USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

A Journey into Defensible Architecture: A Defenders' Guide

Cybersecurity and Digitalization: Supply Chain Risks in the Electricity Sector

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

Markus Mueller
Principle Industrial Consultant
Dragos

LinkedIn: www.linkedin.com/in/markusmuellerics

Email: mmueller@dragos.com

Website: www.dragos.com

DRAGOS

USAID
FROM THE AMERICAN PEOPLE

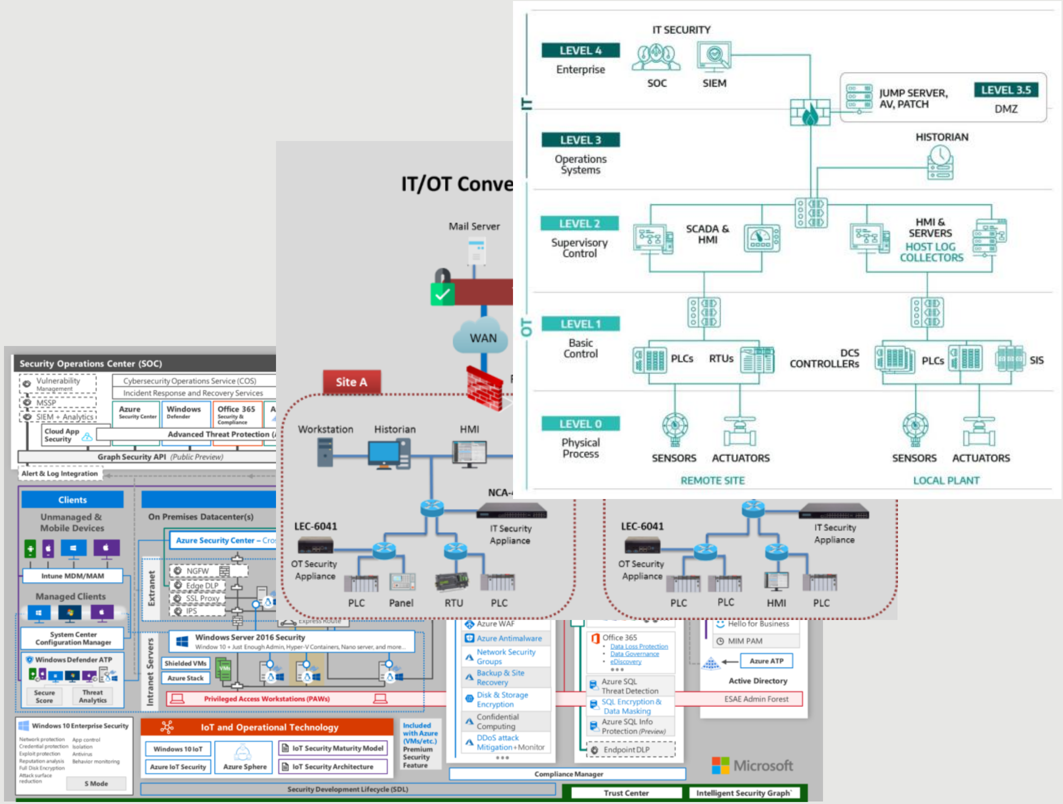
USEA
United States Energy Association

Brian Foster
Senior OT Cybersecurity Architect
Southern California Edison

Reference Architectures

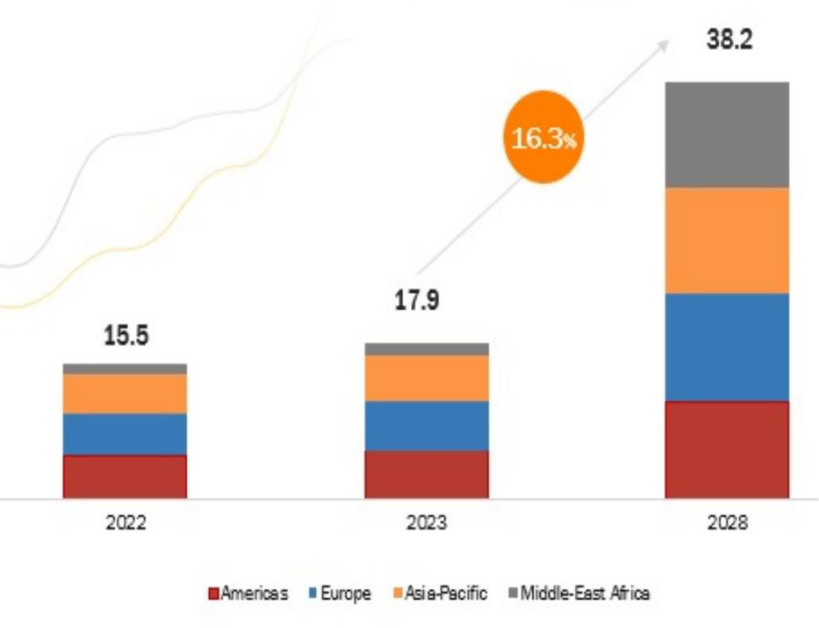
Best Practices May Not Be The Best Approach

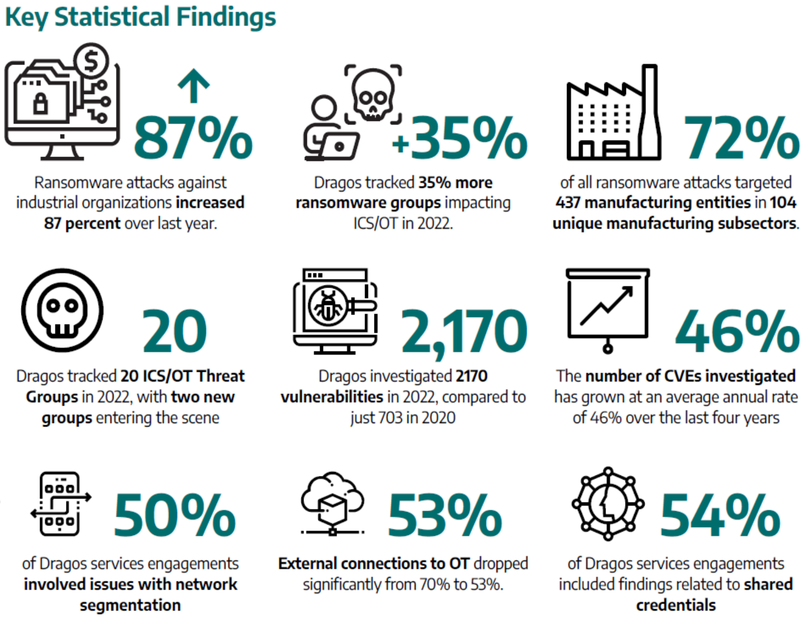
- Define and segment the layers
- Defense at each layer
- Traffic inspection and filtering between layers
- Encrypt critical data
- Deploy security solutions on the network and endpoints
- Zero Trust



Reference Architectures

Failure To Understand The Why Can Result In Failure





Key Statistical Findings

↑ **87%**
Ransomware attacks against industrial organizations **increased 87 percent** over last year.

+35%
Dragos tracked **35% more ransomware groups** impacting ICS/OT in 2022.

72%
of all ransomware attacks targeted **437 manufacturing entities** in **104 unique manufacturing subsectors**.

