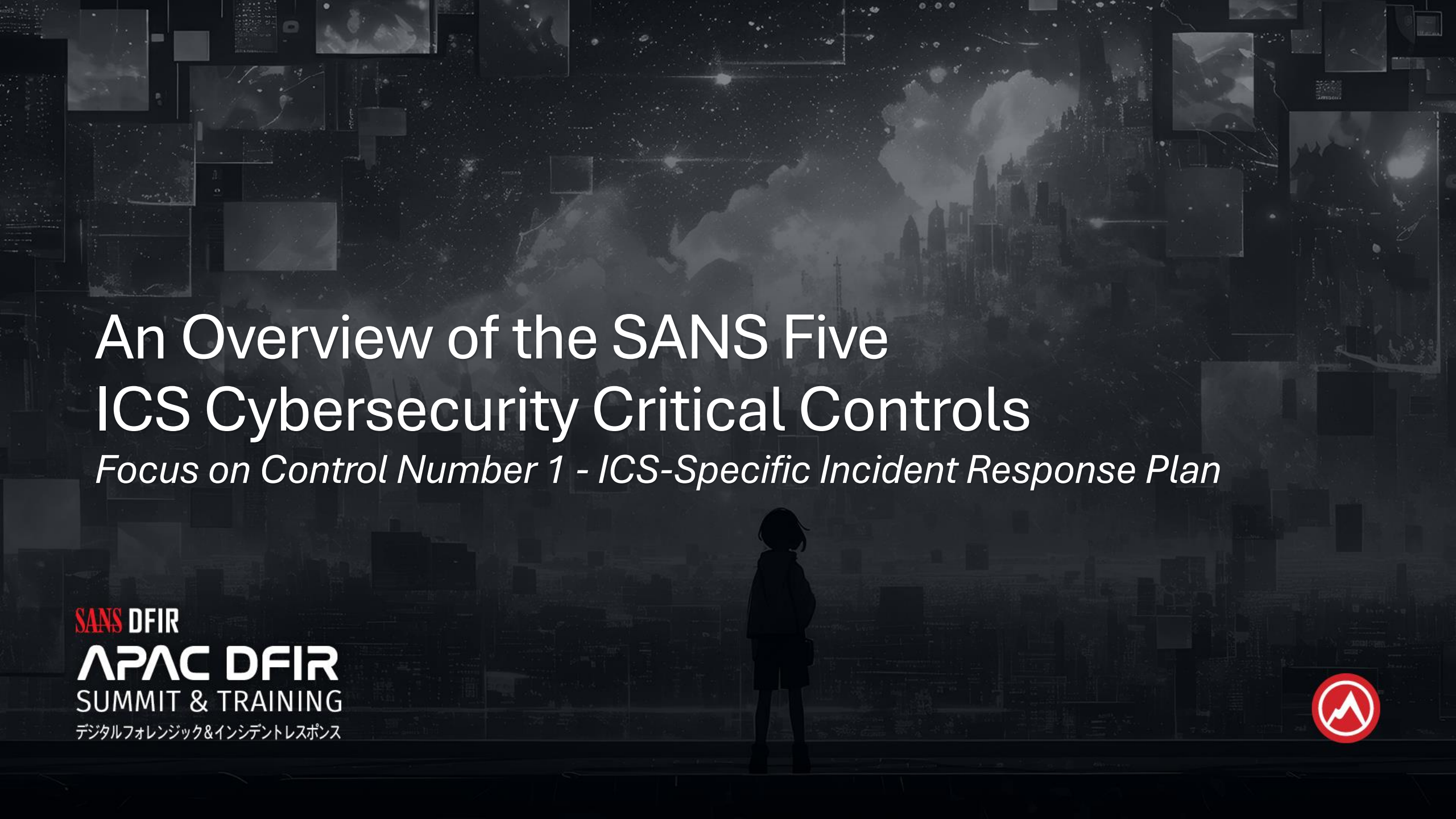


An Overview of the SANS Five ICS Cybersecurity Critical Controls

Focus on Control Number 1 - ICS-Specific Incident Response Plan

SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

/whoami

- Cyber Security Architect with an interest in OT Active Defense and Cyber Security Operations
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Worked in Electricity Generation and Transmission, Rail, Aviation, Emergency Services and Consulting
- Chartered Professional Engineer (CPEng) in Information, Telecommunications and Electronics Engineering (ITEE)
- Bachelor Engineering (Telecomms) QUT and Master Business (Applied Finance) QUT

Agenda

1. A brief overview of Operational Technology & Industrial Control Systems
2. The SANS Five ICS Cyber Security Critical Controls
3. Deep Dive into Critical Control #1 – ICS Specific Incident Response Plan
4. Key OT Incident Response Concepts from ICS515
5. SANS ICS Security Community Resources
6. Summary

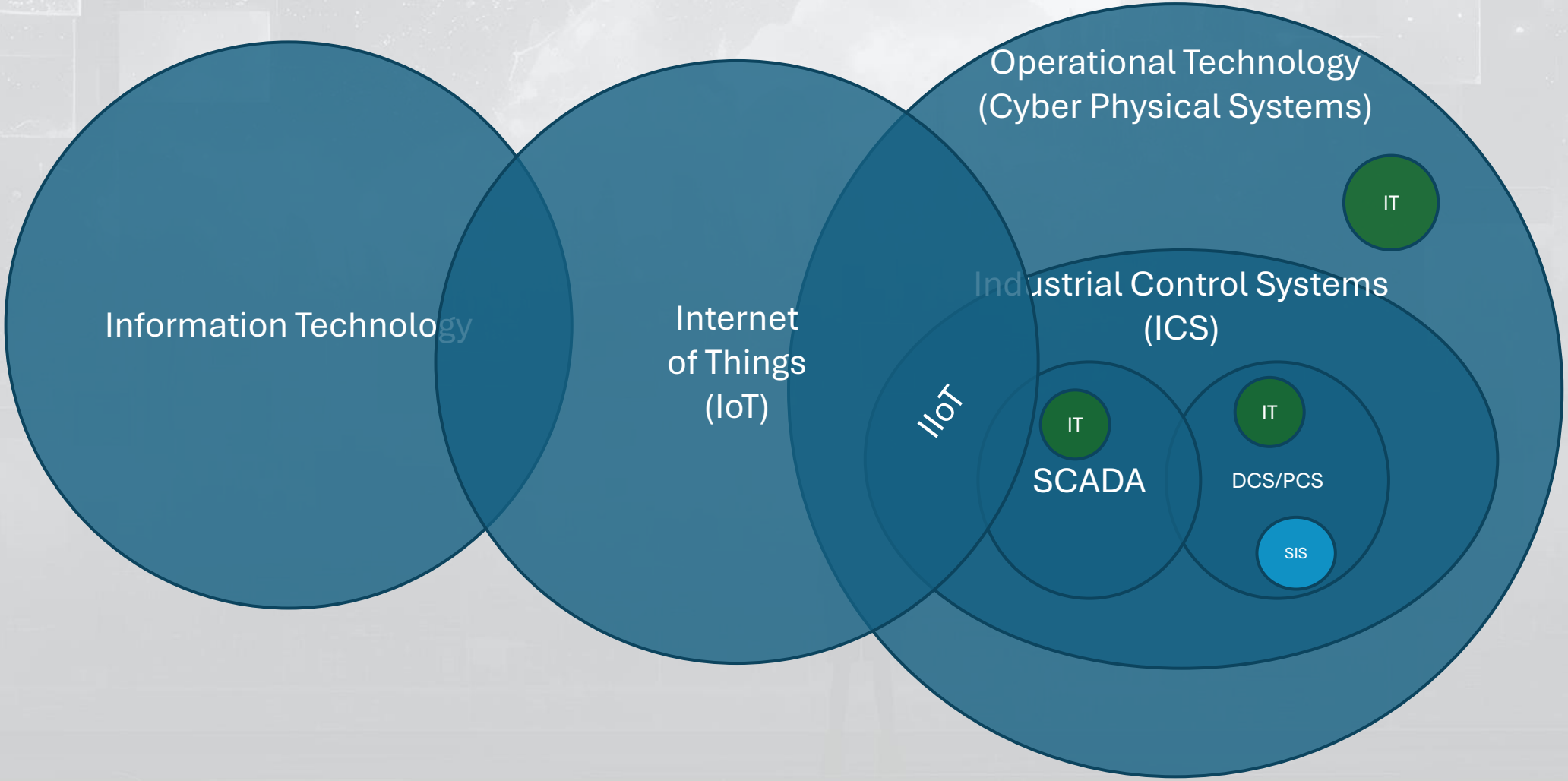
SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

