OT Security made simple

Dillon Lee

Principal TAM at Dragos
Key Volunteer at ICS Village
IT Cybersecurity Advisor at Northwood Technical College
Dillon.Lee@icsvillage.com
https://www.linkedin.com/in/dillon-lee/

OT SECURITY GOALS

Safety

Ensure safe operations

“What is your why?”

Reliability

Infrastructure that is trusted by operations

Availability

Solutions need to be available during both maintenance and operations

Safety
What is your why?

Enjoy a bunch of stock photos

Reliability

Trustworthiness measurement on the length of time between failures

Availability

The network 's ability to quickly make connections, process traffic, and respond to user requests

5 Critical Controls

Created by Rob Lee* & Tim Conway

*Not Related to Rob

5. Risk-based vulnerability management

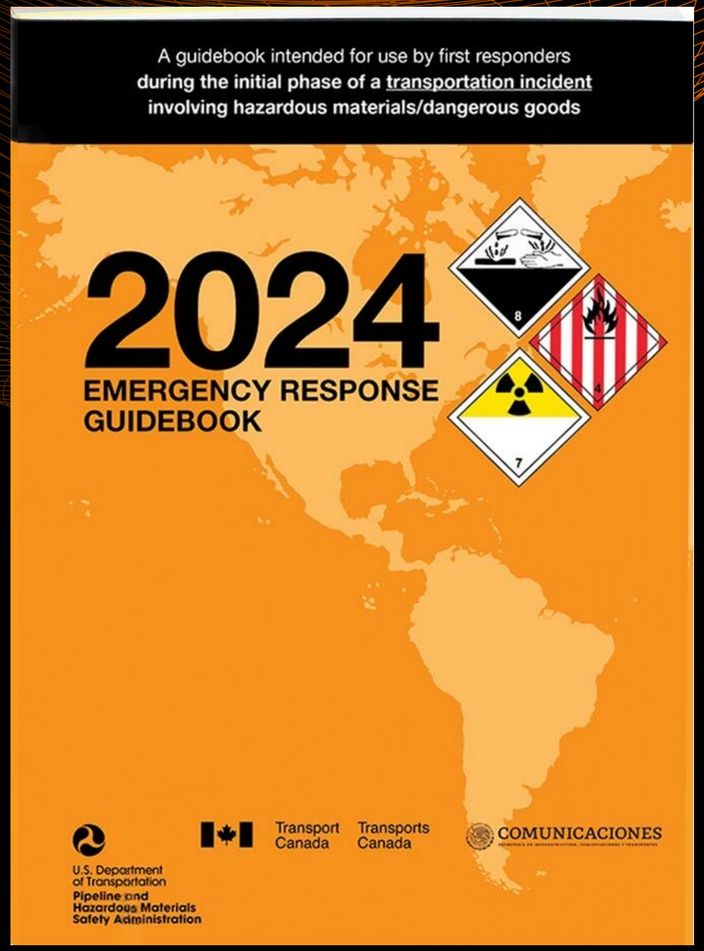
4. Secure remote access

3. Visibility and monitoring

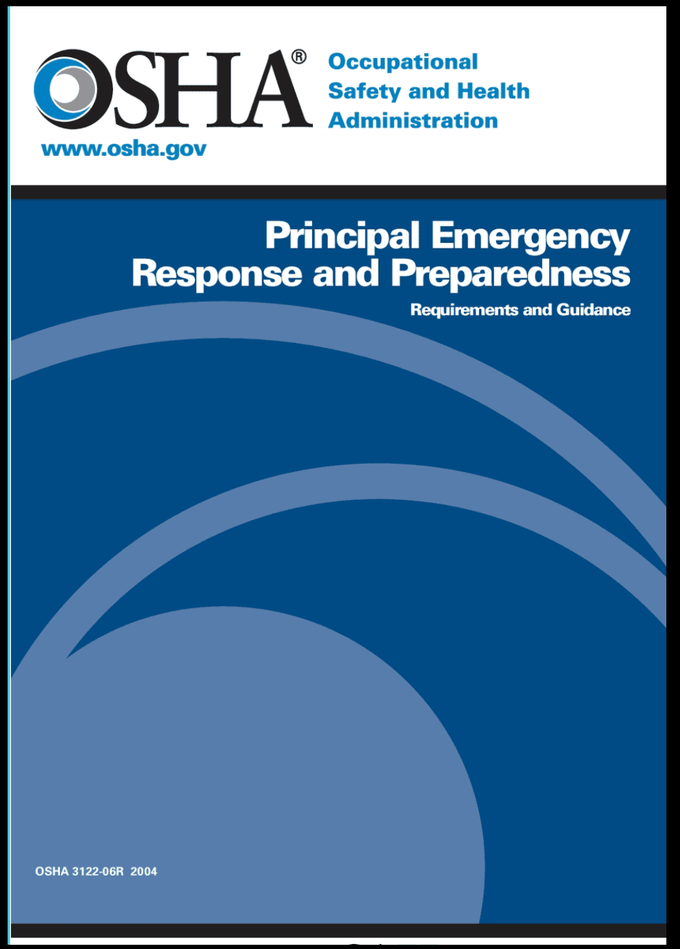
