Using a Scenario to Reason About Implementing a Zero Trust Strategy

Tim Morrow

Rhonda Brown

Elias Miller

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.

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.

DM24-0515

Overview

Security model developed by John Kindervag and team at Forrester approximately 2009.

Goals

- Remove implicit trust.
- Move security from the network to users, applications, and workloads.

NIST Special Publication 800-207 Zero Trust Architecture

- Identifies Zero Trust Architecture (ZTA) as a strategy

Zero Trust will be a journey.

[NIST 800-207 2020]

Principles

Ensure all resources are accessed securely, regardless of location.

Adopt a least privilege strategy and strictly enforce access control.

Inspect and log all traffic.

Ensure all components support application programming interface (API)s for event and data exchange.

Automate actions across environments and systems, driven by context and events.

Audit continuously.

[Zero Trust Security 2021]

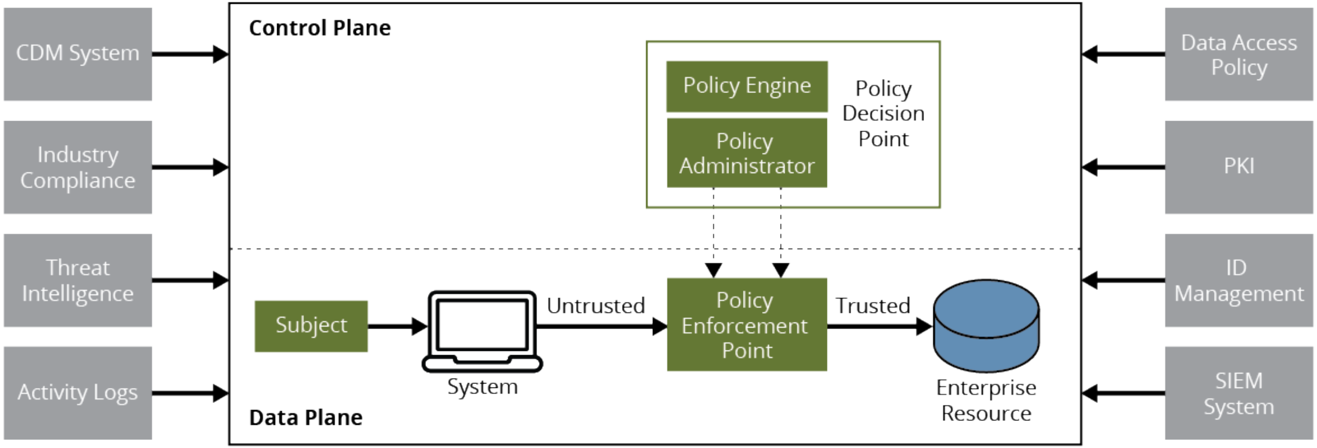
Working Definition

A zero trust system is an *integrated security platform* that uses *contextual information* from identity, security and IT infrastructure, and risk analytics tools to inform and enable the *dynamic enforcement of security policies uniformly across the enterprise*.

Zero trust shifts security from an ineffective perimeter-centric model to a *resource- and identity-centric model*. As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility.

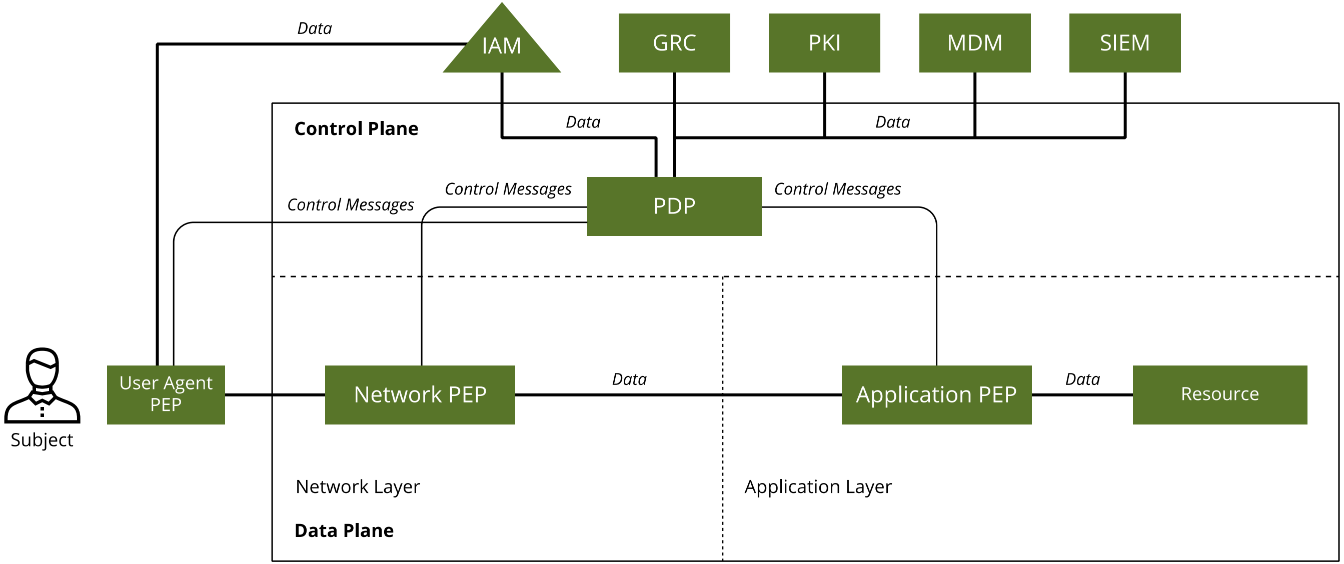
[Zero Trust Security 2021]

