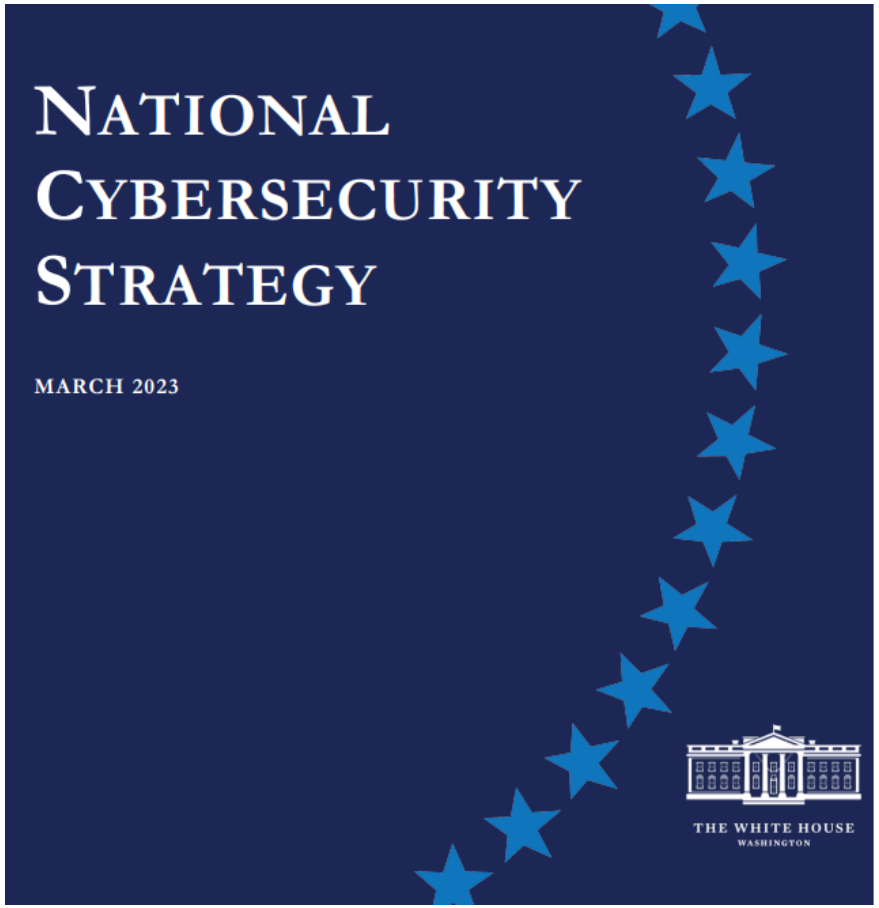
TEXAS RE

Zero Trust Architecture

Kenath Carver
Director, Compliance Assessments

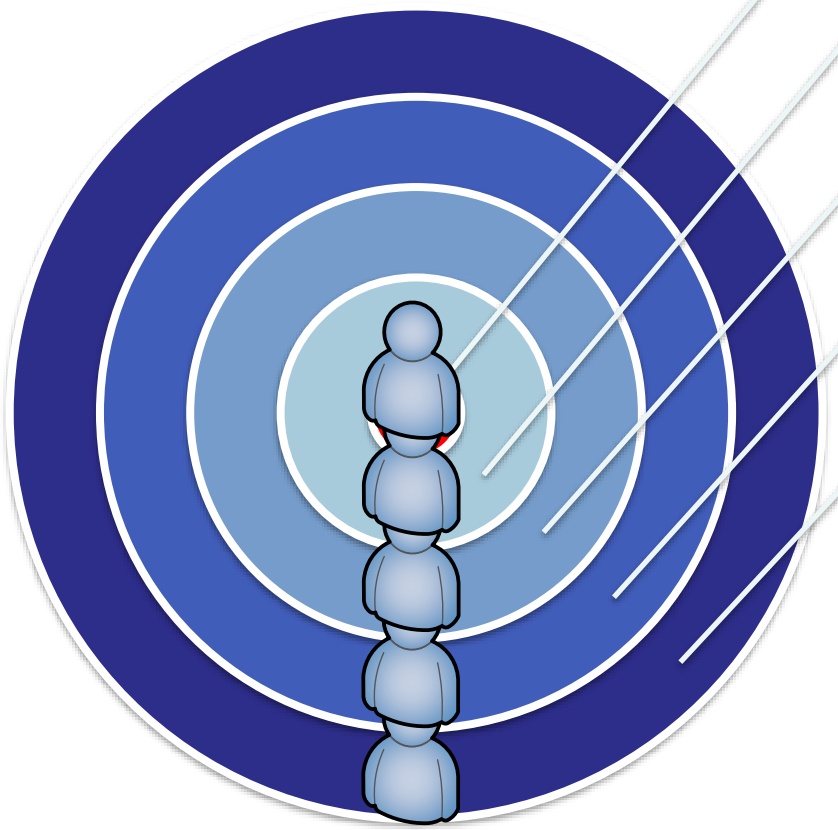
December 1, 2023

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**

Zero Trust Architecture



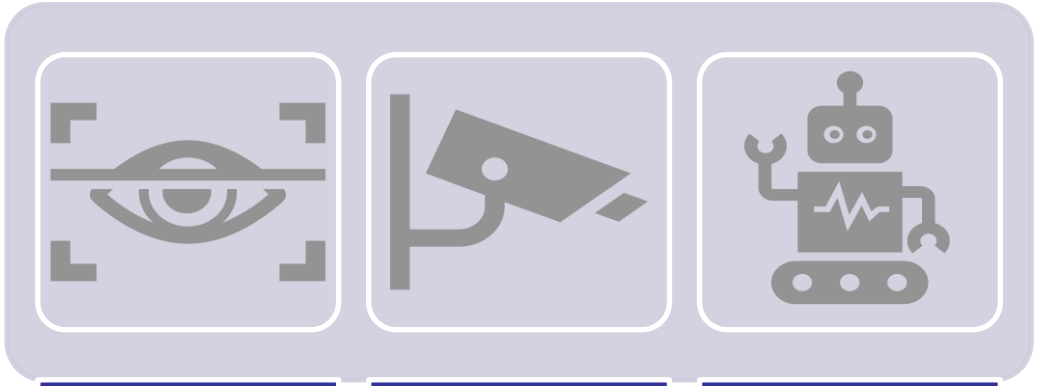
Data

Network

Applications

Devices

Users



Identification & Authentication

Monitor & Alert

AI Learning

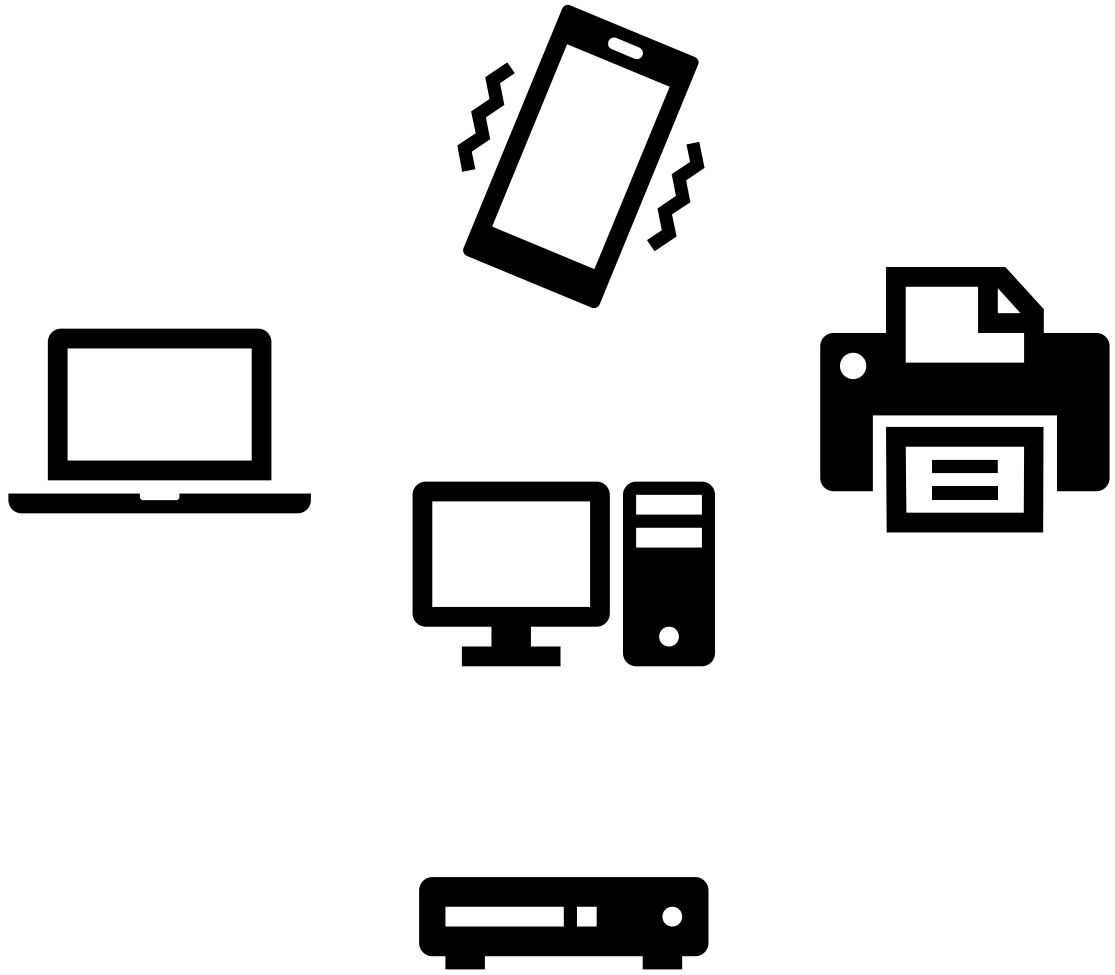
Zero Trust Architecture - Users

Identify

Access

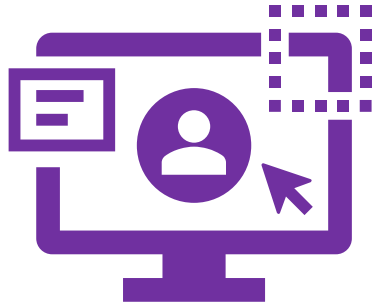
Zero Trust Architecture - Devices

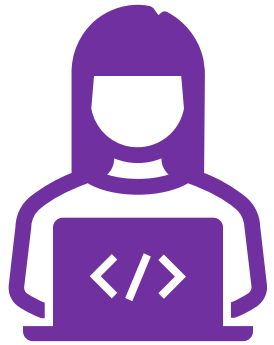
- Identify
- Authenticate
- Authorize
- Inventory
- Isolate
- Secure
- Remediate
- Control

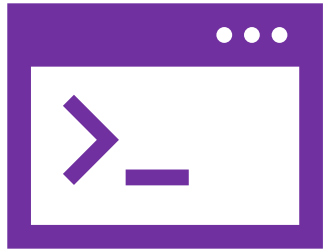


Zero Trust Architecture - Applications

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







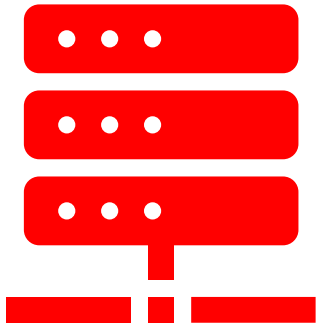
Zero Trust Architecture - Network

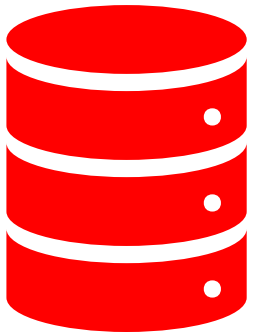
- Segment
- Isolate
- Control

Zero Trust Architecture - Data

Categorization

Protection





Department of Defense (DOD)

Zero Trust Reference Architecture

Cybersecurity and Infrastructure Security Agency (CISA)

Zero Trust Maturity Model

TEXAS RE
Ensuring electric reliability for Texans

Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Register Now

