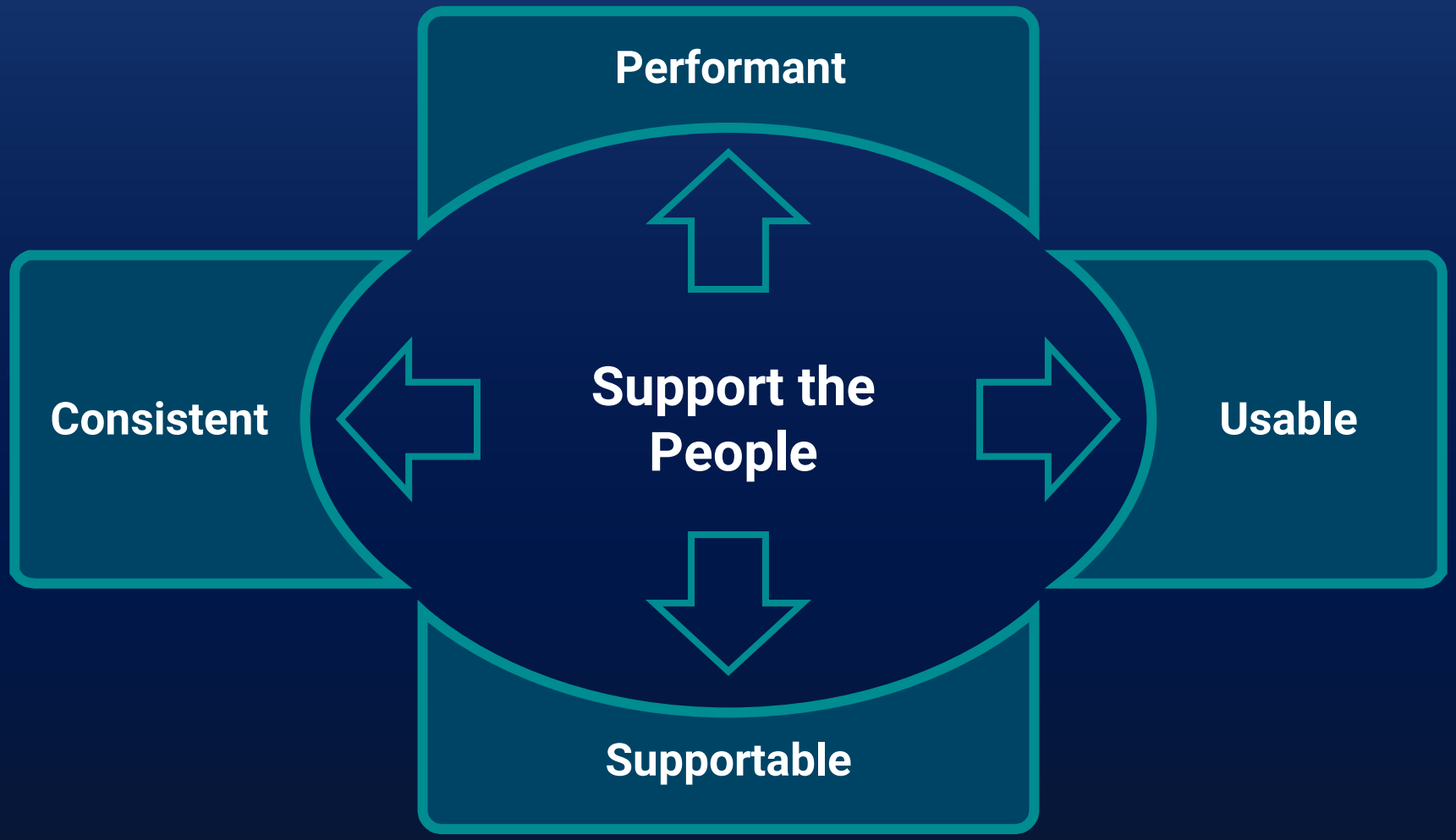
Securing Identities in Complex OT Environments

STEPHEN MATHEZER
CERTIFIED INSTRUCTOR,
SANS INSTITUTE

ICS Functional Objective



Things We'd Like to See

Minimize technical debt

- Don't overcomplicate

User Identities

- One identity, one password – used everywhere in OT
- Easy to provision
- Easy to troubleshoot