NIST Zero Trust Architecture Components



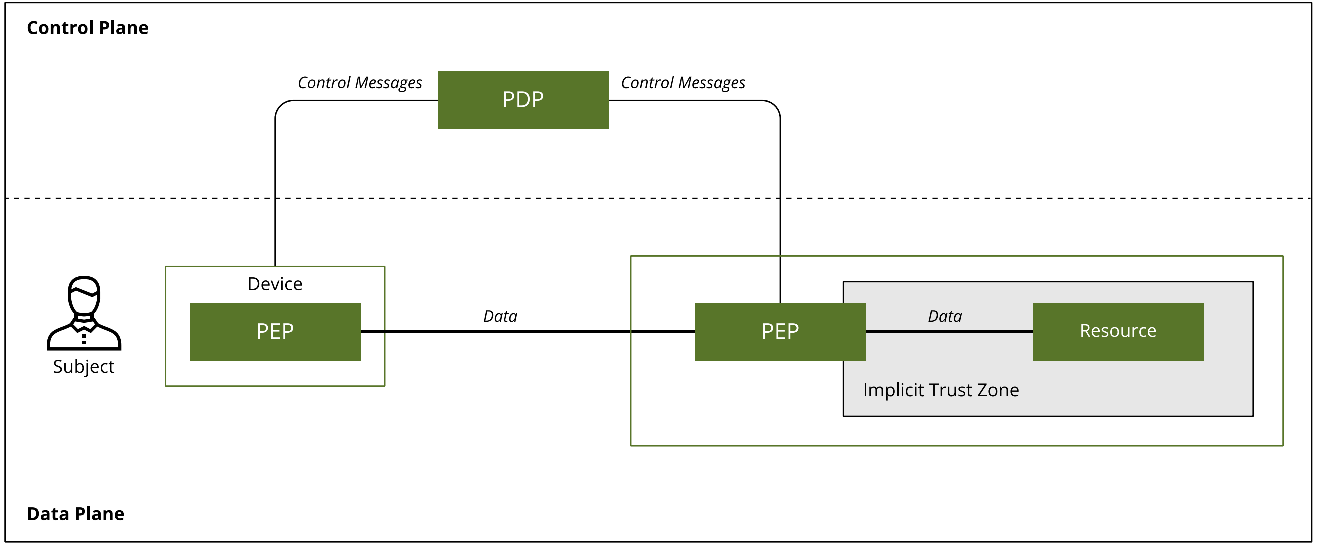
[NIST 800-207 2020]

Policy Enforcement Point Types



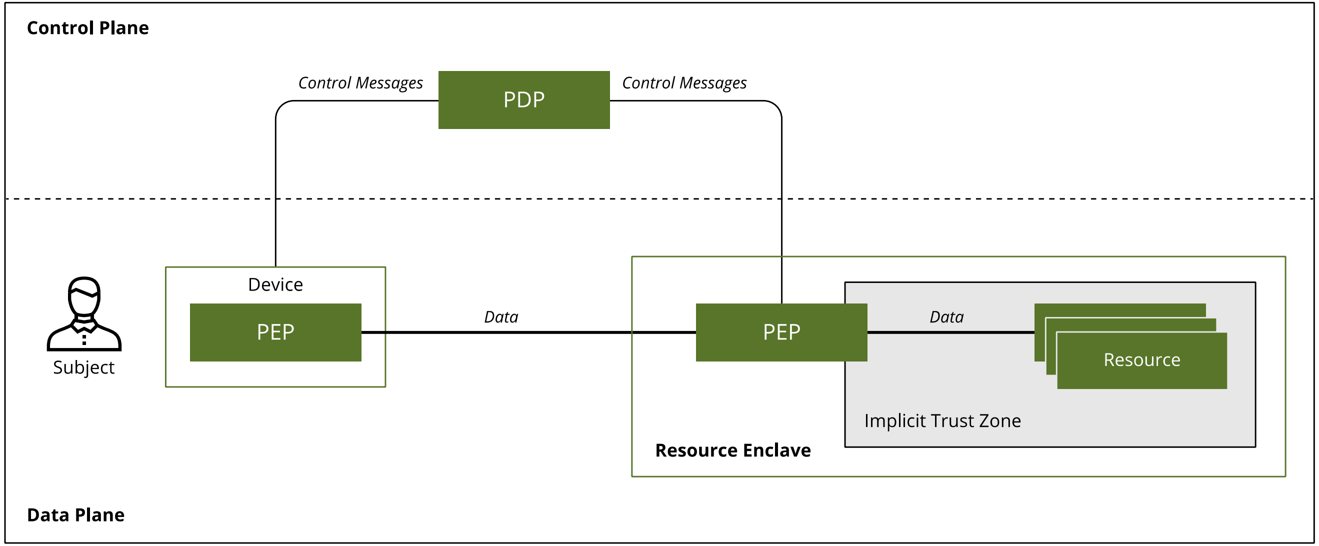
[Zero Trust Security 2021]