2. A defensible architecture

1. ICS incident response plan

ICS Incident Response Plan



- Safety has something. Start there first.
- Identify the biggest risks to the company
- Build relationships with local staff
- What is a bad day? How do we protect against that?
- Site recovery plan? Non-Cyber



What is needed to get started?

Personal Protection Equipment or PPE

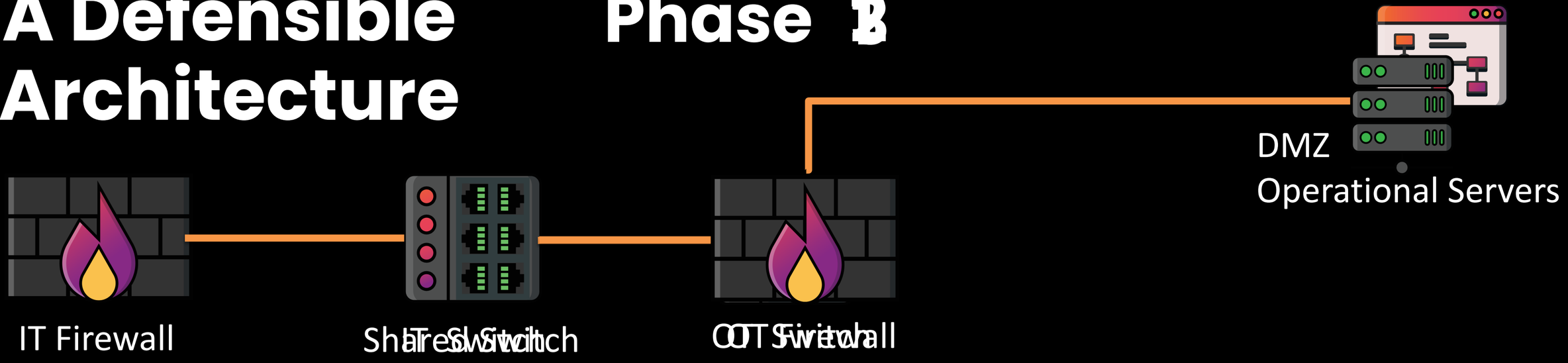
Site Contact

A Bribe


1. ICS incident response plan
2. A defensible architecture
3. Visibility and monitoring
4. Secure remote access
5. Risk-based vulnerability management

A Defensible Architecture

Phase 1



Physically segment your networks

Implement OT Firewalls between segmented networks

Move operational processes from IT into a DMZ

Key points for defensible architecture

1

Policy Enforcement

Maintain well-defined policy around IT/OT points—policy, not rules.