20
Dragos tracked **20 ICS/OT Threat Groups** in 2022, with **two new groups** entering the scene

2,170
Dragos investigated **2170 vulnerabilities** in 2022, compared to just 703 in 2020

46%
The **number of CVEs investigated** has grown at an average annual rate of 46% over the last four years

50%
of Dragos services engagements **involved issues with network segmentation**

53%
External connections to OT dropped significantly from 70% to 53%.

54%
of Dragos services engagements included findings related to **shared credentials**

Defensible Architecture

A More Intelligent Approach

Defendable Architectures

Achieving Cyber Security by Designing for Intelligence Driven Defense®

Scott C. Fitch, Michael Muckin
Lockheed Martin Corporation

Abstract

Conventional approaches to security architecture focus on hardening systems against attack. The implicit expectation is that, once deployed, it is the system's responsibility to block all attacks against it. However, systems that rely strictly on hardening cannot learn from, or adapt themselves to, changes in attacker techniques, capabilities, and objectives over their lifecycle. Nor can they address the reality that attackers occasionally succeed. The ongoing efforts of sophisticated adversaries, including the Advanced Persistent Threat (APT), require systems that can be actively defended in an equally sophisticated manner. An intelligence-based model that builds an understanding of attackers from a variety of intelligence sources, including their interactions with the system itself, enables defenders to adapt to and anticipate changes in adversaries' attacks.

Defendable Architectures describe an alternative approach to system architecture by explicitly designing, implementing, and maintaining systems to support Intelligence Driven Defense® practices. The result is a virtuous cycle of greater visibility into systems to gather intelligence, faster translation of intelligence into defensive measures, and more effective deployment of those measures into the system's security controls. Moreover, threat intelligence can be leveraged when building systems to ensure their design is well adapted to current and emerging threats. This concept is also extended to the enterprise as a whole, describing how organizations can plan and deploy their systems and infrastructure with the Intelligence Driven Defense framework in mind.

Applying this approach, organizations can build systems that are resilient to cyber attacks,

"Defendable Architecture: Achieving Cyber Security by Designing for Intelligence Driven Defense®"
– Fitch & Mukin, Lockheed Martin Corp

Explicitly design, implement, & maintain systems to support intelligence driven defense processes

SANS

Whitepaper

The Five ICS Cybersecurity Critical Controls

Written by Robert M. Lee and Tim Conway
October 2022

Control #2 of SANS Five Critical Controls:

Architectures that supports visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement meets the definition.

Intelligence Driven Defensible Architecture

Threat
Scenarios

Operational
Constraints

Business
Constraints

Process
Understanding

Capabilities

— Implementing These Principles A small Utility

ACME - Small

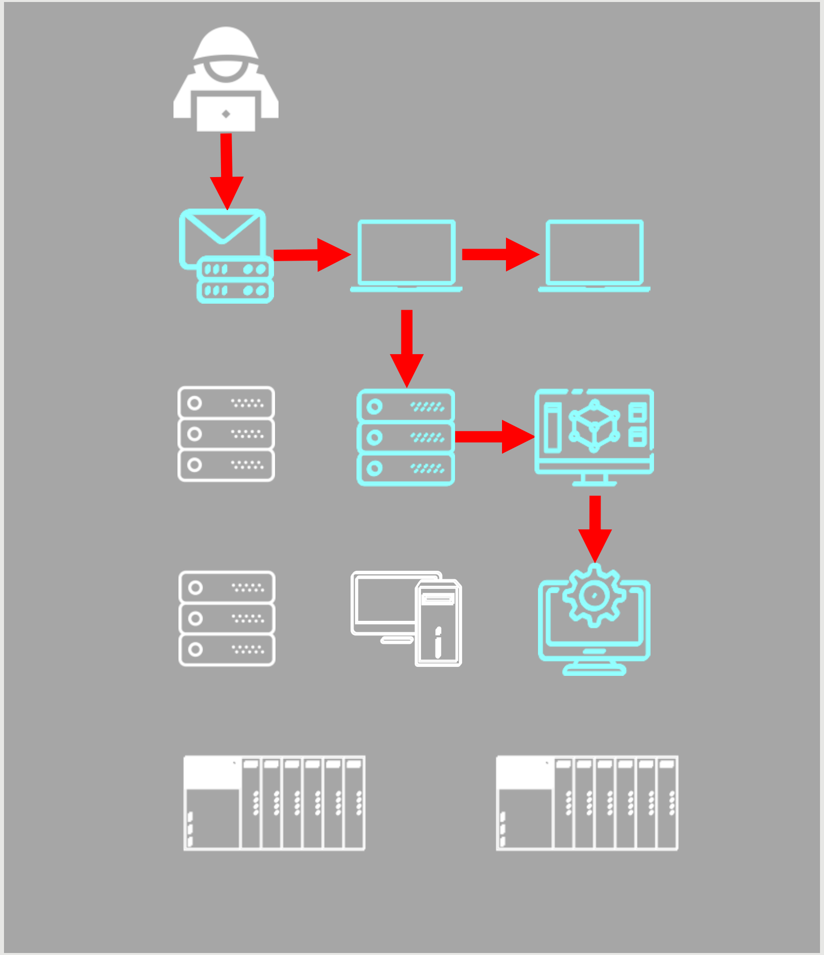
The Start of the Journey

- Sector: Utility
- Subsector: Water\Wastewater
- Employees: 76
- Customers: 6000
- Forecasted Growth: 150% YoY
- Infrastructure
    - 7 Wells
    - 2 Large Water Tanks
    - 4 Small Water Tanks
    - 1 Treatment Plant
    - 2 Lift Stations

- Technology Stack:
- Business Systems
    - O365
    - Cloud Customer Information System (CIS)
- OT Systems
    - Rockwell PLCs
    - Ignition Plant SCADA
    - Badger Meter System - Automatic meter reading (AMR)

ACME - Small
The Catalyst

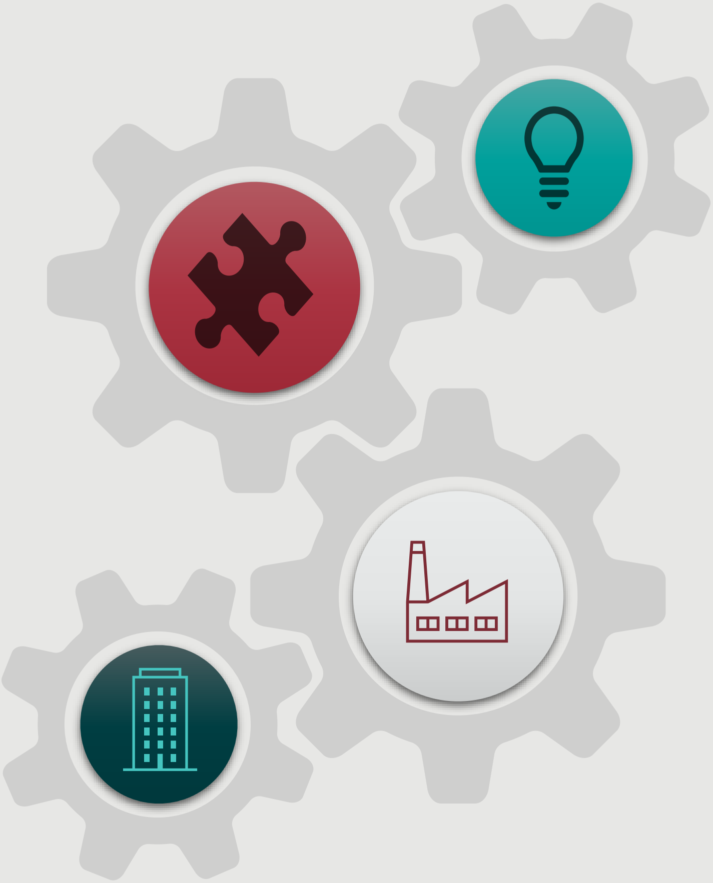
- A business user clicked a link on a phishing email which resulted in:
  - Downloaded Malware
  - Infected and encryption of ~20 computers
  - Impacted 2 operations systems
    - Meter System
    - Engineering Station