Resource-Based Deployment Model



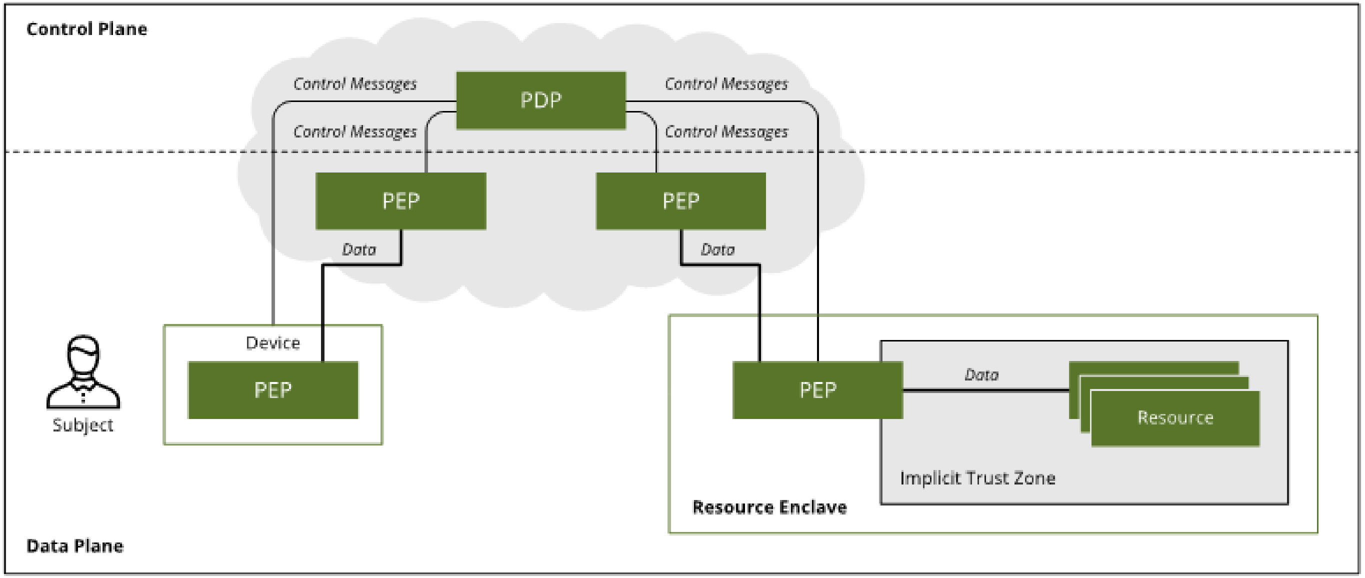
[Zero Trust Security 2021]

Enclave-Based Deployment Model



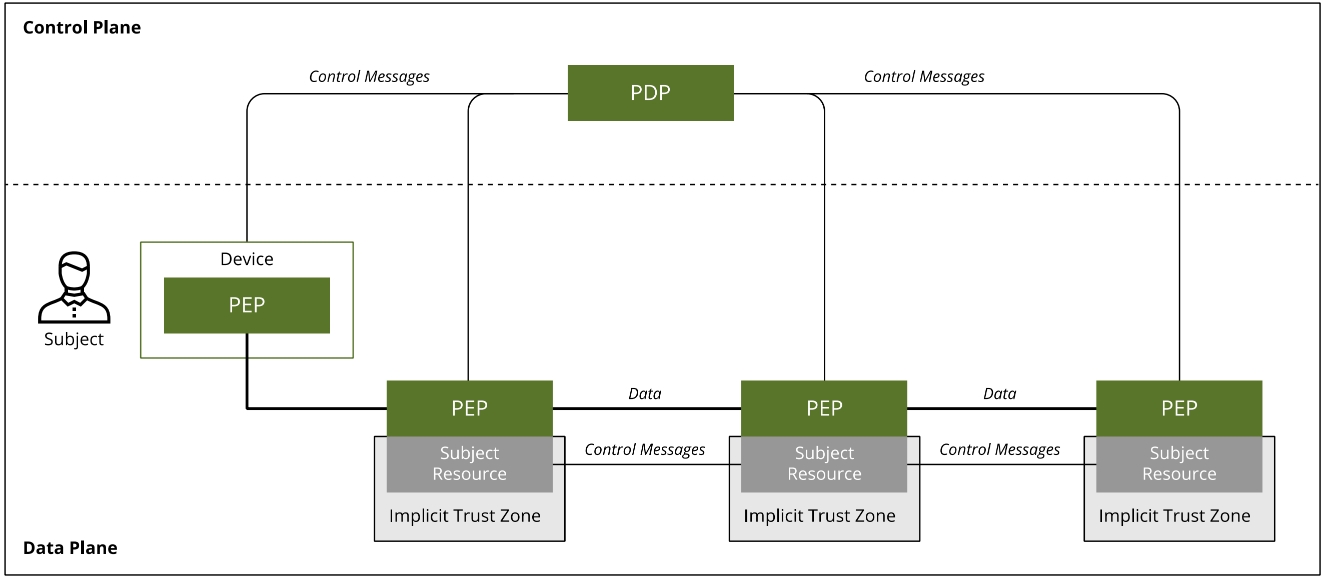
[Zero Trust Security 2021]

Cloud-Routed Deployment Model



[Zero Trust Security 2021]

Microsegmentation Deployment Model



[Zero Trust Security 2021]

Zero Trust Planning

Strategy Comes First, Understanding Your Data Comes Next.

