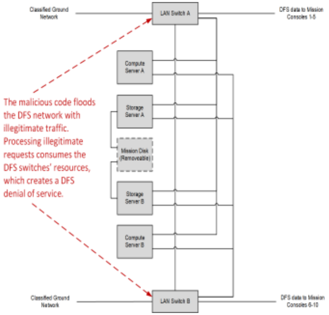
Candidate Goal 2: Generate an inaccurate picture of the battlespace (integrity issue).

System Interfaces


Mission Plan
Mission Planning System (MPS)
Data Fusion System (DFS)
Operations and Maintenance System (OMS)
Upgrades
Mission Data Monitoring Data
Mission Data Monitoring Data
Removable Mission Disk

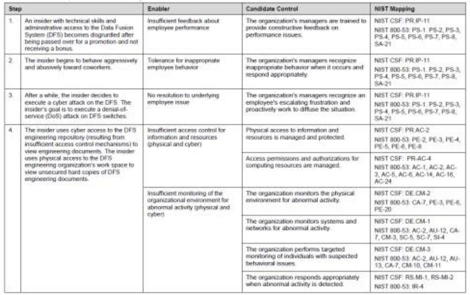
The insider uploads the malicious code to the DFS via the software upgrade process and changes log files to erase evidence of the action.

System Architecture


Classified Ground Network
LAN Switch A
DFS data to Mission Consoles 1-5
Compute Server A
Storage Server A
Mission Disk (Removeable)
Storage Server B
Compute Server B
Classified Ground Network
LAN Switch B
DFS data to Mission Consoles 6-10

The malicious code floods the DFS network with illegitimate traffic. Processing illegitimate requests consumes the DFS switches' resources, which creates a DFS denial of service.

Threat Profile



Step		Enabler	Candidate Control	NIST Mapping
1.	An insider with technical skills and administrative access to the Data Fusion System (DFS) becomes disgruntled after being passed over for a promotion and not receiving a bonus.	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-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
2.	The insider begins to behave aggressively and abusively toward coworkers.	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-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 insider's goal is to execute a denial-of-service (DoS) attack on DFS switches.	No resolution 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-5, PS-6, PS-7, PS-8, SA-21
4.	The insider uses cyber access to the DFS engineering repository (resulting from insufficient access control mechanisms) to view engineering documents. The insider uses physical access to the DFS engineering organization's work space to view unsecured hard copies of DFS engineering documents.	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.MI-1, RS-MI-2 NIST 800-53: IR-4

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

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