Navigating Plant Risk: How IT Can Kill ICS - Increasing Risk to Plant Managers

SANS | ASSOCIATION OF METROPOLITAN WATER AGENCIES

Dean Parsons

REMINDERS

1. All attendees will be muted. If you have any questions or comments, please put them in the chat.

2. The slides and recording will be available after the presentation on the AMWA website.

SANS

INDUSTRIAL CONTROL SYSTEMS SECURITY

Dean Parsons B.SC., GICSP, GRID, CISSP, GSLC, GCIA

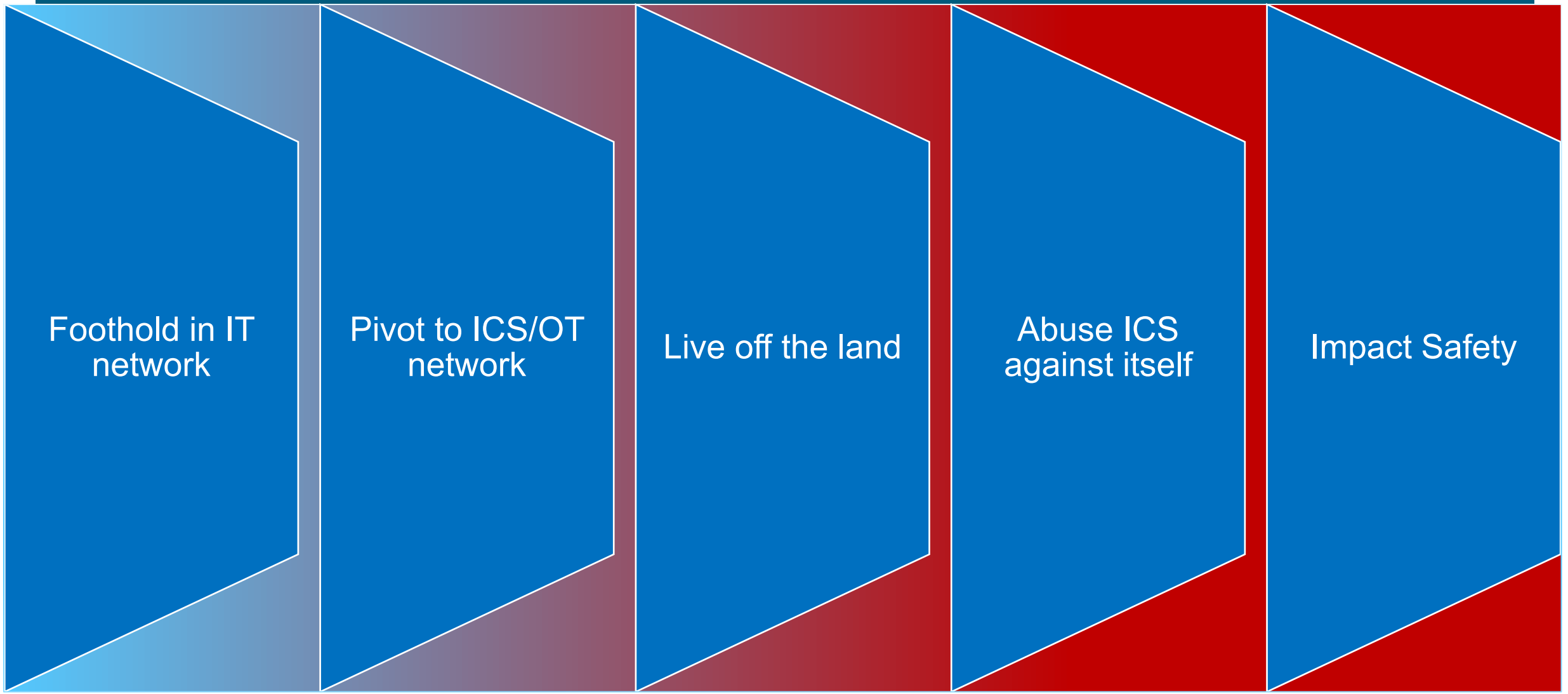
- Certified SANS Instructor
- *ICS515:ICS Visibility, Detection and Response*
- *NEW ICS418: ICS Security Essentials for Mangers (co-author)*

22 years IT & OT/ICS cyber defense
Telecommunications
Power power generation, transmission, distribution
Oil & Gas, refineries, marine, storage and fuel distribution
OT/ICS Security Assessments across multiple sectors

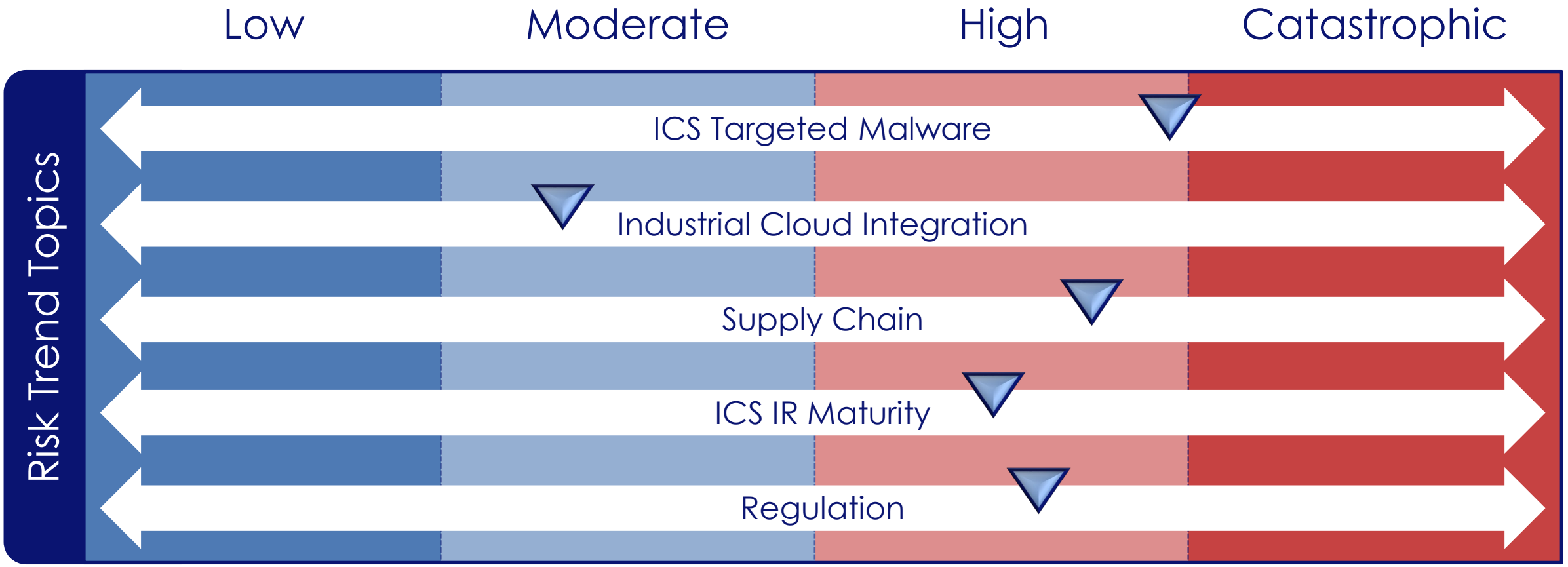

SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY
Only 52% of OT/ICS facilities actually have an ICS specific Incident Response plan. 17% are unsure whether they have such a plan.


SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY
38% of compromises to ICS comes from IT networks allowing threats into ICS networks.

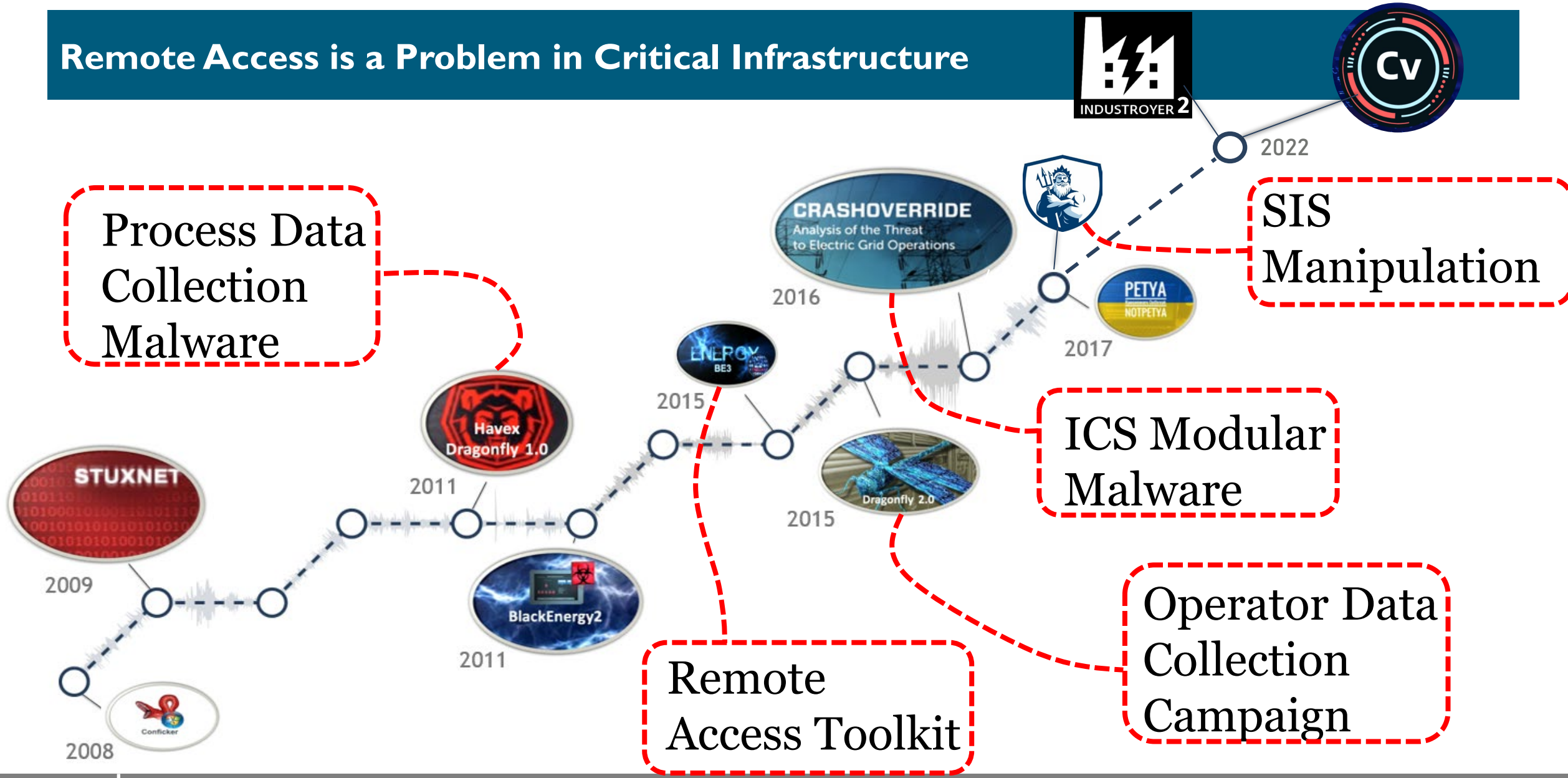
Related Business Case Walkthroughs (4)