A brief overview of Operational Technology and Industrial Control Systems

What is Operational Technology (OT)

- Operational Technology are the systems that monitor and control the physical world
- It is a nebulous term and is also referred to as:
  - Industrial Control Systems
  - Cyber Physical Systems
- The International Society of Automation (ISA) Defines Industrial Automation and Control Systems (IACS) as -
  - *“Collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.”*

What is Operational Technology (cont.)

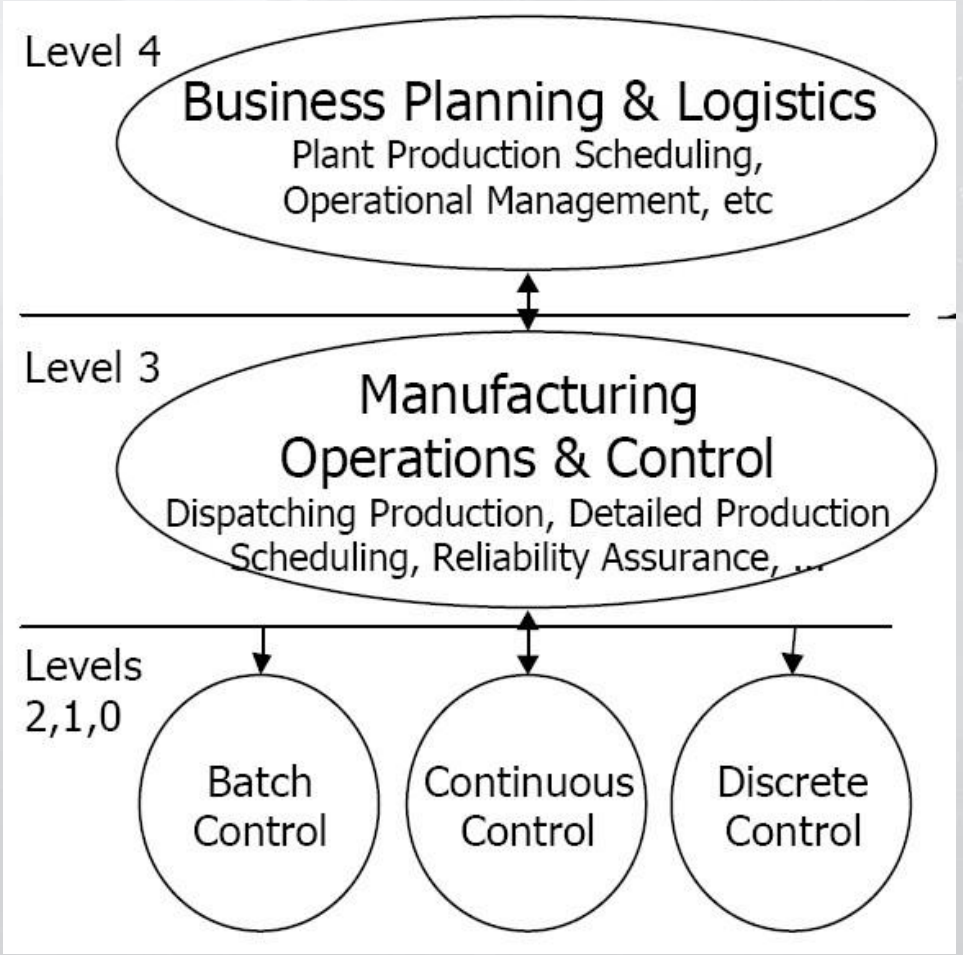


Key OT Assets

- SCADA/Control Server/DCS Server
- Human Machine Interface (HMI)
  - Operator Work Stations (OWS)
  - Local HMI
- Engineering Work Stations (EWS)
- Local Controllers
  - Programmable Logic Controller
  - DCS Controller
  - Remote Terminal Unit
- Safety Instrumented System (SIS)

The Purdue Enterprise Reference Architecture (PERA)

- Often referred to as the “Purdue Model”
- Is often mistaken as a network segmentation model …
- Rather, it is a **functional model** and describes time
- Referenced by ISA-95 to describe how to integrate IT and ICS Networks in the 1990s



Ref - https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

ICS-CERT Recommended Architecture

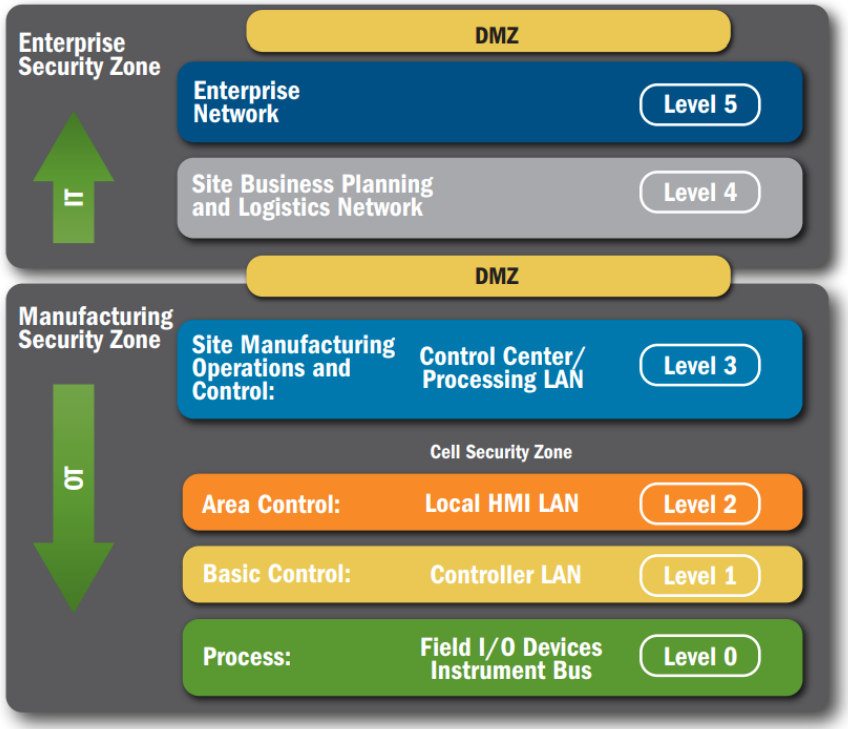


Figure 6. Zone segmentation of business & ICS architecture.

