U.S. DEPARTMENT of ENERGY | Federal Energy Management Program

Zero Trust Architecture: How to Contract and Procure Zero Trust Products and Services

T02-S04, August 6th, 2025

FEMP Summer CAMP (Courses Aligned with Mission Priorities)

Sandy MacMurtrie

Director Federal Business Development
Johnson Controls Federal Systems

Agenda

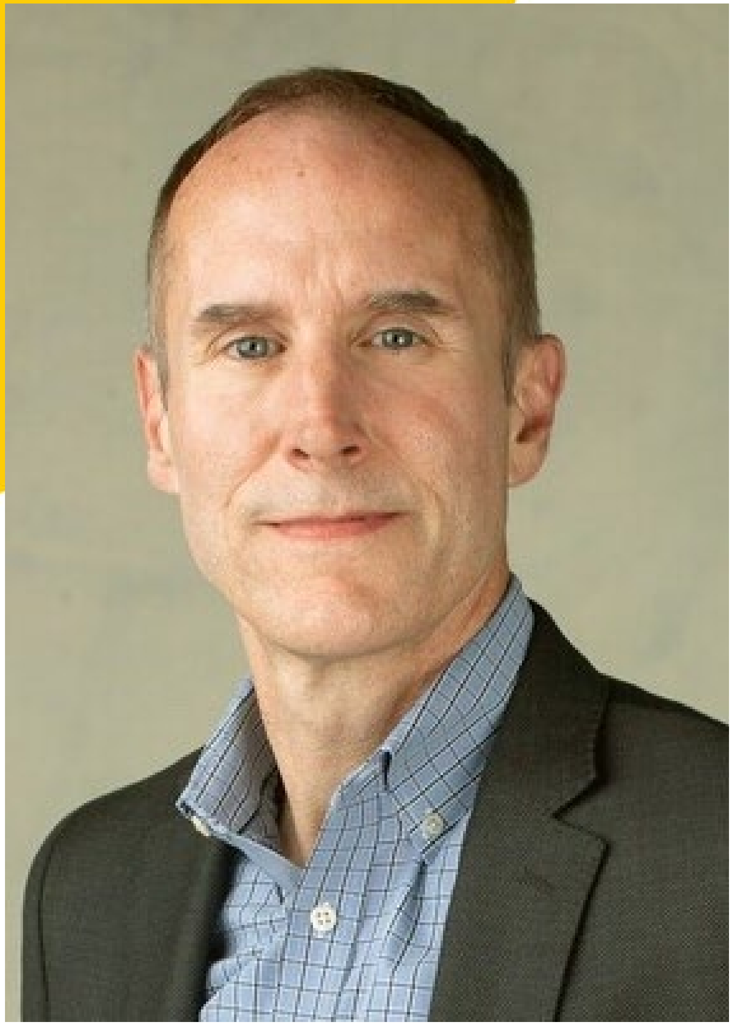
- Session Learning Objectives
- Advancing Cyber-Resilience Through Zero Trust
- The Role of Zero Trust in Modernizing Cybersecurity
- Questions and Answers
- Conclusion

Session Learning Outcomes

1. Identify the core principles of the zero trust security model.
2. Recognize the benefits of implementing zero trust to reduce organizational risks.
3. Identify key components required to apply least privilege and verification controls.
4. Determine a plan for zero trust integration in procurement processes.

Mr. Daryl Haegley

Technical Director,
Department of the Air Force Cyber Resiliency Office for Control Systems (CROCS)