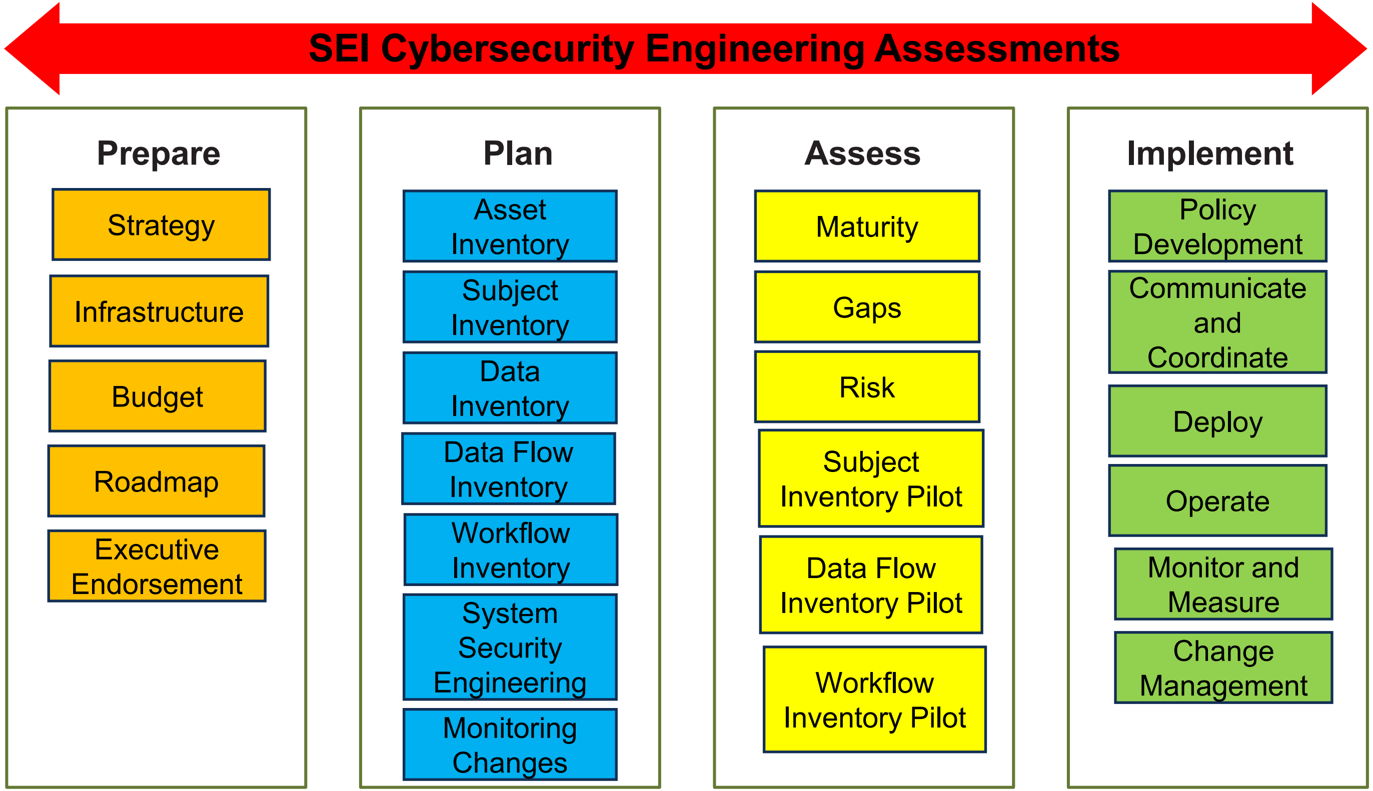
- Defining the authorizations, conditions, and entitlements to access data represents approximately 83% of ZT implementation costs. (Based on Greg Touhill's research at CMU's Heinz College)

Adopt the Zero Trust security strategy

- "Zero Trust is the starting point on the road to Digital Trust"
- People, Process, Technology (aka hw/sw/wetware)
- The strategy applies everywhere: Enterprise Information Technology (EIT), Operational Technology (OT), Industrial Control System (ICS), Internet of Things (IoT), & Spectrum (i.e., 5G/6G)

[Understanding Zero Trust 2022]

Software Engineering Institute (SEI) Zero Trust Journey



SEI Cybersecurity Engineering Assessments

Prepare

- Strategy
- Infrastructure
- Budget
- Roadmap
- Executive Endorsement

Plan

- Asset Inventory
- Subject Inventory
- Data Inventory
- Data Flow Inventory
- Workflow Inventory
- System Security Engineering
- Monitoring Changes

Assess

- Maturity
- Gaps
- Risk
- Subject Inventory Pilot
- Data Flow Inventory Pilot
- Workflow Inventory Pilot

Implement

- Policy Development
- Communicate and Coordinate
- Deploy
- Operate
- Monitor and Measure
- Change Management

Common Challenges

Governance

- Inventories (asset, subject, data, data flow, workflow, APIs)

