Carnegie Mellon University
Software Engineering Institute

Cyber Education Presentation

MAY 31, 2023

Greg Touhill
CMU/SEI CERT Division Director

Document Markings

Discussion Areas

Identity and API Security

The hidden cost of Zero Trust success

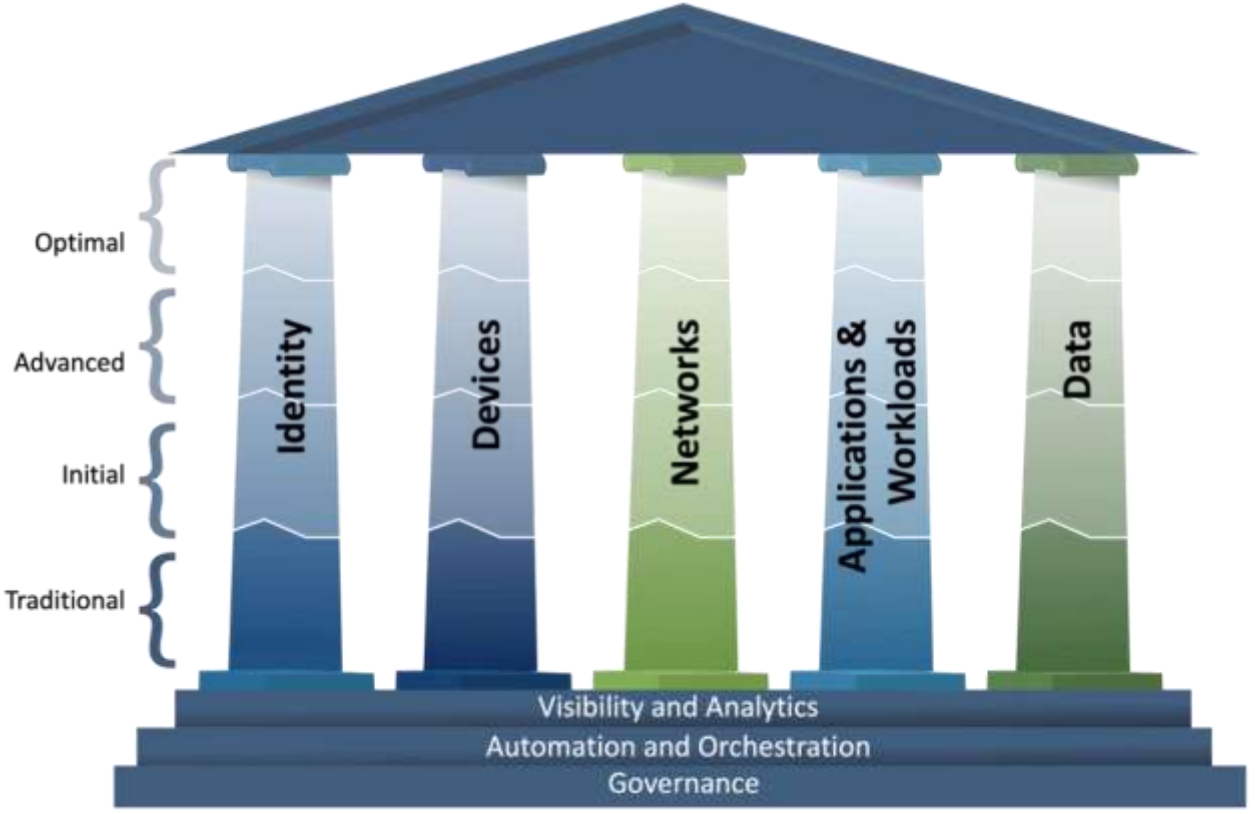
Understanding your data

When and Why Zero Trust fails

Identity and API Security

Carnegie Mellon University
Software Engineering Institute

CISA Zero Trust Maturity Model



[CISA 2023]

Identity

- zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities (NPE) through use of capabilities such as multi-factor authentication (MFA) and Privileged Access Management (PAM) for privileged functions. [DISA/NSA 2022]
- Organizations need the ability to continuously authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions. [DISA/NSA 2022]
- 43% of respondents identified "Identity and Access Management" as the first task to address as they begin to move to zero trust. [NSTAC 2022]

Application Programming Interface Security

- Application programming interface (API) is an interface that defines how different software interacts.
- API security refers to the practice of preventing or mitigating attacks on APIs.