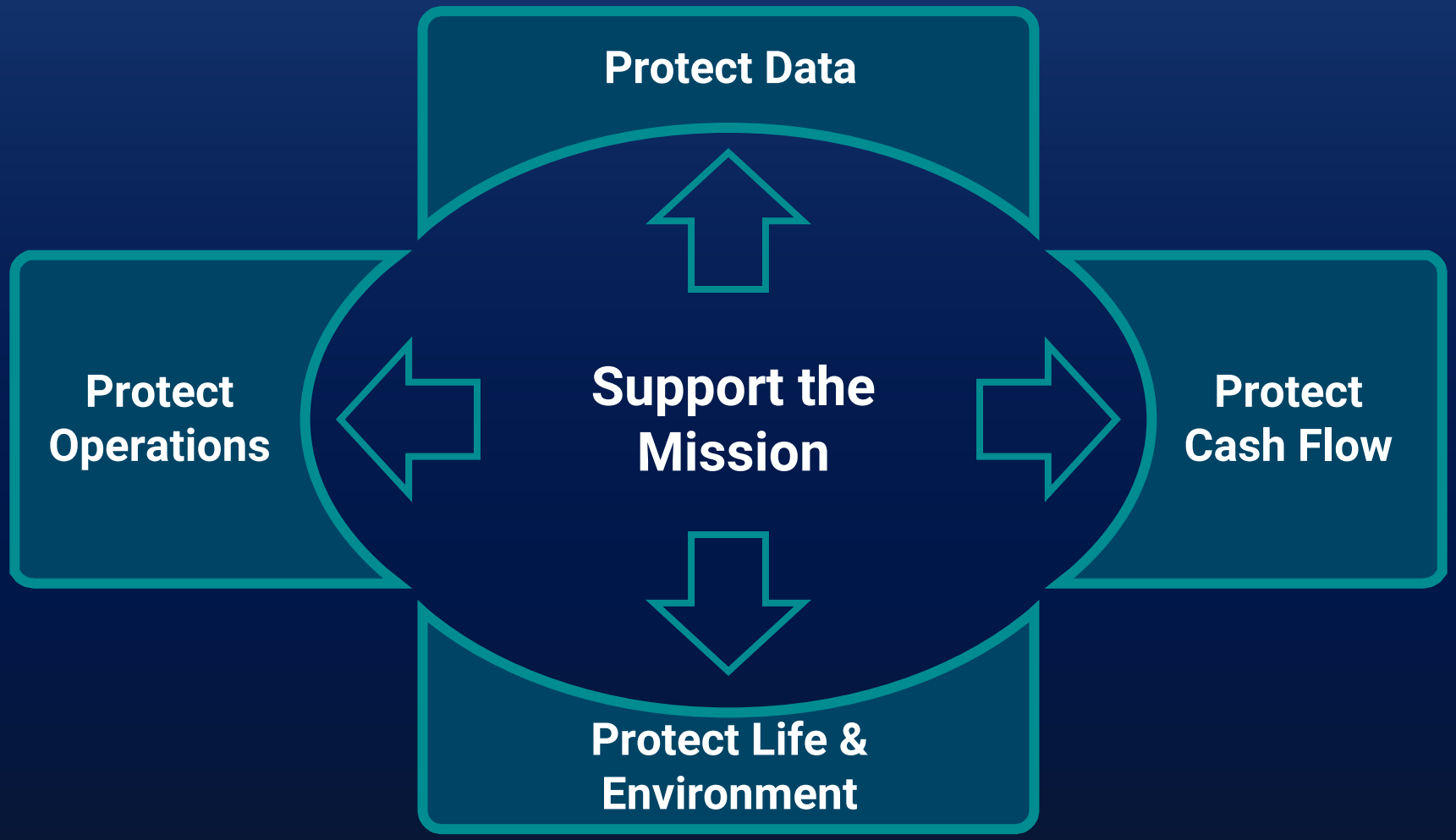
Consistent Processes

- Login
- Password reset
- Groups and permissions

Application Integration

- Common ground
- Single source of truth

ICS Cybersecurity Objective



Identity Related Exposures

SHARED & LOCAL ACCOUNTS

Passwords are known by all and don't change

Limited logging / auditing

REMOTE ACCESS

Publicly exposed attack surface

Heavily used by many users

UNCONTROLLED PERMISSIONS

Default or overly permissive access is easier to manage and becomes the norm

LACK OF STANDARDIZATION

Site-by-site approach to naming, structure, configuration, and control

SHARED/EXPOSED MANAGEMENT

OT systems managed from IT

IT credentials have elevated access

COMPROMISED ACCOUNTS

Long-lived credentials

Limited control over 3rd party / vendor practices

POOR HYGIENE

Limited centralized policy / configuration

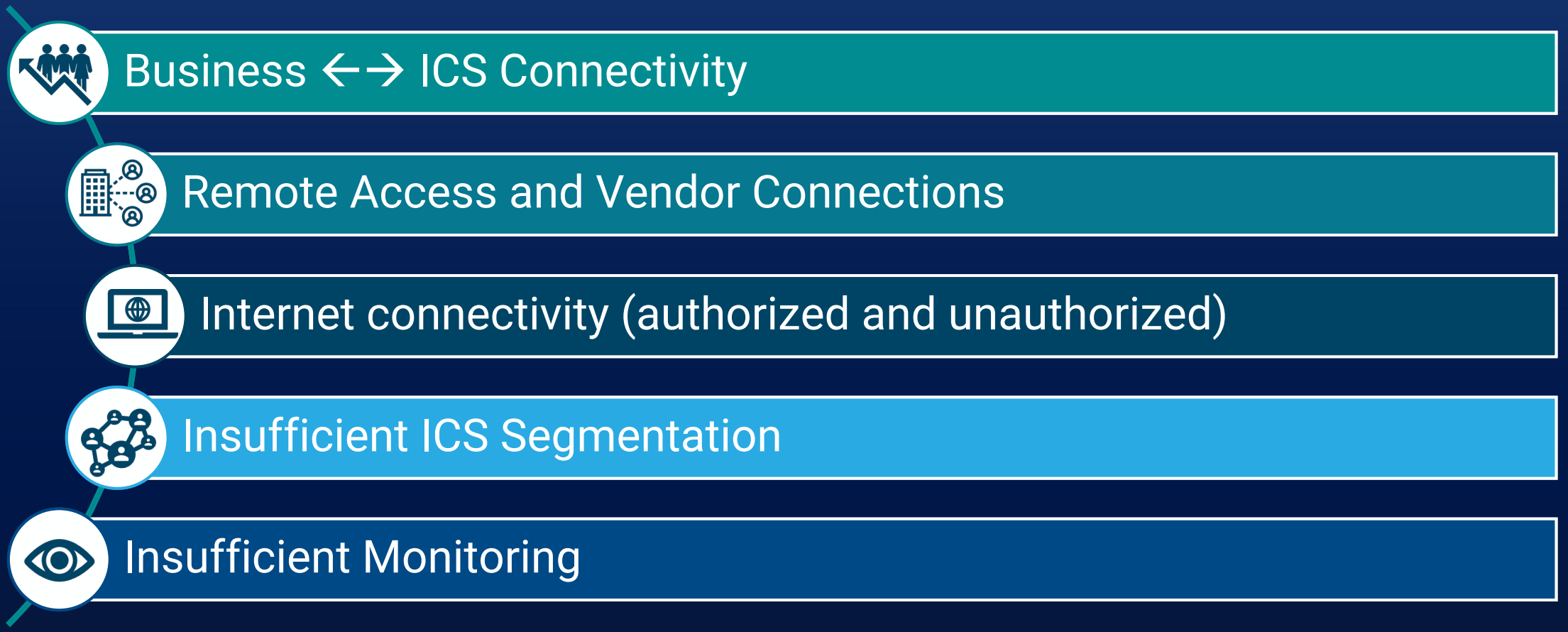
Informal onboarding / offboarding

PERMISSIVE DATA ACCESS

Open file shares

Static service accounts

Common ICS Security Exposures



Can “Zero Trust” Help?

- Many different approaches
- Often driven by capabilities rather than requirements or outcomes
- No shortage of guidance, everyone has an opinion
- But where can we start and what will work?

What Does Zero Trust Mean Anyways?

Firewall vendors	• Zero Trust Network Access (ZTNA)
Identity vendors	• People and identities are the single control point
AI	• Never trust, always verify • …importance of identity verification • …identity and integrity of users and devices

NIST 800-207 – Zero Trust Architecture

> …least privilege, per-request access decisions in the face of a network viewed as compromised

As I mentioned earlier, Zero Trust, or at least Zero Trust concepts have a part to play

- Zero Trust isn't necessarily the solution to all your problems, but is can be a useful guide
- Network segmentation – something we focus a lot on in ICS - is one part of Zero Trust (ZTNA)
- Identities are another critical point of control for Zero Trust

NIST 800-207 – Overview

Zero Trust Challenges for ICS

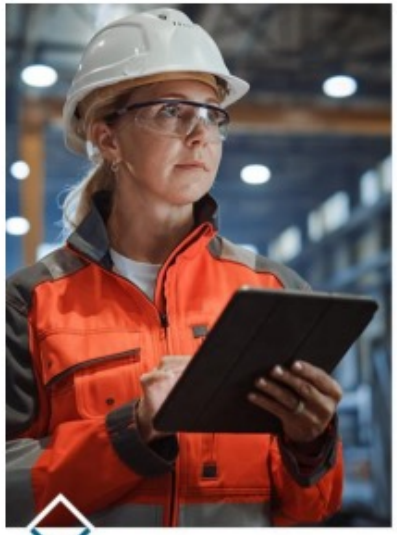
Technical Challenges

- Overall cybersecurity maturity is low
- Incomplete asset inventory
- Limited authentication / identity management

Organizational Challenges

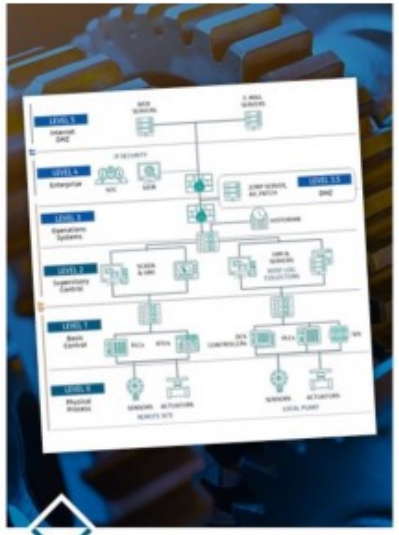
- Limited appetite and opportunity for change
-  We've been operating for X years and nothing bad has happened
- Every site is unique

5 ICS Cybersecurity Critical Controls: Identity is part of all of them



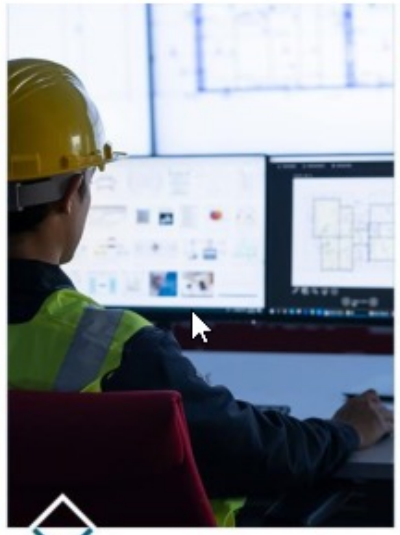
ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.



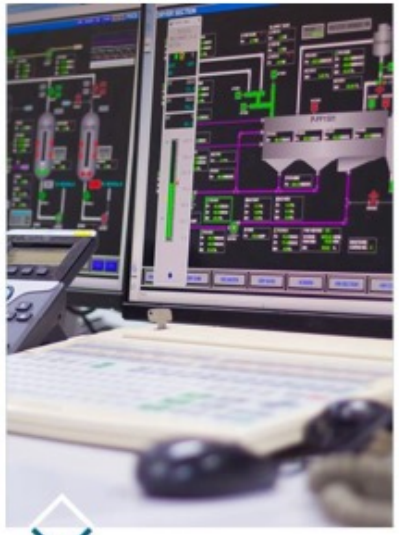
DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, Industrial DMZ's, process communication enforcement.



ICS NETWORK VISIBILITY AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.



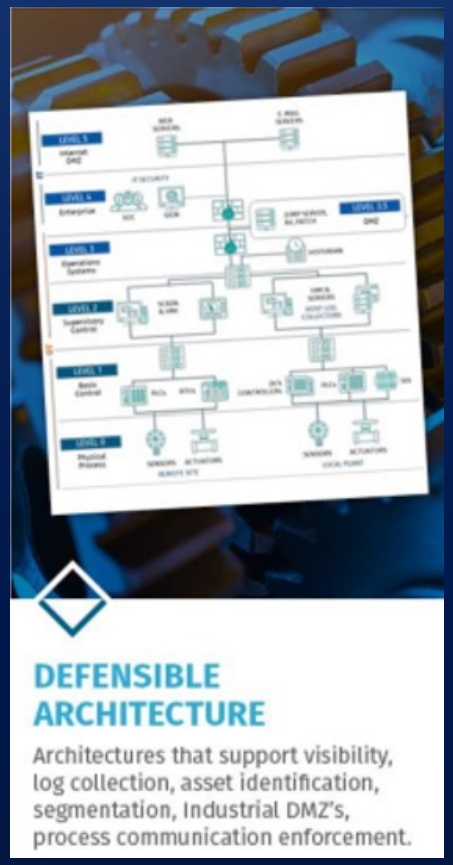
SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

Moving ICS Towards ZT – Easy Steps

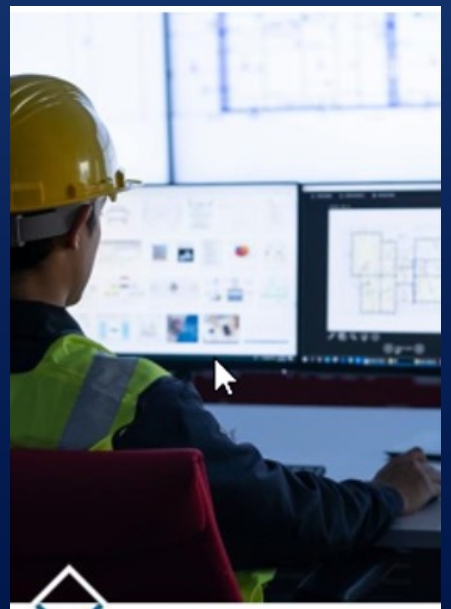


Control of communications at Internet/IT/OT boundary

Network segmentation from DMZ down to Level 0/1/2

Establish “choke points” for network monitoring

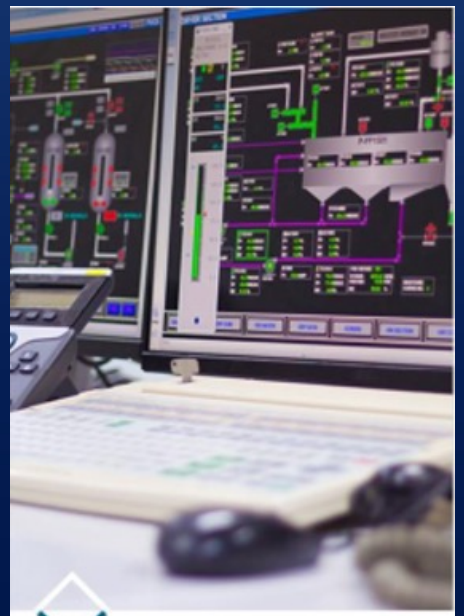
Moving ICS Towards TZ – Moderate Difficulty



ICS NETWORK VISIBILITY AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.

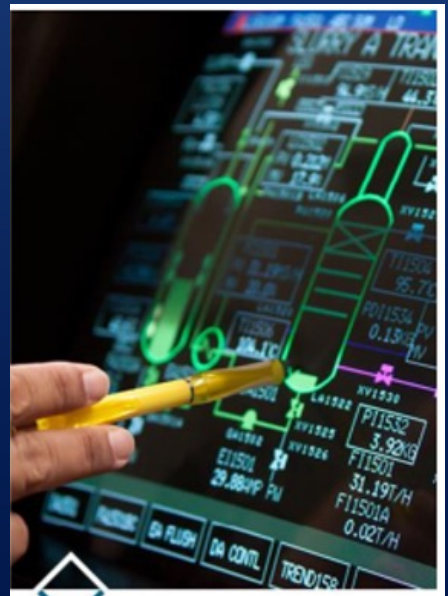
- Authentication and authorization of remote users
- Secure file transfer
- Improved visibility and asset inventory



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

Moving ICS Towards ZT – Harder Steps



RISK BASED VULNERABILITY MANAGEMENT

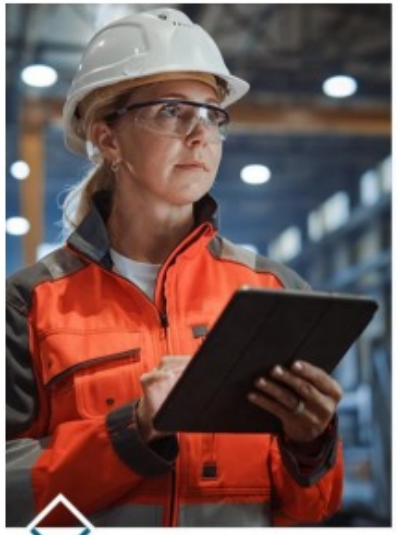
Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

- Vulnerability management and patching
- Continuous authentication and authorization of devices
- Active defense

ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.

