Ransoming Critical Infrastructure

Thinking about ransomware in an OT world

Tim Conway

– SANS Institute

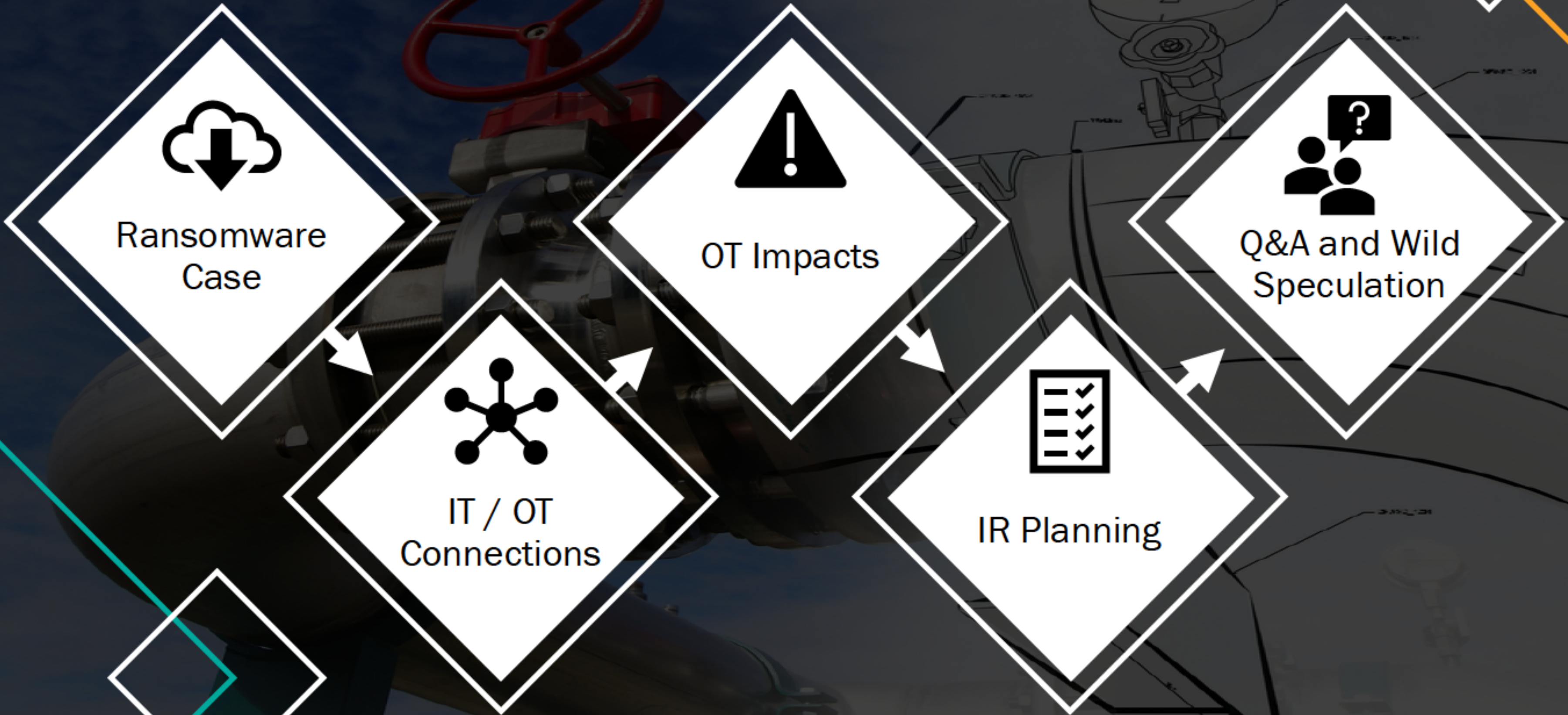
– Instructor

Jeff Shearer

– SANS Institute

– Instructor / Author ICS612

Agenda



Ransomware Case

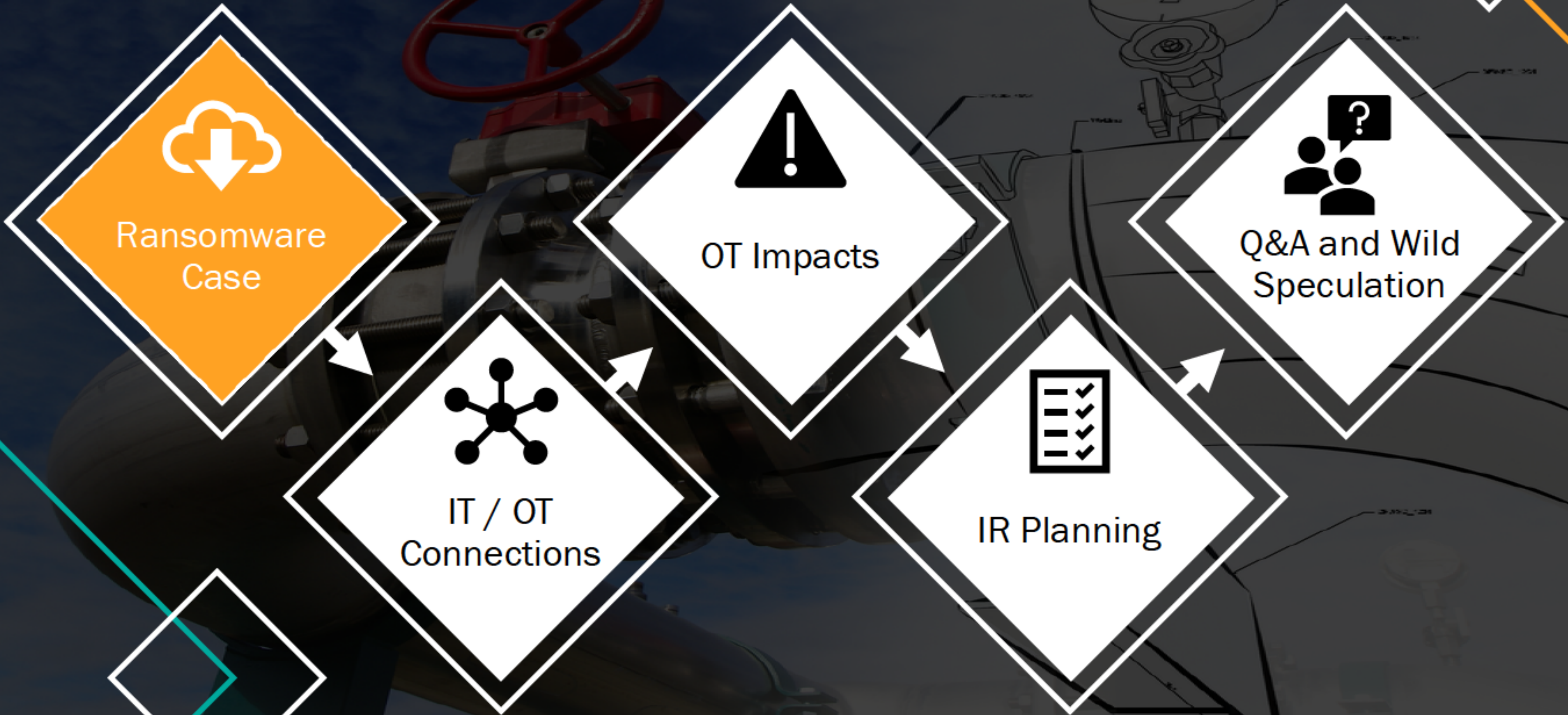
IT / OT Connections

OT Impacts

IR Planning

Q&A and Wild Speculation

The Basics



Ransomware Case

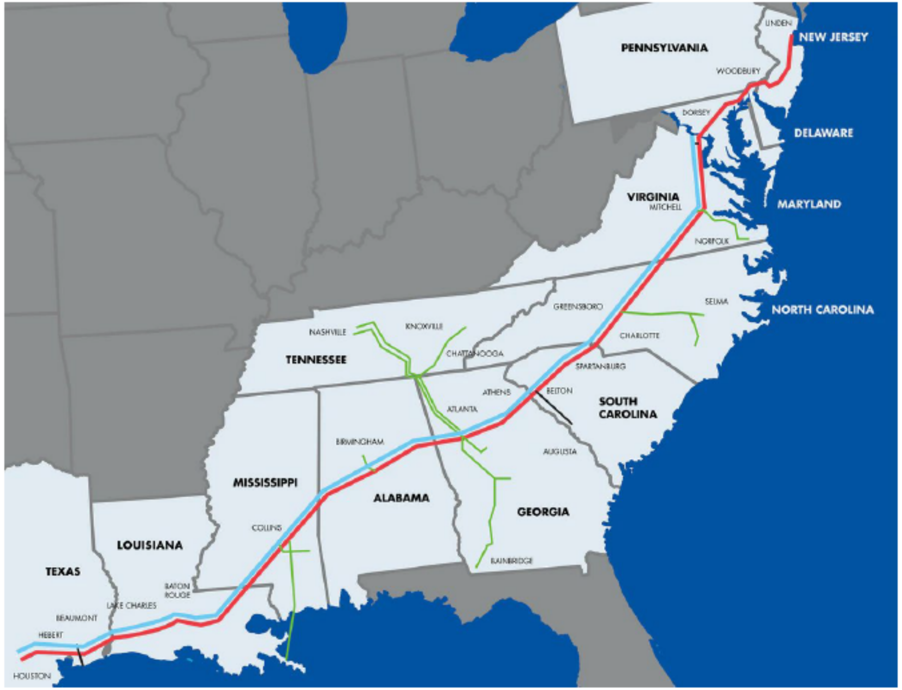
IT / OT Connections

OT Impacts

IR Planning

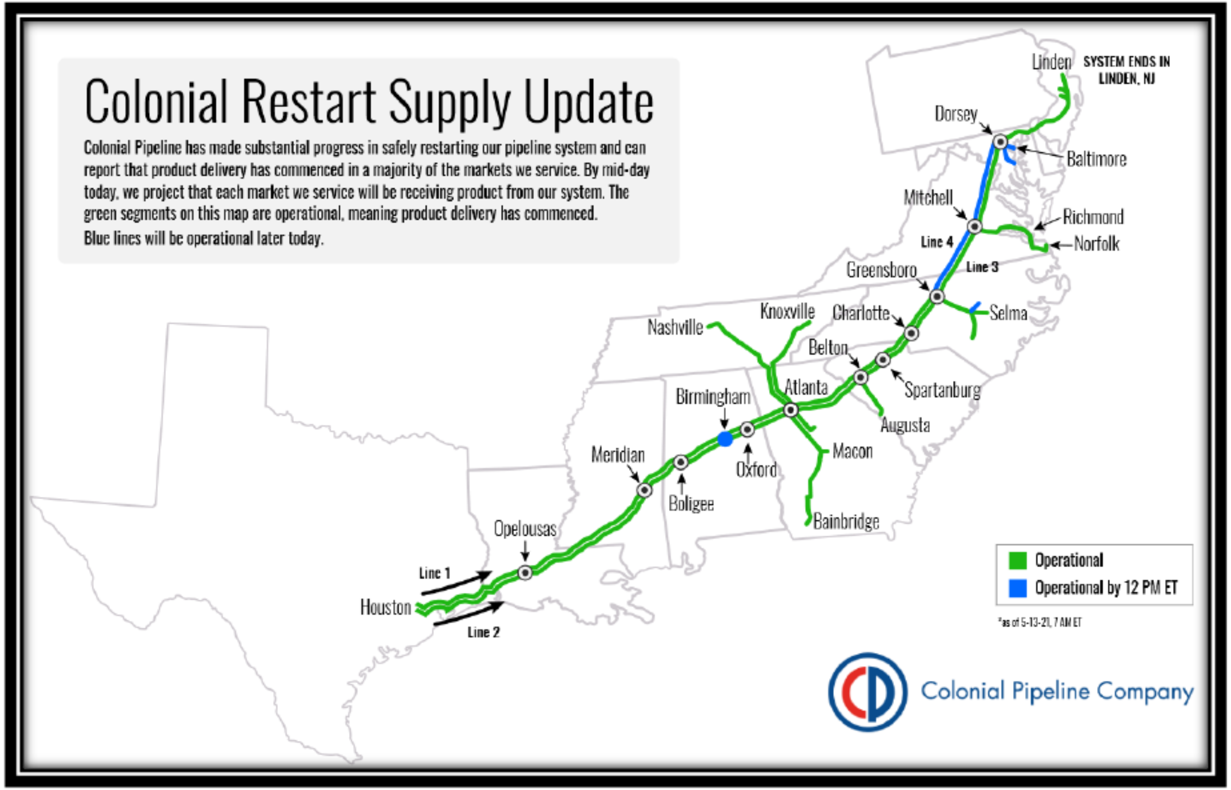
Q&A and Wild Speculation

Colonial Pipeline Details



- Largest refined products pipeline in the US
- Moves 100 million gallons of fuel daily across 5,500 miles of pipeline
- Over 280 facilities and field terminals, transporting 45% of the fuel to the East Coast
- On Friday May 7th Colonial temporarily shut down all pipeline operations due to a ransomware attack on its IT business systems

Restoration of Service



Colonial Restart Supply Update

Colonial Pipeline has made substantial progress in safely restarting our pipeline system and can report that product delivery has commenced in a majority of the markets we service. By mid-day today, we project that each market we service will be receiving product from our system. The green segments on this map are operational, meaning product delivery has commenced.

