

# Zero Trust Discussion

Greg Touhill

Geoff Sanders

Tim Morrow

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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).

DM21-0900

# Agenda

Overview

Campus Zero Trust Security Interest

Challenges

SEI Zero Trust Journey

Next Steps

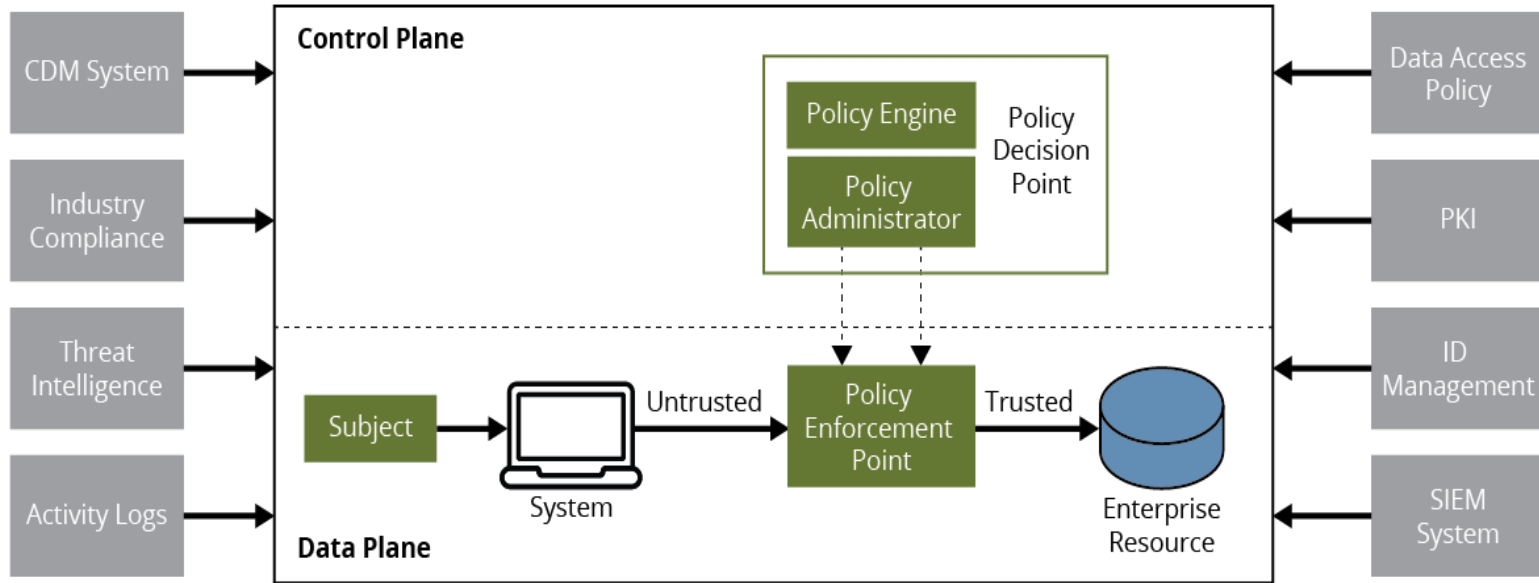
# Zero Trust Tenets

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

# Campus Zero Trust Security Interest

University appears to focus on Google's office products. Is BeyondCorp being considered for Zero Trust or are there other initiatives being pursued?

International campuses – Are all treated the same way from a security standpoint?

Curious as to how comfortable you are with how the university's is keeping track of its inventories of assets, subjects, data, data flows, and workflows?

What is the security strategy that your office is pursuing?