Architecture

- Awareness and accuracy

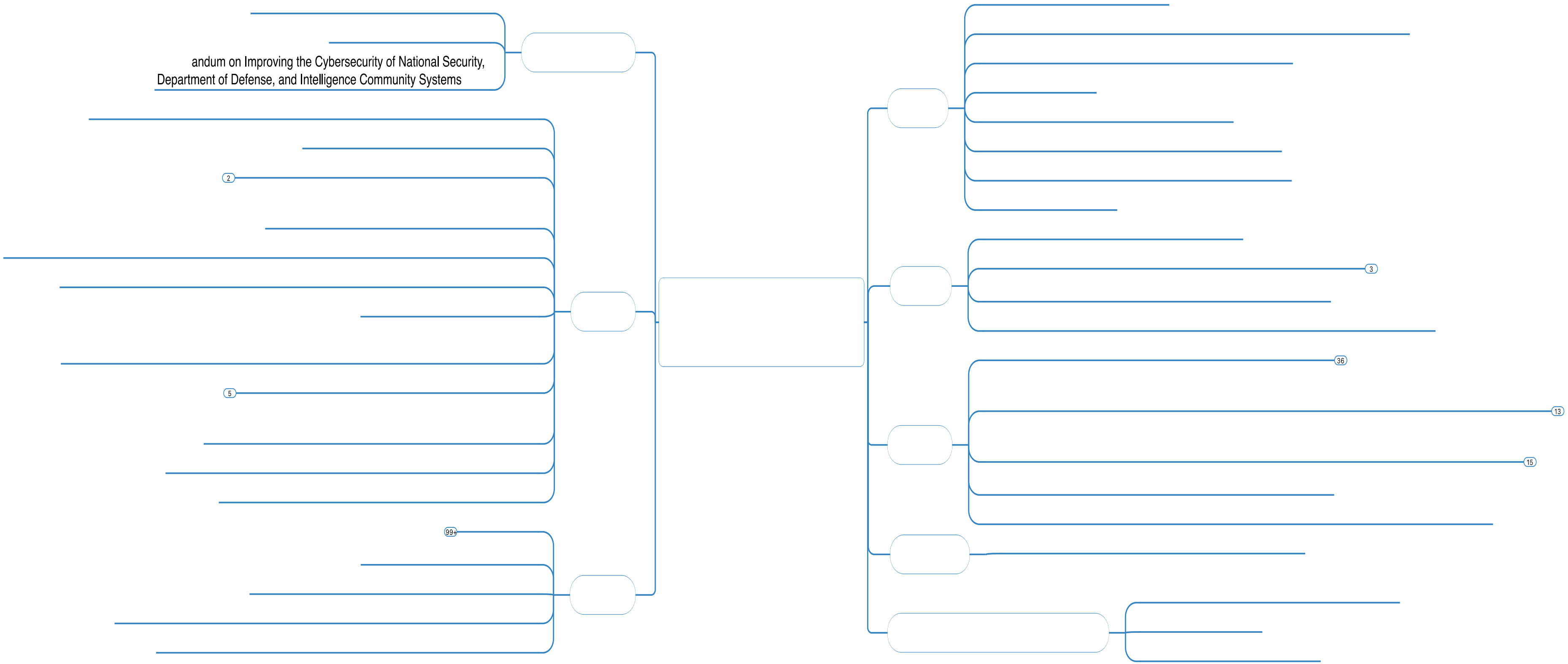
Cost

- Adoption cost

Measurement

- What is success?

Zero Trust Guidance Documents


andum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems
2
5
99+
3
36
13
15

CISA Zero Trust Maturity Model

(maturity stages)	Identity Pillar	Devices Pillar	Networks Pillar	Applications and Workloads Pillar	Data Pillar
Optimal					
Visibility and Analytics		Automation and Orchestration (cross cutting)		Governance	
Advanced					
Visibility and Analytics		Automation and Orchestration (cross cutting)		Governance	
Initial					
Visibility and Analytics		Automation and Orchestration (cross cutting)		Governance	
Traditional					

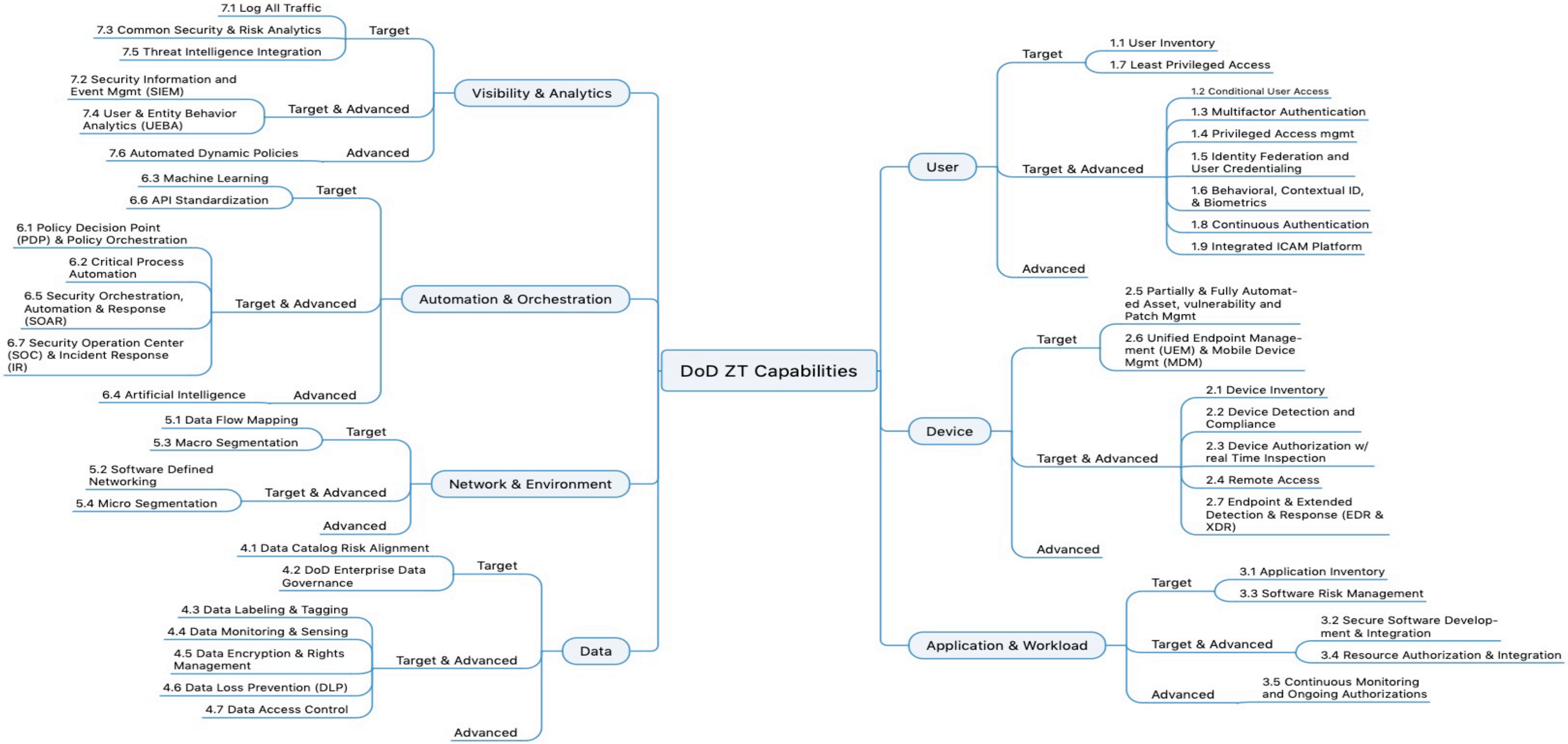
[CISA ZTMM 2023]