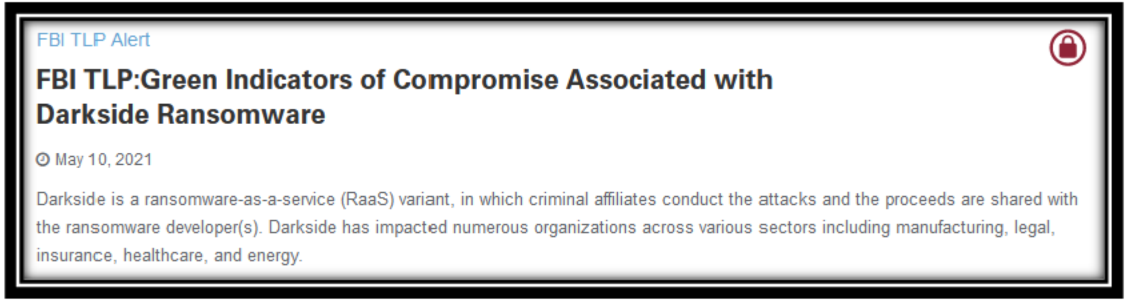
Blue lines will be operational later today.

🟩 Operational
🟦 Operational by 12 PM ET

*as of 5-13-21, 7 AM ET

- 5 days after the operational impact – startup began at Wednesday May 12 at 5:11PM
- May 13th - product delivery has commenced in most markets served
- All markets anticipated to be receiving product by mid-day

Entity Information Sharing

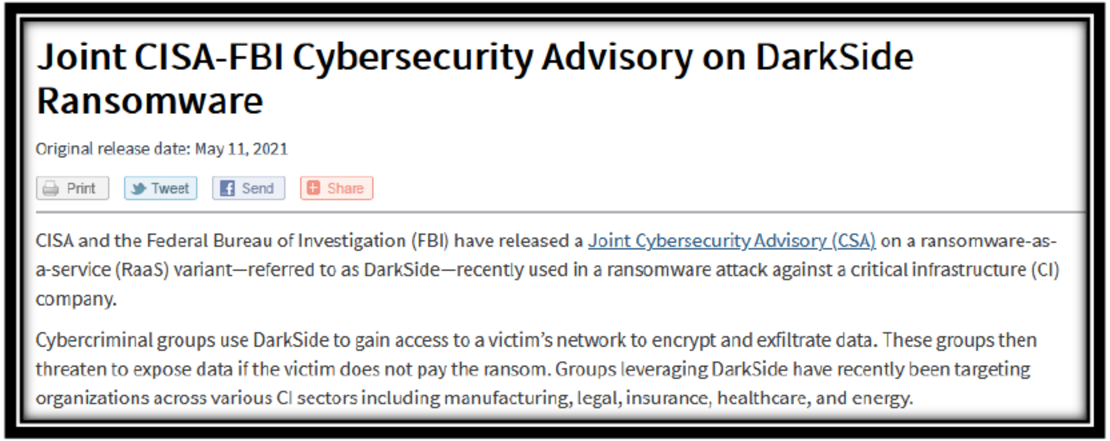


FBI TLP Alert

FBI TLP:Green Indicators of Compromise Associated with Darkside Ransomware

May 10, 2021

Darkside is a ransomware-as-a-service (RaaS) variant, in which criminal affiliates conduct the attacks and the proceeds are shared with the ransomware developer(s). Darkside has impacted numerous organizations across various sectors including manufacturing, legal, insurance, healthcare, and energy.

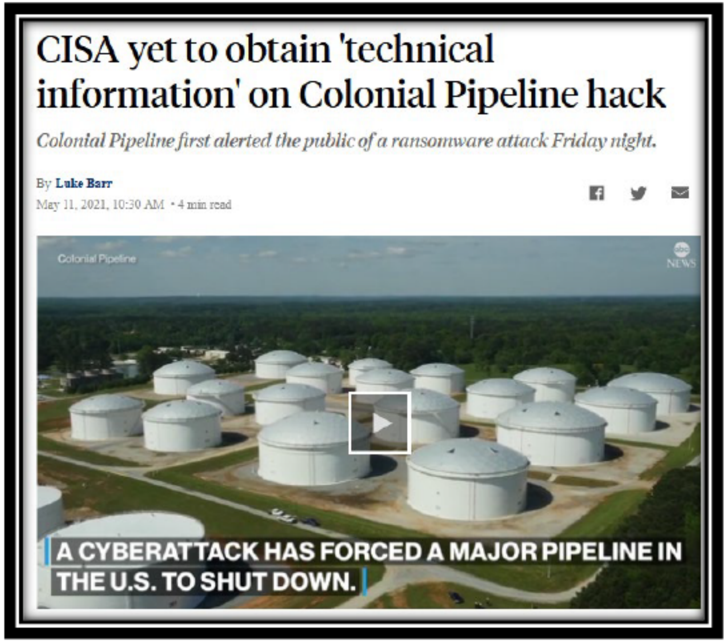


Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware

Original release date: May 11, 2021

CISA and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on a ransomware-as-a-service (RaaS) variant—referred to as DarkSide—recently used in a ransomware attack against a critical infrastructure (CI) company.

Cybercriminal groups use DarkSide to gain access to a victim's network to encrypt and exfiltrate data. These groups then threaten to expose data if the victim does not pay the ransom. Groups leveraging DarkSide have recently been targeting organizations across various CI sectors including manufacturing, legal, insurance, healthcare, and energy.



CISA yet to obtain 'technical information' on Colonial Pipeline hack

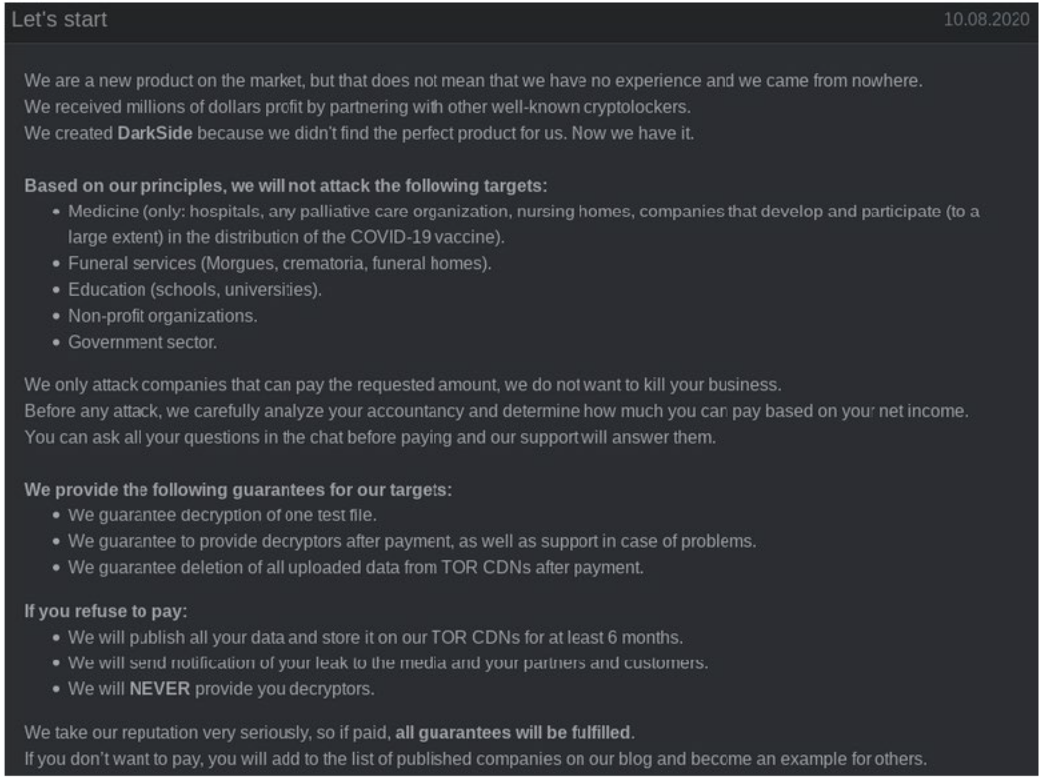
Colonial Pipeline first alerted the public of a ransomware attack Friday night.

By Luke Barr

May 11, 2021, 10:30 AM • 4 min read

Colonial Pipeline
abc NEWS
A CYBERATTACK HAS FORCED A MAJOR PIPELINE IN THE U.S. TO SHUT DOWN.

DarkSide Ransomware



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

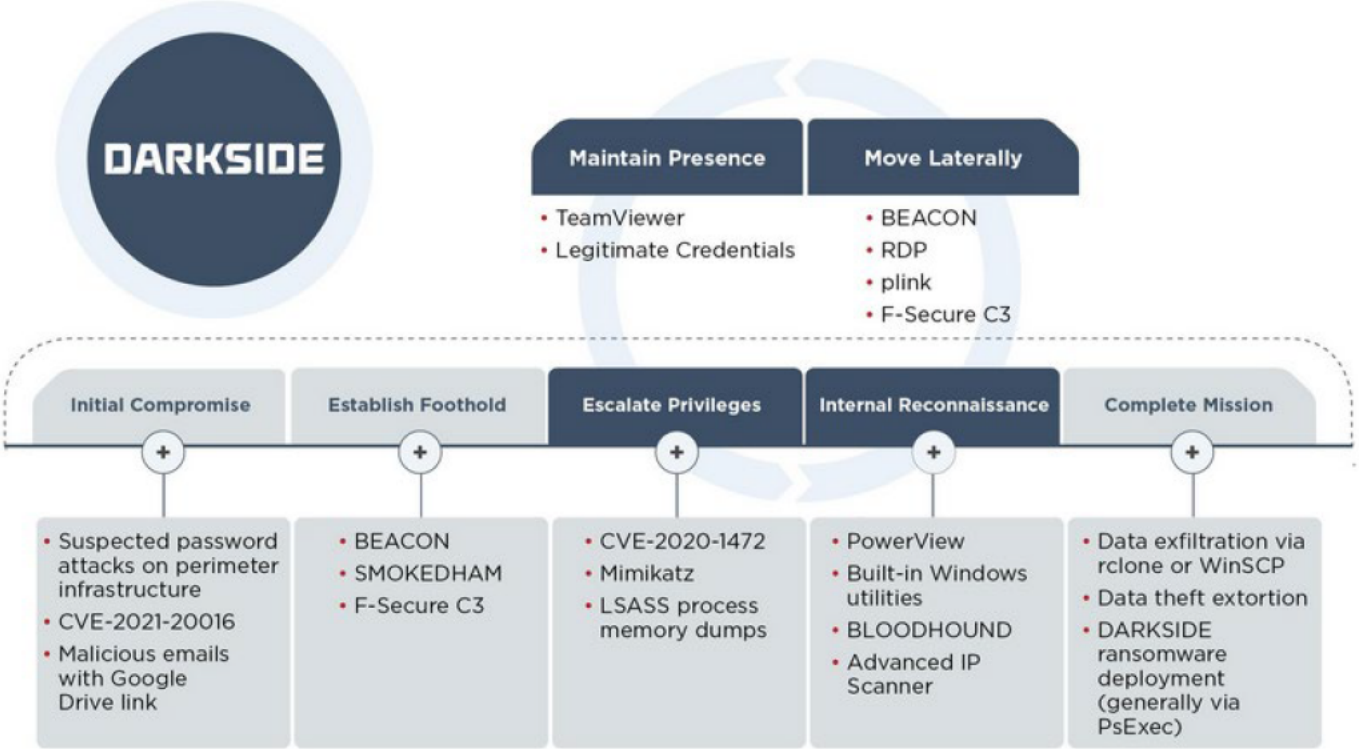
If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

- Ransomware-as-a-service
- Double extortion – payment for decryption and payment to delete stolen data
- Operates with affiliates
- Claims no geopolitical affiliation and claims only driver is financial
- Intends to provide moderation and review future targets

FIREEYE Released Darkside Report - Attack Lifecycle



DARKSIDE

Maintain Presence

- TeamViewer
- Legitimate Credentials

Move Laterally

- BEACON
- RDP
- plink
- F-Secure C3

Initial Compromise

- Suspected password attacks on perimeter infrastructure
- CVE-2021-20016
- Malicious emails with Google Drive link

Establish Foothold

- BEACON
- SMOKEDHAM
- F-Secure C3

Escalate Privileges

- CVE-2020-1472
- Mimikatz
- LSASS process memory dumps

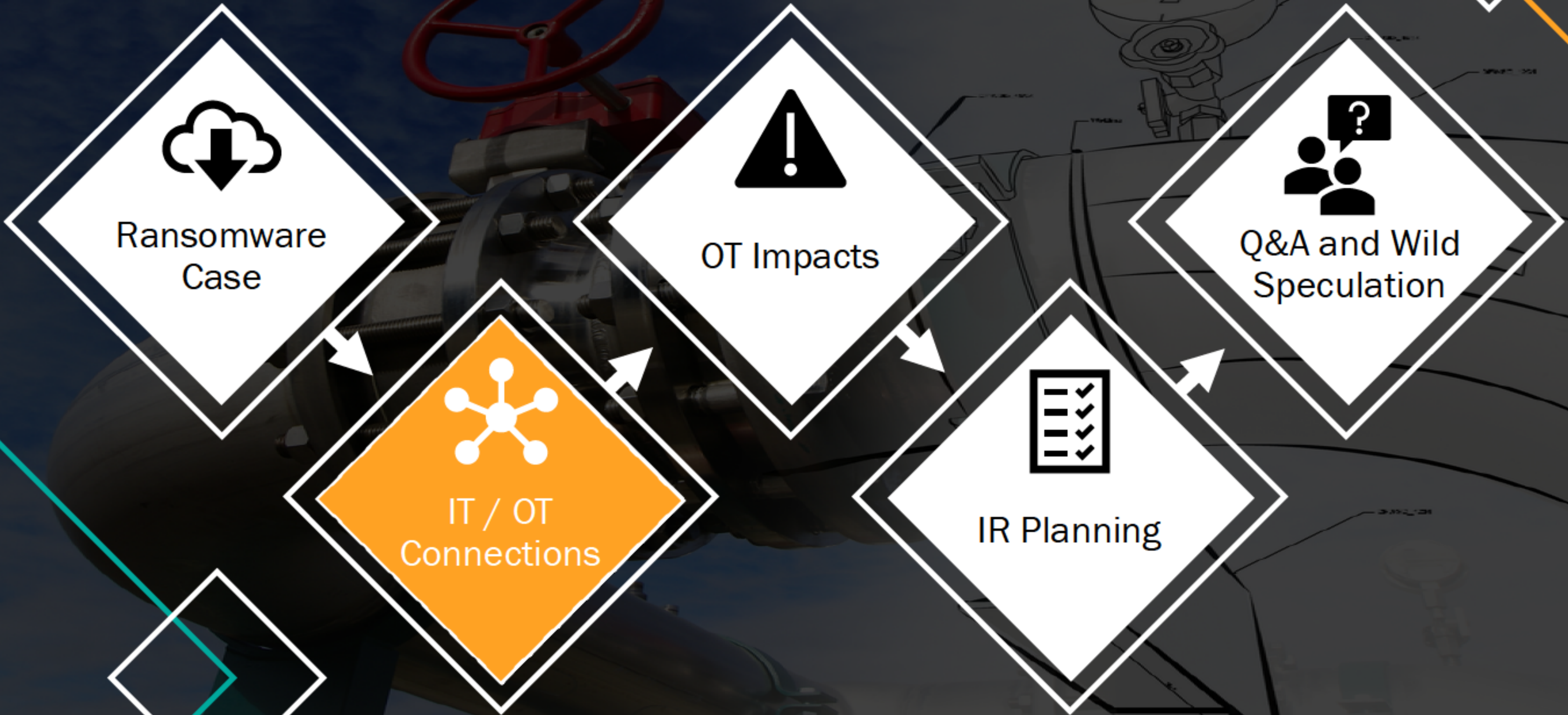
Internal Reconnaissance

- PowerView
- Built-in Windows utilities
- BLOODHOUND
- Advanced IP Scanner

Complete Mission

- Data exfiltration via rclone or WinSCP
- Data theft extortion
- DARKSIDE ransomware deployment (generally via PsExec)