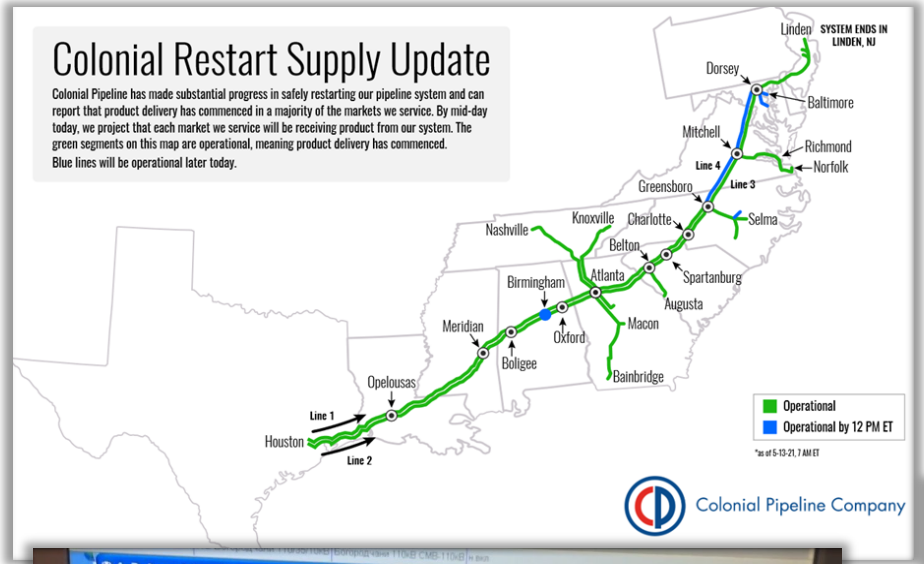
Trends 2023-2024

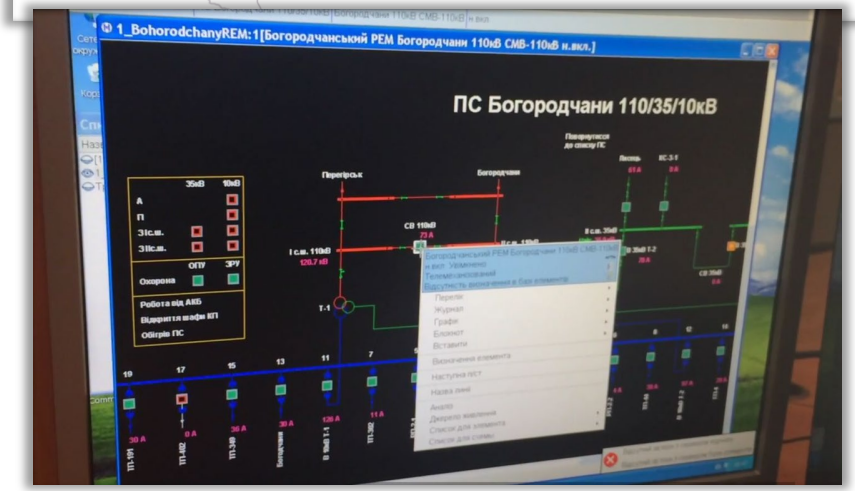


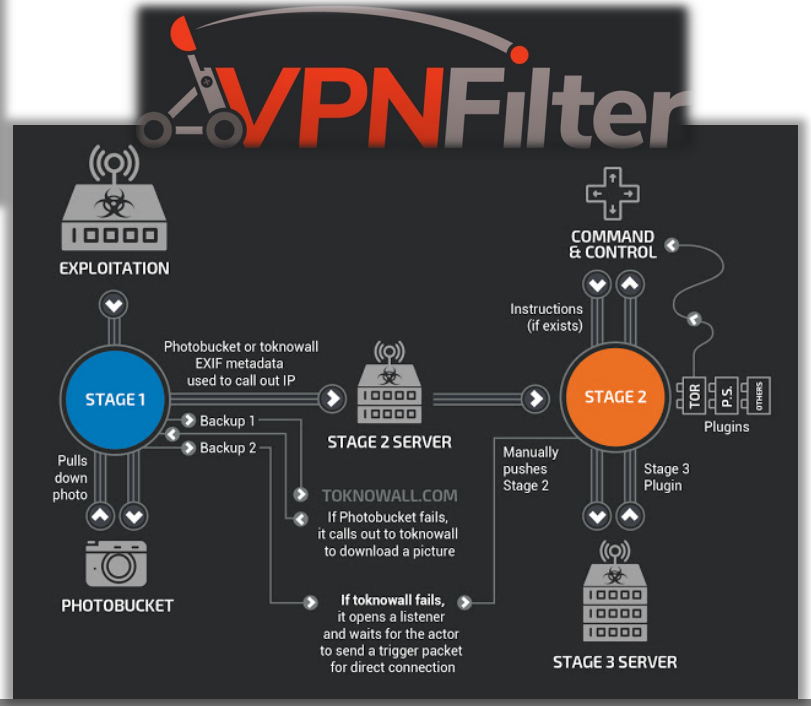
Remote Access is a Problem in Critical Infrastructure

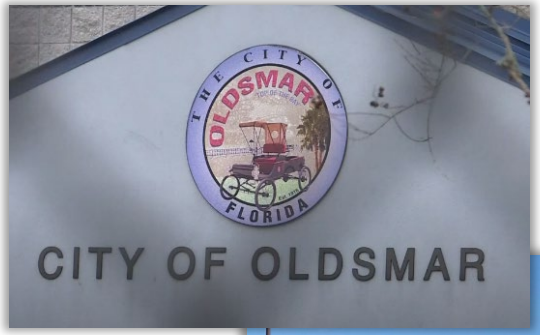


Remote Access is a Problem in Critical Infrastructure

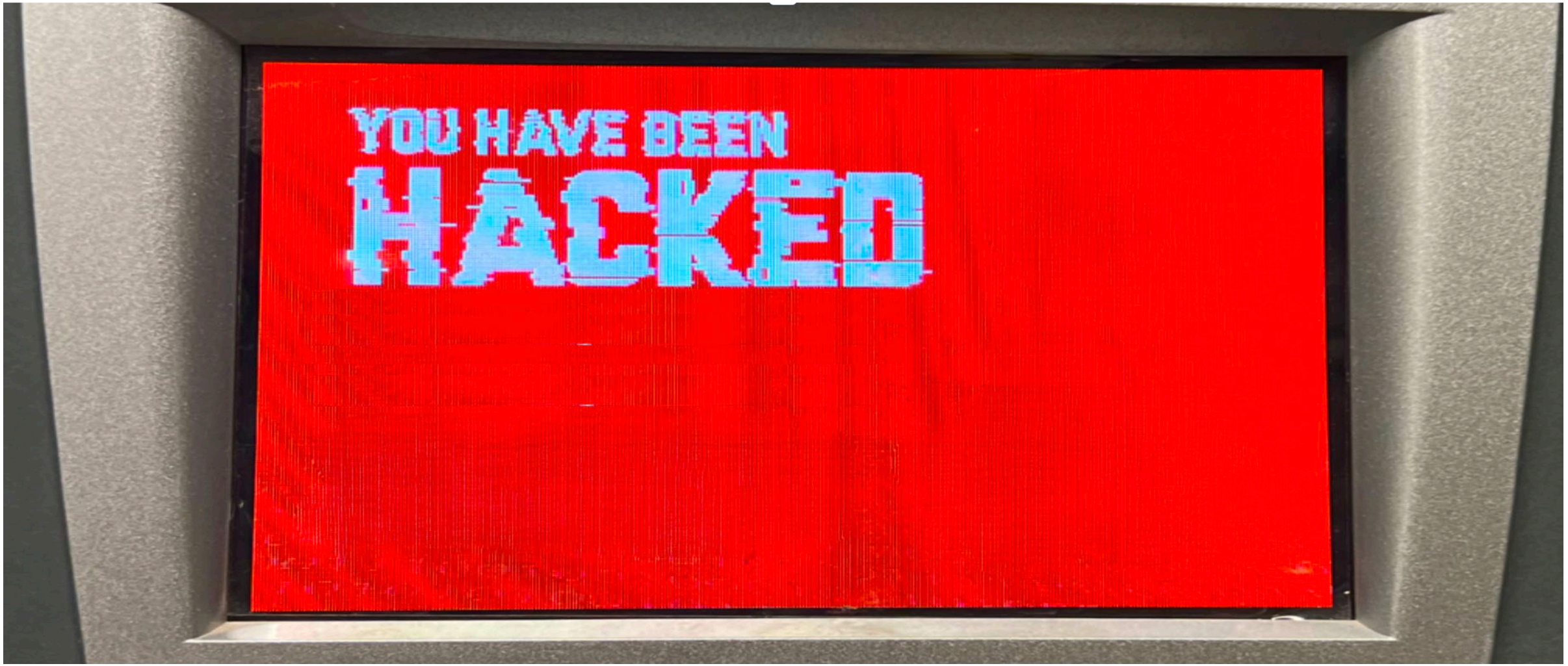




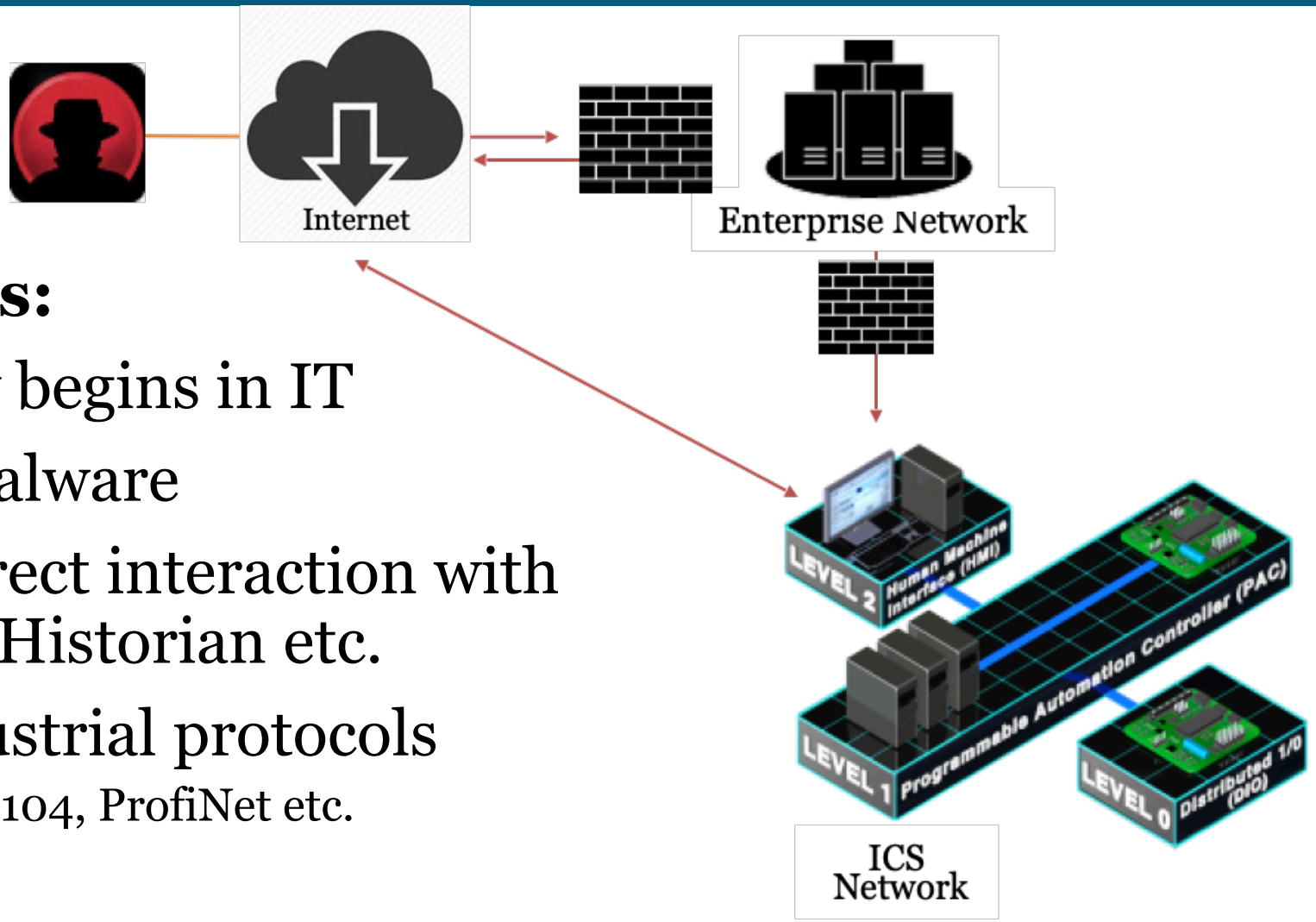




Remote Access is a Problem in Critical Infrastructure



Remote Access is a Problem in Critical Infrastructure



Threat Intel illustrates:

1. ICS attacks commonly begins in IT
2. ICS attacks not just Malware
3. ICS attacks include direct interaction with HMI, after pivot Data Historian etc.
4. ICS attacks abuse industrial protocols
   - OPC, DNP3, ModbusTCP, IEC-104, ProfiNet etc.