Cybersecurity Training for the Utility Wor…

Orlando, FL
Nov 28 - 30, 2023

Register Now

Cybersecurity Training for the Utility Wor…

Kansas City, MO
Dec 5 - 7, 2023

Register Now

Registration Coming Soon

Cybersecurity Training for the Utility Wor…

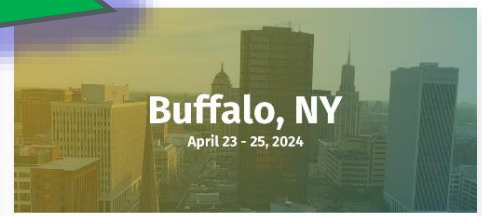
San Diego, CA
Jan 17 - 19, 2024

Registration Coming Soon

Cybersecurity Training for the Utility Wor…

Richardson, TX
Jan 23 - 25, 2024

Registration Coming Soon



Cybersecurity Training for the Utility Wor…

Amherst, NY
Apr 23 - 25, 2024

Registration Coming Soon

Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Agenda

Day 1

DOE CyberStrike (Full Day)

Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

OR

ICS Foundations (Full Day)

This course serves the purpose of introducing people into the field of industrial control systems (ICS) / operational technology (OT) and the cybersecurity considerations unique to securing these environments.

Day 2 Morning

CHOOSE 1 Morning Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

OR

DOE CyberStrike (Full Day)
Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

Day 2 Afternoon

CHOOSE 1 Afternoon Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

Day 3

Red Team / Blue Team Challenge Competition