ACME - Small

Steps Taken

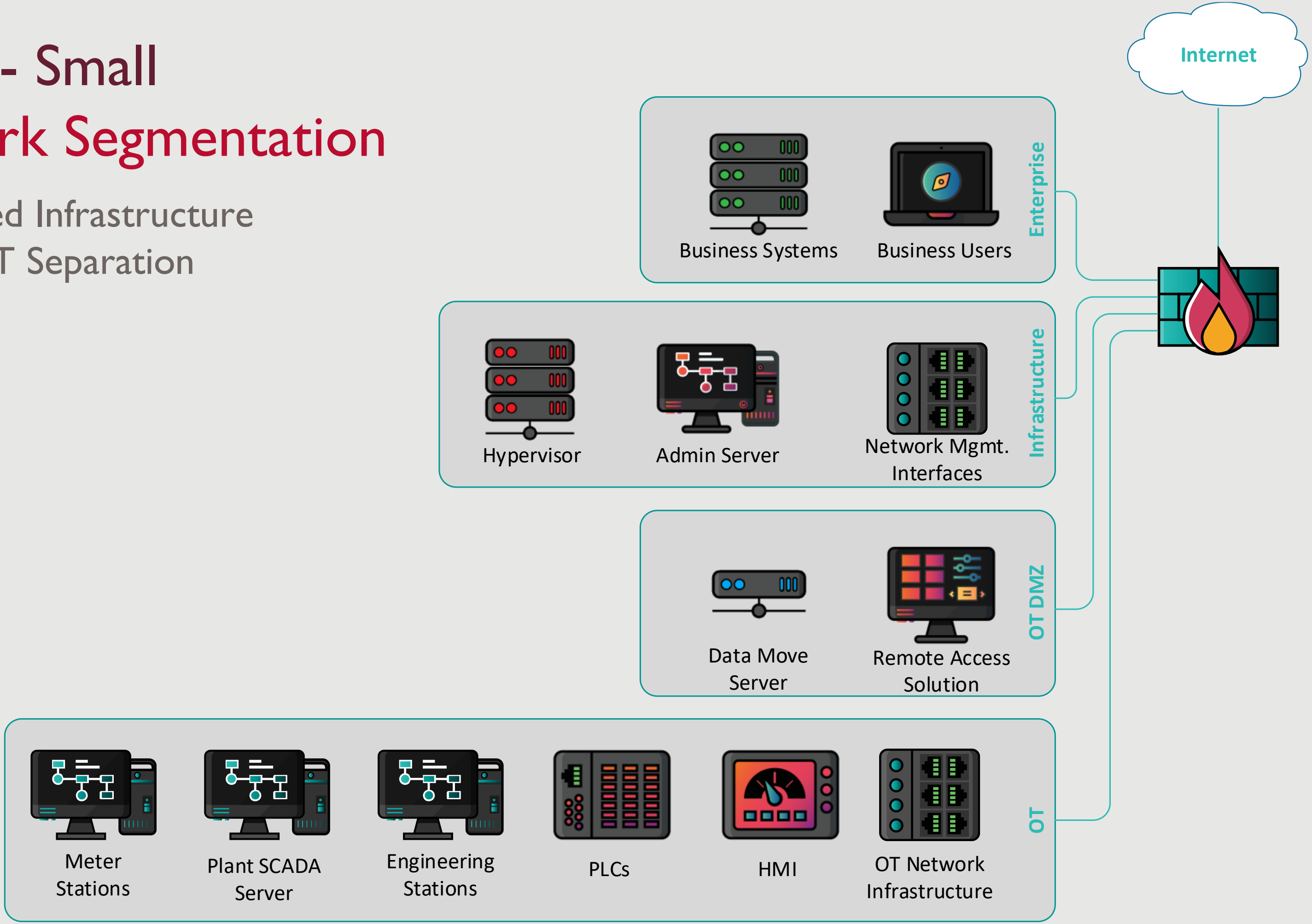
- Crown Jewels Analysis
  - Well 1 & Tank 1
  - Treatment Plant
- Threat Scenario Approach
  - Opportunistic Ransomware
- Identify Constraints
  - Limited Budget
  - Limited Staff
  - Infrequent Production Outages



ACME - Small

Network Segmentation

- Shared Infrastructure
- IT/OT Separation



ACME - Small

Security Controls

- System Hardening
    - Password Vault
    - Role Based Levels (Servers, Applications, PLCs)
        - Admin
        - Operator
        - Read Only
- FactoryTalk AssetCentre
    - Secure Project Files
    - Config Management
    - Config Backup

- MFA OT Remote and Admin
- Backup Solution for OT
    - Local NAS
    - Offline Removable Disk

ACME - Small

Making it Defensible

- **Intel Feeds**
  - WISAC
  - OT-Cert
- **Monitoring**
  - CMF
  - SIEM
  - Security Use Case
- **Workforce**
  - Training
  - OT/OPS
  - Cross Training
- **Playbooks**
  - IT/OT Disconnect
  - OT Restoration
  - Ransomware
- **Respond**
  - IR Tabletop Exercise
  - Test Restore

Implementing These Principles
A Medium Utility

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

ACME - Medium

The Mid Point in the Journey

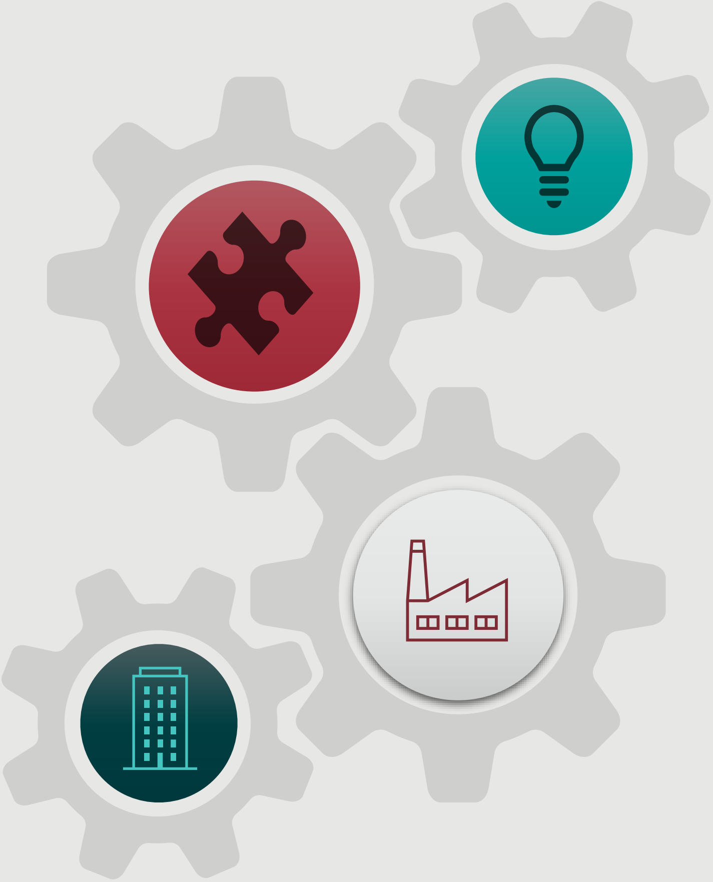
- Sector: Utility
- Subsector: Water\Wastewater & Electric
- Employees: 254
- Customers: ~9000
- Forecasted Growth: 25% YoY
- Infrastructure
    - 11 Wells\ 7 Tanks
    - 2 Treatment Plant
    - 3 Lift Stations
    - 4 Distribution Substations
    - 70 kV System
    - 12/21 kV System