Primary areas of focus

1. Application Access

- Implement authentication and authorization (identity)

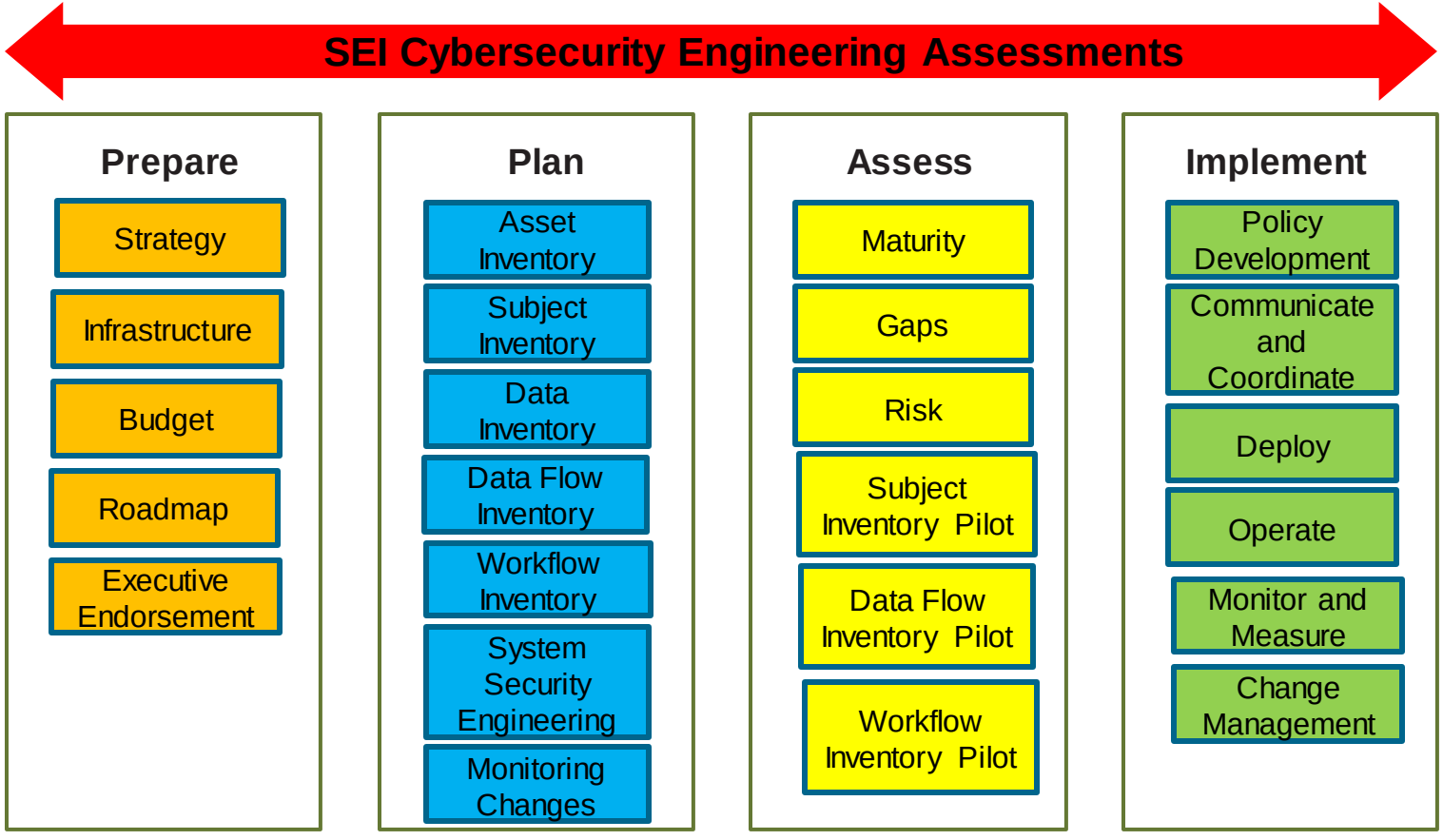
2. Application Security

- Validate all requests, encrypt all requests and responses, log API activity, conduct tests of the API

