TEXAS RE

Zero Trust Architecture

Kerrick Rosemond, Jr.
CIP Cyber & Physical Security Analyst

July 18, 2024

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

July 30, 2024

Inverter-Based Resources

August 6, 2024

IBR Data Collection and Reports

August 28, 2024

Cyber & Physical Security Workshop

Upcoming ERO Enterprise Events

July 24, 2024

CMEP Conference

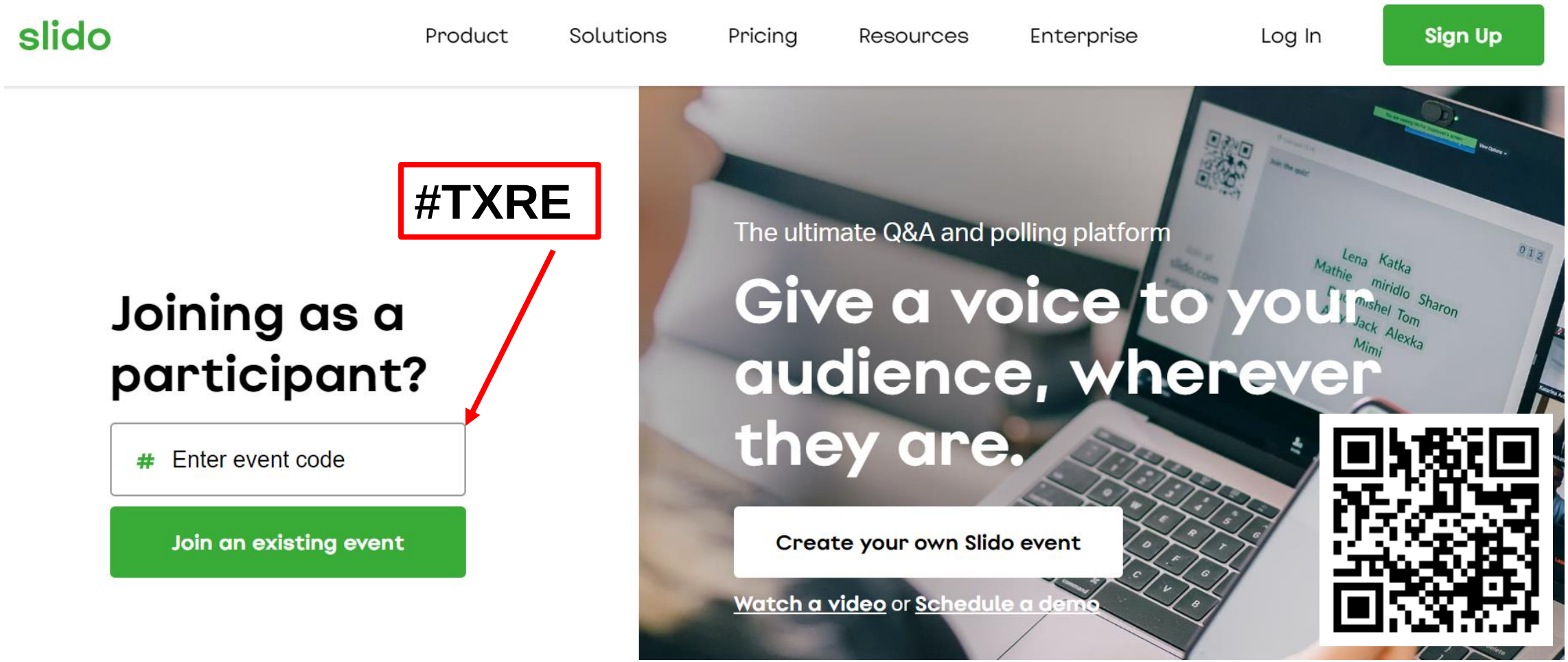
August 7, 2024

Protection System Workshop

