DRAGOS

OT Cybersecurity for IT Professionals

Mike Hoffman

MIKE HOFFMAN

Principal Industrial Consultant

@ICSSecurityGeek

linkedin.com/in/mjhoffman7

- 1.5 Years at Dragos and 20 Years in O&G with roles in downstream, upstream, and global technical leadership
- Past titles have included: Principal ICS Security Engineer, Controls and Automation Specialist, Process/CEMS Analyzer Specialist, and Instrumentation & Electrical Technician
- Masters in Information Security Engineering from SANS Technology Institute, SANS instructor in development

GICSP *gold* GRID *gold* GCIP GCIA GSEC GCCC GCIH GPYC GPEN GSTRT CISSP PMP CCNA

The Differences Between OT & IT

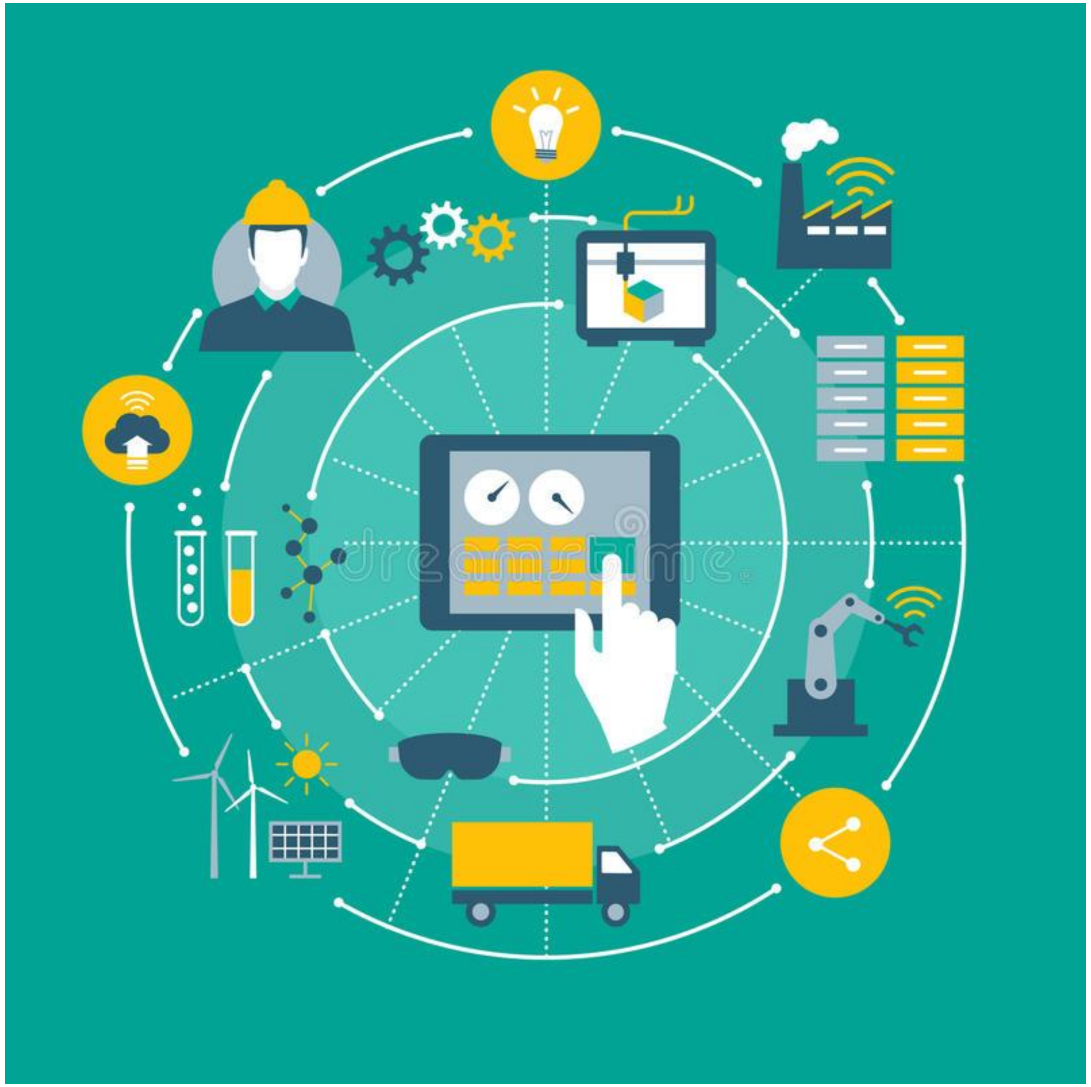
It’s Still About People, Process, & Technology

- Convergence of Operations Technology (OT) & Information Technology (IT) has “mostly” occurred
- Can we apply similar security controls in IT to OT?
- What preventative detective and recovery controls should we be focusing on?
- Where to begin?

A Little on Perspective

The IT Challenge

- This HMI looks like it’s IT
- It’s running Windows…
- But it’s running an older OS than we are running on the enterprise.
- We need to patch it, scan it, and eventually upgrade it.
- How critical is this computer by the way?



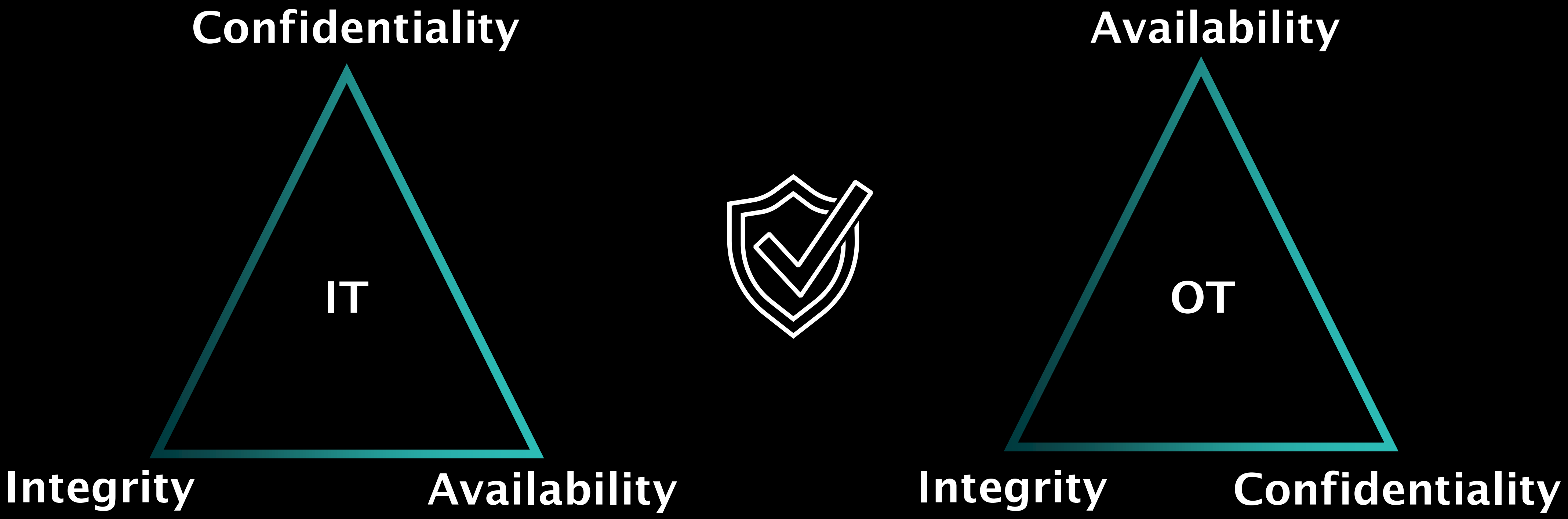
Managing Risks in an OT Environment

Common IT-Centric Mistakes

- Too much emphasis on vulnerability management
- Expecting OT to keep pace with IT for asset refresh
- Treating OT security as a project and not continual processes
- Hyper focused on moving to the cloud
- Ownership and accountability