- Technology Stack:
- Business Systems
    - O365
    - Cloud CIS\CRM\OMS
- OT Systems
    - Water SCADA
    - Electric DMS
    - Meter Systems
- Communication
    - Wireless
    - Fiber
    - Leased Cellular (Private APN)
    - Leased Line

ACME - Medium

Steps Taken

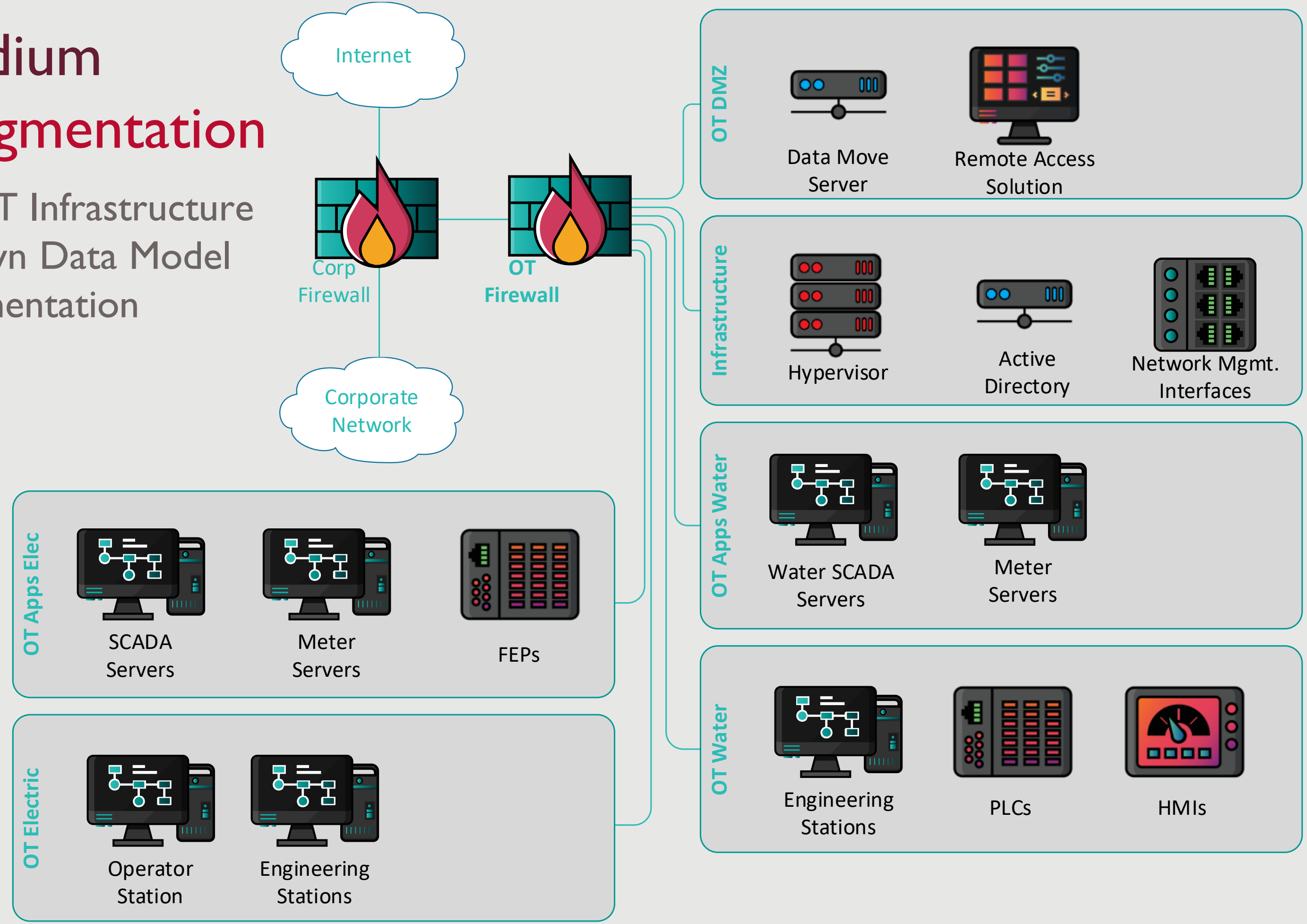
- Crown Jewels Analysis
  - Water SCADA
  - Electric SCADA
- Threat Scenario Approach
  - Opportunistic and Targeted Ransomware
  - Hacktivism
- Identify Constraints
  - Limited Budget
  - Limited Staff
  - Infrequent Production Outages