# Common Challenges

## Governance

- Asset inventory

## Architecture

- Awareness and accuracy

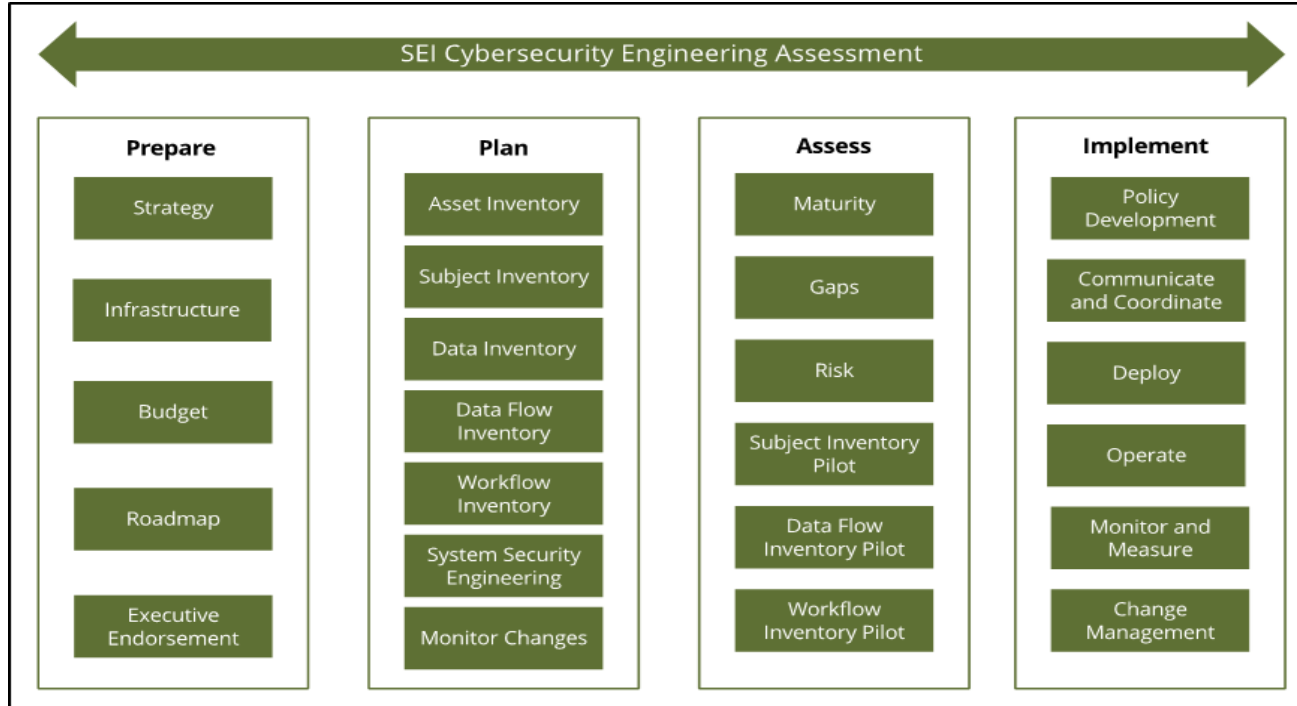
## Cost

- 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 that provide operational, lifecycle, and development context.