Let’s Talk Fundamentals

CIA or AIC…More to the Discussion Than Shapes



Confidentiality

IT

Integrity

Availability

Availability

OT

Integrity

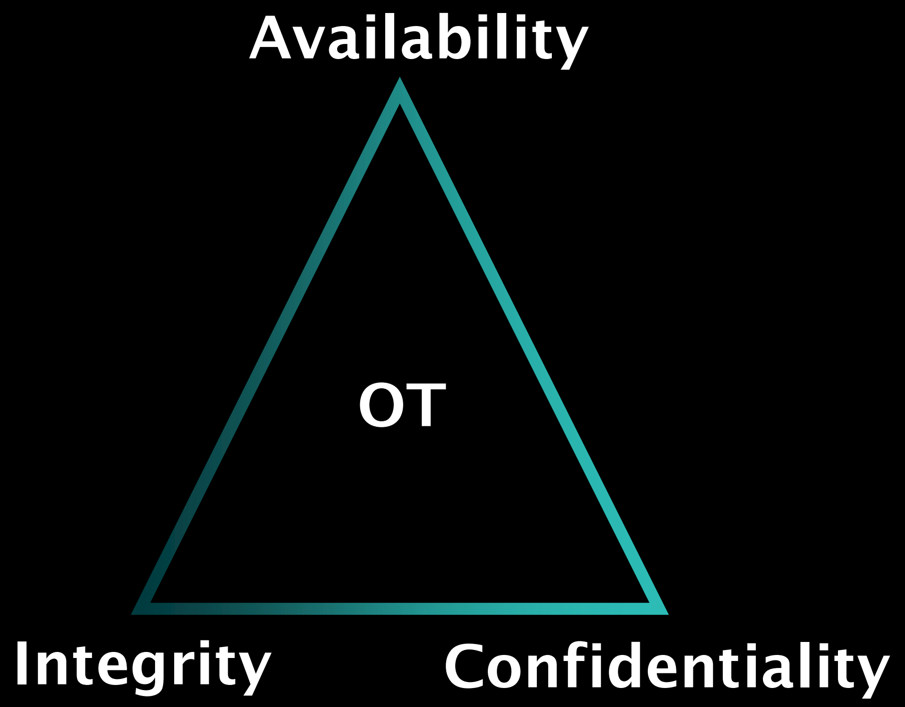
Confidentiality

Let’s Talk Fundamentals

CIA or AIC…More to the Discussion Than Shapes

SAFETY CONSIDERATIONS

- Process safety
- Environmental safety
- Personal safety



Delivering Core Business Functions

Protecting the Business Value

Generating, transmitting, and distributing power

Producing, transporting, and refining oil & gas products

Melting, casting, and forming metals

Converting raw ingredients into foods and packaging

Attributes of OT Systems

A Look at the Primary Level

- ✓ Interacting directly with physical systems
- ✓ Running production and manufacturing equipment
- ✓ Performing continuous and batch processing
- ✓ Bringing often significant inherent HSSE risks

OT Environments

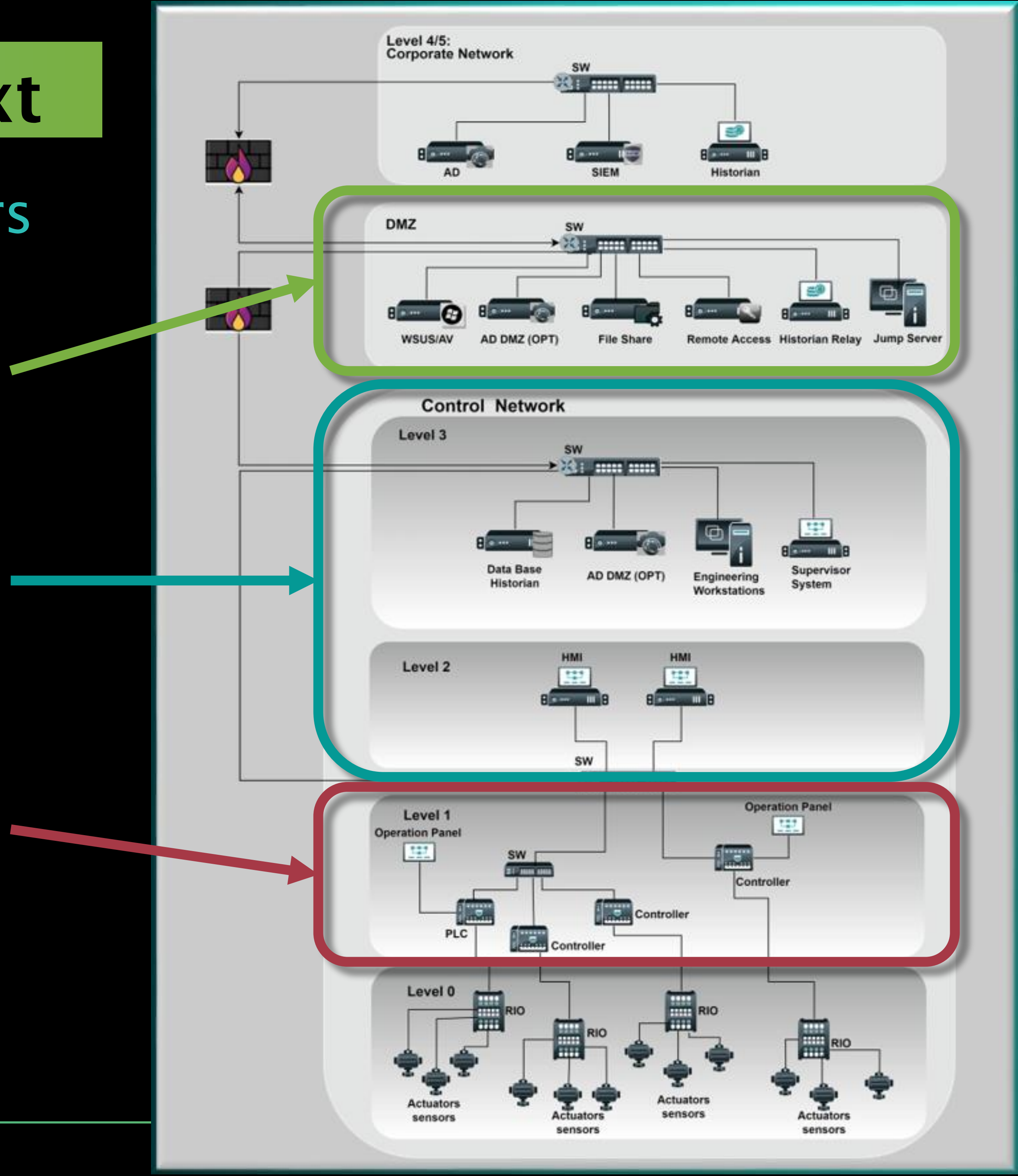
Stringent Requirements & Regulations

- High uptime
- Redundancy
- Low latency
- Strict vendor requirements
- Regulations (NERC-CIP, TSA, etc.)