2

People and Process

The resources and technical skills required to maintain and overcome the ever-changing landscape

3

High Risk Vulnerabilities

Mitigate High-risk vulnerabilities in IT networks creating layered defense


1. ICS incident response plan
2. A defensible architecture
3. Visibility and monitoring
4. Secure remote access
5. Risk-based vulnerability management

Visibility and Monitoring

Inventory of assets

Building a live list of assets that are currently active on the wire and not just a snapshot in time like an excel or drawing

Monitors traffic

Looking for everything on the wire from misconfigurations, abuse of protocols, rogue assets, improper segmentation, and policy violations

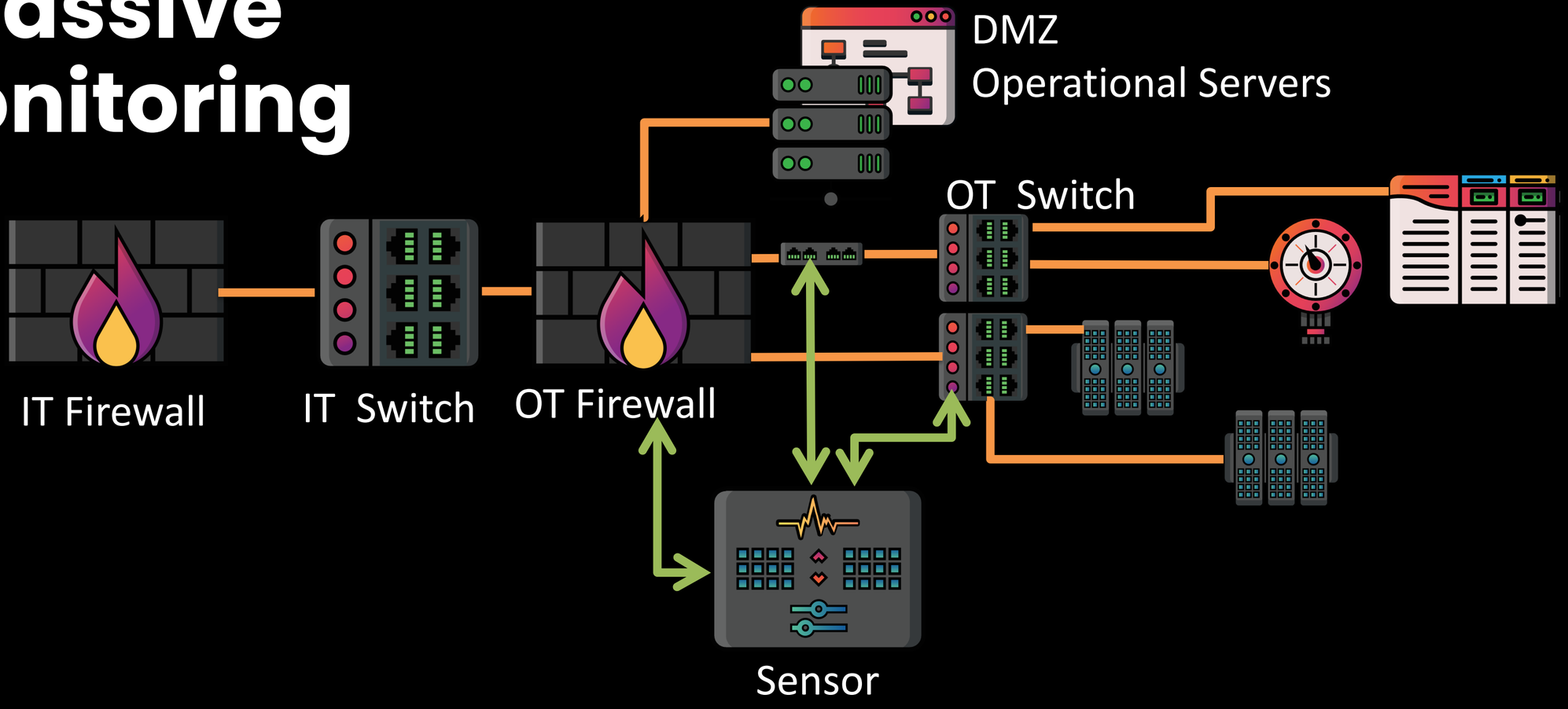
Maps Vulnerabilities

Taking know vulnerabilities and mapping them against your live asset list allows you to build a risk profile when informed about mitigation opportunities.

Threat Detection

Scaling and automation for large and complex networks.

