Building an Effective ICS/OT Security Monitoring and Defense Program

Kai Thomsen, Dragos Inc

whoami

- Director, International Incident Response Services at Dragos Inc.

- 22+ years of DFIR experience in IT, ICS/OT, and I have done a little IR around vehicles 😉

- Certified SANS Instructor in the ICS curriculum

DRAGOS

Safeguarding Civilization

500+ EMPLOYEES

300+ CUSTOMERS

20 COUNTRIES

11 INDUSTRY VERTICALS

Built For Practitioners, By Practitioners

The largest & most experienced team of ICS security specialists make the best technology.

- ELECTRIC
- OIL & GAS
- MANUFACTURING
- BLDG AUTO SYS
- CHEMICAL
- GOVERNMENT
- WATER
- FOOD & BEV
- MINING
- TRANSPORTATION
- PHARMACEUTICAL

HQ | Hanover, MD

REGIONAL | US & Canada, Australia-New Zealand, Gulf Coast, UK/Europe

Agenda

- Short ICS/OT Intro
- IT <-> ICS Differences
- Examples of ICS/OT Cyber Attacks
- ICS IR Case Study
- Active Cyber Defense Cycle
  - Threat Intelligence
  - Visibility
  - Detection
  - Incident Response
  - Threat & Environment Manipulation
- Collection Management Frameworks
- Threat Hunting

Intro into ICS/OT

Some Common Acronyms

OT	Operational Technology	IT Systems that control industrial or physical processes
ICS	Industrial Control Systems	Specialized computing equipment that directly manipulate and/or control
IACS	Industrial Automation and Control Systems	Same as above, this term is more commonly used in Oil & Gas and Offshore
PLC	Programmable Logic Controller	A computer that is ruggedized and adapted for industrial control.
RTU	Remote Terminal Unit	More advanced version of a PLC that interfaces with DCS or SCADA systems
IED	Intelligent Electronic Device	Controllers for power system equipment in the electric industry
DCS	Distributed Control System	Combination of OT and ICS to enable realtime control industrial processes
SCADA	Supervisory Control And Data Acquisition	Even larger scale visualization and control of industrial processes, not realtime
HMI	Human Machine Interface	Your fancy operations UX
EWS	Engineering Workstation	The computers used to program, configure, and update control systems
SIS	Safety Instrumented System	Dedicated controllers to maintain safety of industrial processes

What is OT/ICS?

IT + Physics

The Mission is Different

Priorities are:

1. Safety & Reliability of Operations
2. Business
3. Everything else

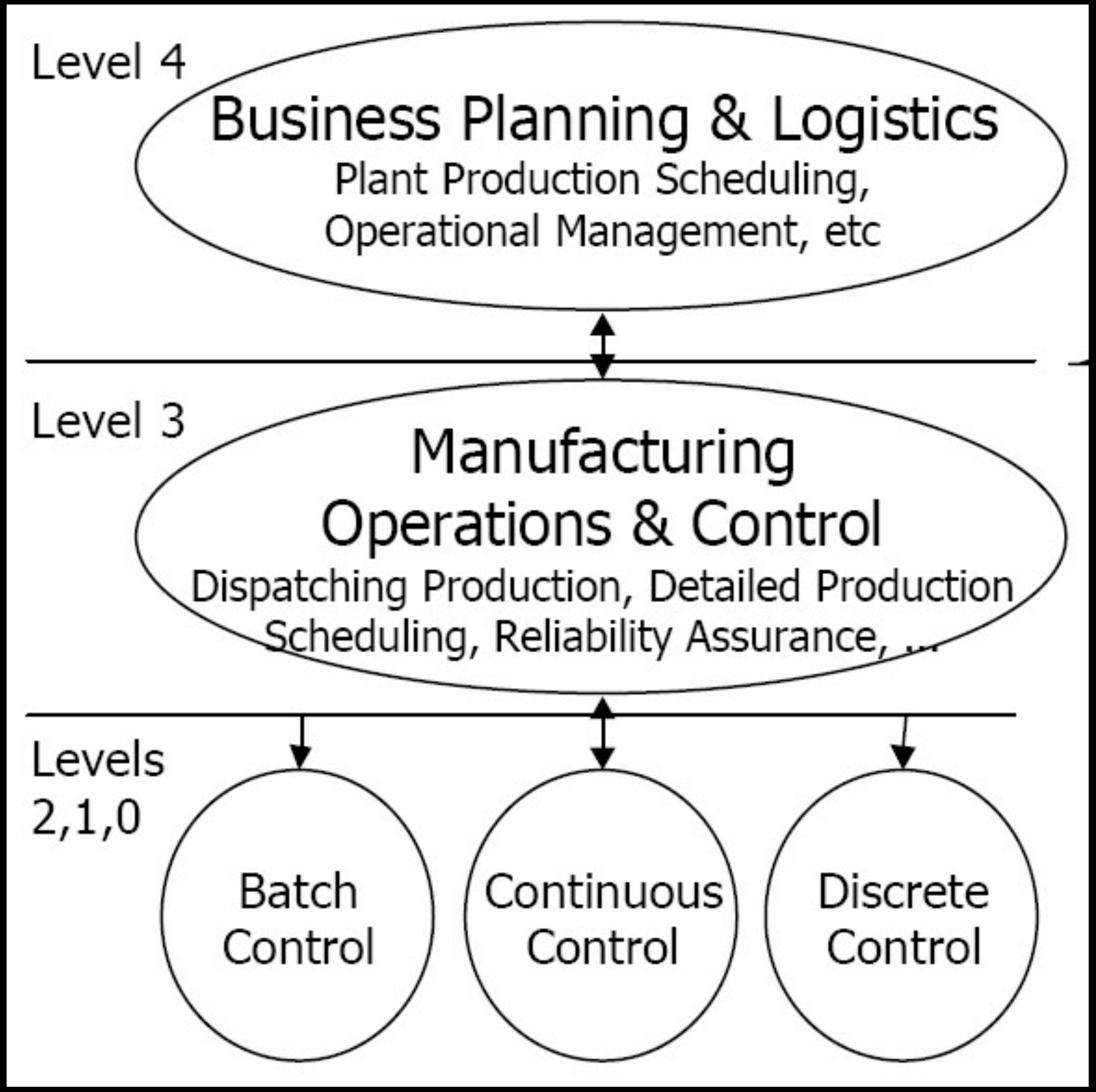
Safety & Reliability

In ICS environments we are dealing with hard real-time requirements, proprietary systems that often must not be rebooted during plant operation and equipment lifecycles of 10-30+ years.

Interaction with these environments requires understanding the procedures, regulations, and risks involved. Physical impact can often lead to huge financial losses, environmental damage or even danger to loss of limb or life.

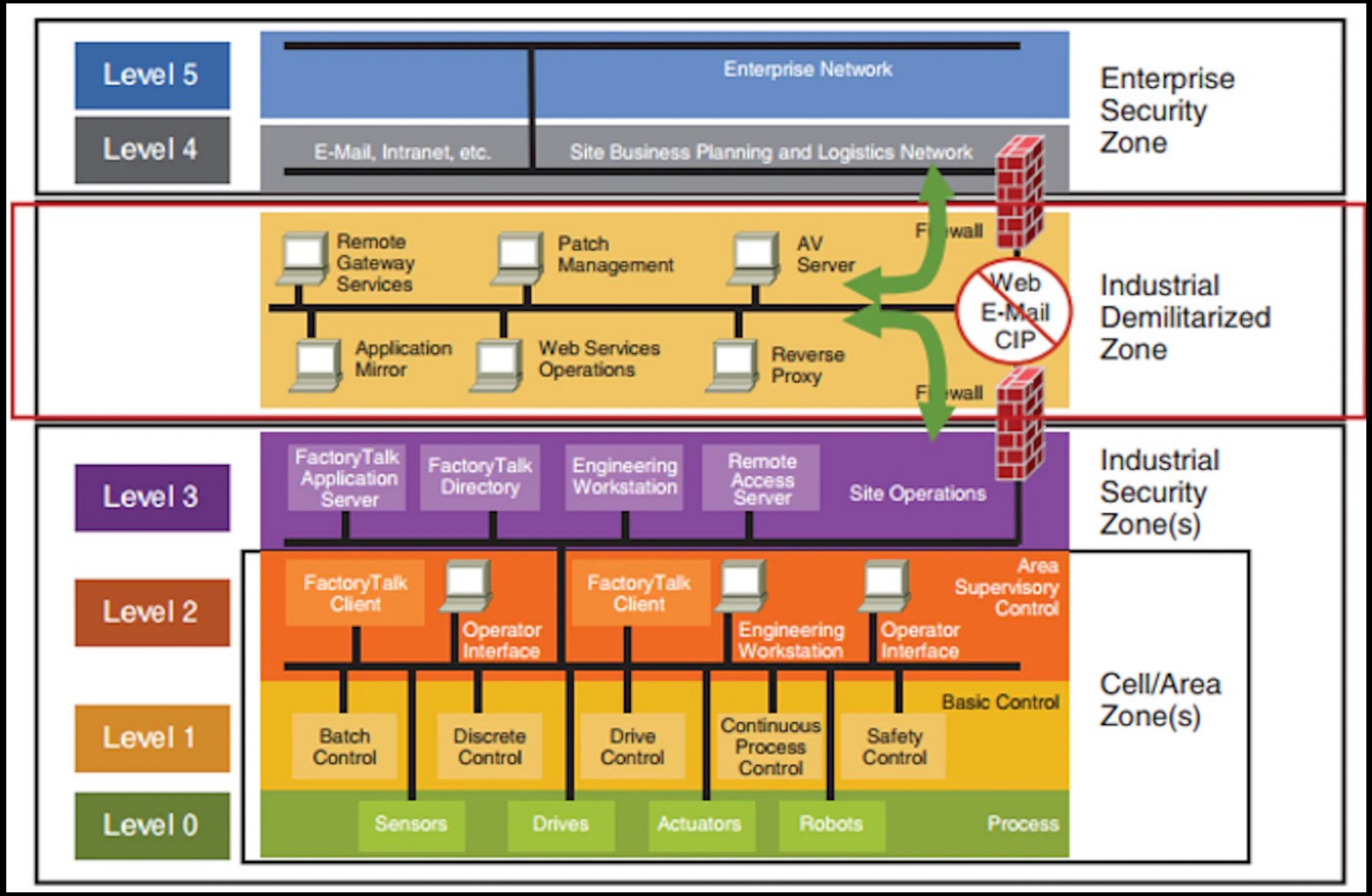
The Purdue Model

- The Purdue Model (PERA, Purdue Enterprise Reference Architecture) is a reference architecture that can model the enterprise in multiple layers and in multiple stages of the architectural life cycle
- This was not (strictly) built with security in mind, but is a good model to understand zoning and different requirements
- Oftentimes, especially in manufacturing, this is rather conceptual and zoning recommendations are not strictly followed


Level 4
Business Planning & Logistics
Plant Production Scheduling,
Operational Management, etc
Level 3
Manufacturing
Operations & Control
Dispatching Production, Detailed Production
Scheduling, Reliability Assurance, ...
Levels
2,1,0
Batch
Control
Continuous
Control
Discrete
Control

SCADA

DCS



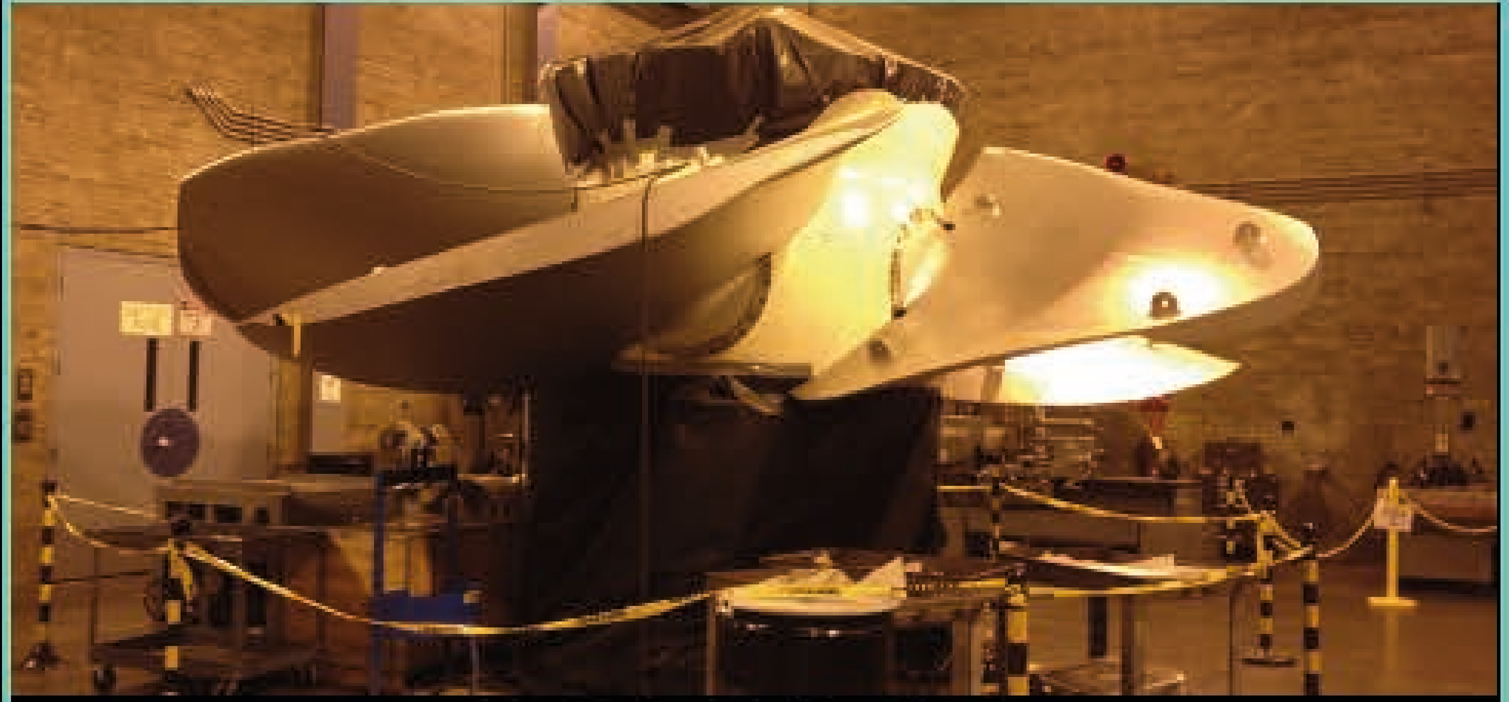
Source: https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

Source: https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant

What this Means for ICS/OT Security

UNDERSTAND OT

ICS incident responders must be able to effectively communicate with OT teams. Ultimately only OT staff should be directly interacting with ICS equipment under guidance of experienced ICS incident responders. Adversaries are aiming for physical impact. Incident responders must ensure they don't cause it unintentionally.



SAFETY PROCEDURES

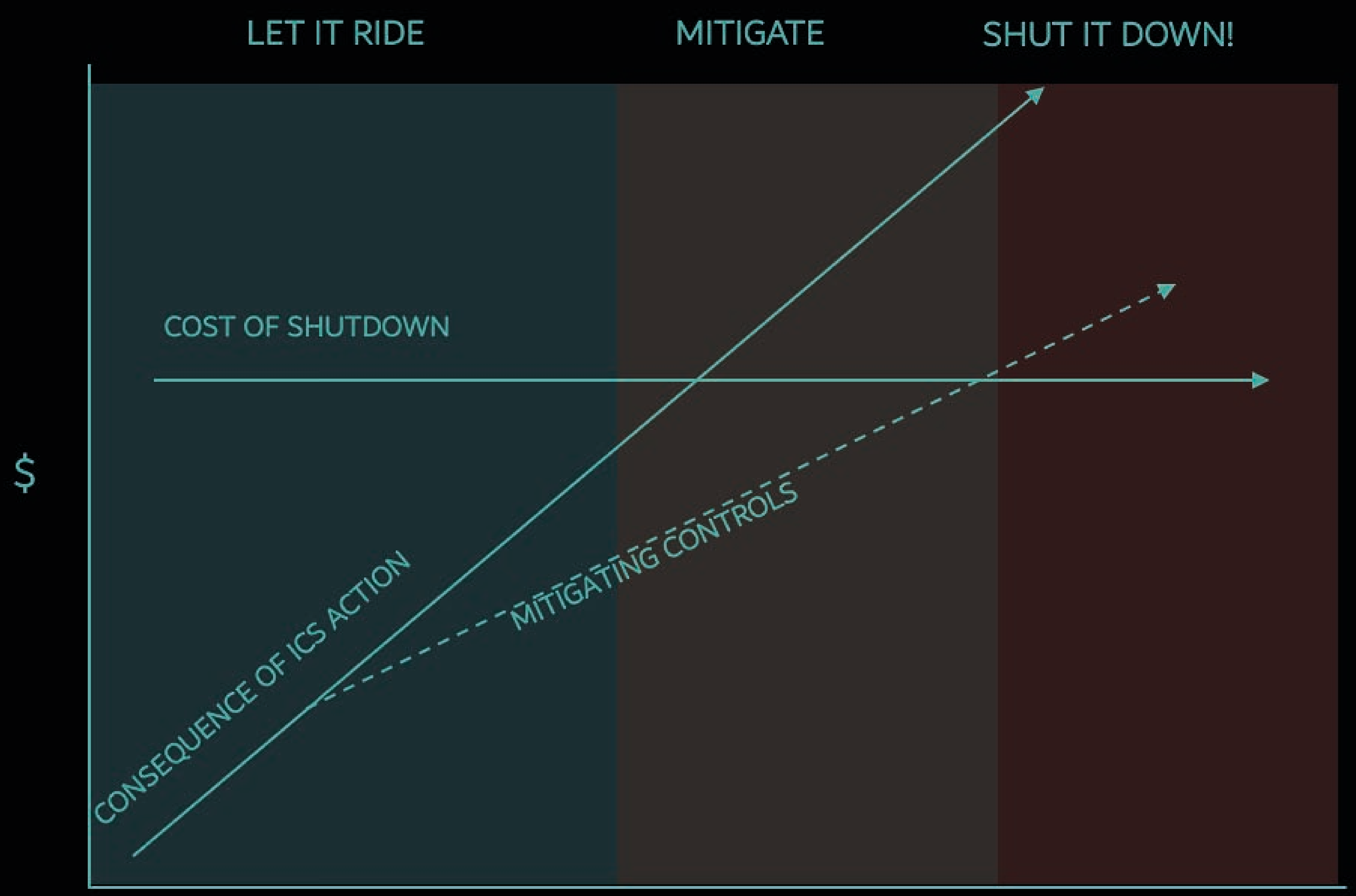
For certain ICS environments, mandatory safety trainings & certifications are required to be allowed to enter. ICS incident responders must meet these requirements and know how to take care of themselves and their peers.

PROPRIETARY HARD- AND SOFTWARE

In ICS it's not only about Windows systems. ICS equipment, software, and network protocols are highly proprietary. To understand the potential impact of an intrusion to the plant process, incident responders need to have deep knowledge about ICS equipment and protocols.

Working in Live Environments

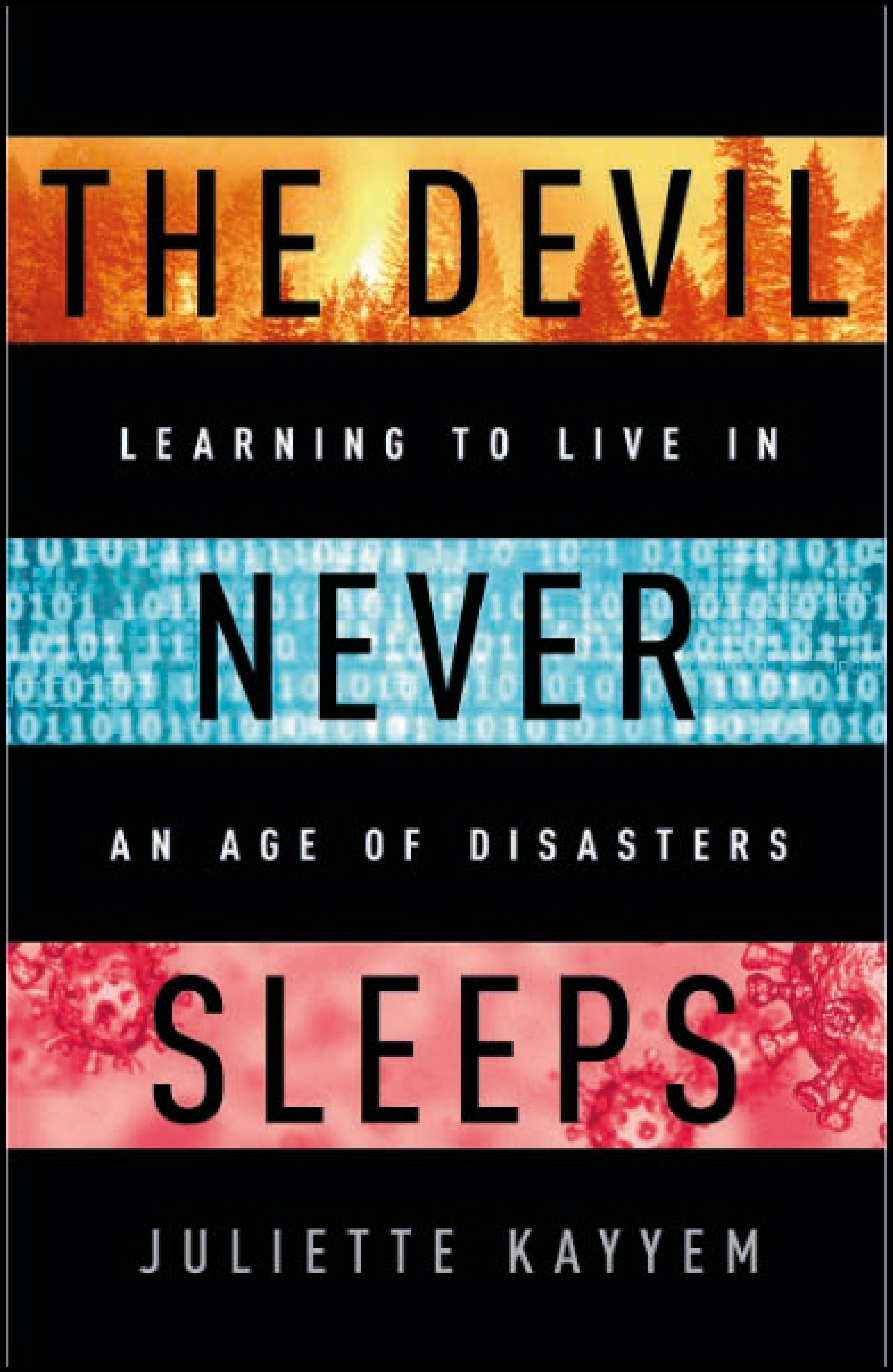
- In many scenarios, ICS incident responders will be engaging in live environments.
- Plant operators may choose to defer shutdown procedures to scheduled windows or determine the risk of an intrusion is lower than the operational impact of shutdown.
- Even if a plant is shut down, various systems are still running to ensure a safe state. Causing these systems to malfunction during an investigation might lead to hazardous situations.



Short Interlude

Read this book!

- We live in - very - volatile times
- Given our current posture, we will hardly be able to avert serious incidents
- Organizations, companies, and individuals need to learn to adapt to living through „right of boom“



Current Challenges in ICS/OT

Cultural:

- Many CISOs do not understand IT <> ICS/OT differences
- IT Security requirements clash with Safety regs and regulations
- IT and OT staff often do not understand each other
- „Our OT environment is air-gapped“
    - What they believe this means: there is no connection between Internet and OT
    - What it actually means: you cannot reach OT directly from the Internet

Technical/Procedural:

- Standards are 90% prevention focused, detection & response capabilities are afterthoughts at best
- Lack of ICS/OT aware visibility
- No dedicated ICS/OT Incident Response Plan
- Plans don’t get exercised

Examples of ICS Cyber Attacks

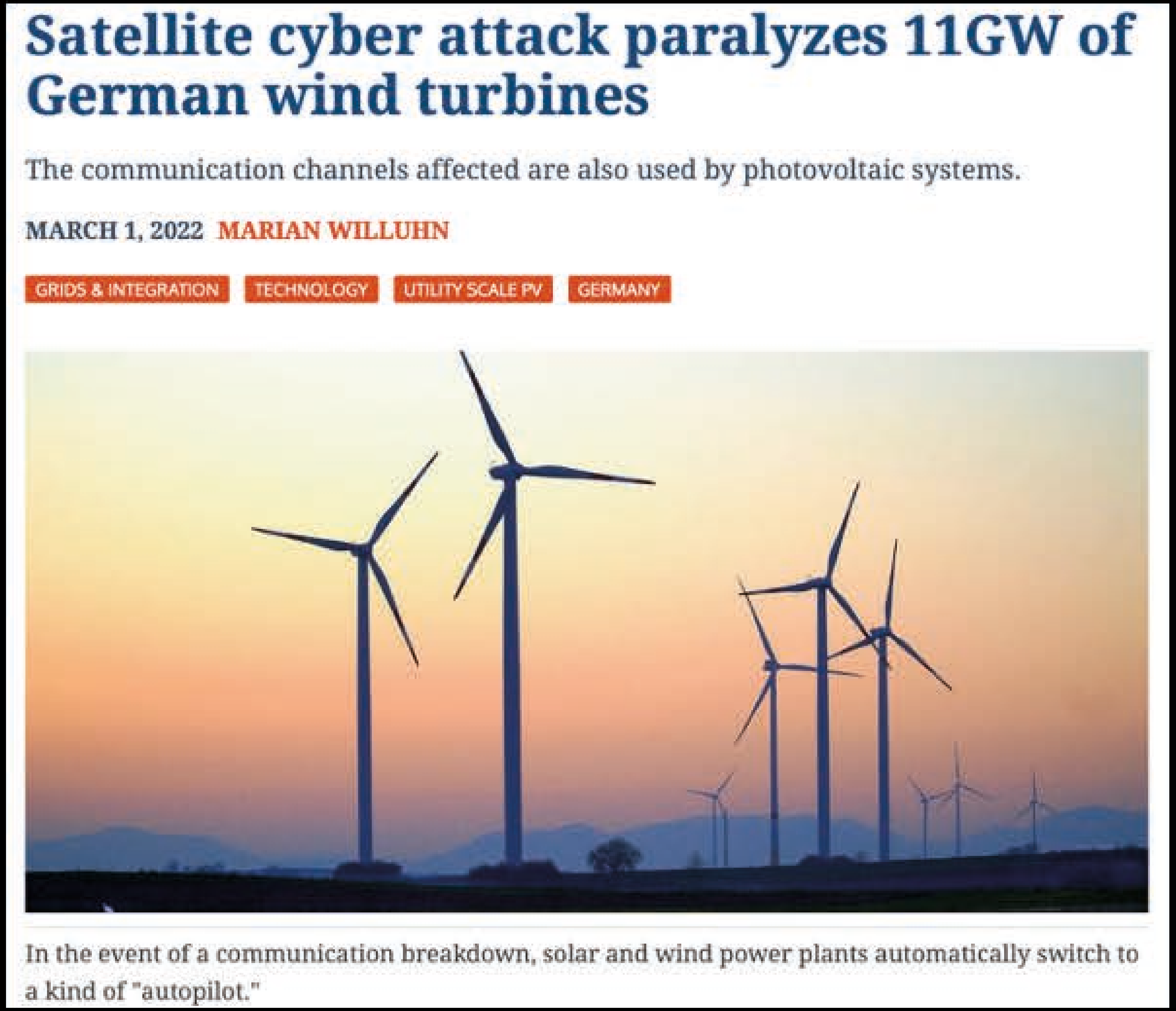
- June 2010: A malware called “Stuxnet” affects the uranium enrichment facility in Natanz, Iran, damaging ~2300 centrifuges. In 2015, the New York Times publishes a comprehensive article, attributing the attack to the USA and Israel, conducted under the code name “Operation Olympic Games”
- December 2015: a cyber attack against 3 electric power distribution substations in central Ukraine leaves ~225000 people without electricity for ~9 hours. The damage to the SCADA systems took about 9 months to fix
- December 2016: a cyber attack against an electric power distribution substation north of Kiev leaves a few thousand people without power for less than an hour. The *intended impact* of the attack was much worse. Due to errors by the attacker, the impact was low

August 2017: a refinery in Saudi Arabia, belonging to Petro Rabigh, goes into emergency shutdown. Incident responders discover a malware installed on a Safety System in the refinery that Dragos names TRISIS. The attackers had also manipulated a highly volatile petrochemical process. This would have resulted in a large explosion, potentially causing a huge number of fatalities, if not for one small programming error by the attacker

Source: https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/

Hybrid Warfare

Because there is no Cyberwar



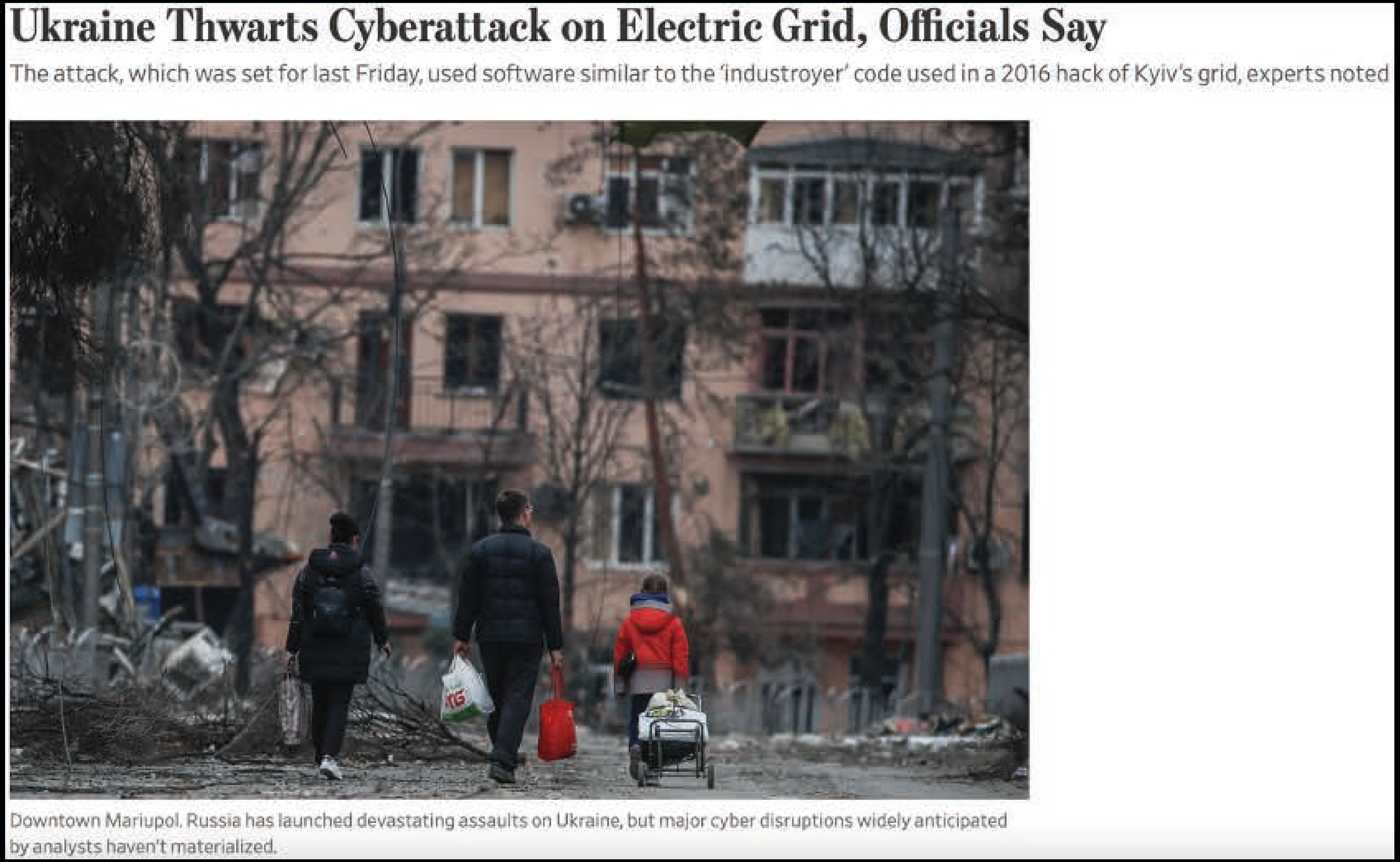
Satellite cyber attack paralyzes 11GW of German wind turbines

The communication channels affected are also used by photovoltaic systems.