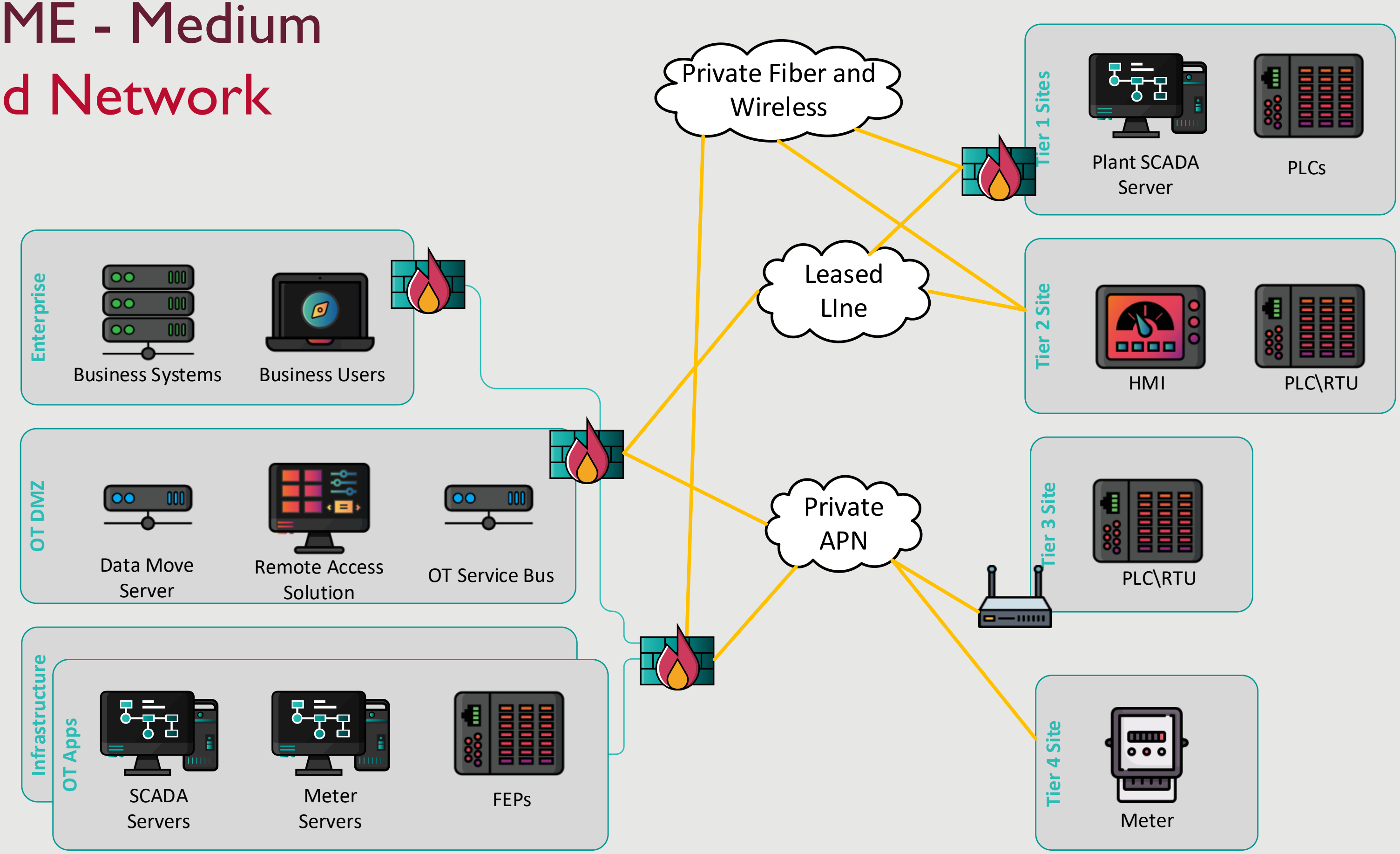
ACME - Medium

Network Segmentation

- Dedicated OT Infrastructure
- One Up\Down Data Model
- Internal Segmentation

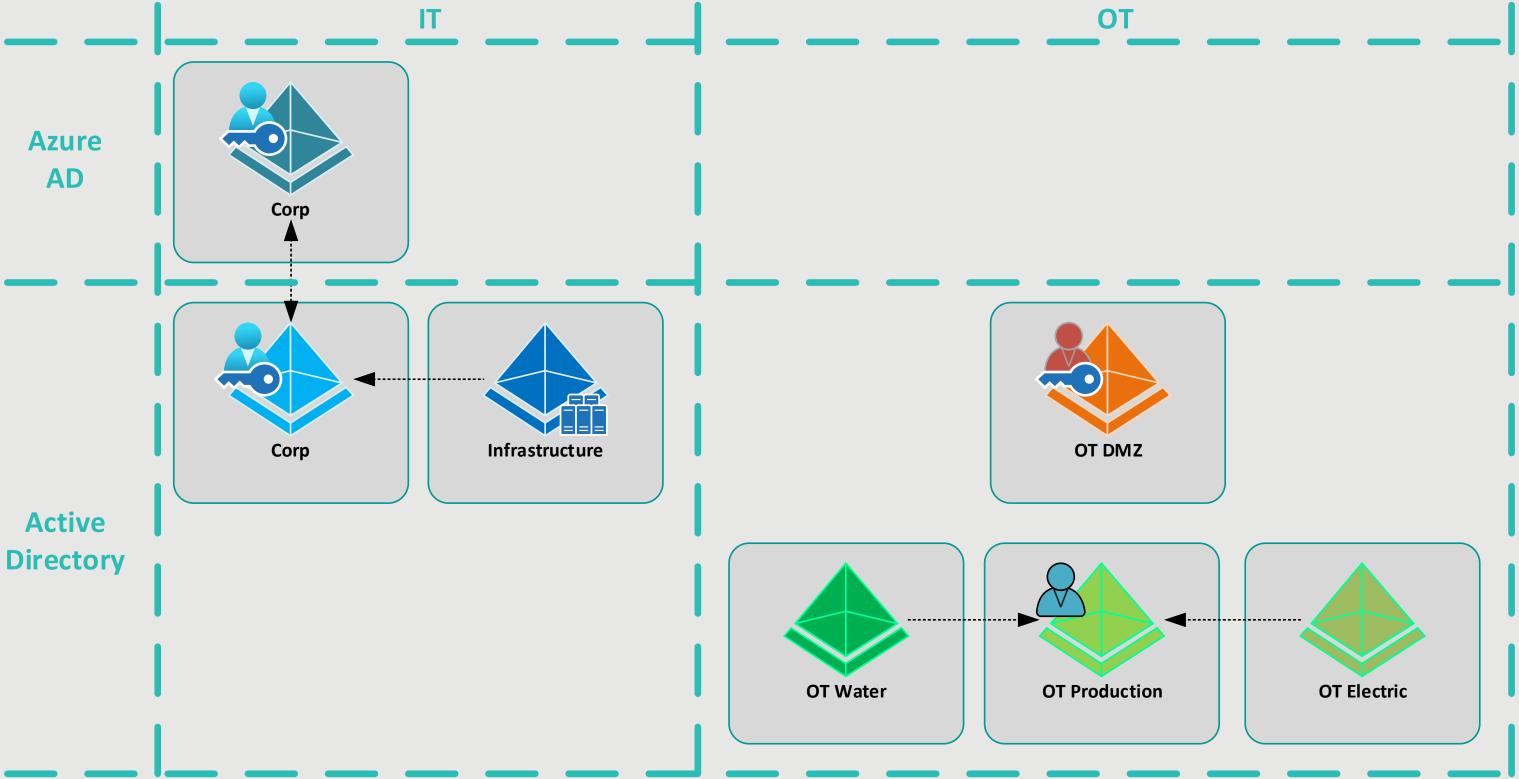


ACME - Medium Field Network



ACME - Medium

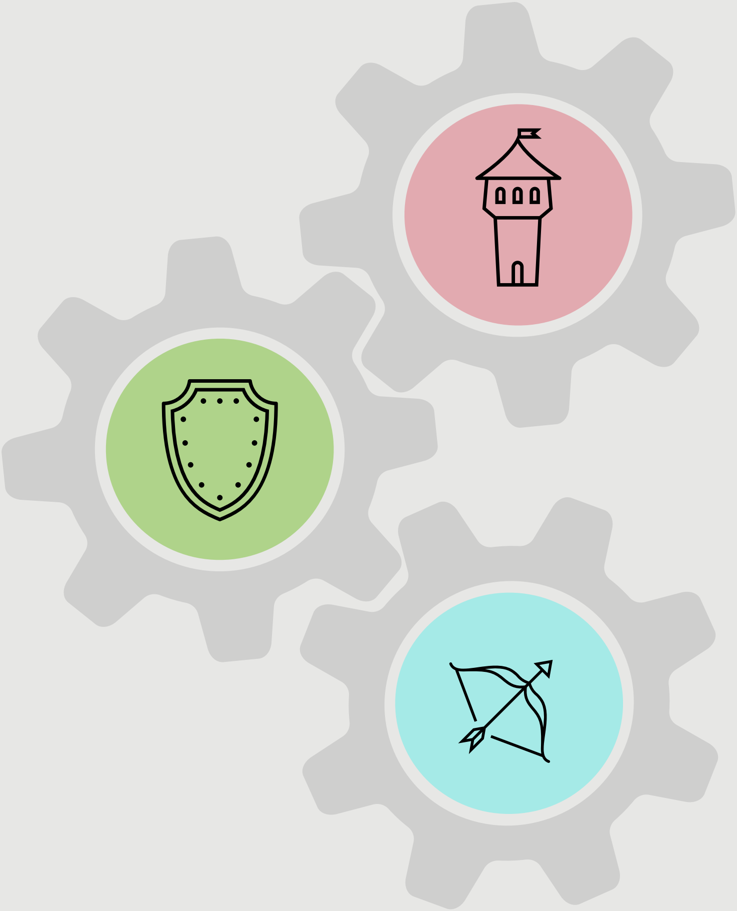
Identity Management



ACME - Medium

Security Controls

- System Hardening
  - Application Allowlisting
- EDR
- Privileged Access Management (PAM)
- Backup Solution for OT
  - Local\Site-to-Site Replication
  - Offline to Tape