Example: CISA Zero Trust Maturity Model Identity Pillar Functions

Function	Traditional	Initial	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password	Agency continuously validated identity with phishing-resistant MFA, not just when access is initially granted.
Risk Assessments	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.

[CISA ZTMM 2023]

DoD Zero Trust Strategy



- DoD ZT Capabilities
  - User
    - Target
      - 1.1 User Inventory
      - 1.7 Least Privileged Access
    - Target & Advanced
      - 1.2 Conditional User Access
      - 1.3 Multifactor Authentication
      - 1.4 Privileged Access mgmt
      - 1.5 Identity Federation and User Credentialing
      - 1.6 Behavioral, Contextual ID, & Biometrics
      - 1.8 Continuous Authentication
      - 1.9 Integrated ICAM Platform
    - Advanced
  - Device
    - Target
      - 2.5 Partially & Fully Automated Asset, vulnerability and Patch Mgmt
      - 2.6 Unified Endpoint Management (UEM) & Mobile Device Mgmt (MDM)
    - Target & Advanced
      - 2.1 Device Inventory
      - 2.2 Device Detection and Compliance
      - 2.3 Device Authorization w/ real Time Inspection
      - 2.4 Remote Access
      - 2.7 Endpoint & Extended Detection & Response (EDR & XDR)
    - Advanced
  - Application & Workload
    - Target
      - 3.1 Application Inventory
      - 3.3 Software Risk Management
    - Target & Advanced
      - 3.2 Secure Software Development & Integration
      - 3.4 Resource Authorization & Integration
    - Advanced
      - 3.5 Continuous Monitoring and Ongoing Authorizations
  - Visibility & Analytics
    - Target
      - 7.1 Log All Traffic
      - 7.3 Common Security & Risk Analytics
      - 7.5 Threat Intelligence Integration
    - Target & Advanced
      - 7.2 Security Information and Event Mgmt (SIEM)
      - 7.4 User & Entity Behavior Analytics (UEBA)
    - Advanced
      - 7.6 Automated Dynamic Policies
  - Automation & Orchestration
    - Target
      - 6.3 Machine Learning
      - 6.6 API Standardization
    - Target & Advanced
      - 6.1 Policy Decision Point (PDP) & Policy Orchestration
      - 6.2 Critical Process Automation
      - 6.5 Security Orchestration, Automation & Response (SOAR)
      - 6.7 Security Operation Center (SOC) & Incident Response (IR)
    - Advanced
      - 6.4 Artificial Intelligence
  - Network & Environment
    - Target
      - 5.1 Data Flow Mapping
      - 5.3 Macro Segmentation
    - Target & Advanced
      - 5.2 Software Defined Networking
      - 5.4 Micro Segmentation
    - Advanced
  - Data
    - Target
      - 4.1 Data Catalog Risk Alignment
      - 4.2 DoD Enterprise Data Governance
    - Target & Advanced
      - 4.3 Data Labeling & Tagging
      - 4.4 Data Monitoring & Sensing
      - 4.5 Data Encryption & Rights Management
      - 4.6 Data Loss Prevention (DLP)
      - 4.7 Data Access Control
    - Advanced

DoD Zero Trust Maturity Model

Discovery

- Identify Data, Assets, Applications, Services (DAAS)
- Map data flows
- Inventory User and Devices
- Identify privilege accounts
- Log network traffic

Assessment

- Determine compliance state leveraging existing hardening standards
- Determine proper account privilege levels
- Identify, if existing network/environment security policies as implemented in least privilege manner

Baseline

- Access to DAAS is determined by cybersecurity policy
- Networks are segmented with deny all/permit by exception
- Devices are managed and compliant to IT security policies
- Implement least privileged access
- MFA technologies are in use
- Begin data classification and tagging of critical data
- Meet encryption requirements

Intermediate

- Enhanced cybersecurity policies are used to determine access based on fine-grained user and device attributes
- Micro-segmentation across majority of network
- User identity based on Enterprise Federated Identity Service
- Enhance LPA with privileged access mgmt. solution
- Initial DLP and DRM implementations
- Data is tagged and classified via flow analysis and simple automation
- User and Entity Behavior Analytics (UEBA) to develop baseline

Advanced

- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation
- Continuous and adaptive authentication and authorization
- User and device identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating data tags
- Advanced analytics enable automated and orchestrated threat detection

[DISA/NSA 2022]

How to Develop the Context Necessary to Apply ZT?

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.