MARCH 1, 2022 MARIAN WILLUHN

GRIDS & INTEGRATION TECHNOLOGY UTILITY SCALE PV GERMANY

In the event of a communication breakdown, solar and wind power plants automatically switch to a kind of "autopilot."



Ukraine Thwarts Cyberattack on Electric Grid, Officials Say

The attack, which was set for last Friday, used software similar to the 'industroyer' code used in a 2016 hack of Kyiv's grid, experts noted

Downtown Mariupol. Russia has launched devastating assaults on Ukraine, but major cyber disruptions widely anticipated by analysts haven't materialized.

The 5 Critical Controls

Because you need to focus

1. Defensible Architecture
2. ICS/OT Aware Monitoring
3. ICS Incident Response Plan
4. Key Vulnerability Management
5. Multi-Factor Remote Access Authentication

The 5 Critical Controls

Because you need to focus

1. Defensible Architecture
2. ICS/OT Aware Monitoring
3. ICS Incident Response Plan
4. Key Vulnerability Management
5. Multi-Factor Remote Access Authentication

We will focus on these

Case Study: The Ghost in the Machine

Scenario

- In February 2021, dead of the night, somewhere in the Middle of Nowhere (TM), in North America, the gas turbines at a peak power generation site, turn on and idle
- The SCADA operations had not issued a START command
- There was no need for peak electric power generation
- The local operations team had not issued a START command

- The operator activated their ICS Incident Response Retainer and Dragos responders arrived at the site within 8 hours
- There was no OT (or IT) monitoring solution in place
- The firewall had not recorded any incoming connections
- No one from the local operations crew had entered the control shed next to the turbine & generator hall

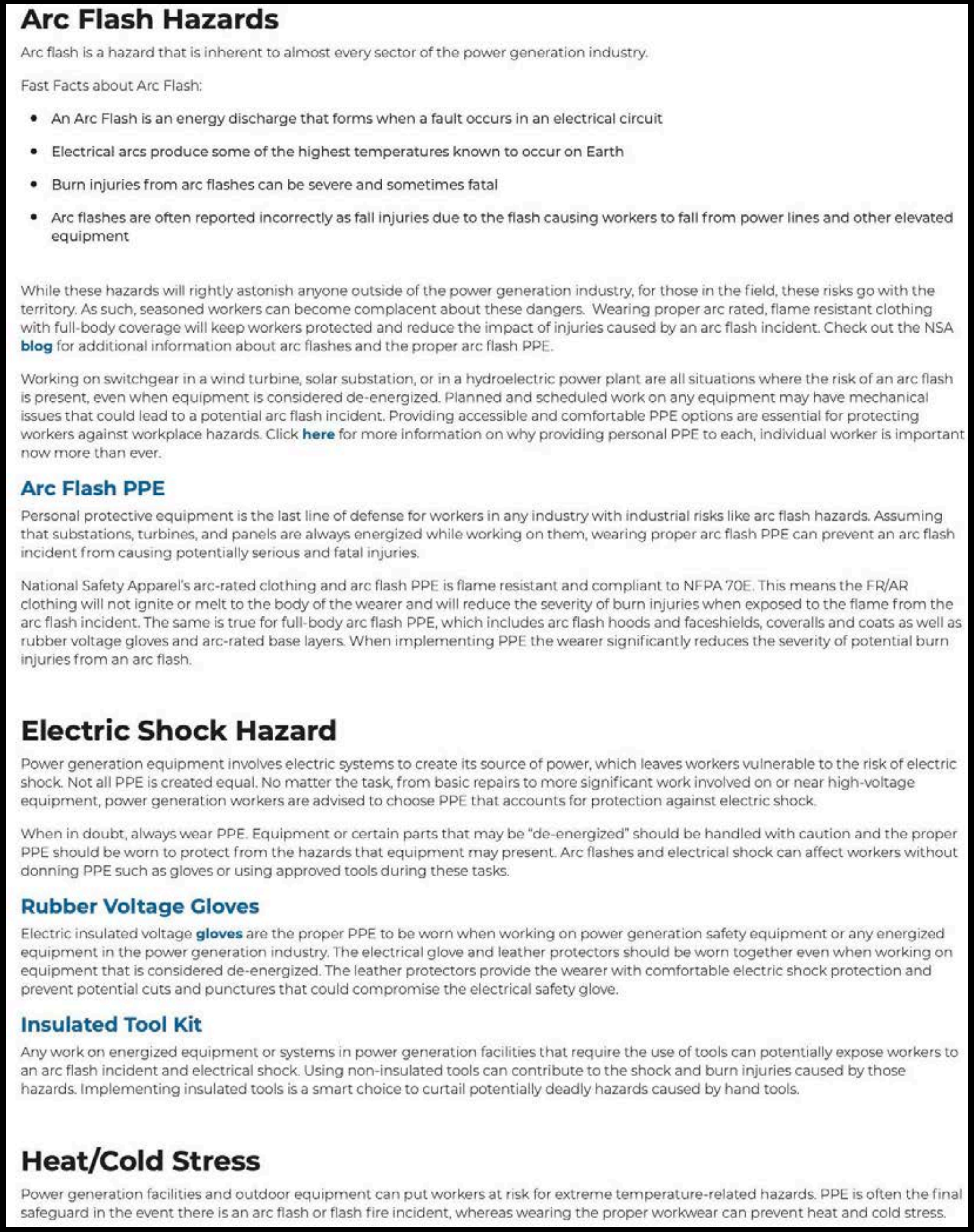
How would you investigate?

Who said you can just dive right in?

Remember

Safety & Reliability come first!

You will go exactly nowhere without proper PPE



Arc Flash Hazards

Arc flash is a hazard that is inherent to almost every sector of the power generation industry.

Fast Facts about Arc Flash:

- An Arc Flash is an energy discharge that forms when a fault occurs in an electrical circuit
- Electrical arcs produce some of the highest temperatures known to occur on Earth
- Burn injuries from arc flashes can be severe and sometimes fatal
- Arc flashes are often reported incorrectly as fall injuries due to the flash causing workers to fall from power lines and other elevated equipment

While these hazards will rightly astonish anyone outside of the power generation industry, for those in the field, these risks go with the territory. As such, seasoned workers can become complacent about these dangers. Wearing proper arc rated, flame resistant clothing with full-body coverage will keep workers protected and reduce the impact of injuries caused by an arc flash incident. Check out the NSA **blog** for additional information about arc flashes and the proper arc flash PPE.

Working on switchgear in a wind turbine, solar substation, or in a hydroelectric power plant are all situations where the risk of an arc flash is present, even when equipment is considered de-energized. Planned and scheduled work on any equipment may have mechanical issues that could lead to a potential arc flash incident. Providing accessible and comfortable PPE options are essential for protecting workers against workplace hazards. Click **here** for more information on why providing personal PPE to each, individual worker is important now more than ever.

Arc Flash PPE

Personal protective equipment is the last line of defense for workers in any industry with industrial risks like arc flash hazards. Assuming that substations, turbines, and panels are always energized while working on them, wearing proper arc flash PPE can prevent an arc flash incident from causing potentially serious and fatal injuries.

National Safety Apparel's arc-rated clothing and arc flash PPE is flame resistant and compliant to NFPA 70E. This means the FR/AR clothing will not ignite or melt to the body of the wearer and will reduce the severity of burn injuries when exposed to the flame from the arc flash incident. The same is true for full-body arc flash PPE, which includes arc flash hoods and faceshields, coveralls and coats as well as rubber voltage gloves and arc-rated base layers. When implementing PPE the wearer significantly reduces the severity of potential burn injuries from an arc flash.

Electric Shock Hazard

Power generation equipment involves electric systems to create its source of power, which leaves workers vulnerable to the risk of electric shock. Not all PPE is created equal. No matter the task, from basic repairs to more significant work involved on or near high-voltage equipment, power generation workers are advised to choose PPE that accounts for protection against electric shock.

When in doubt, always wear PPE. Equipment or certain parts that may be "de-energized" should be handled with caution and the proper PPE should be worn to protect from the hazards that equipment may present. Arc flashes and electrical shock can affect workers without donning PPE such as gloves or using approved tools during these tasks.

Rubber Voltage Gloves

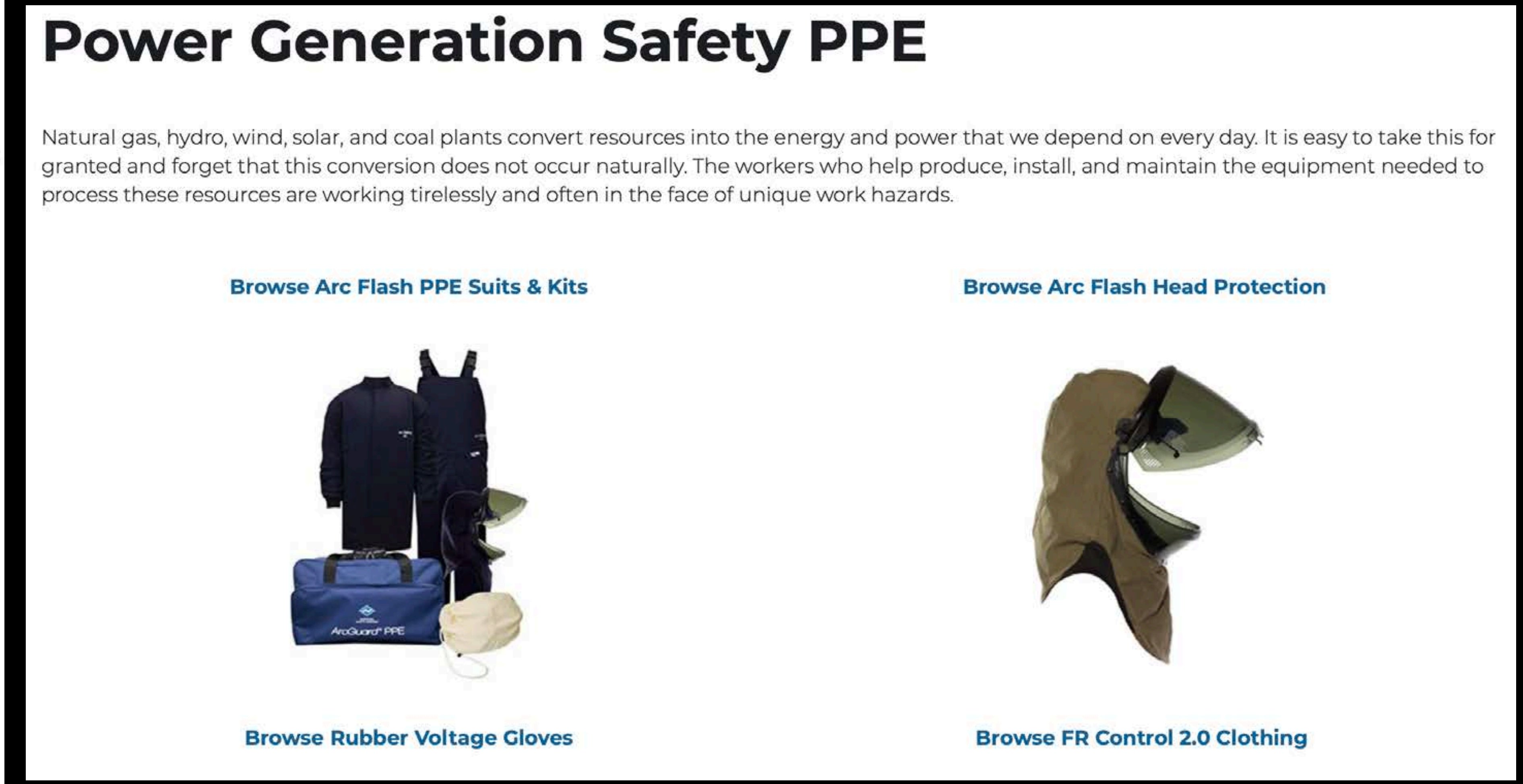
Electric insulated voltage **gloves** are the proper PPE to be worn when working on power generation safety equipment or any energized equipment in the power generation industry. The electrical glove and leather protectors should be worn together even when working on equipment that is considered de-energized. The leather protectors provide the wearer with comfortable electric shock protection and prevent potential cuts and punctures that could compromise the electrical safety glove.

Insulated Tool Kit

Any work on energized equipment or systems in power generation facilities that require the use of tools can potentially expose workers to an arc flash incident and electrical shock. Using non-insulated tools can contribute to the shock and burn injuries caused by those hazards. Implementing insulated tools is a smart choice to curtail potentially deadly hazards caused by hand tools.

Heat/Cold Stress

Power generation facilities and outdoor equipment can put workers at risk for extreme temperature-related hazards. PPE is often the final safeguard in the event there is an arc flash or flash fire incident, whereas wearing the proper workwear can prevent heat and cold stress.



Power Generation Safety PPE

Natural gas, hydro, wind, solar, and coal plants convert resources into the energy and power that we depend on every day. It is easy to take this for granted and forget that this conversion does not occur naturally. The workers who help produce, install, and maintain the equipment needed to process these resources are working tirelessly and often in the face of unique work hazards.

Browse Arc Flash PPE Suits & Kits
Browse Arc Flash Head Protection
ArcGuard PPE
Browse Rubber Voltage Gloves
Browse FR Control 2.0 Clothing

Source: https://www.thinknsa.com/power-generation-safety-ppe

What questions would you ask?

The Knowns

- Neither the SCADA control center nor the local team issued a START command for the gas turbines
- At the time the turbines were started (and a few days before) there were no incoming connections logged by the local firewall
- CCTV footage did not reveal anyone walking up to the door of the control shed
- Initial forensic triage of the HMI that controls the turbines did not reveal any unauthorized access. Actually no access at all.
- But right around the startup of the turbines, some applications were launched, including the one that starts the turbines

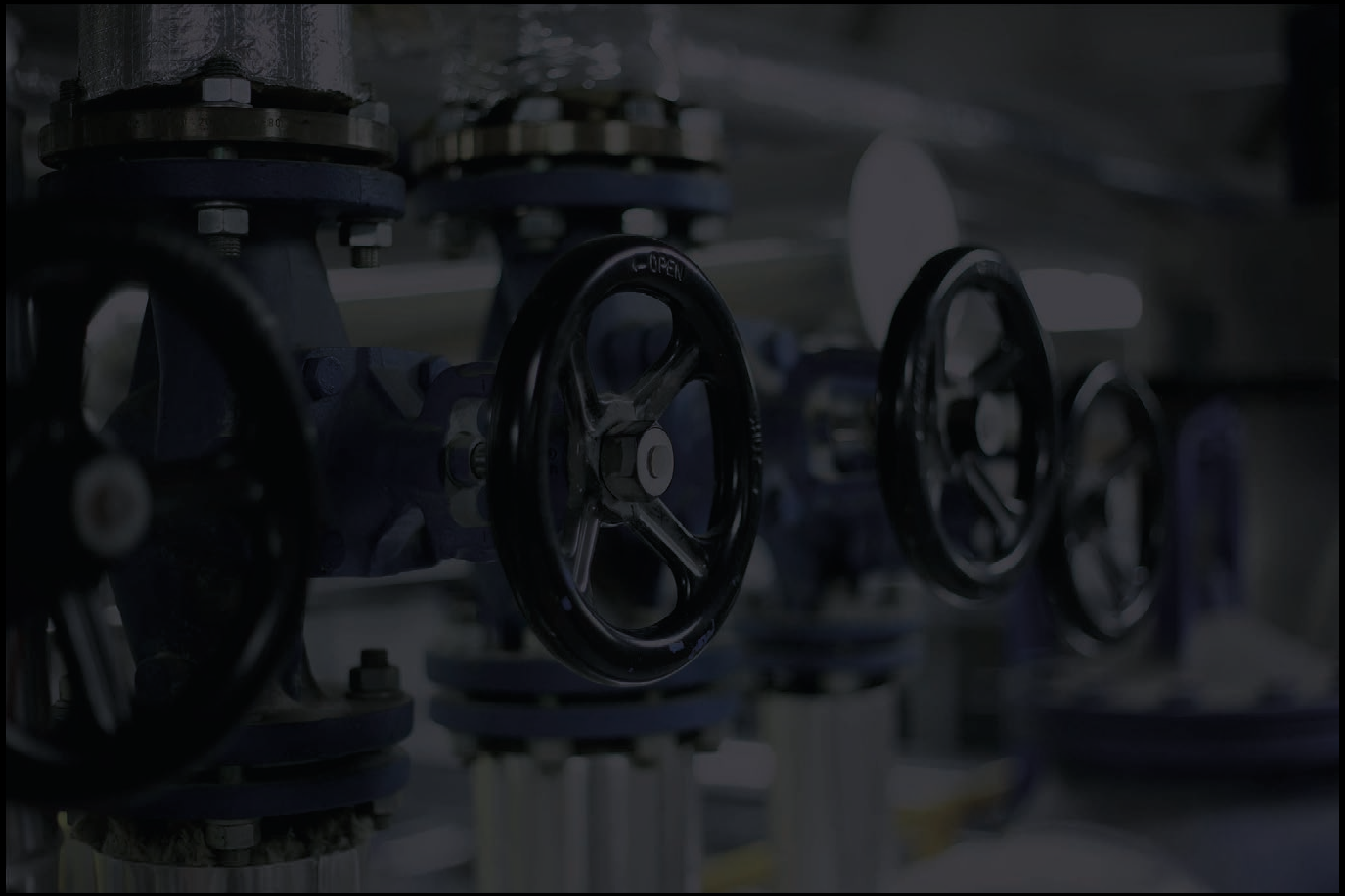
The Unknowns

- Are there other remote connections into the local network?
- Might there be another way into the control shed not monitored by CCTV?
- Might malware have been planted on the HMI some time ago
- There might be an insider threat
- There might be a root cause entirely unrelated to „cyber“

The Unknown Unknowns

Your guess is as good as mine 😉

Remember: every investigation requires the right combination of thoroughness, process, and an open mind.



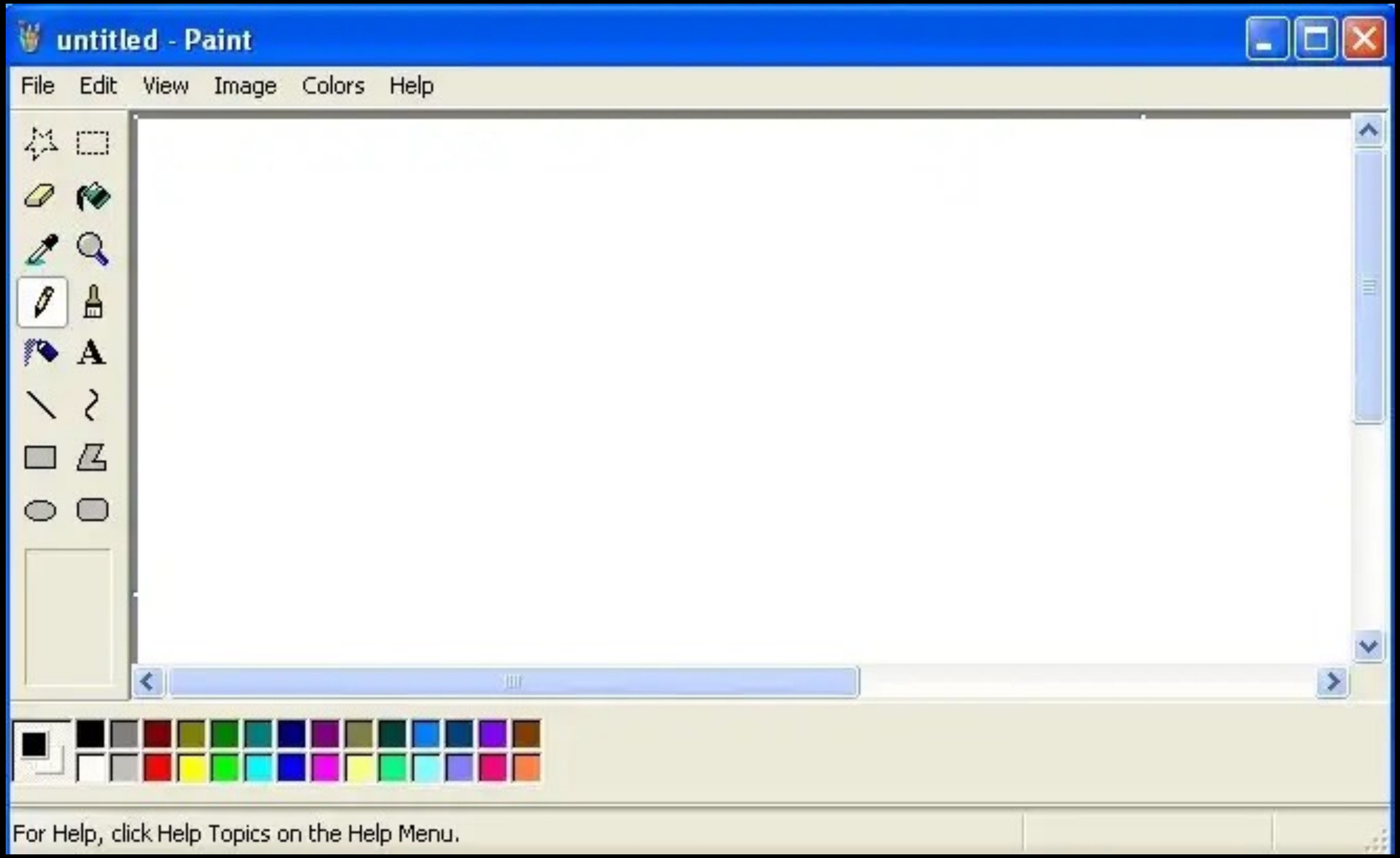
- While examining the control shed, the responder notes it is very cold in there
- Moisture has condensed on the HMI

Hypothesis: moisture might have caused „ghost input“ on the HMI’s touch screen

How do you verify this hypothesis?

Meet an unexpected built-in Windows forensics tool

- Usually you are not allowed to install any software on ICS/OT systems
- Sometimes even running forensics tools from removable media is an issue, depending on regulations
- No forensic tool can help you determine a broken touch panel



For Help, click Help Topics on the Help Menu.

Investigation Result

- It was determined a faulty touch screen on the HMI registered ghost input due to overpressure

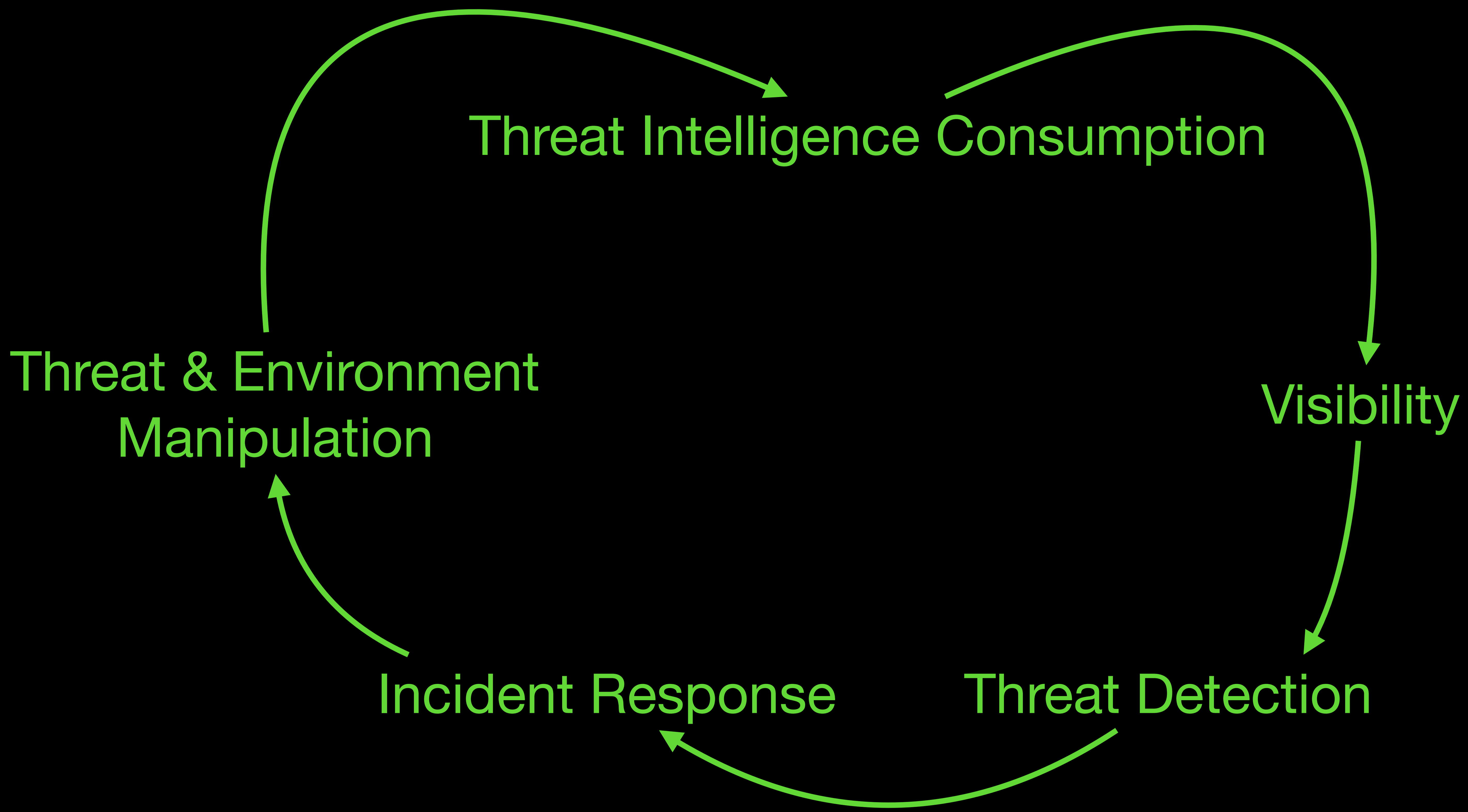
- In ICS/OT Root Cause Analysis, it is important to understand the industrial processes involved, potential environmental effects, and overall context

- Remember:

  ICS/OT = IT + Physics

07.05.2020

Active Cyber Defense Cycle


Threat Intelligence Consumption

Visibility

Threat Detection

Incident Response

Threat & Environment Manipulation

Threat Intelligence Consumption

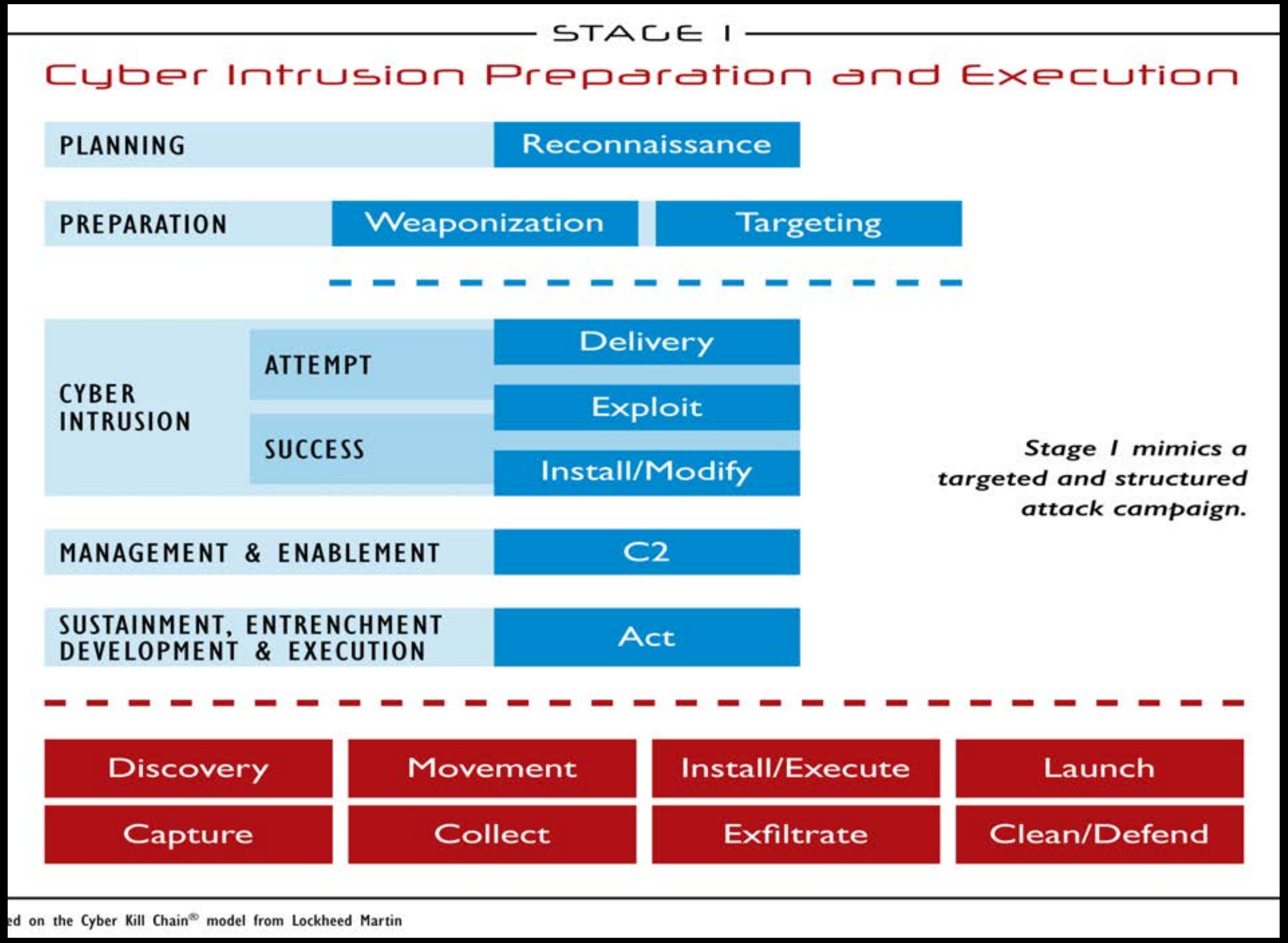
The ICS Cyber Kill Chain

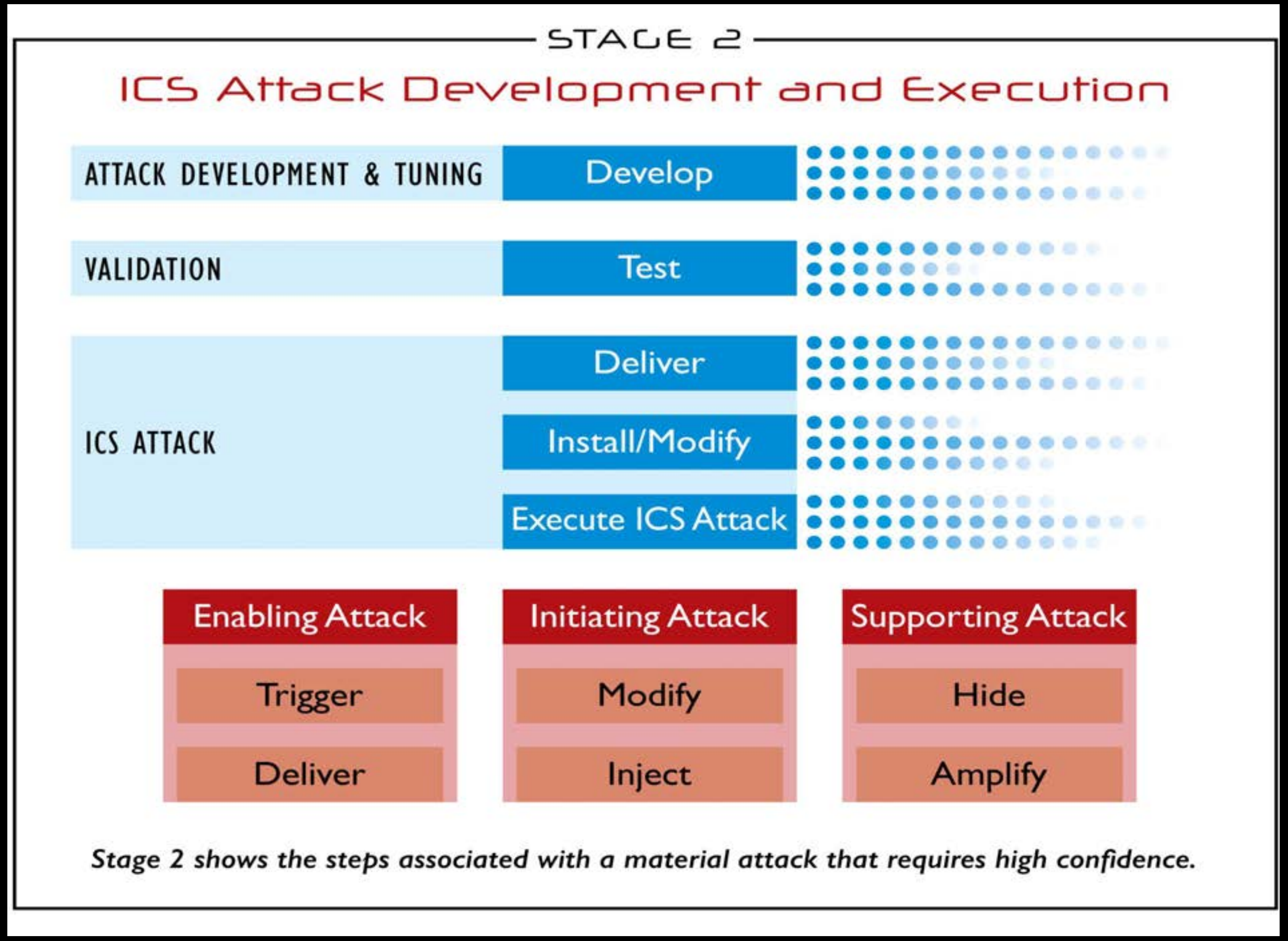
- High confidence attacks with the aim of process manipulation or physical damage require deep ICS knowledge

- This results in significantly longer dwell time of the adversary in a target environment

- An adversary might inadvertently disrupt the ICS during their „research“

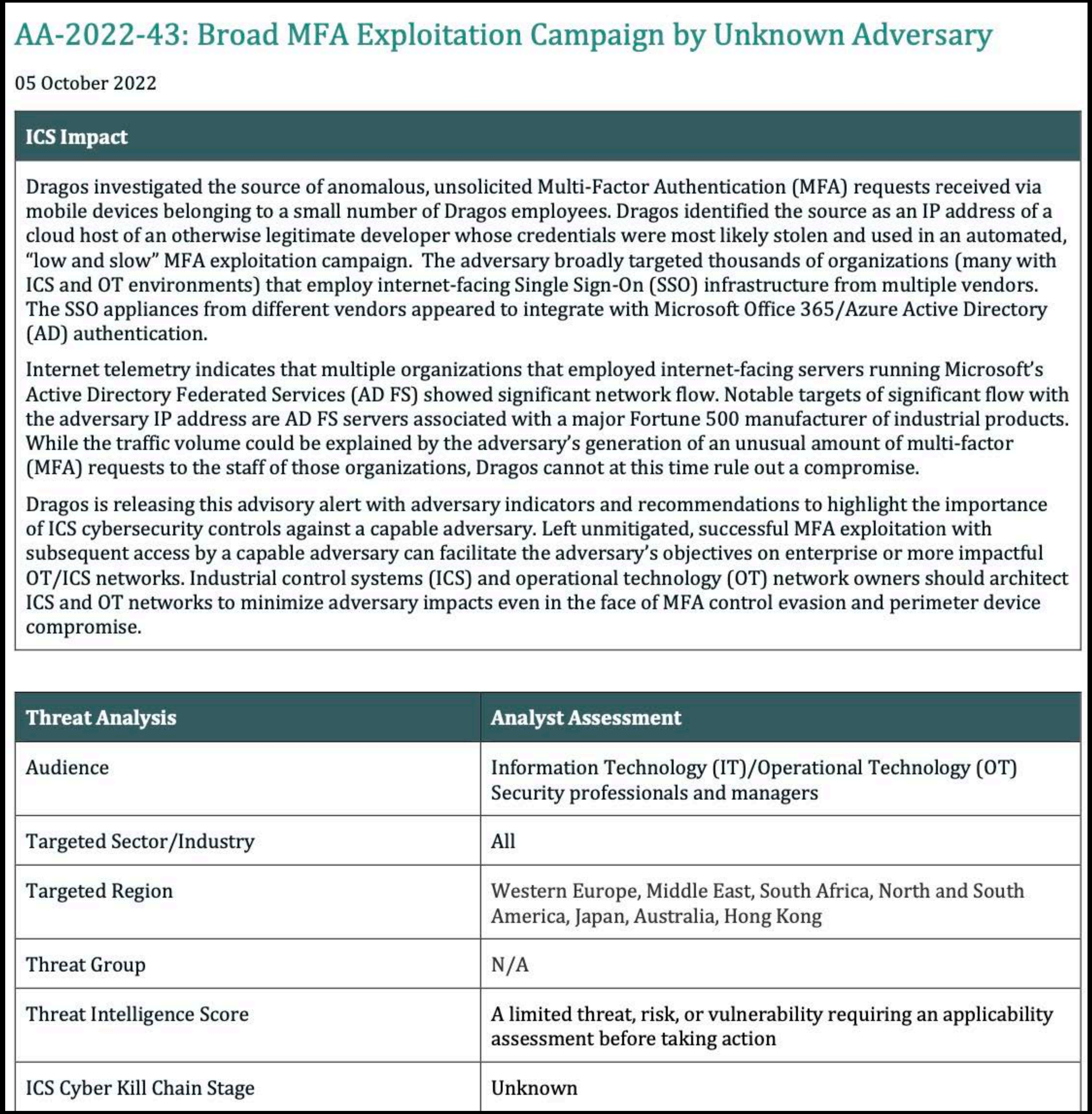
- All of this presents more opportunities to detect the adversary „left of boom“





ICS TI Reports

- Consume reports focused on your
  - Industrial vertical(s)
  - Region
- Favor TTPs over IOCs
- Ensure you provide actionable intelligence internally, i.e. recommendations & guidance
- Understand your organization's
  - Threat Landscape
  - Information Attack Surface
- ICS/OT Threat Intel providers
  - ISACs
  - CERTs
  - Commercial



AA-2022-43: Broad MFA Exploitation Campaign by Unknown Adversary

05 October 2022

ICS Impact

Dragos investigated the source of anomalous, unsolicited Multi-Factor Authentication (MFA) requests received via mobile devices belonging to a small number of Dragos employees. Dragos identified the source as an IP address of a cloud host of an otherwise legitimate developer whose credentials were most likely stolen and used in an automated, "low and slow" MFA exploitation campaign. The adversary broadly targeted thousands of organizations (many with ICS and OT environments) that employ internet-facing Single Sign-On (SSO) infrastructure from multiple vendors. The SSO appliances from different vendors appeared to integrate with Microsoft Office 365/Azure Active Directory (AD) authentication.

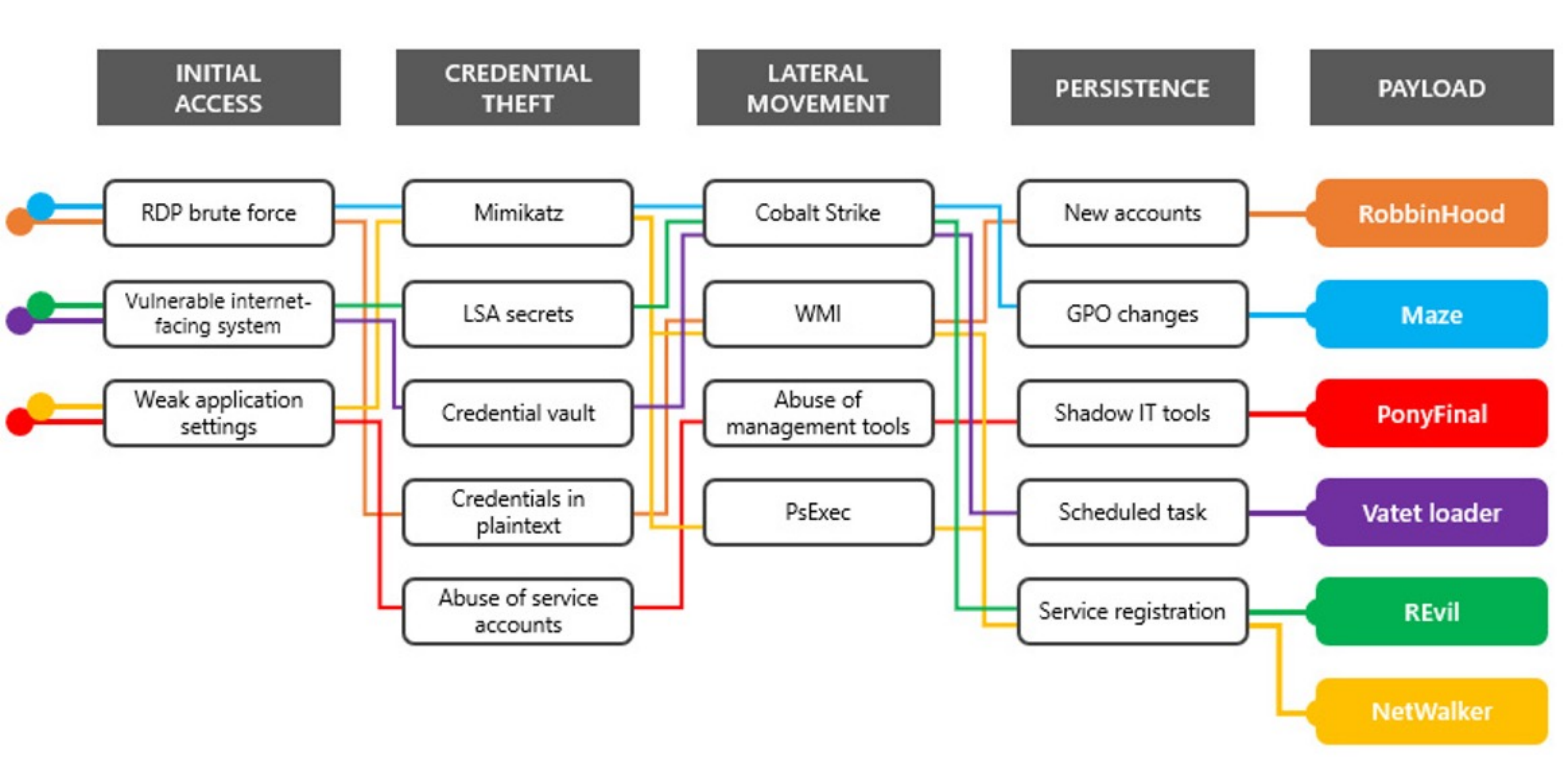
Internet telemetry indicates that multiple organizations that employed internet-facing servers running Microsoft's Active Directory Federated Services (AD FS) showed significant network flow. Notable targets of significant flow with the adversary IP address are AD FS servers associated with a major Fortune 500 manufacturer of industrial products. While the traffic volume could be explained by the adversary's generation of an unusual amount of multi-factor (MFA) requests to the staff of those organizations, Dragos cannot at this time rule out a compromise.

Dragos is releasing this advisory alert with adversary indicators and recommendations to highlight the importance of ICS cybersecurity controls against a capable adversary. Left unmitigated, successful MFA exploitation with subsequent access by a capable adversary can facilitate the adversary's objectives on enterprise or more impactful OT/ICS networks. Industrial control systems (ICS) and operational technology (OT) network owners should architect ICS and OT networks to minimize adversary impacts even in the face of MFA control evasion and perimeter device compromise.

Threat Analysis	Analyst Assessment
Audience	Information Technology (IT)/Operational Technology (OT) Security professionals and managers
Targeted Sector/Industry	All
Targeted Region	Western Europe, Middle East, South Africa, North and South America, Japan, Australia, Hong Kong
Threat Group	N/A
Threat Intelligence Score	A limited threat, risk, or vulnerability requiring an applicability assessment before taking action
ICS Cyber Kill Chain Stage	Unknown

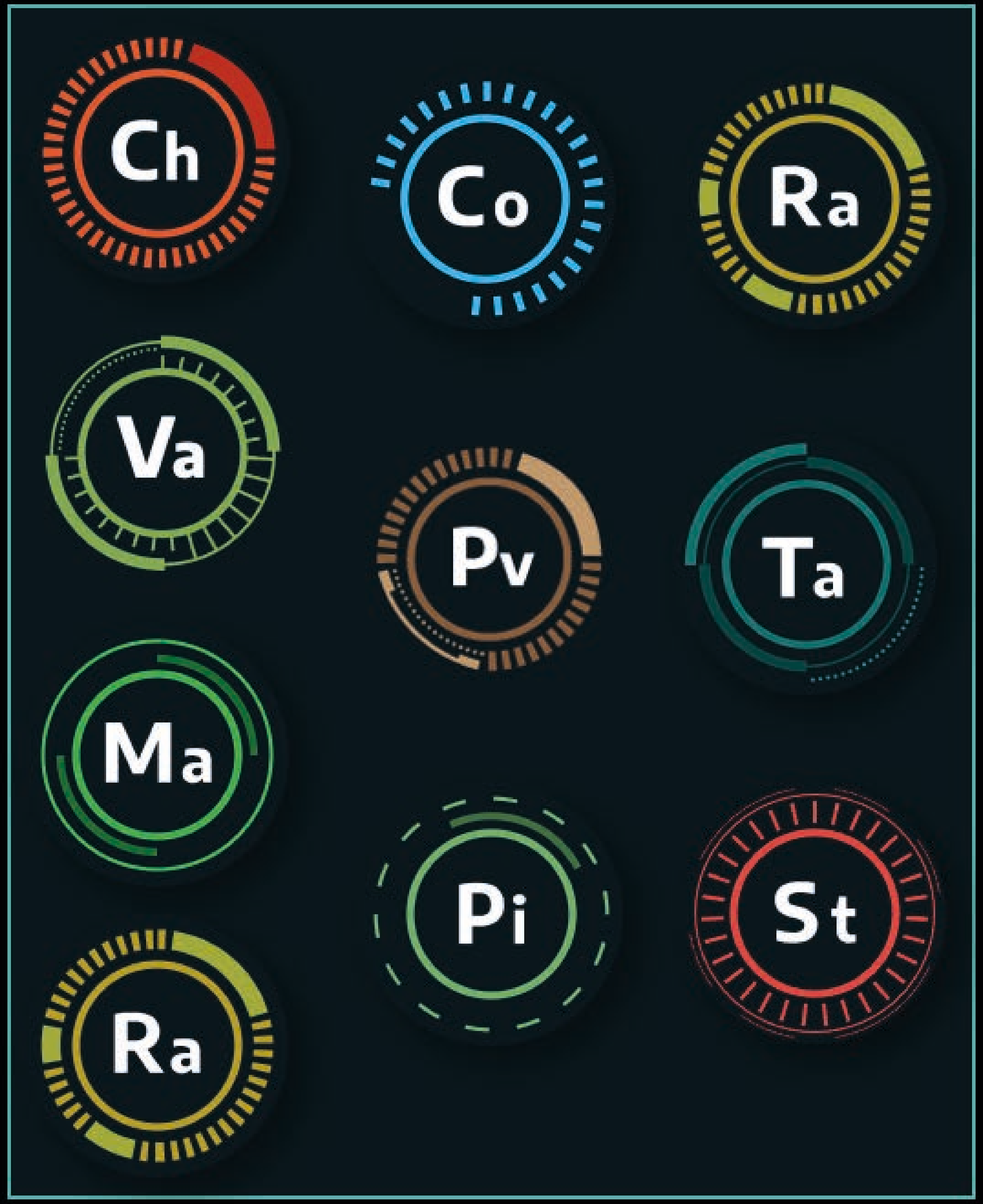
„Actionable Threat Intel“

- Good Threat Intelligence provides immediate value to defenders
- Common questions it should answer
  - What do I need to focus on?
  - What adversaries might be targeting my organization and what are their TTPs?
  - What TTPs are they using along the Kill Chain?



Current Threat Landscape

ICS Curious (ICS CKC Stage 1)



ICS Capable (ICS CKC Stage 2)

Wa
Hx
Dy
Er
AL

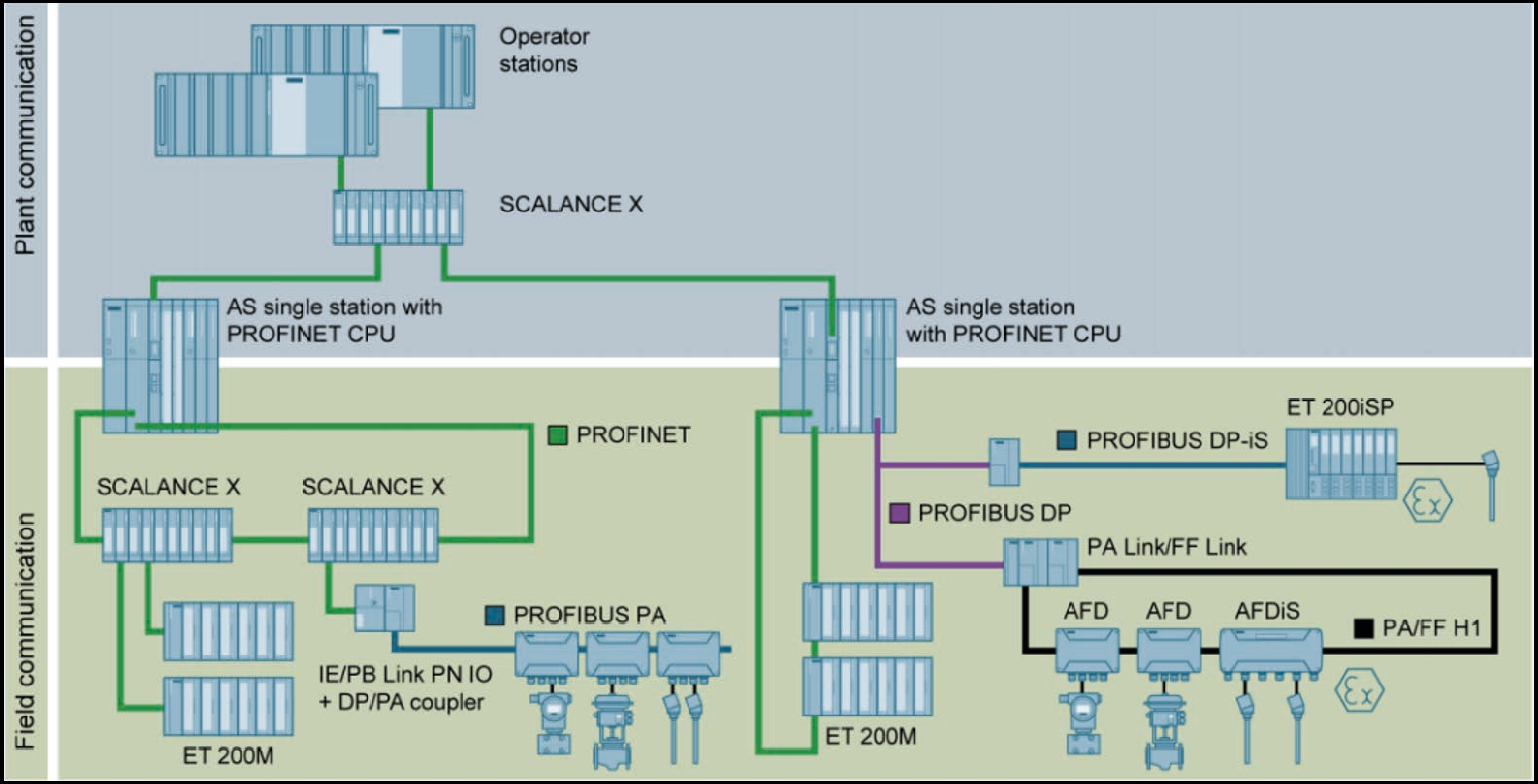
ICS ~~Clowns~~ (ICS CKC Stage 2 – Act)

EL
Ko
Xt
Ka
Cv

Visibility

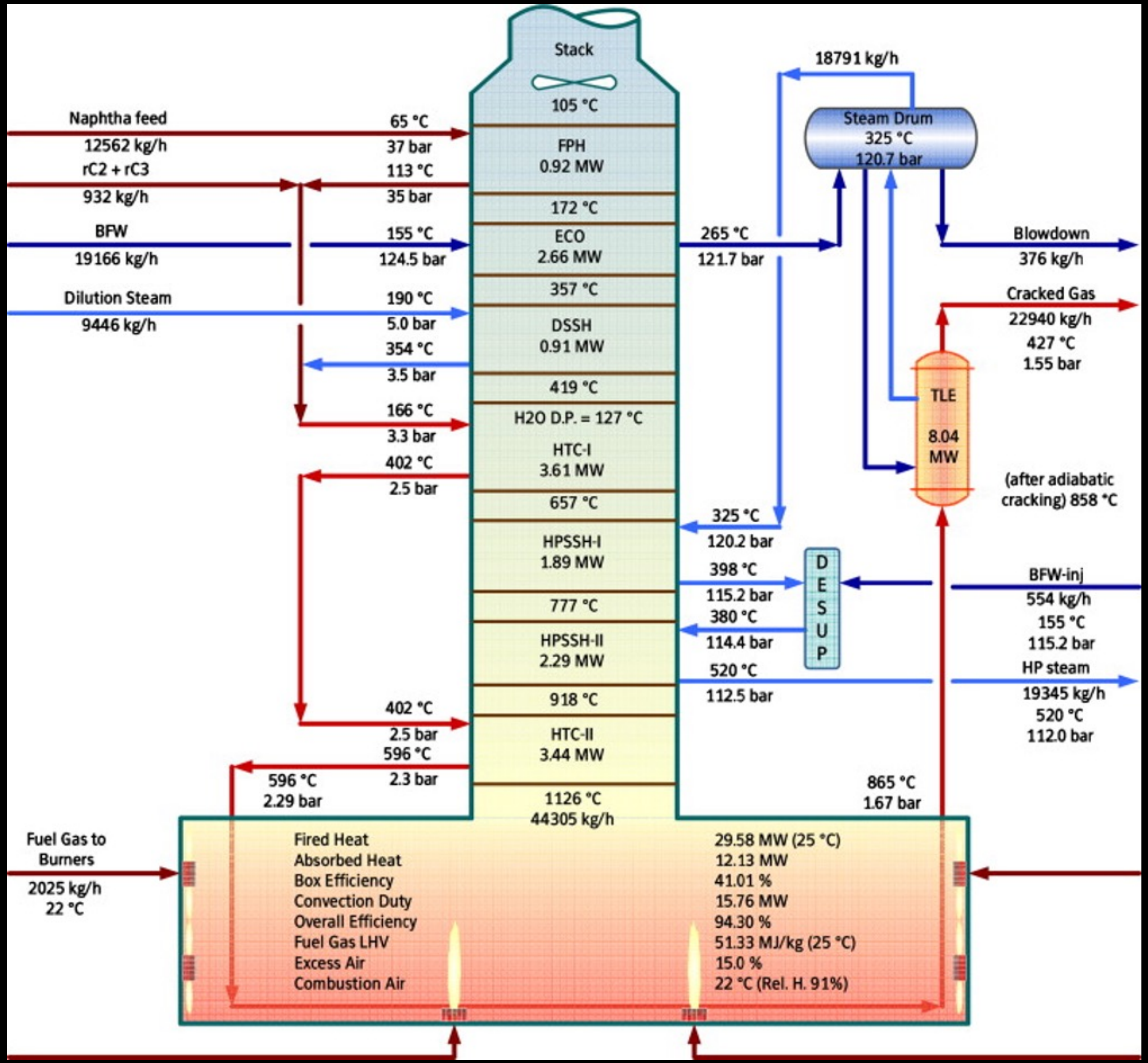
OT = IT + Physics, remember?

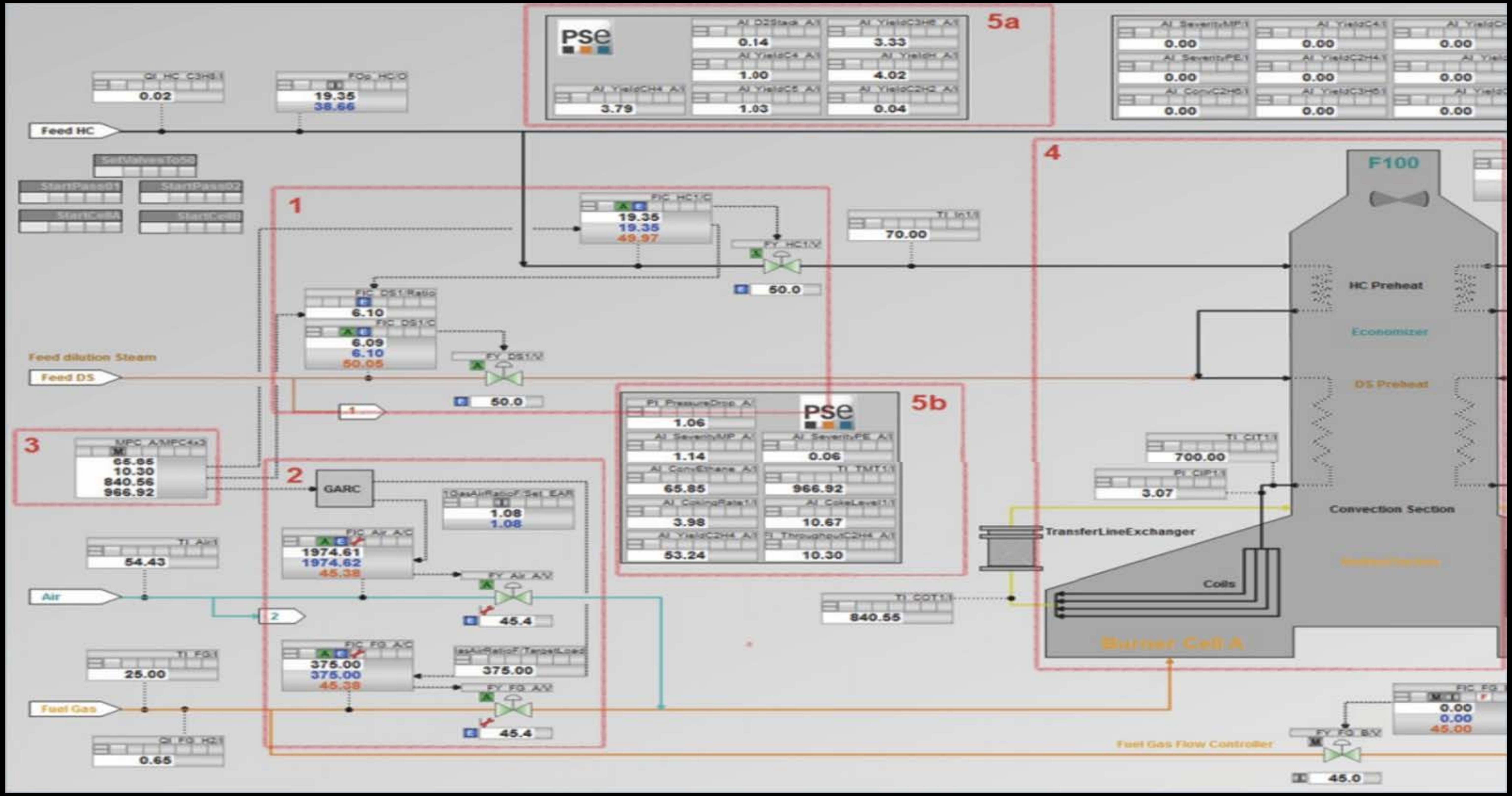
IT



OT = IT + Physics, remember?