The Big Question



Ransomware Case

IT / OT Connections

OT Impacts

IR Planning

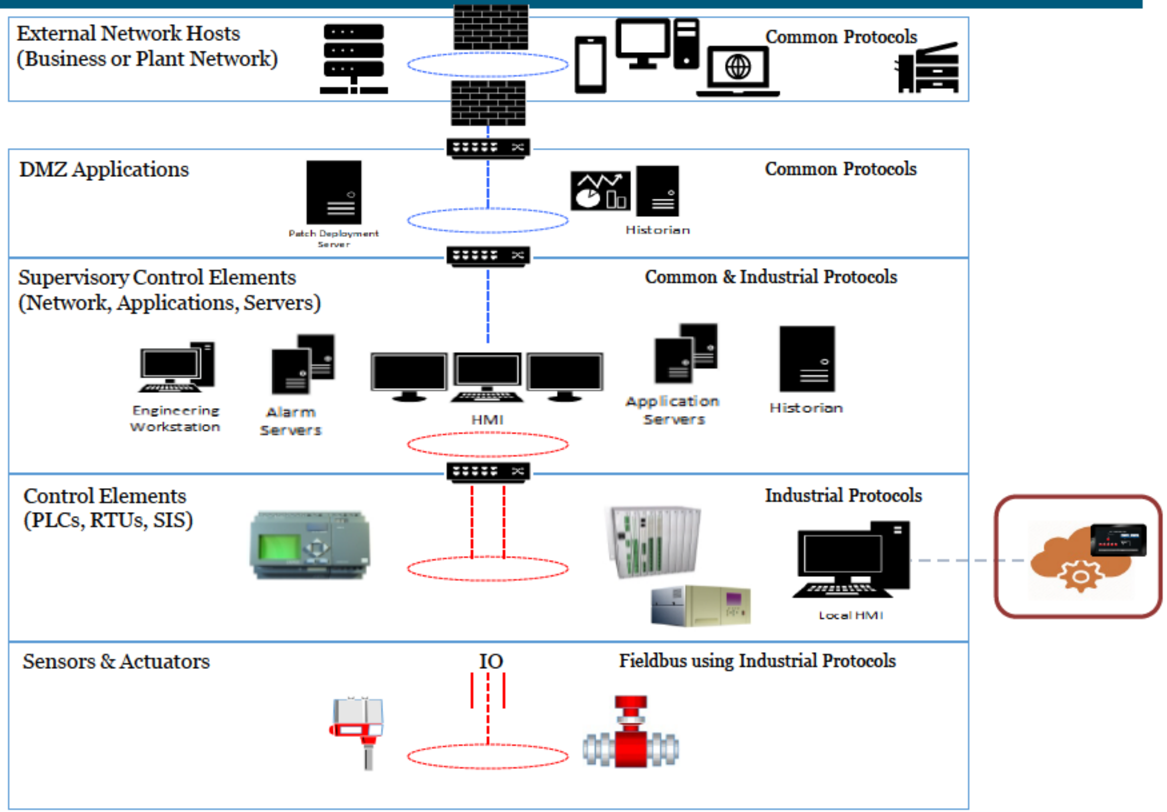
Q&A and Wild Speculation

Elephant in the Room

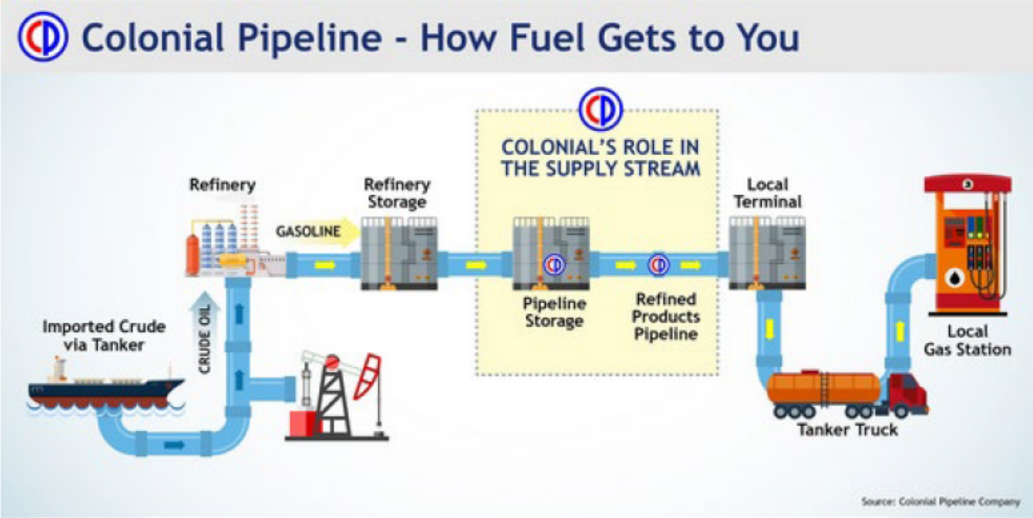
On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we ***proactively took certain systems offline*** *to contain the threat, which has temporarily* ***halted all pipeline operations****, and* ***affected some of our IT systems****.*

IT / OT and the “in between” aka bridges for business / badness

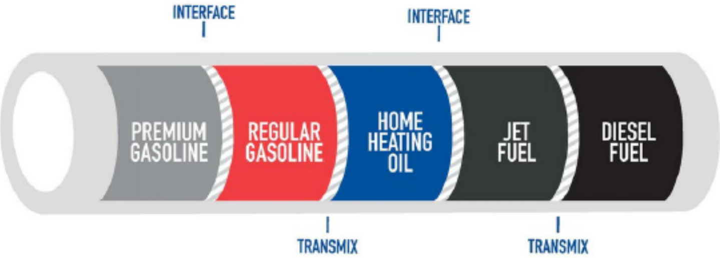
- Attacks on corporate IT networks that pivot over trusted communications to resources in industrial DMZs
- Connections to partner networks that could extend impacts beyond target



Numerous Products


Colonial Pipeline - How Fuel Gets to You
COLONIAL'S ROLE IN THE SUPPLY STREAM
Refinery
Refinery Storage
GASOLINE
Local Terminal
Imported Crude via Tanker
CRUDE OIL
Pipeline Storage
Refined Products Pipeline
Local Gas Station
Tanker Truck

Source: Colonial Pipeline Company



Product Sequencing

- Loaded in as batches
- Products blend with each other at interface points
- Interfaces are removed at destination sites
- Control Center SCADA system monitors flow, temperature, pressure, quality, and leak detection

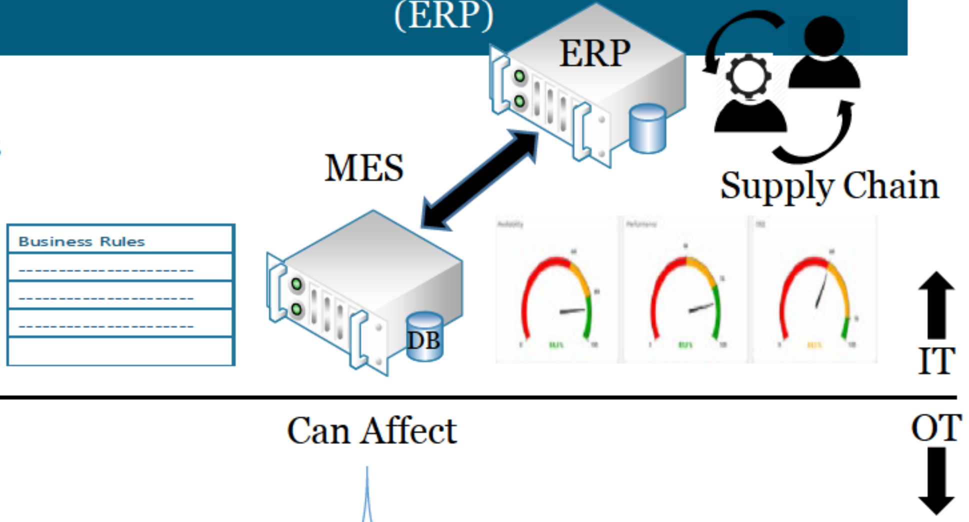
IT Assets that Affect OT Production

Manufacturing Execution Systems (MES) is a bridge between Information Technology (IT) and Operations Technology (OT)

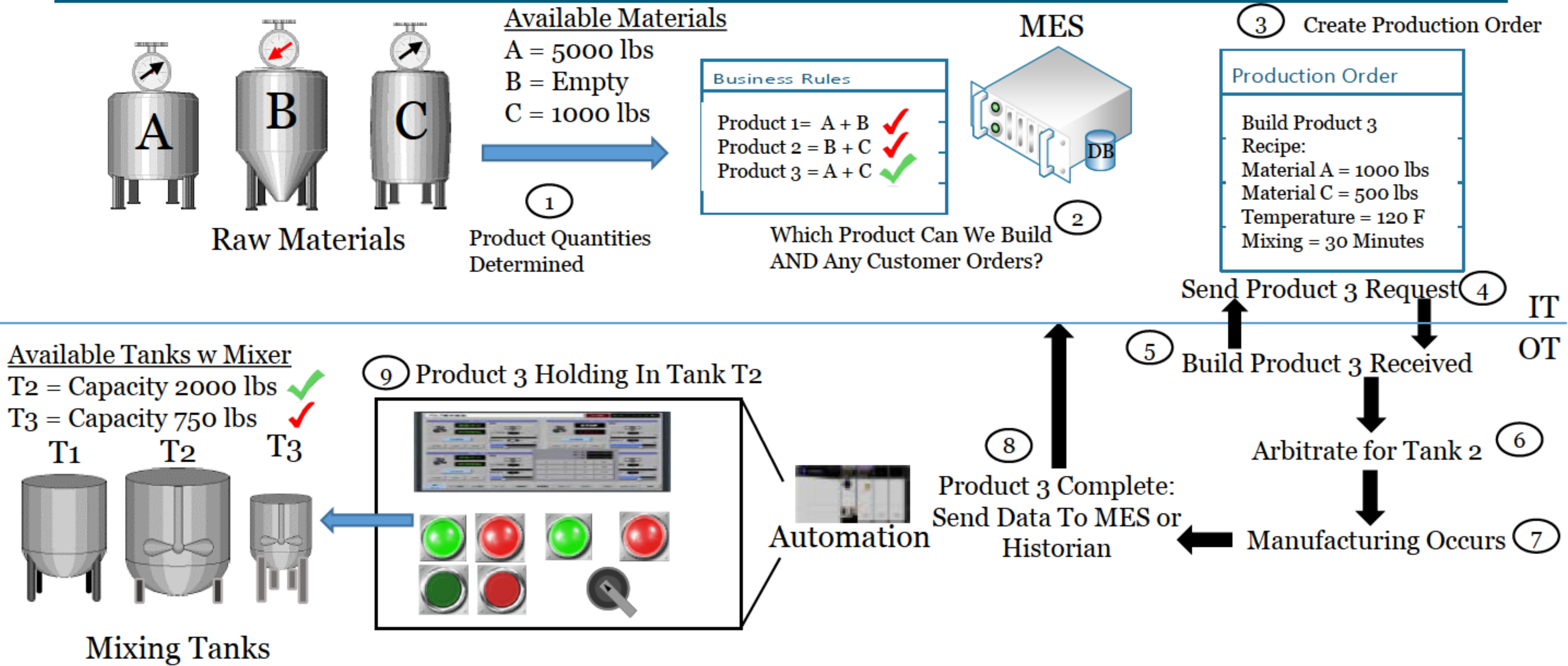
Used for:

- Recipe management
- Quality assurance
- Work In Process (WIP) tracking and genealogy
- Performance management
- Material tracking

Enterprise Resource Planning (ERP)



Autonomous Control With Dependencies on Higher Level Systems



Raw Materials

Available Materials

A = 5000 lbs

B = Empty

C = 1000 lbs

1 Product Quantities Determined

Business Rules

Product 1= A + B ✗

Product 2 = B + C ✗

Product 3 = A + C ✓

2 Which Product Can We Build AND Any Customer Orders?

3 Create Production Order

Production Order

Build Product 3

Recipe:

Material A = 1000 lbs

Material C = 500 lbs

Temperature = 120 F

Mixing = 30 Minutes

4 Send Product 3 Request

5 Build Product 3 Received

6 Arbitrate for Tank 2

7 Manufacturing Occurs

8 Product 3 Complete: Send Data To MES or Historian

9 Product 3 Holding In Tank T2

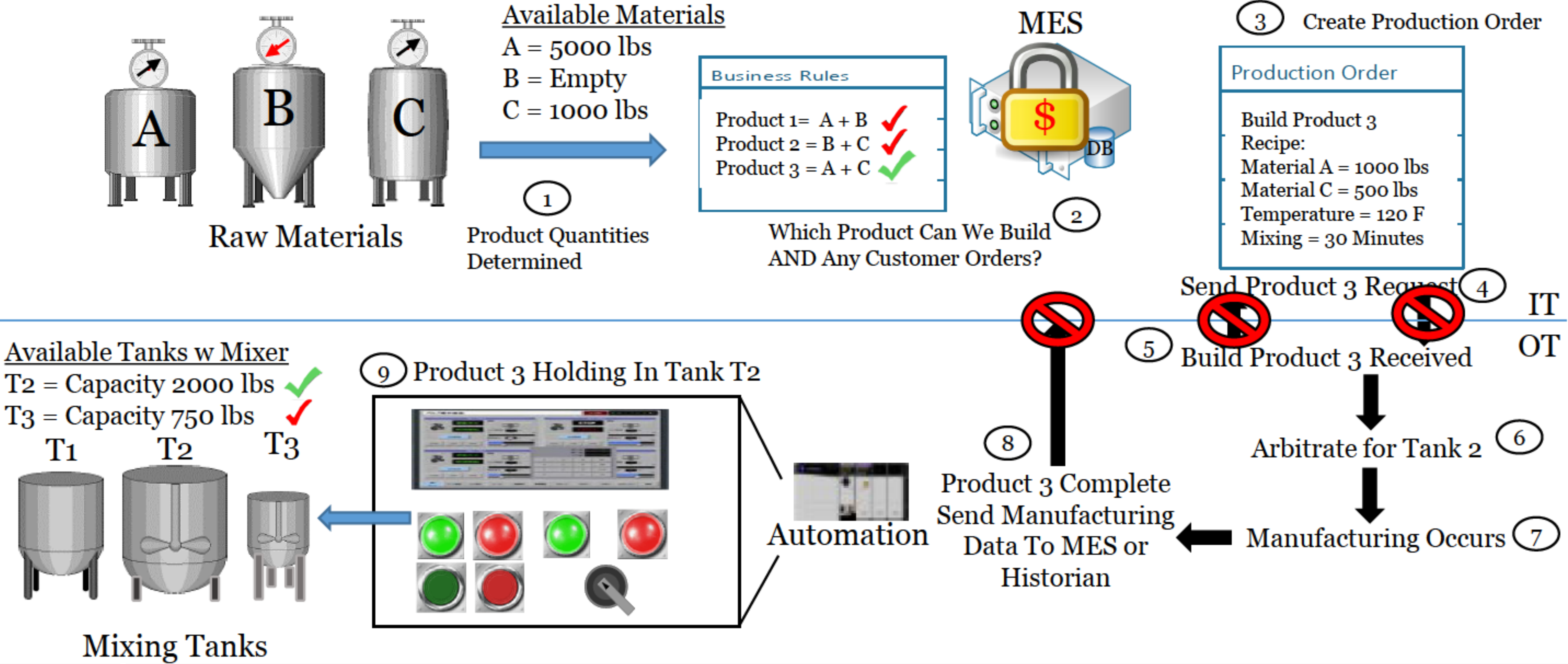
Available Tanks w Mixer

T2 = Capacity 2000 lbs ✓

T3 = Capacity 750 lbs ✗

Mixing Tanks

Autonomous Control With Dependencies on Higher Level Systems
Scenario: MES is unavailable AND Holding Product



Raw Materials

Available Materials
A = 5000 lbs
B = Empty
C = 1000 lbs

1 Product Quantities Determined

Business Rules

Product 1= A + B ✓
Product 2 = B + C ✓
Product 3 = A + C ✓

MES

2 Which Product Can We Build AND Any Customer Orders?

3 Create Production Order

Production Order

Build Product 3
Recipe:
Material A = 1000 lbs
Material C = 500 lbs
Temperature = 120 F
Mixing = 30 Minutes

4 Send Product 3 Request

IT

OT

5 Build Product 3 Received

6 Arbitrate for Tank 2

7 Manufacturing Occurs

8 Product 3 Complete Send Manufacturing Data To MES or Historian

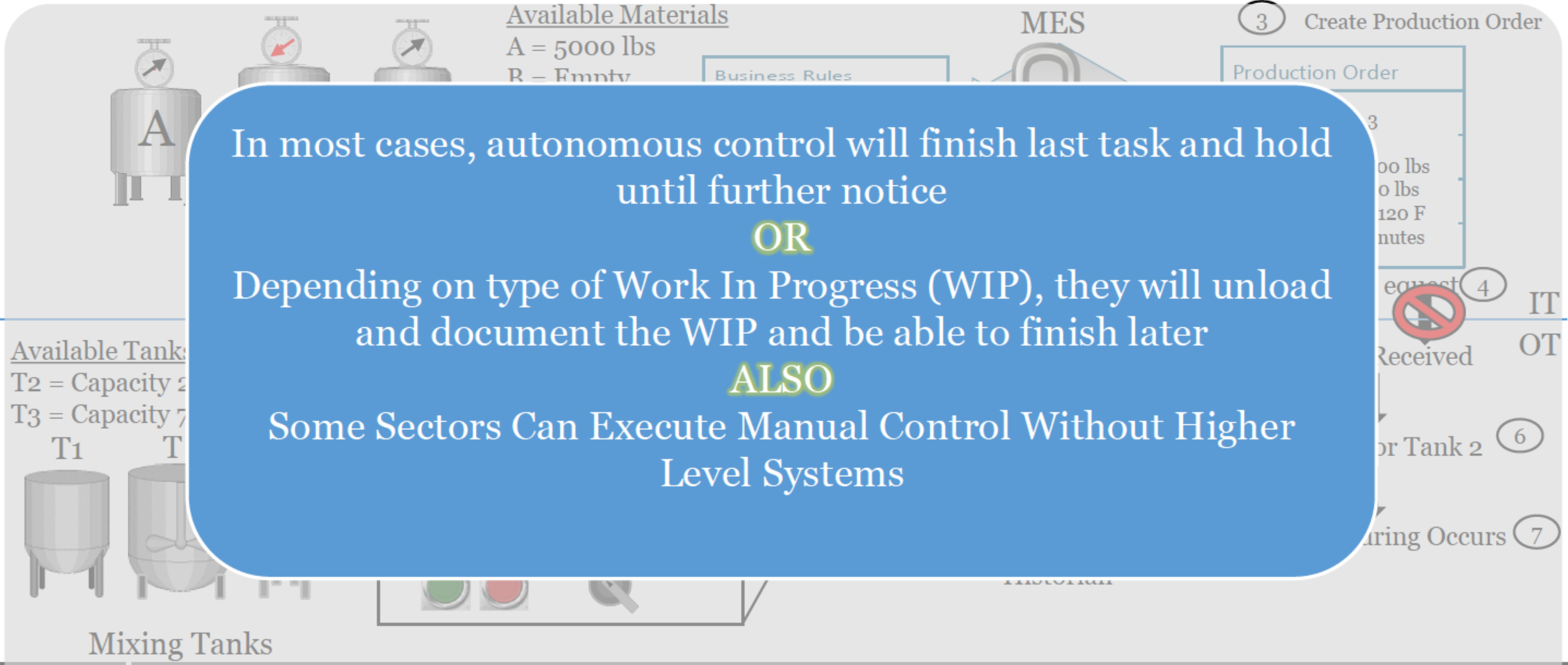
9 Product 3 Holding In Tank T2

Automation

Available Tanks w Mixer
T2 = Capacity 2000 lbs ✓
T3 = Capacity 750 lbs ✓

Mixing Tanks

Autonomous Control With Dependencies on Higher Level Systems
Scenario: MES is unavailable AND Holding Product



In most cases, autonomous control will finish last task and hold until further notice

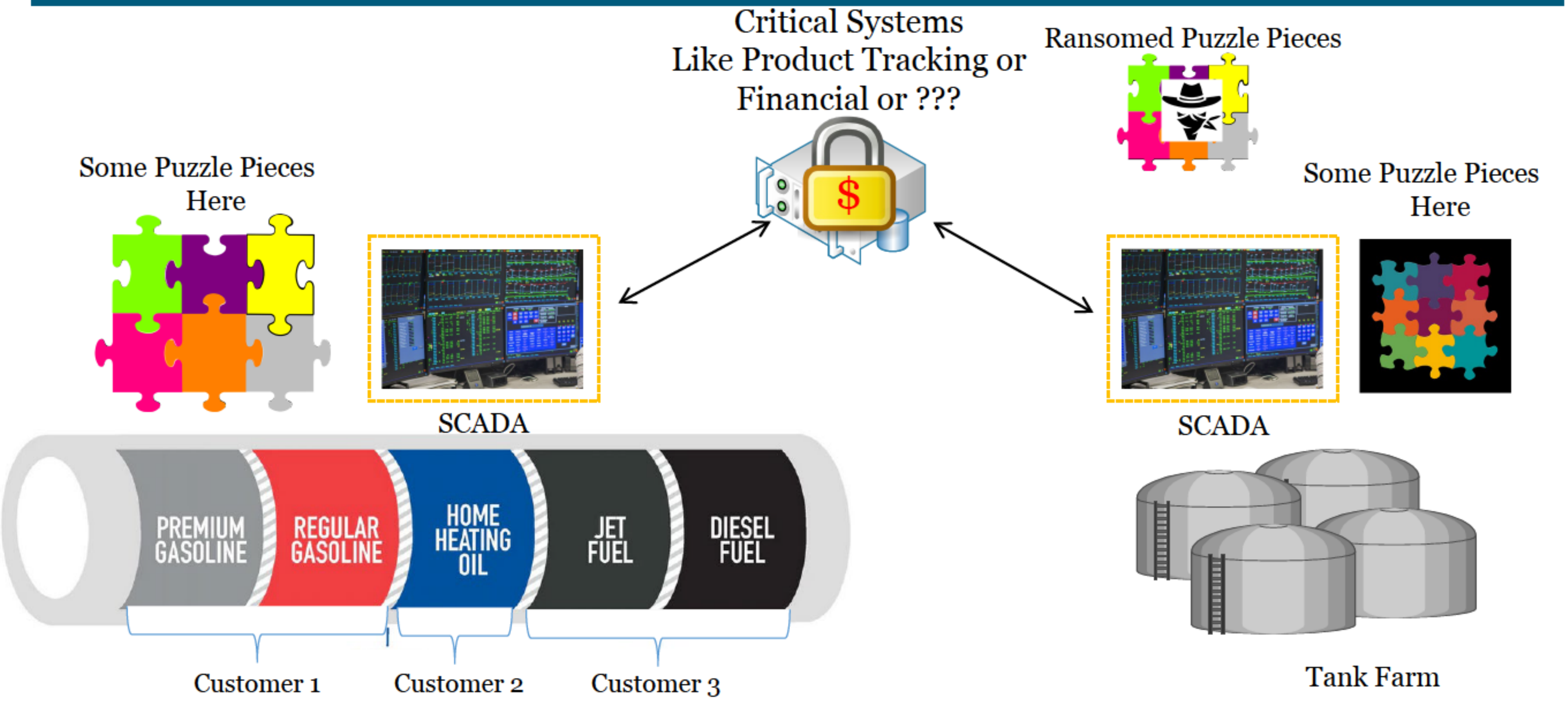
OR

Depending on type of Work In Progress (WIP), they will unload and document the WIP and be able to finish later

ALSO

Some Sectors Can Execute Manual Control Without Higher Level Systems

IT and OT Asset Critical Interdependencies



Critical Systems
Like Product Tracking or
Financial or ???