August 13-15, 2024

Power Systems Security Conference

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

TEXAS RE

Zero Trust Architecture

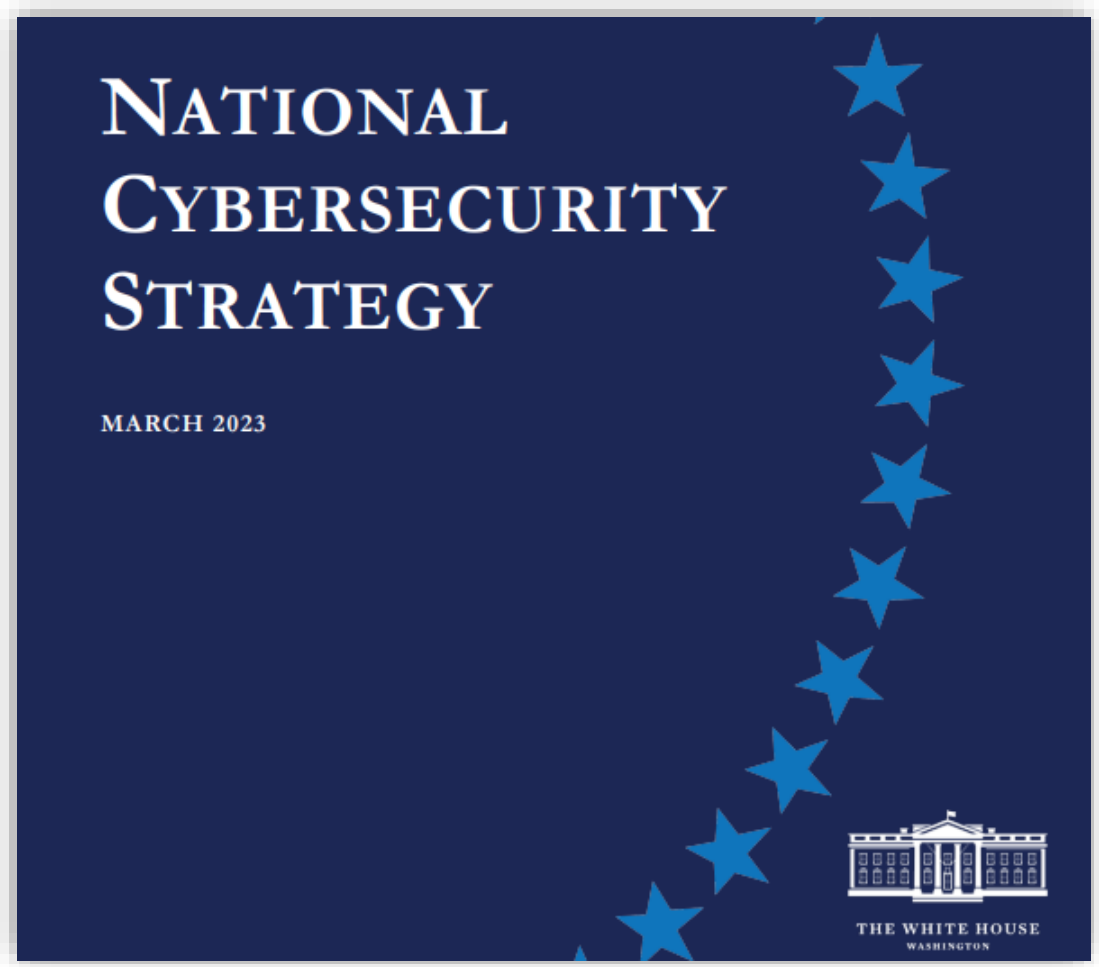
Kerrick Rosemond, Jr.
CIP Cyber & Physical Security Analyst

July 18, 2024

Agenda

- National Cybersecurity Strategy
- Understanding Zero Trust Architecture
- Concepts of Zero Trust
- How it Works
- Zero Trust Security Model
- Journey to Zero Trust
- CIP Standards

