CMU/SEI Zero Trust Pilot Proposal

September 16, 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 Homeland Security 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 sponsored by the United States Department of Defense.

DM21-0804

Agenda

1. Discuss current Trusted Internet Connections (TIC) and CISA challenges
2. Hypotheses for a Zero Trust (ZT) Architecture (ZTA) pilot
3. The ZTA pilot would address
4. Outcomes

Current TIC Challenges - 1

TIC is expensive for CISA to manage and agencies to implement.

Service provider implementations are vendor-unique.

- Agencies lack implementation guidance.

TIC 3.0 Security Capabilities Catalog

- Identifies Universal Security and Policy Enforcement Point capabilities and associated NIST Cybersecurity Framework (CSF) mapping.

TIC 3.0 Overlay Handbook

- TIC Overlay used to map products/services to security capabilities for both vendors and agencies.
- Overlays don't provide agencies with agnostic, implementation specific guidance to be successful.

Current TIC Challenges - 2

CISA TIC 3.0 Program Guidebook

- As an agency implements security capabilities, artifacts (telemetry information) are produced that provide visibility into the agency's environment and security posture.
- Specific guidance concerning what telemetry information agencies need to provide to CISA programs is missing.

Current CISA Challenges

System-of-systems (SoS) vision is still being developed.

- Point solutions have been piloted
  - Cybersentry
  - CLAW
- Lack of an integrated logging system

E3A – expensive active defense with no contextual information provided to agencies.

What will be CISA's role as agencies implement ZTA?

- What telemetry information will be needed for alignment with CISA's programs.