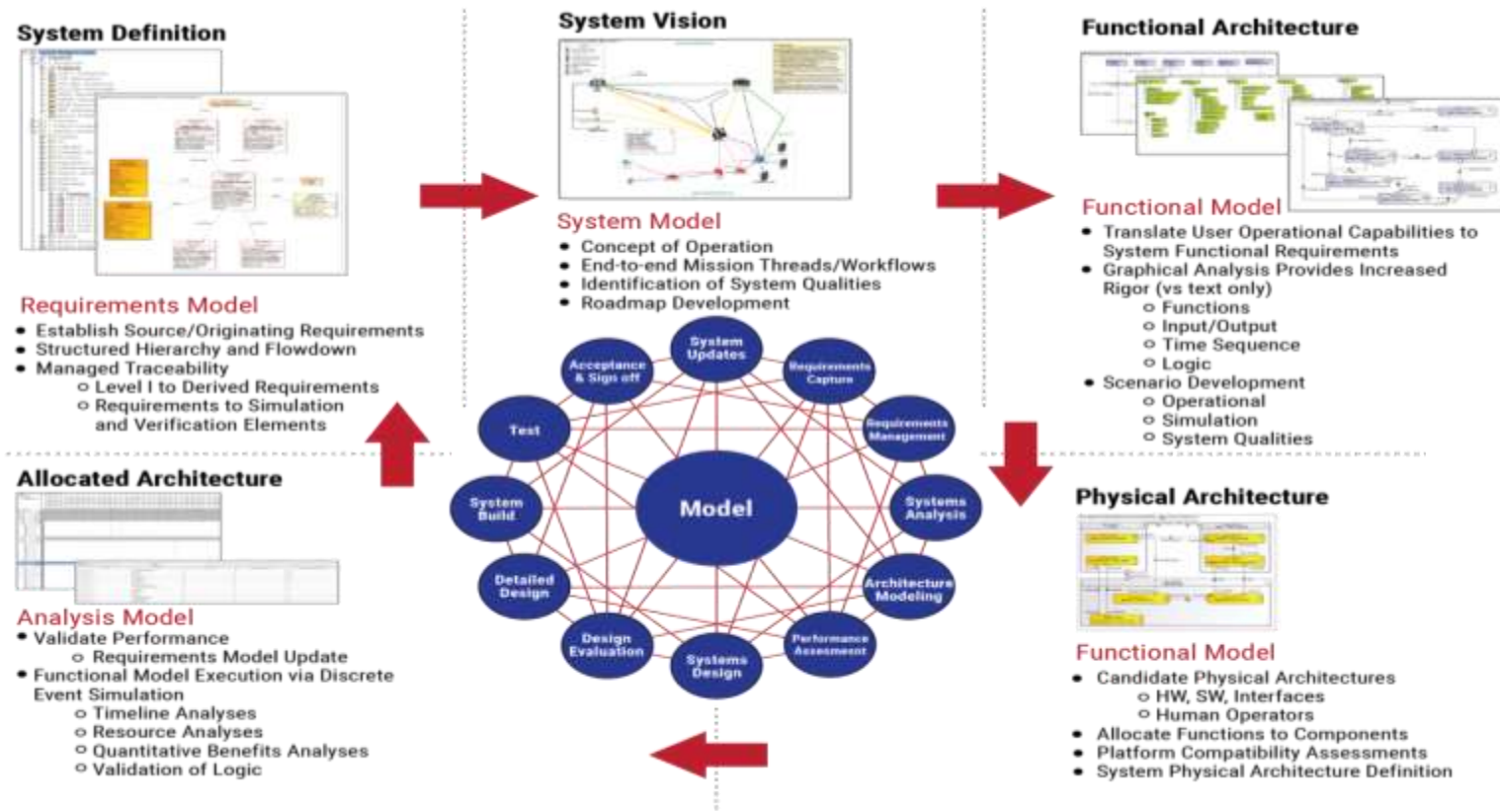
# Systems Security Engineering

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)



# 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.*

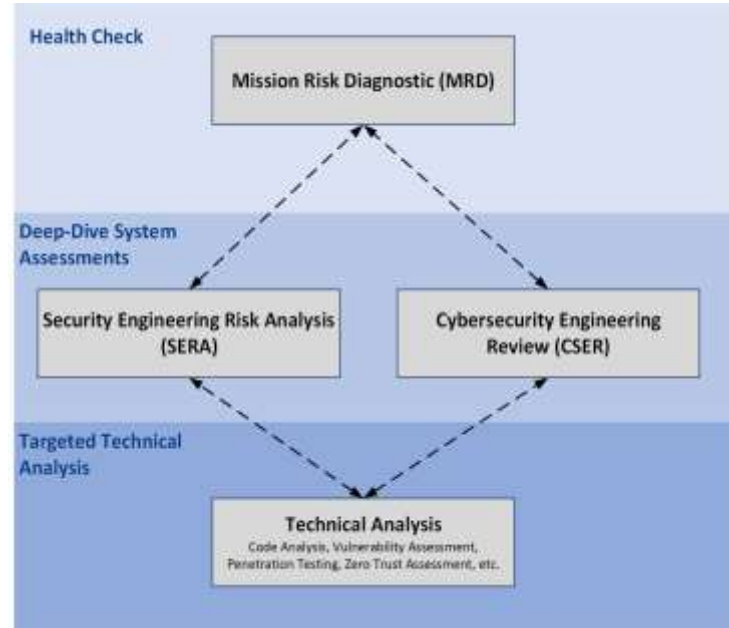
# Cybersecurity Engineering Assessments

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.



# Next Steps

Pilots.

ZT Journey paper.

Document CSE assessment application.

Example enterprise ZT Journey.

# Contact Information

Greg Touhill

Director, CERT Division

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

412.268.4728

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@cert.org](mailto:tbm@cert.org)

412.268.4792