Passive Monitoring

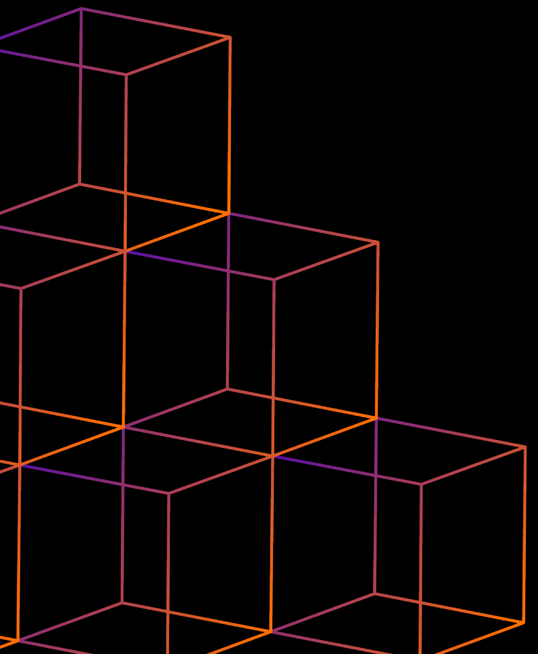


Passive Sensors sit on the network in key OT areas

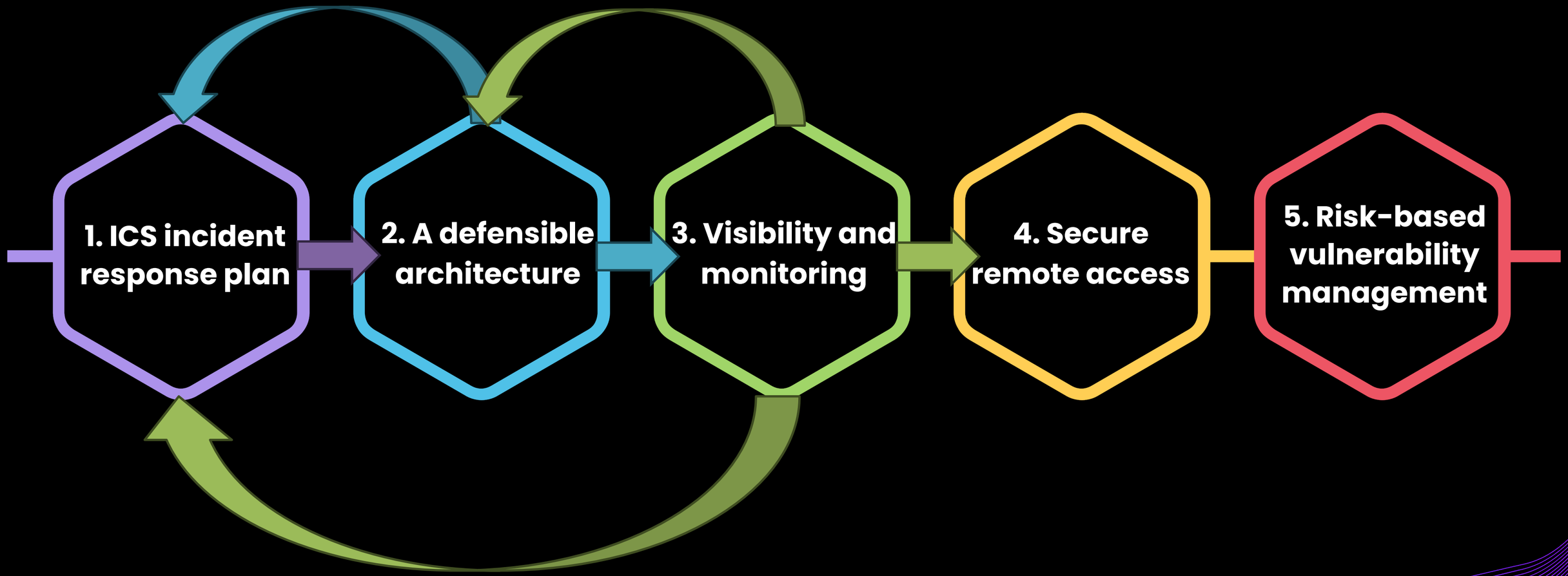
North / South from the firewall or TAPS

East / West from lower in cell area zone switches gathering Layer 2 traffic

Asset inventory goals



1. Automated identification
2. Process zone labeling
3. Vulnerability tracking
4. Crown jewel tracking by criticality
5. Companies want people who have worked with real equipment


1. ICS incident response plan
2. A defensible architecture
3. Visibility and monitoring
4. Secure remote access
5. Risk-based vulnerability management

Secure remote access

1

Large Gap 29%

Often overlooked for both implementation and management over time

2

Implement MFA

Do it!