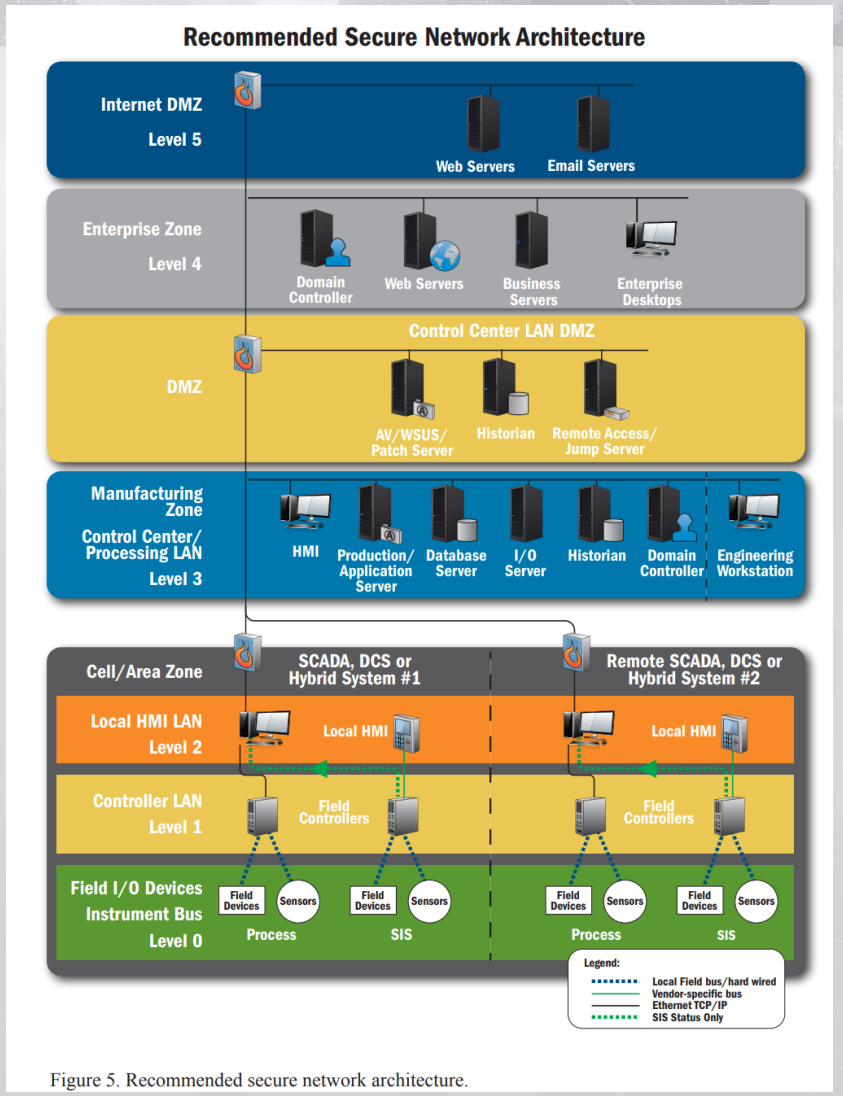
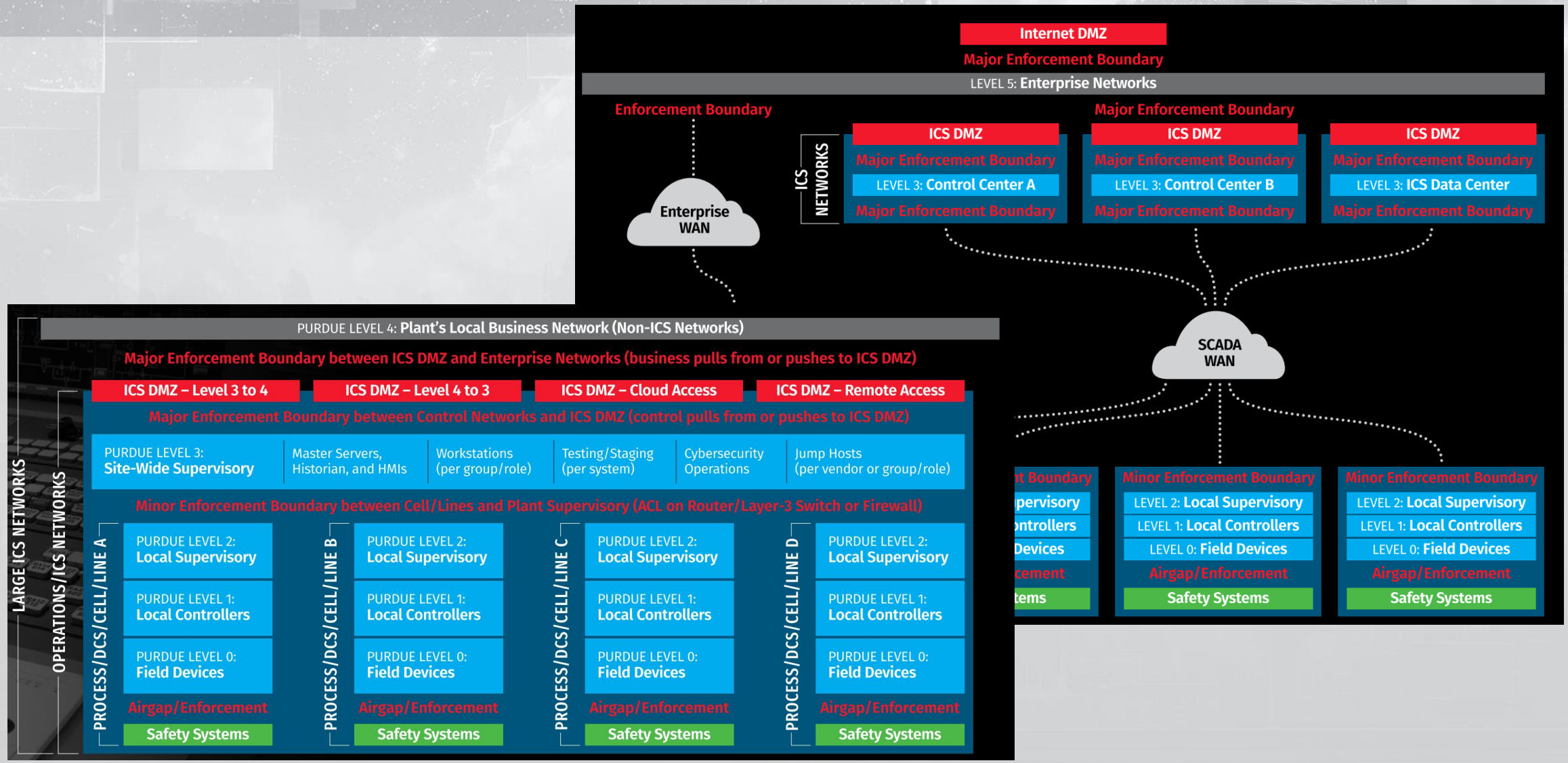


Figure 5. Recommended secure network architecture.