IT and OT/ICS Security Differences

- Safety of people and physical industrial assets
- Operational drivers
- Constraints that shape design, operations, maintenance
- Interactions with OT environments

Safety of People and Physical Industrial Assets (1)

Moving/Securing Data

IT

Vs.

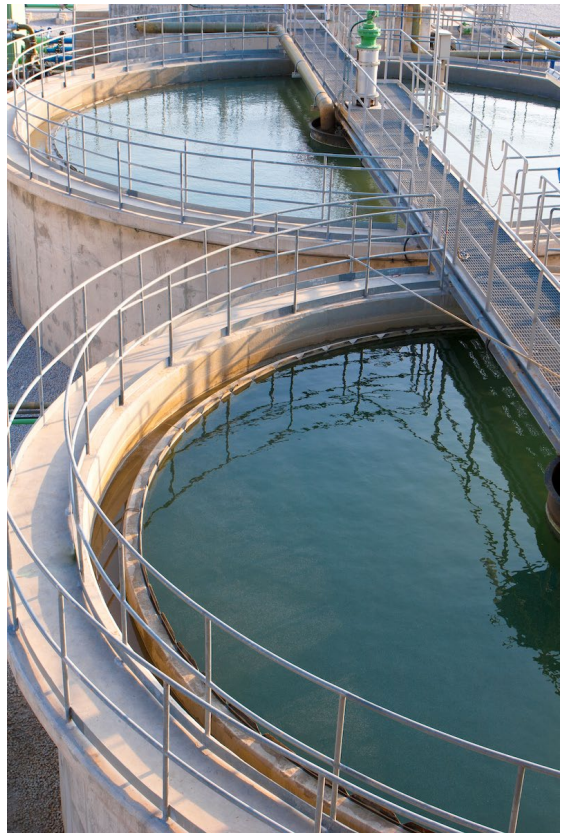
Enabling/Securing Physics

OT

- Industrial engineering control system assets are often compared to traditional IT assets. Traditional IT assets focus on data at rest or data in transit.

OT/ICS engineering processes and operating technology environments focus on managing, monitoring and controlling real-time systems for physical input values and controlled output physical actions.

Water Sector Equipment



Safety of People and Physical Industrial Assets (2)

Impacts

IT

Vs.

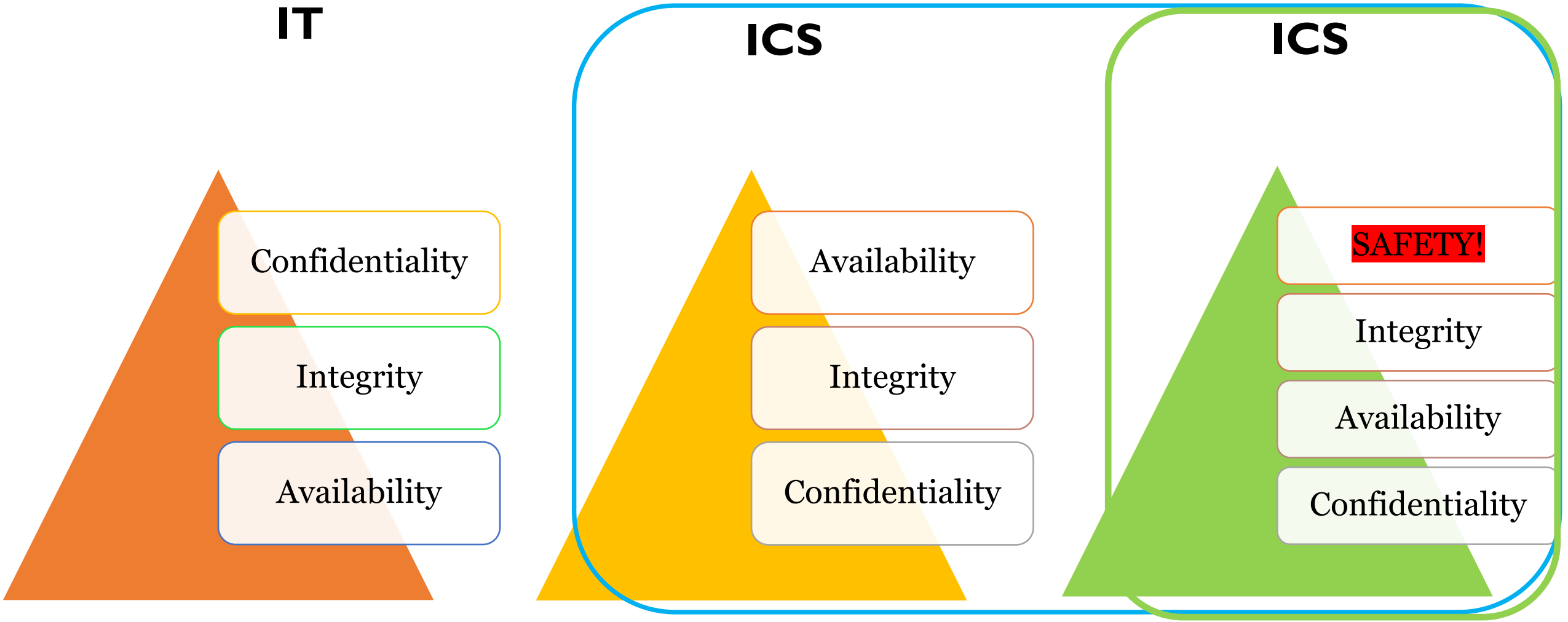
OT

IT INCIDENT	ICS INCIDENT
Business applications unavailable	Loss control of physical process
Data corruption	Manipulation of physical process
Data loss	Personnel Safety, loss of life

At a Glance…

	IT Systems	ICS/OT Systems
System Availability	Low/Moderate	24 x 7 x *Forever*
Data Integrity	Low/Moderate	*Very High*
Data Confidentiality	Low-High	Low
Time Criticality	Outages/delays tolerated	Critical
Operating Systems	COTS	COTS, RTOS, Embedded
Interoperability	Indifferent	Critical
Patching	Frequent	Infrequent/Impossible
Endpoint Protection	Common	Difficult/Impossible
Network Detection	Common	Uncommon
User authentication	Common	Uncommon/Impossible
Lifecycle	3-5 years	10-30+ years

ICS #1 Goal – Safety of People: The Process



IT Security, ICS/OT Security Controls Compared

SECURITY CONTROL	IT	ICS/OT
Antivirus	Signatures, heuristics - Quarantine	Whitelisting - Alerting
Firewalls	Segment - users, servers	Segment - business, process zones, Int. - PURDUE
Vulnerability Scanning	Regular internals, automated	Tested, run during maintenance window. Passive options.
Security Awareness	IT Users - Email, Data xFer, Web Surfing	Safety, Transient Devices, Architecture, Remote Access
Event Detection	Windows Event Logs, FW ACLs	RTU/PLC Changes, ICS Protocol Abuse
Incident On Asset	Wipe it! Patch It! Redeploy It!	Contain, Run ICS operations, clean next maint.
Patching	Monthly like clock work	Less frequent, compliance controlled
Network IDS/IPS	Intrusion Prevention System	Intrusion Detection System

Safety of People and Physical Industrial Assets (3)

Moving Data vs. Enabling Physics

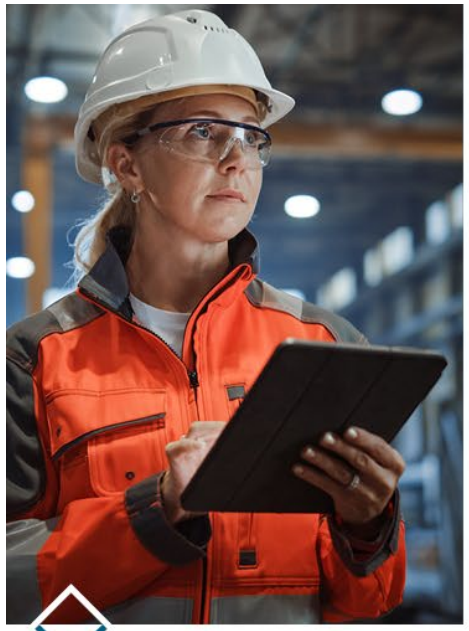
- Primary technical differences between IT and OT exist in these six areas:

SANS | ICS SECURITY

THE 5 ICS CYBERSECURITY CRITICAL CONTROLS

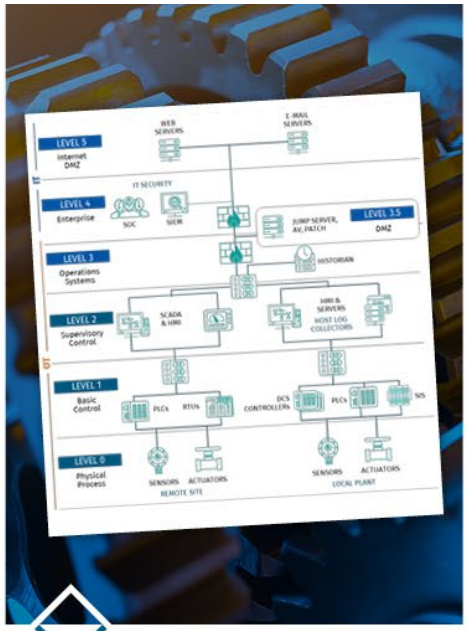
- When managers & practitioners come together, they naturally want to try to help in some way
- Other things exist and work, but..... there is always a “but...”
- Need for Action

Five Critical Controls for ICS/OT Cybersecurity



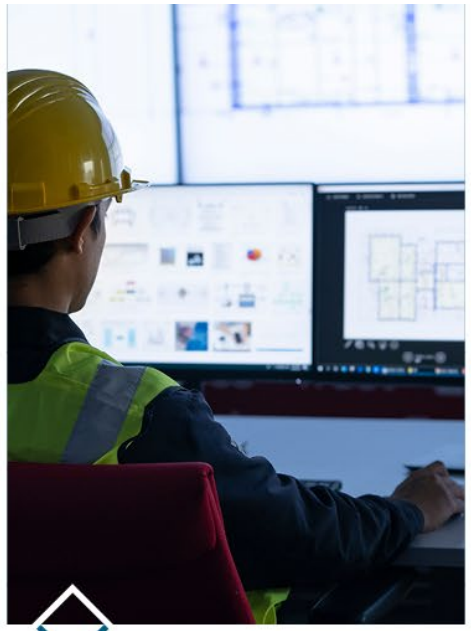
ICS INCIDENT RESPONSE

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.