Participants will work through a series of interactive learning scenarios that enable Operational Technology security professionals to develop and master the real-world, in-depth skills they need to defend real-time systems. It is designed as a challenge competition and is split into separate levels so that advanced players may quickly move through earlier levels based on their expertise. The Grid Netwars experience has been themed for the electricity industry and the scenario has been coordinated to align with industry exercise events.

Upcoming Events

Upcoming Events

Date	Title
11/29/2023	Talk with Texas RE: Risk Assessment Best Practices for Self-Reports
11/30/2023	Talk with Texas RE: O&P Practice Guide Review
12/01/2023	CIPWG
12/05/2023	Talk with Texas RE: Supply Chain/Risk Management Best Practices
12/07/2023	Talk with Texas RE: 2024 Implementation Plan
12/13/2023	Member Representatives Committee Meeting
12/13/2023	Audit, Governance, & Finance Committee Meeting
12/13/2023	Annual Membership Meeting
12/13/2023	Board of Directors Meeting
12/19/2023	Talk with Texas RE: Asset Management, the Foundation of a Solid Cybersecurity Program
12/25/2023	Christmas - Texas RE Office Closed
12/26/2023	Christmas - Texas RE Office Closed
03/05/2024	Women's Leadership in Grid Reliability and Security
04/24/2024	Spring Standards, Security, & Reliability Workshop
08/28/2024	Cyber and Physical Security Workshop

Calendar

News

Align Page