Ransomed Puzzle Pieces

Some Puzzle Pieces
Here

SCADA

Some Puzzle Pieces
Here

SCADA

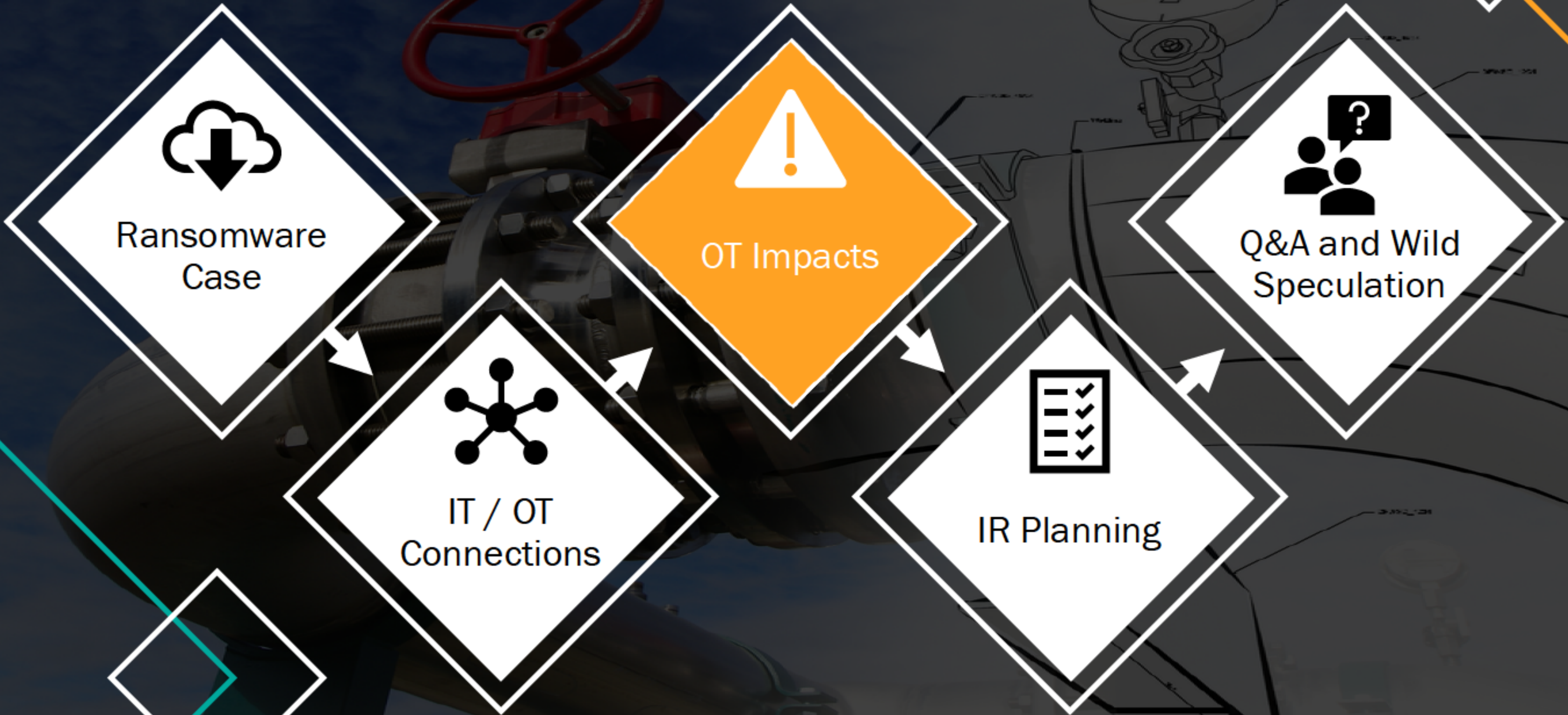
Tank Farm

Customer 1

Customer 2

Customer 3

What If?



Ransomware Case

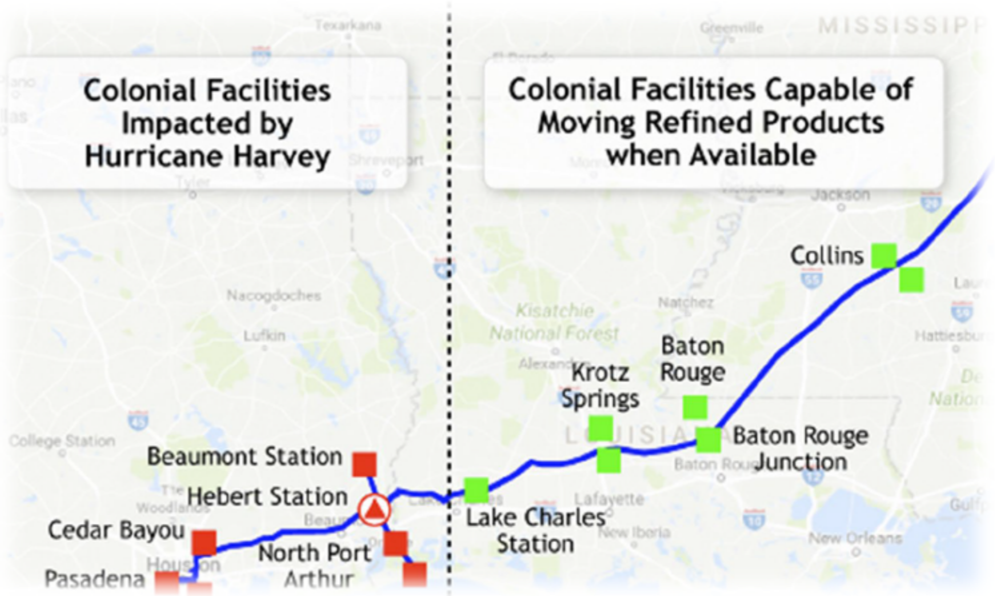
IT / OT Connections

OT Impacts

IR Planning

Q&A and Wild Speculation

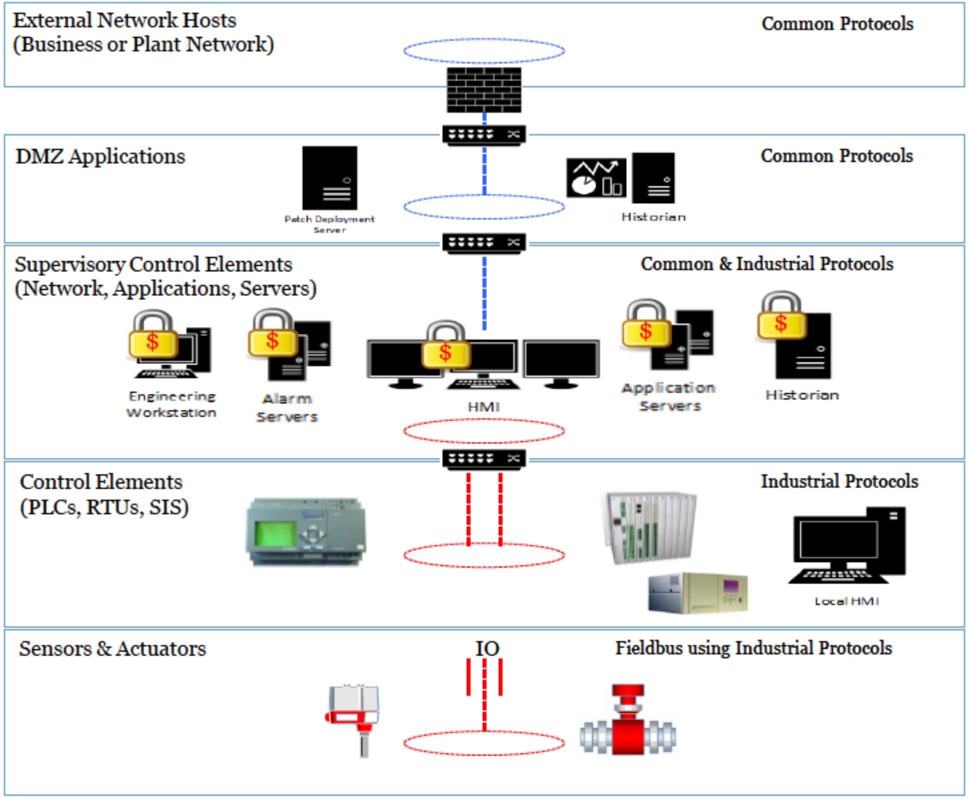
Emergency Operations



cks line up at a Colonial Pipeline facility in Pelham, Ala. (Jay Reeves/AP)

OT Assets – Ransomware Low Hanging Fruit

- Right now, Ransomware targets computer systems, not embedded systems like PLC's
  - Albeit there has been embedded system malware
- Affects include but are not limited to:
  - No access to design tools on engineering workstations
  - Loss of process visibility (HMI) & alarm servers
  - Loss of historical data
  - Loss of quality assurance systems
  - Loss of analytics tools
  - Loss of SCADA functions
  - Inability to authenticate users



External Network Hosts (Business or Plant Network) | Common Protocols

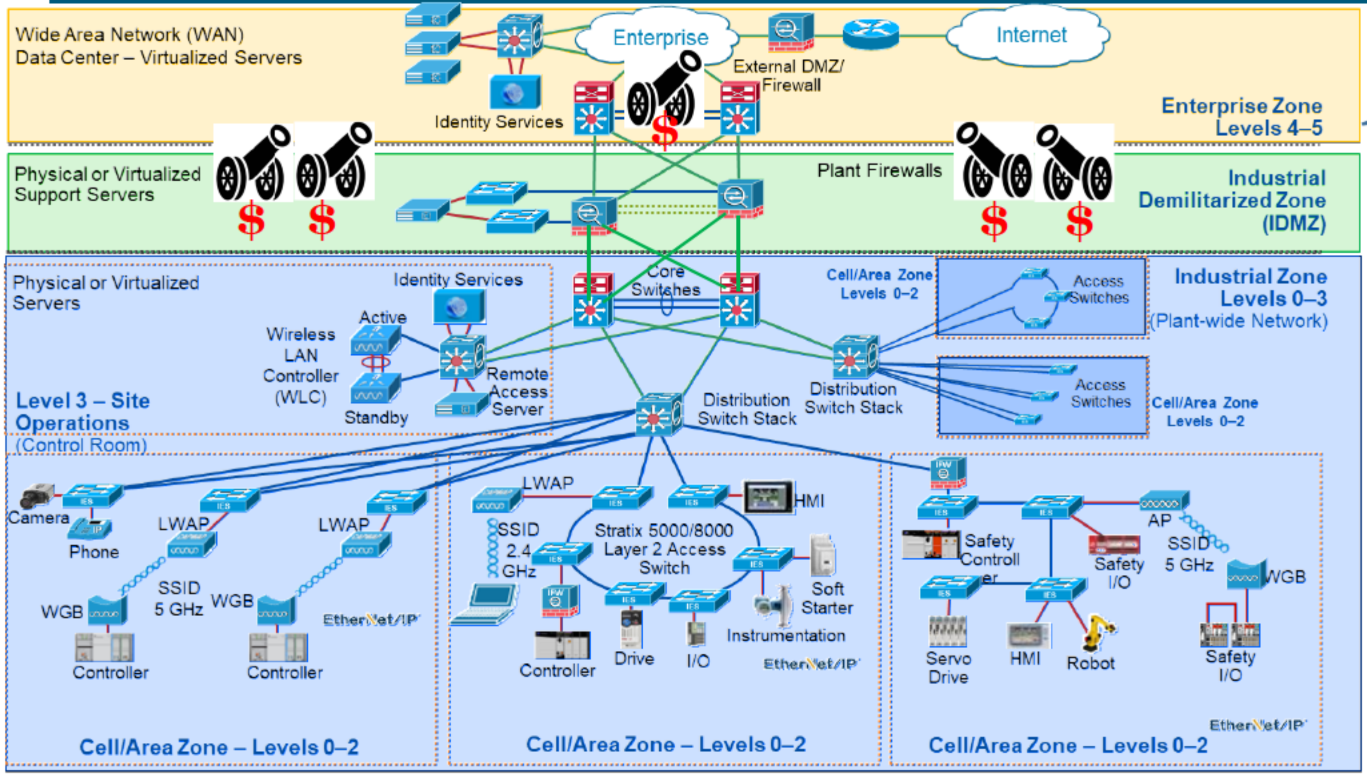
DMZ Applications | Common Protocols

Supervisory Control Elements (Network, Applications, Servers) | Common & Industrial Protocols

Control Elements (PLCs, RTUs, SIS) | Industrial Protocols

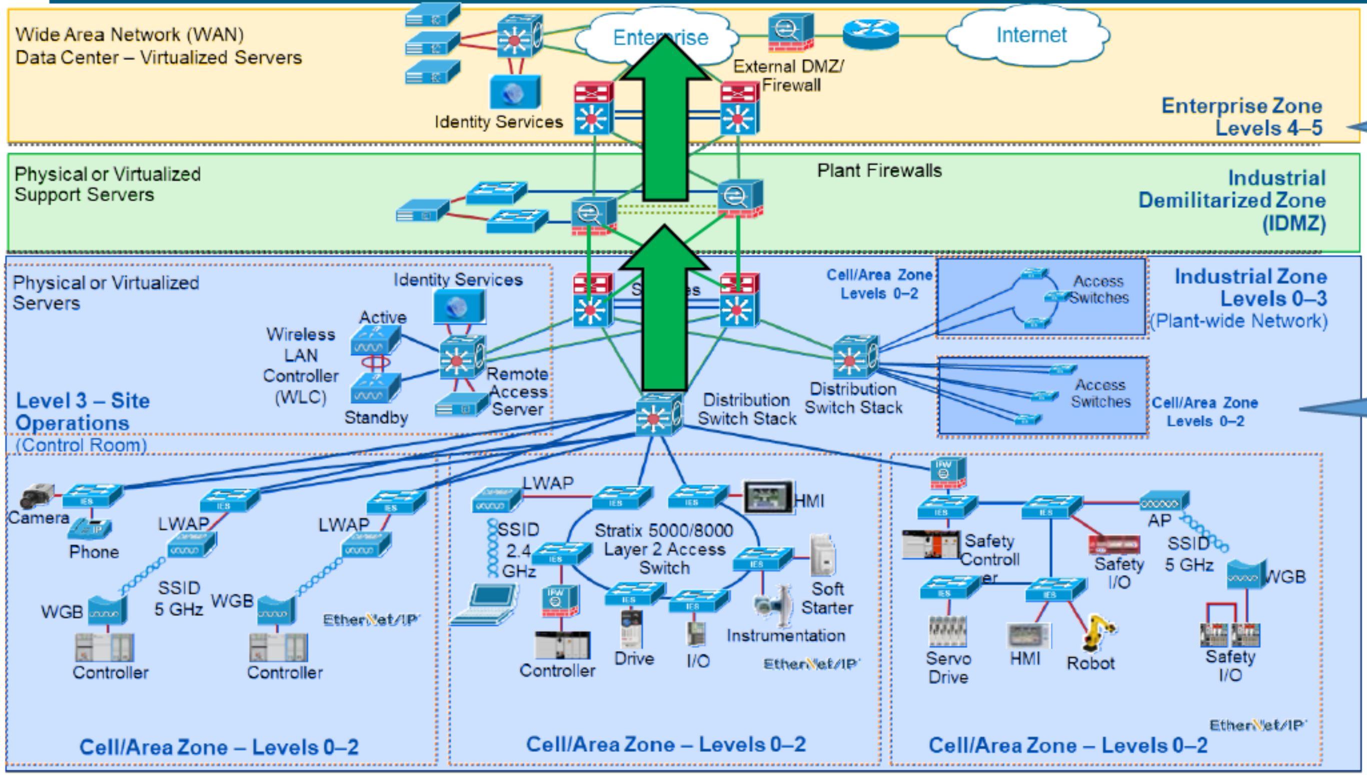
Sensors & Actuators | IO | Fieldbus using Industrial Protocols