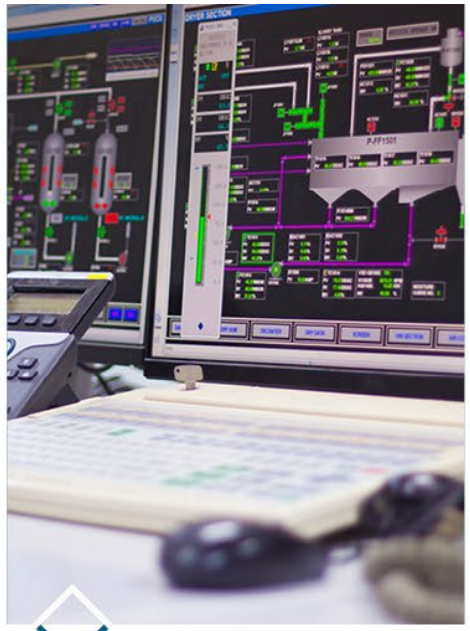
DEFENSIBLE ARCHITECTURE

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



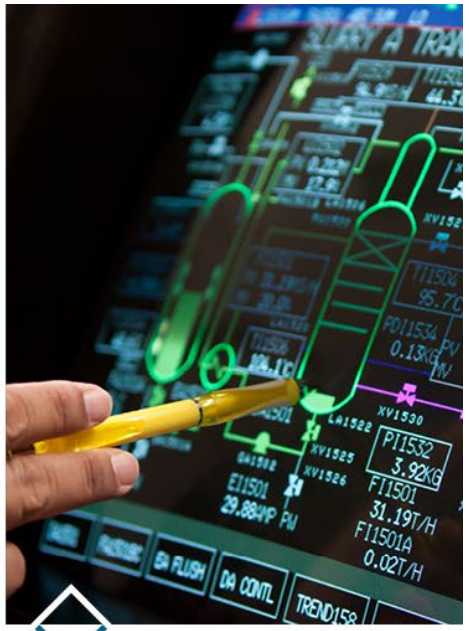
ICS NETWORK VISIBILITY AND MONITORING

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

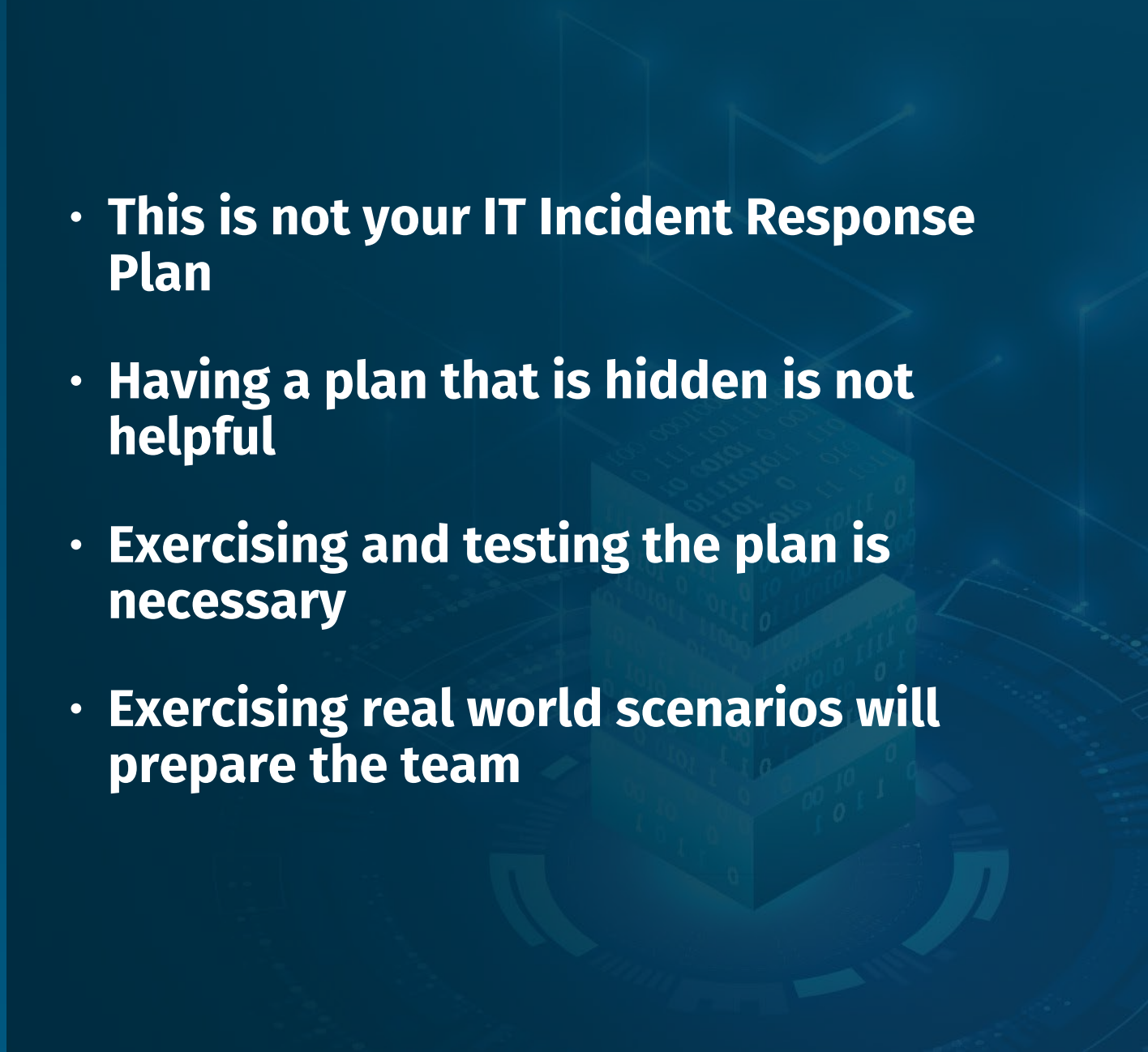
Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

SANS | ICS SECURITY

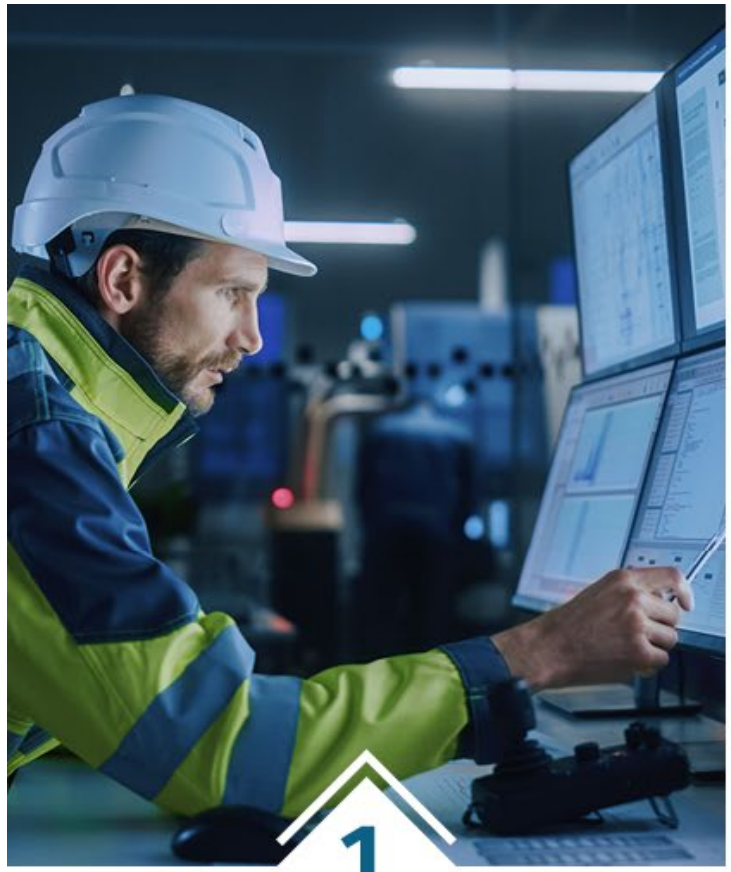
ICS Incident Response

If you do nothing else, you should at least have a plan

- This is not your IT Incident Response Plan
- Having a plan that is hidden is not helpful
- Exercising and testing the plan is necessary
- Exercising real world scenarios will prepare the team



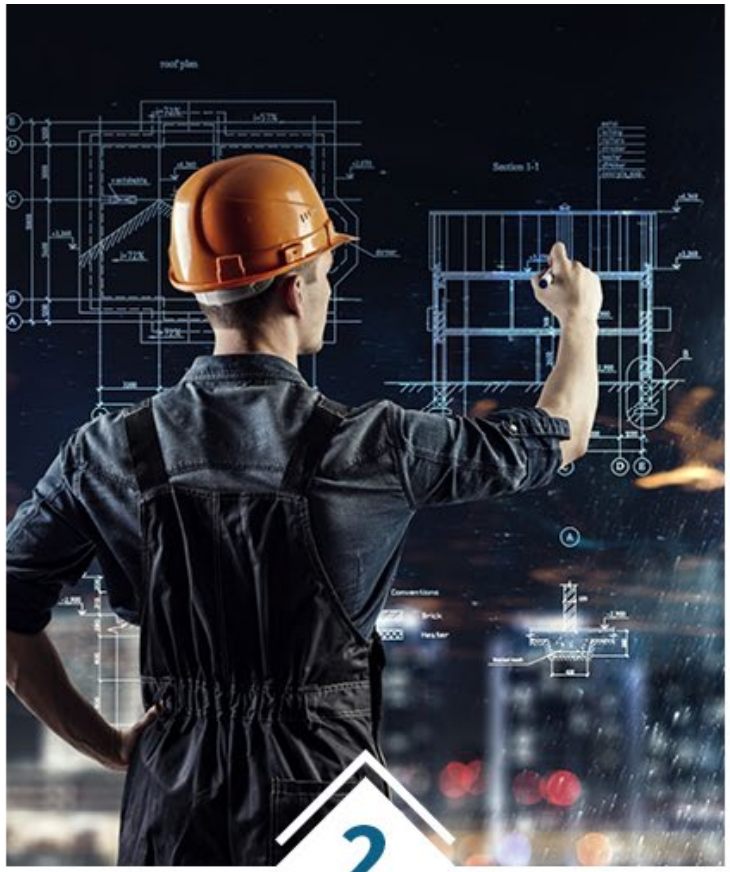
OT Incident Response Scenarios



1

Determine which scenarios pose the most risk and need to be defended against.

Look to real-world examples in your industry



2

CONSIDER CONSEQUENCE-BASED SCENARIOS.

Chart out what the adversary would need to do to complete the attack.