The hidden cost of Zero Trust success

Carnegie Mellon University
Software Engineering Institute

Software Engineering Institute (SEI) Zero Trust Journey



Implementing a ZTNA is our most important task

Carnegie Mellon University Software Engineering Institute

- integrating the zero trust security strategy into the enterprise business strategy is the most important task.
- gain support from the highest levels of leadership by demonstrating the value of implementing the zero trust security strategy to the goals and objectives of the organization.
- Focus on the people, process, and technology components.
- to identify and prioritize the key cyber terrain of the business: its data.
- ensure that for every piece of data throughout its lifecycle (including that within their OT, ICS, IoT and RF-enabled devices) there are business rules that define who can see, access, edit, share, destroy, etc. the data under well-documented conditions and entitlements.
- create plans of action focused on an enterprise-wide governance structure enforcing those business rules regarding the data that fuels their organization.

Beware those who say, “When we get to Zero Trust we are secure”

- zero trust is the starting point, not the destination.
- As a former senior military commander, I learned that those whose objective is to get risk to equal zero *always* lose. I contend that zero trust is the starting point on the journey to get to an acceptable level of risk based on technical and procedural security controls that establish a level of “digital trust” that is within your risk tolerance.
- The World Economic Forum defines digital trust as, “individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.”
- as you implement the zero trust principles, your starting point is that you don’t trust anything or anyone until they prove to your satisfaction, through a series of technical and procedural controls, that your data, access, and transactions are secure and congruent with your security policies and expectations.

Understanding your data

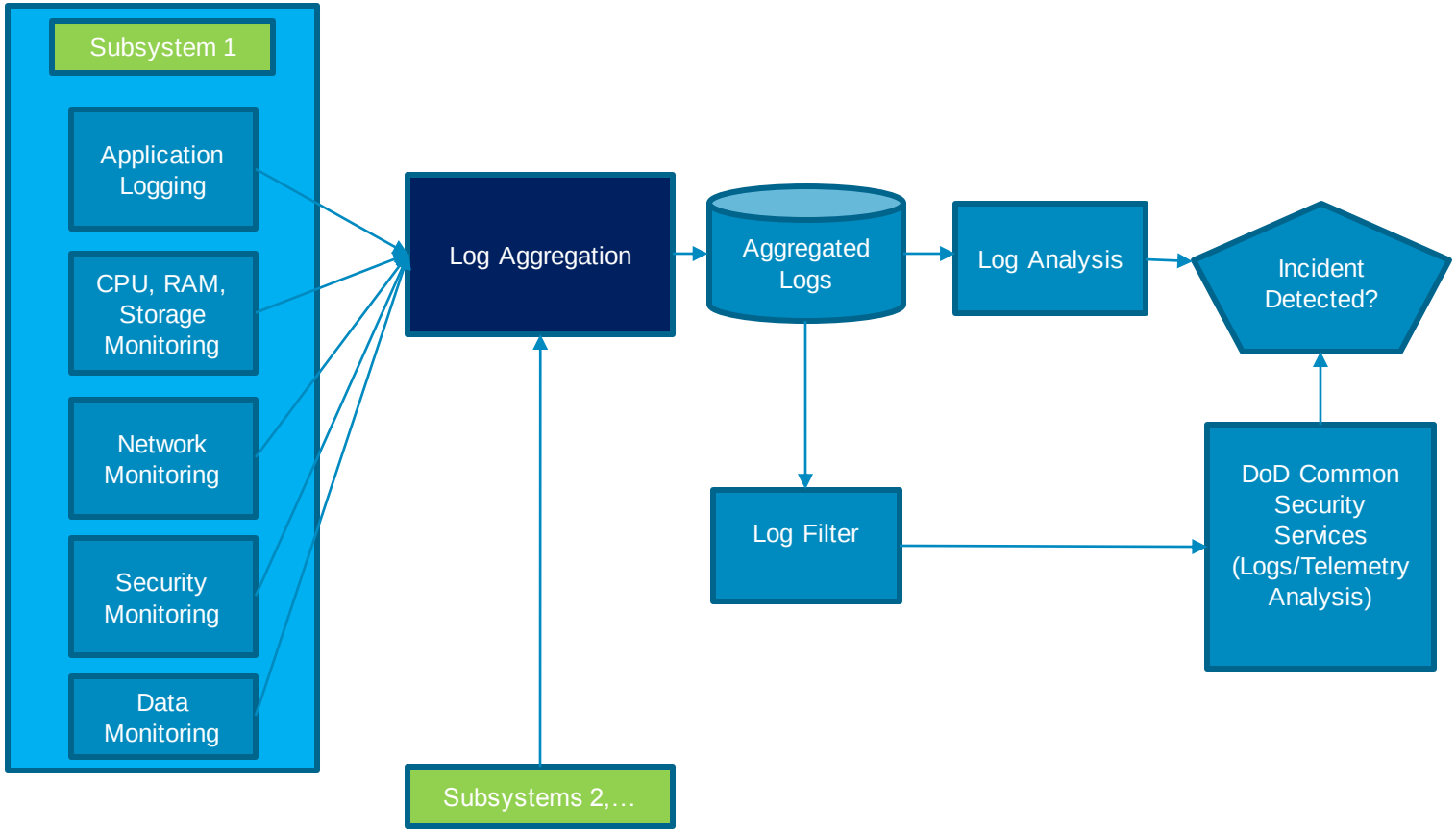
Carnegie Mellon University
Software Engineering Institute