Typical Architectures and Trust Models



Lots of spending and effort defending "forward" with less regards to ICS to Enterprise communications

Typical Architectures and Trust Models

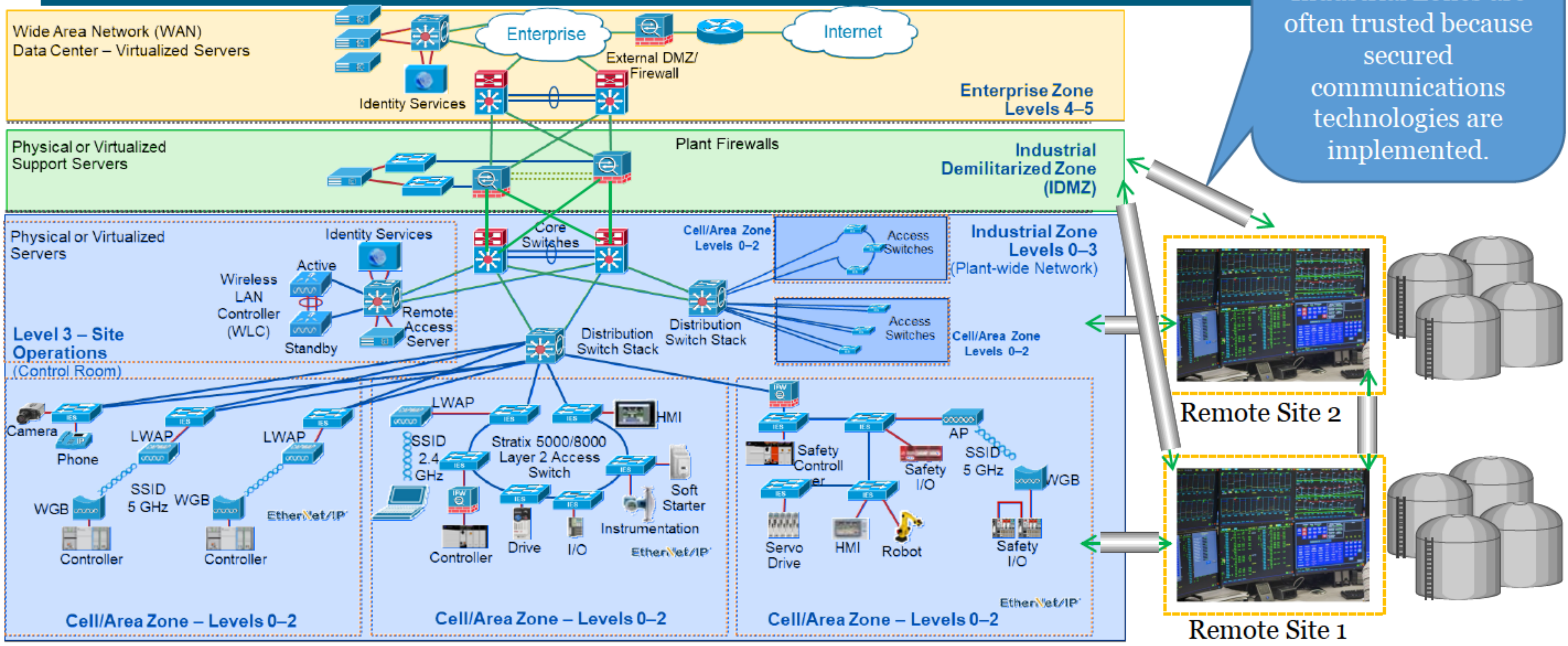

Wide Area Network (WAN)
Data Center – Virtualized Servers
Enterprise
Internet
External DMZ/ Firewall
Identity Services
Enterprise Zone Levels 4–5
Physical or Virtualized Support Servers
Plant Firewalls
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Level 3 – Site Operations
(Control Room)
Distribution Switch Stack
Distribution Switch Stack
Cell/Area Zone Levels 0–2
Access Switches
Industrial Zone Levels 0–3
(Plant-wide Network)
Access Switches
Cell/Area Zone Levels 0–2
Camera
Phone
LWAP
LWAP
SSID 5 GHz
WGB
WGB
Controller
Controller
EtherNet/IP
Cell/Area Zone – Levels 0–2
LWAP
SSID 2.4 GHz
Stratix 5000/8000 Layer 2 Access Switch
HMI
Soft Starter
Instrumentation
Controller
Drive
I/O
EtherNet/IP
Cell/Area Zone – Levels 0–2
Safety Controller
Safety I/O
AP
SSID 5 GHz
WGB
Servo Drive
HMI
Robot
Safety I/O
EtherNet/IP
Cell/Area Zone – Levels 0–2

Oftentimes, traffic originating from the OT zone is trusted implicitly and allowed to traverse to the IDMZ or Enterprise zone

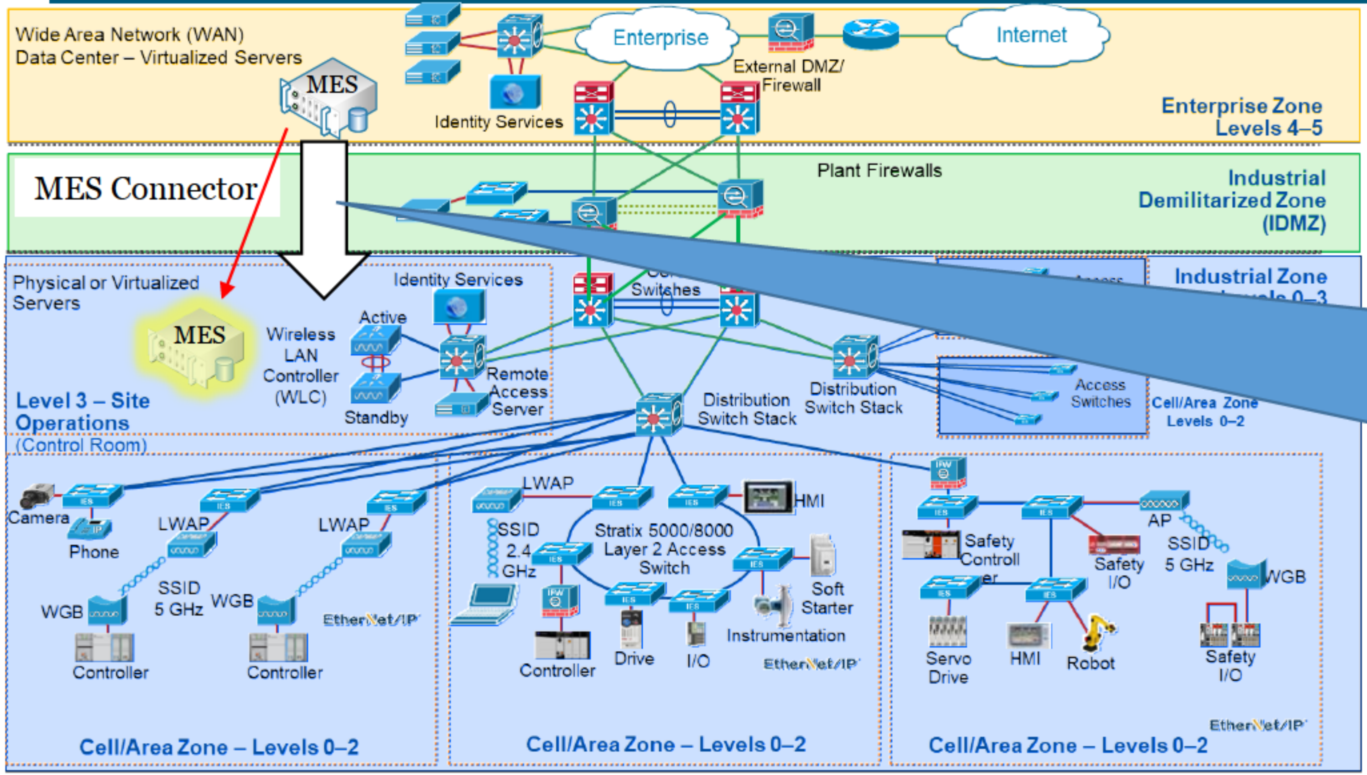
ICS Trust Zones are often large due to shared services and plant wide applications

Typical Architectures and Trust Models

Remote Site communications, call this extended Industrial Zones are often trusted because secured communications technologies are implemented.



Typical Architectures and Trust Models

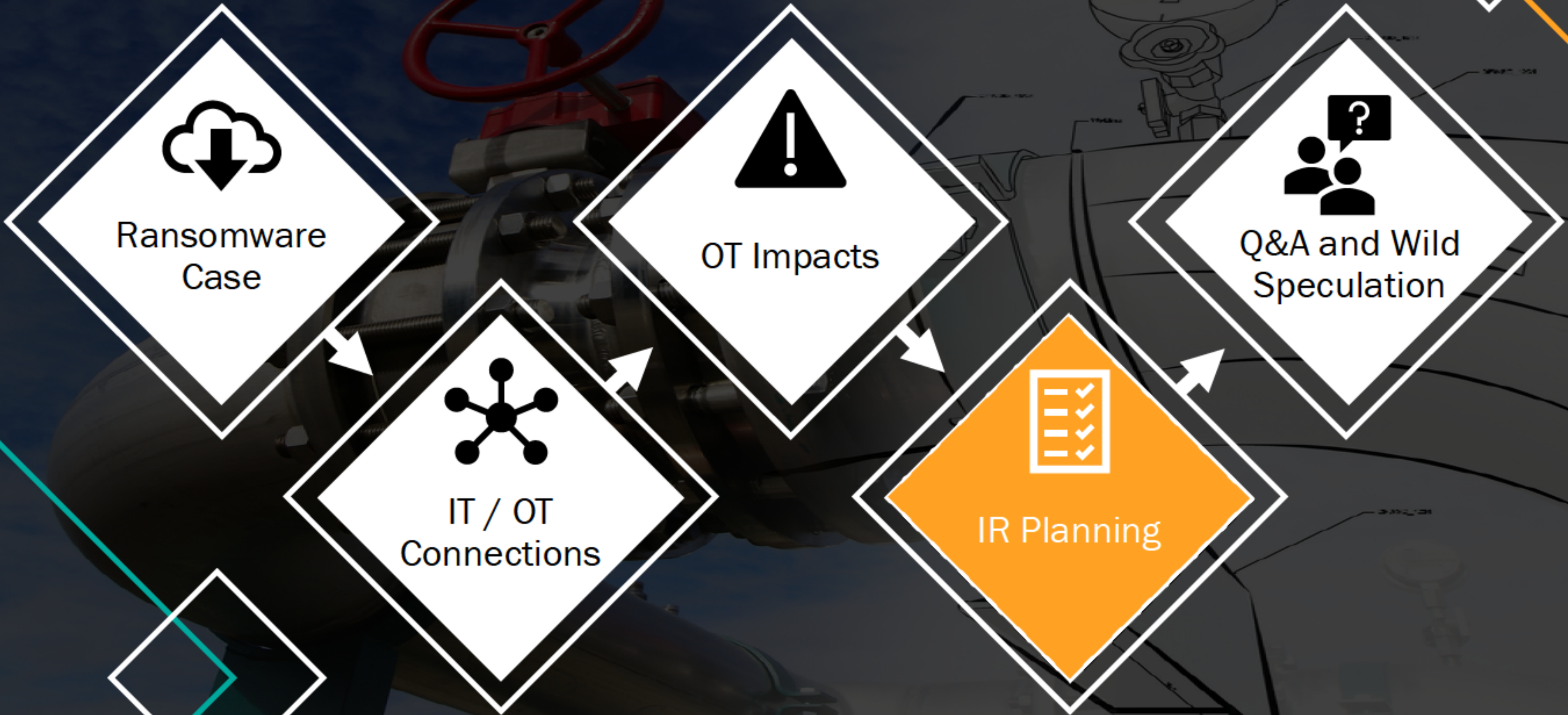


MES Connector

In some cases, IDMZ Firewalls allow entire IT networks to communicate with ICS assets or vice versa (Example Historian or MES)

Some MES technologies don't support a proxy in the IDMZ so direct connection from the Enterprise to the Industrial Zone is chosen. Alternatives would be architecting the MES solution in the Industrial Zone

Incident Response



Ransomware Case

IT / OT Connections

OT Impacts

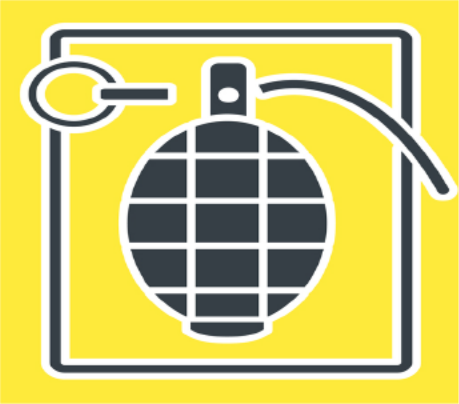
IR Planning

Q&A and Wild Speculation

Considerations and Time Horizons

BEFORE

- □ Training and exercises
- □ Operations focused architecture
- □ OT specific detection
- □ Procedural reviews for incident response