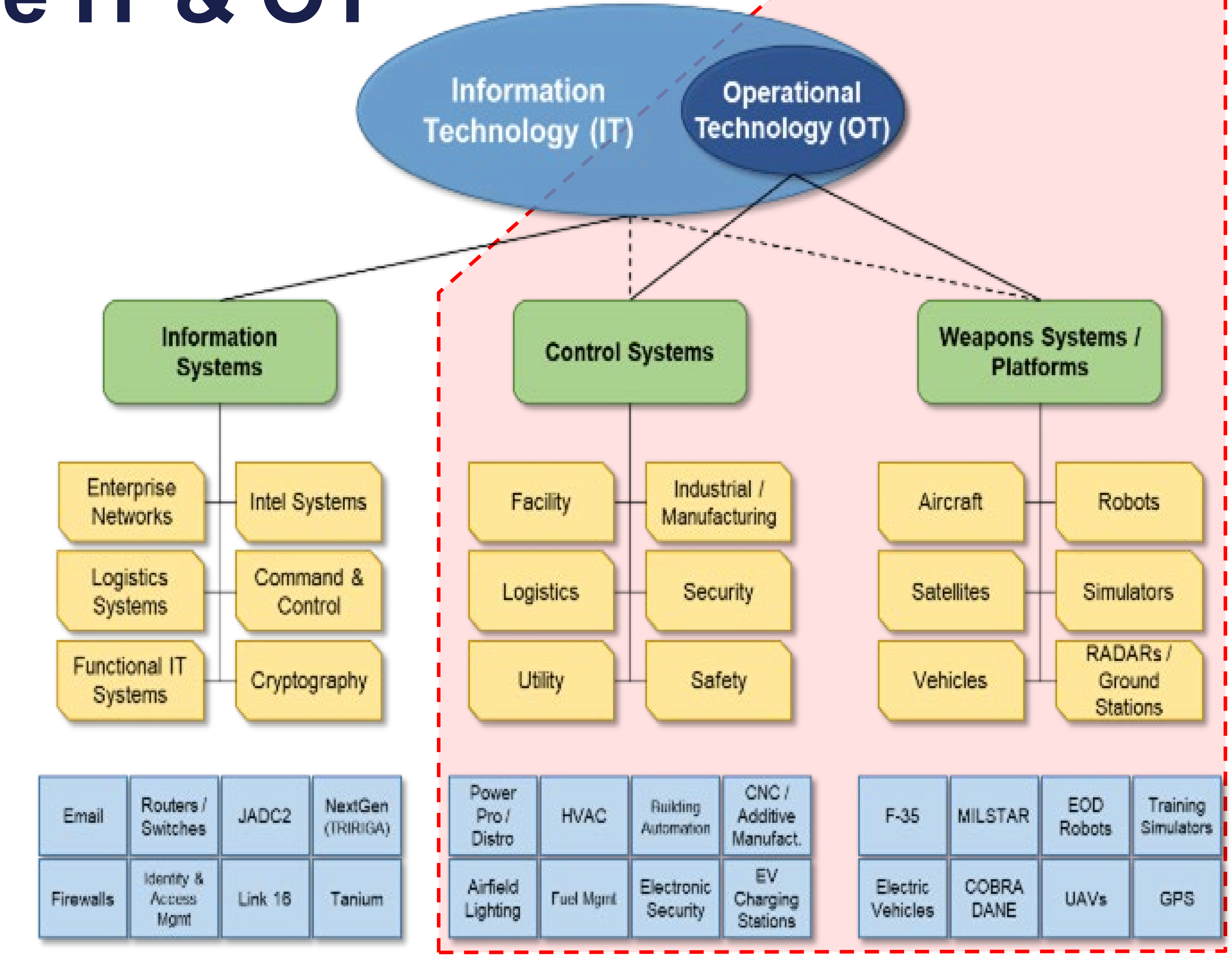


Mr. David Forbes

Director, Cyber Physical Defense
Booz Allen

Missions Require IT & OT

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." ***Sun Tzu***



Information Technology (IT)

Operational Technology (OT)

Information Systems

Enterprise Networks

Intel Systems

Logistics Systems

Command & Control

Functional IT Systems

Cryptography

Email

Routers / Switches

JADC2

NextGen (TRIRIGA)

Firewalls

Identity & Access Mgmt

Link 16

Tanium

Control Systems

Facility

Industrial / Manufacturing

Logistics

Security

Utility

Safety

Power Pro / Distro

HVAC

Building Automation

CNC / Additive Manufact.