ACME - Medium
Making it Defensible

- **Monitoring**
  - ICS Network Visibility
  - Hunts

- **Intel Feeds**
  - EISAC

- **Workforce**
  - SOC (MSSP)

- **Respond**
  - OT Tabletop Exercise
  - Site Recovery Drill

- **Playbooks**
  - Compromised Credentials
  - Compromised System
  - Forensic Triage

Implementing These Principles
A Large(ish) Utility

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

ACME - Large

The Last Part of the Journey

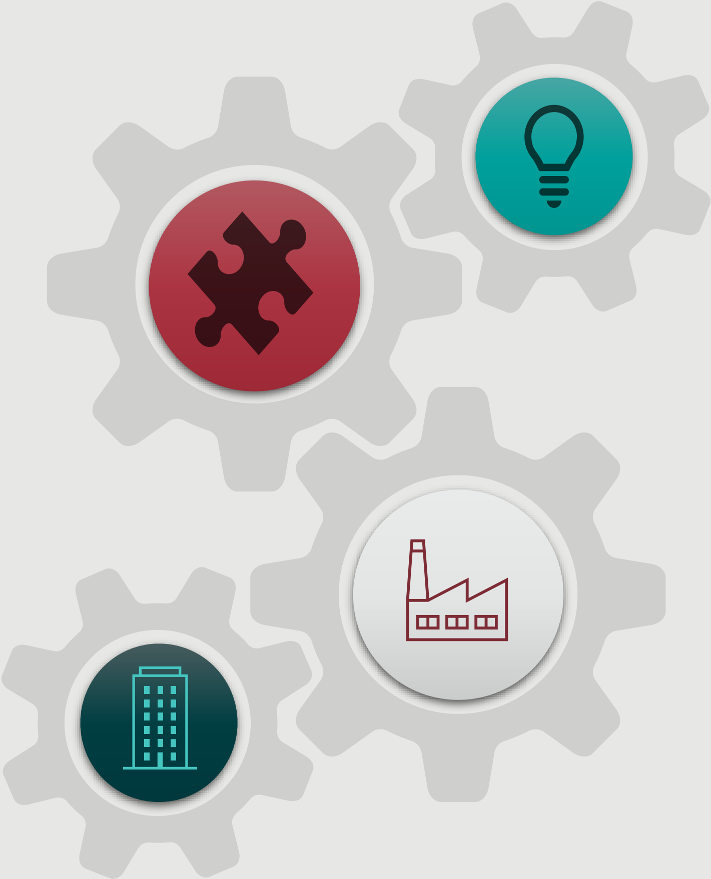
- Sector: Utility
- Subsector: Water\Wastewater & Electric & Generation
- Employees: 500
- Customers: ~27,000
- Forecasted Growth: 25% YoY
- Infrastructure
  - 11 Wells\ 7 Tanks
  - 2 Treatment Plant
  - 3 Lift Stations
  - 6 Distribution Substations
  - 40 MW Solar & Wind Farm
  - 20 MWh BESS
  - Distributed Solar\BESS

- Technology Stack:
- Business Systems
  - Cloud CIS\CRM
  - OMS
  - GIS
- OT Systems
  - Water SCADA
  - Electric ADMS
  - AMI Meter Systems
- Communication
  - Wireless
  - Fiber
  - Private Cellular
  - Leased MPLS

ACME - Large

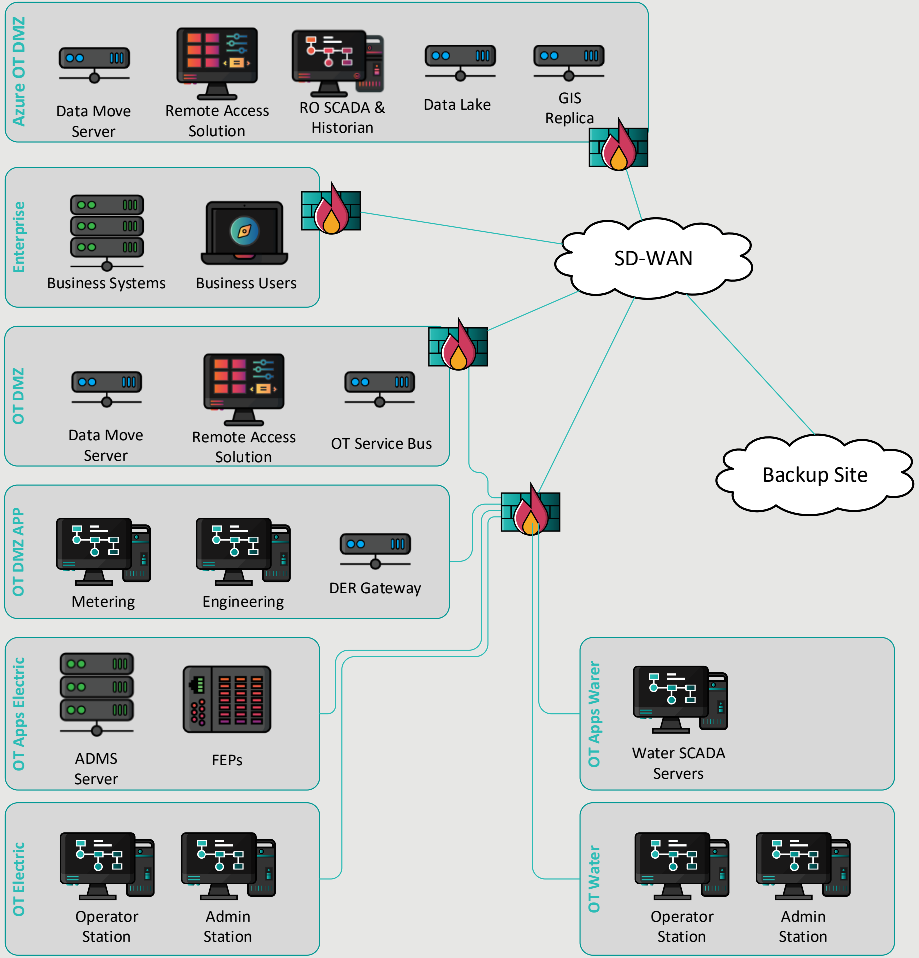
Steps Taken

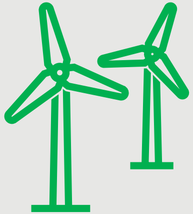
- Crown Jewels Analysis
  - ADMS
  - Water SCADA
- Threat Scenario Approach
  - Ransomware
  - APT
- Identify Constraints
  - Limited Budget
  - Limited Staff
  - Infrequent Production Outages
  - Regulatory Oversight