3

PERFORM A TABLE TOP EXERCISE *(TTX)*

Overlay scenarios against the organization's environments and sites

OT Incident Response

Breaking Down the ICS Assets Into Their Atomic Elements

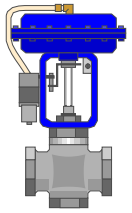
PLC

- Firmware
- Program
- Data
- Configuration
- Design Software

HMI

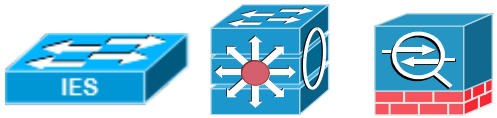
- Firmware
- Program
- Receipt Data
- Configuration
- Design Software

Smart Valves



- Firmware
- Configuration
- Design Software

Switches, Routers and Firewall



- Firmware
- Configuration
- Design Software

Server(s) and Applications

- Operating System
- O.S. Patches
- Applications
- Application Patches
- What "tweaks" were required to get the applications running

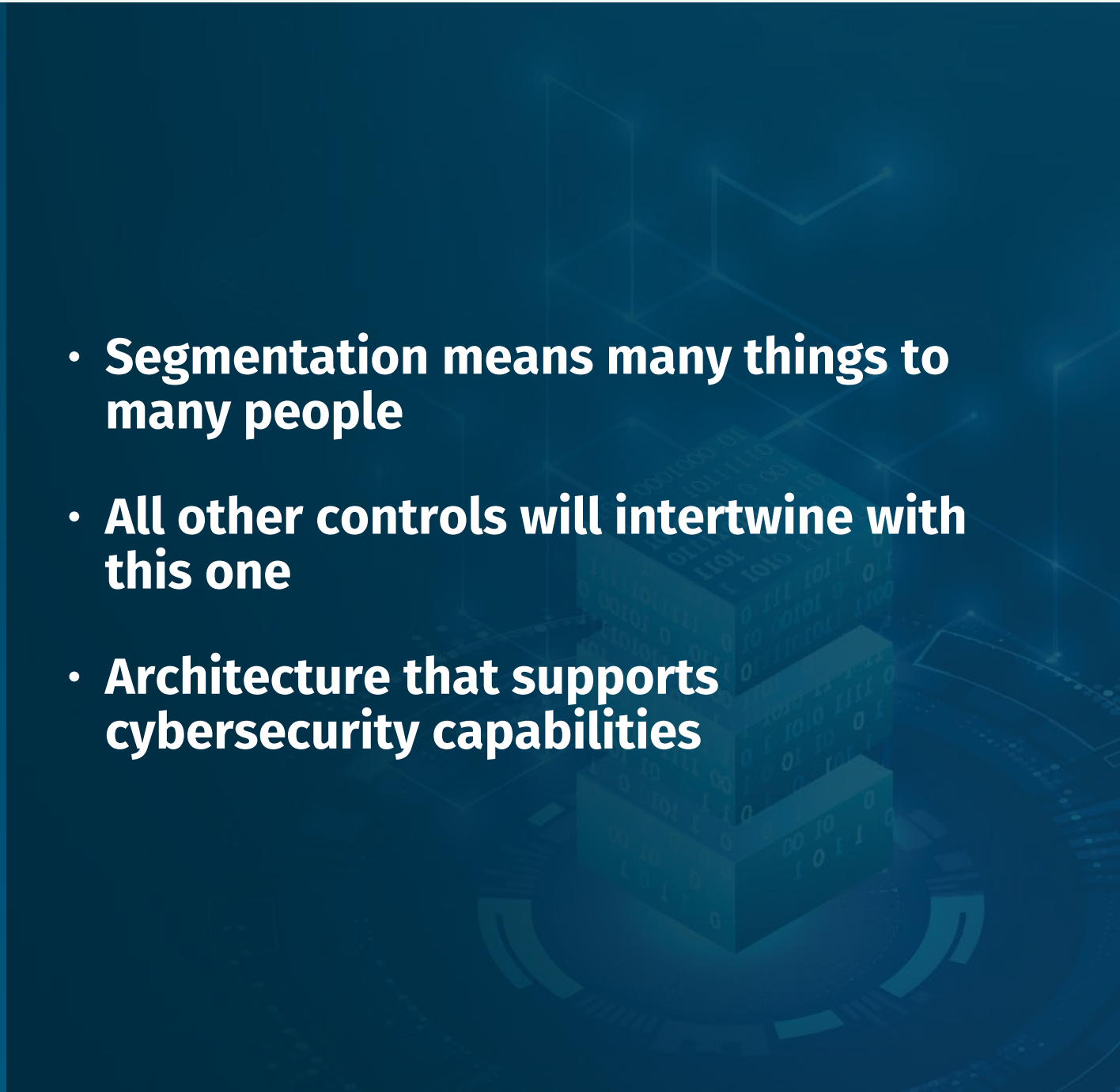
- Determining the fundamental building blocks within the ICS environment
- Practice rebuilding a system so you can when you are forced to do so
- Document and store configurations changes
  - What O.S. tweaks did you do to get the applications running
  - What firmware levels are the devices running at? Can you still get the running system firmware?
  - Licensing

SANS | ICS SECURITY

Defensible Architecture

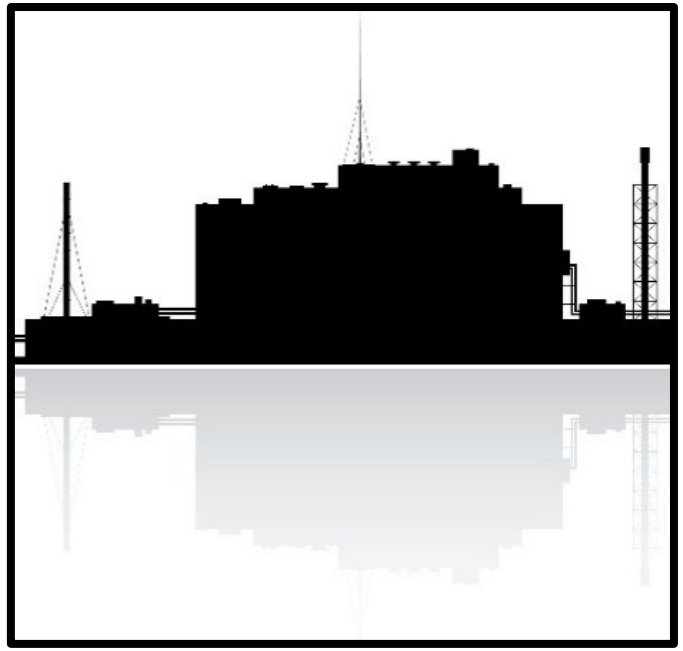
Going Beyond Segmentation and Perimeter Defense

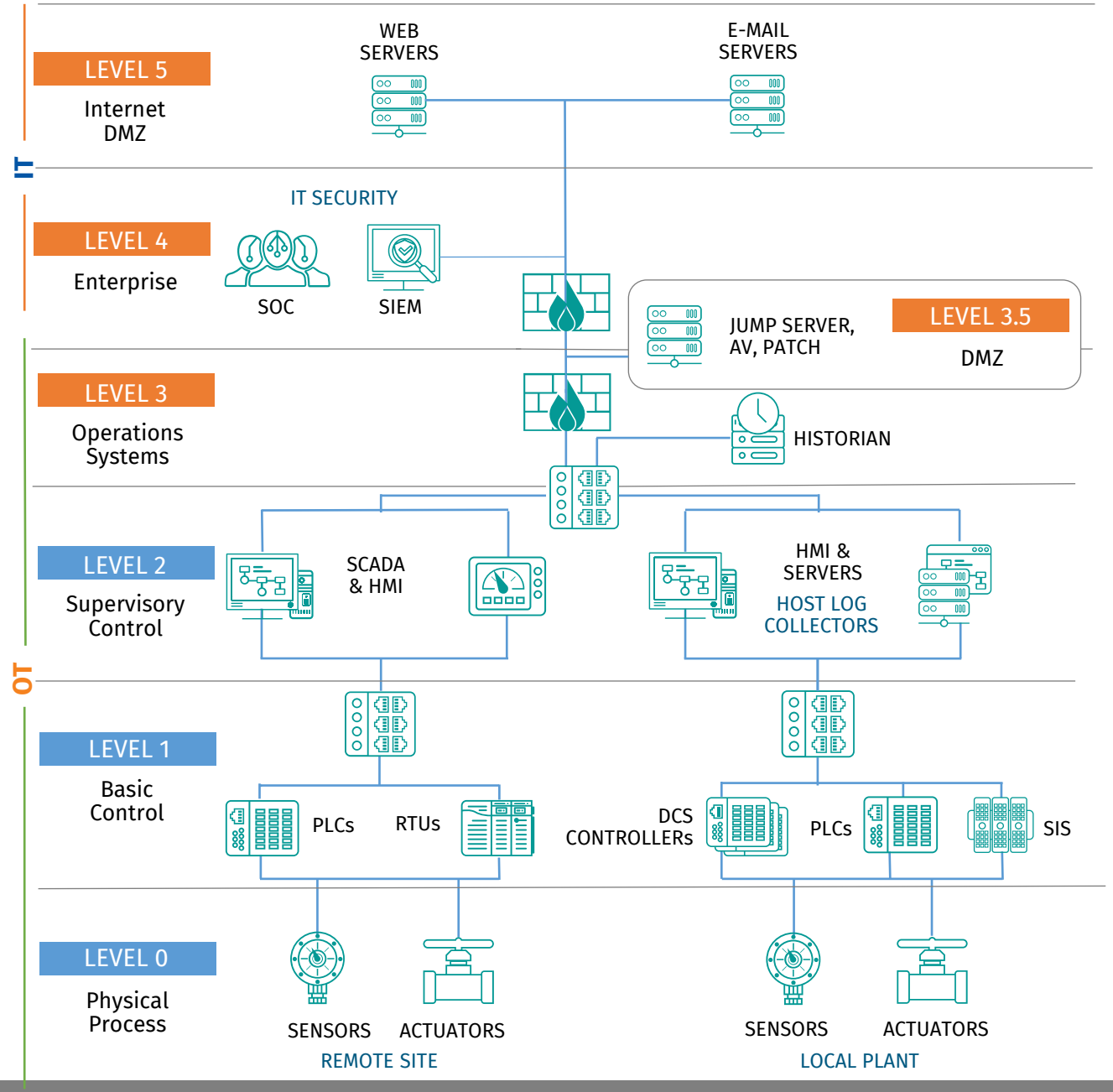
- **Segmentation means many things to many people**
- **All other controls will intertwine with this one**
- **Architecture that supports cybersecurity capabilities**



FUNDING BASED ON THREATS?

FUNDING TO PROTECT THE ACTUAL BUSINESS?





SANS | ICS SECURITY

ICS Network and Visibility Monitoring

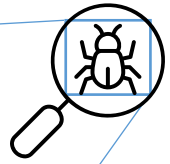
Elephant in the Room

- Why this was identified…. Not driven exclusively by day jobs
- Not just enterprise solutions
- ICS protocol specific capabilities
- Operationalized response actions
- Best fit deployment and solutions


SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY
Ranked #1 in importance to
ICS organizations: Deploying trained
OT security defenders to leverage
ICS specific network visibility.

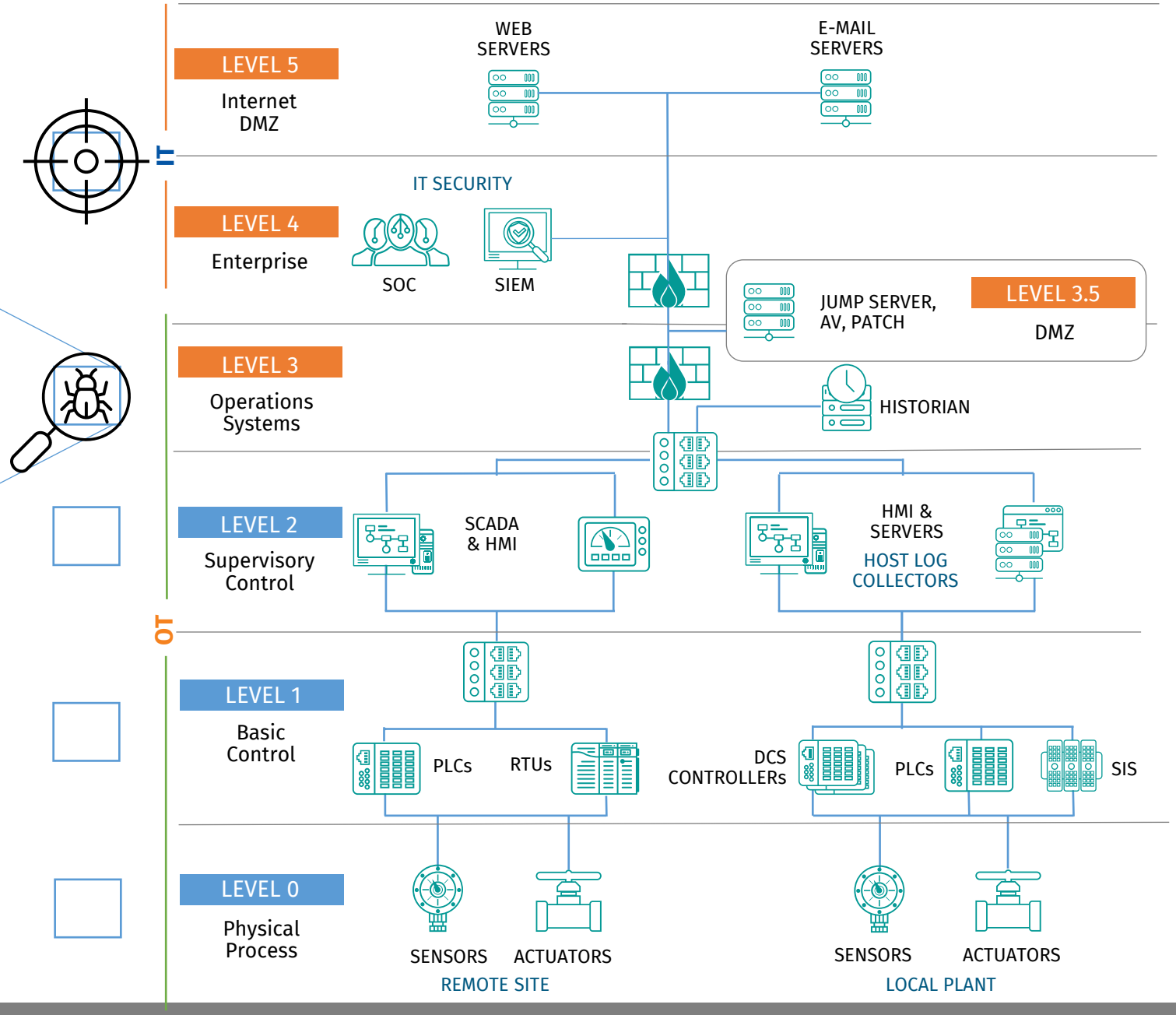
Visibility focus Across IT and OT

- Attacks from corporate IT networks that pivot to OT
- Attacks from vendor support IT networks that pivot to remote OT environments