Airfield Lighting

Fuel Mgmt

Electronic Security

EV Charging Stations

Weapons Systems / Platforms

Aircraft

Robots

Satellites

Simulators

Vehicles

RADARs / Ground Stations

F-35

MILSTAR

EOD Robots

Training Simulators

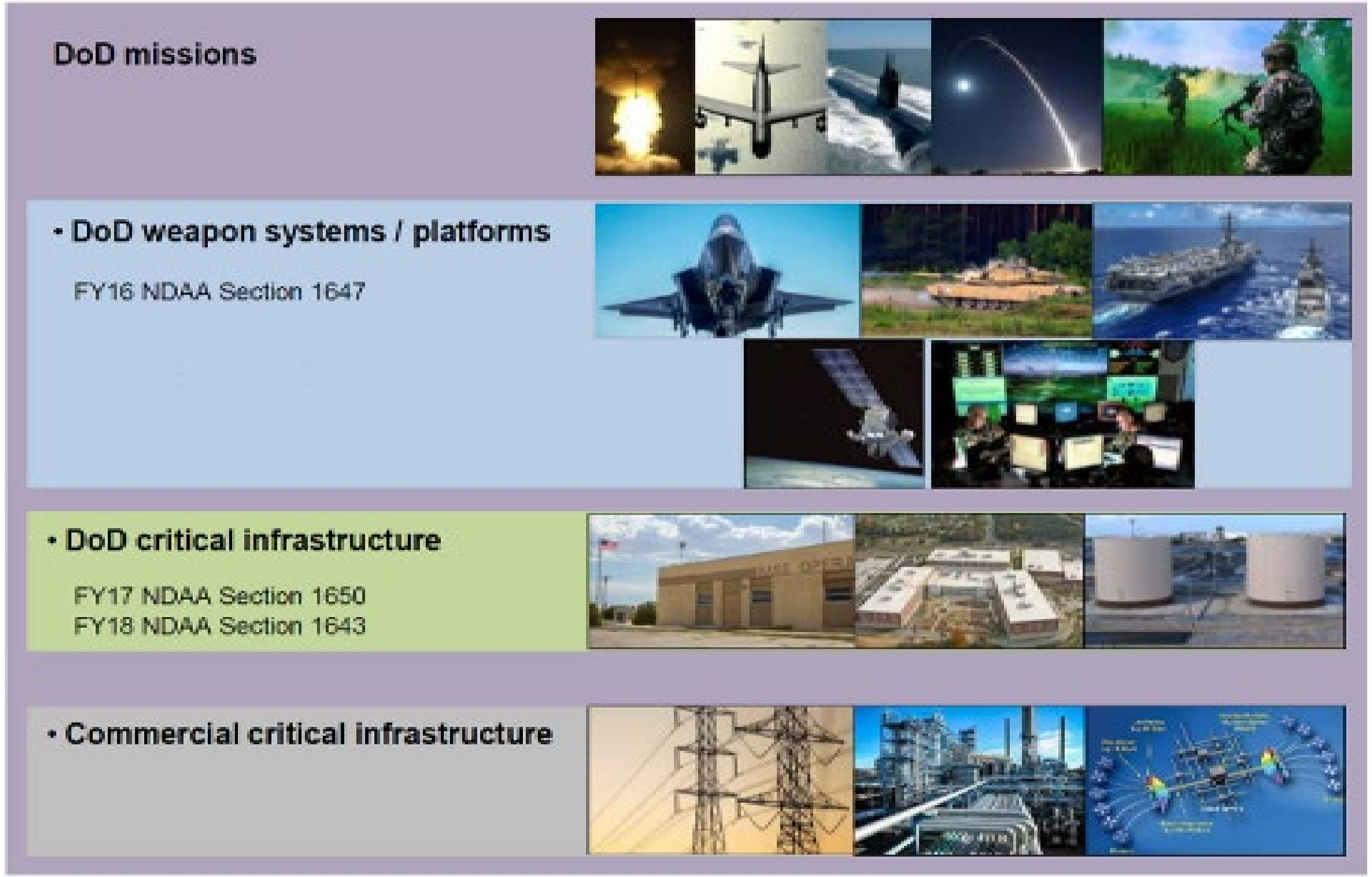
Electric Vehicles

COBRA DANE

UAVs

GPS

Missions Require IT & OT



DoD missions

- DoD weapon systems / platforms

FY16 NDAA Section 1647

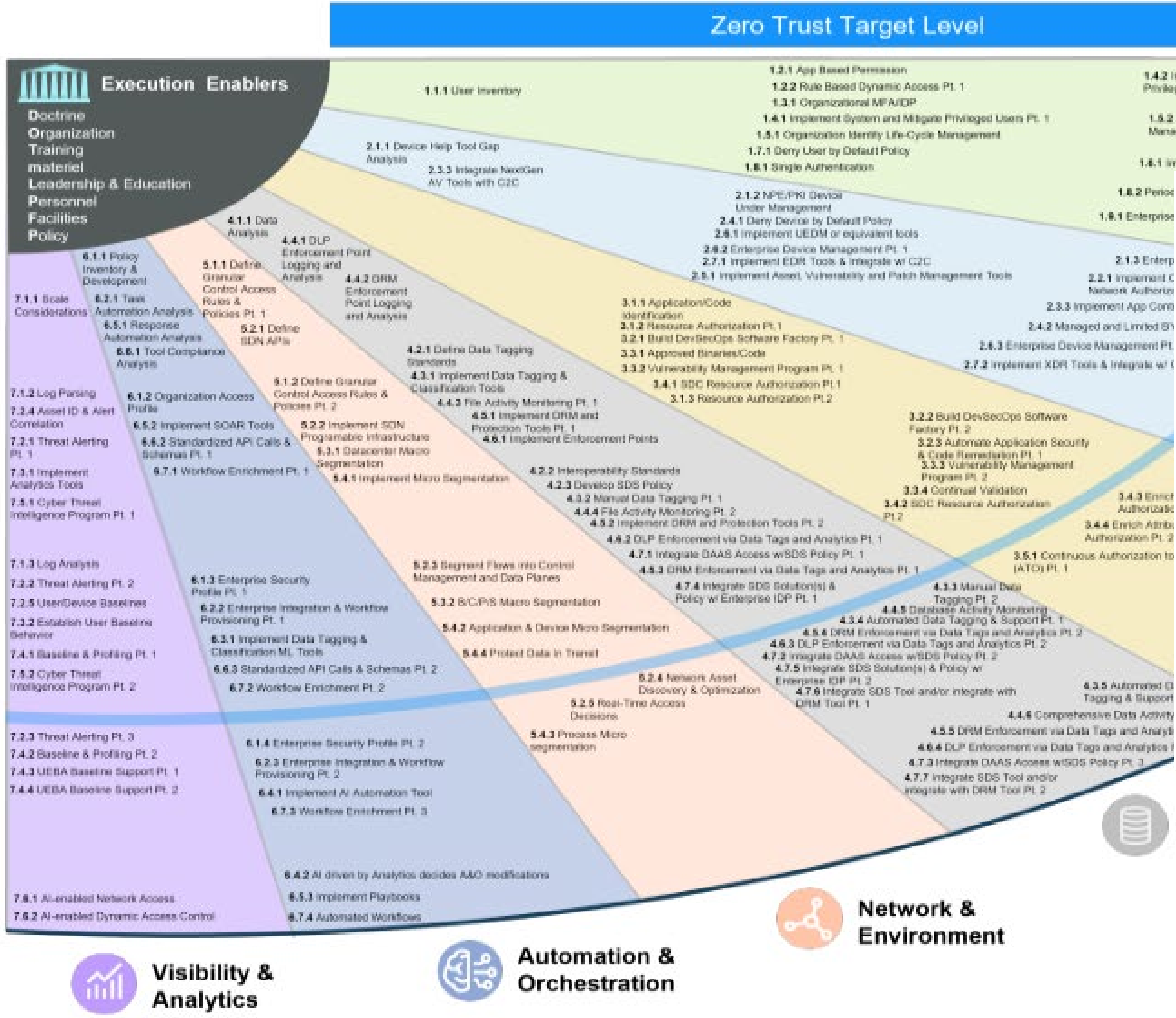
- DoD critical infrastructure

FY17 NDAA Section 1650
FY18 NDAA Section 1643

- Commercial critical infrastructure

100% of missions depend on power, water, or cooling

ZT ACTIVITIES APPLY = IT (152)



Zero Trust Target Level

Advanced Zero Trust

Execution Enablers

Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy

1.1.1 User Inventory
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Mitigate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.7.1 Deny User by Default Policy
1.8.1 Single Authentication
1.4.2 Implement System and Mitigate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.1 Implement UEBA Tooling
1.8.2 Perioc
1.9.1 Enterprise

1.2.3 Rule Based Dynamic Access Pt. 2
1.2.4 Enterprise Roles and Permissions Pt. 1
1.3.2 Alternative Flexible MFA Pt. 1
1.4.3 Real Time Approvals & JIT/JEA Analytics Pt. 1
1.2.5 Enterprise Roles and Permissions Pt. 2
1.3.3 Alternative Flexible MFA Pt. 2
1.4.4 Real Time Approvals & JIT/JEA Analytics Pt. 2

2.1.1 Device Help Tool Gap Analysis
2.3.3 Integrate NextGen AV Tools with C2C
2.1.2 NPE/PKI Device Under Management
2.4.1 Deny Device by Default Policy
2.6.1 Implement UEDM or equivalent tools
2.6.2 Enterprise Device Management Pt. 1
2.7.1 Implement EDR Tools & Integrate w/ C2C
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.1.3 Enterp
2.2.1 Implement C Network Authoriz
2.3.3 Implement App Cont
2.4.2 Managed and Limited B
2.6.3 Enterprise Device Management Pt.
2.7.2 Implement XDR Tools & Integrate w/ C

3.1.1 Application/Code Identification
3.1.2 Resource Authorization Pt. 1
3.2.1 Build DevSecOps Software Factory Pt. 1
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
3.4.1 SDC Resource Authorization Pt.1
3.1.3 Resource Authorization Pt.2
3.2.2 Build DevSecOps Software Factory Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.3.3 Vulnerability Management Program Pt. 2
3.3.4 Continual Validation
3.4.2 SDC Resource Authorization Pt.2
3.4.3 Enrich Authorizatio
3.4.4 Enrich Attrib Authorization Pt. 2
3.5.1 Continuous Authorization to (ATO) Pt. 1