OT Systems Require Context

Where the System is Located Matters

- A WSUS/AV server in the DMZ may not be “business” critical
- The Engineering Workstations, HMIs, Automation Servers, and DCs, are more critical
- The PLCs and controllers are absolutely critical



The Classic Cyber Risk Equation

… A Starting Point…

IN·DUS·TRI·AL CY·BER RISK

/ INˈDƏSTRĒƏL ˈSĪBƏR RISK/

The potential loss of life, injury, damaged assets, financial loss, and other harm from the failure or misuse of digital technologies and communication networks used for information and/or operational capabilities.

$$Cyber\ Risk = Consequence \times \ Threat \times \ Vulnerability$$

The Classic Cyber Risk Equation

… A Starting Point…

IN·DUS·TRI·AL CY·BER RISK

/ INˈDƏSTRĒƏL ˈSĪBƏR RISK/

The potential loss of life, injury, damaged assets, financial loss, and other harm from the failure or misuse of digital technologies and communication networks used for information and/or operational capabilities.

$$Cyber\ Risk = Consequence \times Threat \times Vulnerability$$

$$Disaster\ Risk = Hazard \times Exposure \times \frac{Vulnerability}{Capacity}$$

DRAGOS

The Classic Cyber Risk Equation

(Revised)

IN·DUS·TRI·AL CY·BER RISK

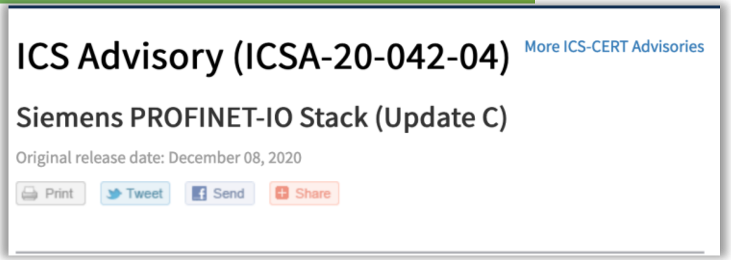
/ INˈDƏSTRĒƏL ˈSĪBƏR RISK/

The potential loss of life, injury, damaged assets, financial loss, and other harm from the failure or misuse of digital technologies and communication networks used for information and/or operational capabilities.

$$Industrial\ Cyber\ Risk = Consequence \times \frac{Threat\ \times Vulnerability}{Resilience}$$

The Classic Cyber Risk Equation

(Revised)

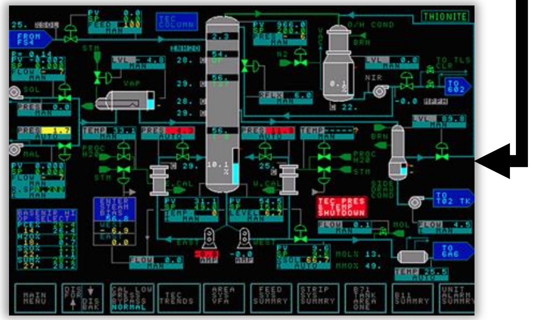


ICS Advisory (ICSA-20-042-04)

Siemens PROFINET-IO Stack (Update C)

Original release date: December 08, 2020

$$Industrial\ Cyber\ Risk = Consequence \times \frac{Threat \times Vulnerability}{Resilience}$$



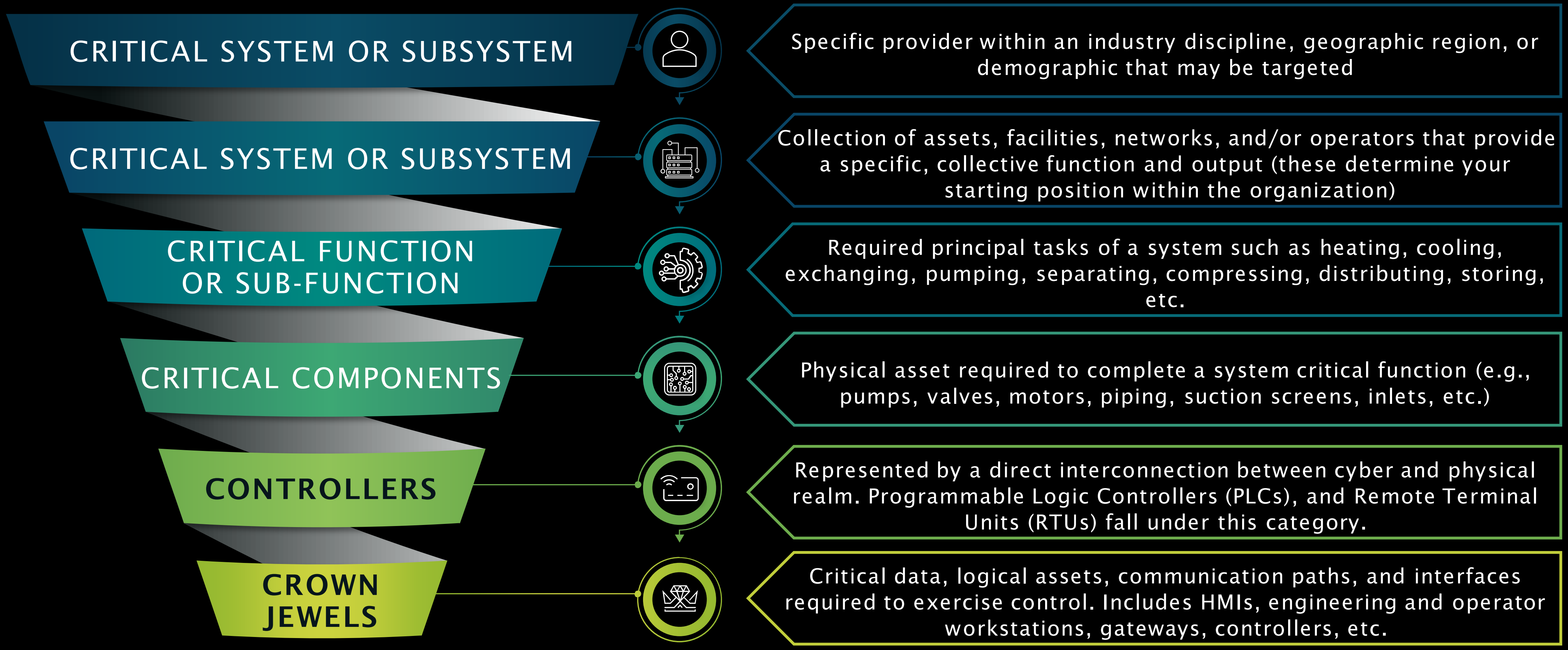
CROWN JEWEL ANALYSIS (CJA)

Understanding What Really Matters

- Not all ICS devices and systems are the same
- Each may have different levels of criticality based on process impact
- Higher levels of criticality require additional security countermeasures
- Going through the CJA processes requires a multidiscipline team
- Results in identifying key systems and components that need enhanced prevention, detection, and recovery capabilities

Crown Jewel Analysis

Overview of the Process



CRITICAL SYSTEM OR SUBSYSTEM

Specific provider within an industry discipline, geographic region, or demographic that may be targeted

CRITICAL SYSTEM OR SUBSYSTEM

Collection of assets, facilities, networks, and/or operators that provide a specific, collective function and output (these determine your starting position within the organization)

CRITICAL FUNCTION OR SUB-FUNCTION

Required principal tasks of a system such as heating, cooling, exchanging, pumping, separating, compressing, distributing, storing, etc.

CRITICAL COMPONENTS

Physical asset required to complete a system critical function (e.g., pumps, valves, motors, piping, suction screens, inlets, etc.)