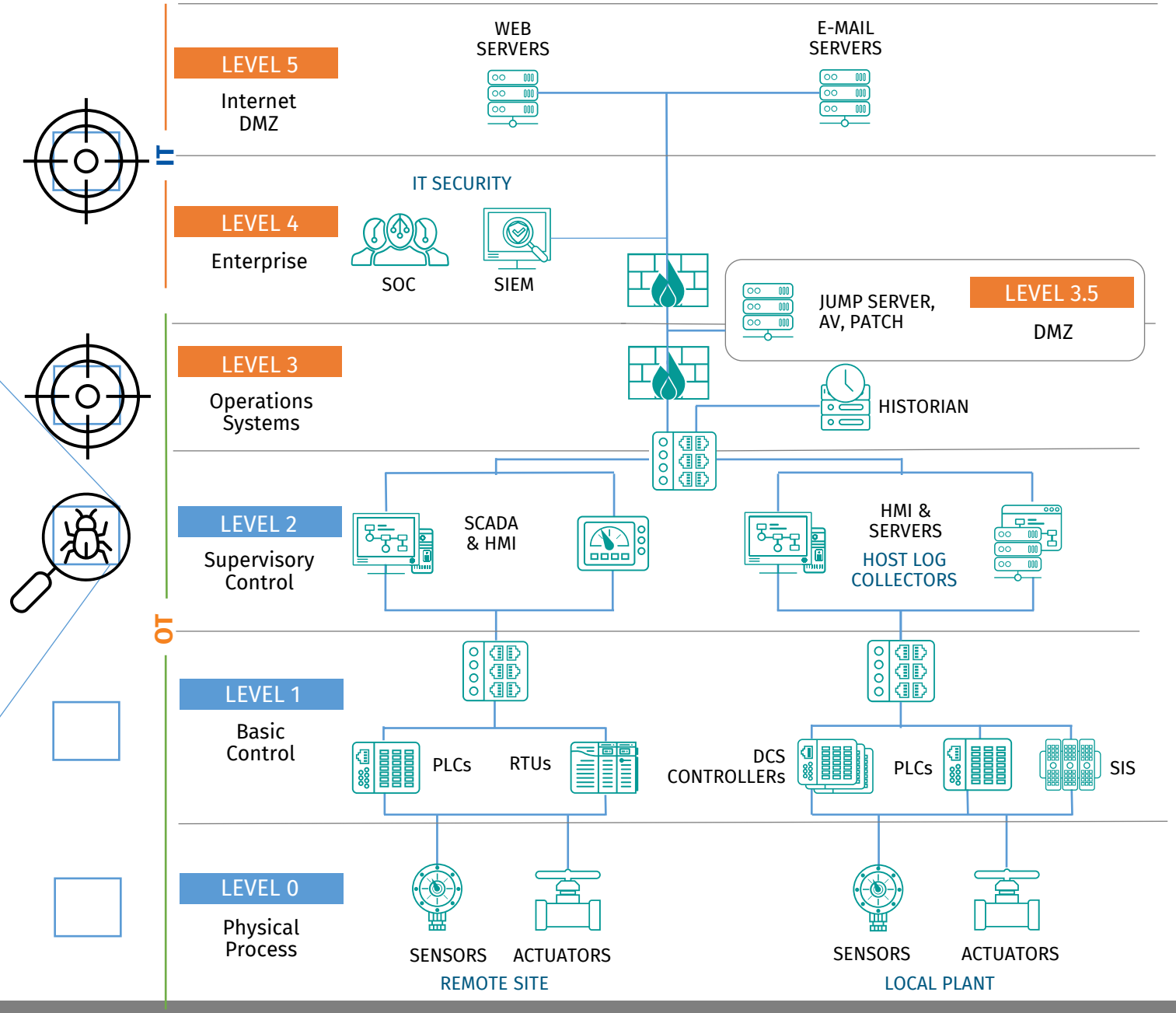
Visibility focus Across IT and OT

- Attacks targeting trusted communications and applications communicating in and out of ICS environments



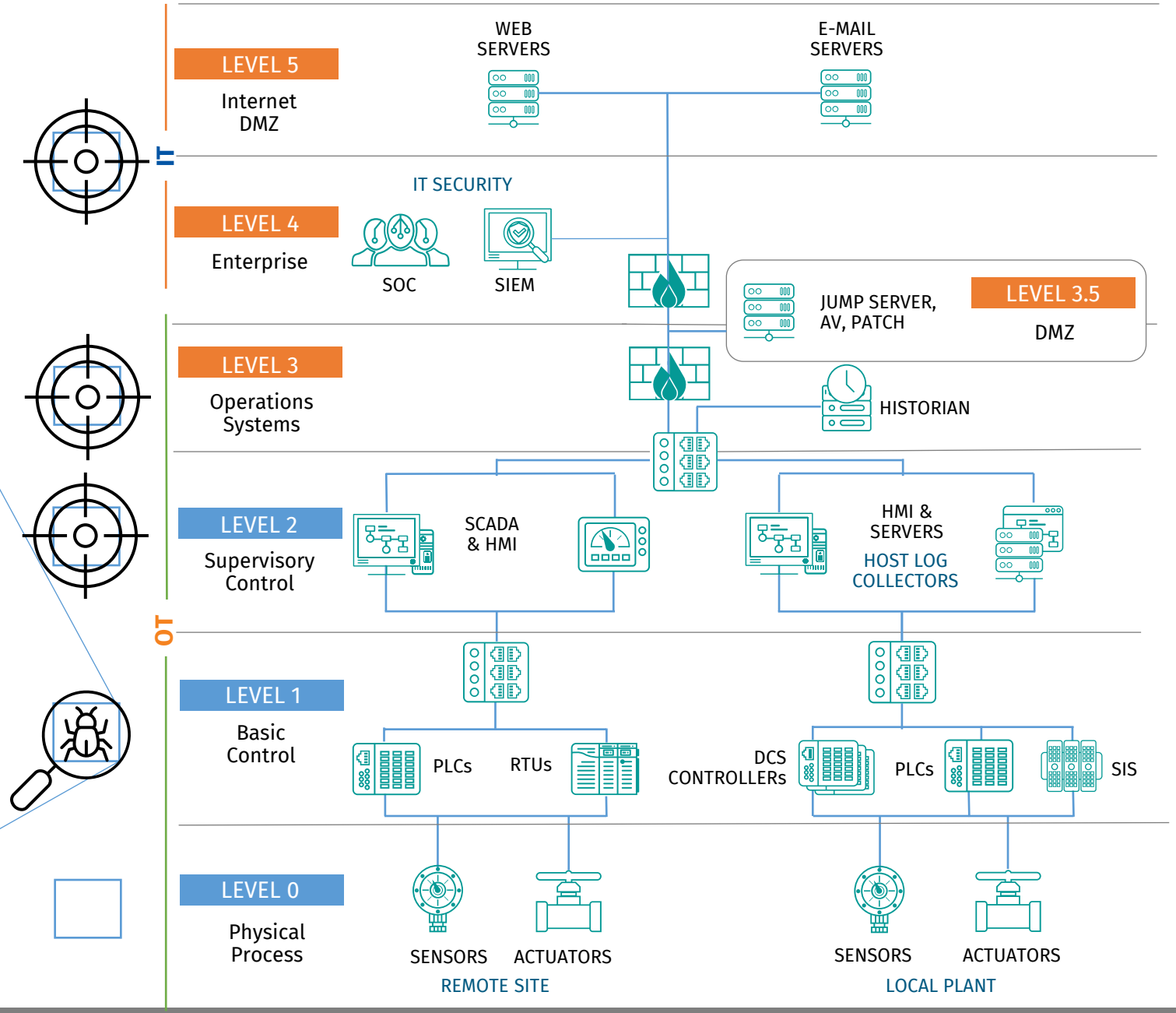
Visibility focus Across IT and OT

- Attacks utilizing engineering workstations to obtain connectivity, and configurations to develop or inform an ICS attack
- Attacks that mis-operate the control system through an operator workstation
- Attacks sending manipulated commands directly to field devices



Visibility focus Across IT and OT

- Attacks on supply chain lifecycles
- Attacks over direct OEM access paths
- Attacks directly targeting process controls – Access, Denial, Manipulation
- Combination attack targeting equipment