4.1.1 Data Analysis
4.4.1 DLP Enforcement Point Logging and Analysis
4.4.2 DRM Enforcement Point Logging and Analysis
4.2.1 Define Data Tagging Standards
4.3.1 Implement Data Tagging & Classification Tools
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.6.1 Implement Enforcement Points
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
4.3.2 Manual Data Tagging Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
4.3.3 Manual Data Tagging Pt. 2
4.4.5 Database Activity Monitoring
4.3.4 Automated Data Tagging & Support Pt. 1
4.5.4 DRM Enforcement via Data Tags and Analytics Pt. 2
4.6.3 DLP Enforcement via Data Tags and Analytics Pt. 2
4.7.2 Integrate DAAS Access w/SDS Policy Pt. 2
4.7.5 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2
4.7.6 Integrate SDS Tool and/or integrate with DRM Tool Pt. 1
4.3.5 Automated D Tagging & Support
4.4.6 Comprehensive Data Activity
4.5.5 DRM Enforcement via Data Tags and Analy
4.6.4 DLP Enforcement via Data Tags and Analytics
4.7.3 Integrate DAAS Access w/SDS Policy Pt. 3
4.7.7 Integrate SDS Tool and/or integrate with DRM Tool Pt. 2

5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.2.2 Implement SDN Programable Infrastructure
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data In Transit
5.2.4 Network Asset Discovery & Optimization
5.2.5 Real-Time Access Decisions
5.4.3 Process Micro segmentation

6.1.1 Policy Inventory & Development
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
6.1.2 Organization Access Profile
6.5.2 Implement SOAR Tools
6.6.2 Standardized API Calls & Schemas Pt. 1
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
6.3.1 Implement Data Tagging & Classification ML Tools
6.6.3 Standardized API Calls & Schemas Pt. 2
6.7.2 Workflow Enrichment Pt. 2
6.1.4 Enterprise Security Profile Pt. 2
6.2.3 Enterprise Integration & Workflow Provisioning Pt. 2
6.4.1 Implement AI Automation Tool
6.7.3 Workflow Enrichment Pt. 3
6.4.2 AI driven by Analytics decides A&O modifications
6.5.3 Implement Playbooks
6.7.4 Automated Workflows

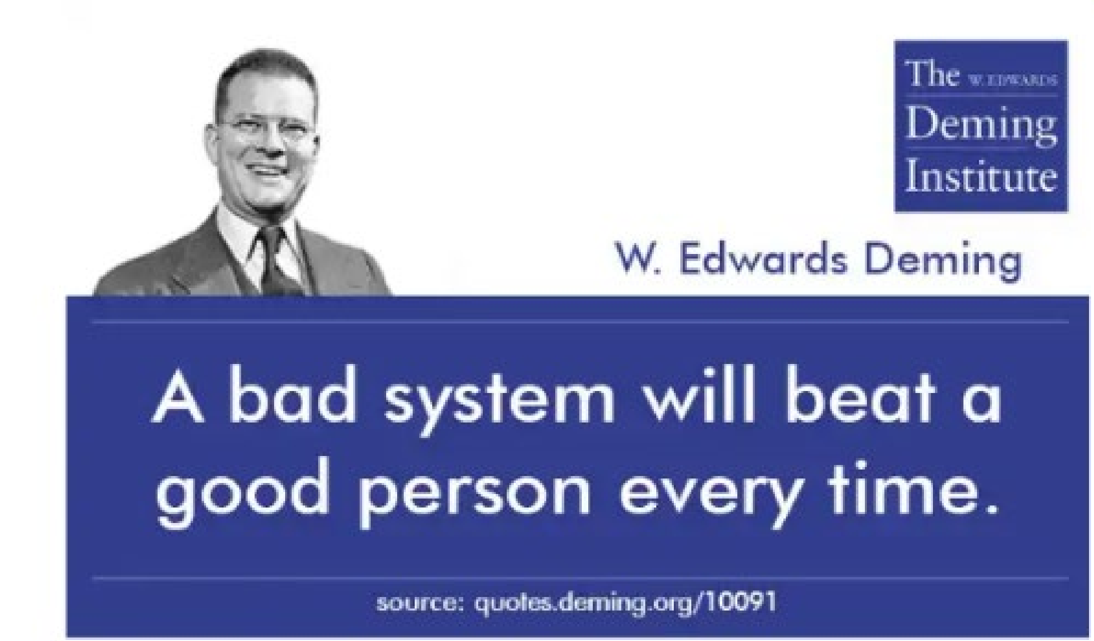
7.1.1 Scale Considerations
7.1.2 Log Parsing
7.2.4 Asset ID & Alert Correlation
7.2.1 Threat Alerting Pt. 1
7.3.1 Implement Analytics Tools
7.5.1 Cyber Threat Intelligence Program Pt. 1
7.1.3 Log Analysis
7.2.2 Threat Alerting Pt. 2
7.2.5 User/Device Baselines
7.3.2 Establish User Baseline Behavior
7.4.1 Baseline & Profiling Pt. 1
7.5.2 Cyber Threat Intelligence Program Pt. 2
7.2.3 Threat Alerting Pt. 3
7.4.2 Baseline & Profiling Pt. 2
7.4.3 UEBA Baseline Support Pt. 1
7.4.4 UEBA Baseline Support Pt. 2
7.6.1 AI-enabled Network Access
7.6.2 AI-enabled Dynamic Access Control

Data

Network & Environment

Automation & Orchestration

Visibility & Analytics



The W. EDWARDS Deming Institute

W. Edwards Deming

A bad system will beat a good person every time.