Physics





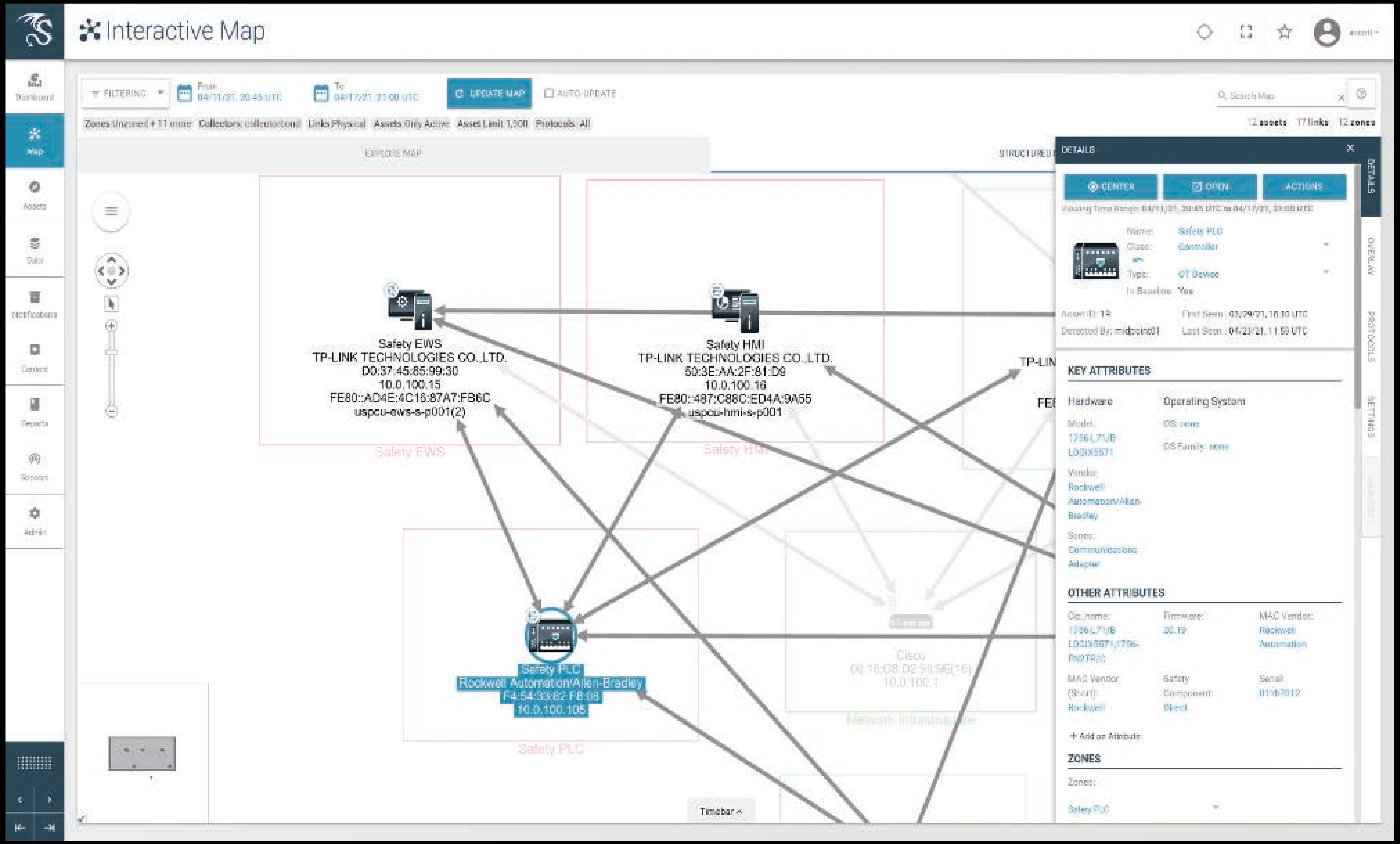
Visibility

- You cannot defend what you don't know you have

- Visibility & monitoring solutions in industrial environments need to be aware of ICS protocols & context

- Whatever solution you choose, ensure it has sufficient protocol coverage for **your ICS environment**

- You will need to at least conceptually map industrial process to network



From: 04/11/21, 20:45 UTC To: 04/17/21, 21:00 UTC

Zones: Unzoned + 11 more Collectors: collector/bond Links: Physical Assets: Only Active Asset Limit: 1,500 Protocols: All

12 assets 17 links 12 zones

Viewing Time Range: 04/11/21, 20:45 UTC to 04/17/21, 21:00 UTC

Name: Safety PLC
Class: Controller
Type: OT Device
In Baseline: Yes

Asset ID: 19 First Seen: 03/29/21, 18:10 UTC
Detected By: midpoint01 Last Seen: 04/23/21, 11:59 UTC

KEY ATTRIBUTES

Hardware
Model: 1756-L71/B LOGIX5571
Vendor: Rockwell Automation/Allen-Bradley
Series: Communications Adapter

Operating System
OS: none
OS Family: none

OTHER ATTRIBUTES

Cip_name: 1756-L71/B LOGIX5571,1756-EN2TR/C
Firmware: 20.19
MAC Vendor: Rockwell Automation
MAC Vendor (Short): Rockwell
Safety Component: Direct
Serial: 011b7012

+ Add an Attribute

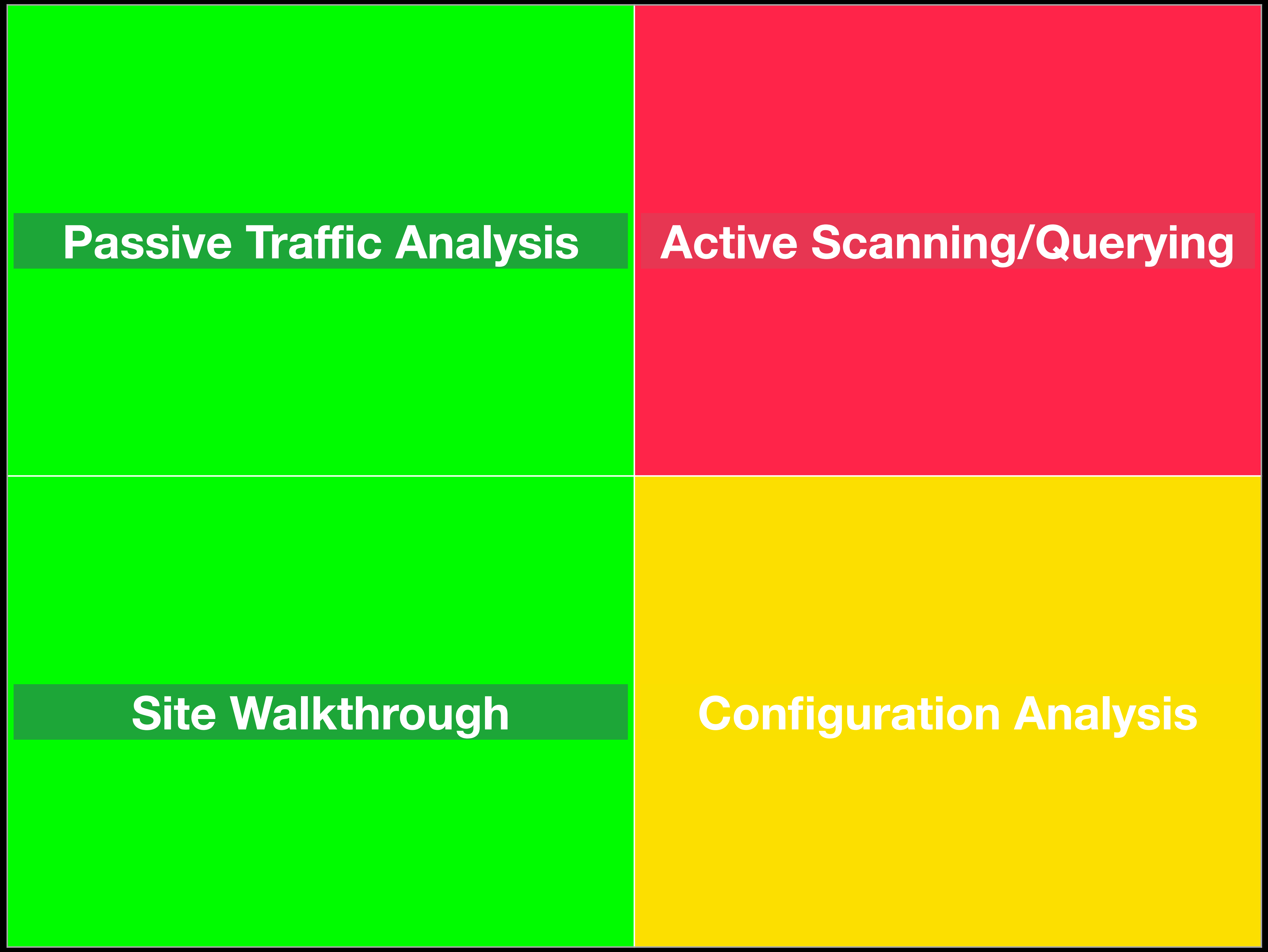
ZONES

Zones: Safety PLC

How to Create an Asset Inventory

Passive Traffic Analysis	Active Scanning/Querying
Site Walkthrough	Configuration Analysis

How to Create an Asset Inventory



🟩 Passive Traffic Analysis	🟥 Active Scanning/Querying
🟩 Site Walkthrough	🟨 Configuration Analysis

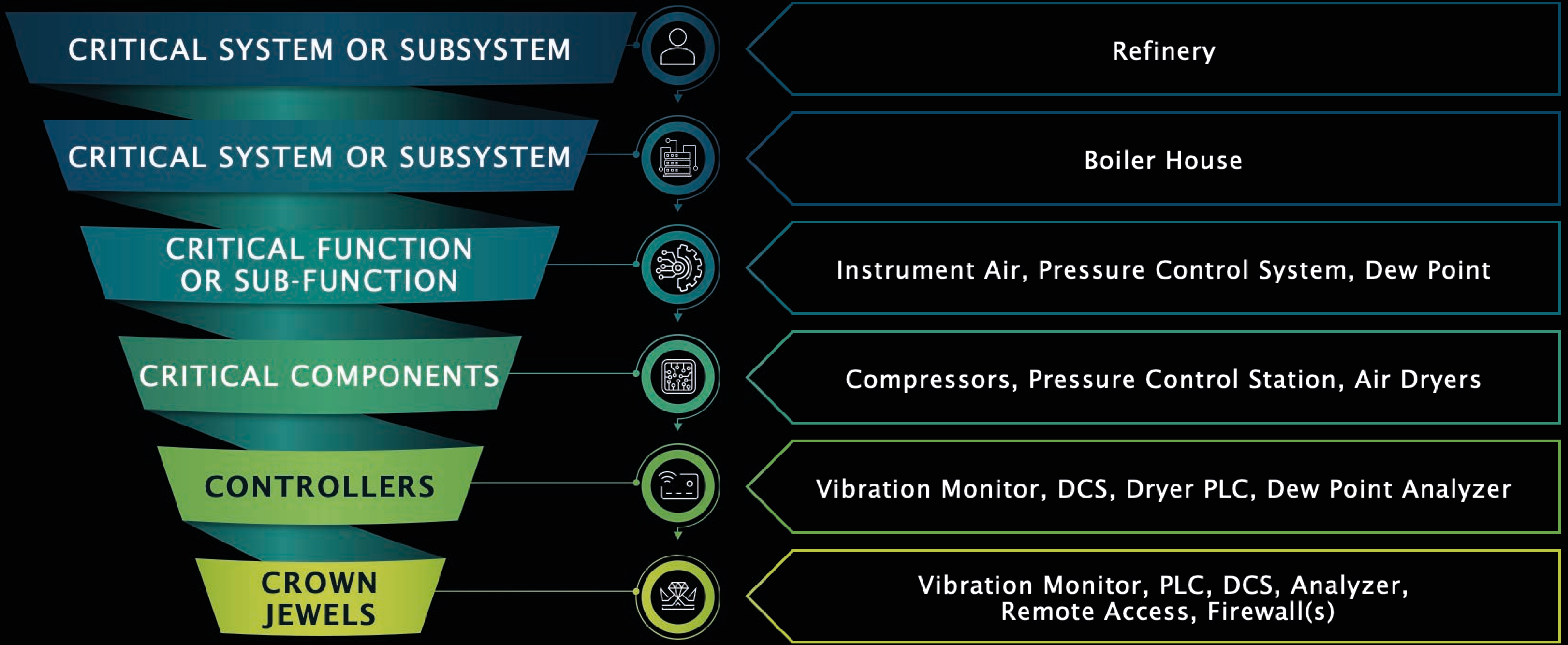
Lowest risk/best results in combination {

High risk of interfering with normal operations

Requires a high amount of subject matter expertise over various technology stacks, but good way to supplement other approaches

PRIORITIZE WHAT MATTERS MOST

RECOMMENDATION: CROWN JEWELS ANALYSIS



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)

Threat Detection

Threat Detection

The 4 Types of Detection

Environment	Threat
Modeling	Threat Behaviors
Configuration Analysis	Indicators

Threat Detection

Configuration Analysis

- Aka Whitelisting
- Great for investigations when baselines exist, especially for any host systems
- Usually generates too many (false) alerts for initial detection

Environment	Threat
Modeling	Threat Behaviors
Configuration Analysis	Indicators

Threat Detection

Modeling

- Aka „Machine Learning“ or (even worse) „AI Based Detection“
- Statistical/Threshold Based Modeling to allow for some variance until an event is triggered
- Great for enhancing analysis and investigations, not only on network activity, but also for alerting on variance in industrial processes that cross a threshold
- Mostly not effective for initial detection as the vendor’s model is certainly not based on *your* ICS environment

Environment	Threat
Modeling	Threat Behaviors
Configuration Analysis	Indicators

Threat Detection

Indicators

- Indicators of Compromise (IOCs) are the most common method for detection
- We are dealing with highly sophisticated adversaries in ICS/OT, they do use different infrastructure for different targets, thus often (even more) ineffective for initial detection than in IT
- IOCs gathered during DFIR investigations are *highly effective* for scoping the extent of a breach, especially when enhanced/extended through Threat Intel consumption

Environment	Threat
Modeling	Threat Behaviors
Configuration Analysis	Indicators

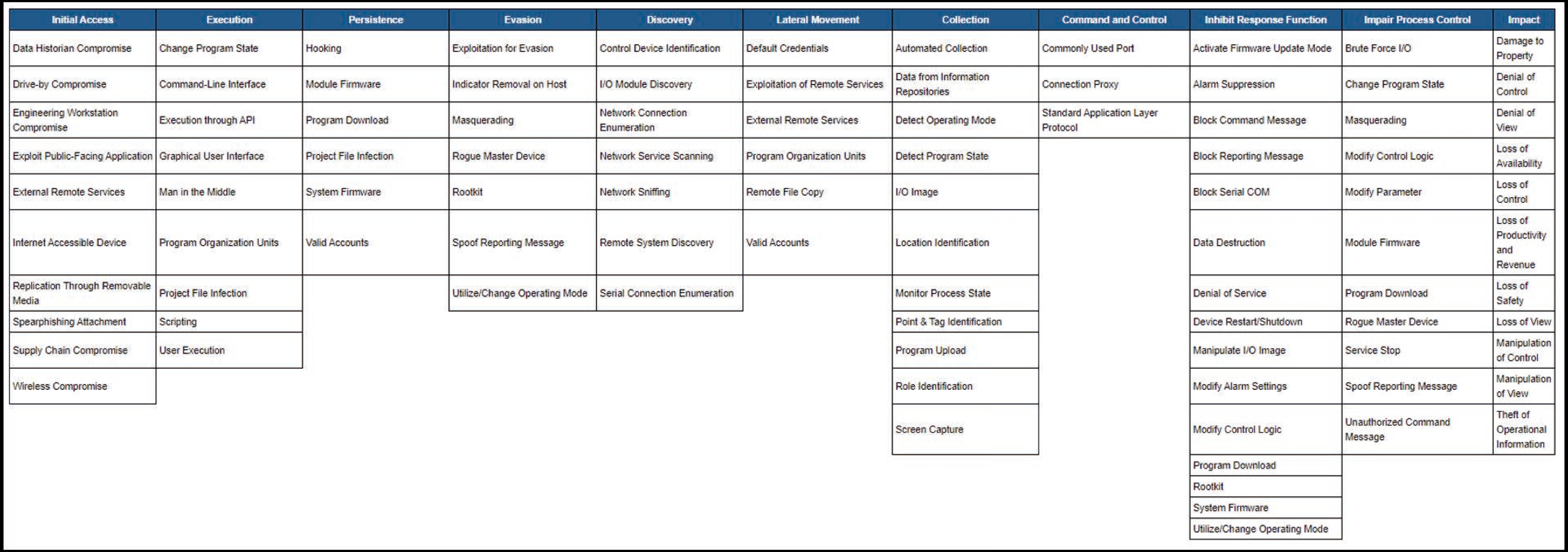
Threat Detection

Threat Behaviors

- Threat Behaviors aka TTPs are the most effective for of detecting potentially malicious behavior
- It is hard for humans (think training, habits, budgets) to change behavior. Adversaries are humans, too 😉
- Sometimes difficult to encode into detections in your (often IOC biased) defense toolkit
- If you are good at detecting typical adversary behavior, you will detect activity even if they are using 0-days

Environment	Threat
Modeling	Threat Behaviors
Configuration Analysis	Indicators

Mitre ICS Att&ck Matrix

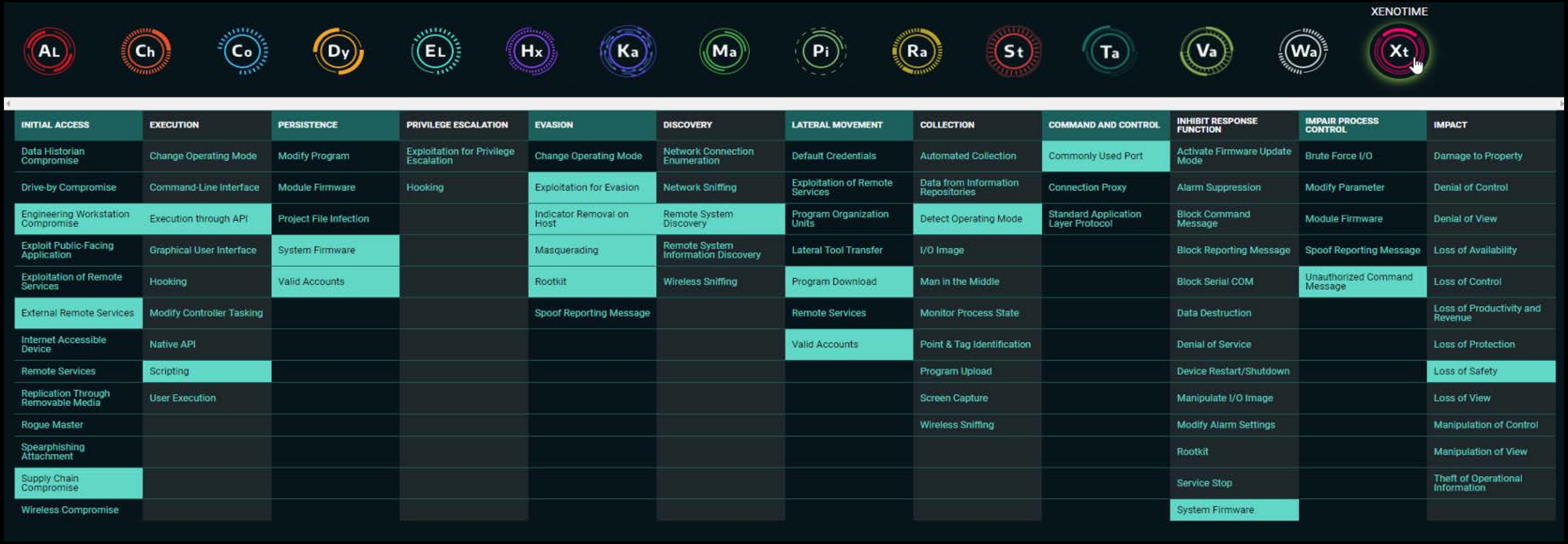


Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Source: https://collaborate.mitre.org/attackics/index.php/Main_Page

Mapping Threat Groups & ICS Att&ck

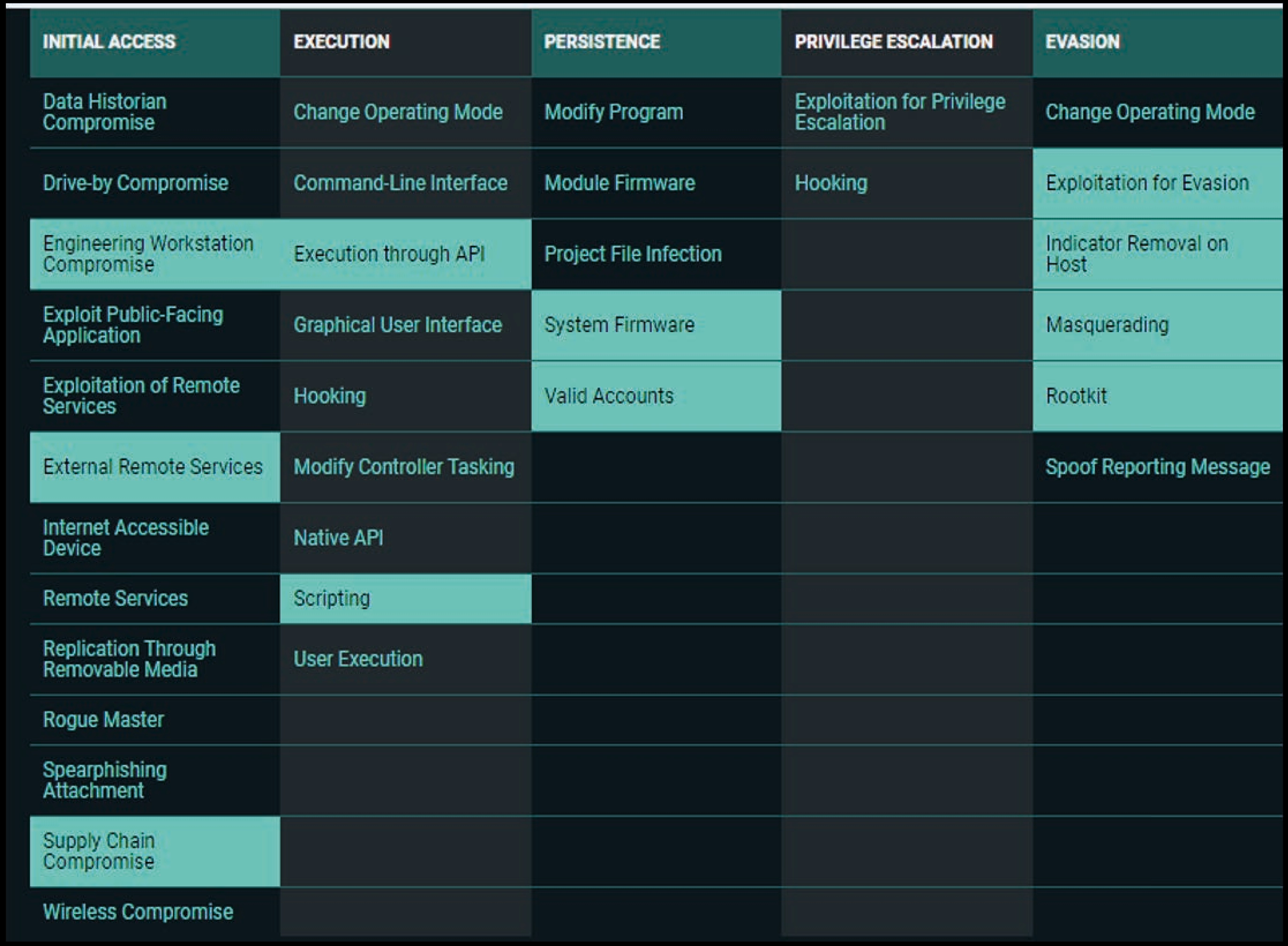
XENOTIME



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	**Commonly Used Port**	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	**Exploitation for Evasion**	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	**Execution through API**	Project File Infection		**Indicator Removal on Host**	**Remote System Discovery**	Program Organization Units	**Detect Operating Mode**	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	**System Firmware**		**Masquerading**	Remote System Information Discovery	Lateral Tool Transfer	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	**Valid Accounts**		**Rootkit**	Wireless Sniffing	**Program Download**	Man in the Middle		Block Serial COM	**Unauthorized Command Message**	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API					**Valid Accounts**	Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	**Scripting**						Program Upload		Device Restart/Shutdown		**Loss of Safety**
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									**System Firmware**		

XENOTIME in Depth

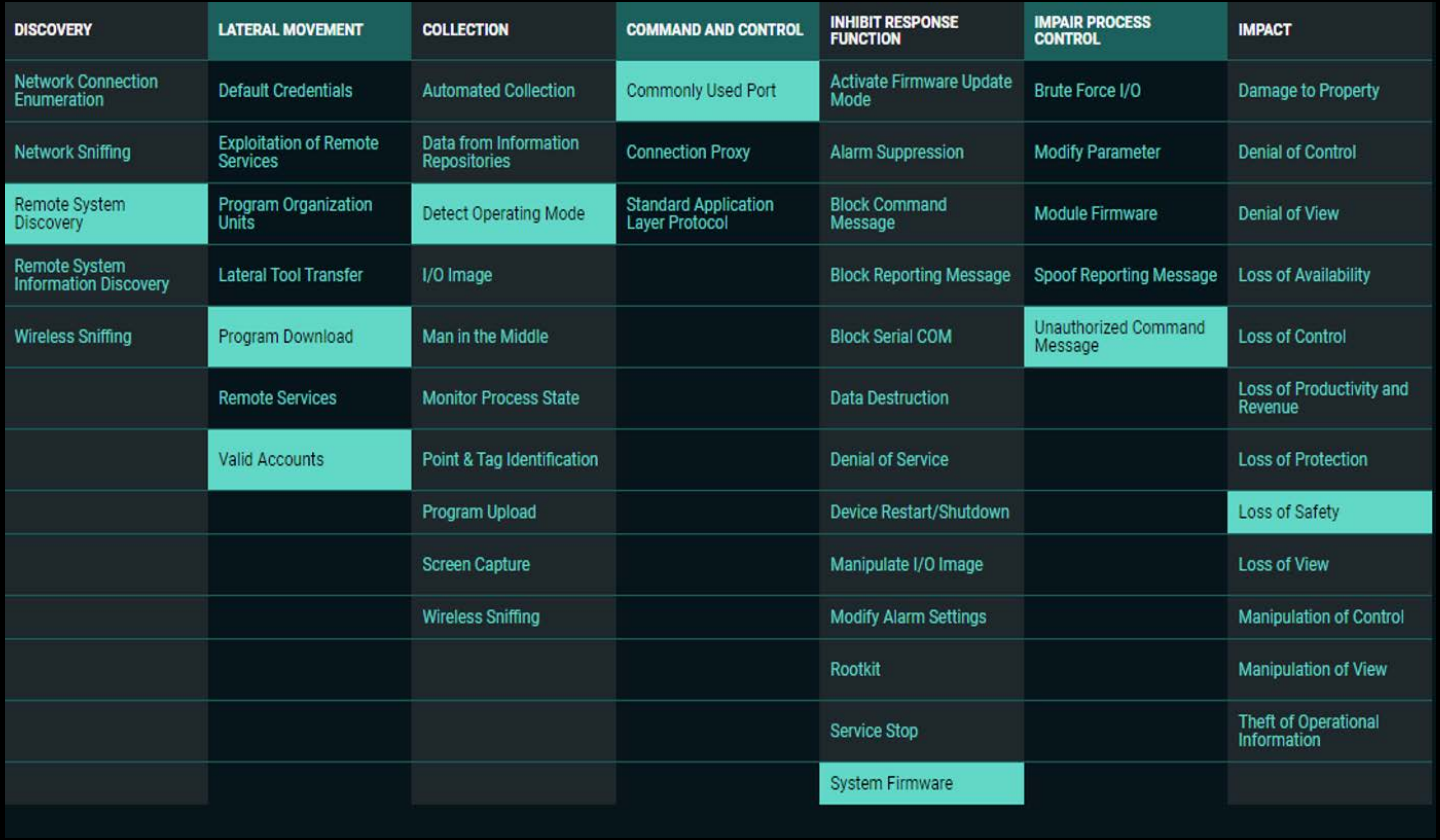
Detect more than one technique per Kill Chain Phase



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit
External Remote Services	Modify Controller Tasking			Spoof Reporting Message
Internet Accessible Device	Native API			
Remote Services	Scripting			
Replication Through Removable Media	User Execution			
Rogue Master				
Spearphishing Attachment				
Supply Chain Compromise				
Wireless Compromise				