5 ICS Cybersecurity Critical Controls: Incident Response



ICS INCIDENT RESPONSE

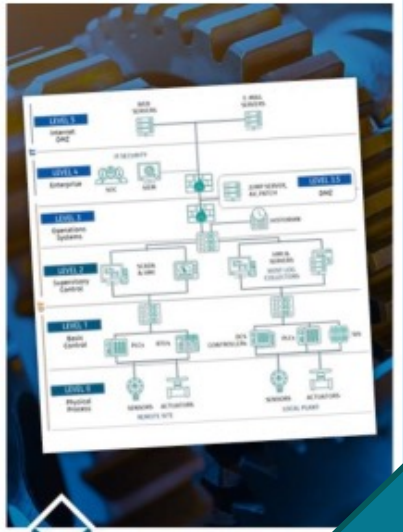
Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.

- Identification
  - Which identities are involved?
  - What are they doing?
- Containment
  - Disable and monitor
- Eradication
  - Reset passwords
  - Disable or delete
- Recovery
  - Re-provision

5 ICS Cybersecurity Critical Controls: Defensible Architecture

ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.



DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, Industrial DMZ's, process communication enforcement.

- Which identities are used where?
- What is the scope for identities?
- How are they share across sites in a controlled way?
- Which identities / directories are accessible where?
- How are directory services provided?

ICS N… AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.

…ACCESS

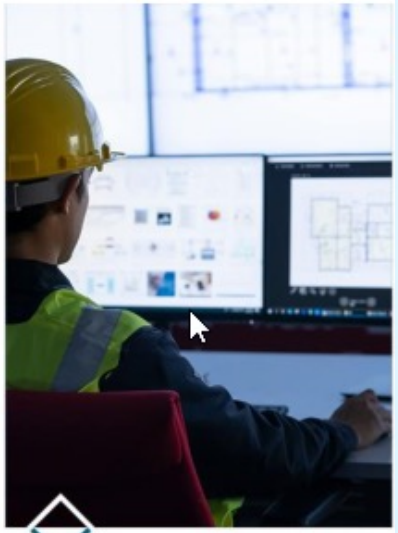
Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

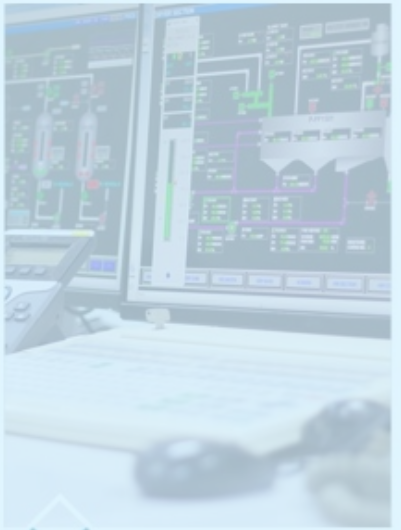
5 ICS Cybersecurity Critical Controls: Network Visibility and Monitoring

- All data sources are resources
- Collect information about assets, infrastructure, communication
- Integrity and security is managed for all assets



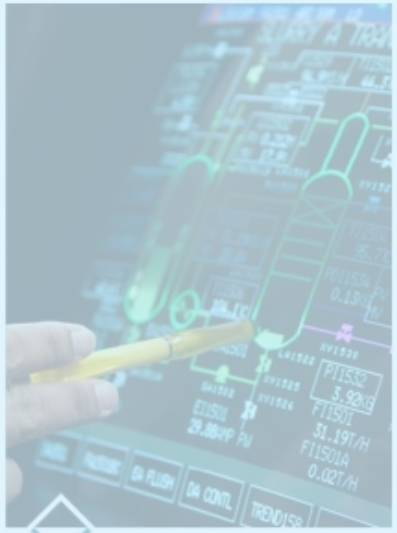
ICS NETWORK VISIBILITY AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

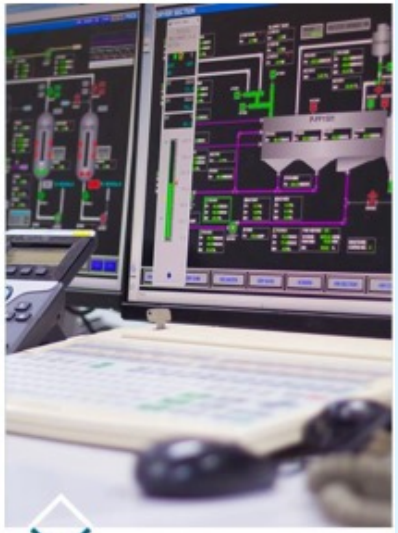


RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

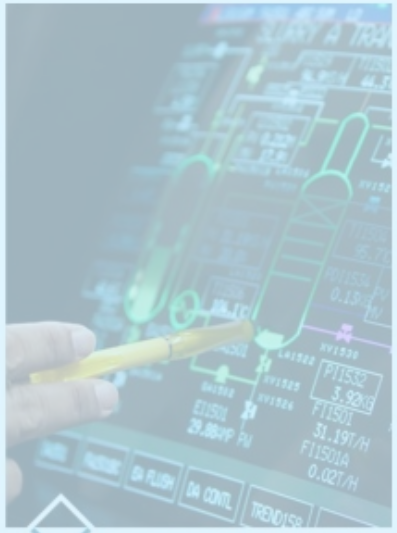
5 ICS Cybersecurity Critical Controls: Secure Remote Access

- Each remote access user is an identity.
- Authentication for remote access.
- File sharing permissions.
- Role based application and network access control.



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.



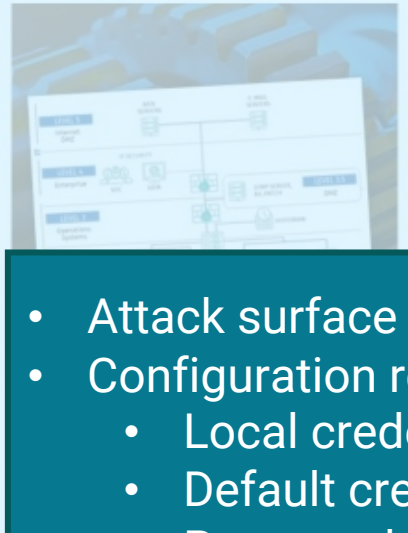
RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

5 ICS Cybersecurity Critical Controls: Vulnerability Management

ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.



process communication enforcement.

system of systems interaction analysis capabilities used to inform operations of potential risks to control.

ification and inventory of all te access points and allowed nation environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

- Attack surface management
- Configuration related to identity:
  - Local credentials
  - Default credentials
  - Password policy
  - Account lockout

RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

STANDARDS and COMPLIANCE

IEC-62443

5.3.1	…provide the capability to identify and authenticate all human users… on all interfaces which provide human user access… support segregation of duties and least privilege
5.4.1	…provide the capability to identify and authenticate all software processes and devices… on all interfaces which provide access to the control system… to support least privilege.
5.5.1	…provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

IEC-62443

6.1	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges
6.3.1	…provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege
6.10.1	…provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events.

THE OT IDENTITY LANDSCAPE

OT Identities (to name a few)

People Roles

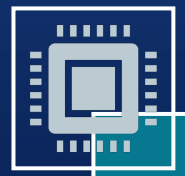
- Engineer
- Operator
- Technician
- Admin
- 3rd Party

Login Targets

- OS
- Remote Access
- Cloud
- Network
- Application
- Device

Application

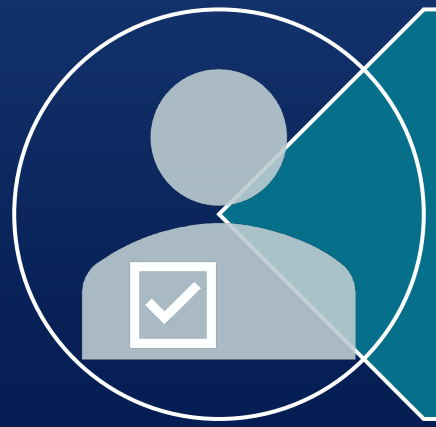
- User
- Admin
- Service
- Database
- API



Devices

- Firmware Signing
- Network Join
- Network Control
- Device Admin

Identity Security and Validation



Identity Validation

Checking credentials to make sure that people/things are who they say they are

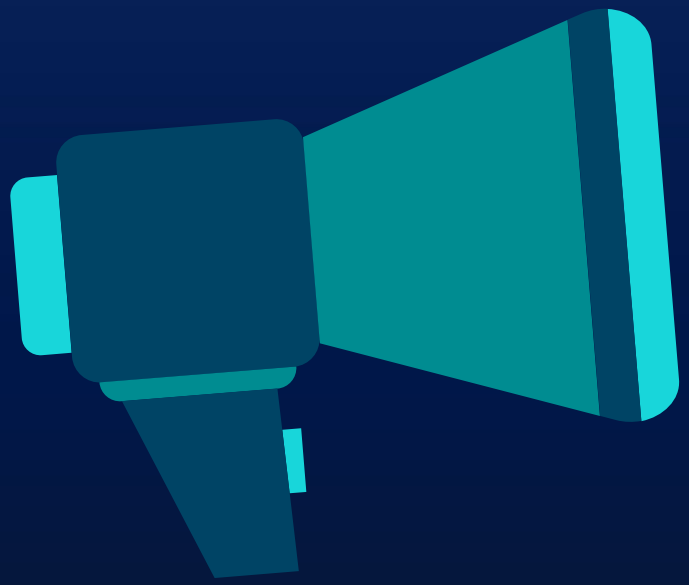
Identity Security

- Protecting the credentials themselves
- Protecting identity systems and stores
- Strong authentication mechanisms