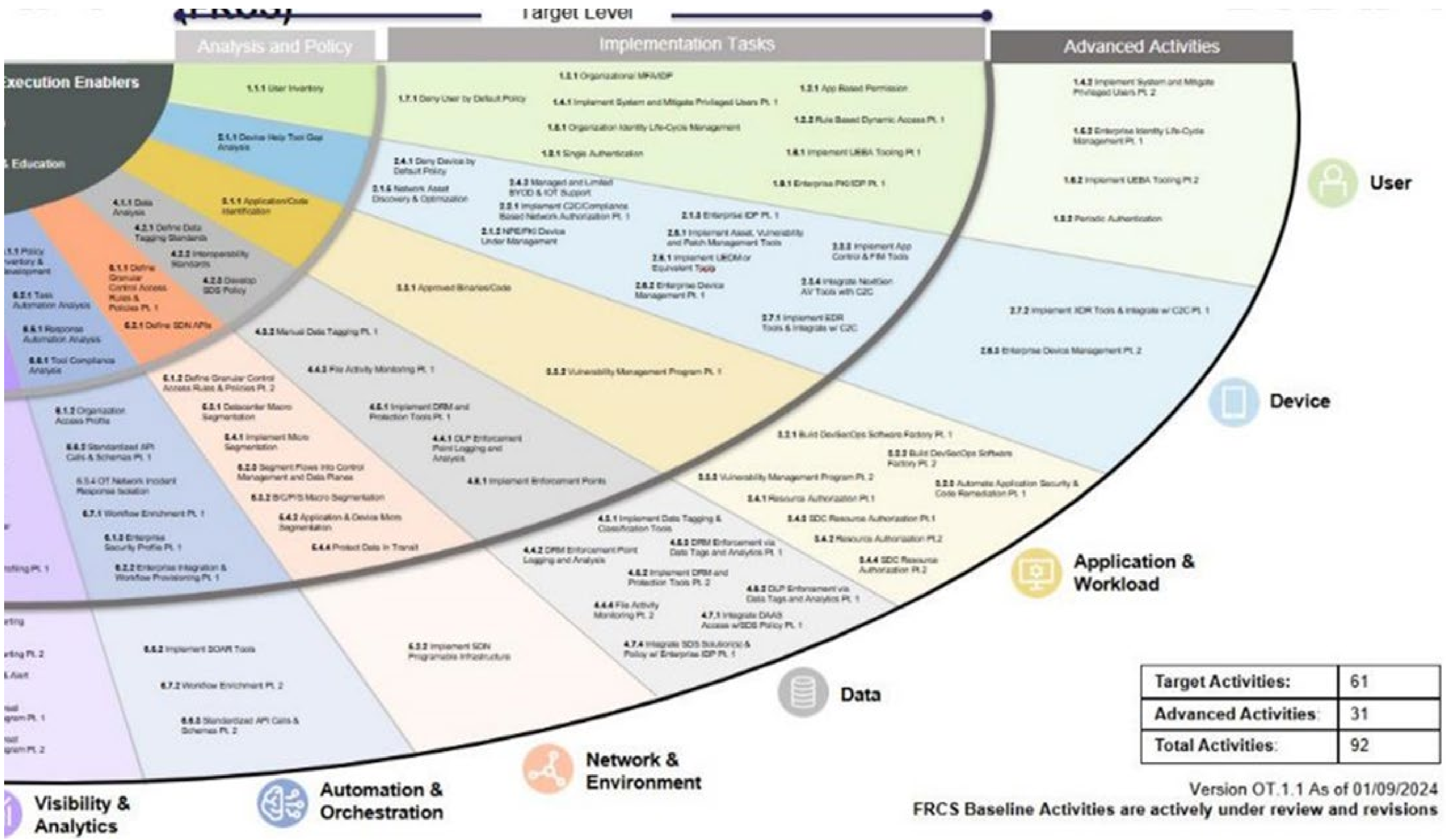
source: quotes.deming.org/10091

Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.0 As of 10/04/2022

DRAFT = ZT ACTIVITIES APPLY = OT (91)


Target Level
Analysis and Policy
Implementation Tasks
Advanced Activities
Execution Enablers
& Education
1.1.1 User Inventory
2.1.1 Device Help Tool Gap Analysis
3.1.1 Application/Code Identification
4.1.1 Data Analysis
4.2.1 Define Data Tagging Standards
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
1.1 Policy ventory & evelopment
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
1.7.1 Deny User by Default Policy
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Migrate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.8.1 Single Authentication
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.6.1 Implement UEBA Tooling Pt. 1
1.9.1 Enterprise PKI/IDP Pt. 1
2.4.1 Deny Device by Default Policy
2.1.6 Network Asset Discovery & Optimization
2.4.2 Managed and Limited BYOD & IOT Support
2.2.1 Implement C2C/Compliance Based Network Authorization Pt. 1
2.1.2 NPE/PKI Device Under Management
2.1.3 Enterprise IDP Pt. 1
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.6.1 Implement UEDM or Equivalent Tools
2.6.2 Enterprise Device Management Pt. 1
2.3.3 Implement App Control & FIM Tools
2.3.4 Integrate NextGen AV Tools with C2C
2.7.1 Implement EDR Tools & Integrate w/ C2C
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
4.3.2 Manual Data Tagging Pt. 1
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.4.1 DLP Enforcement Point Logging and Analysis
4.6.1 Implement Enforcement Points
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data in Transit
6.1.2 Organization Access Profile
6.6.2 Standardized API Calls & Schemas Pt. 1
6.5.4 OT Network Incident Response Isolation
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
ofiling Pt. 1
rting
rting Pt. 2
& Alert
ntel gram Pt. 1
ntel gram Pt. 2
6.5.2 Implement SOAR Tools
6.7.2 Workflow Enrichment Pt. 2
6.6.3 Standardized API Calls & Schemas Pt. 2
5.2.2 Implement SDN Programmable Infrastructure
4.3.1 Implement Data Tagging & Classification Tools
4.4.2 DRM Enforcement Point Logging and Analysis
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
3.2.1 Build DevSecOps Software Factory Pt. 1
3.2.2 Build DevSecOps Software Factory Pt. 2
3.3.3 Vulnerability Management Program Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.4.1 Resource Authorization Pt. 1
3.4.3 SDC Resource Authorization Pt. 1
3.4.2 Resource Authorization Pt. 2
3.4.4 SDC Resource Authorization Pt. 2
1.4.2 Implement System and Migrate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.2 Implement UEBA Tooling Pt. 2
1.8.2 Periodic Authentication
2.7.2 Implement XDR Tools & Integrate w/ C2C Pt. 1
2.6.3 Enterprise Device Management Pt. 2
User
Device
Application & Workload
Data
Network & Environment
Automation & Orchestration
Visibility & Analytics