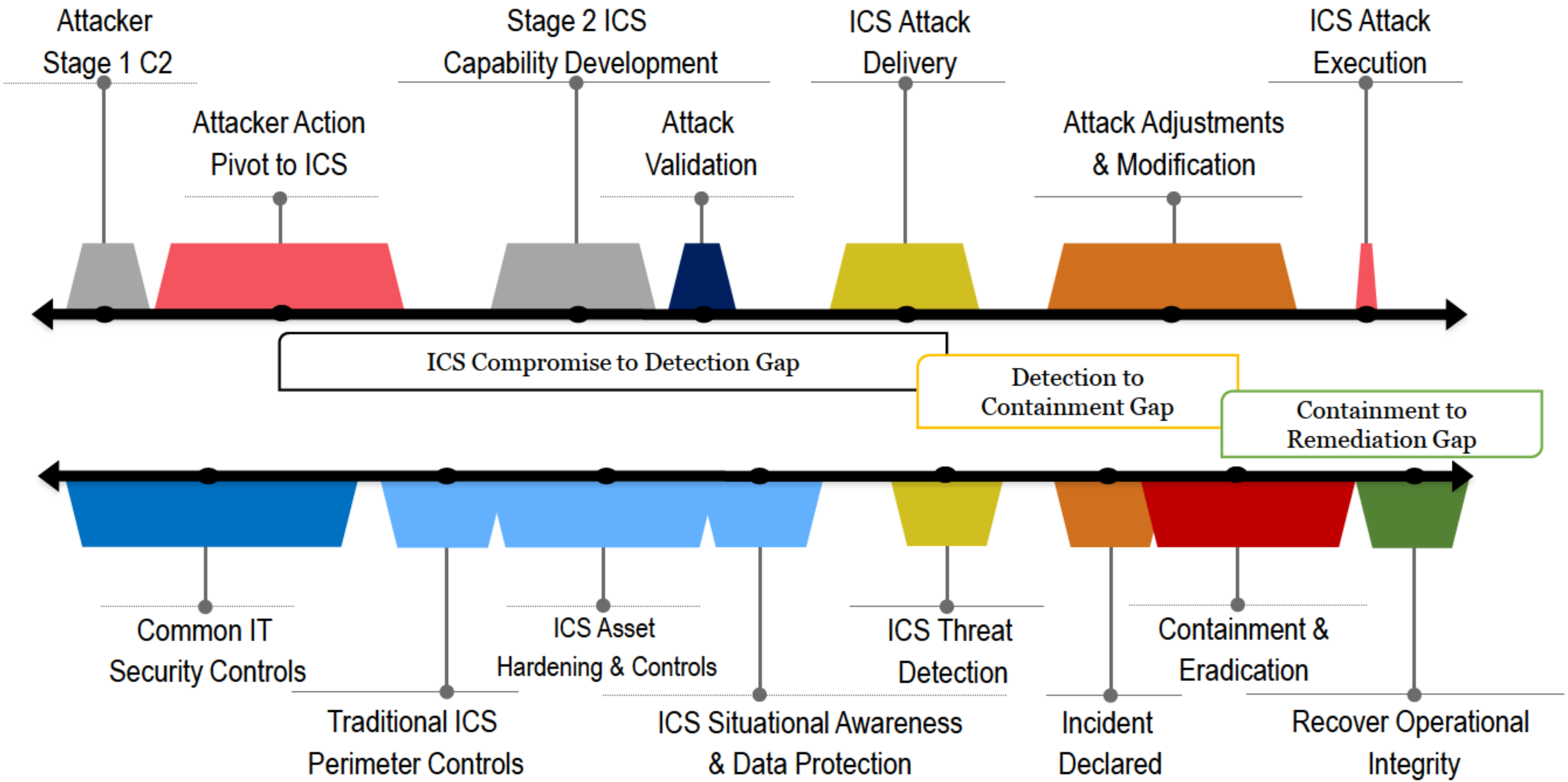
DURING

- □ Control inhibit
- □ Evaluate integrity of system
- □ Operate through or controlled outage
- □ Information sharing

AFTER

- □ Restoration and validation
- □ Safety walk downs
- □ Analysis and after action
- □ Planned startup

ICS Defender Gap Reduction


Attacker Stage 1 C2
Stage 2 ICS Capability Development
ICS Attack Delivery
ICS Attack Execution
Attacker Action Pivot to ICS
Attack Validation
Attack Adjustments & Modification
ICS Compromise to Detection Gap
Detection to Containment Gap
Containment to Remediation Gap
Common IT Security Controls
ICS Asset Hardening & Controls
ICS Threat Detection
Containment & Eradication
Traditional ICS Perimeter Controls
ICS Situational Awareness & Data Protection
Incident Declared
Recover Operational Integrity

Breaking Down the ICS Assets Into Their Atomic Elements

PLC

- Firmware
- Program
- Data
- Configuration
- Design Software

Switches, Routers and Firewall

- Firmware
- Configuration
- Design Software

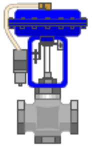
HMI

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

Server(s) and Applications

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

Smart Valves



- Firmware
- Configuration
- Design Software

- Determining the fundamental building blocks within the ICS environment will guide you to how to rebuild a system when you are forced to do so
- Determining the atomic elements of what can be backed up in order to support a system restore is critical
- Also documenting and storing configurations will be key to your success
  - 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?

Breaking Down the ICS Assets Into Their Atomic Elements

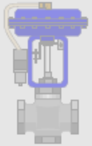
PLC

- Firm
- Pro
- Dat
- Co
- Des

HMI

- Fir
- Pro
- Rec
- Co
- Des

Smart Valves



- Firm
- Config
- Design Software

Switches, Routers and Firewall

- Determining the fundamental
ocks within the ICS
will guide you to
d a system when
d to do so

the atomic
hat can be
order to support
ore is critical

nting and storing
s will be key to

.S. tweaks did
to get the
tions running

irmware levels
he devices running
at? Can you still get the
running system
firmware?

ICS Axioms

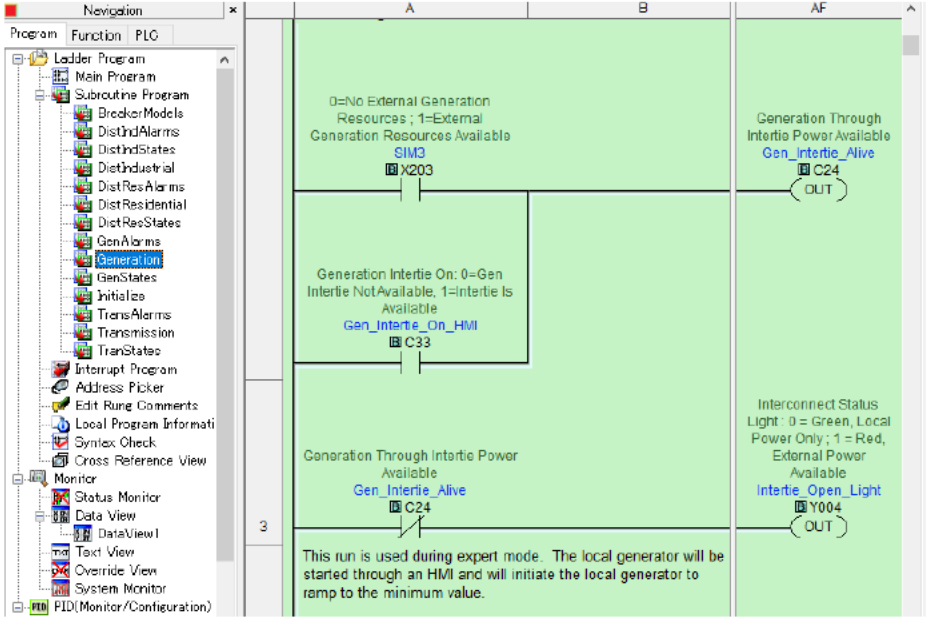
- Backups in ICS exist but are hardly ever current

- Plan for the worst day scenario where you rebuild from "scratch" where scratch is defined with starting from some out of date artifact and a new O.S. install

- Don't expect that your O.E.M. or System Integrator to save you because they won't!

Automation Pre-Ransomware Considerations - Code

Protecting the Code



0=No External Generation Resources ; 1=External Generation Resources Available
SIM3
X203

Generation Through Intertie Power Available
Gen_Intertie_Alive
C24
OUT

Generation Intertie On: 0=Gen Intertie Not Available, 1=Intertie Is Available
Gen_Intertie_On_HMI
C33

Generation Through Intertie Power Available
Gen_Intertie_Alive
C24

Interconnect Status Light : 0 = Green, Local Power Only ; 1 = Red, External Power Available
Intertie_Open_Light
Y004
OUT

This run is used during expert mode. The local generator will be started through an HMI and will initiate the local generator to ramp to the minimum value.

- Code allows one to determine the operation of each asset.
- It removes the conjecture of how something “thinks” it works and clearly shows how it actually works.
- Many times the “Gold” copy of the code that is stored on a drive somewhere will not be updated with operational changes
  - If you know the latest changes are on the backup copy, this will save a lot of time running code comparisons

Automation Pre-Ransomware Considerations - Data

Generally speaking, there are four types of data that exist within an automation controller (PLC/PAC)

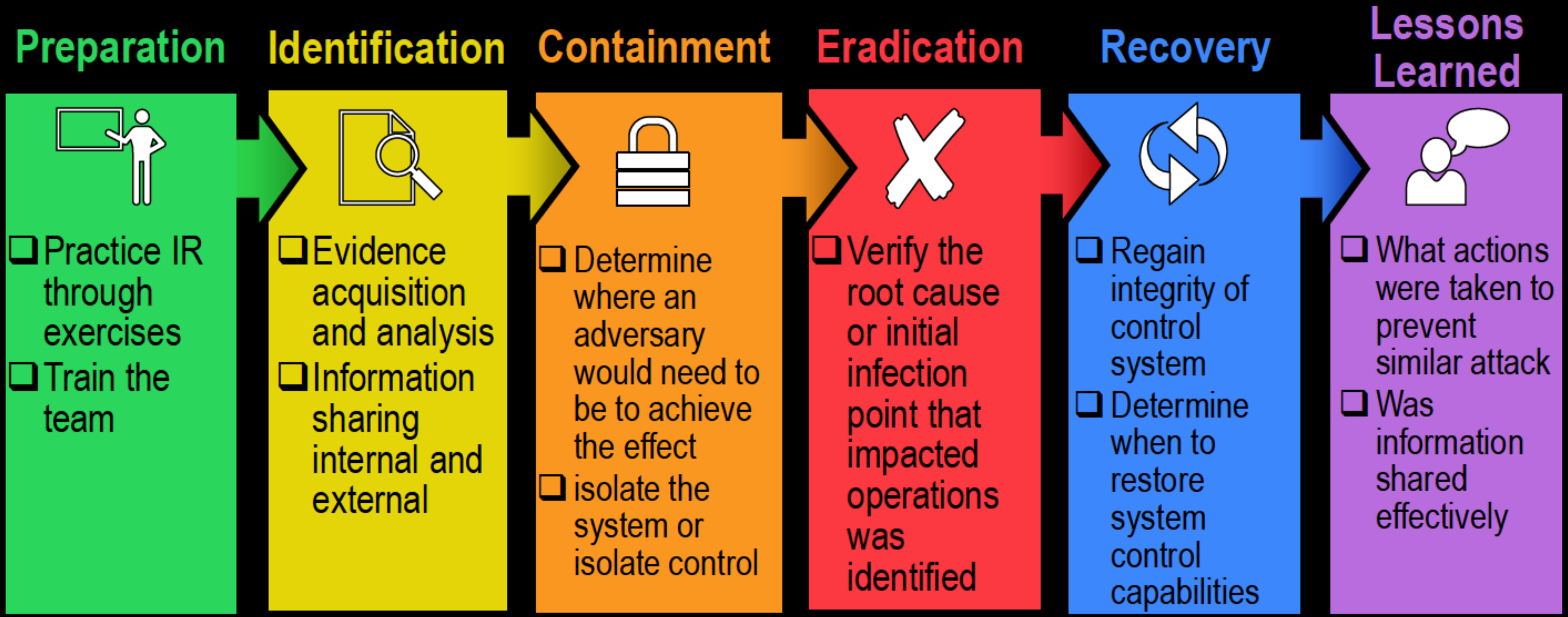
- Dynamic (Process or Computed Variables)
  - No action plan for recovery needed
- Recipe (Setpoints, Valve Spanning, General Configuration)
  - Can be stored in PLC, HMI (local or networked)
  - Recipes can come from higher level systems that can be targets for Ransomware
  - Recover action plan needed
- Current Batch or Product Data
  - Recovery action plan needed
  - You will want to store this if possible so you can track the manufacturing data of the WIP
  - You also need to determine how much data can be stored onboard
- Conditional (Zeroing or Homing a machine)
  - Operators must interact with machine / process
  - Recovery action plan needed

Recovery Plan

Engineering and Operator Recovery Plan	Machine: Dingle Arm Assy Machine 2	
	1	Locate Gold Copy and Compare Running PLC Code. Note differences and verify before loading Gold logic
	2	Validate last running part number and load recipe configuration file to the PLC
	3	Operator moves Dingle Arm Clamping Wedge to full forward position and calibrates spurving linear indicator and verifies offset = 0

Operational Response

Operators are continuously trained to ensure process safety, system reliability, and how to respond in emergencies to recover from system events. Likewise, the cyber operators who support the underlying technologies need to be trained in this way as well and integrate operations into all phases of the response plan.