RECOMMENDATIONS

Protect the OT Environment from IT

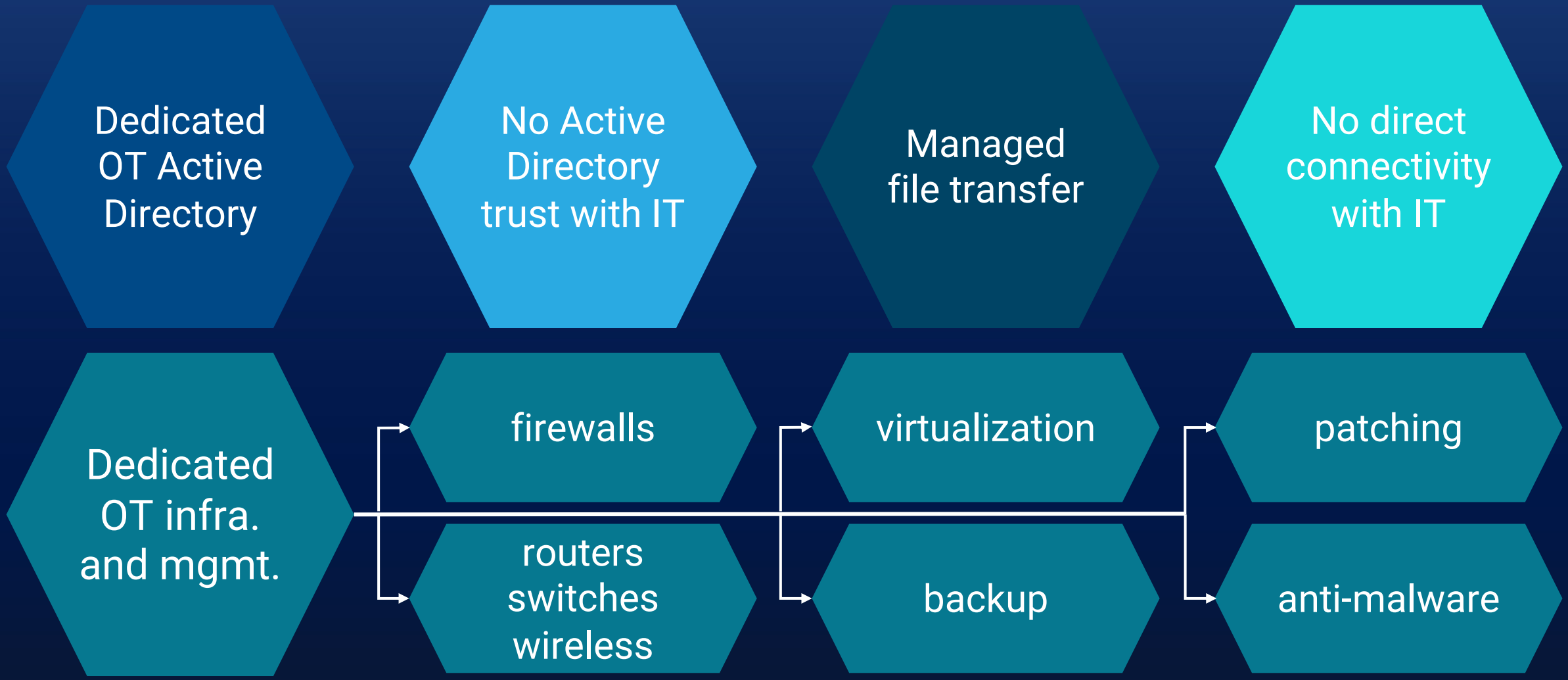
IT is to OT what the Internet is to IT



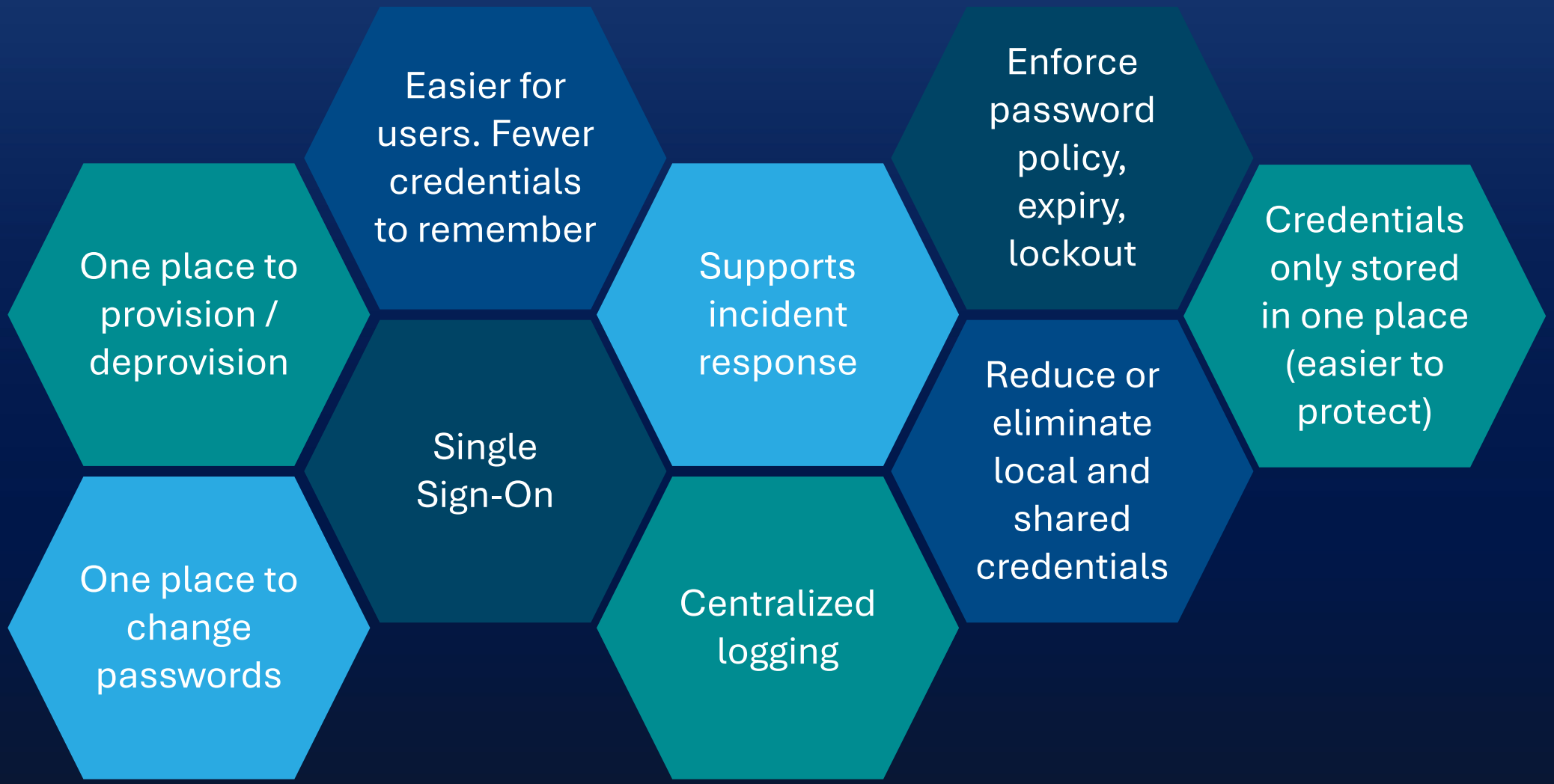
A COMPLETE IT COMPROMISE MUST NOT AFFECT OT!

Network segmentation is a strong first step
We also need to segment identities and accounts

Harden Against IT Compromise



Centralize OT Identity (Active Directory)

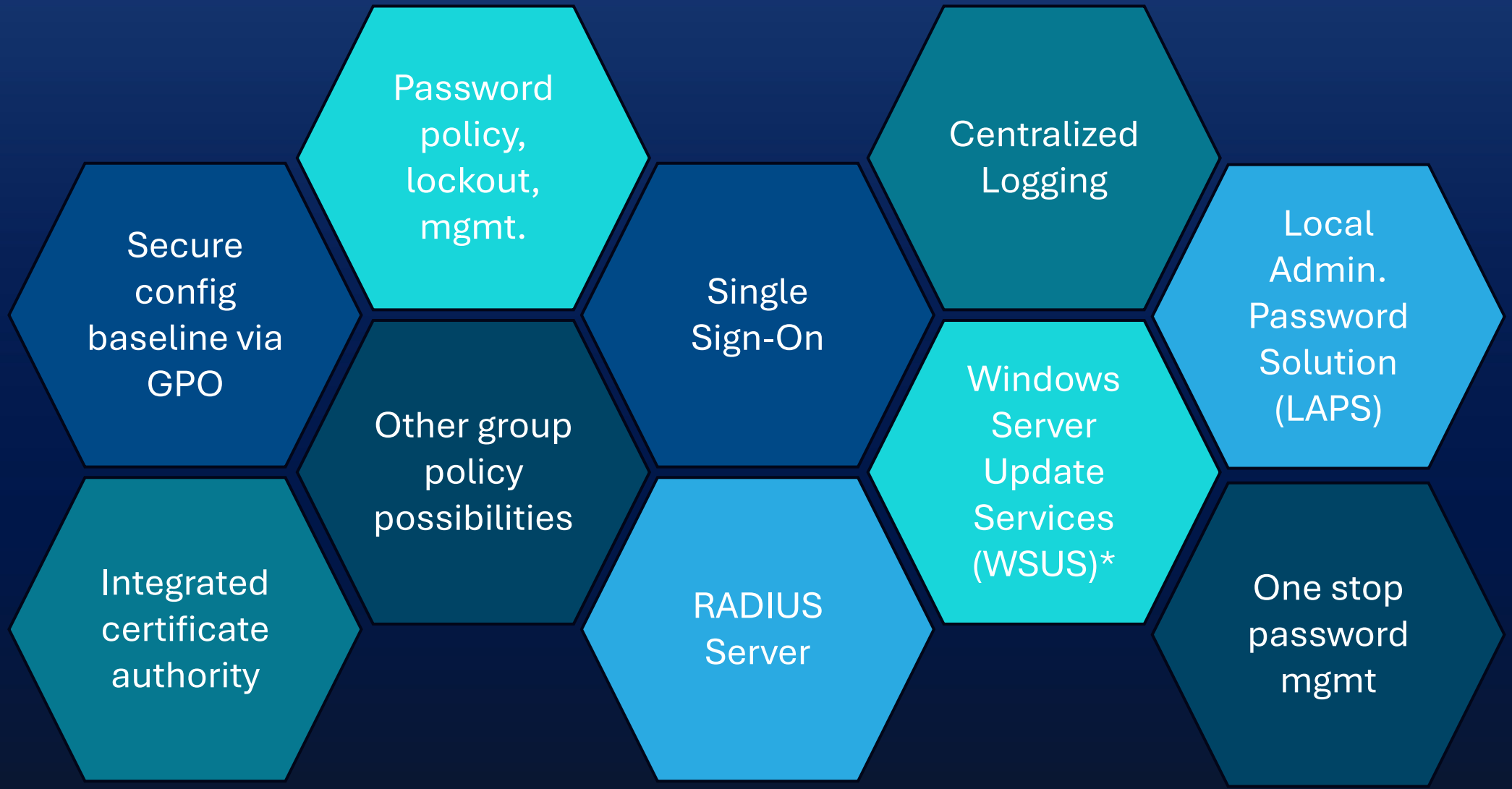


Active Directory for OT

- Supports remote access, file shares, etc
- Broad third-party and application support
- Familiar – plenty of available expertise
- Already licensed
- Patching capabilities
- Most environments are running a lot of Windows anyways
- More and more advanced identity security features

KEEP IT COMPLETELY INDEPENDENT OF IT AD!