Ref - https://www.cisa.gov/sites/default/files/2023-01/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

The SANS ICS410 SCADA Reference Model



Source - https://www.sans.org/posters/control-systems-are-a-target/

MITRE ATT&CK for ICS

ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

View on the ATT&CK® Navigator

Version Permalink

Initial Access 12 techniques	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Source - https://attack.mitre.org/matrices/ics/

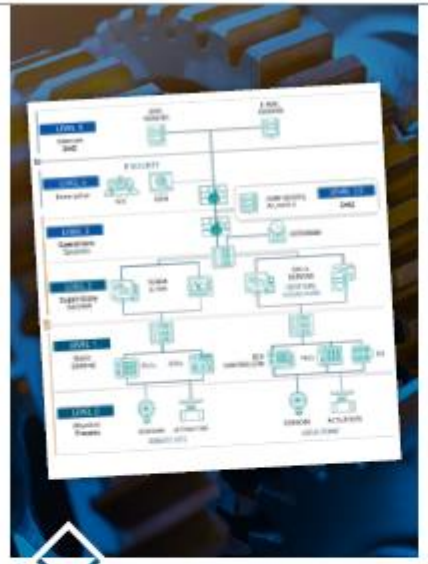
SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

The SANS Five ICS Cybersecurity Critical Controls

The Five ICS Cyber Security Critical Controls

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

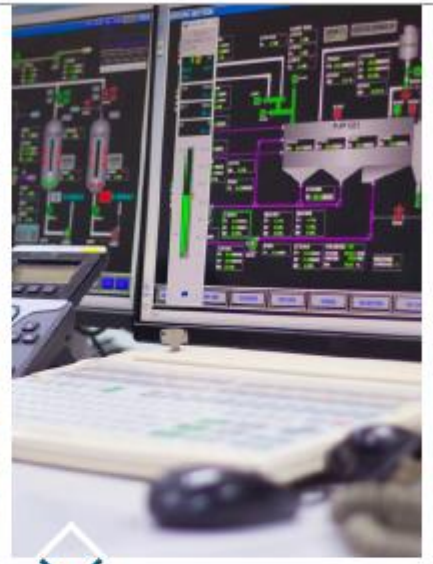


DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

ICS NETWORK VISIBILITY 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

Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

#1 ICS Incident Response

- Starting with the end in mind
- Understand Risk Scenarios and Prioritise remediation and investment efforts
- Your Scenario Planning should start with real world incidents and be cyber threat intelligence informed
- Consider worst case high-consequence scenarios as well but don’t become overwhelmed
- Critical that you tabletop the scenarios and prepare
- We will come back to go into this one in more detail later in this presentation

ICS INCIDENT RESPONSE

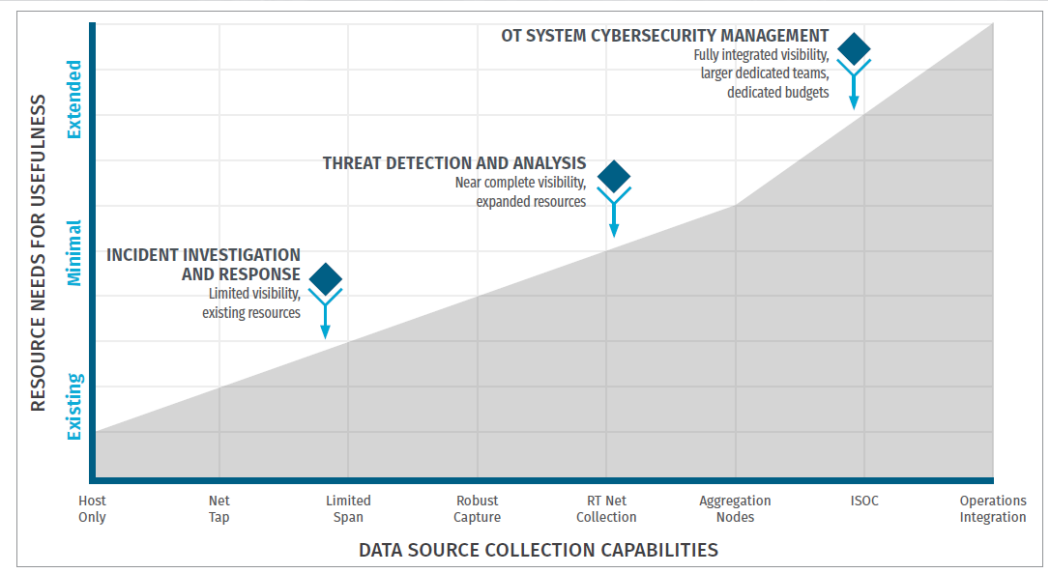
Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

#2 Defensible Architecture

- How are you building systems that can be defended by your cyber teams?
- Need to define your crown jewel assets and know your assets
- Know your network chokepoints and your defensible cyber position
- It’s not just the IT/OT Edge DMZ but needs to consider traffic flows between ICS zones

#3 ICS Network Visibility Monitoring

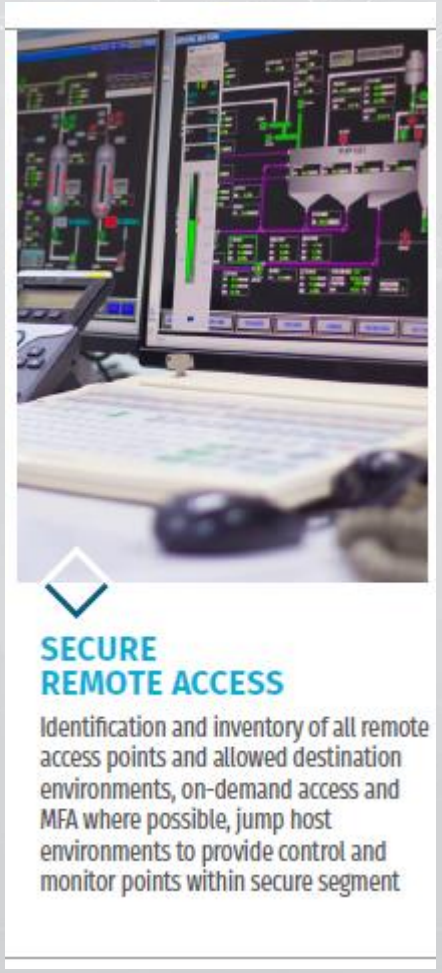
- OT is Systems of Systems – the network is key
- Use your scenarios and understand your threat actor TTPs to ensure you have the right visibility



Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

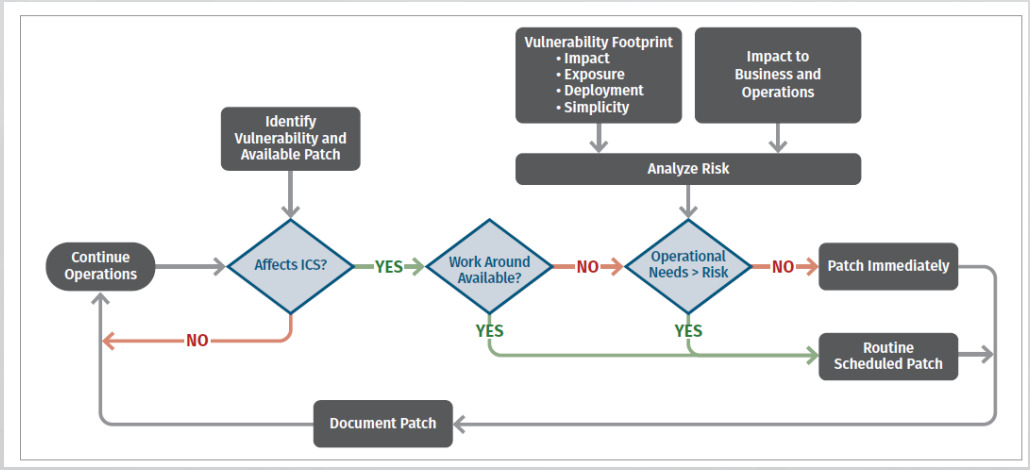
#4 Secure Remote Access

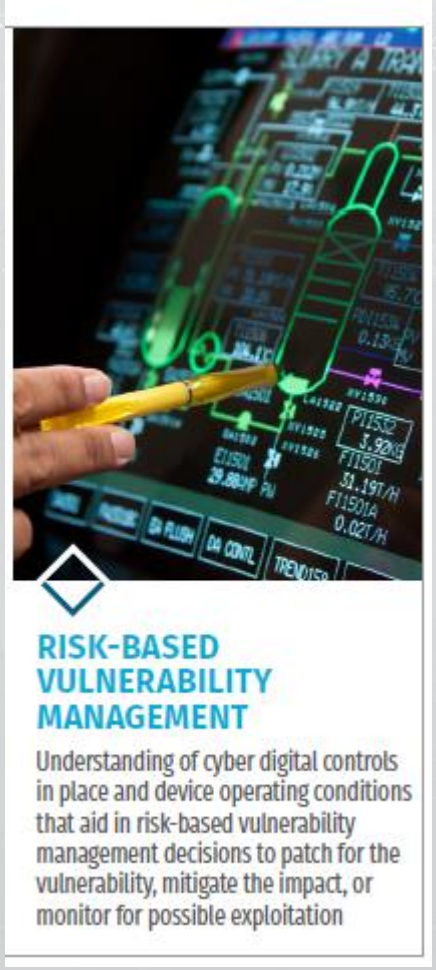
- It’s not just MFA
- COVID-19 has seen the attack surface increase
- Your Stage-1 Kill Chain may now be in your third parties



#5 Risk Based Vulnerability Management

- Use the Now, Next, Never Approach
- Patching is not the only answer –
  only 4% of Patches are a “now” level
- There are other mitigations that are better strategies to manage risk





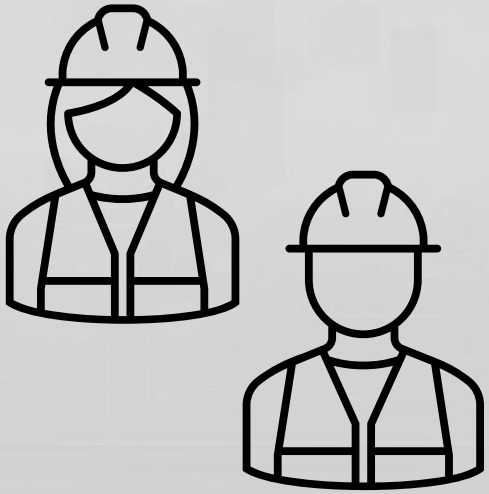
Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

#1 ICS Incident Response Deep Dive

Safety

- **<u>Personal Safety is Critical in ICS Incident Response</u>**
- Vital to understand physical hazards especially ones that the ICS controls
- The response team must have correct inductions, site permits/tickets and appropriate Personal Protective Equipment (PPE)
- Ideally the team should be familiar with sites prior to an incident



Define and Prioritise Scenarios

- The most critical activity in Control #1
- Ransomware must be considered for all Industries
- Electric:
  - Ukraine 2015 and Ukraine 2016 (CRASHOVERRIDE)
- Oil & Gas:
  - TRISIS
- Also consider high-consequence low likelihood events:
  - Work with your Engineering and Operations teams and ask “What does a really bad day look like”

Top 5 Recommended Tabletops

- Dean Parson's Top 5 Recommended Tabletops:
  - Scenario 1 – Living off the Land: Native Industrial Control System Protocol Abuse
  - Scenario 2 – Human Machine Interface Hijack: On-Screen Suspected Activity
  - Scenario 3 – Physical Access to Cyber Access Event
  - Scenario 4 – Ransomware on IT or ICS/OT Networks
  - Scenario 5 – IT or ICS Network Pivot through Trusted Connections/OT Networks
  - BONUS SCENARIO – Contaminated Transient Device
- Read the blog at https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/ which also has a link to a video session

Backdoors and Breaches – ICS/OT

- A card game developed by industry practitioners to help people learn about OT Incident Response
- A great stakeholder engagement tool for teams outside of the core OT Cyber Security Team
- Learn more at www.backdoorsandbreaches.com
- Online version https://play.backdoorsandbreaches.com/play.backdoorsandbreaches.com-Engine-V1/App/

Know your Assets!

- You can’t defend what you don’t know
- Methods to collect:
  - Physical Inspection
  - Configuration Analysis
  - Traffic Capture
  - Active Scanning (Requires Risk Based considerations!)
- Determine how you can find baselines of what is normal configuration and behaviour and what tools exist to find “weird”

What to collect?

Network Visibility

Can work at all levels:

- Need to understand chokepoints
- Need to understand SPAN and Network Tap Capabilities
- Also consider existing switch capabilities (Netflow, local collectors etc.)