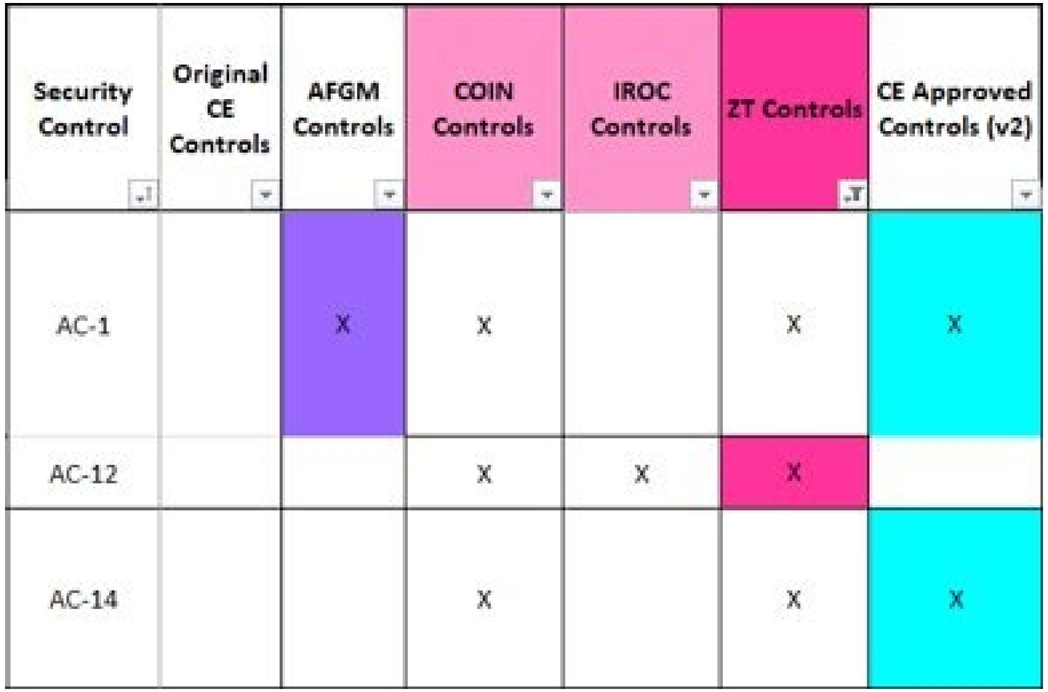
Target Activities:	61
Advanced Activities:	31
Total Activities:	92

Version OT.1.1 As of 01/09/2024

FRCS Baseline Activities are actively under review and revisions

ZT Implementation = TAKE CREDIT!

- NIST control selection shows alignment of ZT and current Civ Engr OT security controls
- Developed to review initial 42 controls as they expanded to 203 controls *(720?)*
- ZT Controls coverage by CE environment:
  - Original CE Approved Controls: ~09%
  - AFGM Controls: ~12%
  - COIN Controls: ~27%
  - IROC Controls: ~17%
  - CE Approved Controls v2: ~30%



Security Control	Original CE Controls	AFGM Controls	COIN Controls	IROC Controls	ZT Controls	CE Approved Controls (v2)
AC-1		X	X		X	X
AC-12			X	X	X	
AC-14			X		X	X

DAF already implementing security controls listed in ZT Strategy Implementation Plan

3 & 3: Advancing Cyber Resilience

3 Actions to Take:

1. Implement Risk-Based Segmentation

   Segmentation prevents attackers from moving laterally through network once they've gained a foothold; Confines impact making it harder for adversaries to compromise critical functions.

2. Establish Robust Vulnerability Management Program Tailored for OT

   Well-designed vulnerability management program identifies & mitigate weaknesses before exploitation

3. Foster Collaboration Between IT & OT Teams

   Isolating IT & OT can lead to gaps in security coverage, collaboration leverages strengths of both

3 Pitfalls to Avoid:

1. Ignoring Legacy Systems

   Legacy systems are often weakest link in security chain. Adversaries often target these systems to gain initial access

2. Prioritizing Availability Over Security:

   Availability is critical in OT environments, neglecting security can lead to catastrophic consequences, including safety incidents, environmental damage, and production downtime.

3. Treating OT Security as a One-Time Project:

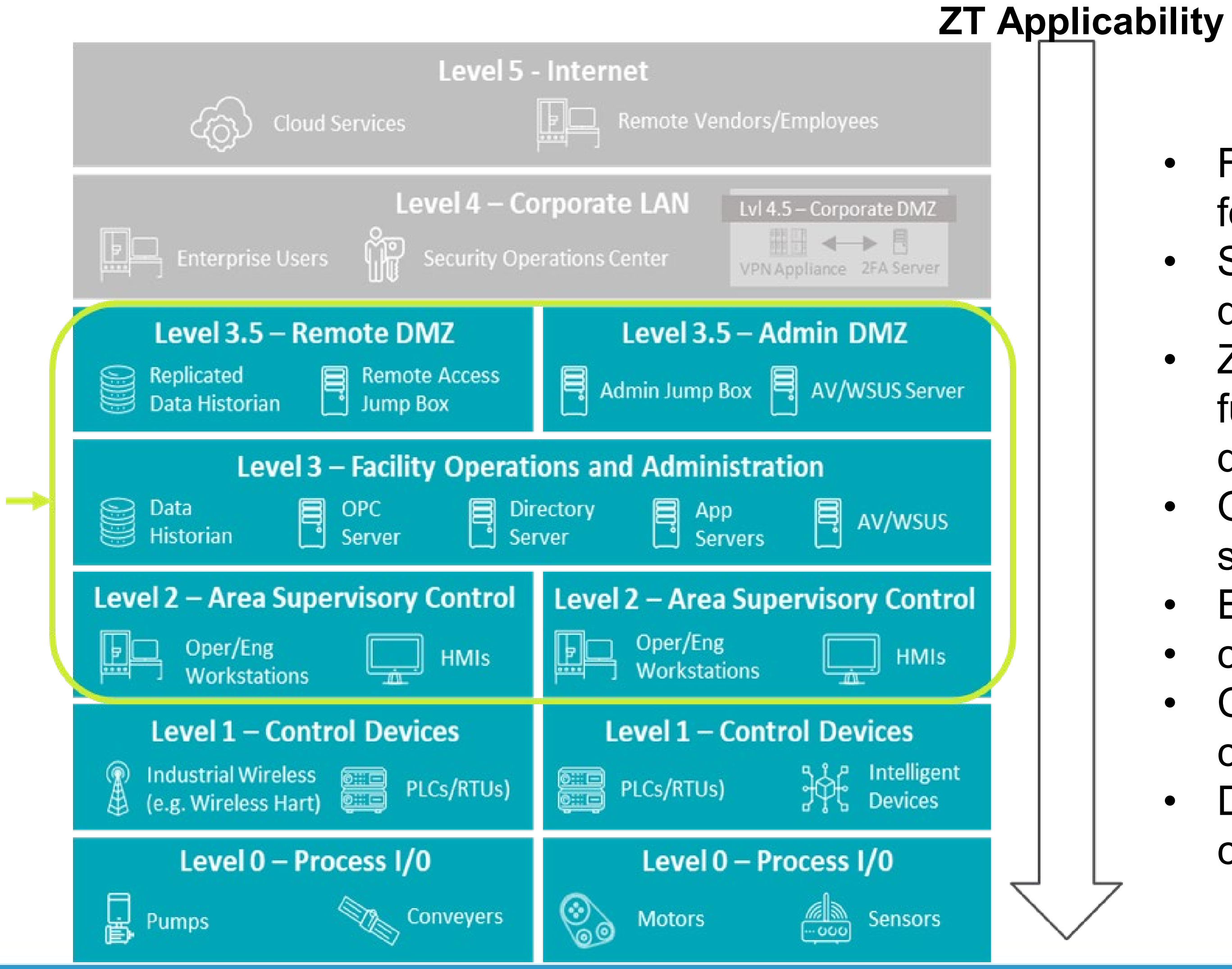
   Incessant threat landscape is constantly evolving; new vulnerabilities discovered regularly; Static security postures quickly become outdated / ineffective