Active Directory Security Benefits



OT Active Directory Risks and Challenges

OBVIOUS TARGET

First thing targeted by attackers

Easy to find / identify

REQUIRES CONSTANT CARE

Must be well managed

Cannot just set and forget

HARD TO SEGMENT

Requires communication across sites

Islanding must be planned and practiced

MUST BE RESILIENT

High availability is a must

Valid logins can never fail

WELL UNDERSTOOD

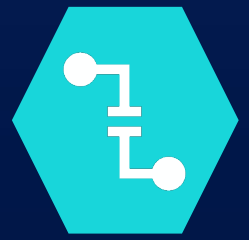
Familiar to attackers

Lots of tradecraft and exploits

COMPROMISE AFFECTS EVERYTHING

Long-lived credentials

Limited control over 3rd party / vendor practices

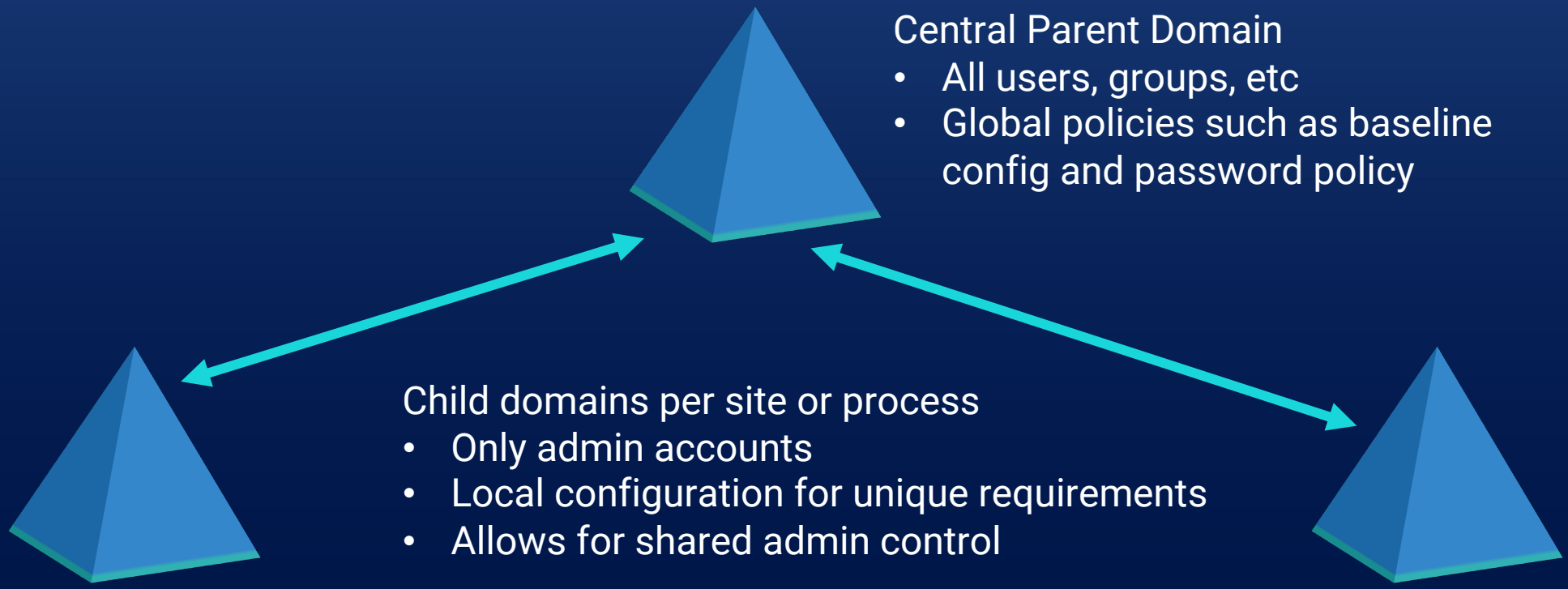


VENDOR INTEGRATION

Vendors have own Active Directory

May be reluctant to connect

Active Directory for OT - Tips



Central Parent Domain
- All users, groups, etc
- Global policies such as baseline config and password policy

Child domains per site or process
- Only admin accounts
- Local configuration for unique requirements
- Allows for shared admin control

- Keep it up to date – little risk in patching aggressively
- Build for resiliency
- Get an experienced administrator

REMOTE ACCESS

Remote Access Key Components

Must Have

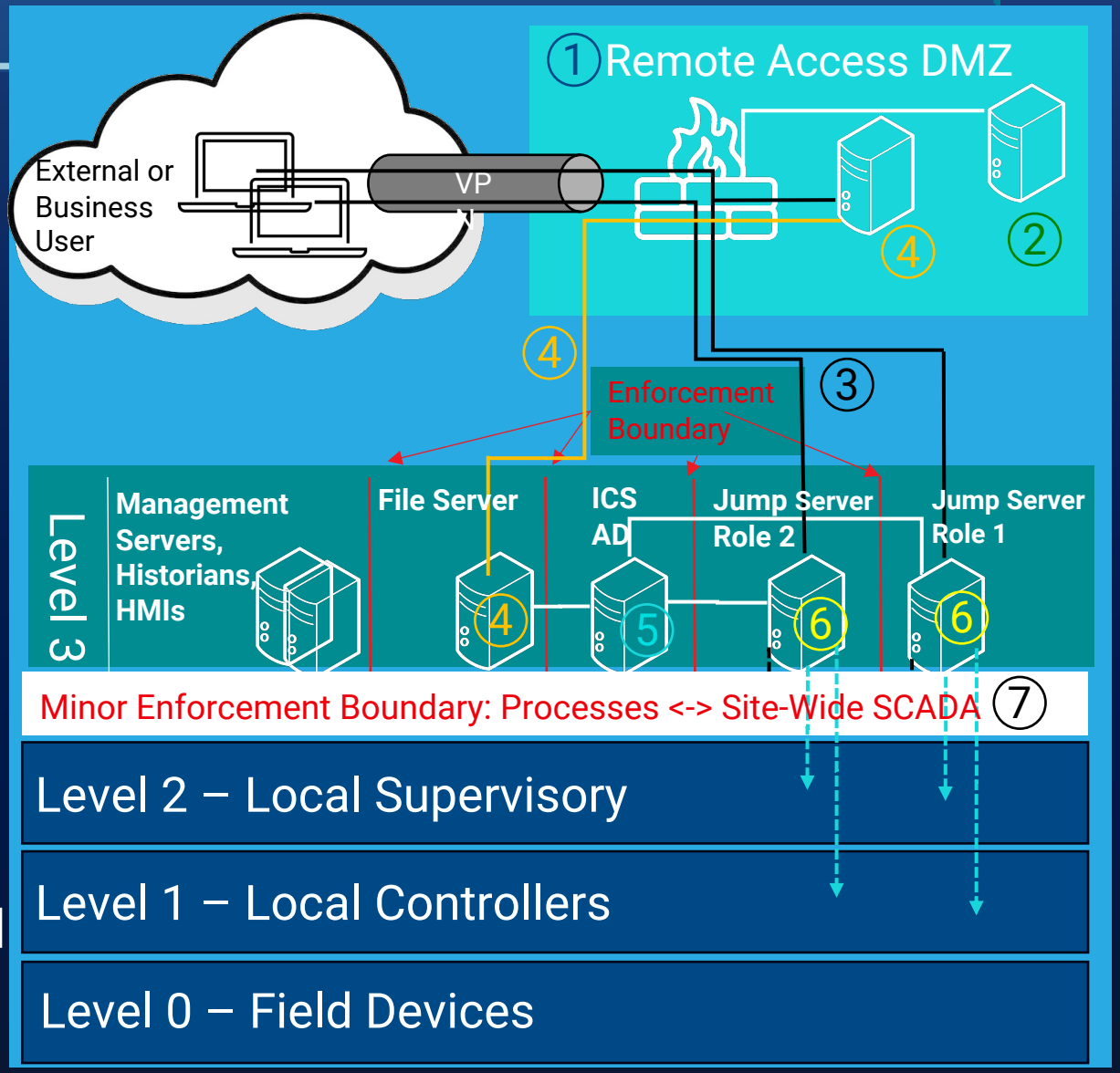
- Distinct credentials
- Multi-factor authentication
- File transfer mechanism
- “Zero Trust” access limited by user/group
- Detailed auditing

Nice to Have

- Credential vaulting
- Session recording
- Session sharing
- Approval workflow

Remote Access Architecture

1. All remote access terminates in the DMZ
2. Dedicated ICS authentication + MFA
3. Remote access only to jump and file servers
4. Files are scanned and sync'd to Level 3
5. Jump servers authenticate against ICS AD
6. Jump servers grant access to specific applications based on user roles
7. Jump server network access further controlled at enforcement boundaries



PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) Uses

- Website certificates
- Network access/authentication, especially wireless
- WAN / VPN security
- Windows Firewall Connection Security
- OT protocol security
- Code and firmware signing and encryption
- Offline authentication

Public Key Infrastructure Tips

Don't be afraid of it

Maintain it well

Test for supportability

Get good administrators

Push for vendor support

Also look at wireless

Start with webservers

Use Active Directory

Keep it simple

DEVICE IDENTITY

Device Identity and Authentication

- Device authentication usually means:
  - Network-level controls by device or
  - Device / application authentication
- Network-level control requires a means to identify devices at a minimum
  - Can be as simple as IP address
  - Various other means to identify through scanning or observation of traffic
- Authentication requires some sort of credential, usually a certificate