- Identify and prioritize data flows.
- how long it takes to implement a zero trust strategy, I advise the most profound influencer on the schedule is understanding your own data. The larger and more complex your data environment (and think beyond enterprise information technology), the longer it will take to inventory and catalog your data and establish the rule sets governing access to the data under conditions and entitlement rules established by the organizations.
- many organizations who have been very successful in their zero trust journeys create plans of action that create basic rule sets for data access based on things such as work groups and define basic conditions and entitlements to data sets.
- As your organization gains confidence in the zero trust strategy implementation and enabling technology (much of which you likely already have), you can refine the rules, conditions, and entitlements to provide much more granular control over data access to reduce your risk exposure and meet your strategic objectives.

Data-centric focus is best

- organization took a data-centric approach to zero trust implementation by first investing in inventorying and prioritizing their data associated with line of business functions and establishing access control rule sets along with defined conditions and entitlement factors.
- Only after conclusion of these activities did these organizations commit to investments in new technologies, architectures, hardware, software, etc. Regardless of which approach taken (i.e. network-centric vs. data-centric), approximately 83% of those surveyed or interviewed indicated that establishing a complete understanding of the data environment along with defining the rules, conditions, and entitlements consistent with application of zero trust principles in the enterprise represented the single largest cost driver of the zero trust implementation.
- the data-centric approach to zero trust implementation was more collaborative across the business enterprise, generated greater employee understanding and buy-in, and yielded a better, more transparent, implementation plan than previous cybersecurity initiatives.

Need to Focus on Logging Data and Log Analysis Process



When and Why Zero Trust fails

Carnegie Mellon University
Software Engineering Institute

My Only Costs Are Upgrades to my Network with ZT-enabled Technology

- 50% of our respondents report that accurately inventorying and cataloging their data and access rule sets were their most difficult and challenging issue. In comparison, 16.2% reported developing and implementing a ZT architecture; 14.7% reported educating and training the workforce on ZT; and 13.2% reported acquiring and properly configuring ZT-enabling technology as their most difficult and challenging issues.
- A significant number of cybersecurity professionals focus on the purchase of hardware, software and services in creating their budget submissions yet discover during the course of their zero trust implementations they did not factor into their budget calculus the costs associated with accurately inventorying and cataloging their data nor the costs associated with establishing the rule sets, conditions, and entitlements required to for the fine-grained identity and access management characteristic of optimum zero trust implementations.