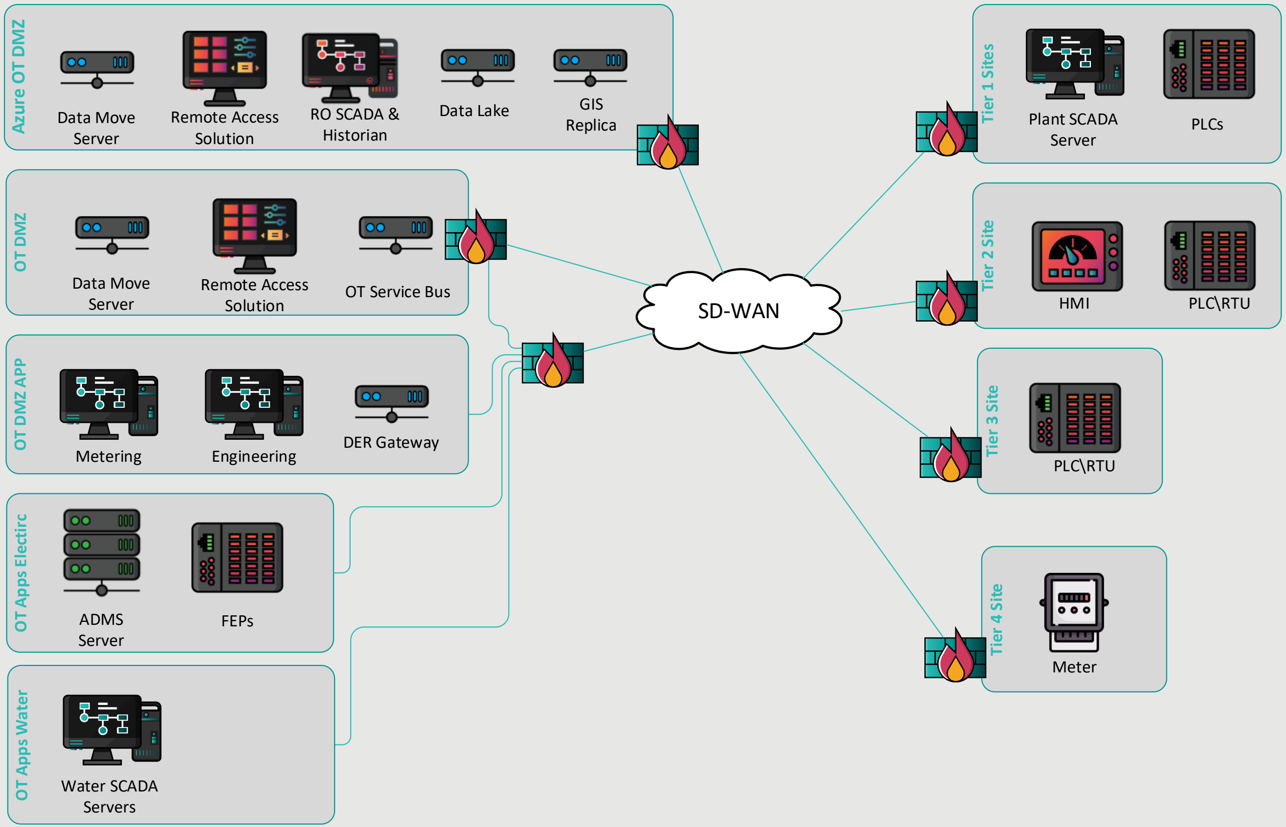
ACME - Large
Network Segmentation

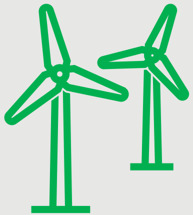
- Micro Segmentation
- Site Resilience
- Path Resilience