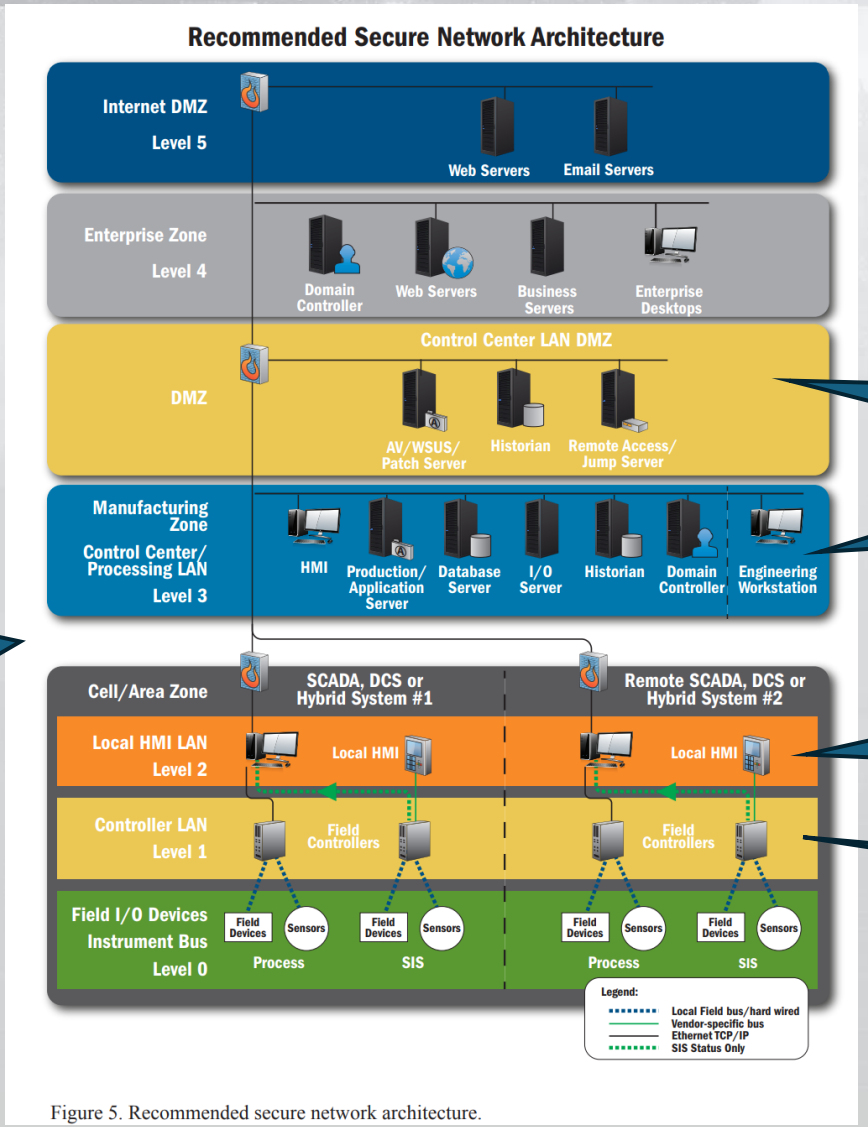


Figure 5. Recommended secure network architecture.

Typical IT Assets and Collection Acquisition – IT IR can really help here!

Likely Legacy Operating Systems
Essential Reliability and Availability Requirements

Local HMIs may be older OS and use embedded operating systems

Custom Electronic Devices, will have specialist software and may require vendor support

Collection Management Framework (Dragos)

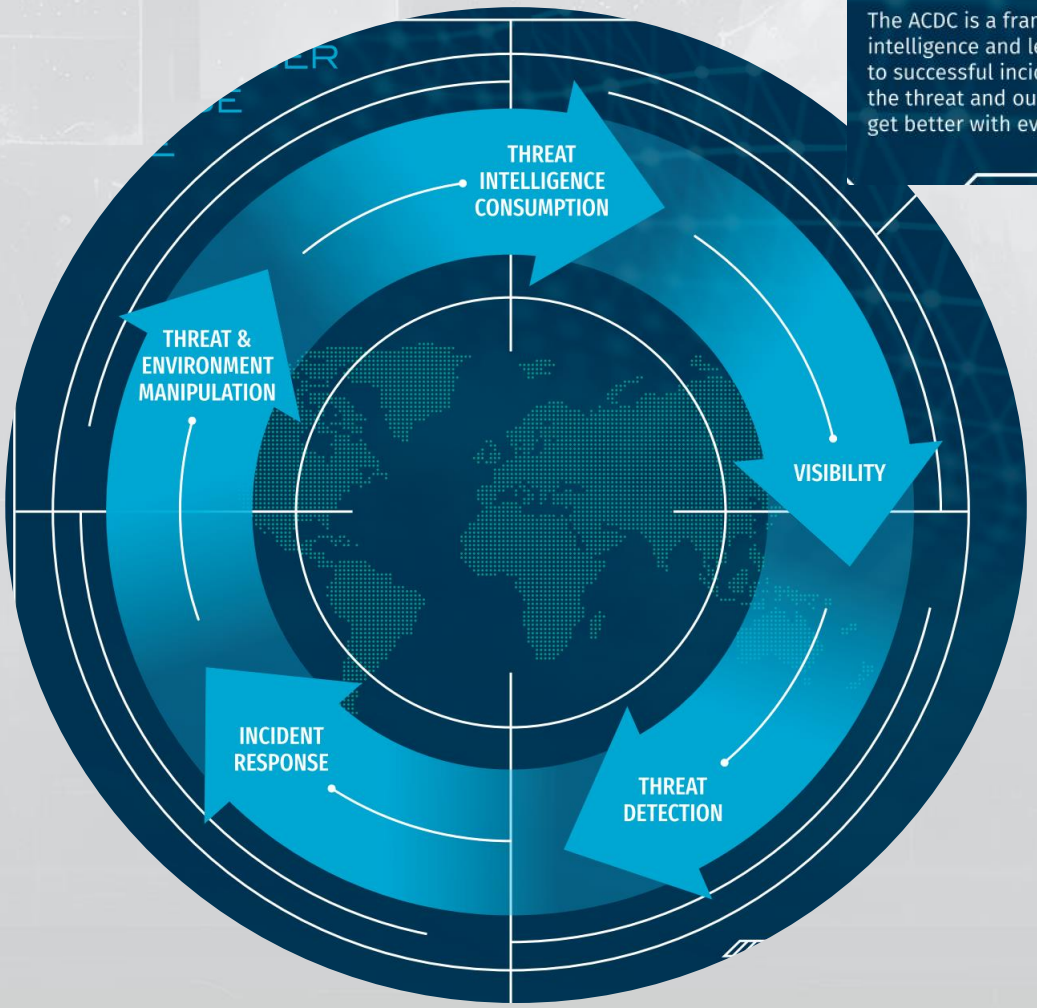
	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Ref - https://www.dragos.com/wp- content/uploads/CMF_For_ICS.pdf

SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

Key OT Incident Response Concepts from SANS ICS515

Active Cyber Defense Cycle (ACDC)



The Active Cyber Defense Cycle (ACDC)

The ACDC is a framework used in SANS ICS515 to teach students how to consume intelligence and leverage it to drive monitoring efforts. This framework will lead to successful incident response engagements and an improved understanding of the threat and our systems. Consistently utilizing this framework, defenders will get better with every engagement with an adversary.

Focus on ICS threat behaviors (tactics and techniques); Indicators of Compromise (IOCs) can be valuable but should be secondary to a focus on threat behaviors which will provide more coverage and a more durable detection strategy.

- **Threat Intelligence Consumption** – Determine how to source and apply Cyber Threat Intelligence for defending your ICS
- **Visibility** – Ensuring you have adequate visibility of your environment
- **Threat Detection** – Combining Visibility with knowledge of Threats to detect
- **Incident Response** – How to Contain and Respond to ICS Threats
- **Threat & Environment Manipulation** – How to safely manipulate threats and determine how to make changes to neutralise or delay their objectives

Source - https://www.sans.org/posters/intelligence-driven-ics-cybersecurity/

ICS Safe Position

- Disconnect/Disable connectivity to outside the ICS
- Isolate critical segments of the ICS
- Enable additional monitoring around critical ICS assets
- Modify physical site procedures with additional monitoring
- Disable unused system and network services
- Verify that the Safety Instrumented System is functioning as expected and isolated if needed