Reliance on Vendor Referrals

- As part of our research, we asked cybersecurity professionals to identify their primary source of zero trust information and best practices. 36.8 % of respondents identified research organizations as their primary source of zero trust information. A very close second, 35.3 % identified vendors trying to sell zero trust products and services as their primary source of information about zero trust. Other identified sources included professional associations (19.1%), government sources (2.9%), media reporting (1.5%), and “other” sources (4.4%).
- Over one third of respondents viewed their vendors, who have a vested stake in particular zero trust solutions, to be their primary source of information.
- From a governance and oversight standpoint, this should sound alarm bells to corporate boards who view potential “vendor lock-in;” lack of due care and diligence in evaluating broad courses of actions; and potential conflicts of interest as presenting unacceptable corporate risk.
- Don’t trust by default; always check references and ask to see the evidence before making a risk-informed decision!

Wrong Focus For Zero Trust Strategy

- Many organizations appoint experienced EIT personnel to lead their zero trust implementations.
- These organizations tend to associate zero trust as an information technology or cyber security initiative rather than an enterprise-wide security strategy-driven initiative.
- Tend to create implementation plans that are heavily-weighted toward the purchase of new hardware and services associated with the creation of the new network architecture.
- These organizations report frustration over long implementation timelines; concerns over costs, vendor lock-in and questionable return on investment calculations; ill-defined or uncertain manning and training requirements; and lack of synchronization with line of business priorities.

Not Addressing Threats to Zero Trust Implementations

1. Subversion of the zero trust architecture (ZTA) decision process
2. Denial-of-service or network disruption
3. Stolen credentials/insider threat
4. Visibility of the network (i.e., awareness of the components and data within a network)
5. Storage of system and network information
6. Reliance on proprietary data formats or solutions
7. Use of NPEs in ZTA administration
8. Attack, which is directed at the APIs, that alters the data stream to permit access through tampered telemetry during conditions/entitlement checks

[Rose 2020]

Summary

Developing context using mission engineering approach enables security architectures to reason about zero trust strategy, design, and possible implementations for weapon systems, as well as enterprises.

Set of zero trust assessments need to be developed to support the life cycle of weapon system/enterprise.

Need to use an approach like ASF to build in security and resilience into weapon systems/enterprise in support of efforts like CROWS SSECG to provide the artifacts to enable zero trust assessments

Backup

Threat Mapping –1

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Subversion of the ZTA Decision Process	Policy Engine Policy Administrator	Configuration Management Monitoring Detection
Denial-of-Service or Network Disruption	Policy Engine Policy Administrator Policy Enforcement Point	Resilience
Stolen Credentials/Insider Threat	ID Management Data Access Policy	Architecture Contextual Trust Algorithm
Visibility on the Network	Activity Logs SIEM	Network Traffic Inspection Network Traffic Logging Metadata Machine Learning

[Sanders 2021]

Threat Mapping –2

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Storage of System and Network Information	Policy Engine Policy Administrator Activity Logs CDM Systems Industry Compliance Data Access Policy PKI ID Management SIEM Information	Restrictive Data Access Policies
Reliance on Proprietary Data Formats and Solutions	Policy Engine Policy Administrator Policy Enforcement Point	Service Provider Evaluation Vendor Security Controls Enterprise Switching Costs Supply Chain Risk Management Performance/Stability

[Sanders 2021]

Threat Mapping –3

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Use of Non-Person Entities (NPEs) in ZTA Administration	Policy Engine Policy Administrator	Regular Retuning Analysis
API Attacks	Policy Engine Policy Administrator CDM System ID Management SIEM Information	Encrypt Requests and Responses Validate the Data Assess API Risks

[Sanders 2021]

References –1

[CISA 2023]
Cybersecurity Infrastructure Security Agency, Cybersecurity Division. *Zero Trust Maturity Model, Version 2.0*. April 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*. September 2022.
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[NSTAC 2022]
The President's National Security Telecommunications Advisory Committee. Draft Report to the President: Zero Trust and Trusted Identity Management. 2022.

[Sanders 2021]
Sanders, G. "Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment." *SEI Blog*. March 2021. https://insights.sei.cmu.edu/blog/zero-trust-adoption-managing-risk-with-cybersecurity-engineering-and-adaptive-risk-assessment