XENOTIME in Breadth

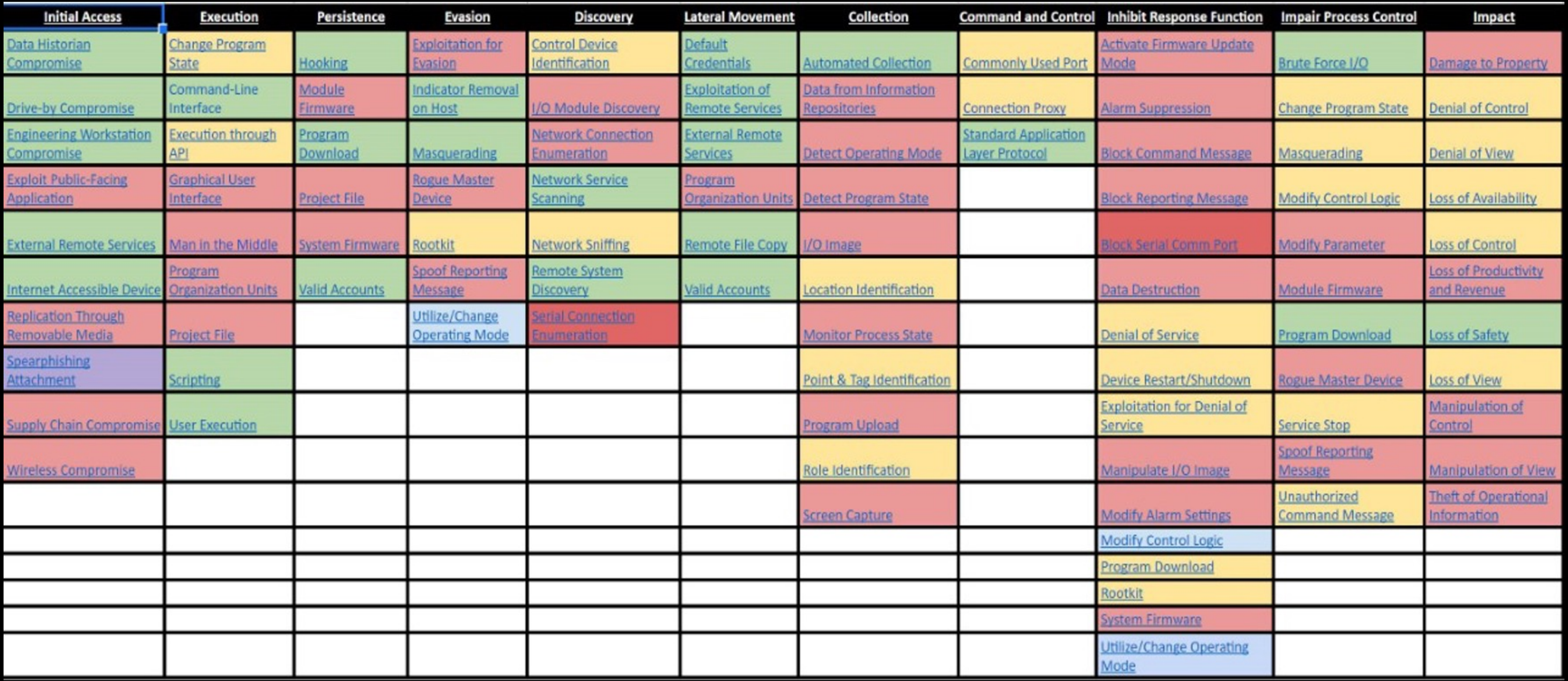
Detections over multiple Kill Chain phases



DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Network Connection Enumeration	Default Credentials	Automated Collection	**Commonly Used Port**	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Remote System Discovery	Program Organization Units	**Detect Operating Mode**	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Remote System Information Discovery	Lateral Tool Transfer	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Wireless Sniffing	**Program Download**	Man in the Middle		Block Serial COM	**Unauthorized Command Message**	Loss of Control
	Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
	Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
		Program Upload		Device Restart/Shutdown		**Loss of Safety**
		Screen Capture		Manipulate I/O Image		Loss of View
		Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
				Rootkit		Manipulation of View
				Service Stop		Theft of Operational Information
				System Firmware		

Coverage and Gap Analysis

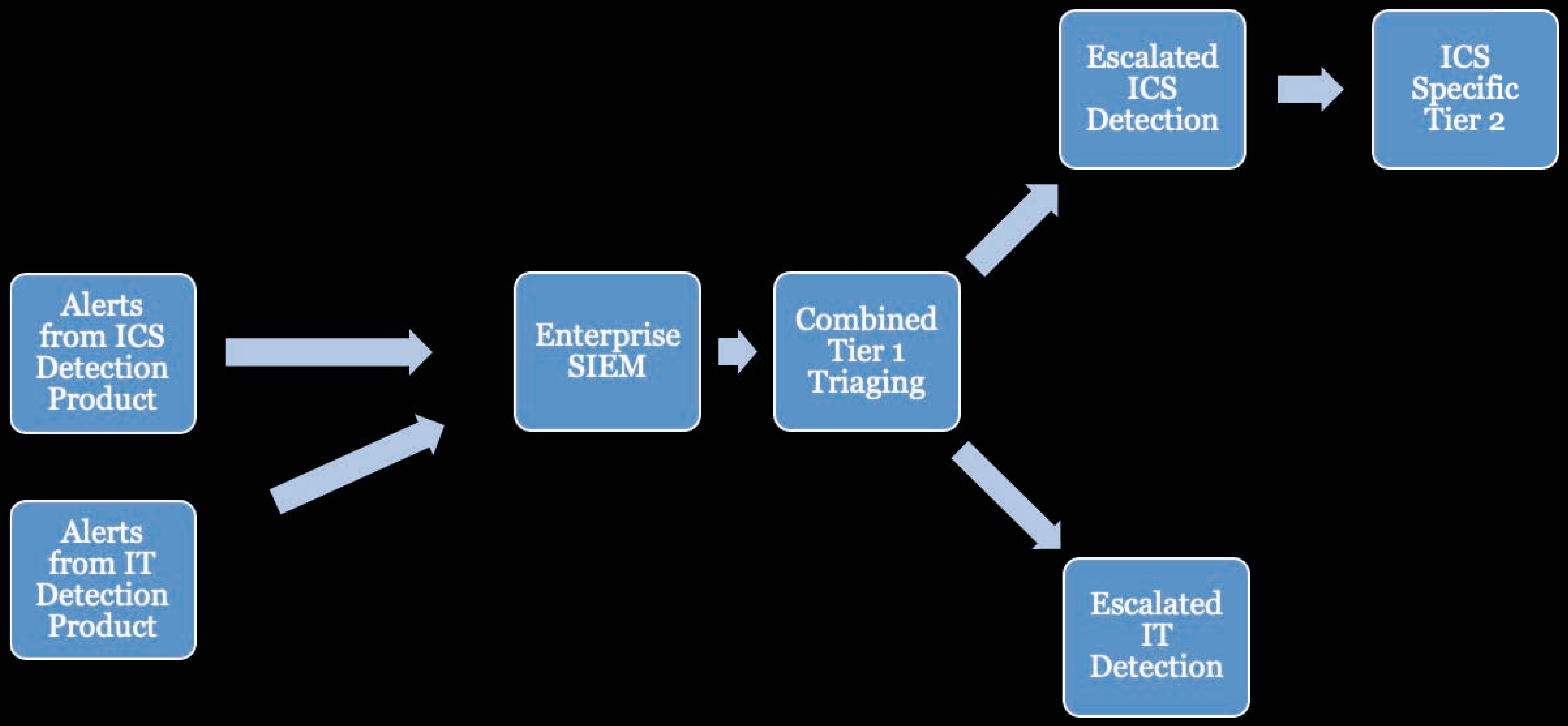
Red and Yellow = Your Security Monitoring Program Roadmap



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial Comm Port	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Exploitation for Denial of Service	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Manipulate I/O Image	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Alarm Settings	Unauthorized Command Message	Theft of Operational Information
								Modify Control Logic		
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

IT/OT SOC Workflow Recommendations

Remember the 2 stages of the ICS Cyber Kill Chain. It starts in IT!



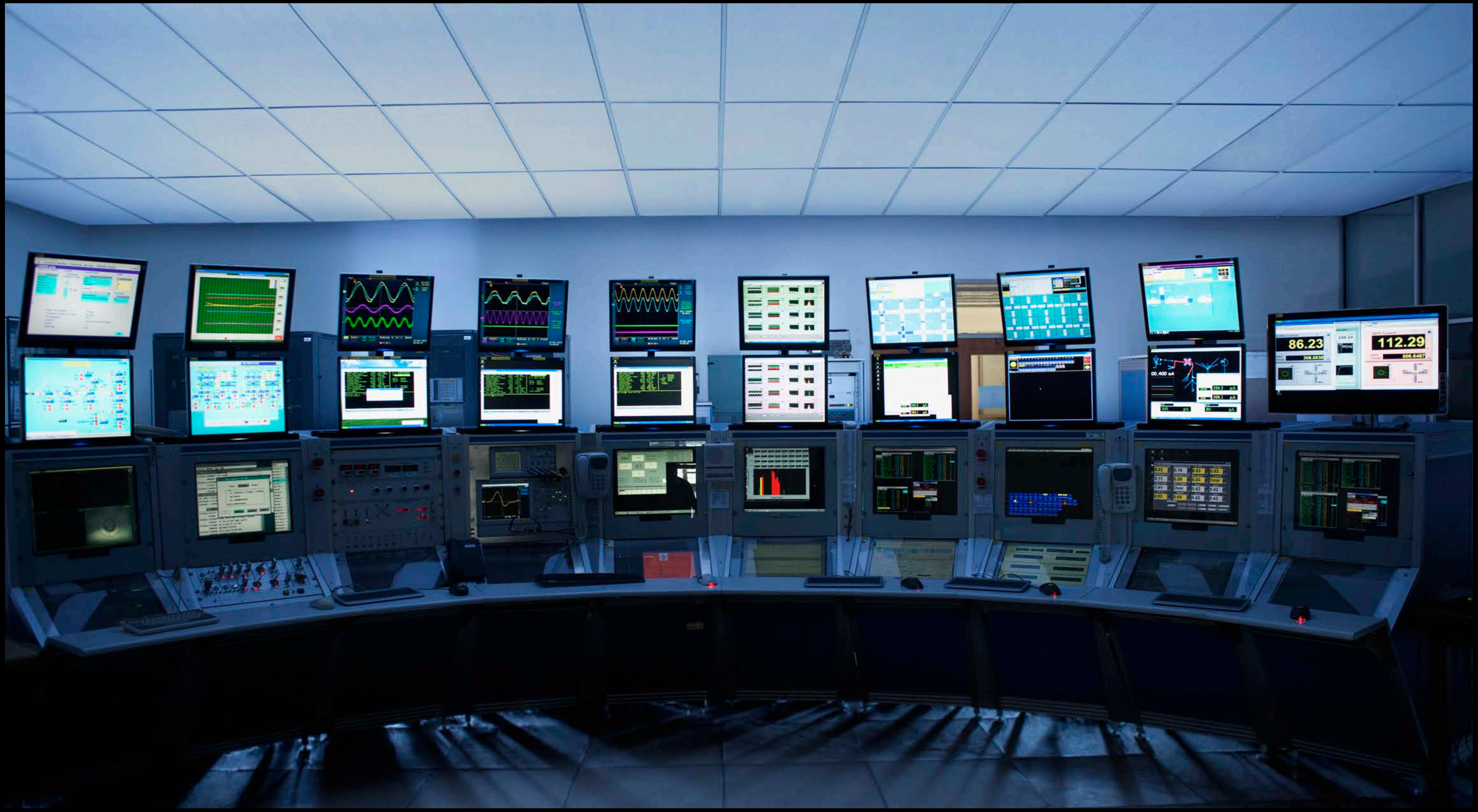
Incident Response

Different Mission, Different Requirements

And a lot of different challenges…

Considerations

- Regulations
- Compliance
- Laws
- Safety & Reliability
- Unions
- Governments
- Vendors
- Legacy/Unique Systems
- Data Collection



PICERL Differences

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

PICERL Differences

Preparation

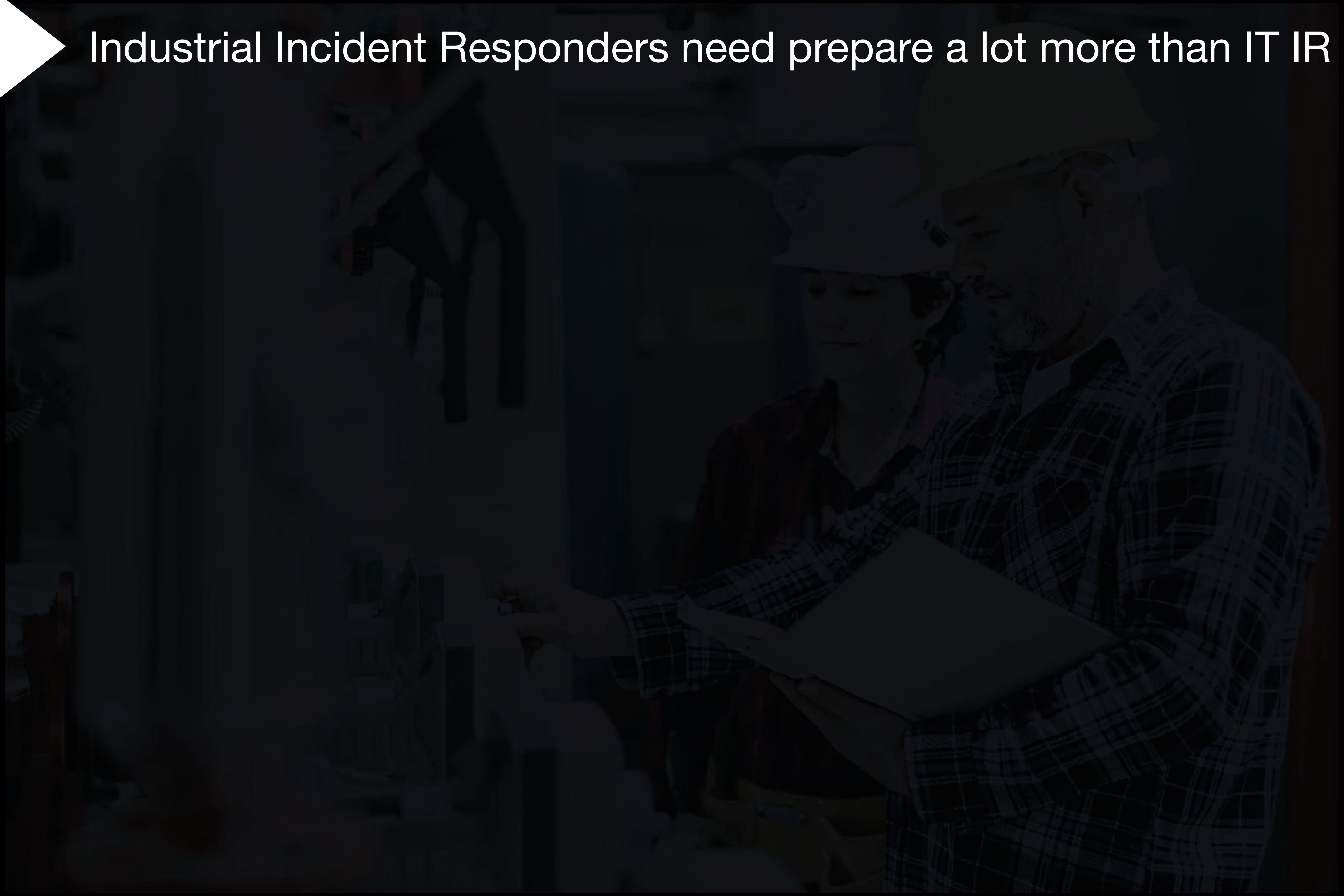
Identification

Containment

Eradication

Recovery

Lessons Learned



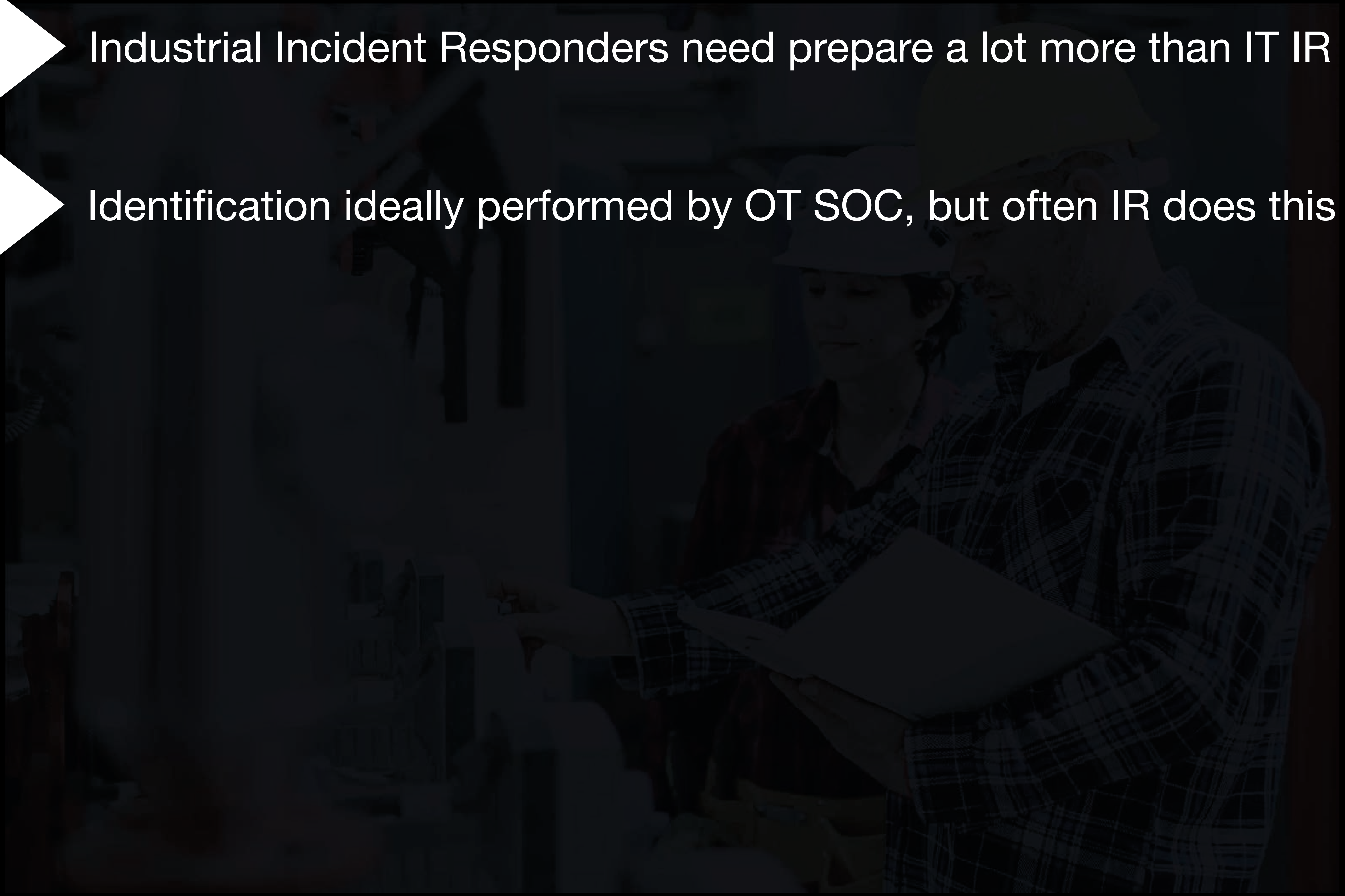
Industrial Incident Responders need prepare a lot more than IT IR

Preparation

Things to consider

- PPE. If you're not wearing the proper gear, no entry
- Safety Certifications. Think NERC CIP, BOSIET, etc.
- Connectors, cables, and SW tools to connect to old/legacy equipment
- Out-of-band comms. Some plants are large and don't have good mobile phone coverage. Verify the comms meet the local safety requirements!
- How to obtain forensic data from ICS systems
- Where to analyze the data. Are you allowed to remove data from the plant? The country?

PICERL Differences



Preparation → Industrial Incident Responders need prepare a lot more than IT IR

Identification → Identification ideally performed by OT SOC, but often IR does this

Containment

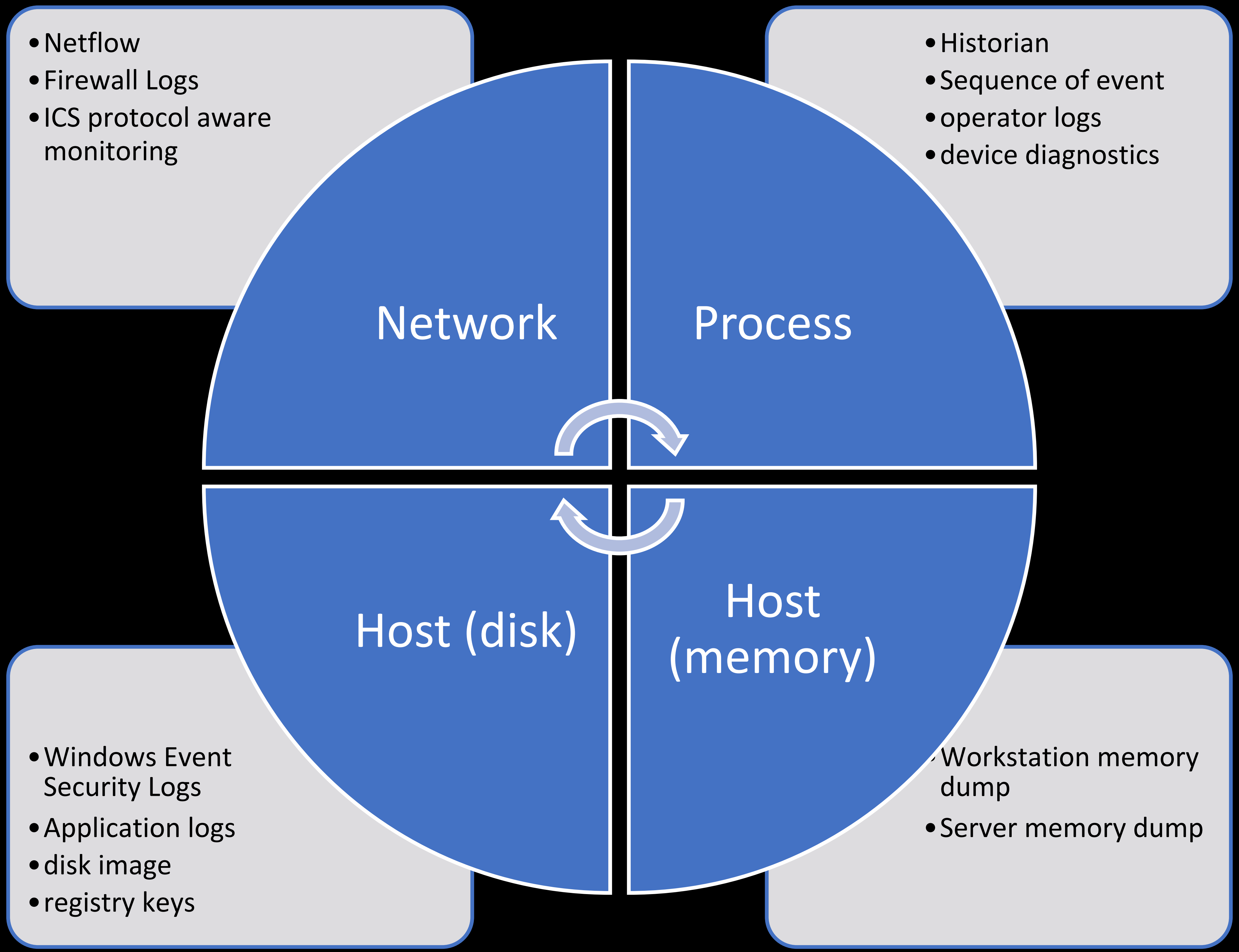
Eradication

Recovery

Lessons Learned

Forensic Data Sets

You need to map cyber to physical process



- Netflow
- Firewall Logs
- ICS protocol aware monitoring

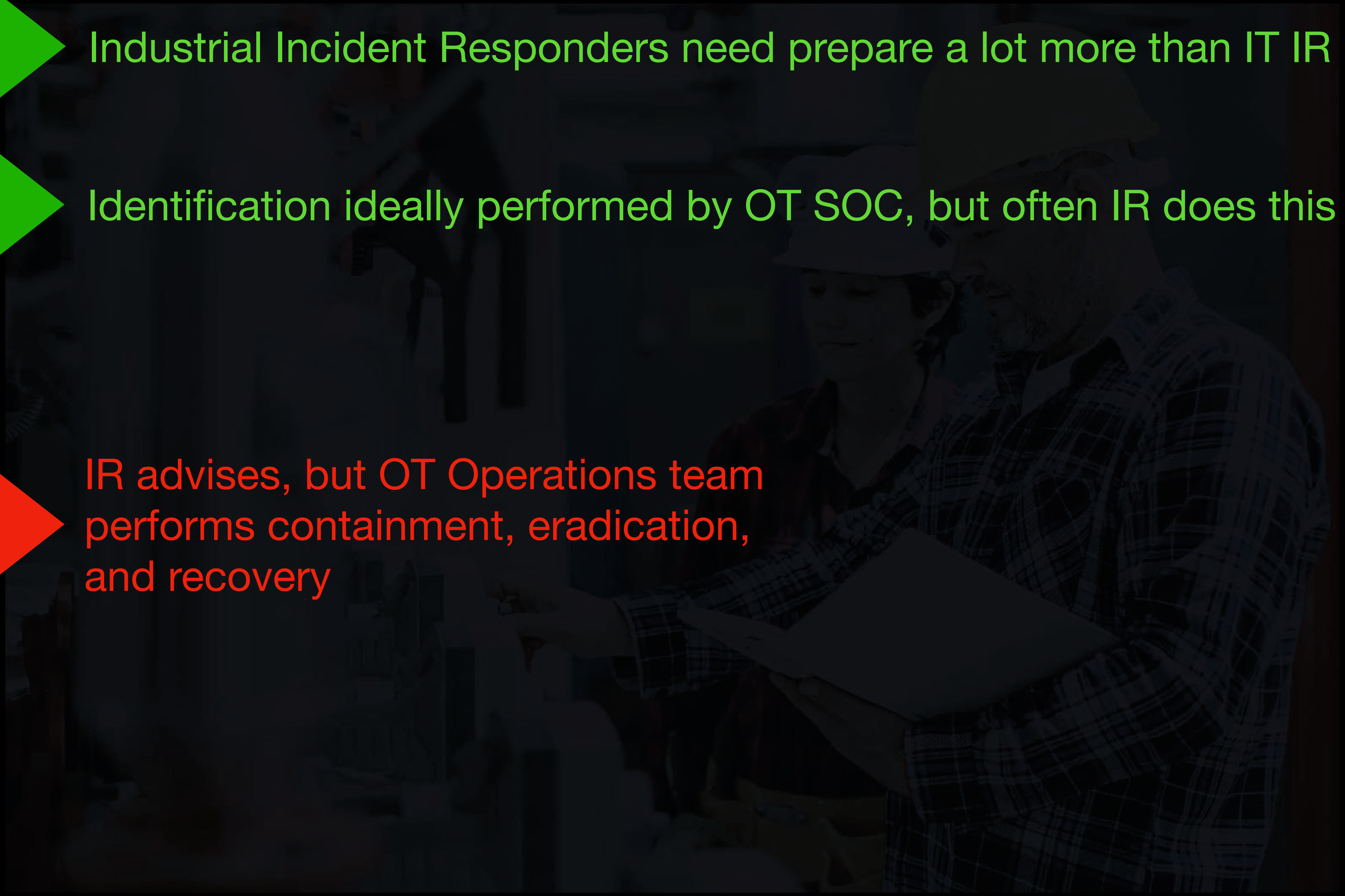
- Historian
- Sequence of event
- operator logs
- device diagnostics

- Windows Event Security Logs
- Application logs
- disk image
- registry keys

- Workstation memory dump
- Server memory dump

This is new territory for you enterprise folks

PICERL Differences



Preparation → Industrial Incident Responders need prepare a lot more than IT IR

Identification → Identification ideally performed by OT SOC, but often IR does this

Containment

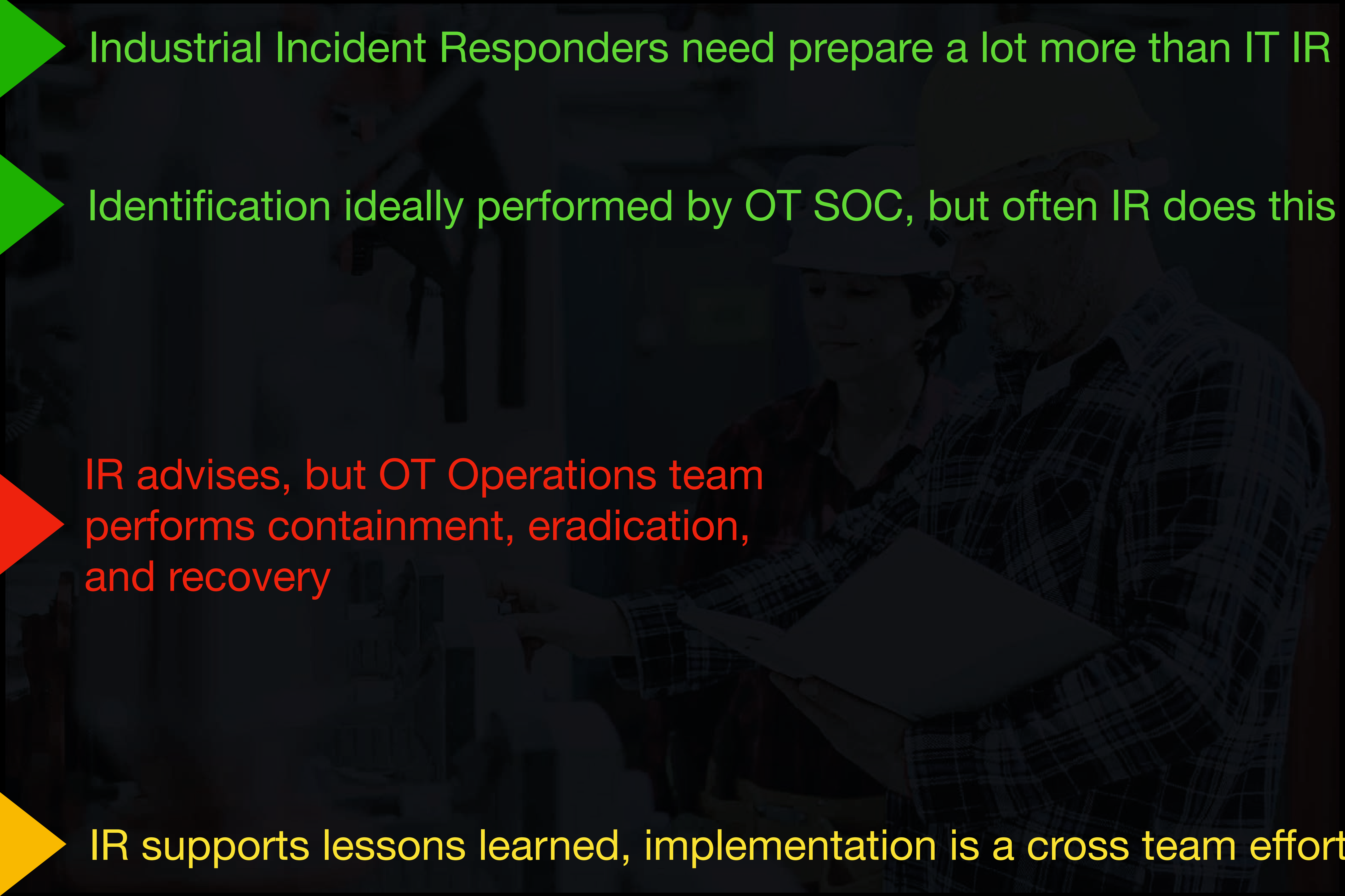
Eradication

Recovery

→ IR advises, but OT Operations team performs containment, eradication, and recovery

Lessons Learned

PICERL Differences



Preparation → Industrial Incident Responders need prepare a lot more than IT IR

Identification → Identification ideally performed by OT SOC, but often IR does this

Containment

Eradication

Recovery

→ IR advises, but OT Operations team performs containment, eradication, and recovery

Lessons Learned → IR supports lessons learned, implementation is a cross team effort

Collection Management Frameworks

Collection Management Framework (CMF)

What:

- A “Collection Management Framework” is a process for identifying and documenting data sources which could answer important business-related questions or investigations

Why:

- Locating resources preemptively reduces a team’s response time to an incident
- Conducting a CMF will identify gaps in visibility and enable defenders to fill them before the data is needed

Process

The 5 Steps of a CMF

1. Develop requirements
2. Develop a collection plan
3. Enhance the collection plan
4. Test the plan
5. Update the plan

Develop Requirements

What:

- Achieving business objectives requires information. “Requirements” are questions which seek that necessary information

Why:

- A list of requirements (questions) enables defenders to search for data sources and decide which are relevant, which exist, and which do not.