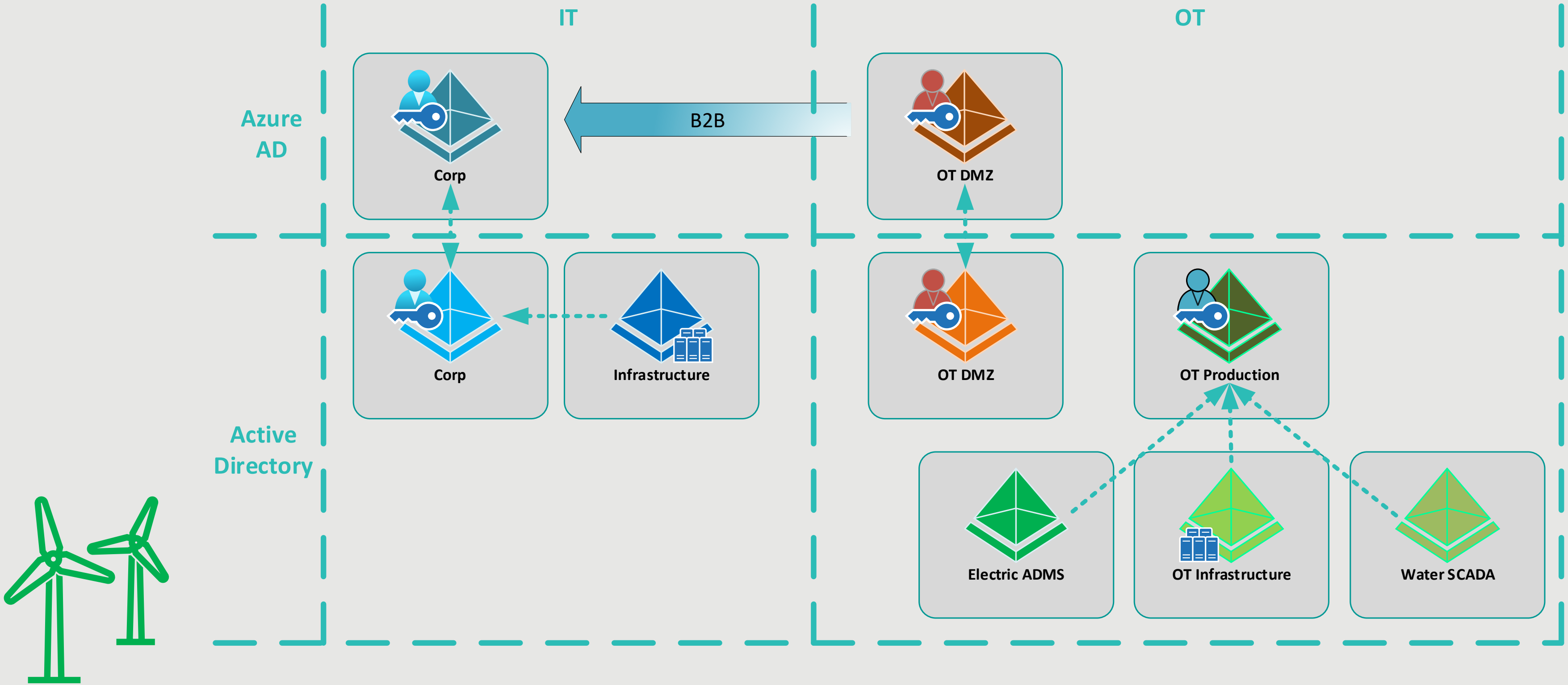
ACME - Large
Field Network





ACME - Large

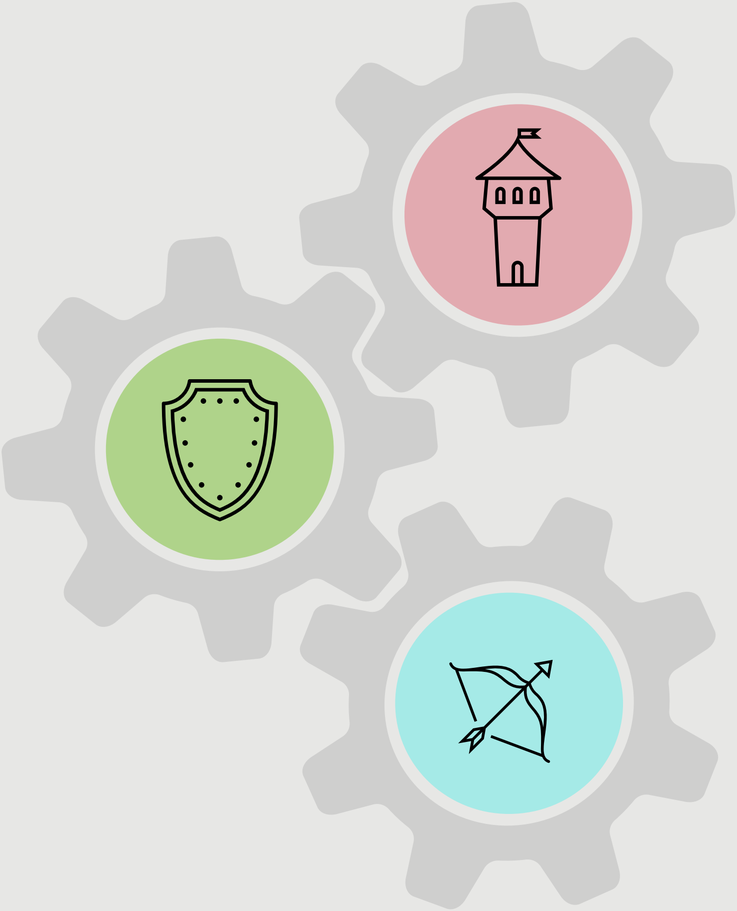
Identity Management



ACME - Large

Security Controls

- Asset Management
- Change Management
- Baseline Tracking
- Risk Based Vulnerability Management Program
- Port Security
- Hunt and Forensic Program
- Backup Solution for OT
  - Local\Cloud Replication
  - Immutable Cloud Storage
  - Standby Systems



ACME - Large

Making it Defensible

- **Intel Feeds**
  - Information Sharing Groups

- **Monitoring**
  - Expanded ICS Network Visibility
  - OT System Logging
  - ICS Device Logging

- **Workforce**
  - SOC IT/OT (L2+)
  - Responders

- **Playbooks**
  - Insider Threat
  - Defensible Cyber Stance

- **Respond**
  - Executive Tabletop Exercise
  - System Recovery Drill

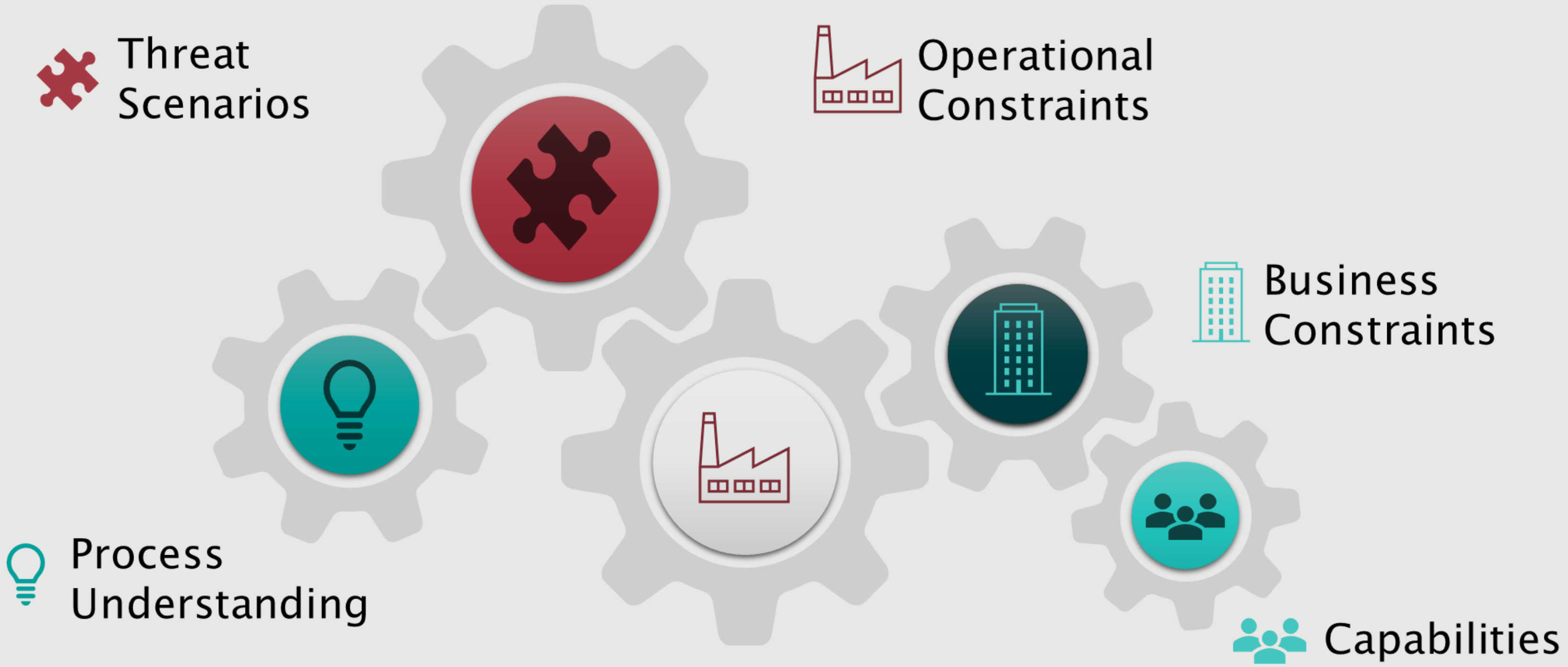
— Summary

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Defensible Architecture

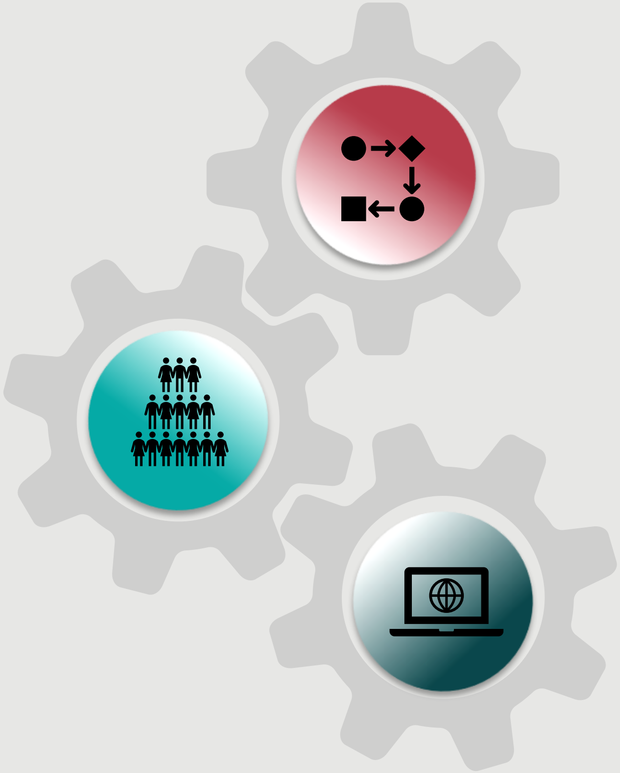
Summary



Intelligence Driven Defensible Architecture

Easy Right?

- Understand how operations and business functions
- Use an intel-driven design that fits the operation environment
- Deploy technology and processes that support the ability to detect and respond to events
- Develop resilience and response capabilities
- Enable and support defenders



Thank You

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association