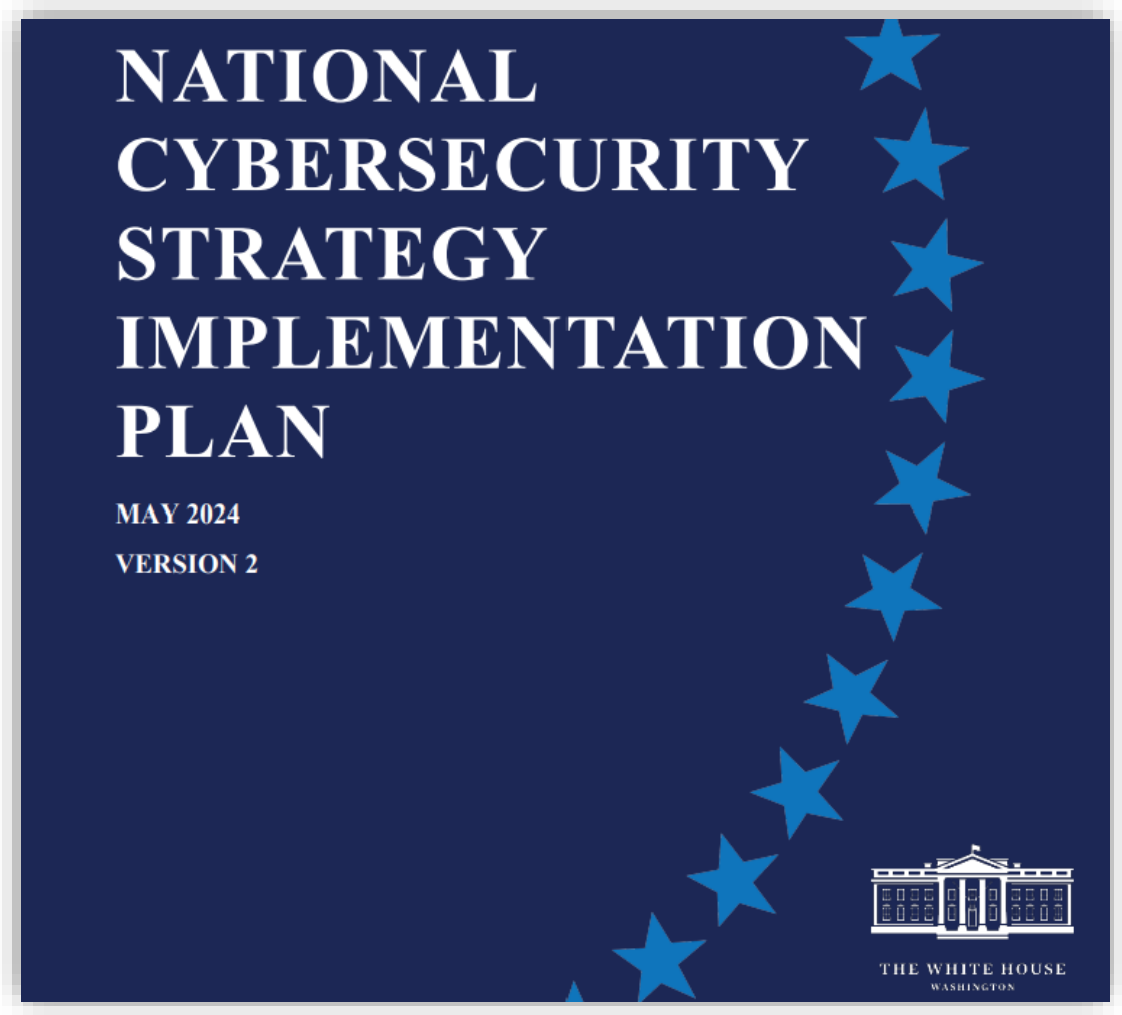
National Cybersecurity Strategy



- Defend Critical Infrastructure
- Disrupt and dismantle threat actors
- Shape market forces to drive security and resilience
- Invest in a resilient future
- Forge international partnerships to pursue shared goals

National Cybersecurity Strategy

- Defend Critical Infrastructure
- Disrupt and dismantle threat actors
- Shape market forces to drive security and resilience
- Invest in a resilient future
- Forge international partnerships to pursue shared goals



Slido.com (#TXRE)

Slido Question

What are some concepts of zero trust architecture?

Understanding Zero Trust Architecture

-Never trust, always verify

What is Zero Trust Architecture (ZTA)?

- Never trust, always verify
- All users and devices are potential threats
- End-to-end approach
- Need-to-know

Zero Trust Architecture Concepts

- Least Privilege
- Microsegmentation
- Multifactor Authentication
- Continuous Monitoring