[MEG]

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems

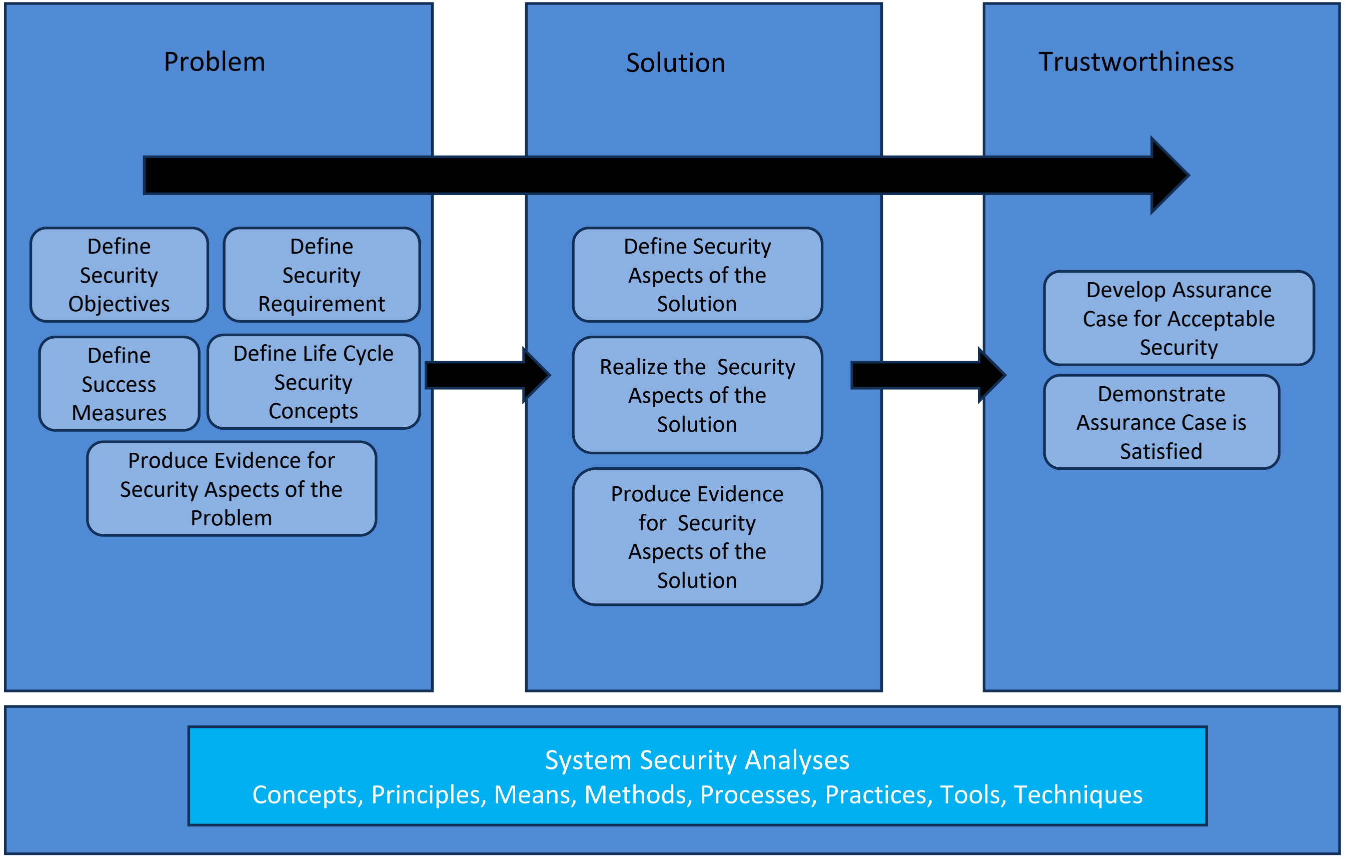

Problem
Solution
Trustworthiness
Define Security Objectives
Define Security Requirement
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Define Security Aspects of the Solution
Realize the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution
Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case is Satisfied
System Security Analyses
Concepts, Principles, Means, Methods, Processes, Practices, Tools, Techniques

Figure 10

Zero Trust Industry Day Event

- Organizations who develop solutions for implementing a zero trust architecture get together and share their ideas, solutions, and experiences
- The SEI asked developers of zero trust solutions how they would solve a problem in a situation that requires cyber protection of data and resources.
- Presenters from each participating organization prepare a 1-hour presentation and address challenges in complying with requirements from six guidance documents.
  - CISA Zero Trust Maturity Model, Version 2.0
  - DoD Zero Trust Strategy
  - National Cybersecurity Strategy
  - OMB M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents
  - OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
  - CISA Zero Trust Implementation Strategy

Zero Trust Industry Day 2022 Scenario

A fictional company operating a hybrid, multi-cloud enterprise.

- two legacy systems
- one database containing Protected Personal Information (PPI)
- four different identity and access management systems
- lacks a centralized security operations center (SOC)
- budget of $3 million and a one-year timeline during which it must start to address Office of Management and Budget (OMB) memoranda

SEI was looking for approaches to zero trust that also address challenges in complying with OMB memoranda.

- OMB M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents
- OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Zero Trust Industry Day 2022

Panel discussions:

- What areas of zero trust need further research?
- What areas do not need further research?
- What are you tired of hearing about from your customers about zero trust?
- Given the SEI's role as an honest broker, what do you suggest that the SEI can do to help you in your work in zero trust?