CONTROLLERS

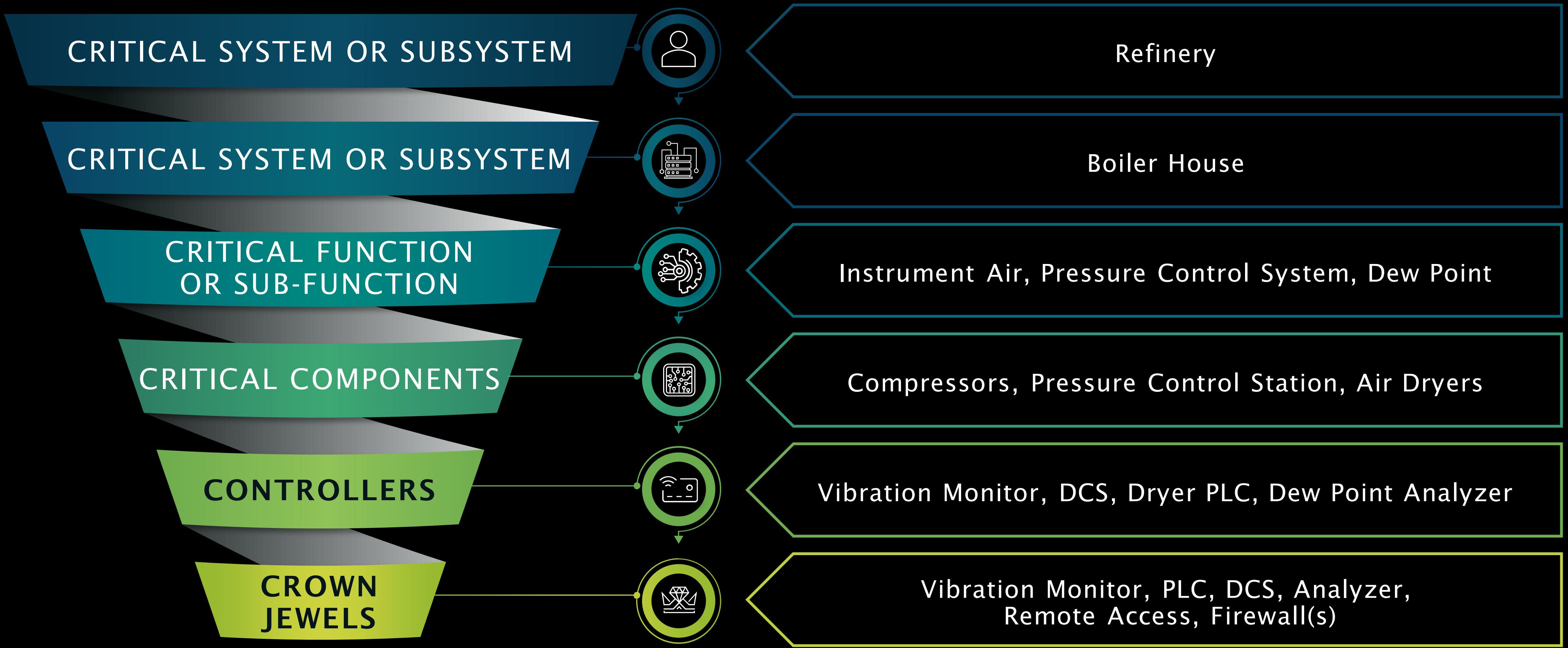
Represented by a direct interconnection between cyber and physical realm. Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) fall under this category.

CROWN JEWELS

Critical data, logical assets, communication paths, and interfaces required to exercise control. Includes HMIs, engineering and operator workstations, gateways, controllers, etc.

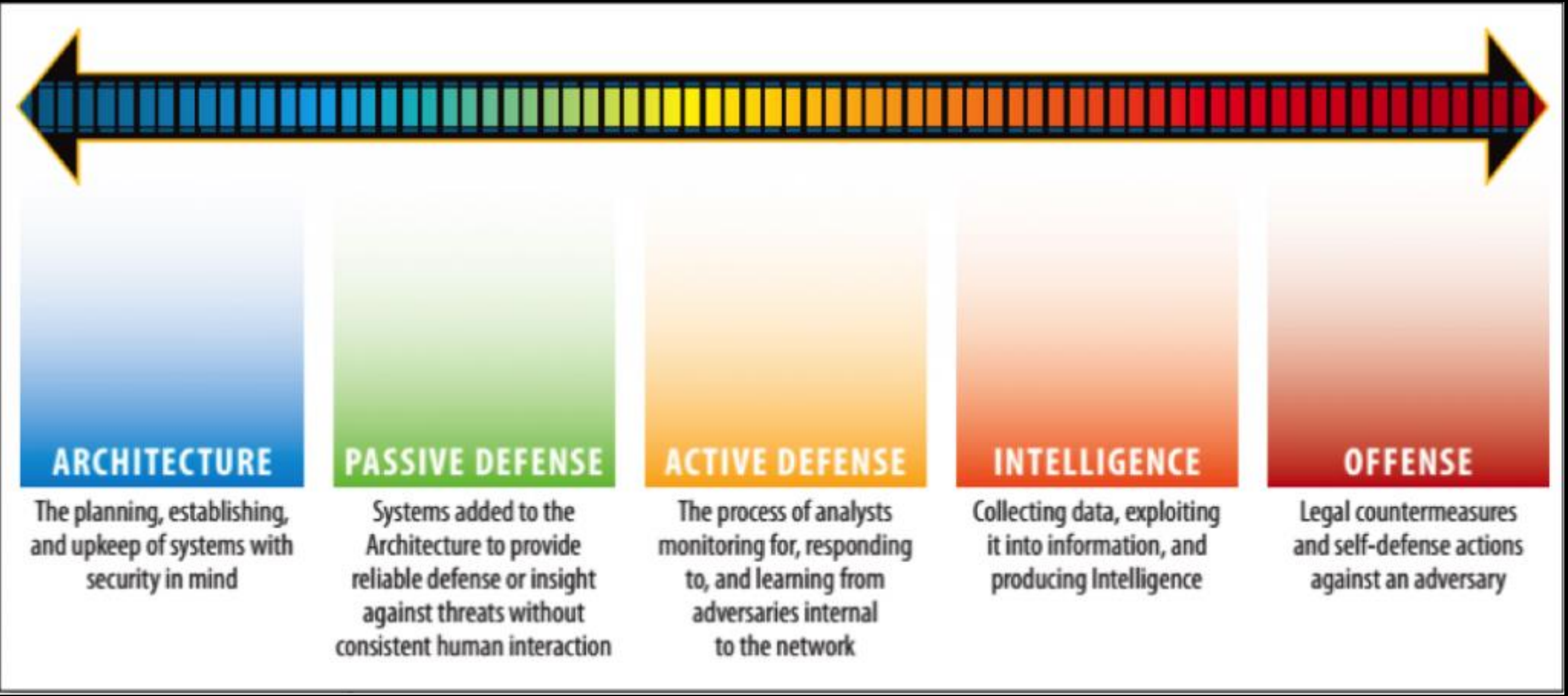
Crown Jewel Analysis

Control And Shutdown Valves Need Air



CRITICAL SYSTEM OR SUBSYSTEM	Refinery
CRITICAL SYSTEM OR SUBSYSTEM	Boiler House
CRITICAL FUNCTION OR SUB-FUNCTION	Instrument Air, Pressure Control System, Dew Point
CRITICAL COMPONENTS	Compressors, Pressure Control Station, Air Dryers
CONTROLLERS	Vibration Monitor, DCS, Dryer PLC, Dew Point Analyzer
CROWN JEWELS	Vibration Monitor, PLC, DCS, Analyzer, Remote Access, Firewall(s)

Sliding Scale Of Cyber Security



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

FIVE CRITICAL CONTROLS

http://www.dragos.com/5controls

5 CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

01
An ICS-specific incident response plan

02
A defensible architecture

03
OT Visibility: asset inventory, vulnerability mapping, & monitoring

04
Vulnerability management program

05
Multi-factor authentication (MFA)

Create an OT Incident Response Plan (IRP)

Develop OT response capabilities

- Create a dedicated incident response plan ICS/OT environments
- OT involves different device types, communication protocols, different types of tactics, techniques, and procedures(TTPs) specific to the industrial threat groups
- The IRP should be regularly exercise with cross-disciplinary teams (IT, OT, Executives, etc.)