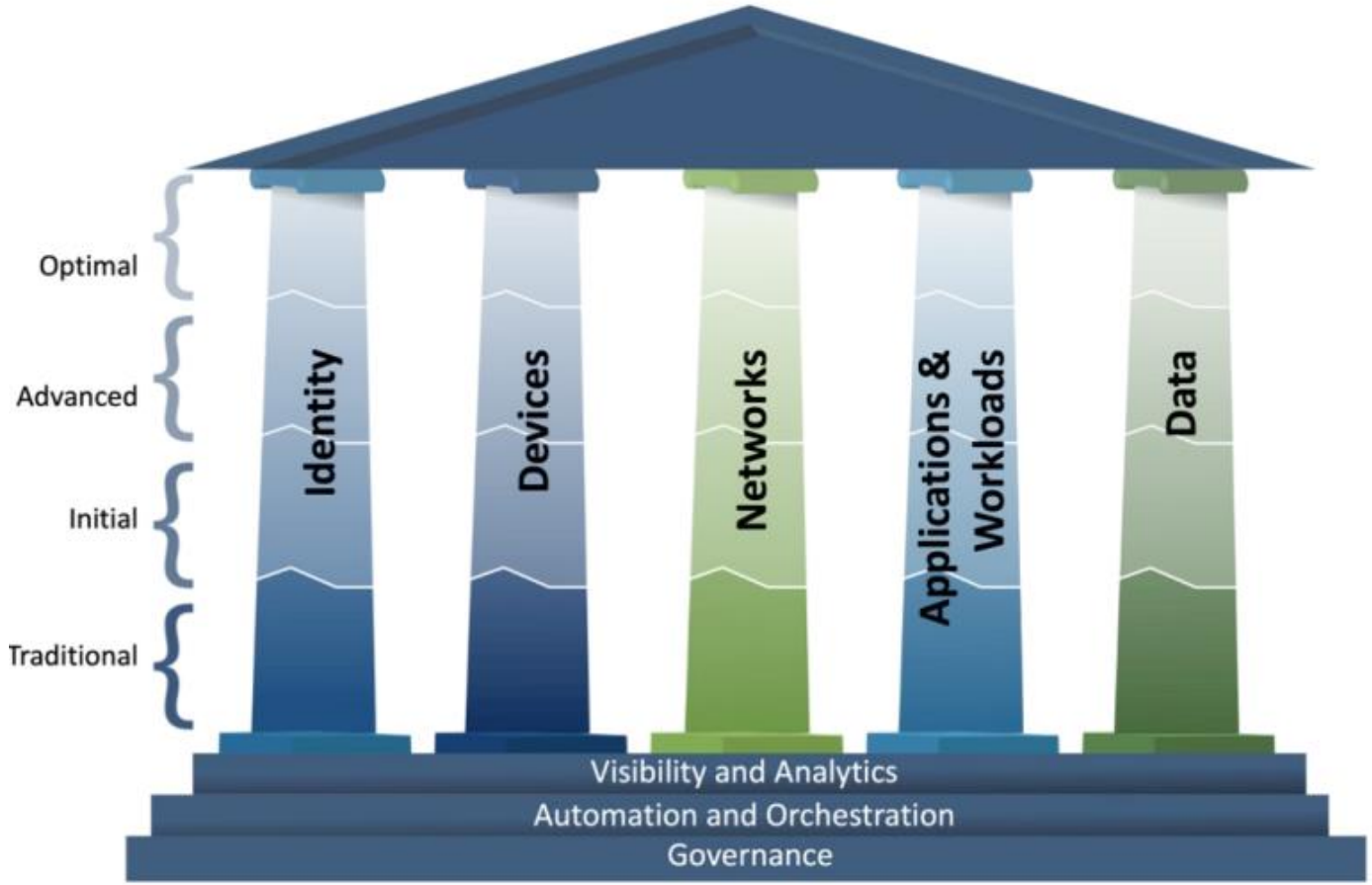
How it Works

*Zero trust architecture is not a single architecture, but a set of guiding principles for workflow, system designs and operations that can be used to improve the security posture of any classification or sensitivity level - **NIST SP 800-207***

NIST—Seven Tenets of Zero Trust

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications, and uses it to improve its security posture