Key Takeaways:

- The Q&A panel session spurred good conversation, where people were free to be honest and talk about their experiences.
- Resulted good networking and teaming among solution providers.
- Hearing the challenges of solution providers.
- Take away for attendees is to not look for a single solution provider to do it all.
  - Many focus their development in one particular zero trust area, e.g., ICAM, segmentation.
  - Need contextual awareness, priorities, before going to solution provider to fill that part of ZT

Zero Trust Industry Day 2024 Scenario

This year’s scenario integrates manufacturing with smart city technologies. Involves a fictitious chip manufacturing facility in a city on an island that integrates smart technologies into its infrastructure.

- Three legacy OT Systems
  - controlling the “clean room”, production of silicon wafers, SCADA system for monitoring
- Facility reliance on OT/IIoT
  - Smart sensors and actuators are connected through the internet to industrial applications
- Smart City reliance on IoT (IoT enabled devices hardware)
  - waste management systems, public transportation systems, traffic management systems
- Heterogenous environments
- Hosted private cloud residing on-premise at facility
- Public Cloud used by manufacturing facility and internet activity in smart city
- Connected Services
  - centralized Identity, credential, and access management (ICAM) service, remote from island
  - cellular and Wi-Fi coverage with 5G capability
  - Satellite network

Scenario Concerns to Address

Handling vulnerabilities and threats in highly connected systems. What concerns do they create?

- Disruption of connectivity
  - ICAM – loss of cloud services, loss of satellite communication
- Ensuring solutions do not impair accessibility and availability for manufacturing environment
- Legacy OT systems
  - security in standard industrial communication protocols
  - older components do not support encryption.
  - devices not designed with security required for internet
  - devices built with a back door for calibration
  - common password for all devices
- IoT and IIoT systems
  - IIoT technology running on older infrastructure
  - vulnerable intercommunication among IIoT devices
  - smart city IoT devices weak on security from the manufacturer

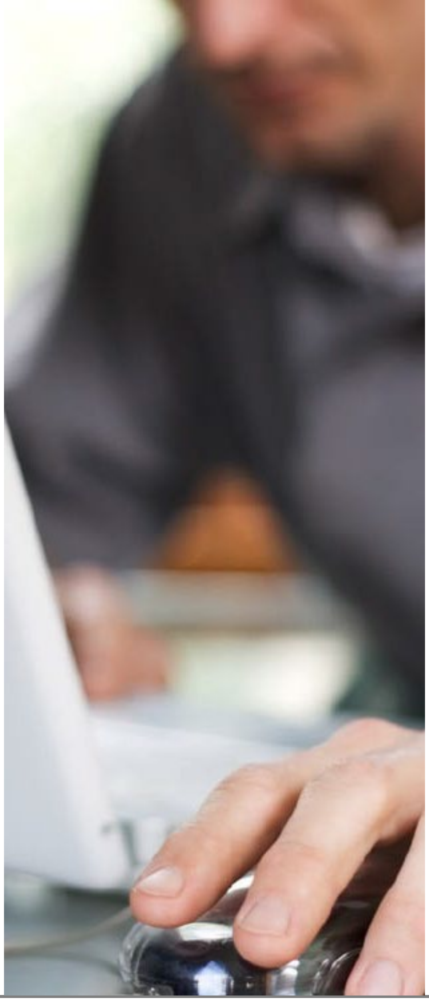
SEI Zero Trust Collection

Our Zero Trust collection contains SEI zero trust publications, including newsletters, blog posts, podcasts, webcasts, presentation videos from our Zero Trust Industry Days events, and related materials of interest.
https://insights.sei.cmu.edu/library/zero-trust-collection/

Information about our Zero Trust Industry Days 2024 event:
Fact Sheet
https://insights.sei.cmu.edu/documents/5851/zero_trust_days.pdf
Scenario
https://insights.sei.cmu.edu/library/zero-trust-industry-day-2024-scenario-secluded-semiconductors-inc/
Web pages
https://resources.sei.cmu.edu/news-events/events/zero-trust/

Zero Trust Security

References



References –1

[CISA ZTMM 2023]
Cybersecurity Infrastructure Security Agency, Cybersecurity Division. *Zero Trust Maturity Model, Version 2.0*. Washington, DC: CISA. 2023.
https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[DISA/NSA 2022]
Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team. *Department of Defense Zero Trust Reference Architecture, Version 2.0*. Washington, DC: Department of Defense (DoD) CIO. 2022.
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

[NIST 800-207 2020]
Rose, S.; Borchert, O.; Mitchell, S.; & Connelly, S. *NIST Special Publication 800-207: Zero Trust Architecture*. Gaithersburg, MD: NIST. 2020.
https://csrc.nist.gov/publications/detail/sp/800-207/final

References –2

[NMM-2022-01A1]
National Security Agency. *National Manager Zero Trust Security Reporting Guidance and Cloud Migration Security Reporting Guidance*. 2022.

[Understanding Zero Trust 2022]
Touhill, G. “Understanding Zero Trust”. *SEI Presentation*. 2022.

[Zero Trust Security 2021]
Garbis, J. & Chapman, J. *Zero Trust Security: An Enterprise Guide*. Berkeley, CA: Apress. 2021. https://link.springer.com/book/10.1007/978-1-4842-6702-8

[MEG]
DoD. *Mission Engineering Guide*. November 2019. https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

Contact Information

Tim Morrow

CERT Division Situational Awareness Technical Manager

tbm@sei.cmu.edu

412.268.4792

Rhonda Brown

CERT Division Situational Awareness Senior Solutions Engineer

rbrown@cert.org

412.268.3963

Elias Miller

CERT Division Situational Awareness Assistant Solutions Engineer

emiller@cert.org

412.268.6453