Certificate Based Authentication

- Hard to accomplish and manage comprehensively
  - Older / legacy devices
  - Lack of vendor support
  - Sheer volume of devices impossible to manage one by one
- PKI is a must
- Vendor support is needed for
  - Certificate deployment and management
  - Enforcement of firmware signing / validation
- Multi-vendor environments tend to revert to the baseline

Some Commercial Products

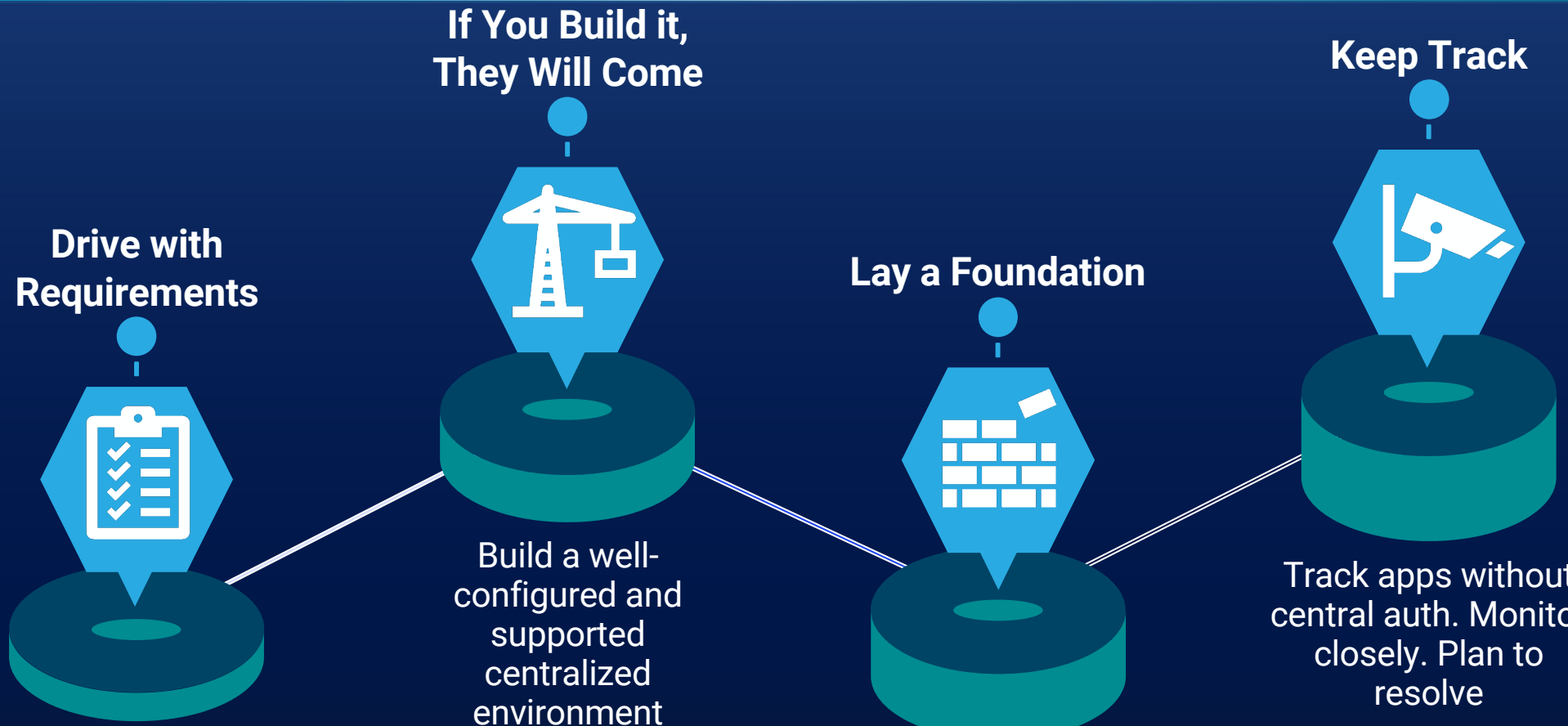
- Usually requires an in-line enforcement point that looks a lot like a transparent firewall
- Outage necessary to install
- Risk of interrupting operations if installed at lower levels
- General recommendations:
  - Install in well understood, static environments
  - Keep policy simple
  - Install at locations where you are comfortable islanding

APPLICATION IDENTITY

Application Authentication & Authorization

- Applications are often an Achilles heel for identity
- Tendency to provision local users
  - Weak or non-existent password policy
  - Default & shared credentials
  - Limited logging
  - Rarely get deprovisioned
- Complex application-specific authentication and authorization
- Uneven support for centralized authentication
- Credentials are often stored (insecurely)
- Long-lasting logins

How to Get Started



FactoryTalk

by ROCKWELL AUTOMATION

CASE STUDY

Rockwell Automation FactoryTalk

Suite of software applications including directory, HMI, MES, communications platform, data analytics and more

May all be installed on a single computer with a single PLC

Can also be distributed across a network sharing a common directory

FactoryTalk Directory provides a central lookup service for tags, applications, servers, displays, etc

We will focus on users, groups, computers, and access control

FactoryTalk Network Directory

- Completely independent of local directories (out of scope today)
- Granular permissions controlling *actions* that can be taken by *users* on *computers* against *resources*
- Controls can also be applied to groups of users or computers
- Structure is well thought-out, but demonstrates the complexity we must consider

FactoryTalk Network Directory

- FactoryTalk users
- FactoryTalk computers
- FactoryTalk groups (users or computers)
- Windows-linked user accounts
- Windows-linked groups
- Resources and actions exist only in the FactoryTalk Directory

FactoryTalk Users

- Can still be centrally administered within FactoryTalk
- Useful when Windows domain connectivity is unreliable
- Necessary when you can’t manage Active Directory users
- Enable individual access controls when a shared account is used to log into Windows and/or the computer is always logged in

FactoryTalk Groups

- Can contain
  - FactoryTalk Users
  - Windows-linked Users
  - Windows-linked Groups
- Permissions are generally applied to FactoryTalk groups
- Exclusions and exceptions may be applied to users of either sort
- Users may be in more than one group

FactoryTalk Computer Accounts

- Computer accounts can be used to restrict *where* a user may be when performing an action
- Computer accounts and computer group accounts are NOT linked to Windows
- But computer account names must match the Windows hostname for permissions to take effect

Windows-linked Users and Groups

- Windows OS where each FactoryTalk application is running handles login
- FactoryTalk never sees credentials
- Access can also be granted at the Windows-linked group level
- *Windows* may cache user credentials, thereby enabling access when the domain is unavailable
- But group information is not cached, and so login will fail if the domain is unavailable
- Entra ID users and groups *are* supported for manual login

Other Things to Note

- FactoryTalk also supports login with RFID Badges
- Certificates are supported for a variety of functions such as authorizing applications and reverse proxy services
  - This is another reason to build out your own PKI
- Users may be marked as “deleted” so that another one cannot be created later to obtain the same access
- Windows-linked groups can be moved from one domain to another, but not windows-linked users

Summary

- Use Windows-linked users and groups where possible
  - Provisioning and deprovisioning is greatly simplified
  - All password and other policies apply
- Ensure that your Active Directory structure and group membership supports the granularity of access that you want to provide
- Maintain FactoryTalk users for emergency use and if Windows connectivity is unreliable
- Permissions are still controlled within FactoryTalk, so you need to have strong procedures to manage that too

Takeaways

5. Solve for five critical controls first
-  Then start with basic AD and remote access
-  Wireless generally has good supports for authentication
-  Then move to applications and finally devices
-  Work with vendors to support central auth through RFx etc
-  Build a PKI and find capable administrator(s)
-  Dynamic policy and continuous validation at scale will be difficult

THANK YOU

Secure ICS Network Architectures

When you can’t touch the endpoints, that only leaves the network

Purdue Levels and Enforcement Boundaries

- Networks should be organized into security zones using
  - Purdue levels are the most common security zone naming scheme used
  - Purdue model is first and foremost a linguistical tool!!!

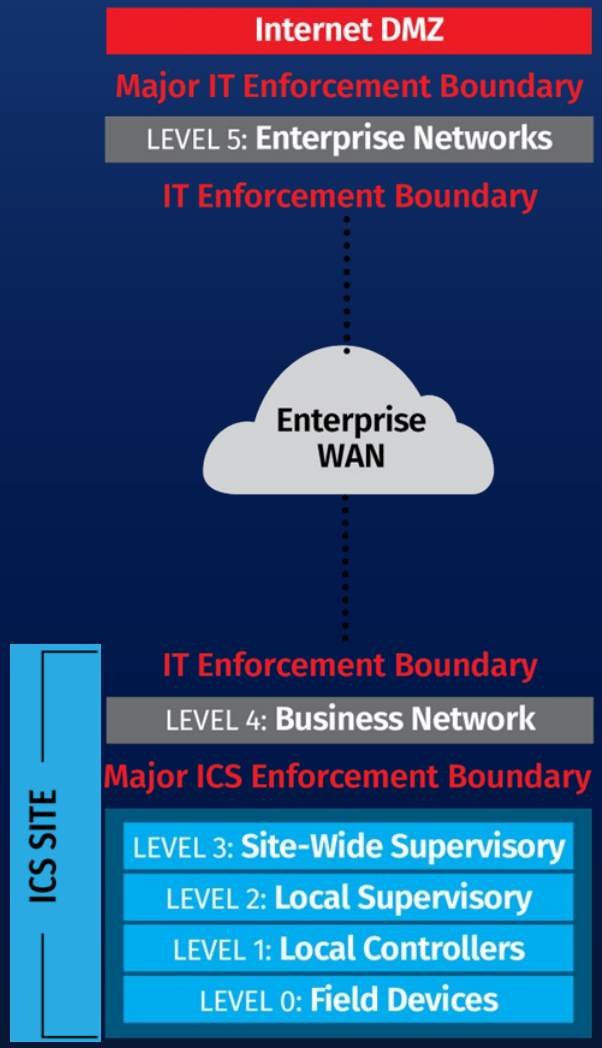
- ICS410 reference model is based on guidance in ISA/IEC 62443
  - Each level has different components, services, and functions
  - A single Purdue level can contain multiple subnets
  - Network defenses can be placed between subnets in the same Purdue level

- Enforcement boundaries are where we place cybersecurity network defenses
  - Limit communications through the boundary (think firewalls)
  - Record and inspect communications through the boundary