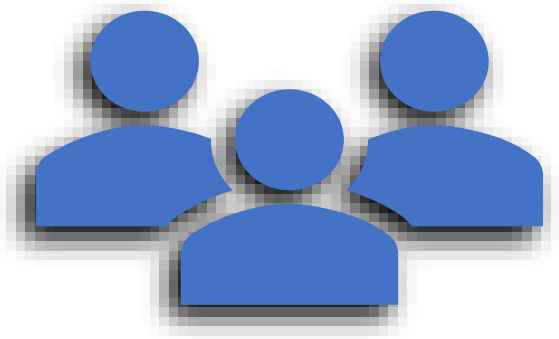
CISA Zero Trust Security Model



CISA Zero Trust Security Model

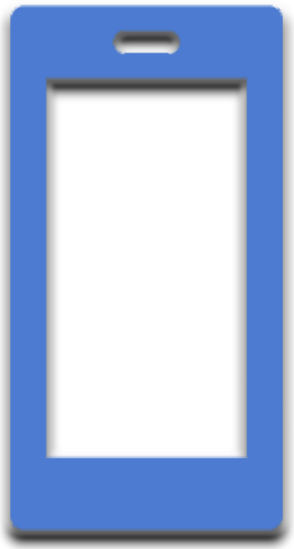
The Journey to Zero Trust: Users

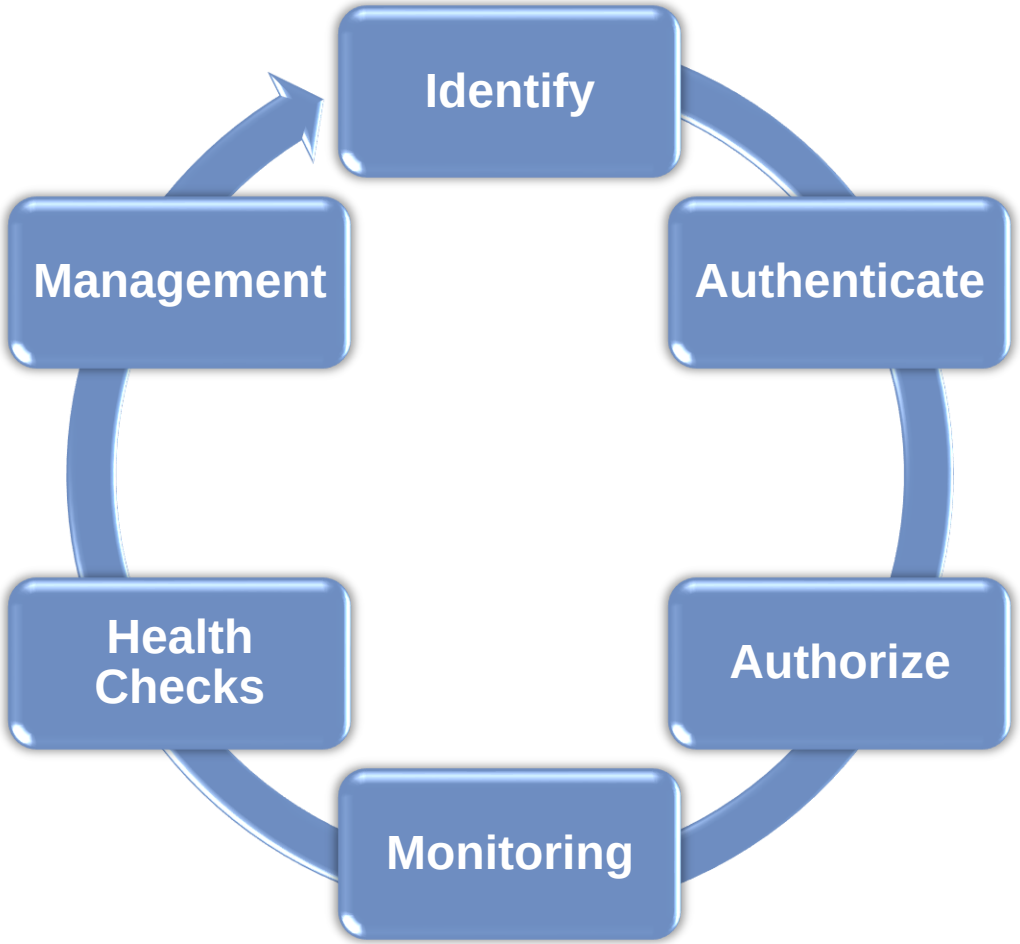
Users



The Journey to Zero Trust: Devices

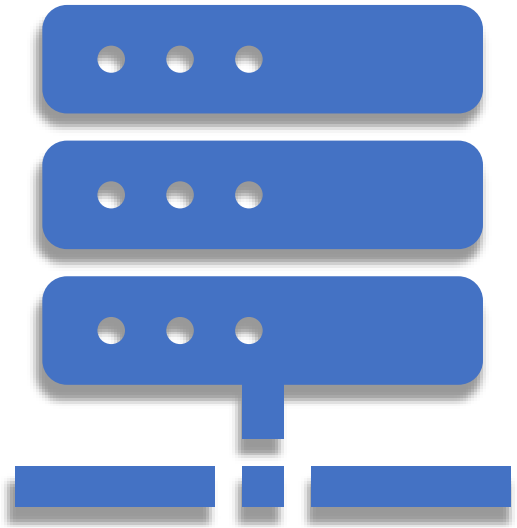
Devices





The Journey to Zero Trust: Network

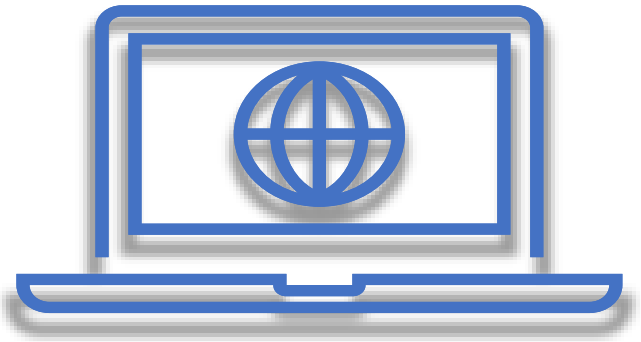
Network



- Segment
- Isolate
- Control

The Journey to Zero Trust: Applications