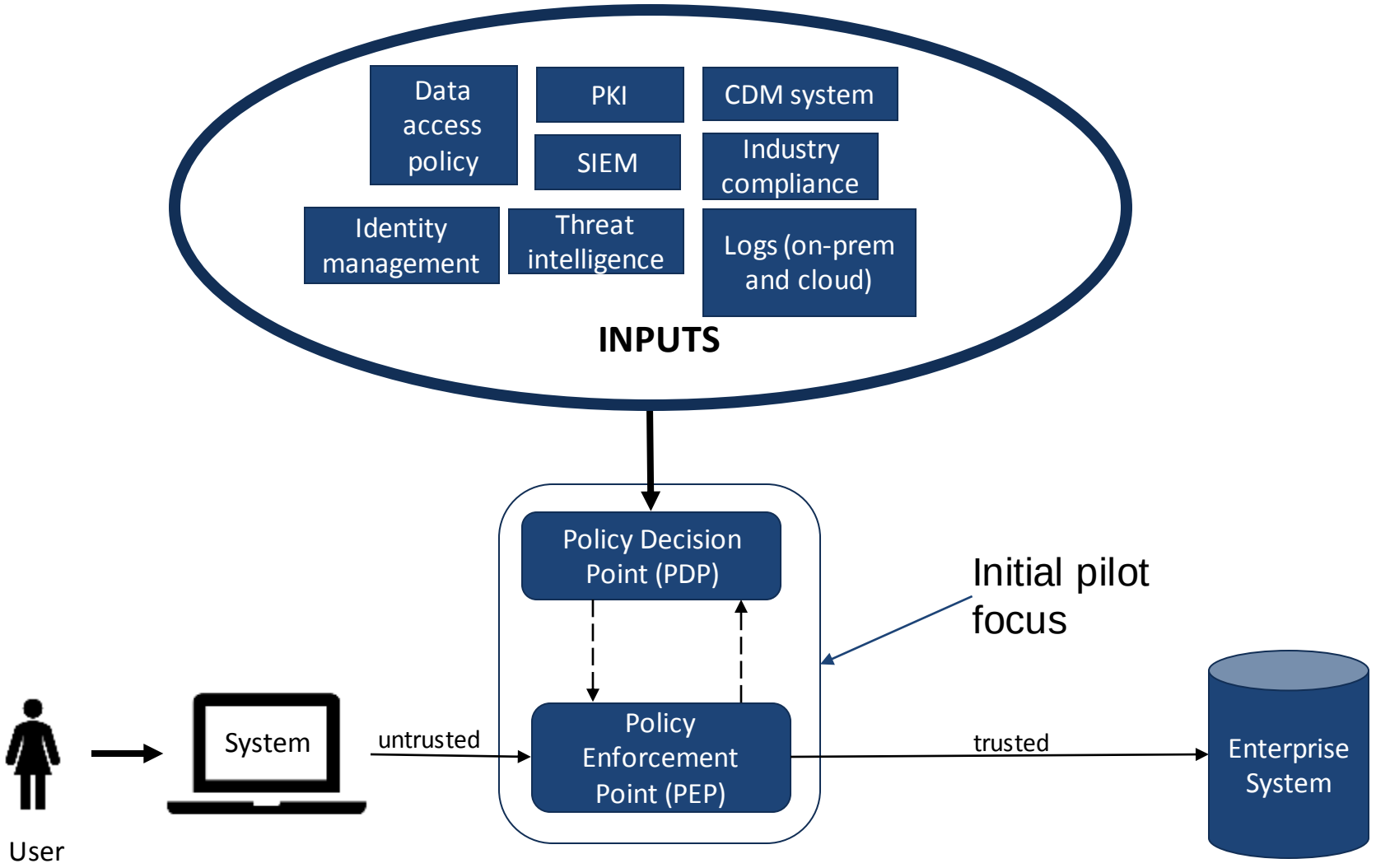
Hypotheses

A ZTA leveraging software-defined perimeter (SDP) technology can provide the data needed to execute the TIC mission at a lower cost and with better performance than the current TIC construct.

A disciplined test of said ZTA will provide decision-quality evidence to support the hypothesis.

Analysis methods can be used to assess an agency's ZT maturity level based on CISA Zero Trust Maturity Model, when finalized.

Additional data sources can be identified for inputs to the ZTA policy decision point (PDP) through cybersecurity engineering analysis which will provide a richer data environment from which to make mission decisions.



ZTA Pilot Phases - 1

- Develop following notional agency's enterprise documentation
  - architecture documentation
  - mission threads/work flows
  - network operations center (NOC)/security operations center (SOC) use cases with supporting operational flows
  - continuous monitoring capabilities to support cybersecurity engineering analysis efforts.