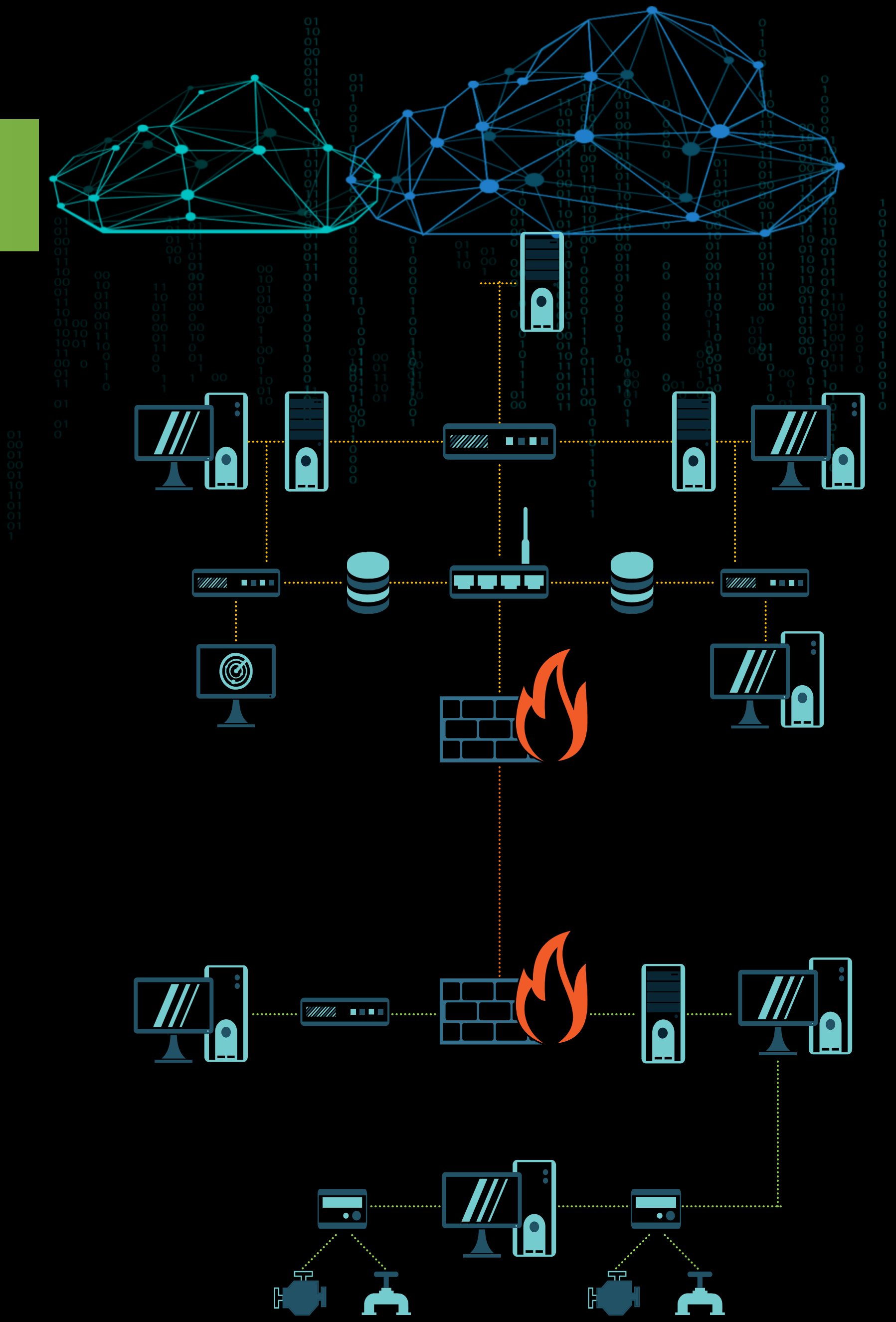
DRAGOS

OT Incident Response Plan

Build A Defensible Architecture

Start At The Edge And Work Your Way In

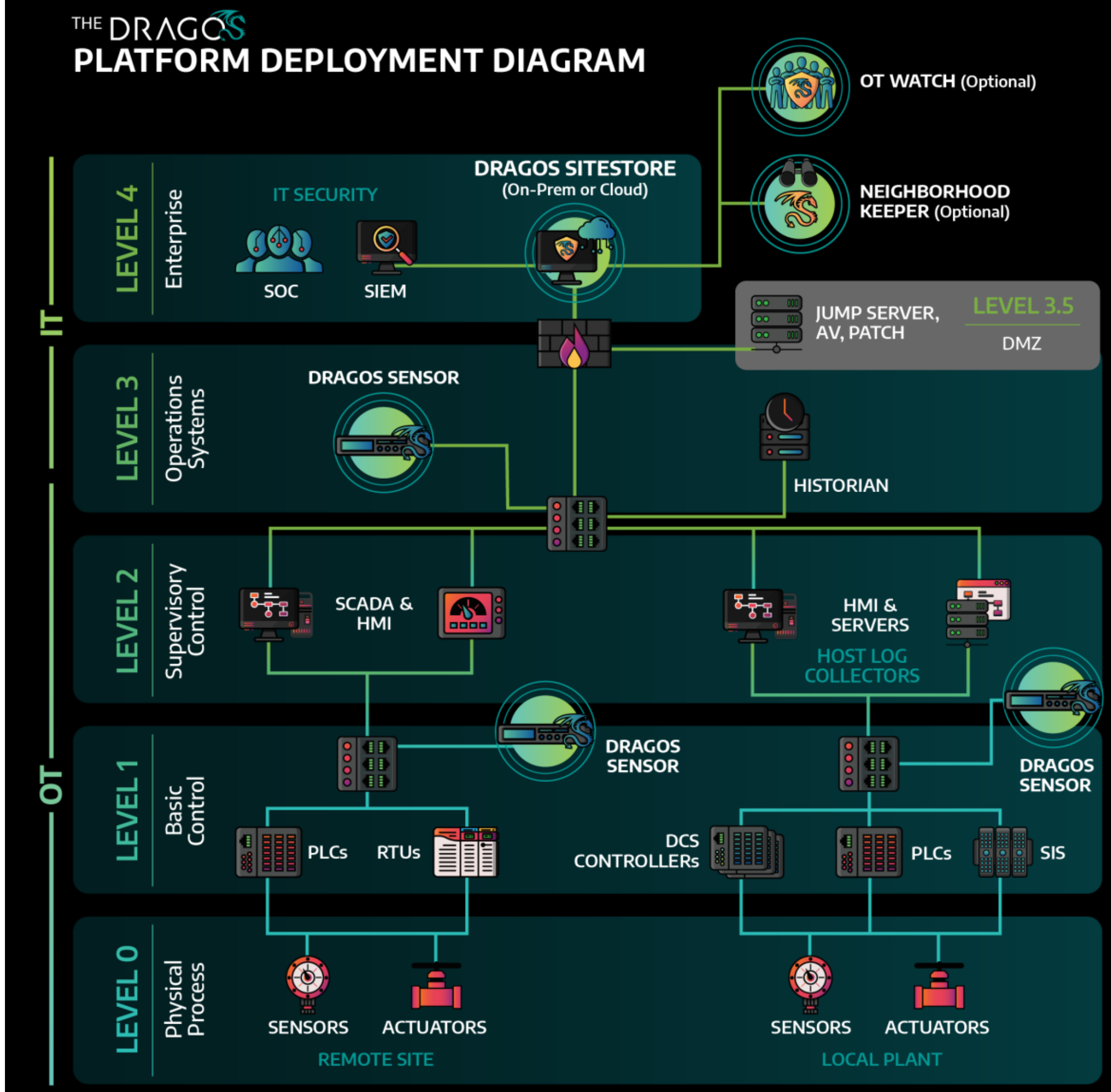
- Leverage traditional IT tools and concepts such as strong segmentation, firewalls, and software defined networks to reduce cyber risk, especially around remote access
- This can take a variety of forms such IEC/ISA 62443 zones and conduits, DMZs, jump hosts, etc.
- Identify and secure OT / IT data flows to the enterprise/cloud environments