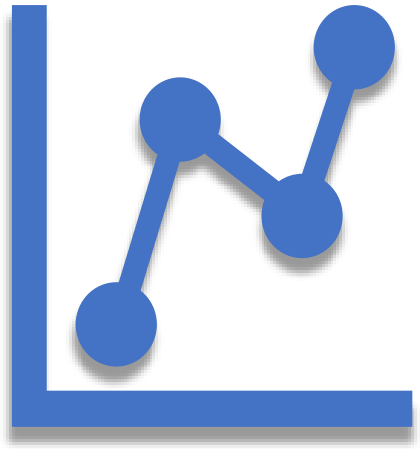
Applications



- Secure & Manage
- Task or Services
- Application Layer
- Containers
- Virtual Machines

The Journey to Zero Trust: Data

Data



- **Categorization**
- **Protection**

Slido.com (#TXRE)

Slido Question

What are some zero trust principles you can implement?

CIP Standards That Indirectly Align with Zero Trust

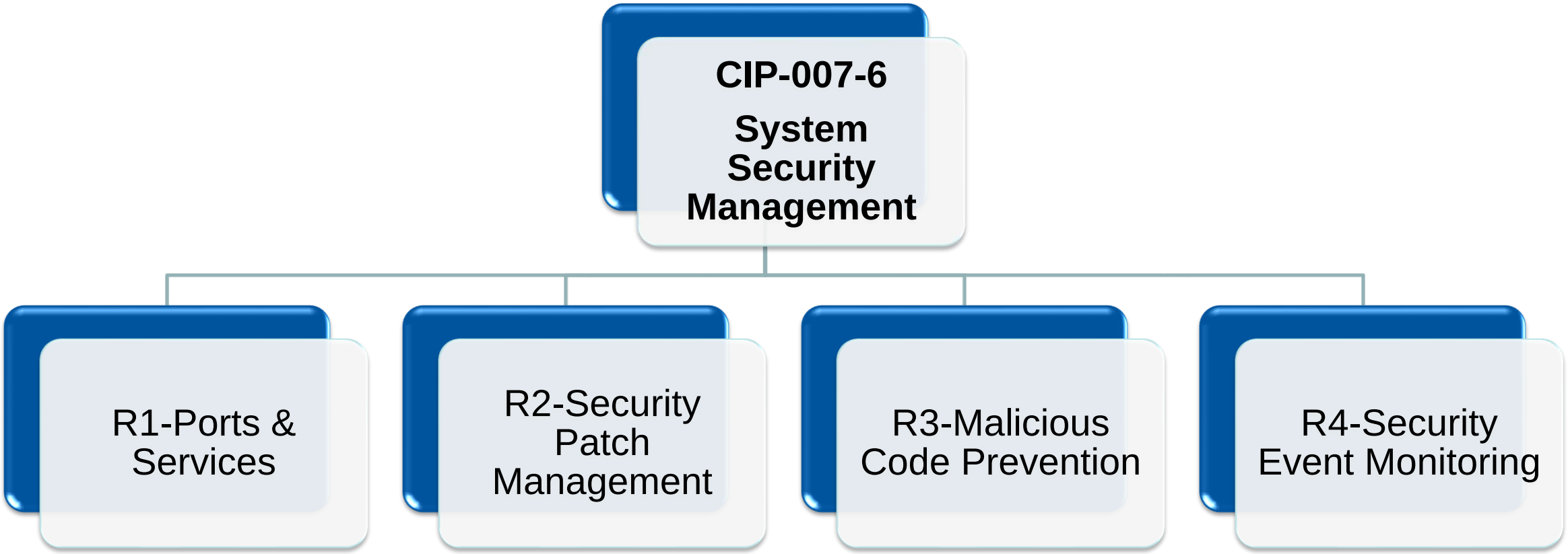
CIP Standards That Indirectly Align with Zero Trust