Preparation

- □ Practice IR through exercises
- □ Train the team

Identification

- □ Evidence acquisition and analysis
- □ Information sharing internal and external

Containment

- □ Determine where an adversary would need to be to achieve the effect
- □ isolate the system or isolate control

Eradication

- □ Verify the root cause or initial infection point that impacted operations was identified

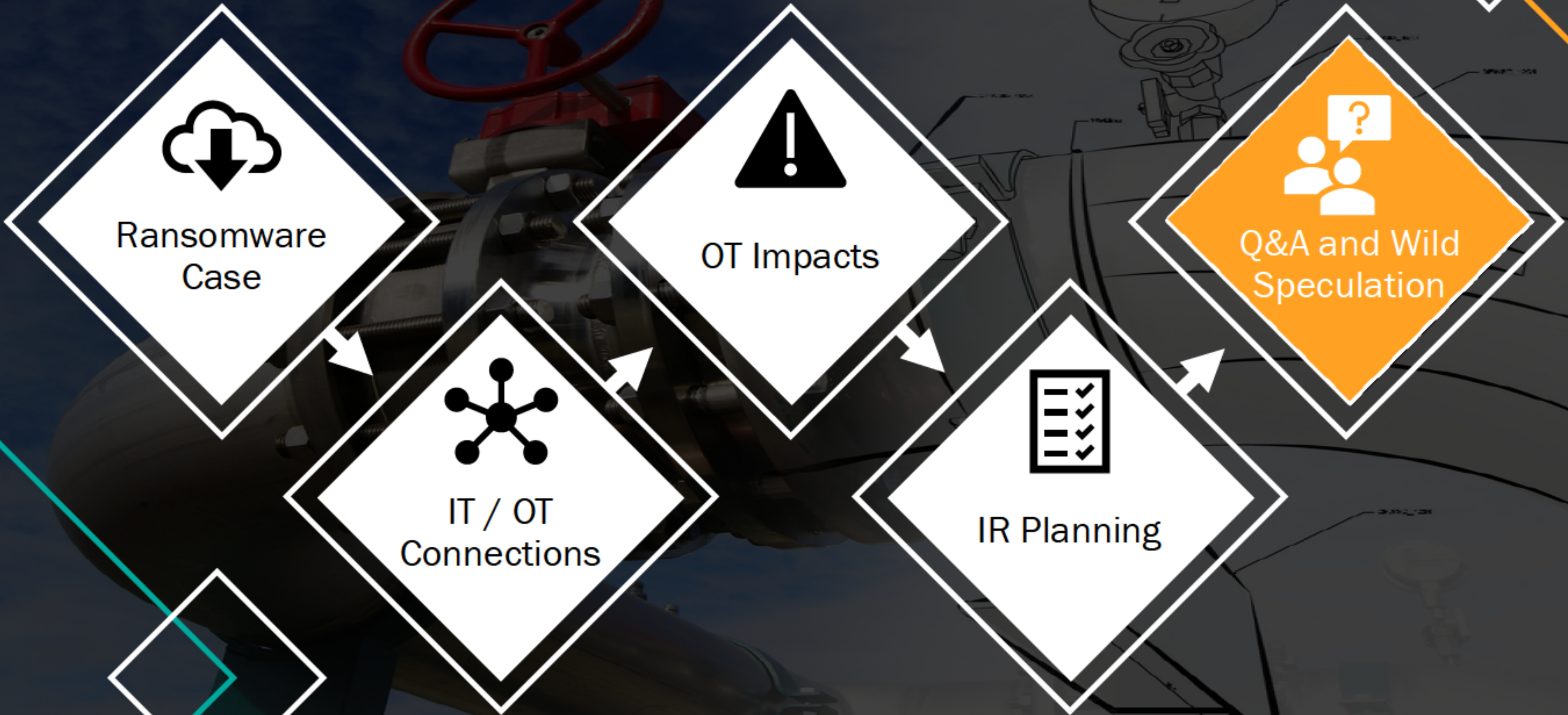
Recovery

- □ Regain integrity of control system
- □ Determine when to restore system control capabilities

Lessons Learned

- □ What actions were taken to prevent similar attack
- □ Was information shared effectively

Next Steps



Ransomware Case

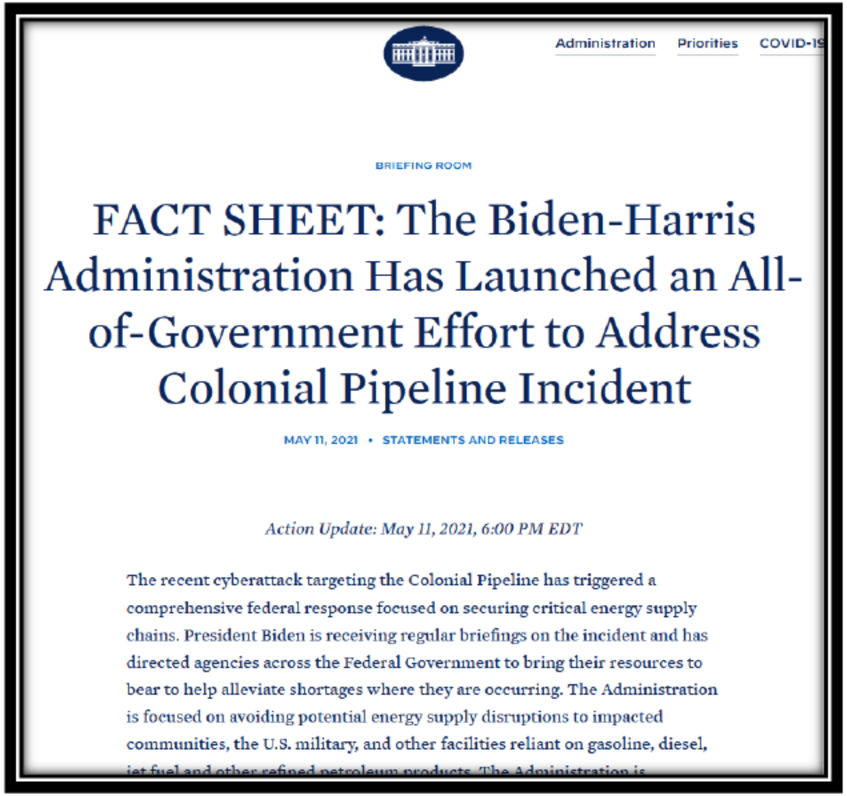
IT / OT Connections

OT Impacts

IR Planning

Q&A and Wild Speculation

Discussion on Lessons Learned



BRIEFING ROOM

FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident

MAY 11, 2021 • STATEMENTS AND RELEASES

Action Update: May 11, 2021, 6:00 PM EDT

The recent cyberattack targeting the Colonial Pipeline has triggered a comprehensive federal response focused on securing critical energy supply chains. President Biden is receiving regular briefings on the incident and has directed agencies across the Federal Government to bring their resources to bear to help alleviate shortages where they are occurring. The Administration is focused on avoiding potential energy supply disruptions to impacted communities, the U.S. military, and other facilities reliant on gasoline, diesel, jet fuel and other refined petroleum products. The Administration is

Federal, state, and multi sector response activities

- Interagency response group including nine different agencies
- EPA waiver for non- compliant fuel
- DOT hours of service waiver for those workers transporting fuel
- Governors expanded weight limits for tank trucks
- Considering alternate transport means via rail and maritime

Resources Referenced

CISA Alert
https://us-cert.cisa.gov/ncas/alerts/aa21-131a

Joint CISA-FBI Advisory
https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware

Wired Darkside Article
https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/

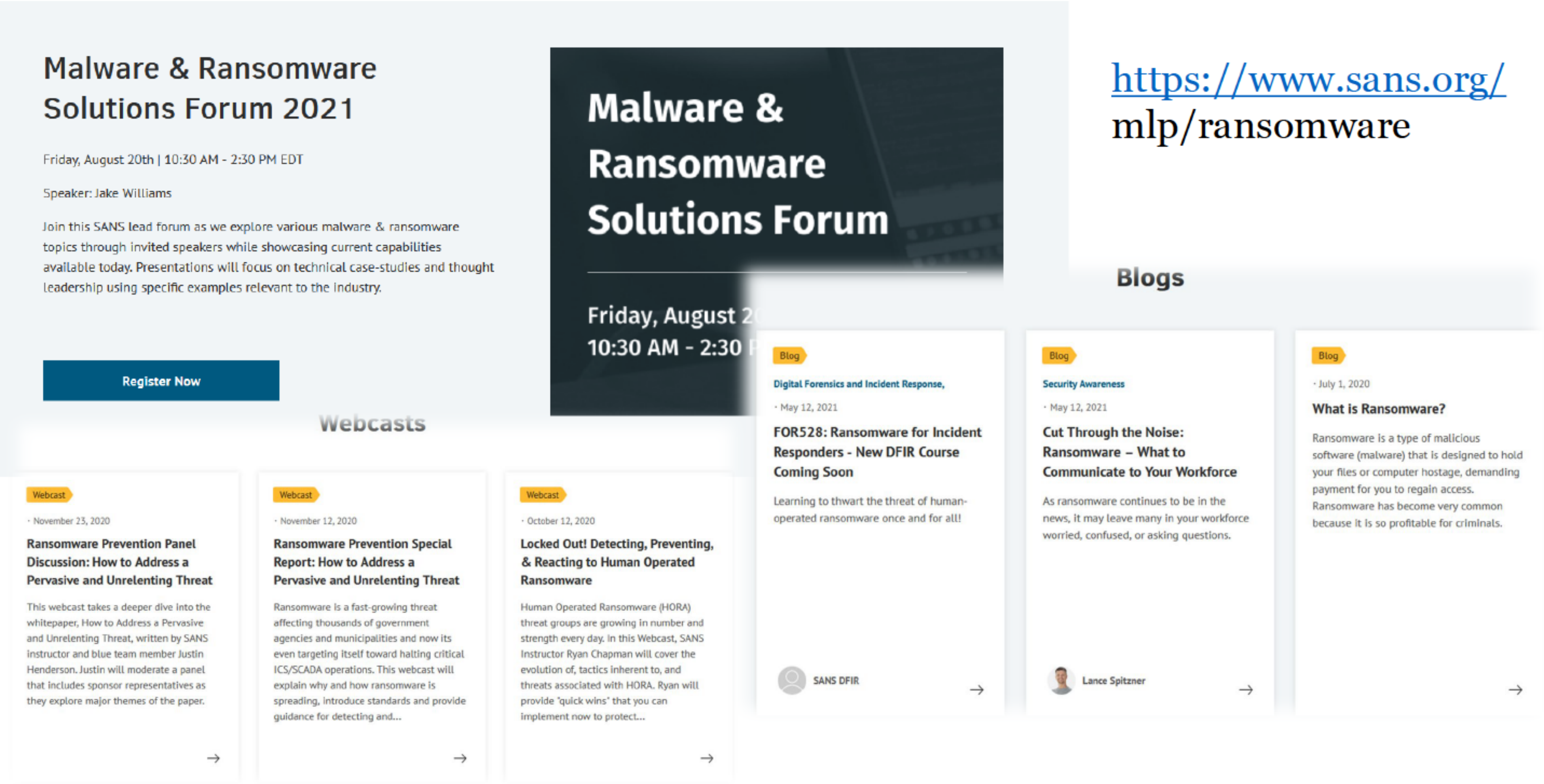
Krebs on security Darkside Article
https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

Fireeye Darkside blog
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

Colonial Pipeline Maps, outage details, and historical events
https://docplayer.net/15258707-Colonial-pipeline-company.html
https://www.colpipe.com/about-us/pipeline-operations-in-todays-world/digital-transformation
https://napipelines.com/colonial-restore-operations-harvey/

White House fact sheet
https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/

https://www.sans.org/mlp/ransomware



Malware & Ransomware Solutions Forum 2021

Friday, August 20th | 10:30 AM - 2:30 PM EDT

Speaker: Jake Williams

Join this SANS lead forum as we explore various malware & ransomware topics through invited speakers while showcasing current capabilities available today. Presentations will focus on technical case-studies and thought leadership using specific examples relevant to the industry.

Register Now

Malware & Ransomware Solutions Forum

Friday, August 2

10:30 AM - 2:30 P

Webcasts

Webcast

· November 23, 2020

Ransomware Prevention Panel Discussion: How to Address a Pervasive and Unrelenting Threat

This webcast takes a deeper dive into the whitepaper, How to Address a Pervasive and Unrelenting Threat, written by SANS instructor and blue team member Justin Henderson. Justin will moderate a panel that includes sponsor representatives as they explore major themes of the paper.

→

Webcast

· November 12, 2020

Ransomware Prevention Special Report: How to Address a Pervasive and Unrelenting Threat

Ransomware is a fast-growing threat affecting thousands of government agencies and municipalities and now its even targeting itself toward halting critical ICS/SCADA operations. This webcast will explain why and how ransomware is spreading, introduce standards and provide guidance for detecting and...

→

Webcast

· October 12, 2020

Locked Out! Detecting, Preventing, & Reacting to Human Operated Ransomware

Human Operated Ransomware (HORA) threat groups are growing in number and strength every day. In this Webcast, SANS Instructor Ryan Chapman will cover the evolution of, tactics inherent to, and threats associated with HORA. Ryan will provide "quick wins" that you can implement now to protect...

→

Blogs

Blog

Digital Forensics and Incident Response,

· May 12, 2021

FOR528: Ransomware for Incident Responders - New DFIR Course Coming Soon

Learning to thwart the threat of human-operated ransomware once and for all!

SANS DFIR →

Blog

Security Awareness

· May 12, 2021

Cut Through the Noise: Ransomware – What to Communicate to Your Workforce

As ransomware continues to be in the news, it may leave many in your workforce worried, confused, or asking questions.

Lance Spitzner →

Blog

· July 1, 2020

What is Ransomware?

Ransomware is a type of malicious software (malware) that is designed to hold your files or computer hostage, demanding payment for you to regain access. Ransomware has become very common because it is so profitable for criminals.

→

CONTACT INFORMATION

CONTACT
Tim Conway
tconway@sans.org

ICS RESOURCES
https://ics.sans.org
https://ics-community.sans.org/
Twitter: @sansics

CONTACT
Jeff Shearer
jshearer@sans.org

RANSOMWARE RESOURCES
https://www.sans.org/mlp/ransomware/