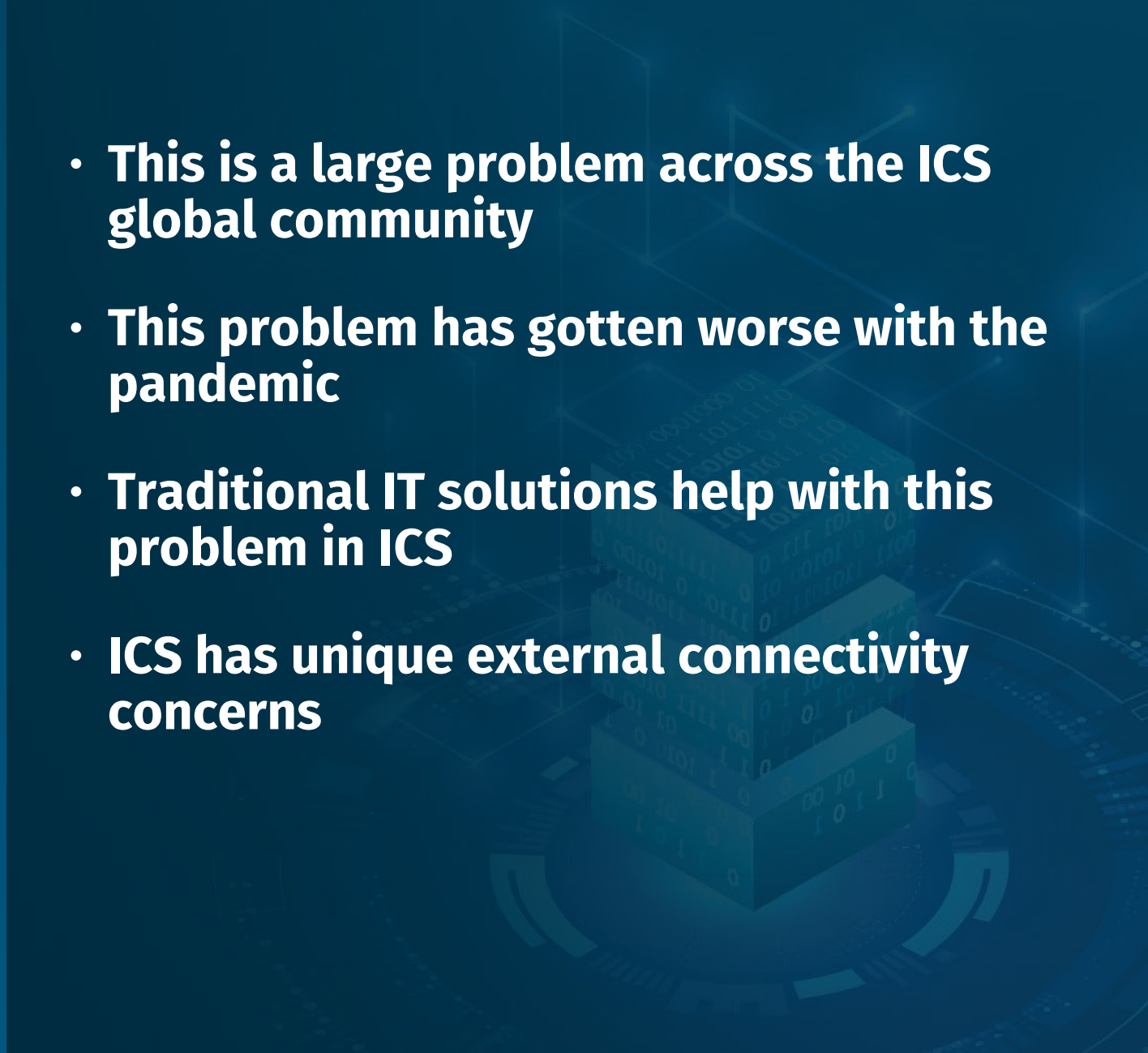


SANS | ICS SECURITY

Secure Remote Access

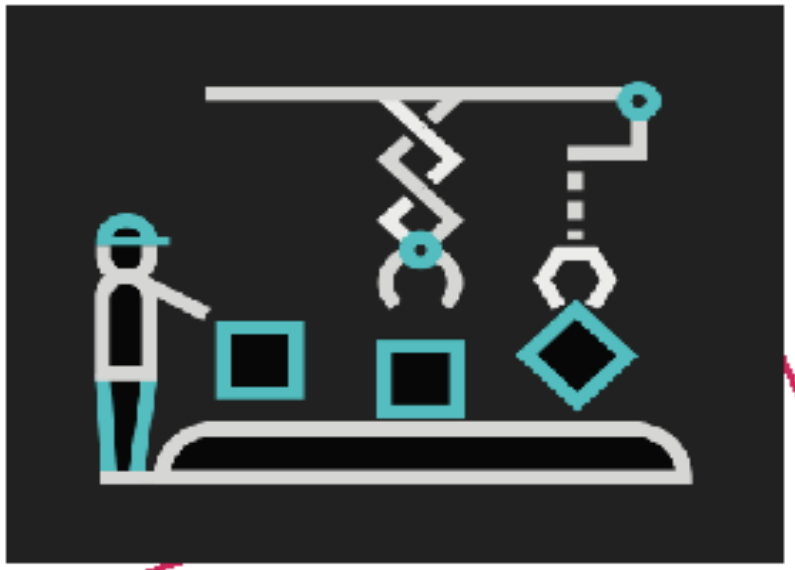
Trusted external communications

- This is a large problem across the ICS global community
- This problem has gotten worse with the pandemic
- Traditional IT solutions help with this problem in ICS
- ICS has unique external connectivity concerns

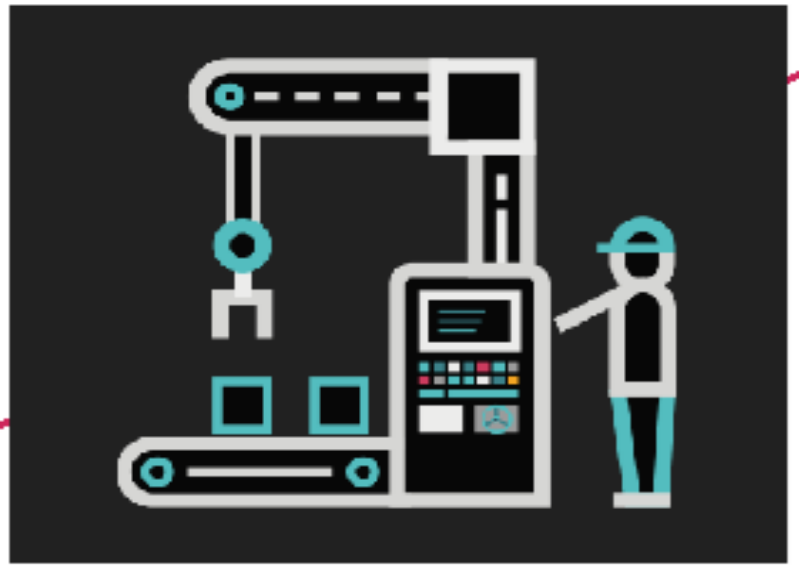


Evolution of Industrial Control Systems – and Connectivity

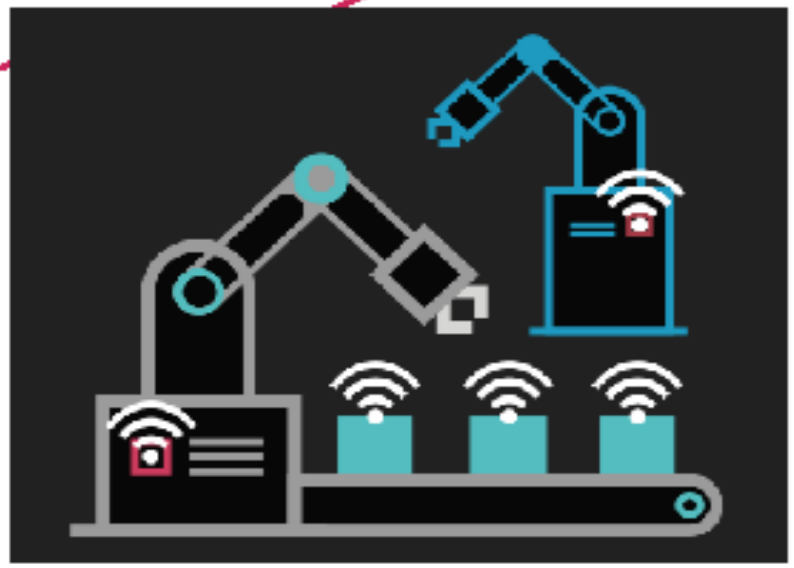
STAND-ALONE



LOOSELY CONNECTED



HIGHLY CONNECTED



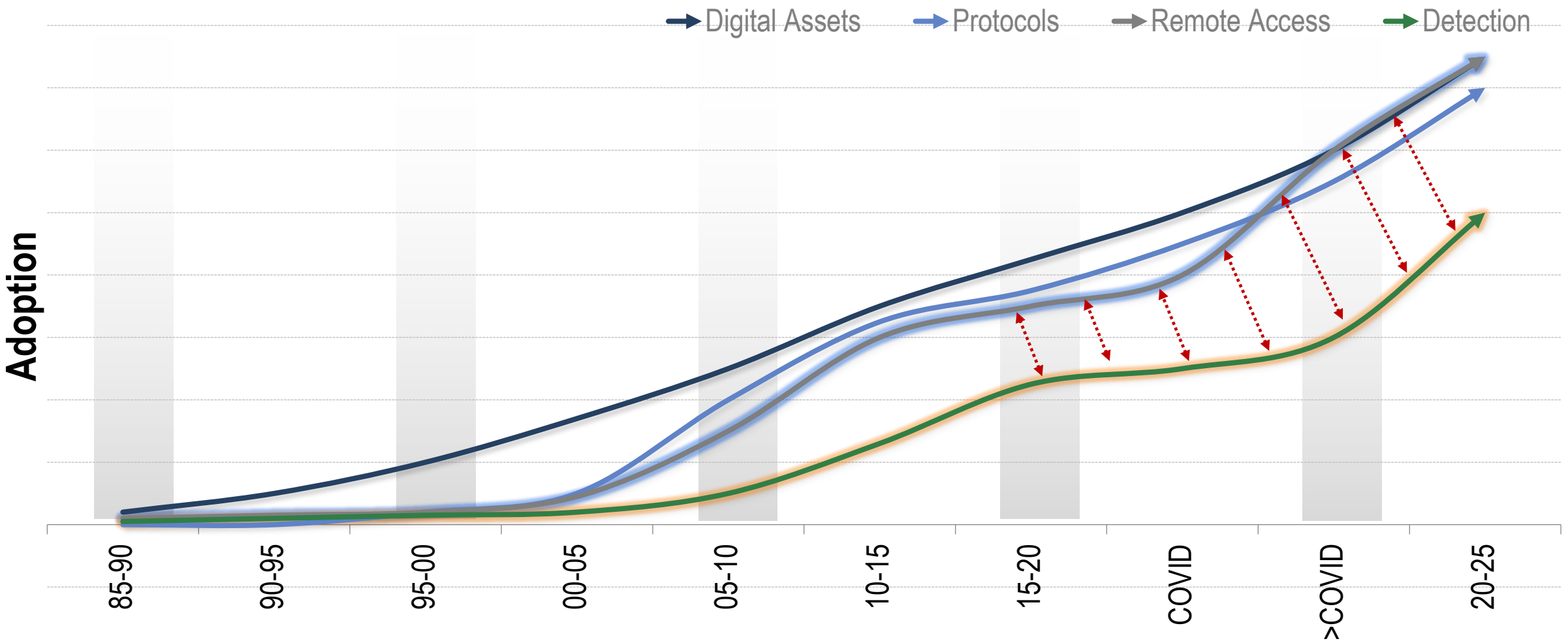
standardization

3rd Industrial Revolution
Automation of Production
by Electronics

DCS | Distributed Control System
SCADA | Supervisory Control &
Data Acquisition

4th Industrial Revolution
Smart Connected Systems
"Industry 4.0" // "Industrial IoT"