CIP-005-7

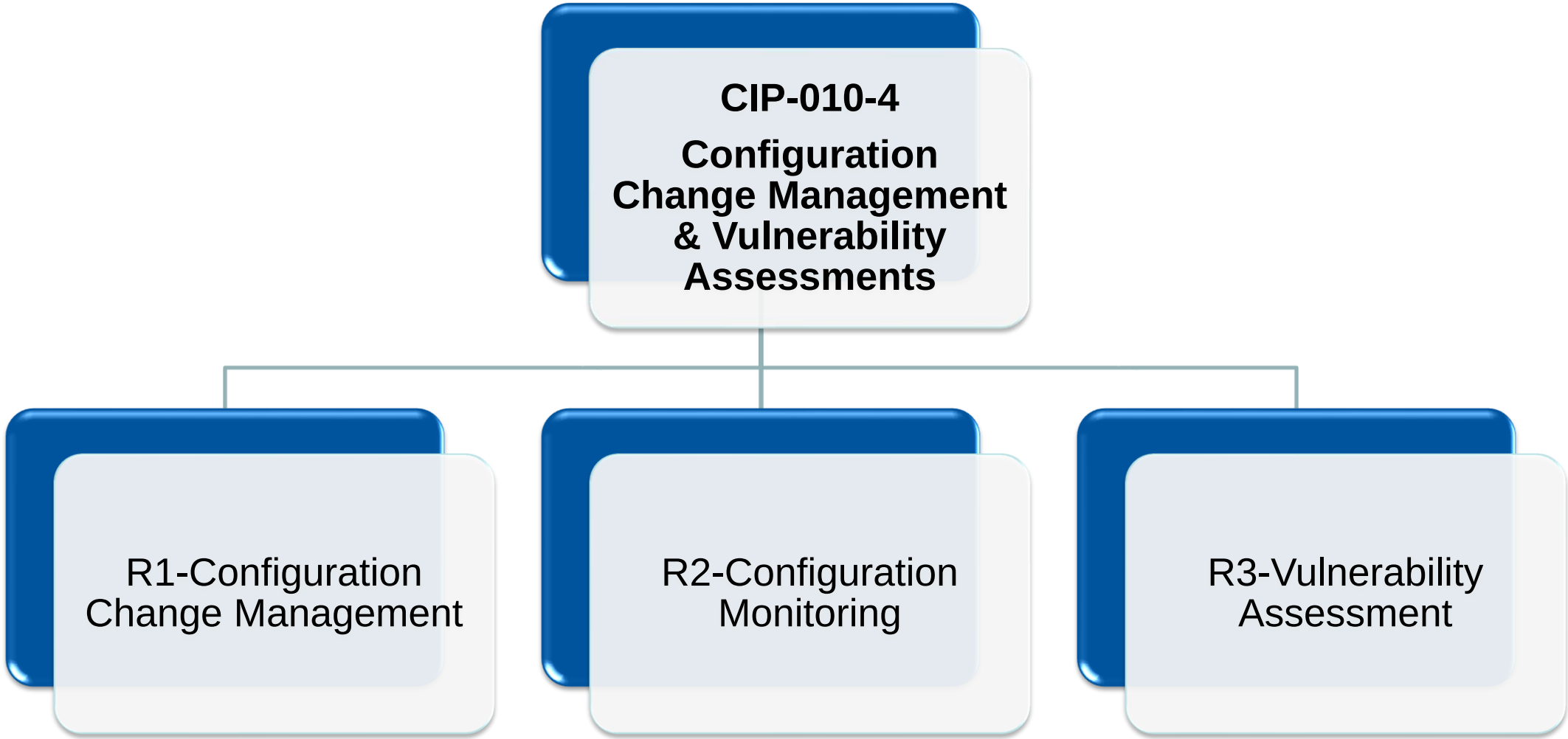
Electronic Security Perimeter

- R1-Electronic Security Perimeter
- R2-Remote Access Management
- R3-Vendor Remote Access Management for EACMS & PACS