How:

- Initial requirements for a CMF generally address the safety of mission-critical systems.
- Other requirements can be drawn from activities like table-top exercises, Crown Jewels Analysis, vulnerability analysis, etc

Example

What were the most critical items in our last vulnerability scan of Refinery A?

How could an adversary exploit these?

What activity-groups target our industry?

Develop a Collection Plan

What:

The Collection Plan is the product – it can take whatever form is useful to the analyst. A Collection Plan for incident responders may be an excel sheet of assets and log repositories while one about vulnerability analysis might be a list of links to documents such as an asset inventory and system update policies.

How:

Break down requirements into specific questions which can be answered by data sources. Identify if the data sources exist and add them to a CP.

Example

An activity group which targets your industry has started a new spear phishing campaign. How could you tell if an employee clicked a malicious link?

- Firewall logs
- DNS logs
- IDS alerts…

Enhance the Collection Plan

What:

In this phase, an organization should enhance existing data sources (e.g. retention period of logs), create data sources where they do not exist but should, and create new policies and procedures to streamline access to data sources.

Why:

As the team investigates its data sources, it will recognize gaps and points of tension which will unacceptably inhibit responses.

Example

- Windows logs on the IT network are forwarded to a central server, but not on the OT network – fix it!
- The current procedure means it takes an analyst at least a day to retrieve firewall logs – consider making an emergency procedure to shorten that time, at a minimum.

Test the Plan

What:

- Implement the collection plan and observe for strengths and weaknesses.

Why:

- Changing the way assets log or various policies and procedures may create new issues.

How:

- Develop and act on training scenarios requiring the use of the collection plans

Example

A system may have greater logging capacity than was previously utilized. Turning on these new logs may reduce retention of all logs below an acceptable level, requiring further tuning.

Update the Plan

What:

- In addition to making any changes made apparent by testing, the entire system must be continually assessed and modified.

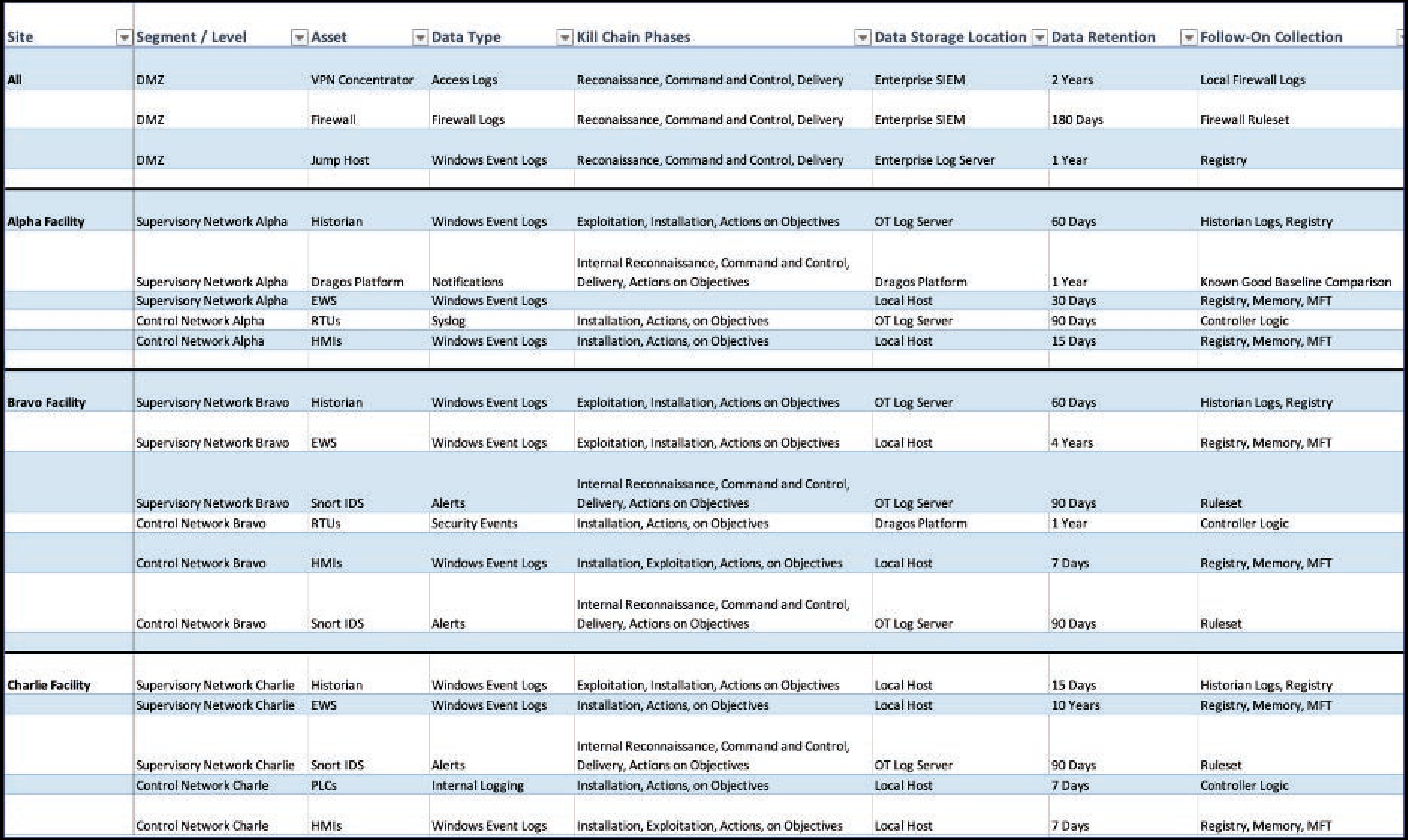
Why:

- Over time, requirements will change, and data sources will cease to exist or new ones will be added. Without editing, it will not provide useful or accurate information.

Example

Your company has sold off a business line whose infrastructure included your Windows logging hub. Build a new hub and update the CMF accordingly.

Example CMF



Site	Segment / Level	Asset	Data Type	Kill Chain Phases	Data Storage Location	Data Retention	Follow-On Collection
All	DMZ	VPN Concentrator	Access Logs	Reconaissance, Command and Control, Delivery	Enterprise SIEM	2 Years	Local Firewall Logs
	DMZ	Firewall	Firewall Logs	Reconaissance, Command and Control, Delivery	Enterprise SIEM	180 Days	Firewall Ruleset
	DMZ	Jump Host	Windows Event Logs	Reconaissance, Command and Control, Delivery	Enterprise Log Server	1 Year	Registry
Alpha Facility	Supervisory Network Alpha	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	OT Log Server	60 Days	Historian Logs, Registry
	Supervisory Network Alpha	Dragos Platform	Notifications	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Dragos Platform	1 Year	Known Good Baseline Comparison
	Supervisory Network Alpha	EWS	Windows Event Logs		Local Host	30 Days	Registry, Memory, MFT
	Control Network Alpha	RTUs	Syslog	Installation, Actions, on Objectives	OT Log Server	90 Days	Controller Logic
	Control Network Alpha	HMIs	Windows Event Logs	Installation, Actions, on Objectives	Local Host	15 Days	Registry, Memory, MFT
Bravo Facility	Supervisory Network Bravo	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	OT Log Server	60 Days	Historian Logs, Registry
	Supervisory Network Bravo	EWS	Windows Event Logs	Exploitation, Installation, Actions on Objectives	Local Host	4 Years	Registry, Memory, MFT
	Supervisory Network Bravo	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
	Control Network Bravo	RTUs	Security Events	Installation, Actions, on Objectives	Dragos Platform	1 Year	Controller Logic
	Control Network Bravo	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	7 Days	Registry, Memory, MFT
	Control Network Bravo	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
Charlie Facility	Supervisory Network Charlie	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	Local Host	15 Days	Historian Logs, Registry
	Supervisory Network Charlie	EWS	Windows Event Logs	Installation, Actions, on Objectives	Local Host	10 Years	Registry, Memory, MFT
	Supervisory Network Charlie	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
	Control Network Charle	PLCs	Internal Logging	Installation, Actions, on Objectives	Local Host	7 Days	Controller Logic
	Control Network Charle	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	7 Days	Registry, Memory, MFT

Threat & Environment Manipulation

Environment

How to Prepare

- Think in scenarios, e.g. ransomware, worms, attacks against crown jewels
- Prepare for segmentation ahead of time, i.e. logical network separation through firewall rules
- Ask yourself, how long the process can sustain separation
- Have a plan & exercise it

Threat

Understand the Threat

- Leverage good Threat Intel
  - Who are you dealing with?
  - What might be their objectives
- Understand their TTPs and tools
- Identify weaknesses in your environment *and their TTPs and tools*
- Leverage your knowledge for defense, buying your team time to eradicate and recover

Threat Hunting

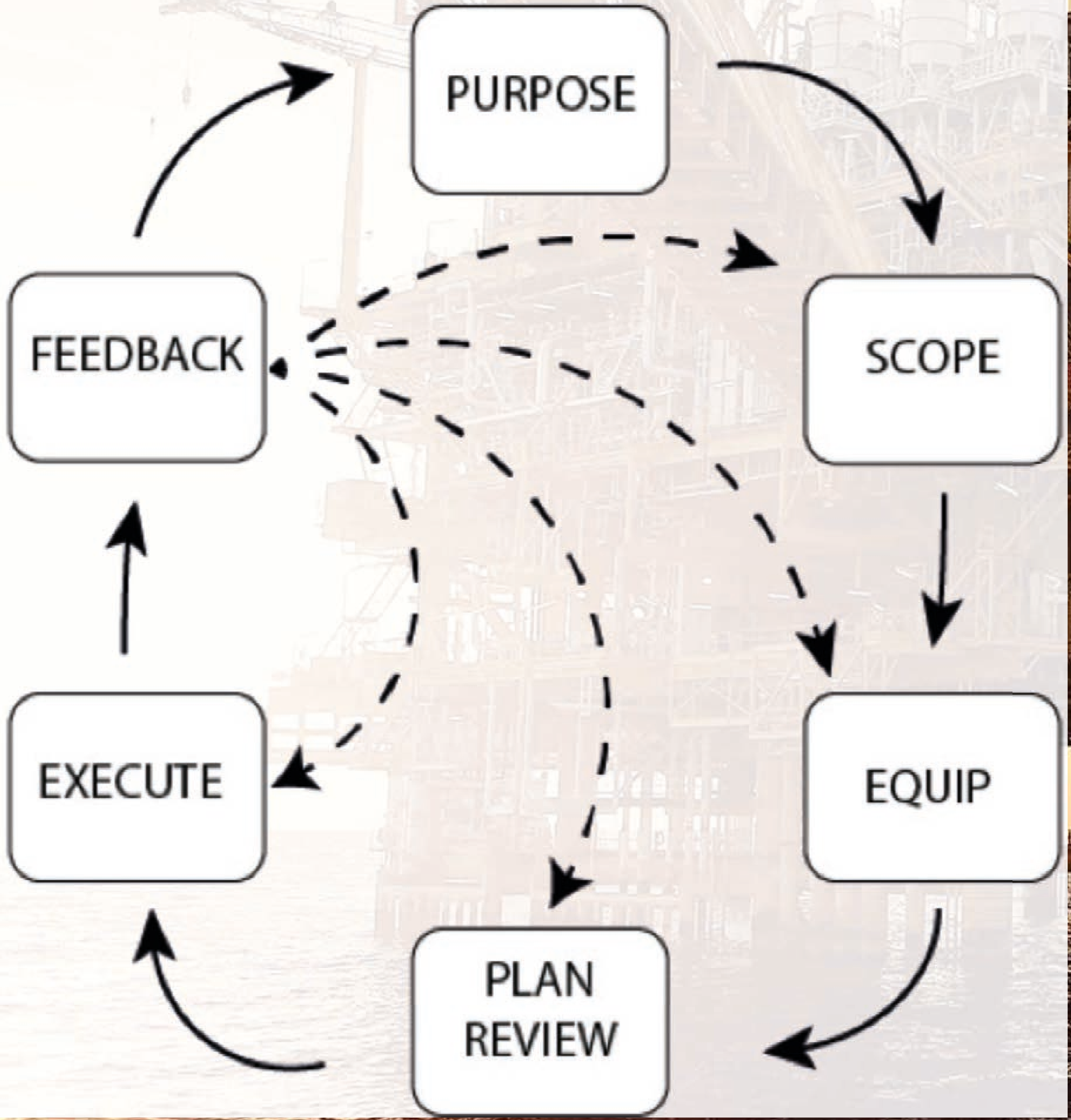
DRAGOS
SAFEGUARDING CIVILIZATION

Consequence Driven Threat Hunting

Risk = (Threat * Vulnerability) * Consequence

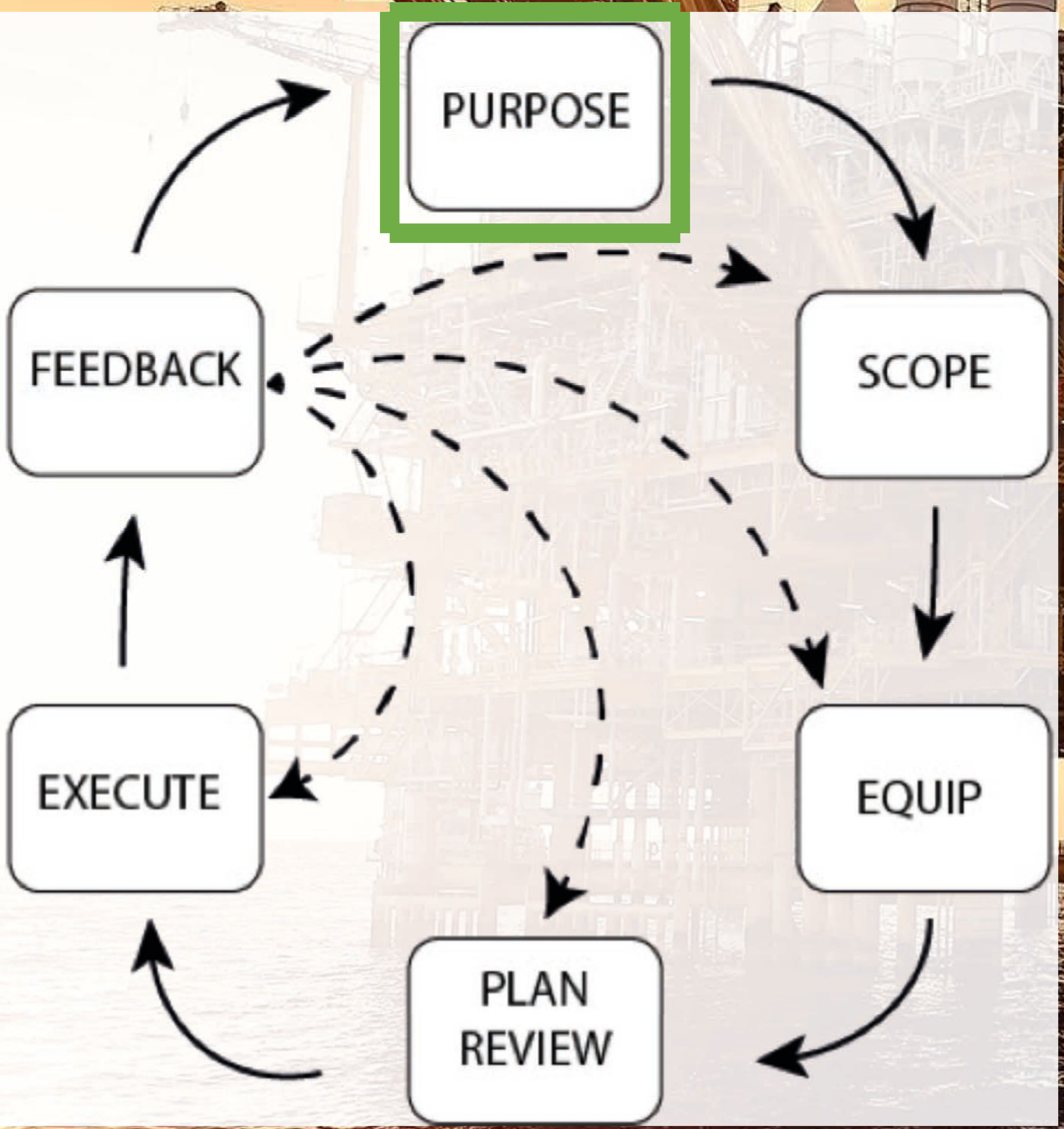
Threat Hunt Model

DRAGOS
SAFEGUARDING CIVILIZATION



- Take actionable information and proactively do actions with it = **Threat Hunting**

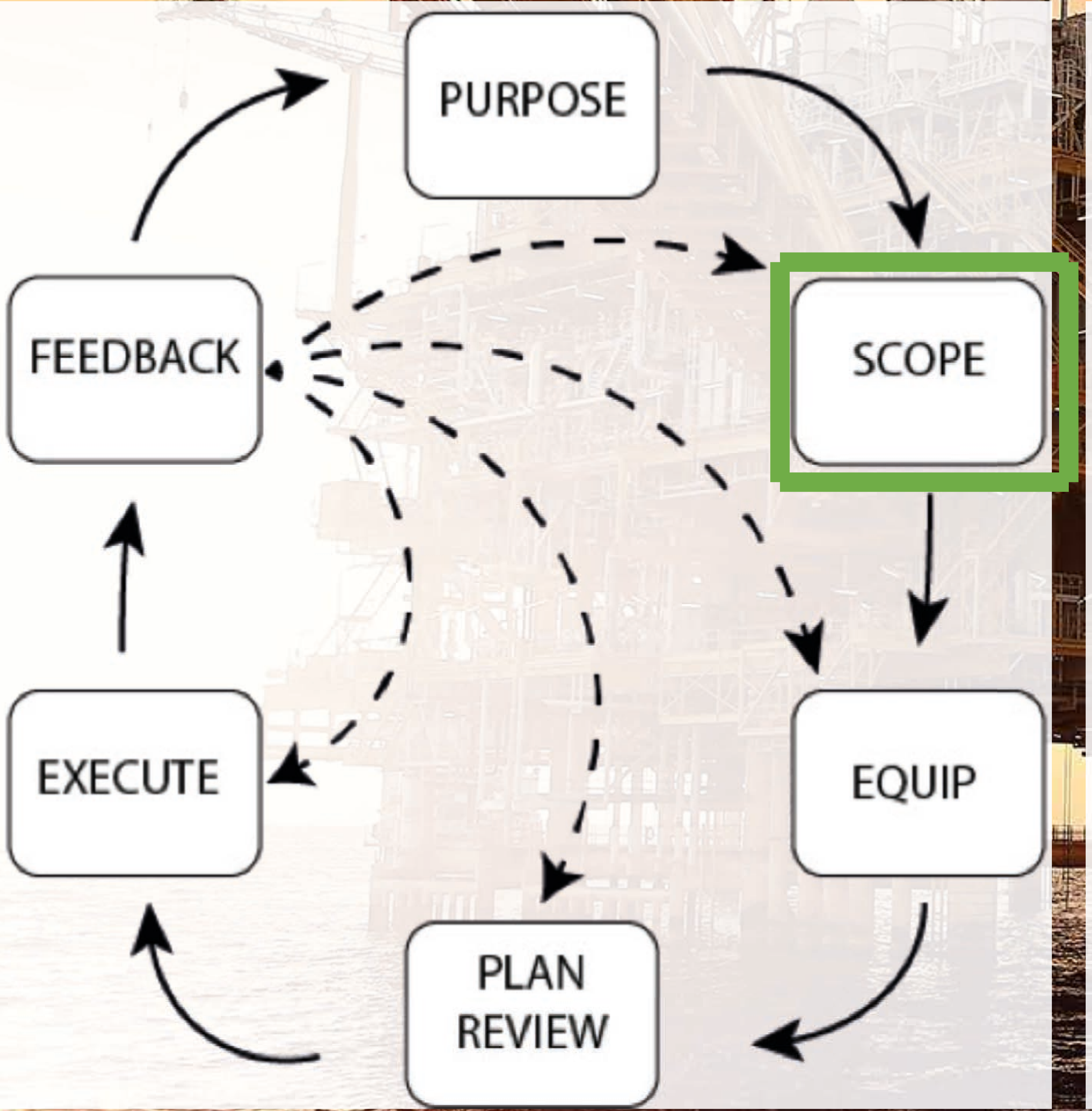
Threat Hunt Model



- Hyp: adversary has compromised EWS in DeltaV DCS of Fanta Coloring Plant and is using DNSTUNNEL for C2

Threat Hunt Model

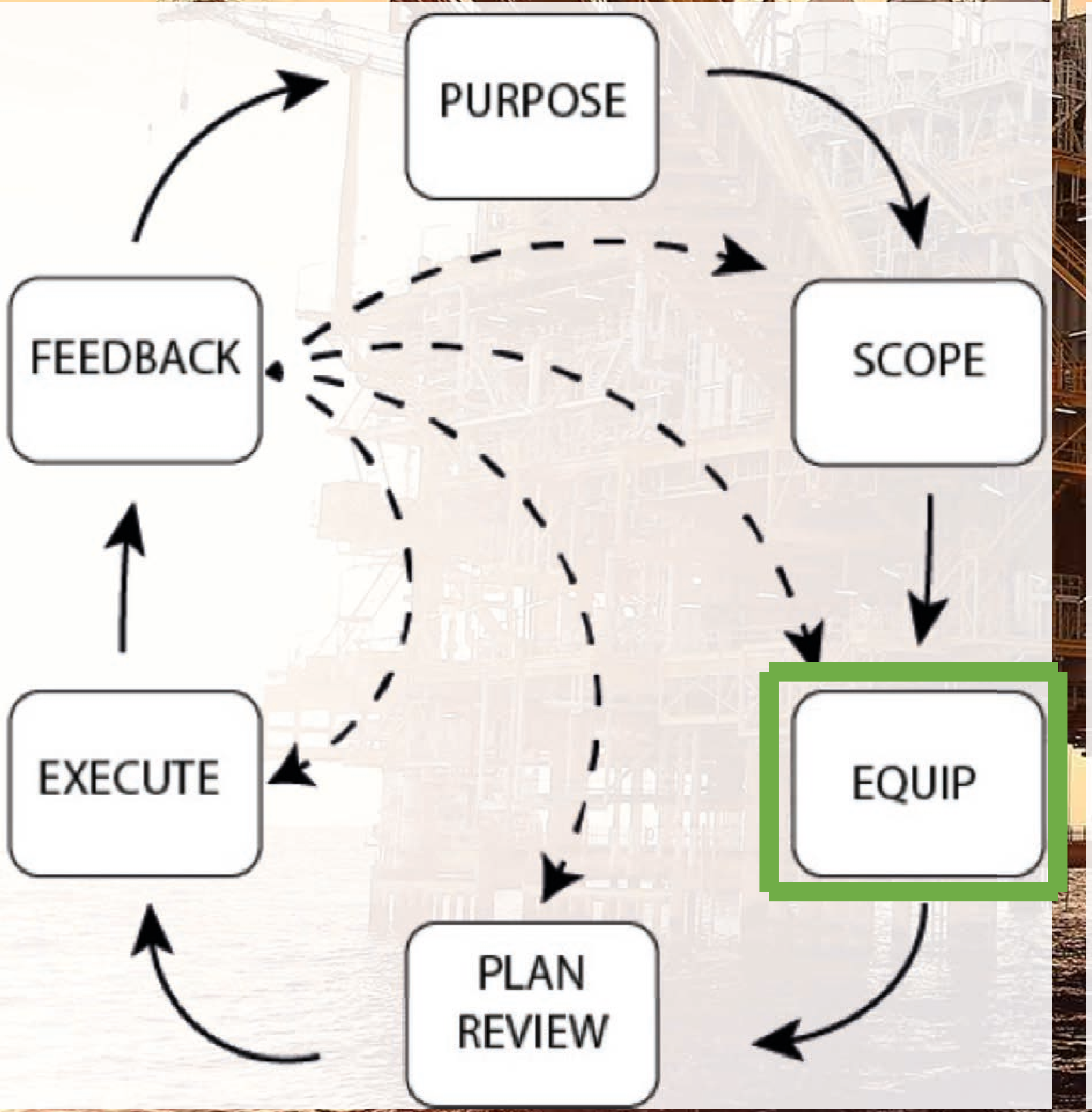
DRAGOS
SAFEGUARDING CIVILIZATION



- Location: DeltaV DCS of Fanta Color Plant
- Logs: DNS records on hosts, passive DNS, DNS Server Logs, hosts files, resolv.conf, Zeek, Windows Event Logs, Proxy logs, FEYE HX/PX logs, FW logs, netflow/IPFIX, syslog, DeltaV logs, Windows registry, DHCP config/logs

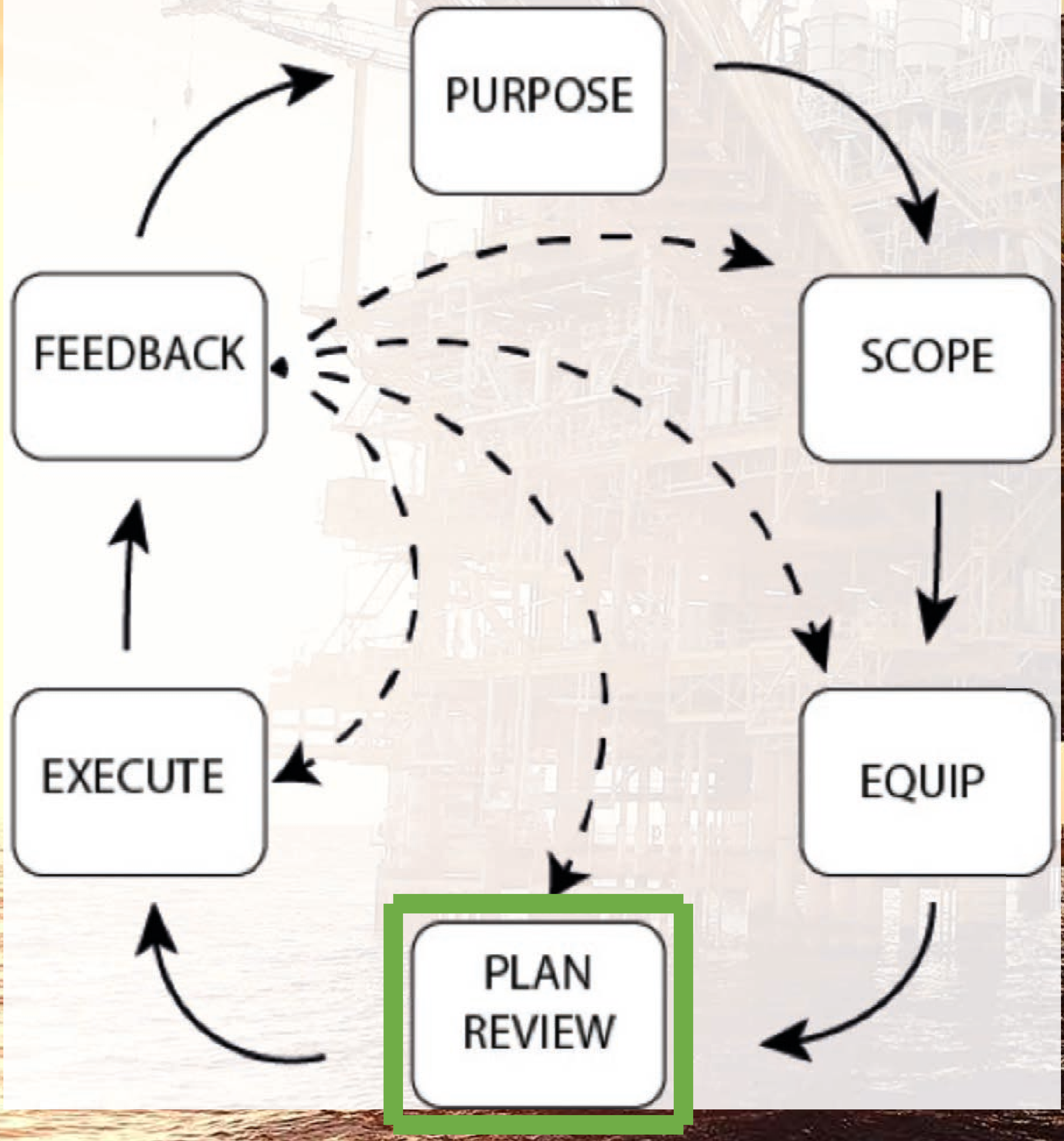
Threat Hunt Model

DRAGOS
SAFEGUARDING CIVILIZATION



- Collection Management Framework
- Logs:
  - passive DNS (Level 4 DMZ)
  - DNS Server Logs (Level 2 DCS)
  - hosts files (on host)
  - resolv.conf (on host)
  - ~~Zeek (not available)~~
  - Windows Event Logs (CMF 30 days)
  - Proxy logs (Level 4 DMZ, but no DNS)
  - FEYE HX/PX logs
  - FW logs (Level 2-4)
  - ~~netflow/IPFIX~~
  - ~~Syslog~~ (depends on plant and location)
  - DeltaV logs (local, 90 days)
  - Windows registry (local)
  - DHCP config/logs (local)
- Is the plant compliant with the BASF data model? (**yes**/no)