Evolution of Industrial Control Systems – and Connectivity

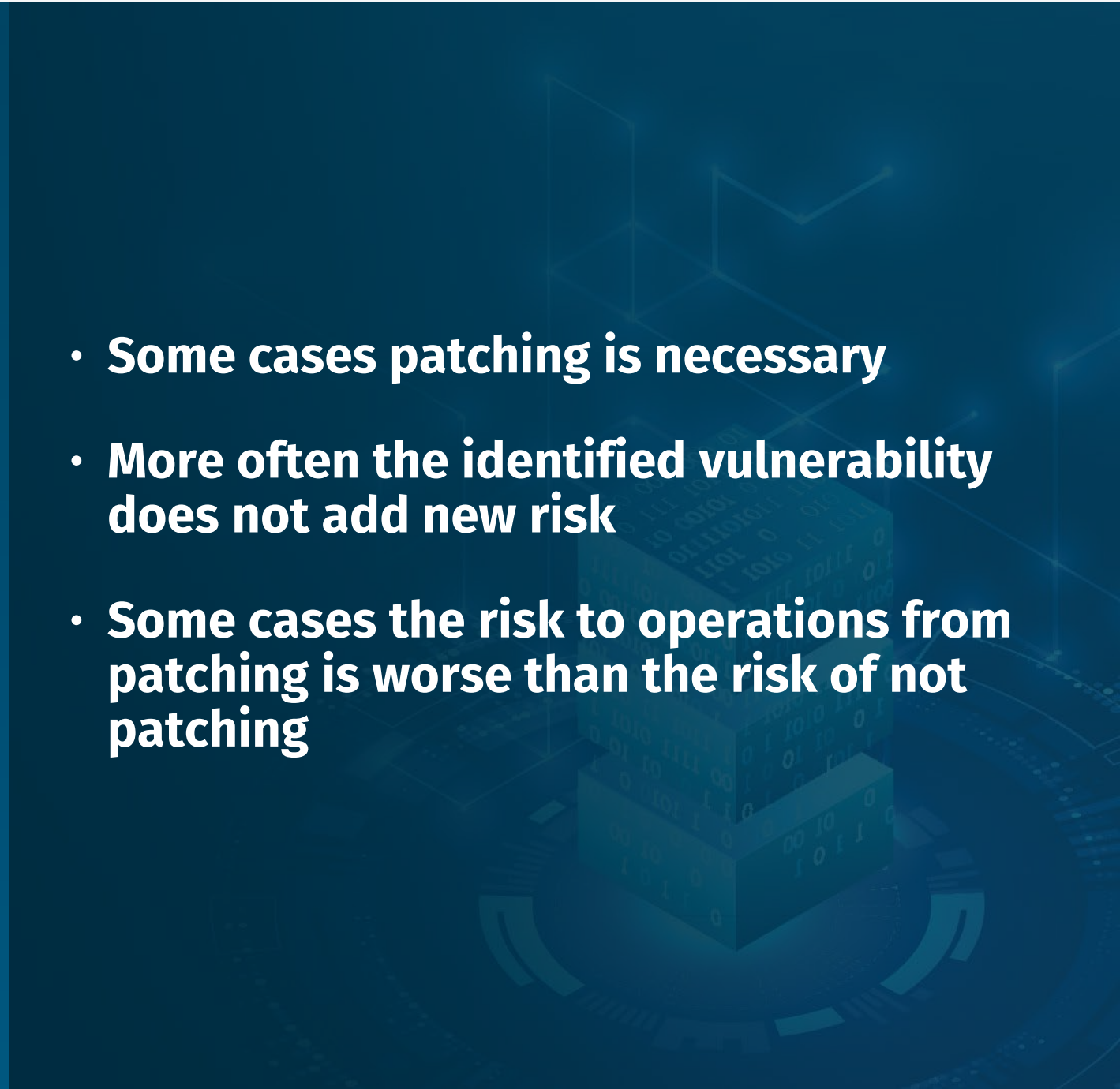


SANS | ICS SECURITY

Risk Based Vulnerability Management

Patching is not the only answer

- Some cases patching is necessary
- More often the identified vulnerability does not add new risk
- Some cases the risk to operations from patching is worse than the risk of not patching

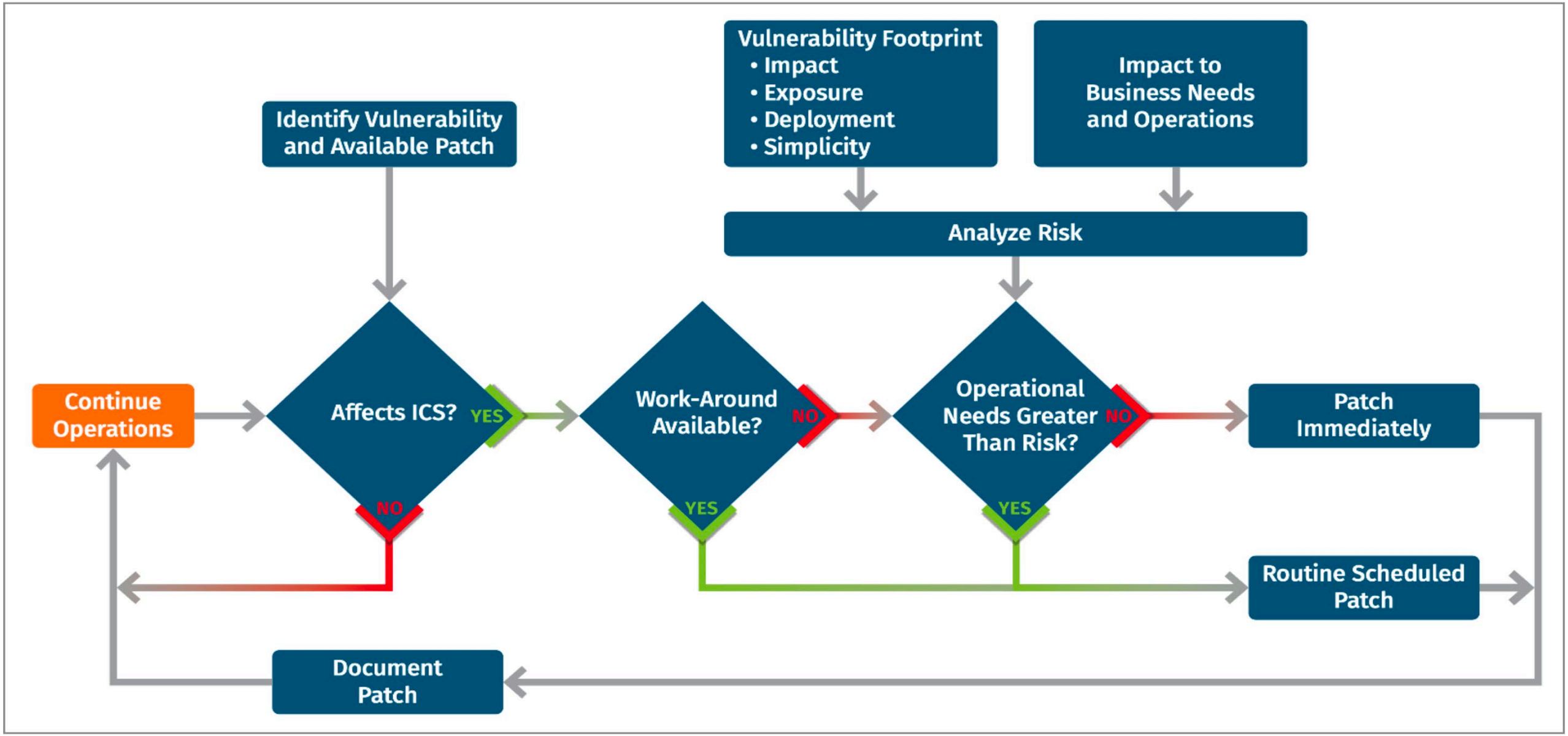


RISK-BASED VUL. MANAGEMENT – PATCHING CONSIDERATIONS

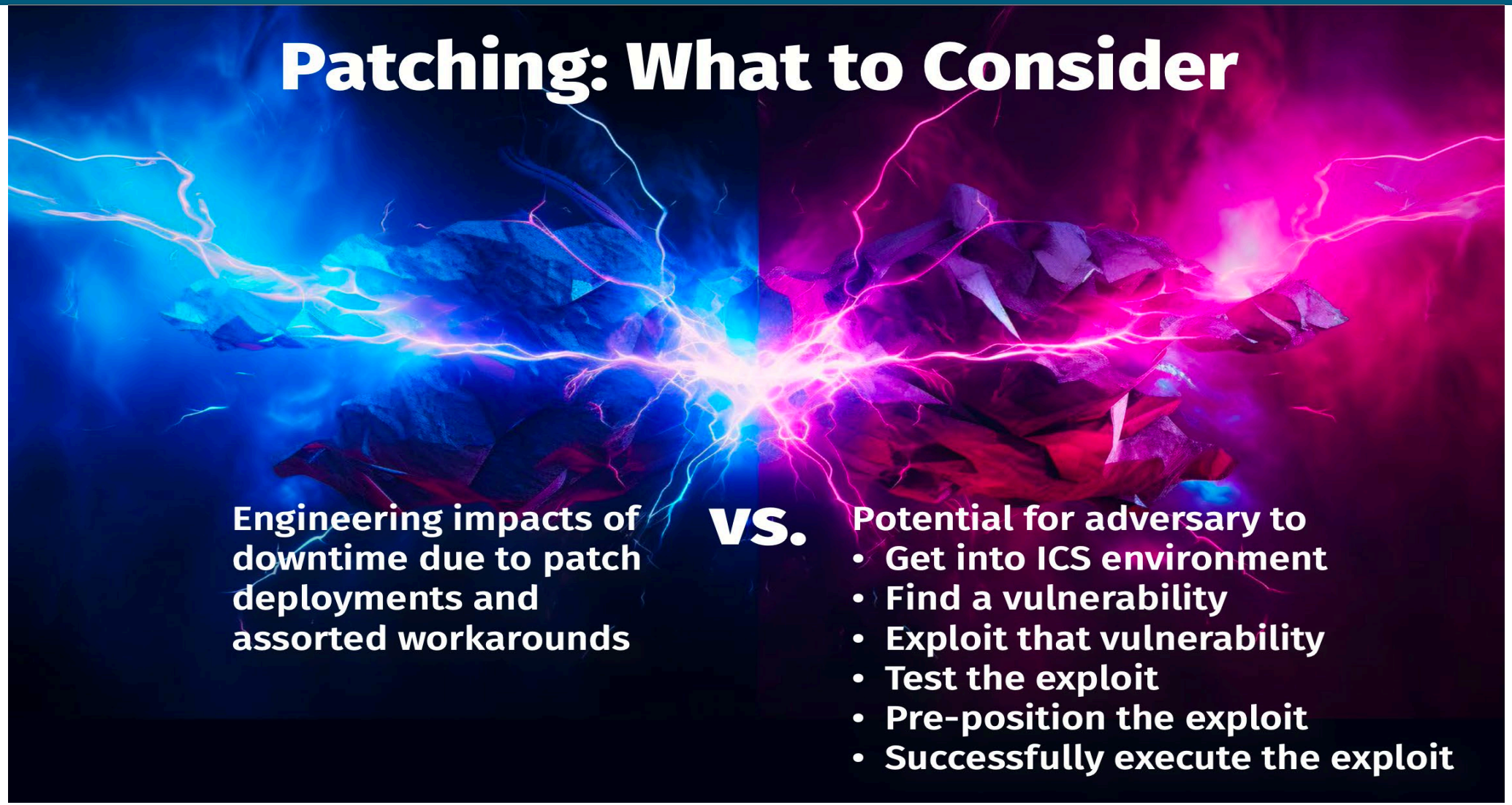
Patching is **not** the only answer

- Some cases patching is necessary
- More often the identified vulnerability does not add new risk
- Some cases the risk to operations from patching is worse than the risk of not patching
- Best patch in engineering scheduled maintenance windows
- Take a risk-based (prioritized approach to ICS patching, always)

RISK-BASED VUL. MANAGEMENT – PATCHING CONSIDERATIONS



RISK-BASED VUL. MANAGEMENT – PATCHING CONSIDERATIONS



SANS | ICS SECURITY

THE REQUIRED Leadership Role

- Top level support and buy in is required
- This is not purely a technical problem to solve
- These controls cannot be viewed as a project to be completed, there are ongoing operational process elements
- There is a balance of the 5 controls and leadership enabling actions

SANS | ICS SECURITY

LEADERSHIP TAKE AWAYS

1

Strategic Move #1

Position the team and budget for the highest return on investment by focusing first on network architecture. All defense controls and processes built on top of a strong network architecture, and strictly controlled segmentation from hostile networks, will have a much higher return on investment and protect that which matters most. Other add-on benefits are for containment during industrial incident response conditions.

2

Strategic Move #2

As a leader in ICS cyber risk management, position your team to be recognized as enabling engineering tasks and supporting operations staff. ICS/OT network visibility is not just about ICS security and industrial incident response. Ensure all the benefits of ICS/OT network-specific visibility are known, communicated to the teams, and support a budget for this type of technology.

SANS ICS

THANK YOU!

ASSOCIATION OF METROPOLITAN WATER AGENCIES

ICS DEFENSE IS DOABLE! 🤝 🛡 🏭

SANS ICS

ANY QUESTIONS?

ICS DEFENSE IS DOABLE! 🤝 🛡 🏭