Implement Network Monitoring

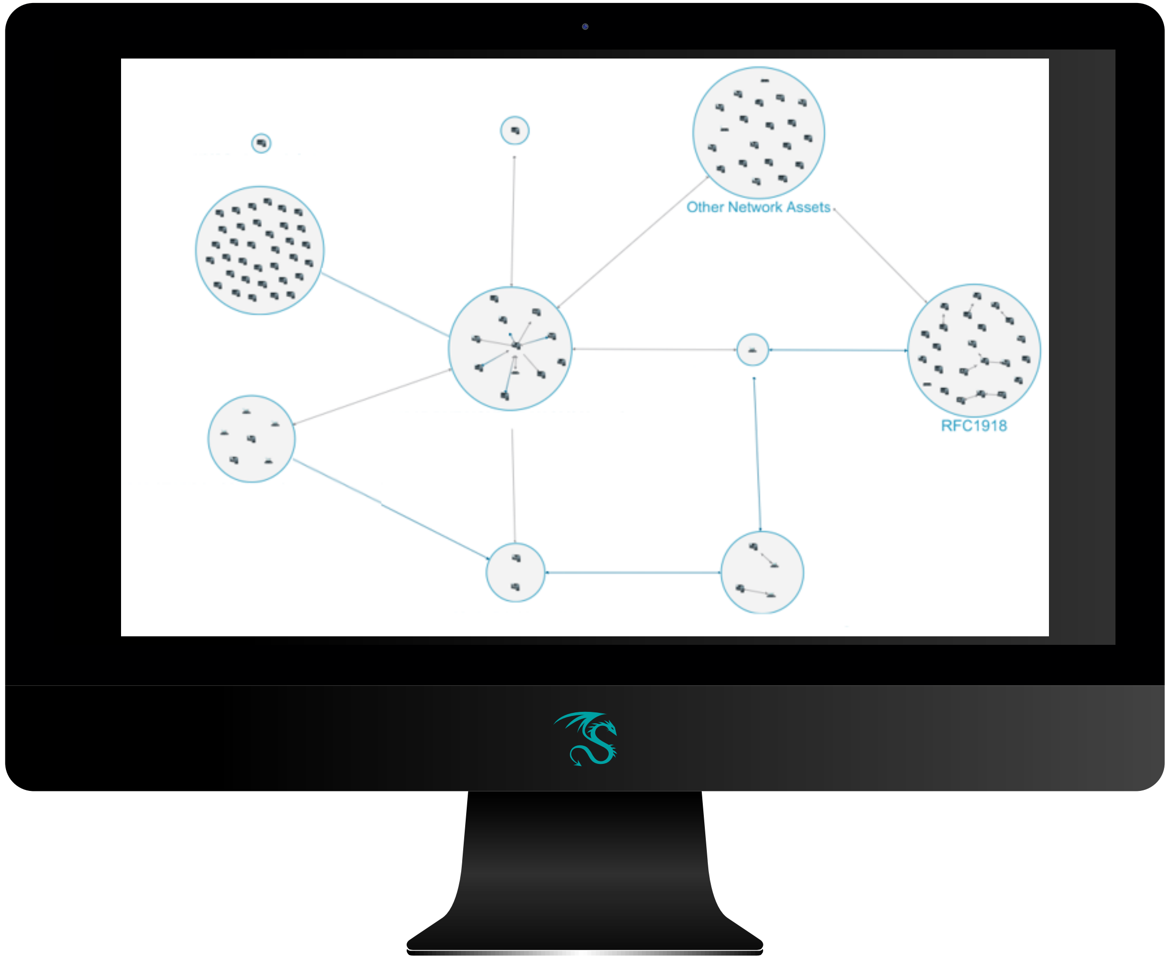
You Can't Protect
What You Can’t See…

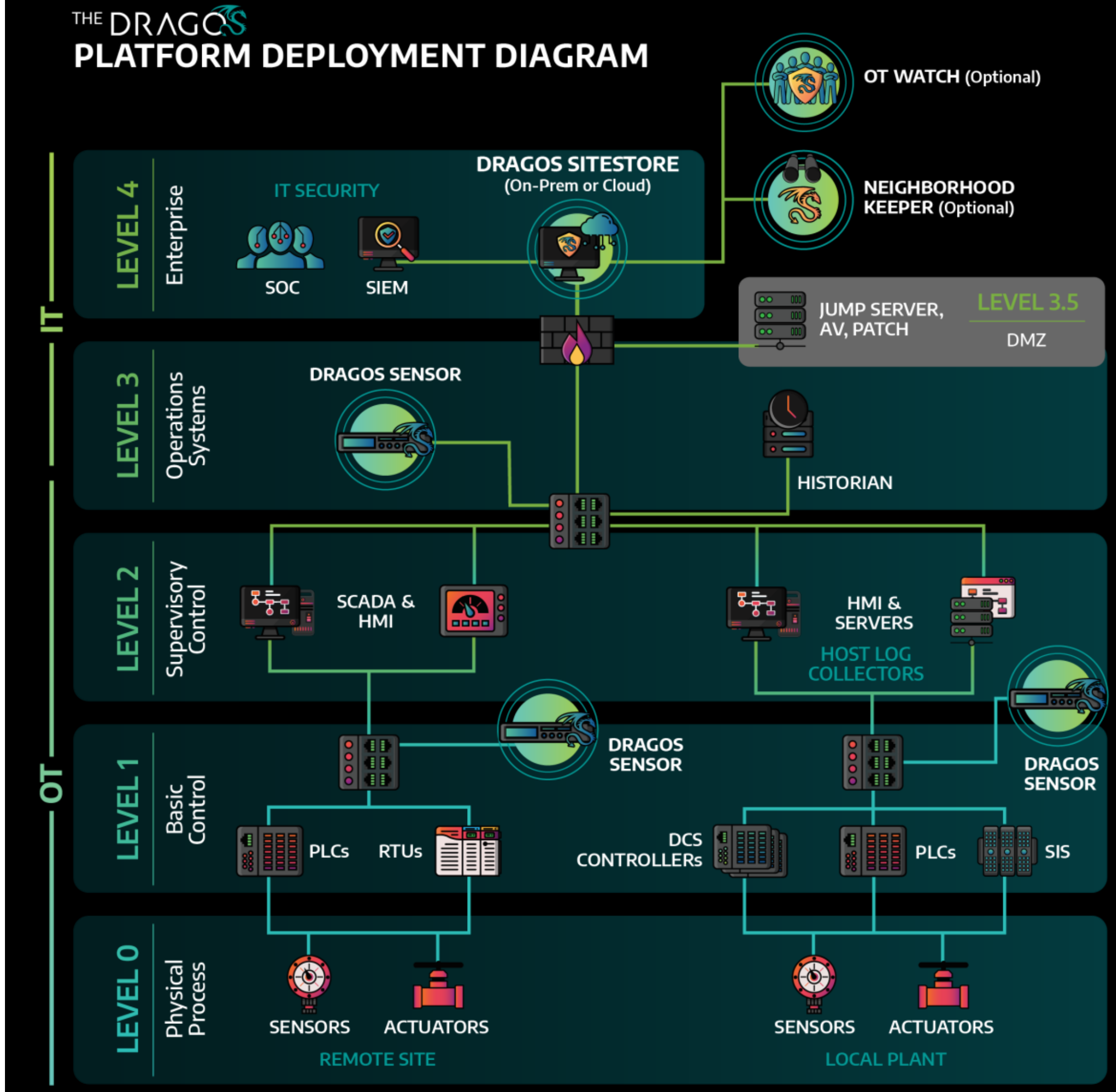
- Visibility gained from monitoring industrial assets validates the security controls implemented
- Threat detection from monitoring allows for scaling and automation for large and complex networks
- Monitoring can also identify vulnerabilities easily for action
- Greatly assists in supporting incident response processes
- Identifies network issues and system configuration errors