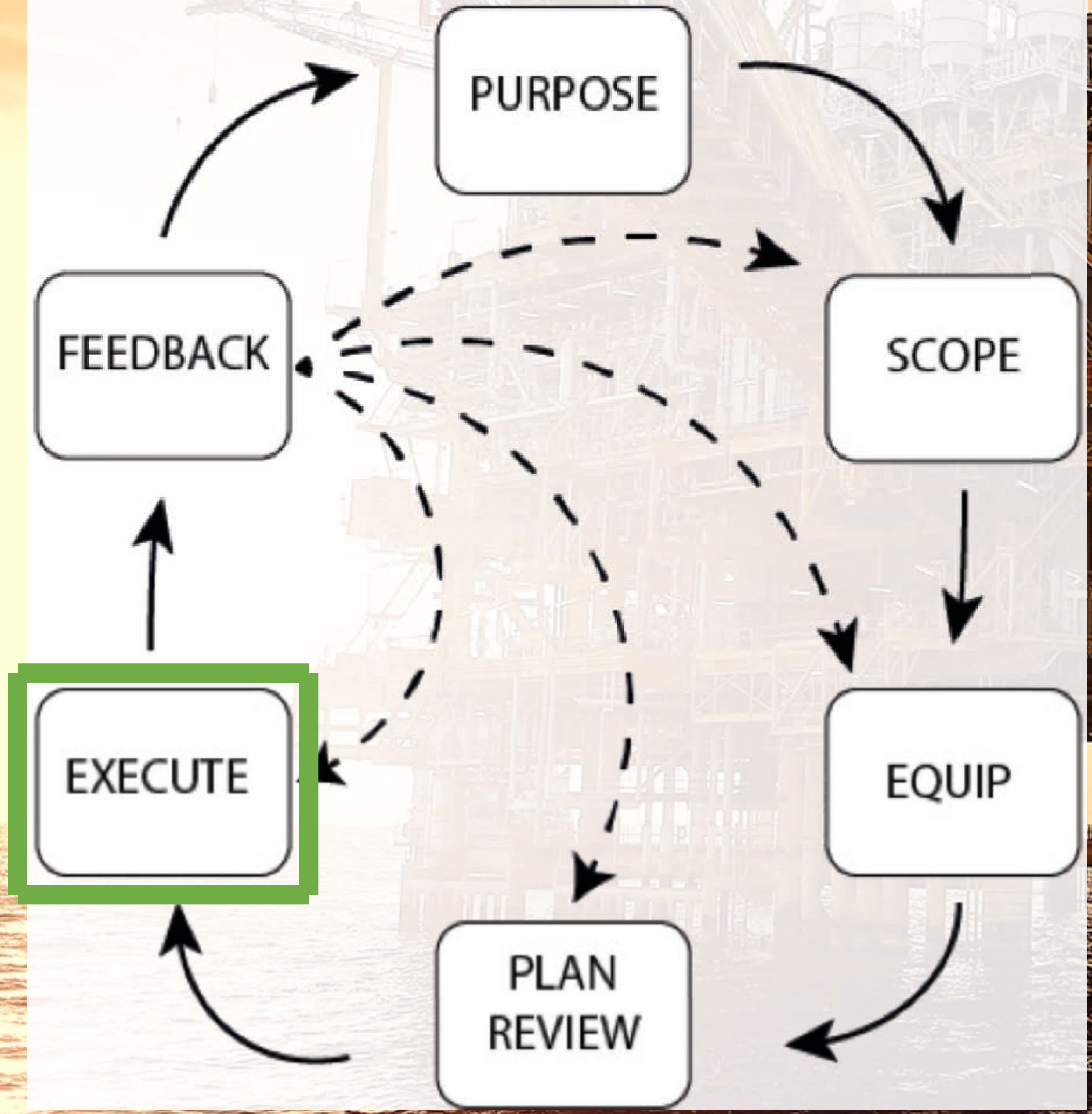
Threat Hunt Model



- Viability
- Fit to Purpose
- Scope modifications

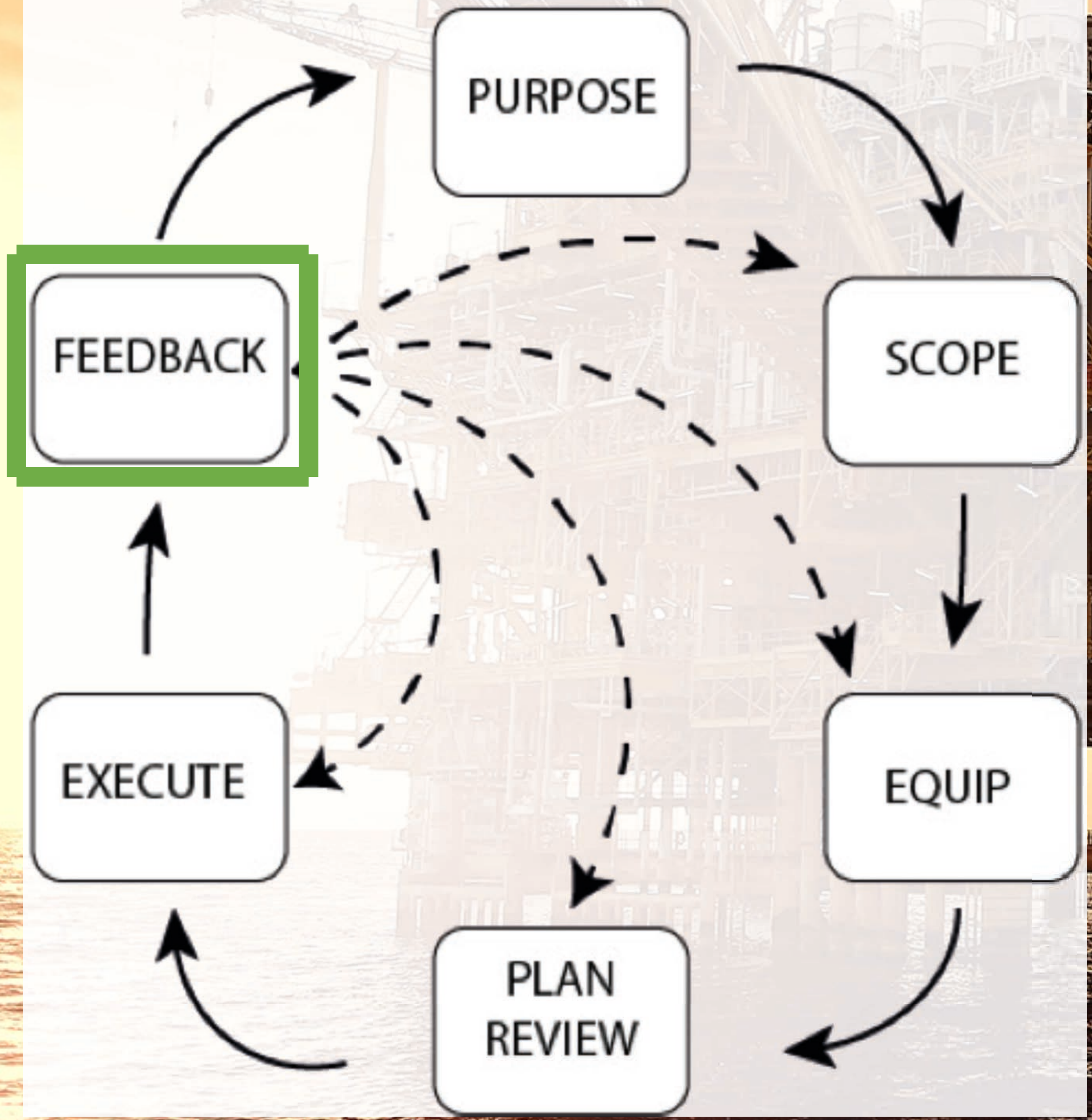
- Logs:
  - passive DNS (Level 4 DMZ)
  - ~~DNS Server Logs (Level 2 DCS)~~
  - ~~hosts files (on host)~~
  - ~~resolv.conf (on host)~~
  - ~~Zeek (not available)~~
  - ~~Windows Event Logs (CMF 30 days)~~
  - Proxy logs (Level 4 DMZ, but no DNS)
  - FEYE HX/PX logs
  - FW logs (Level 2-4)
  - ~~netflow/IPFIX~~
  - ~~Syslog~~ (depends on plant and location)
  - ~~DeltaV logs (local, 90 days)~~
  - ~~Windows registry (local)~~
  - ~~DHCP config/logs (local)~~

Threat Hunt Model



- Carry out Hunt
- Additional Hypotheses
- Generate Report
- Logs:
  - passive DNS (Level 4 DMZ) ? Maybe DNS tied to AD, ask AD ops team, DNS queries are in SIEM, but not replies
  - Proxy logs (Level 4 DMZ, but no DNS), in SIEM
  - FEYE HX/PX logs, Alerts in SIEM, events local
  - FW logs (Level 2-4), SIEM

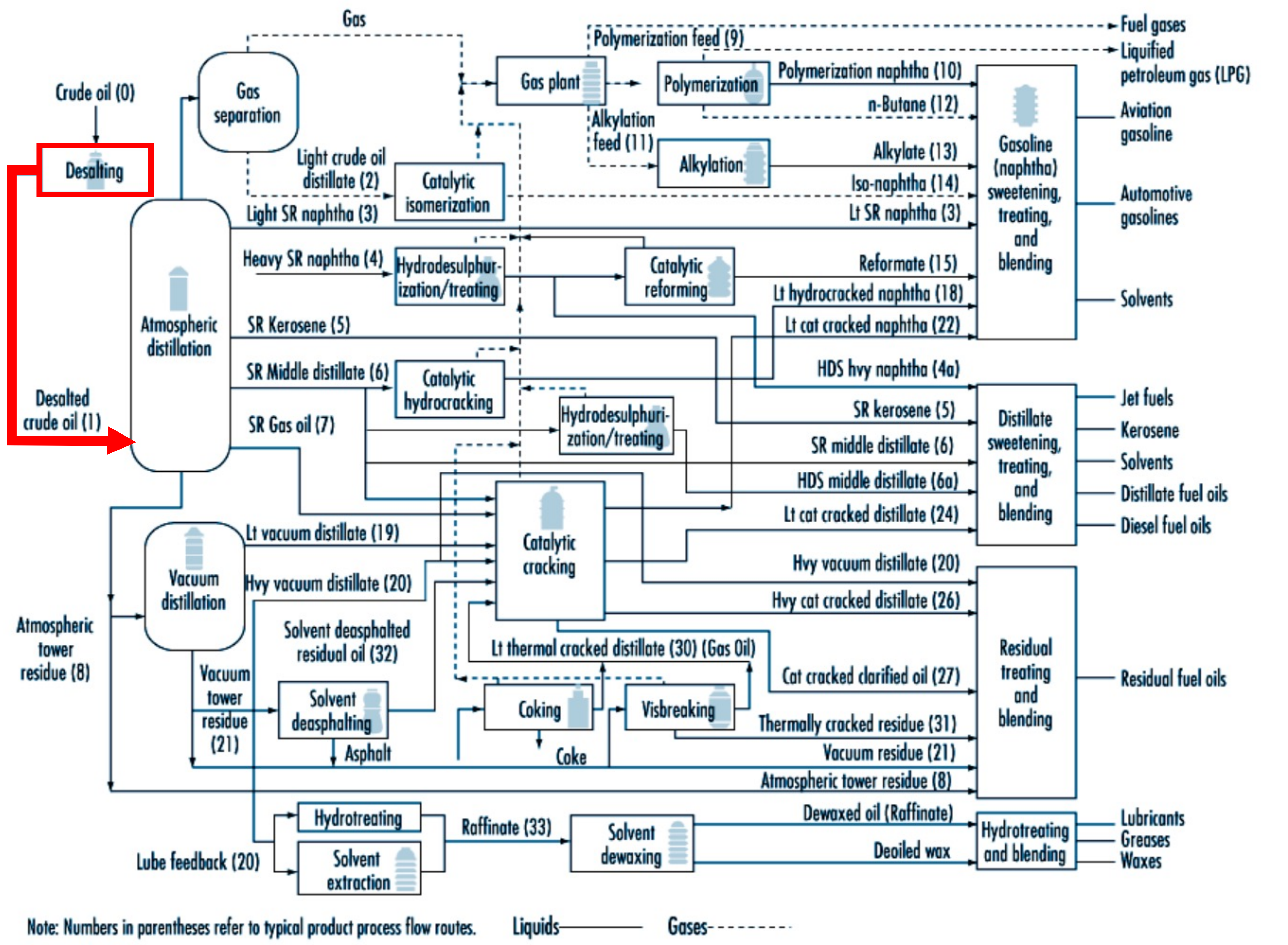
Threat Hunt Model



- Feedback
  - What worked?
  - What can be improved?
- Internal:
  - What are collection gaps?
  - What are policy and procedure gaps?
  - How would we have done if we were patient 0?
- External:
  - Process improvements
  - Resource improvements
  - Provide additional findings back to source
  - What information was useful?

DRAGOS
SAFEGUARDING CIVILIZATION

Case Study: Applied Threat Hunt Model

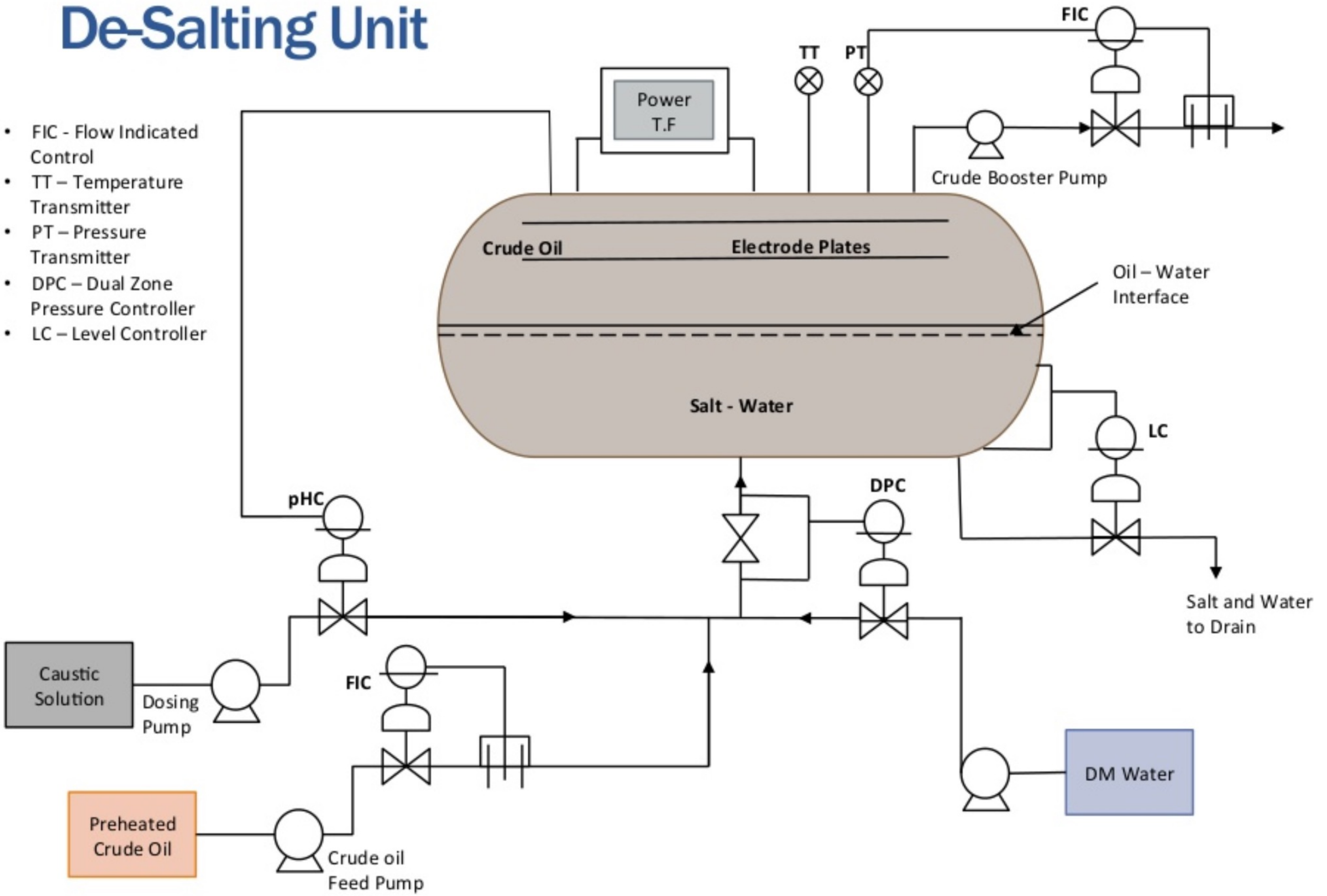


Note: Numbers in parentheses refer to typical product process flow routes.

Source: OSHA 1996.

De-Salting Unit

- FIC - Flow Indicated Control
- TT – Temperature Transmitter
- PT – Pressure Transmitter
- DPC – Dual Zone Pressure Controller
- LC – Level Controller

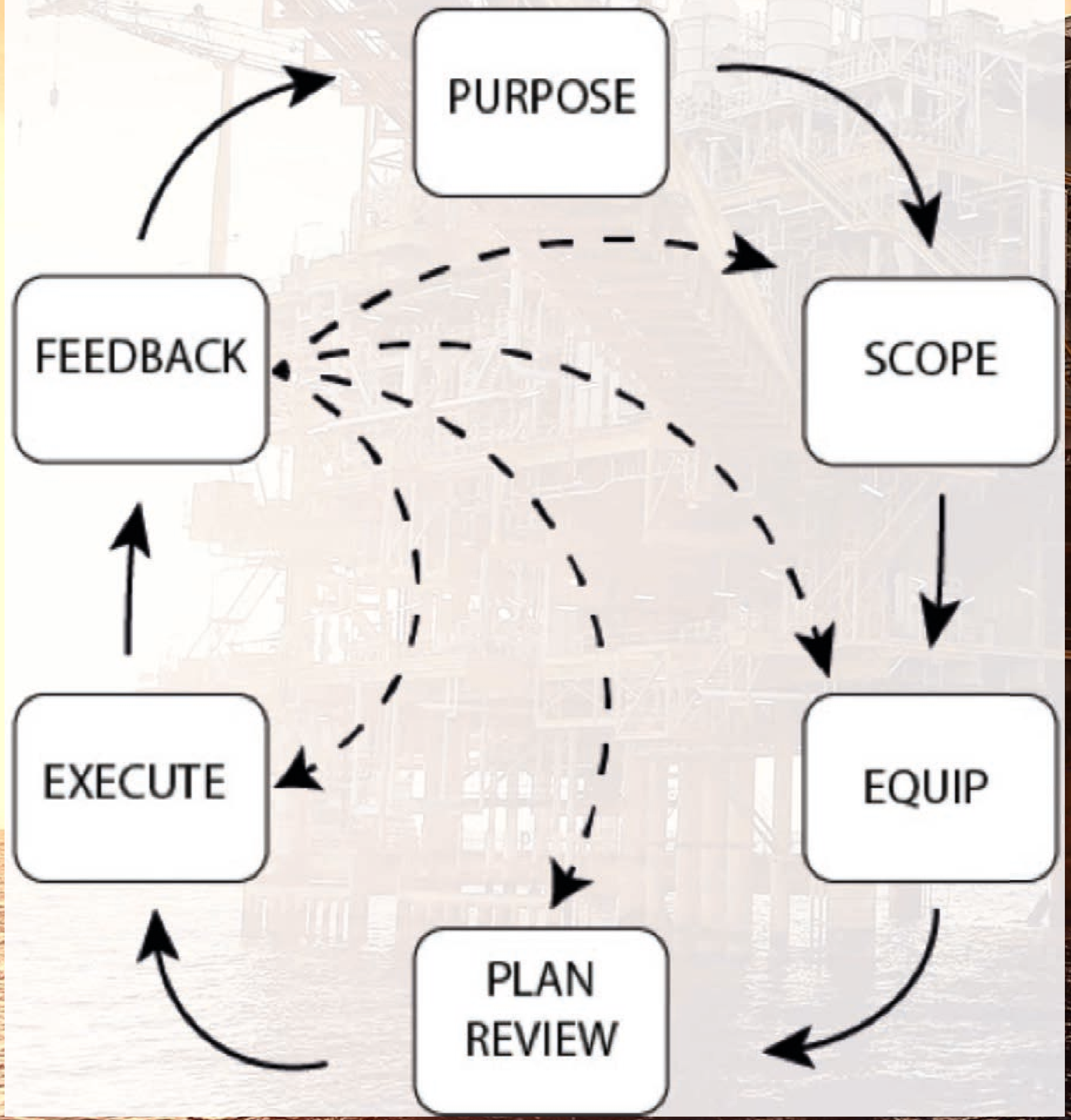


- This is not paid marketing for BGR Energy and we have not worked in collaboration with BGR Energy to produce this webinar. This does not represent BGR Energy views.

Source: https://www.slideshare.net/OctovianCletus/petroleum-introrev-4/10

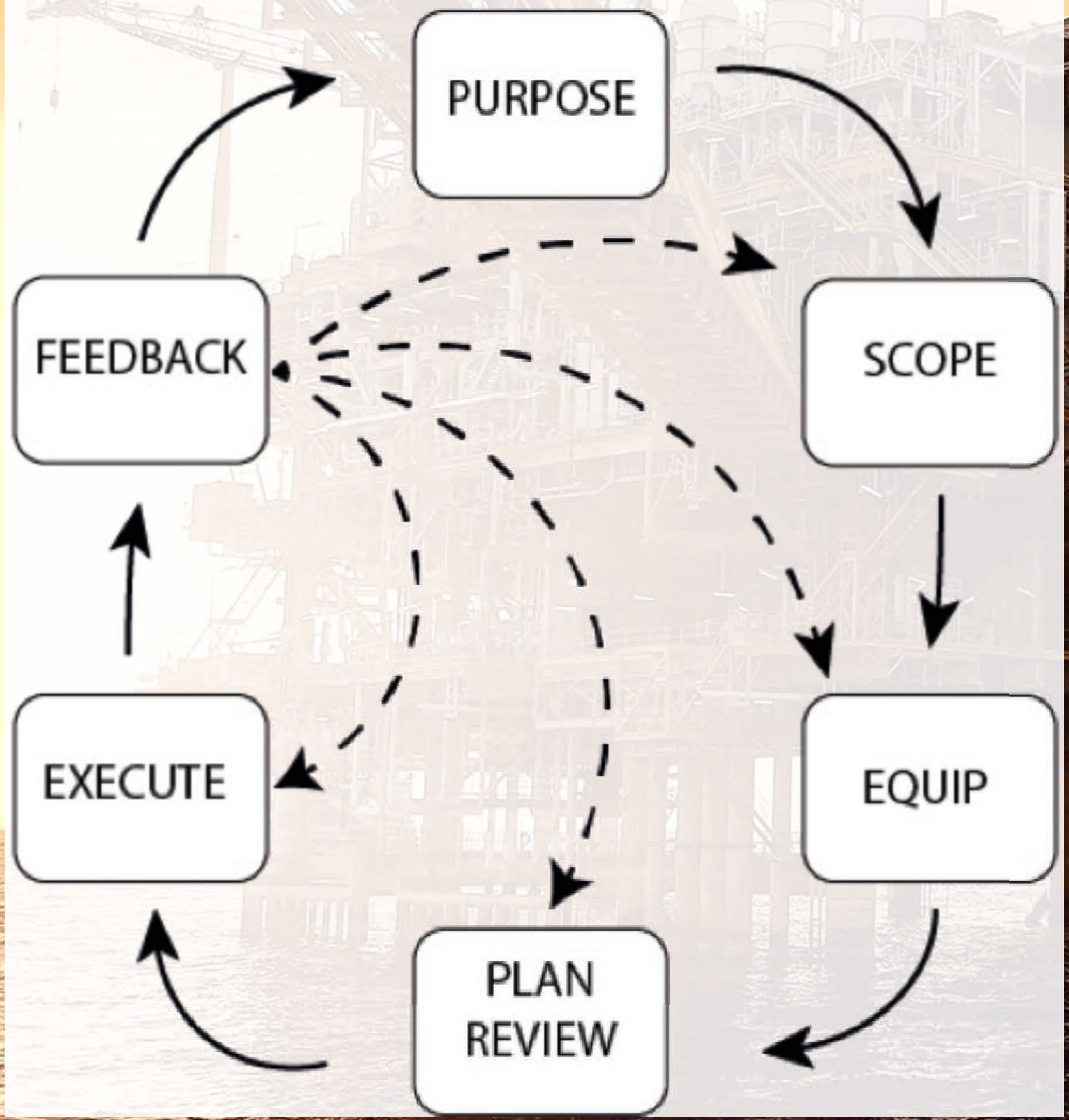
Purpose

DRAGOS
SAFEGUARDING CIVILIZATION



- Gain visibility and understanding into critical process assets in desalination

Scope: Phase 1

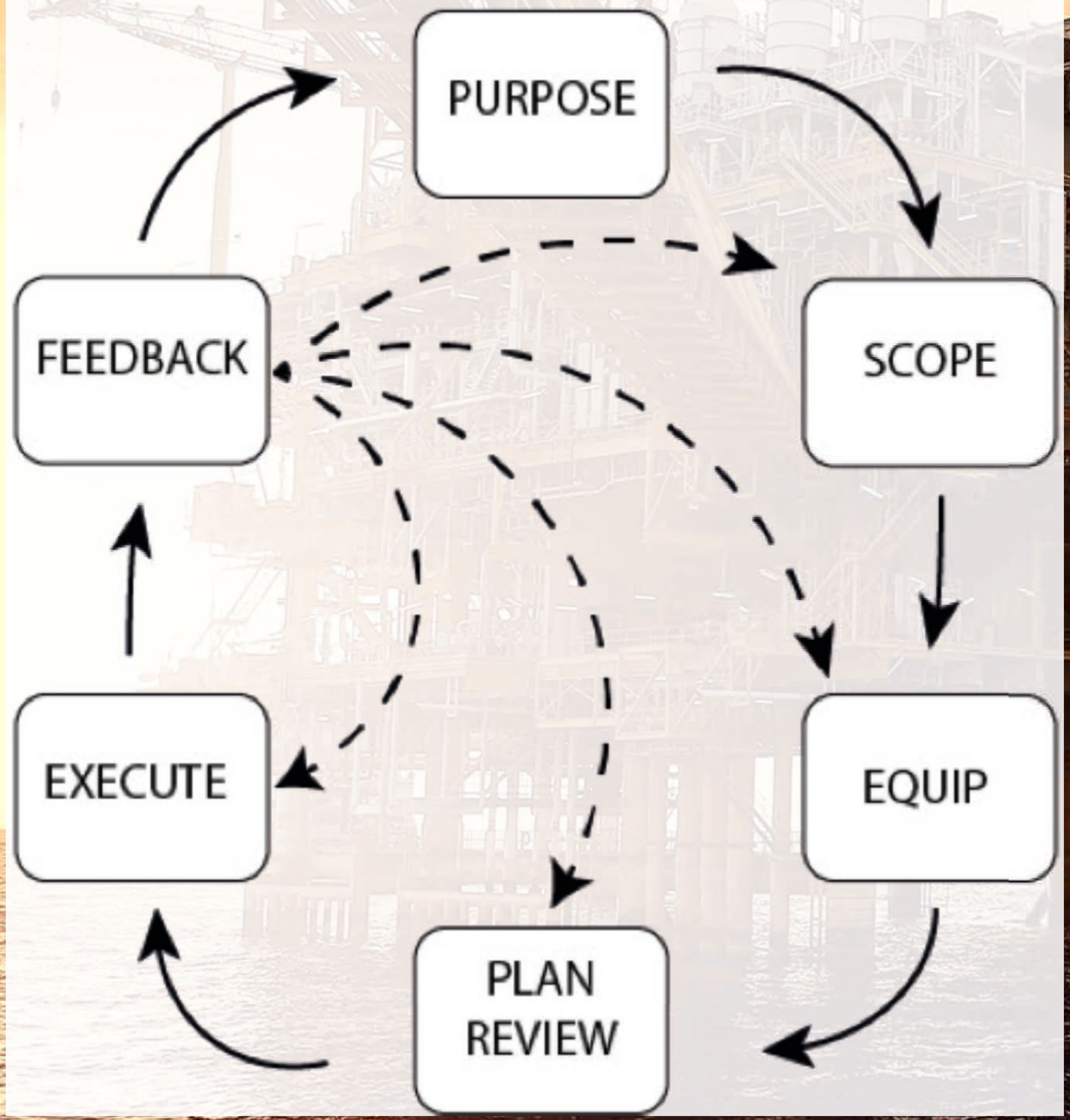


- 1 Refinery in San Antonio, Texas
  - Desalination Process
    - ABB Freelance DCS
      - Freelance Operation Center
      - All AC 900F Controllers
      - All AC 800F Controllers
      - All AC 700F Controllers
        - Profibus, Modbus (RTU and TCP)