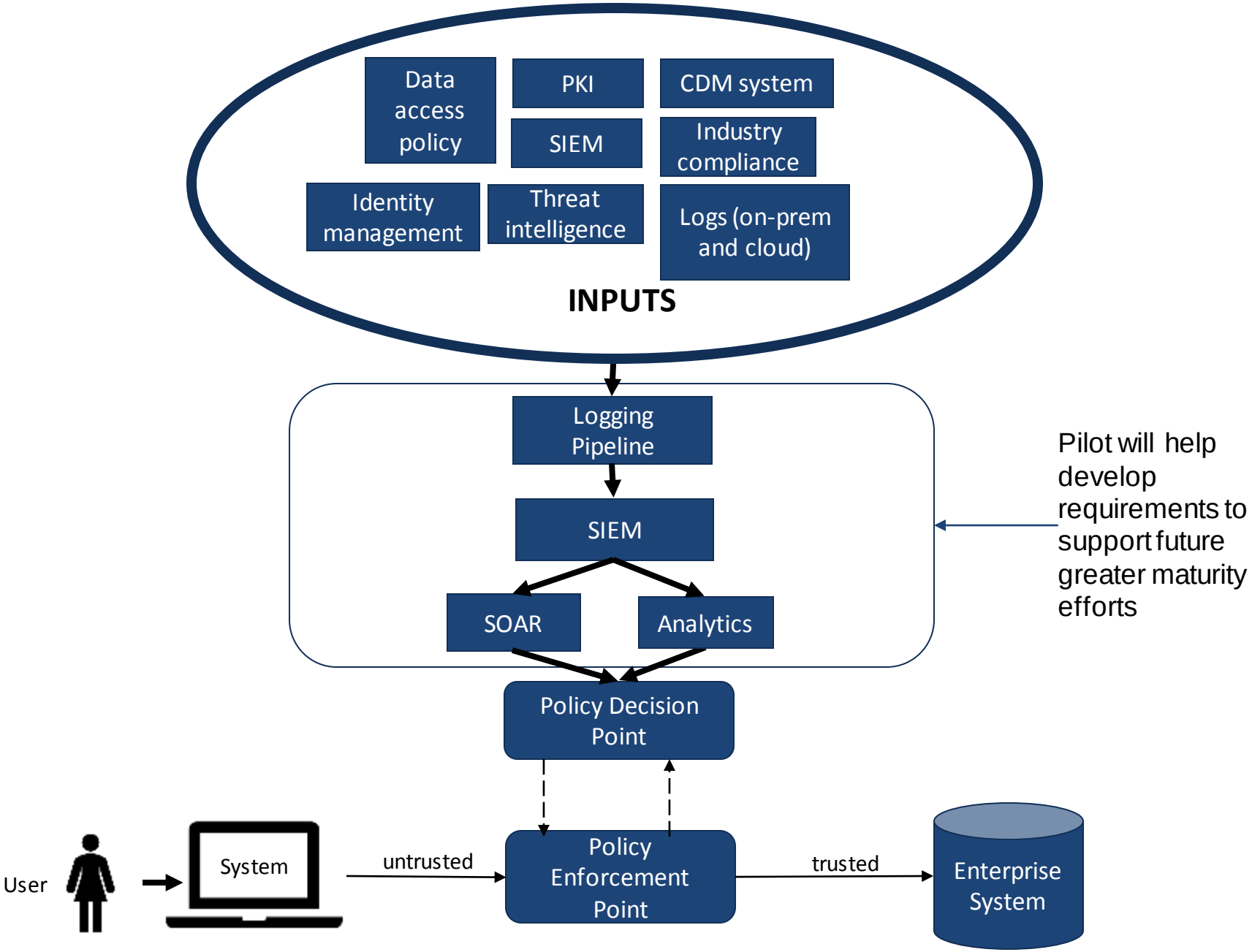
- Use existing assessment(s) to develop sufficient information to evaluate where an agency is in its ZT journey.
  - Tailored assessment processes can be transitionable to both CISA and agencies.

ZTA Pilot Phases - 2

- Develop ZTA roadmap with initial focus on PDP/PEP to help agencies work towards a CISA ZT Maturity Model Advanced stage.
  - Consists of steps and timeframe.
  - Considerations associated with each step.

- Develop ZTA guidance and best practices that are vendor-agnostic to support planning, acquisition, architecture design, implementation, and technical analysis efforts for agencies.
  - ZT journey documentation
  - Architecture model which can be used to support analysis.
  - Requirement wording to support acquisition efforts.

- Prototype the developed ZTA roadmap.
  - Cloud native access, logging pipeline, continuous monitoring, SIEM
  - Identify costs associated with prototype implementation



Outcomes

Pilot will identify how to reduce cost, complexity, and eliminate the need for TIC.

Pilot will validate the ability to implement ZT technologies that meet or exceed TIC 3.0 security capabilities.

Pilot will validate the ability to remove the requirement for service providers to improve CISA and agency agility.

Pilot will develop a ZTA roadmap with initial focus on PDP/PEP for the Advanced stage of CISA Zero Trust Maturity Model.

Pilot will identify ZTA guidance and best practices to implement the Advanced stage.

Pilot will develop telemetry information CISA can use to analyze its role as agencies transition to ZTA.

Take savings produced by removing the service provider requirement and use that to fund agencies in return for CISA compliance program.