IT/OT Demarcation

- Segmentation between IT and OT is key
  - OT environments are overly dependent on network defenses
  - Host-based security solutions are harder and sometimes impossible to deploy
- Vendor and commissioning restrictions make endpoint security harder
  - Older software because of longer life cycle requirements
  - Less ability to harden or patch endpoints
- Determining the demarcation between IT and OT
  - Assets that make up the OT processes are usually obvious
  - Other OT assets should be determined by their ability directly or indirectly affect OT

Levels 4 and 5: Business and Enterprise Networks



- Most OT/ICS sites are connected back to the enterprise
  - MPLS or satellite links are common
  - Enterprise provides many important services to the plants
- Each larger site, plant, or facility usually has a business network
  - This is Purdue Level 4
  - Supporting services, data, etc.
  - HR systems, email servers, print servers
  - Enterprise Security Operations Center (SOC)
- General cybersecurity guidelines
  - Internet access and email should not go deeper than Level 4
  - Level 4 machines should be provided for OT staff to access this data
  - Enterprise Active Directory (AD) should not extend below this point

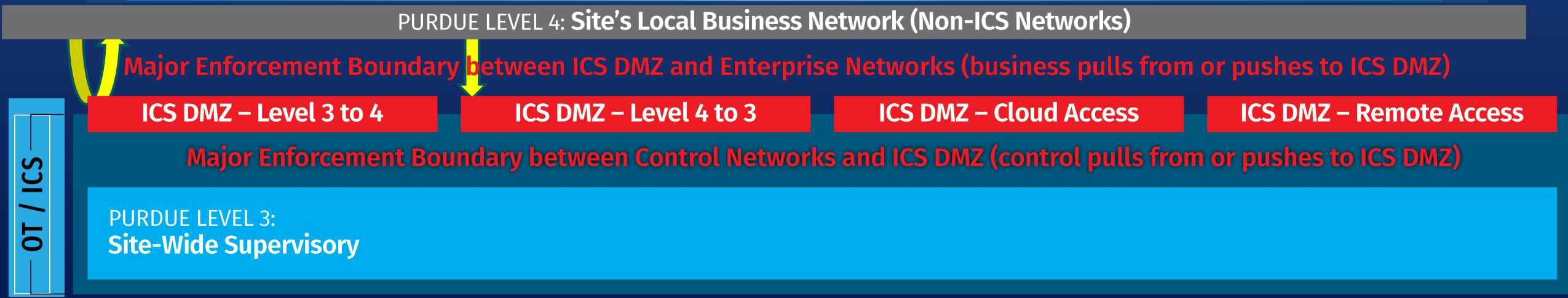
A Strong ICS Perimeter Includes a DMZ

- ICS DMZ allows you to inspect twice
  - greatly decrease the chance of attacker's bidirectional tunnels
  - To realize this benefit, **ALL** inbound and outbound traffic must stop at a server in the DMZ

- Two-firewall solution
  - Firewall rulesets require all traffic to terminate in the Control System DMZ
  - Allows business and control to each manage a firewall, even different vendors
  - Often the best political decision

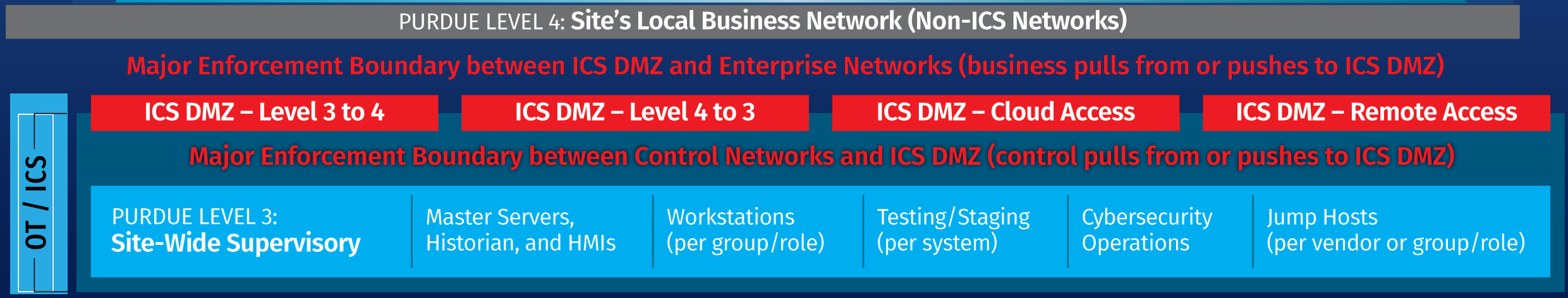
- Single-firewall solution
  - 3-legged firewall with Control System DMZ on a third port
  - Managed from the Control System side
  - No rule permits traffic directly between business and control

ICS DMZ (This is not your internet DMZ!!!)



- ICS DMZ and its enforcement boundaries are your primary ICS perimeter
  - Scale number of ICS DMZs to complexity of IT/OT traffic
  - use micro-segmentation to minimize lateral movement in DMZ
  - Web proxies should be avoided since they blindly pass on exploits
  - Don't place patch management and other security services here, instead place them in Purdue Level 3
- The most secure communications should look like this (overall data flow, not protocol functionality)
  - Level 4/5 pushes to this DMZ, and Level 3 pulls from it
  - Level 3 pushes to this DMZ, and Level 4/5 pulls from it
  - Larger sites can use multiple DMZ to separate traffic further and mitigate risk
  - Smaller sites can use a single ICS DMZ

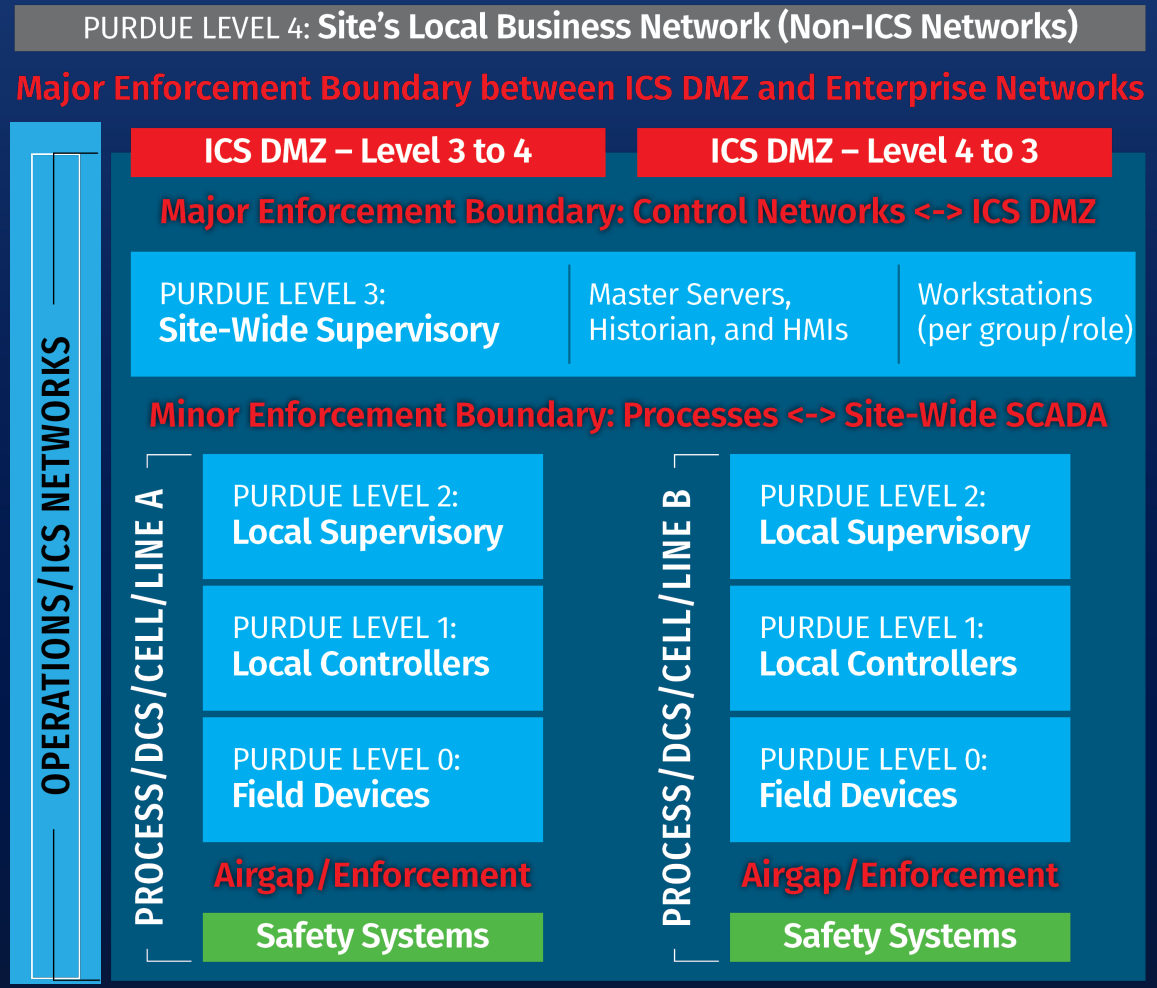
Purdue Level 3: Plant-Wide Supervisory



- Plant-wide monitoring, control, and operational support
  - Level 3 can (and should) be broken into multiple subnets
  - Group systems by function and role, which simplifies network security controls
  - A lesser enforcement boundary should sit between Level 3 and Level 2, appropriate for site
- ICS cybersecurity operations subnet
  - Provides a secure subnet to manage SIEM, patches, and endpoint security solutions
  - Should have ACLs to prevent compromise of this subnet from other Level 3 subnets
  - Patches and endpoint updates should be fed through ICS DMZ

Enforcement Boundaries between Level 3 and Processes

- Identify major process groups at each site
- Consider minor enforcement boundary between them and Purdue Level 3
- Isolate any safety system communication from the rest of the ICS network