Changing the Game

The Role of Zero Trust in Modernizing OT Cybersecurity

FEMP Summer CAMP (Courses Aligned with Mission Priorities)

Demystifying Zero Trust for OT



ZT Applicability

ZT for OT Funnel of Opportunity

Level 5 - Internet
Cloud Services
Remote Vendors/Employees

Level 4 – Corporate LAN
Enterprise Users
Security Operations Center
Lvl 4.5 – Corporate DMZ
VPN Appliance
2FA Server

Level 3.5 – Remote DMZ
Replicated Data Historian
Remote Access Jump Box

Level 3.5 – Admin DMZ
Admin Jump Box
AV/WSUS Server

Level 3 – Facility Operations and Administration
Data Historian
OPC Server
Directory Server
App Servers
AV/WSUS

Level 2 – Area Supervisory Control
Oper/Eng Workstations
HMIs

Level 2 – Area Supervisory Control
Oper/Eng Workstations
HMIs

Level 1 – Control Devices
Industrial Wireless (e.g. Wireless Hart)
PLCs/RTUs)

Level 1 – Control Devices
PLCs/RTUs)
Intelligent Devices

Level 0 – Process I/0
Pumps
Conveyers

Level 0 – Process I/0
Motors
Sensors

- Focus on ***The Funnel of Opportunity*** for ZT implementation (Purdue L3-L1)
- Successful OT cybersecurity programs do the basics well
- ZT & OT Cybersecurity are fundamentally both engineering disciplines
- OT data isn’t always sensitive Novel solutions don’t scale
- Endpoints can’t always be hardened, but
- can always be secured
- Connectivity and bandwidth are often constrained
- Detection/response dwell time directly correlates to risk of impact