Implement Network Monitoring

Seeing Is Believing





THE DRAGOS
PLATFORM DEPLOYMENT DIAGRAM

OT WATCH (Optional)

NEIGHBORHOOD KEEPER (Optional)

IT

OT

LEVEL 4 Enterprise: IT SECURITY — SOC, SIEM; DRAGOS SITESTORE (On-Prem or Cloud)

LEVEL 3.5 DMZ: JUMP SERVER, AV, PATCH

LEVEL 3 Operations Systems: DRAGOS SENSOR; HISTORIAN

LEVEL 2 Supervisory Control: SCADA & HMI; HMI & SERVERS; HOST LOG COLLECTORS

LEVEL 1 Basic Control: DRAGOS SENSOR; DRAGOS SENSOR; PLCs; RTUs; DCS CONTROLLERs; PLCs; SIS

LEVEL 0 Physical Process: SENSORS; ACTUATORS; REMOTE SITE; SENSORS; ACTUATORS; LOCAL PLANT

DRAGOS

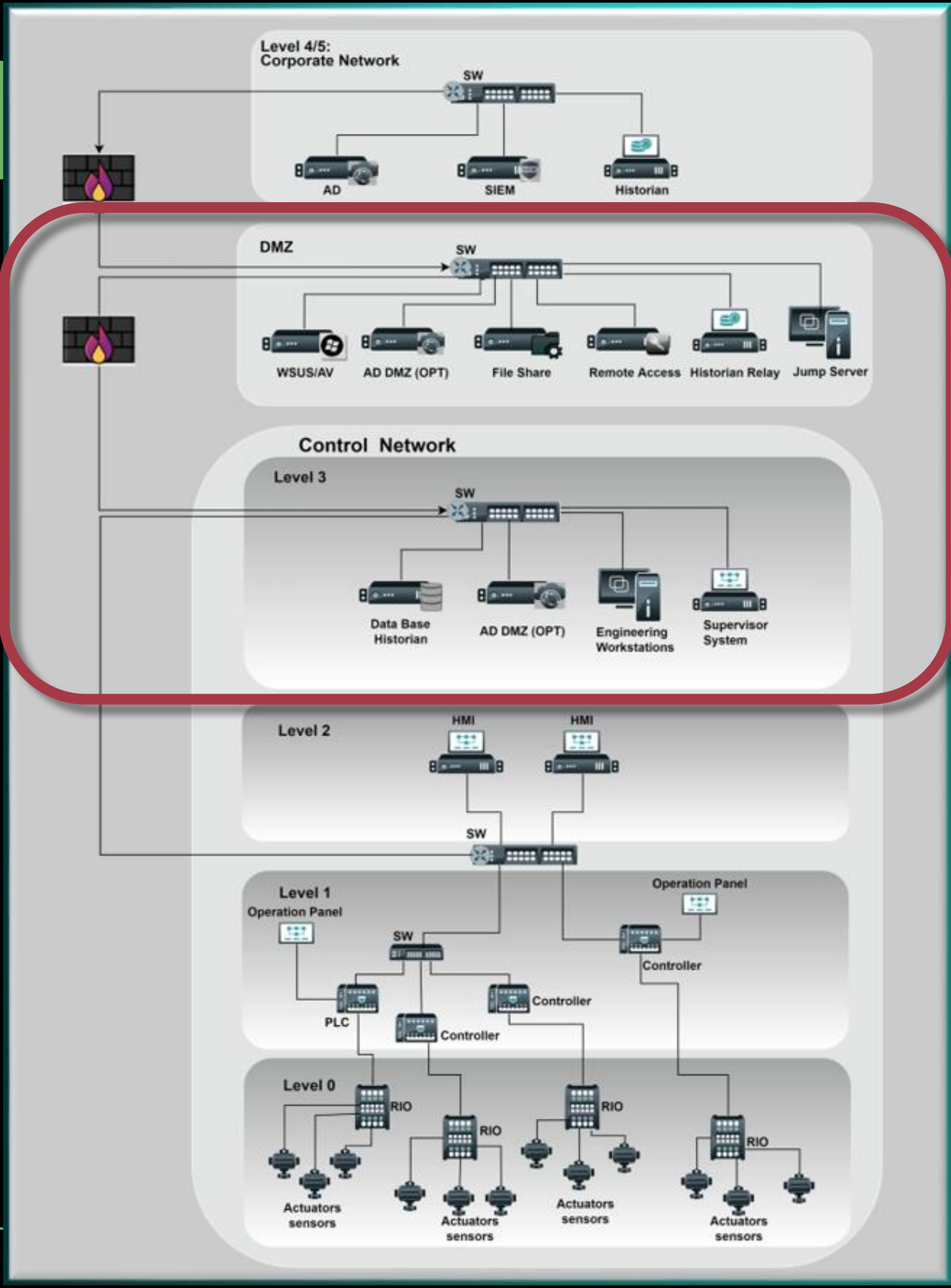
Manage Key Vulnerabilities

Focused Vulnerability Remediation

- Most vulnerabilities have limited impact if you have a defensible architecture

- Dragos recommends defenders prioritize those that bridge IT and OT over those residing deep within the ICS/OT network