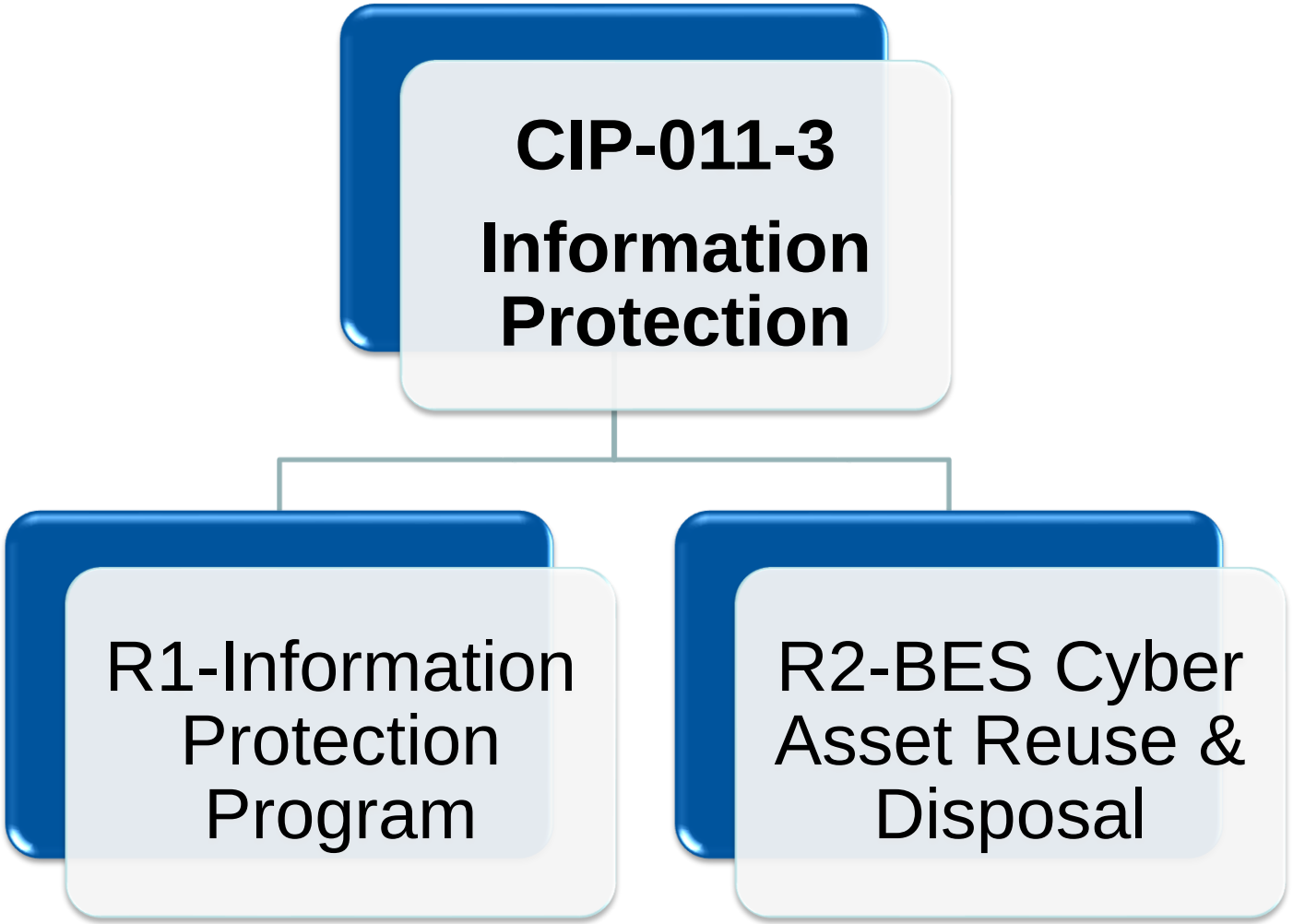
CIP Standards That Indirectly Align with Zero Trust



CIP Standards That Indirectly Align with Zero Trust



CIP Standards That Indirectly Align with Zero Trust



Resources

- **NIST SP 800-207**
  - Zero Trust Architecture (nist.gov)
  - Zero Trust Architecture - Glossary | CSRC (nist.gov)
- **National Cybersecurity Strategy**
  - National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)
- **National Cybersecurity Strategy Implementation Plan**
  - NCSIP-Version-2-FINAL-May-2024.pdf (whitehouse.gov)
- **CISA Zero Trust Security Model**
  - Zero Trust Maturity Model Version 2.0 (cisa.gov)

TEXAS RE
Ensuring electric reliability for Texans