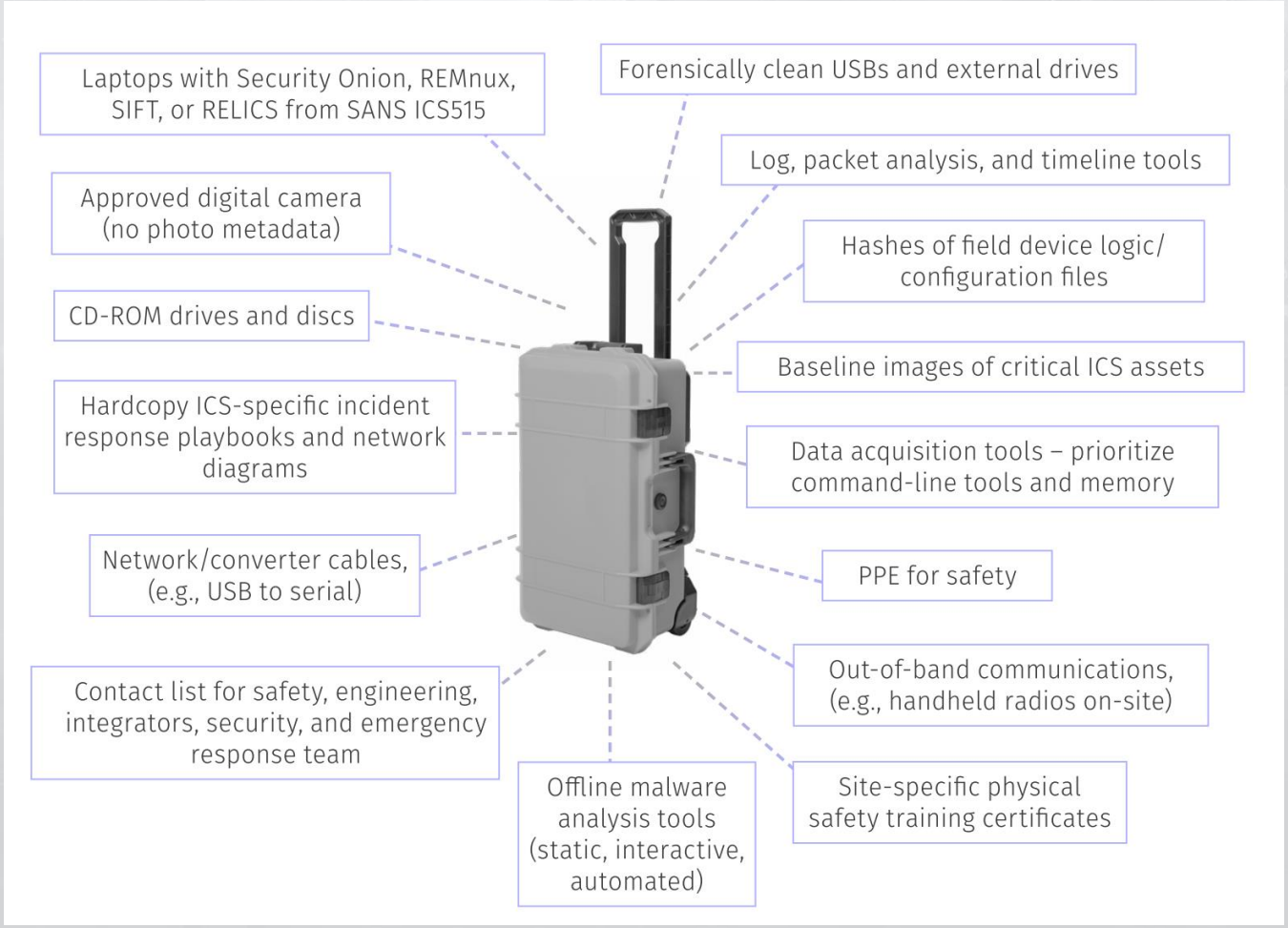
Source - https://www.sans.org/posters/industrial-control-system-cyber-incident-response/

ICS Response Life Cycle

Source - https://www.sans.org/posters/industrial-control-system-cyber-incident-response/

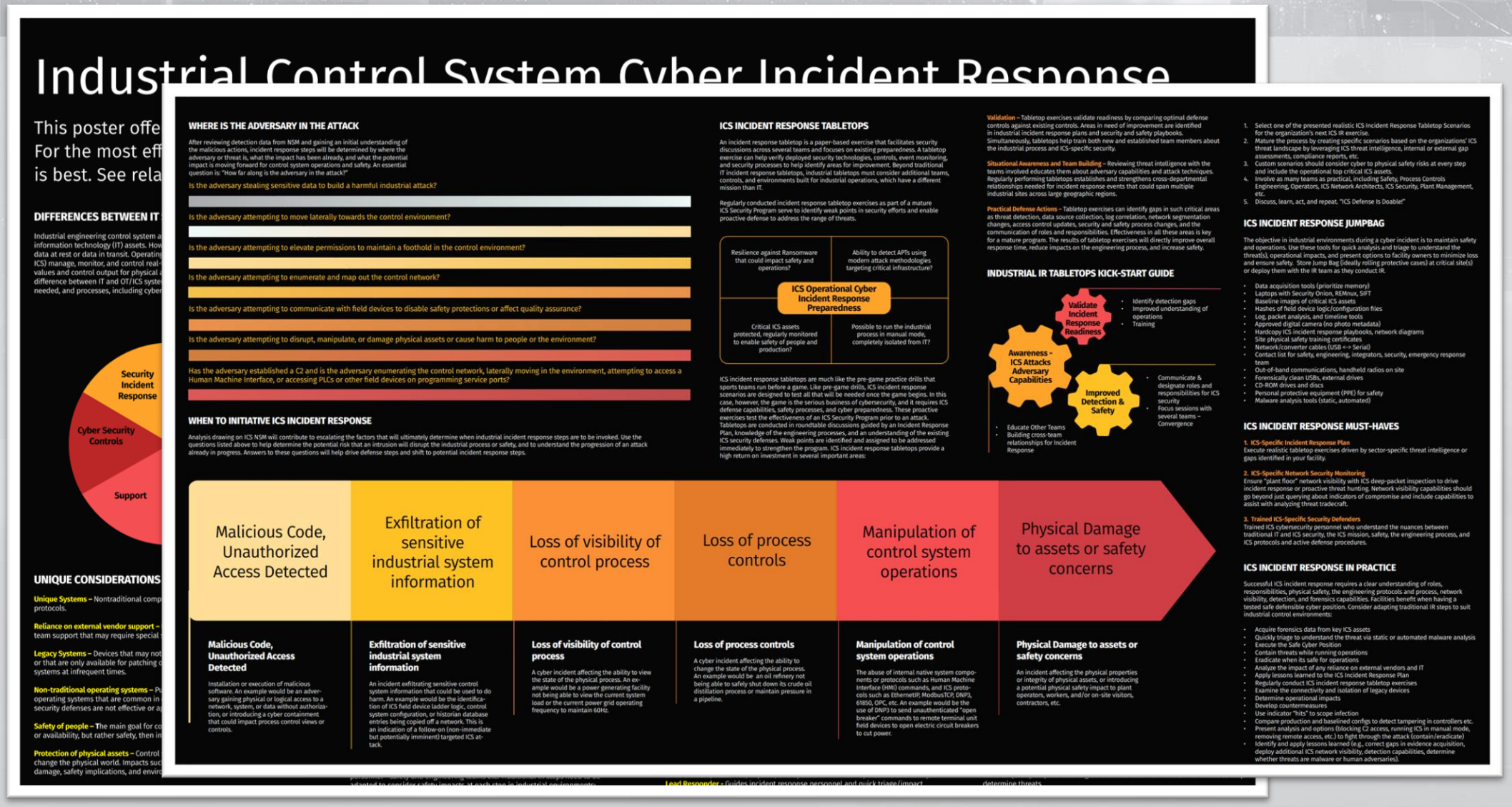
ICS Jump Bag Contents

- Essential equipment to have this ready to go prior to an incident
- Ideally have them pre-deployed at your OT Sites and train site teams on how to use acquisition tools