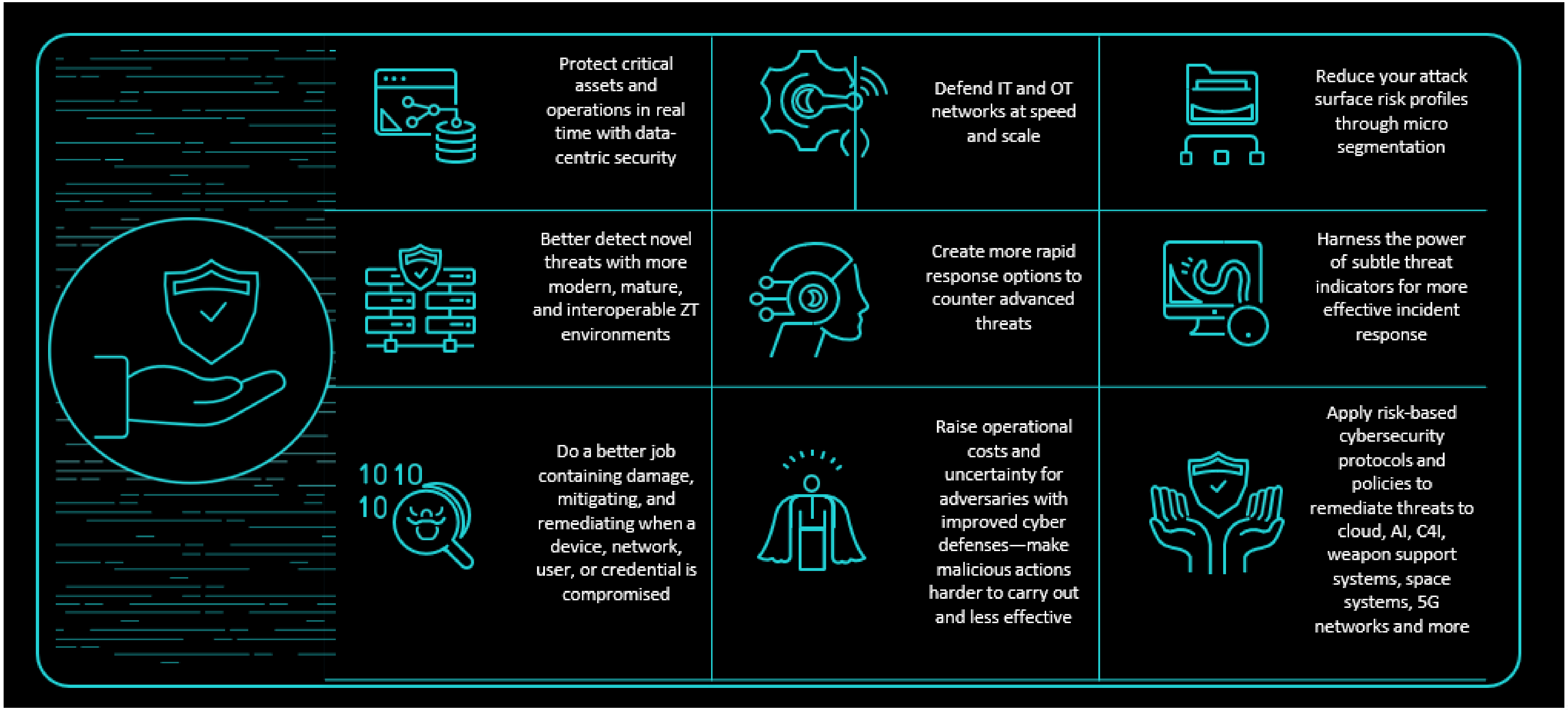
Benefits of Implementing Zero Trust

Stronger Protection

More Stable Cyber Investments

Accelerated Mission Outcomes

Stronger Protection - Examples



Protect critical assets and operations in real time with data-centric security

Defend IT and OT networks at speed and scale

Reduce your attack surface risk profiles through micro segmentation

Better detect novel threats with more modern, mature, and interoperable ZT environments

Create more rapid response options to counter advanced threats

Harness the power of subtle threat indicators for more effective incident response

Do a better job containing damage, mitigating, and remediating when a device, network, user, or credential is compromised

Raise operational costs and uncertainty for adversaries with improved cyber defenses—make malicious actions harder to carry out and less effective

Apply risk-based cybersecurity protocols and policies to remediate threats to cloud, AI, C4I, weapon support systems, space systems, 5G networks and more

Zero Trust Myths Dispelled

MYTH: YOU CAN BUY ZERO TRUST

REALITY:

- Zero trust (ZT) is a security mindset that protects high-value assets in real time
- A zero trust architecture (ZTA) is not a product that can be bought off the shelf
- It is an architectural approach that can be implemented systematically

MYTH: ONE VENDOR IS THE SOLUTION

REALITY:

- No one vendor can provide a comprehensive ZT solution
- An array of cyber vendor solutions and cloud service providers can equip asset owners with the ZT solutions they need to achieve mission objectives
- This includes integrating various vendor products to deploying solutions that provide continuous risk monitoring through prevention, detection, response, and prediction.

MYTH: ZERO TRUST IS IMPRACTICAL

REALITY:

- Organizations can apply ZT's three design principles to create practical solutions for vital missions
- ZT assessment models let organizations scrutinize their strengths and challenges and then chart a path to a ZTA

MYTH: LEGACY SYSTEMS ≠ ZERO TRUST

REALITY:

- There is no single approach to implementing ZT. Legacy infrastructure is a common challenge, but it's not a showstopper. Existing systems may already provide robust ZT capabilities.
- Your ZT journey starts with baselining your existing environment, measuring against the ZT maturity model and then developing an architecture that can leverage your existing legacy systems to achieve your ZT goals.

Keys to Success

- Identify a key system to pilot your ZT implementation. Set realistic expectations on scope and timelines.
- Once validated, scale gradually across the organization, applying lessons learned from the pilot to expand coverage systematically.
- Implement network macro- and micro-segmentation; deploy OT network visibility and monitoring tools.
- Where remote access is required, deploy secure remote access technologies that enforce MFA/CAC authentication.

Pitfalls to Avoid

Don't let perfect be the enemy of good. Set a goal and iterate toward it rather than trying to achieve complete ZT implementation immediately.

Perform proper due diligence on ZT technologies. Ensure selected technologies meet requirements and that the technology actually delivers on what it promises.

Avoid treating ZT as a single product purchase rather than recognizing it as an architectural approach requiring process and cultural changes.

Don’t overlook ongoing OT cybersecurity practices; a sound network security process often can be mapped to multiple zero trust activities.

Tactics, Techniques, & Procedures

What we have learned so far:

- Prioritize high criticality systems to make meaningful impacts to the overall security posture.
- Implement continuous monitoring and verification rather than relying on periodic security assessments.
- Establish metrics for success early – this might be asset inventory, network visibility Vulnerability numbers, MTTR/MTTD, etc.
- Focus on identity and device verification as foundational elements before expanding to network and application controls.
- Create a shared responsibility model and incentives for collaborations.

Questions?

U.S. DEPARTMENT of ENERGY | Federal Energy Management Program

This Training Is Accredited

How to obtain your CEUs:

1. Log in to https://edu.wbdg.org/ using your WBDG credentials
   - The assessment and evaluation will be made available to attendees at 8:00am ET on Monday, August 11th
   - The assessment and evaluation will close on September 22nd
2. In the list of trainings you attended, click on the Visit link by the course you wish to complete
   - If the course you're looking for is not listed, click on My Account in the top right menu
   - If you still can't find your course, contact the WBDG support team to check your eligibility
3. Complete the assessment with a score of 80% or above
4. Upon passing the assessment, click the Post-Evaluation Survey button
5. Complete and submit the evaluation
6. Click Download Your Certificate to generate your certificate of completion, which can be downloaded for your records

Questions or issues? Contact WBDG Support at wbdg@nibs.org.

ⓘ

What's an IACET CEU?

A continuing education unit (CEU) from the International Association for Continuing Education and Training (IACET) equals 10 hours of learning in an approved program for licensed or certified professionals.

Thank You

U.S. DEPARTMENT of ENERGY | Federal Energy Management Program

FEMP Summer CAMP (Courses Aligned with Mission Priorities)

Connect With FEMP!

Stay connected with FEMP by subscribing to newsletters, following along on LinkedIn, and submitting questions to the Technical Assistance Portal.

Ask Questions

Visit FEMP's Technical Assistance Portal.

Subscribe

Receive periodic emails to stay informed.

Find Trainings

Explore the FEMP Training Catalog to find live and on-demand trainings and events.

Follow FEMP

Follow FEMP on LinkedIn for of-the-moment news.