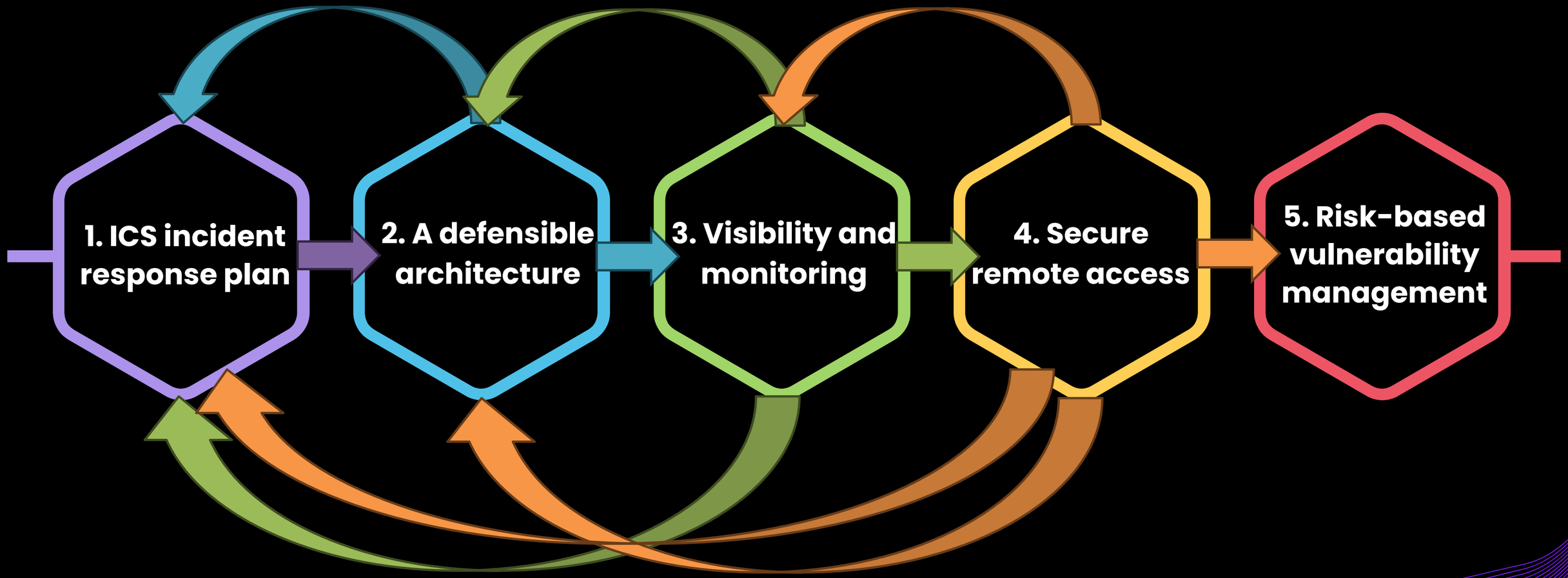
Seriously implement MFA

3

Secondary Controls

When MFA is not available build jump hosts or other manageable services to complete the work with logging and monitoring

Seriously, Enable MFA


1. ICS incident response plan
2. A defensible architecture
3. Visibility and monitoring
4. Secure remote access
5. Risk-based vulnerability management

Determining Risk

1.

You discovered two S7-1500s on the same firmware from when purchased. You identified vulnerabilities that should be patched or mitigated.

2.

Compressor	**Process**	Compressor
Maintenance Shop	**Location**	Process Air system
Firewalls	**External Mitigations**	No
No timeline	**Lifecycle date**	Next week

Timeline

Q1 2024

Vulnerability Identified

Q1 2024

Firewall Mitigation Deployed

Q1 2025

Next Maintenance Window

Q4 2025

Device Lifecycle out

One last time


Always has been
5 Critical Controls
So, it's a feedback loop?

Contact Information

Dillon.Lee@ICSVillage.com

www.ICSVillage.com