Source – ICS Cyber Security Field Manual – https://www.sans.org/mlp/ics-resources/

Tying it all Together – SANS ICS IR Poster



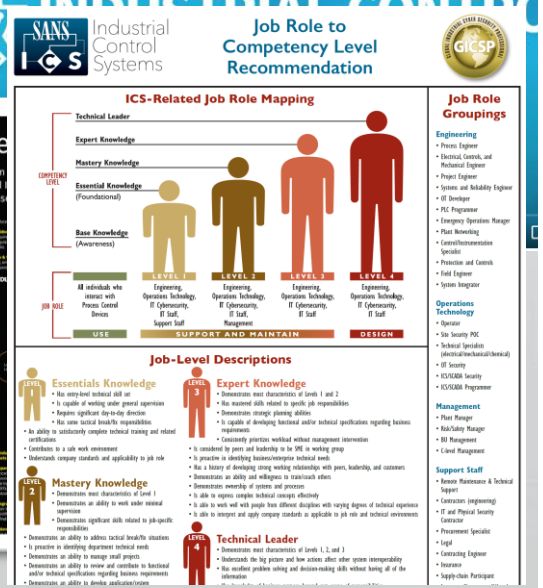
Source - https://www.sans.org/posters/industrial-control-system-cyber-incident-response/

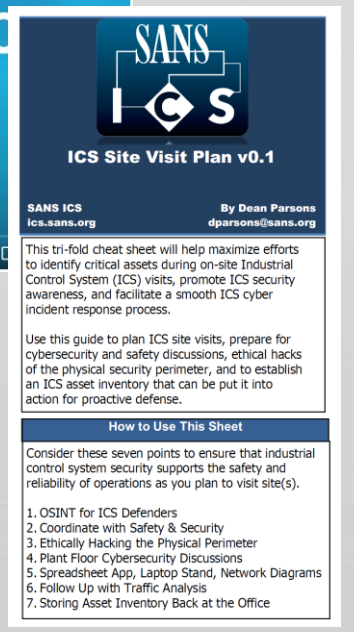
SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

SANS ICS Security Community Resources

Free SANS Community Resources

- SANS ICS Field Manual
- SANS ICS Youtube – Concepts Series, Summit Recordings and many more resources
- SANS Posters –Active Defense Poster, Site Visit, Job Poster and Many More
- SANS ICS Community Forum – ics.sans.org



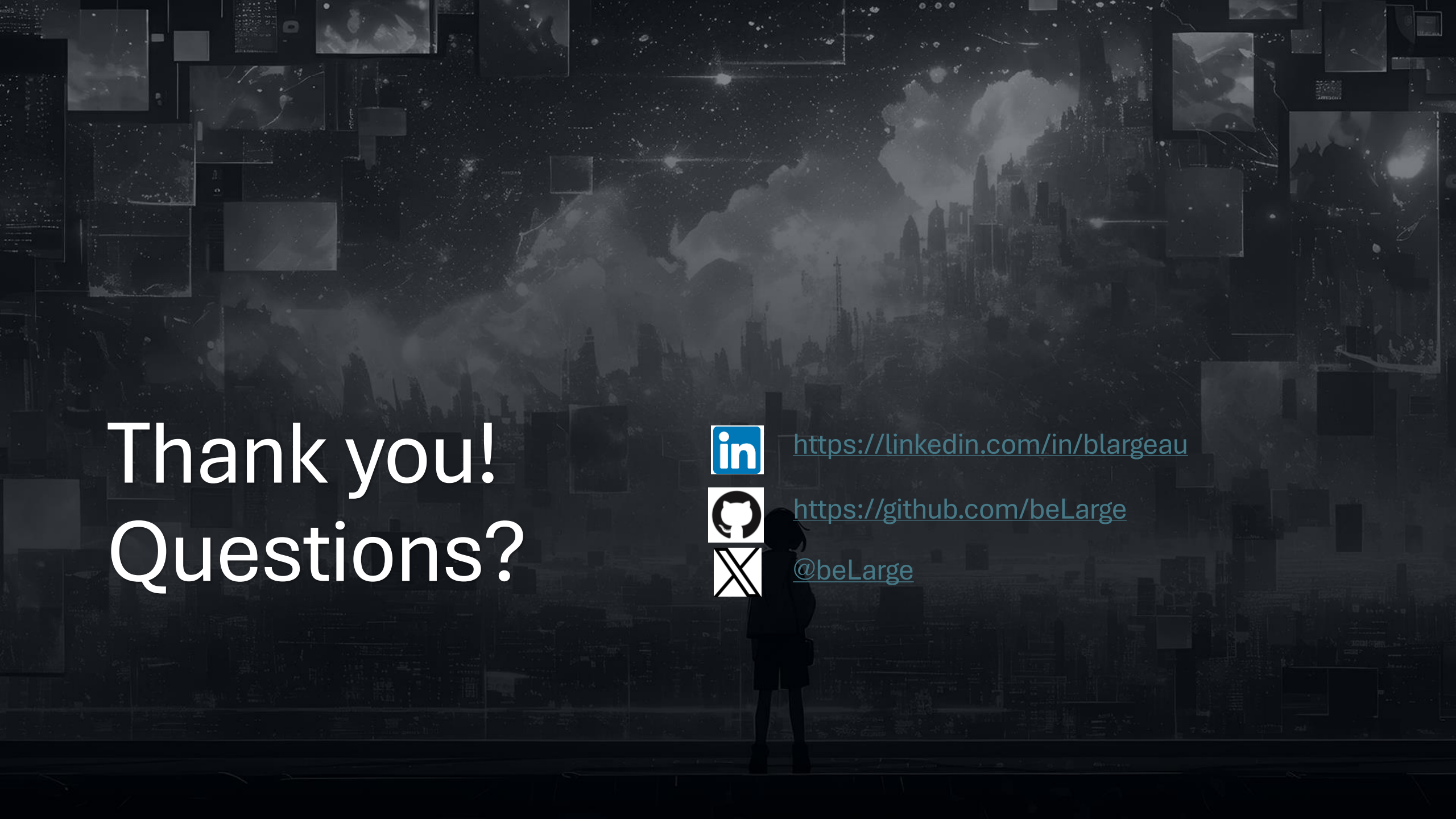


SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス

Summary

Summary

- The Five ICS Cyber Security Critical Controls
  - Read the White Paper
  - Watch the Webinar Recording
- Control #1 – ICS Specific Incident Response Plan
  - Determine your scenarios and prioritise
  - Run the 5 SANS ICS Table tops
  - Practice, Practice, Practice
- SANS ICS515 Resources
  - Apply the Active Cyber Defense Cycle (ACDC)
  - Know your Cyber Safe Position – practice it
  - Review the Incident Response Poster
- SANS ICS Community Resources
  - Read the ICS Field Manual
  - Watch the SANS ICS Youtube Channel
  - Review the SANS ICS Posters


Thank you!
Questions?
https://linkedin.com/in/blargeau
https://github.com/beLarge
@beLarge