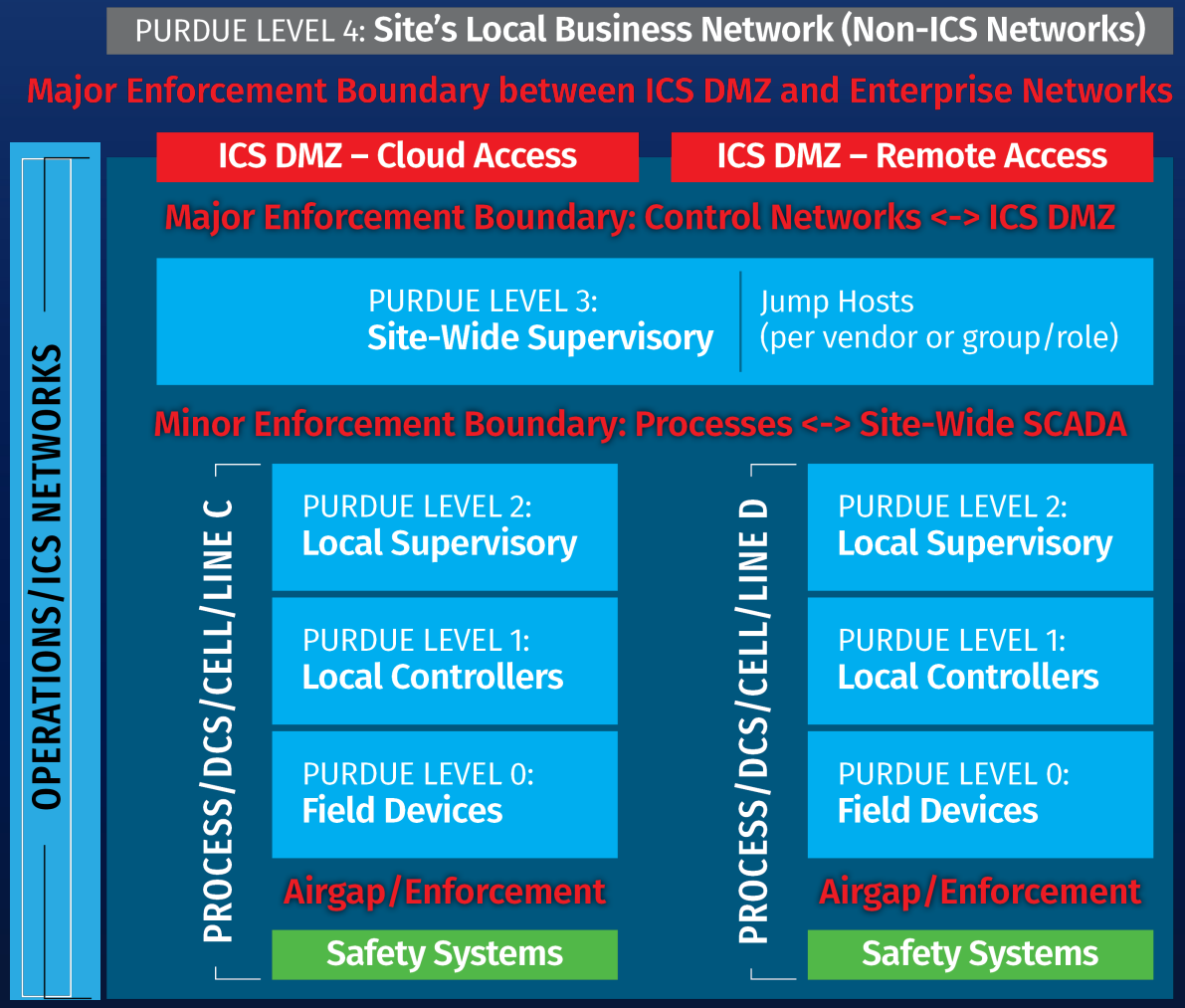
Individual Remote Access – Two Separate Steps

1: VPN or ZTA from the Internet to the ICS DMZ
- Two-factor authenticates REQUIRED
- Use standalone authentication or Enterprise AD
- Success makes remote machine member of DMZ

2: RDP/VNC/Citrix or ZTA to jump host in Level 3
- Use OT AD authentication
- Leverage different jump hosts per employee role or vendor
- ZTA solutions could provide limited access direct to asset

- Additional recommendations
  - Solution in step 1 or 2 should record session
  - Prevent most remote users from bringing data
  - If permitted, use file server in ICS 4 to 3 DMZ or ZTA to
  - Hash files for IR and forensics
  - Scan files for malware, if passes, enables download from jump host
  - Prevent most from using of software on remote host

Cloud Connectivity and IIoT



- Cloud connectivity should be considered very carefully
  - Is it required?
  - Does it affect security, reliability, and safety?
  - Treat traditional 24x7 vendor remote access like cloud
- When needed, assume attack and isolate traffic patterns
  - Use TLS protected protocols or VPNs
  - Firewall rules should use IPs if possible, hostnames if not
  - Firewall rules should be highly specific in both directions
  - All traffic should move through a system in ICS Cloud DMZ
    - Either a server that brokers traffic between cloud and ICS assets
    - Or a web proxy with allow lists between specific systems and services
    - Both solutions should support logging, tuned appropriately
  - If connections to level 2, 1, or 0 are needed, place secondary defenses around those assets to block pivots

ICS410 Site Reference Model

PURDUE LEVEL 4: **Site's Local Business Network (Non-ICS Networks)**

Major Enforcement Boundary between ICS DMZ and Enterprise Networks (business pulls from or pushes to ICS DMZ)

ICS DMZ – Level 3 to 4 | **ICS DMZ – Level 4 to 3** | **ICS DMZ – Cloud Access** | **ICS DMZ – Remote Access**

Major Enforcement Boundary between Control Networks and ICS DMZ (control pulls from or pushes to ICS DMZ)

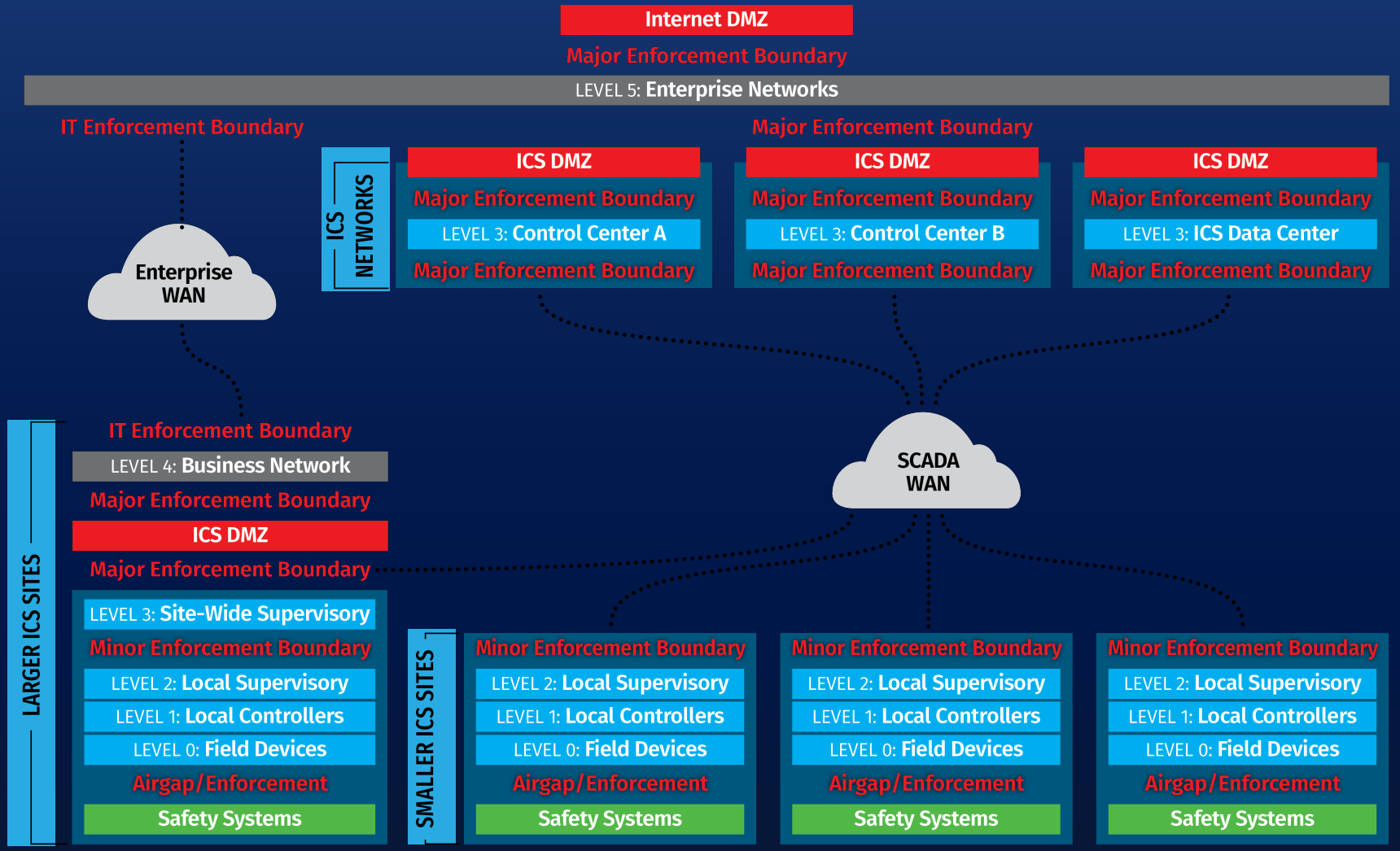
PURDUE LEVEL 3: **Site-Wide Supervisory**	Master Servers, Historian, and HMIs	Workstations (per group/role)	Testing/Staging (per system)	Cybersecurity Operations	Jump Hosts (per vendor or group/role)

Minor Enforcement Boundary between Processes and Site-Wide Supervisory (ACL on Router/Layer-3 Switch or Firewall)

OPERATIONS/ICS NETWORKS

PROCESS/DCS/CELL/LINE A	PROCESS/DCS/CELL/LINE B	PROCESS/DCS/CELL/LINE C	PROCESS/DCS/CELL/LINE D
PURDUE LEVEL 2: **Local Supervisory**	PURDUE LEVEL 2: **Local Supervisory**	PURDUE LEVEL 2: **Local Supervisory**	PURDUE LEVEL 2: **Local Supervisory**
PURDUE LEVEL 1: **Local Controllers**	PURDUE LEVEL 1: **Local Controllers**	PURDUE LEVEL 1: **Local Controllers**	PURDUE LEVEL 1: **Local Controllers**
PURDUE LEVEL 0: **Field Devices**	PURDUE LEVEL 0: **Field Devices**	PURDUE LEVEL 0: **Field Devices**	PURDUE LEVEL 0: **Field Devices**
Airgap/Enforcement	**Airgap/Enforcement**	**Airgap/Enforcement**	**Airgap/Enforcement**
Safety Systems	**Safety Systems**	**Safety Systems**	**Safety Systems**

Regional SCADA



- Control centers and central ICS data centers are Purdue Level 3
- Think of each field site as a separate process/cell/line
- SCADA WAN links considered untrusted
- Filter and monitor each WAN link in/out
- Nothing prevents you from defining LVL 3 or 4 on smaller sites if needed