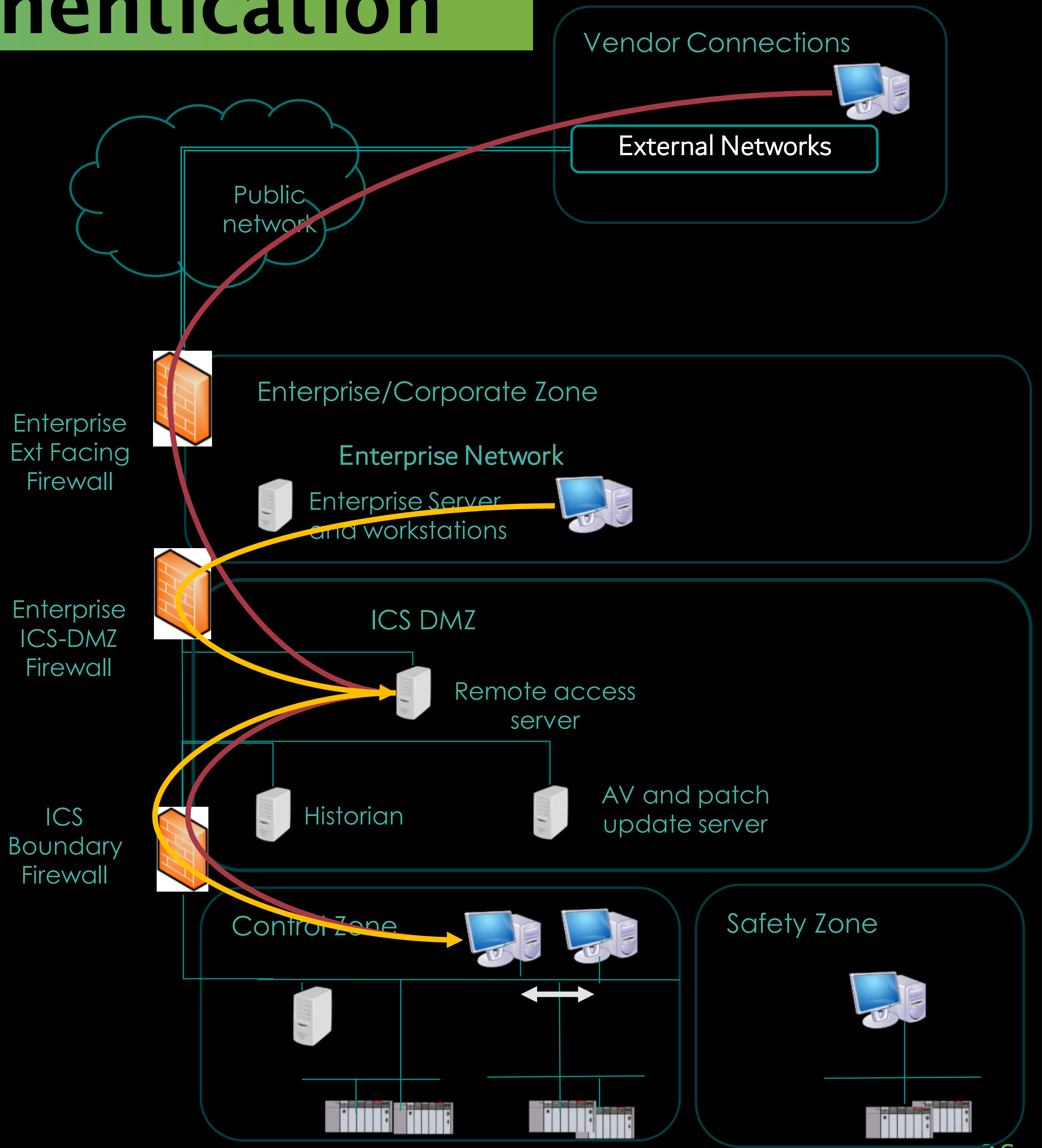
*These systems could be considered in-scope for vulnerability scanning



Establish Remote Access Authentication

Secure Remote Access

- The most effective control for remote access authentication is multi-factor authentication (MFA)
- Where MFA is not possible, consider alternate controls such as jump hosts with focused monitoring
- The focus should be placed on connections in and out of the OT network and not on connections inside the network



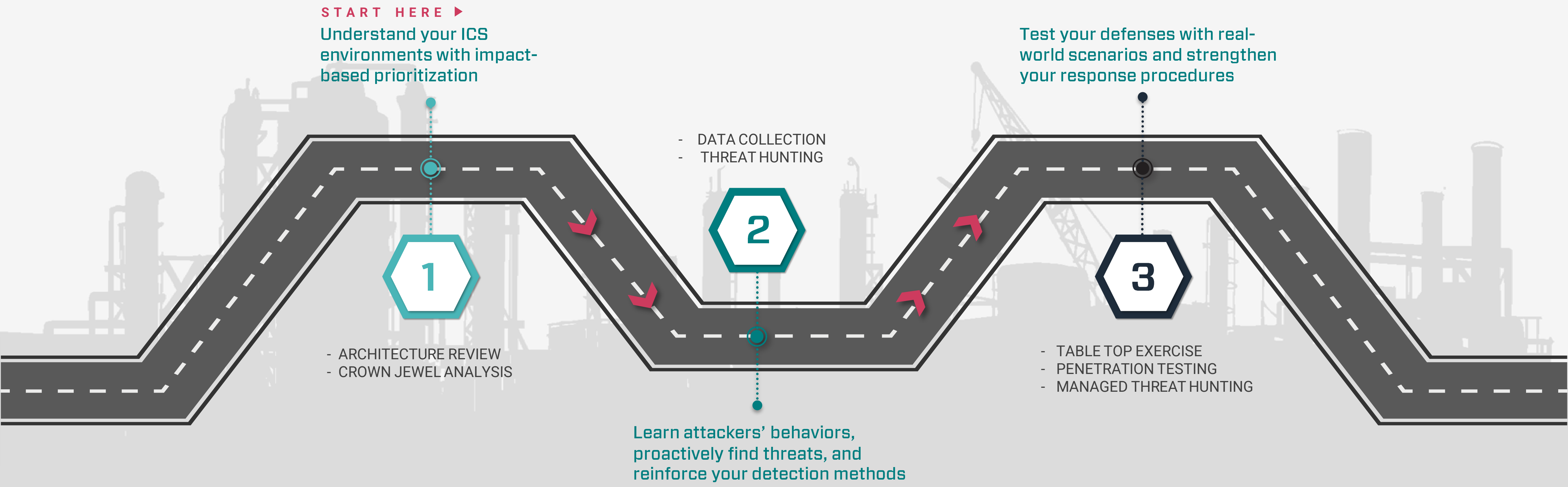
Working Together

Bring In The Best Of The OT & IT Side

- Form a cross functional team
- Bring in people from IT and OT backgrounds
- Leverage operations and process/electrical/control engineers - they are MVPs for understanding what’s important and what needs to be secured
- OT Security is a journey, not a project

Roadmap for ICS Security Sustainability

Establish, Enable, & Enhance Your ICS Defenses



START HERE ▶

Understand your ICS environments with impact-based prioritization

1

- ARCHITECTURE REVIEW
- CROWN JEWEL ANALYSIS

- DATA COLLECTION
- THREAT HUNTING

2

Learn attackers' behaviors, proactively find threats, and reinforce your detection methods

Test your defenses with real-world scenarios and strengthen your response procedures

3

- TABLE TOP EXERCISE
- PENETRATION TESTING
- MANAGED THREAT HUNTING

Summary

Yes, OT is different than IT

- It all depends on context and how the IT component is utilized
- Identify critical systems though the CJA process and devise mitigative solutions
- Look for ways to engineer out the problem, then work to mitigate, i.e., Prevent, Detect, Respond
- Start with the 5 Critical Controls
- Remember – defense is doable, and you have an important role to play

Q&A

QUESTIONS AND ANSWERS

Thank You!