ABB: Freelance DCS

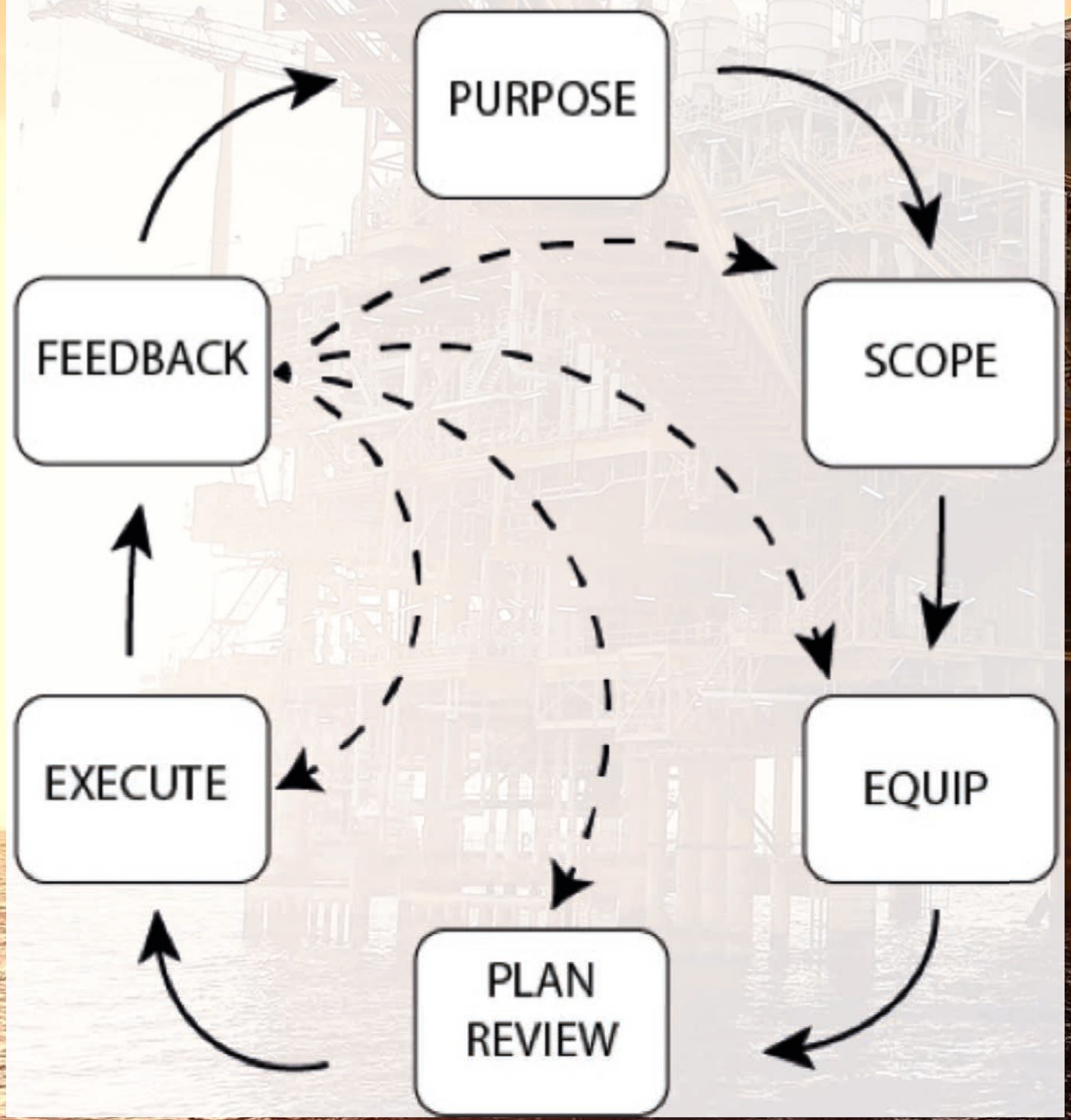
- Modernized Control System
- Variety of implementations
- Integrations with many other applications
- Hundreds of IOs and field devices
- Controllers:
  - AC 700F, AC 800F, AC 900F
  - Remote IO: S700, S800, S900
- Freelance Operations
- Freelance Engineering

Scope: Phase 2: Hypotheses



- Hypotheses
  - Attackers are leveraging Freelance Operation Center login information to do reconnaissance on desalination process.
  - Attackers are sending malicious commands to AC 900F and AC 700F controllers to manipulate desalination process.

Equip: Phase 1: CMF

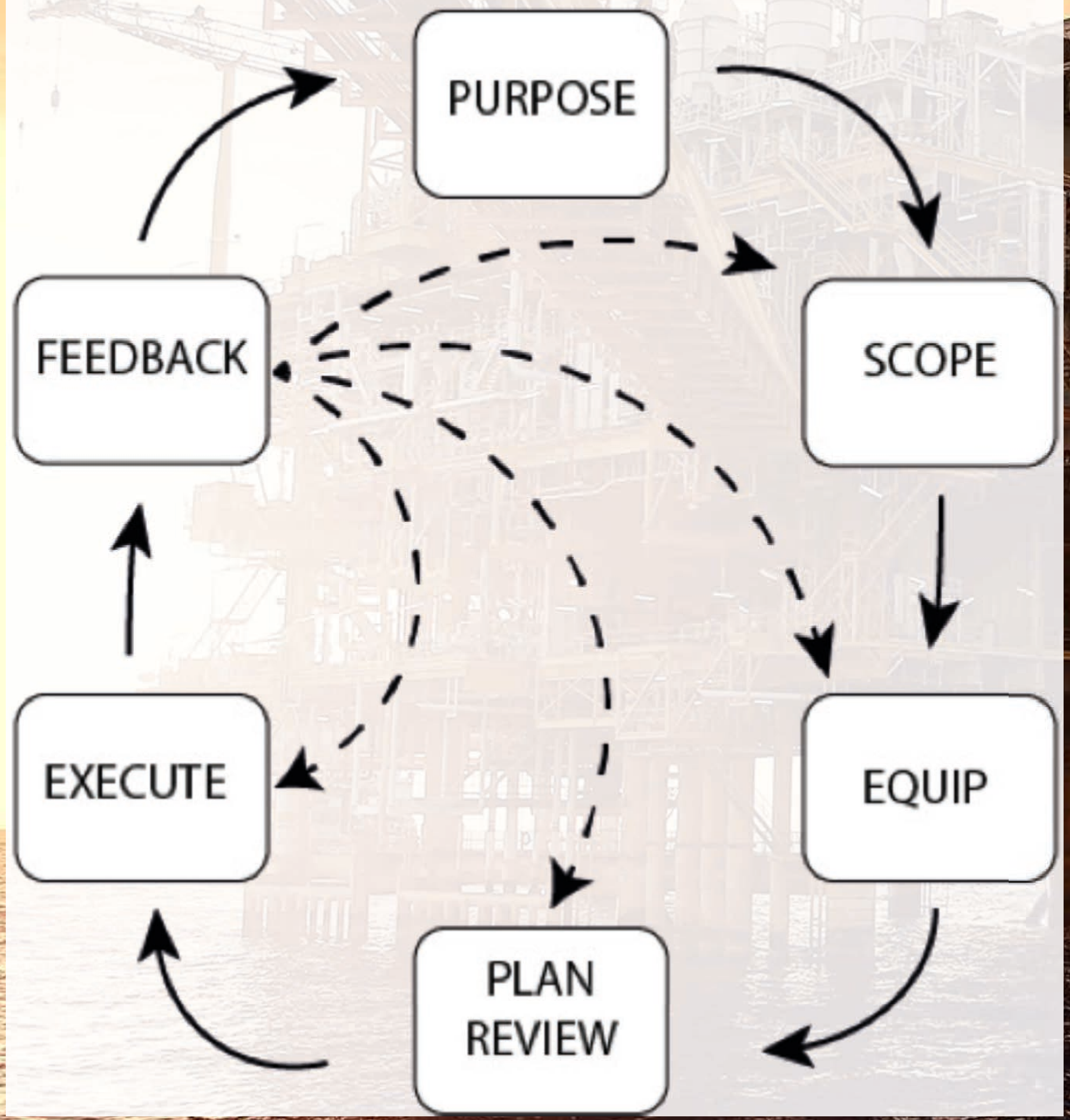


- Freelance Operations center
  - Asset Management
  - Process information
  - User logging + Timestamps
  - System Changes
- Freelance Engineering
  - Database
  - Project configurations
- Network Traffic to Controllers
- Historian Assets

Collection Management Framework

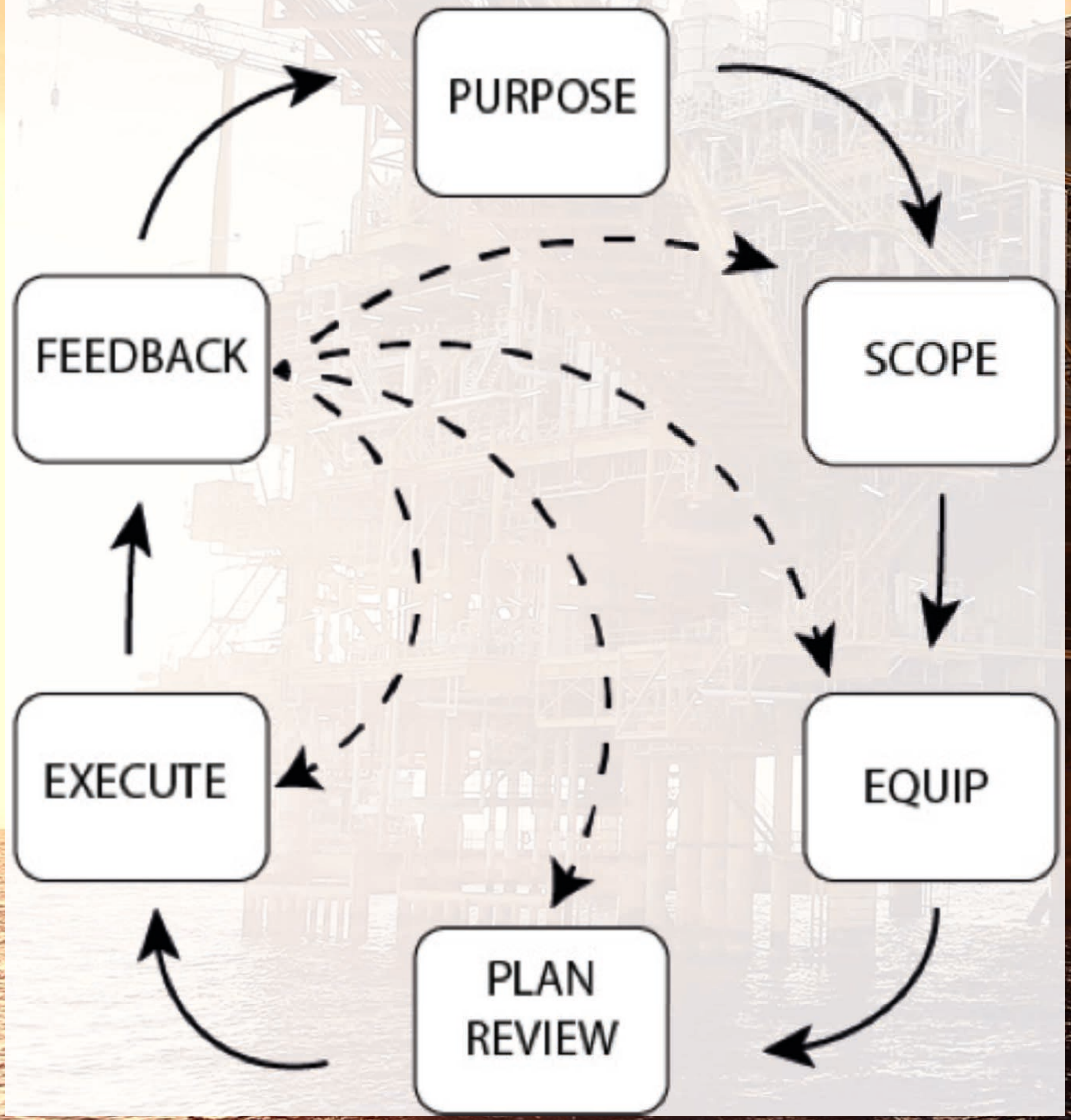
Data Source	Desalination Process
Firewall Logs	2 Days
Freelance Operations	30 Days
FreeLance Engineering	30 Days
Full Network Capture	7 Days
Process Historian	60 Days
Controllers	None Available

Equip: Phase 2: Resource Allocation



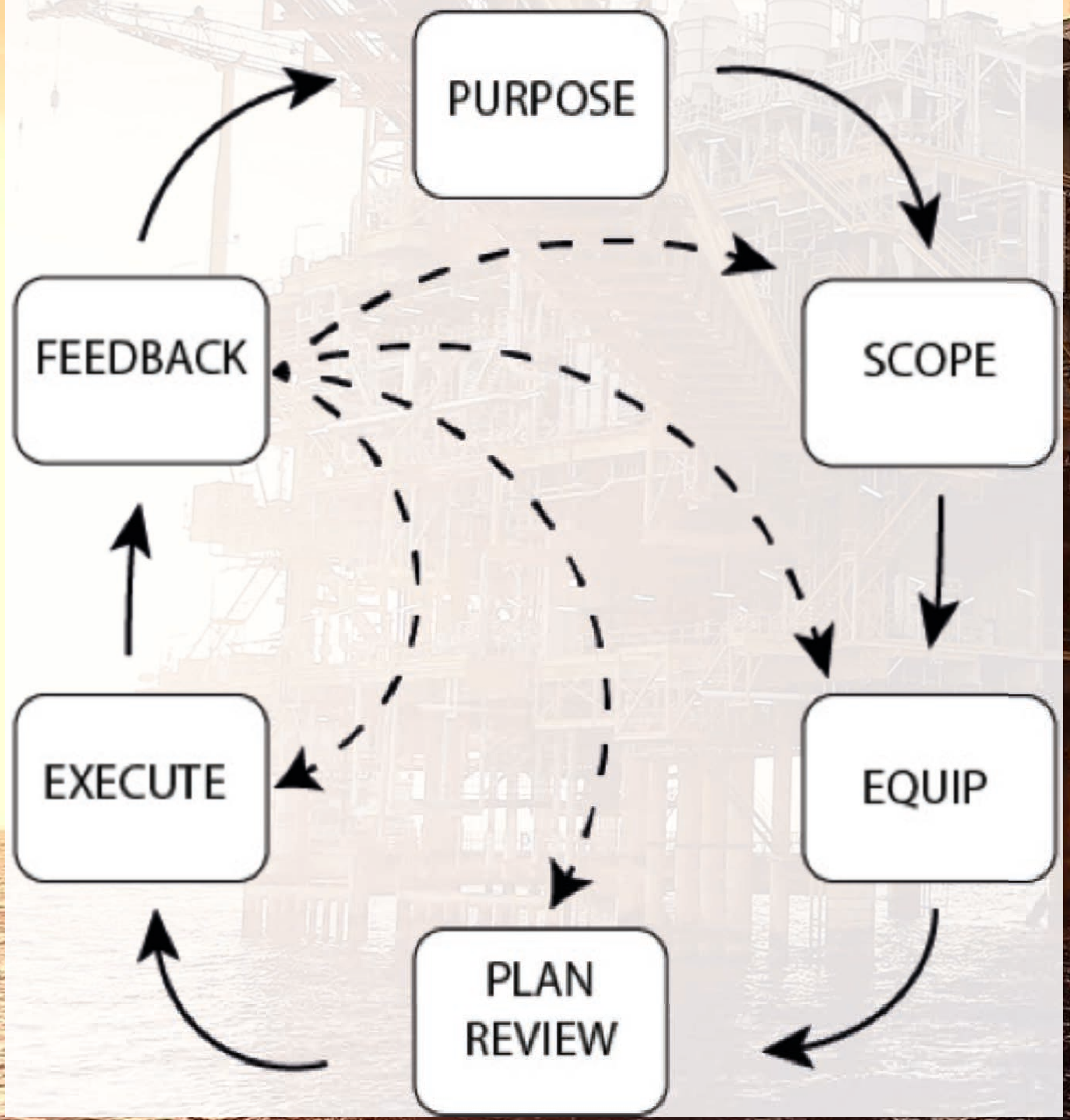
- Team members
  - Senior
  - Junior
- Tools
  - Approved
  - Custom vs General
- Time

Plan Review



- Stakeholder awareness
- Potential issues with achieving purpose success
- Any alterations

Execute



- Use hypotheses to structure hunts with relevant data sources
- Discussions with Subject Matter Experts on what is “normal”
- Hunt to find what does not fit the expected normal
- Observables of known adversary behavior

Hypothesis #1

- Attackers are leveraging Freelance Operation Center login information to do reconnaissance on desalination process.

- Data Source
  - Freelance Operation Center
    - Weird logons
    - Unknown users
    - Timestamps during non-working hours
    - Un-successful logon attempts in high frequency and volume

- Data Source
  - Network Capture
    - Timestamps during non-working hours
    - Unknown addressing space
    - Scanning activity
    - Exfiltration of data

Hypothesis #2

DRAGOS
SAFEGUARDING CIVILIZATION

- Attackers are sending malicious commands to AC 900F and AC 700F controllers to manipulate desalination process.

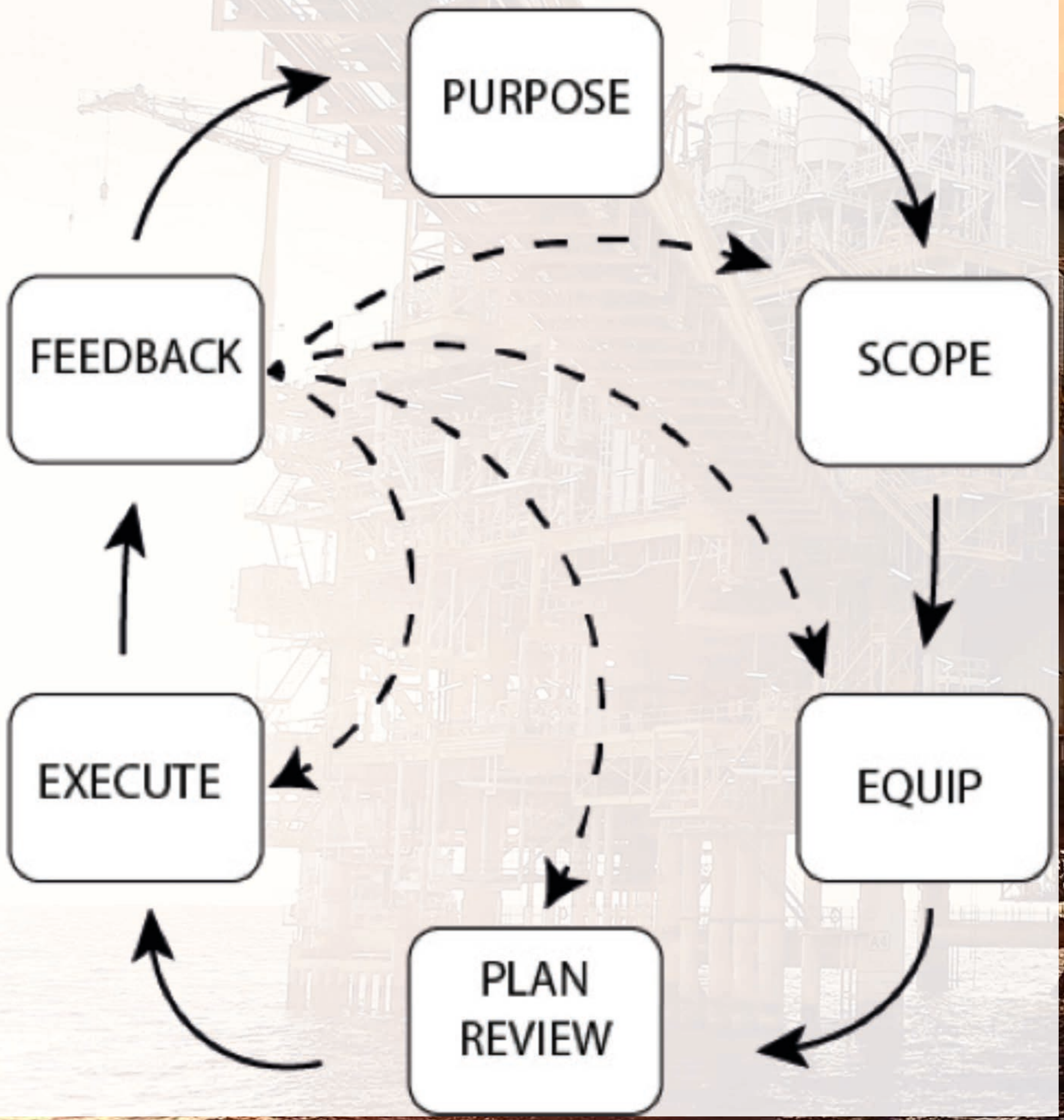
- Freelance Operation Center
  - Trend Analysis
  - Normal operations as baseline
  - Event logs
  - User Authentication

- Network Capture
  - Controller Command Responses
  - Controller Status

- Freelance Engineering
  - Understanding of PLC configuration files
  - Stateful analysis

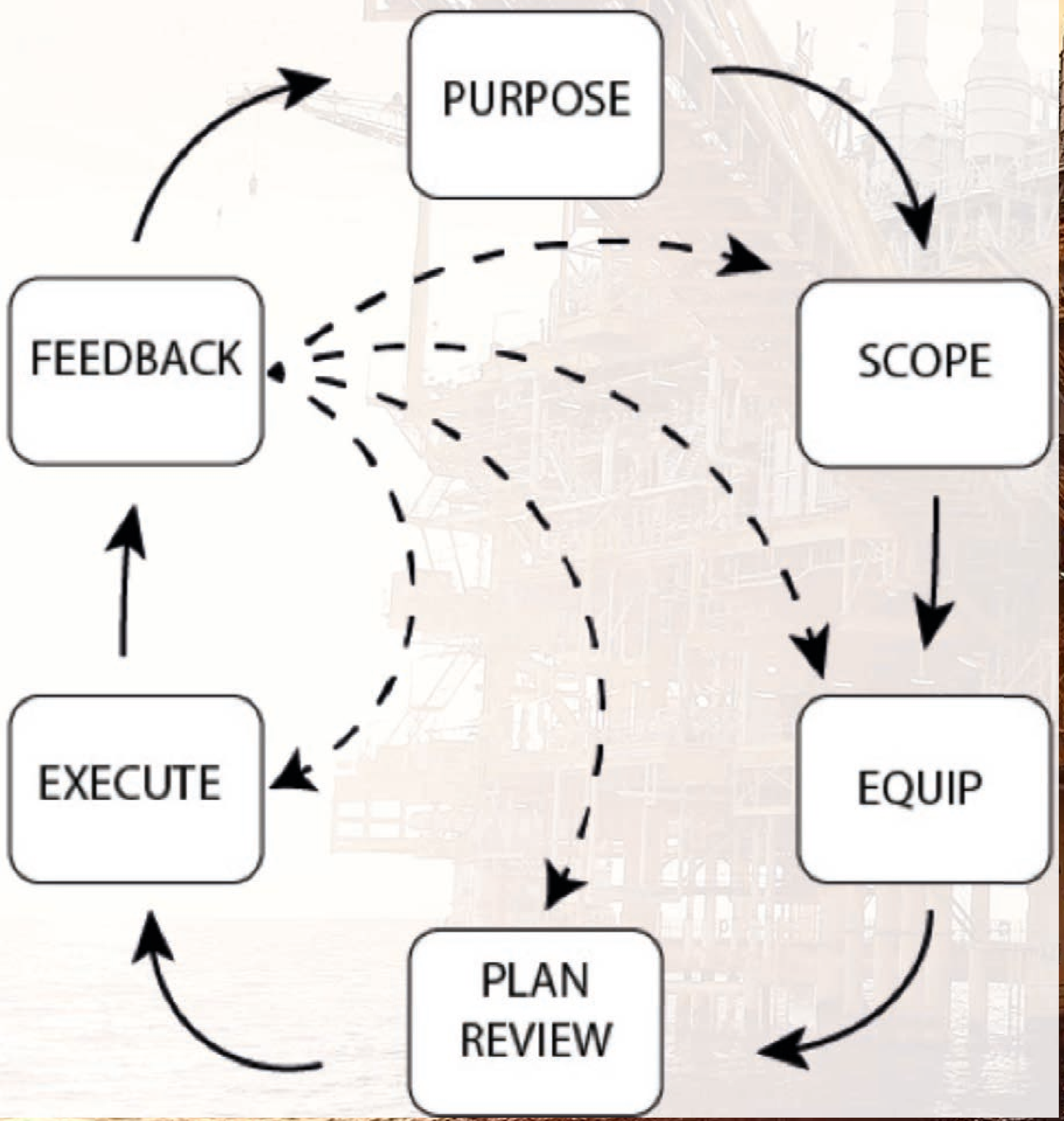
- Process Historian
  - Alarm Events
  - Trend Analysis

Execute: Report



- Summary of all findings
- Hypothesis confirmation or falsification
- Better understanding of environment
- Establish baseline of operations for follow on hunts with new scopes

Feedback



- **Purpose**: How was the report received?
- **Scope**: Too broad or narrow? Follow on hunts?
- **Equip**: Data sources? Team Experience?
- **Plan Review**: Any blatant issues missed?
- **Execute**: Did we prove or disprove hypothesis with confidence?

Threat Hunting Summary

- A Hunt activity should (ideally) always start with good hypotheses generation, otherwise, hunters would be groping in the dark, looking for "something" without a clear target and scope.
- There is a substantial difference between
    - Hunting in one's own network
    - Hunting for threats in someone else's environment and/or from the outside.

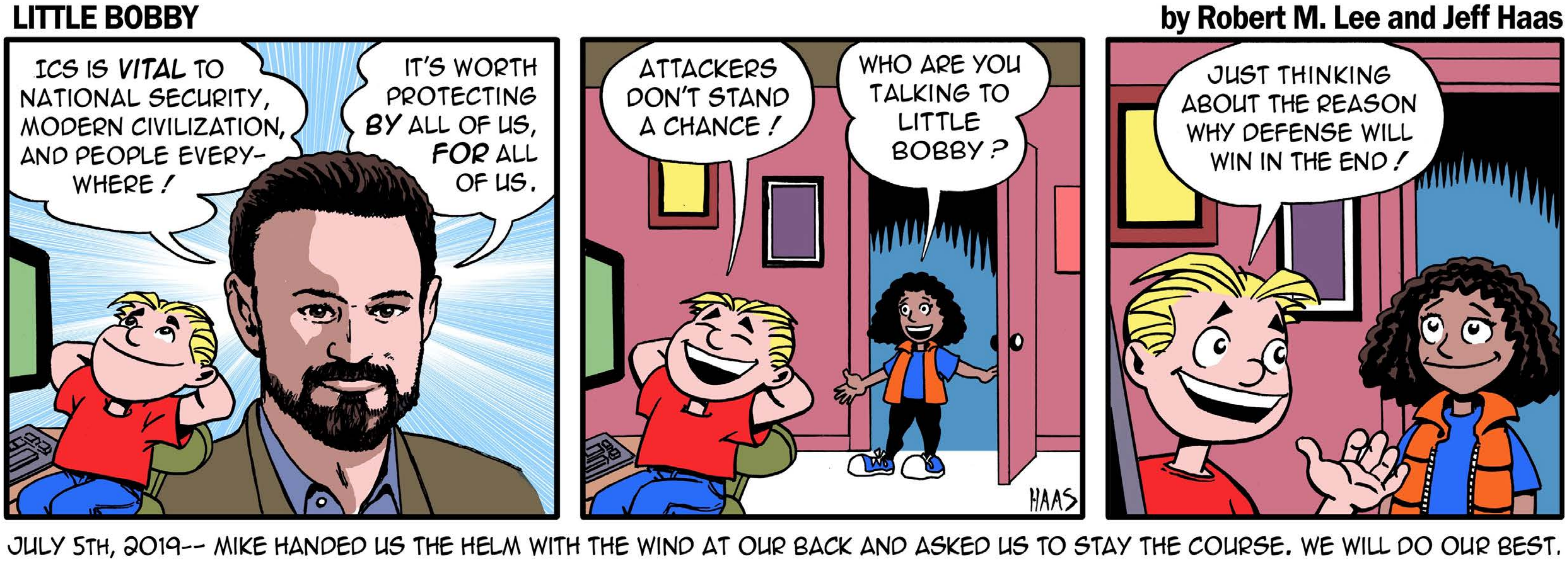
Threat Hunting - Hypotheses

- Generating good Hypotheses
  - From Observation
    - E.g. how did previous intrusion look like?
  - With Testability in mind
    - Need to come up with hypotheses that we know we can test (validate/invalidate) given the data we have.
    - Once all the previous research has been completed, hunters should generate (or discard) hypotheses based on what technical data/telemetry is at their disposal: a hypothesis for which the data to prove/disprove it is not (or mostly not) available, it is not a good hypothesis.

Threat Hunting - Hypotheses

- One more thing to consider before structuring the activity, it's what type of "approach" one is going for:
  - Victim Centric
  - Technology Centric
  - Adversary Centric
  - Socio-Political Centric
  - etc.

That’s all folks! And remember: defense is doable!


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
ICS IS *VITAL* TO NATIONAL SECURITY, MODERN CIVILIZATION, AND PEOPLE EVERYWHERE!
IT'S WORTH PROTECTING *BY* ALL OF US, *FOR* ALL OF US.
ATTACKERS DON'T STAND A CHANCE!
WHO ARE YOU TALKING TO LITTLE BOBBY?
JUST THINKING ABOUT THE REASON WHY DEFENSE WILL WIN IN THE END!
HAAS
JULY 5TH, 2019-- MIKE HANDED US THE HELM WITH THE WIND AT OUR BACK AND ASKED US TO STAY THE COURSE. WE WILL DO OUR BEST.

Thank you for your time! Questions?
Twitter: @kaithomsen
Email: kthomsen@dragos.com