DRAGOS

HIDING IN PLAIN SIGHT

THE ASSET VISIBILITY CHALLENGE

MIKE HOFFMAN

Principal Industrial Consultant

@ICSSecurityGeek

linkedin.com/in/mjhoffman7

- 20 Years in O&G with roles in downstream, upstream sites, and global oversight positions
- Past titles have included: Principal ICS Security Engineer, Controls and Automation Specialist, Process/CEMS Analyzer Specialist, and Instrumentation & Electrical Technician
- Masters in Information Security Engineering from SANS Technology Institute, SANS instructor in development for the ICS612 course

GICSP *gold* · GRID *gold* · GCIP · GCIA · GSEC · GCCC · GCIH · GPYC · GPEN · GSTRT · CISSP · PMP · CCNA

DRAGOS

JOSH CARLSON

Sr. Business Development Manager

@mrjcarlson

linkedin.com/in/joshcarlsoncybersecurity

- 20+ years of diverse cybersecurity experience in engineering and business development roles within high tech companies supporting governments, global financial institutions, and customers in the various critical infrastructure sectors

- Representative in ISA Global Cybersecurity Alliance seeking to improve Industrial Control Systems safety and security through guidelines / standards adoption and implementation

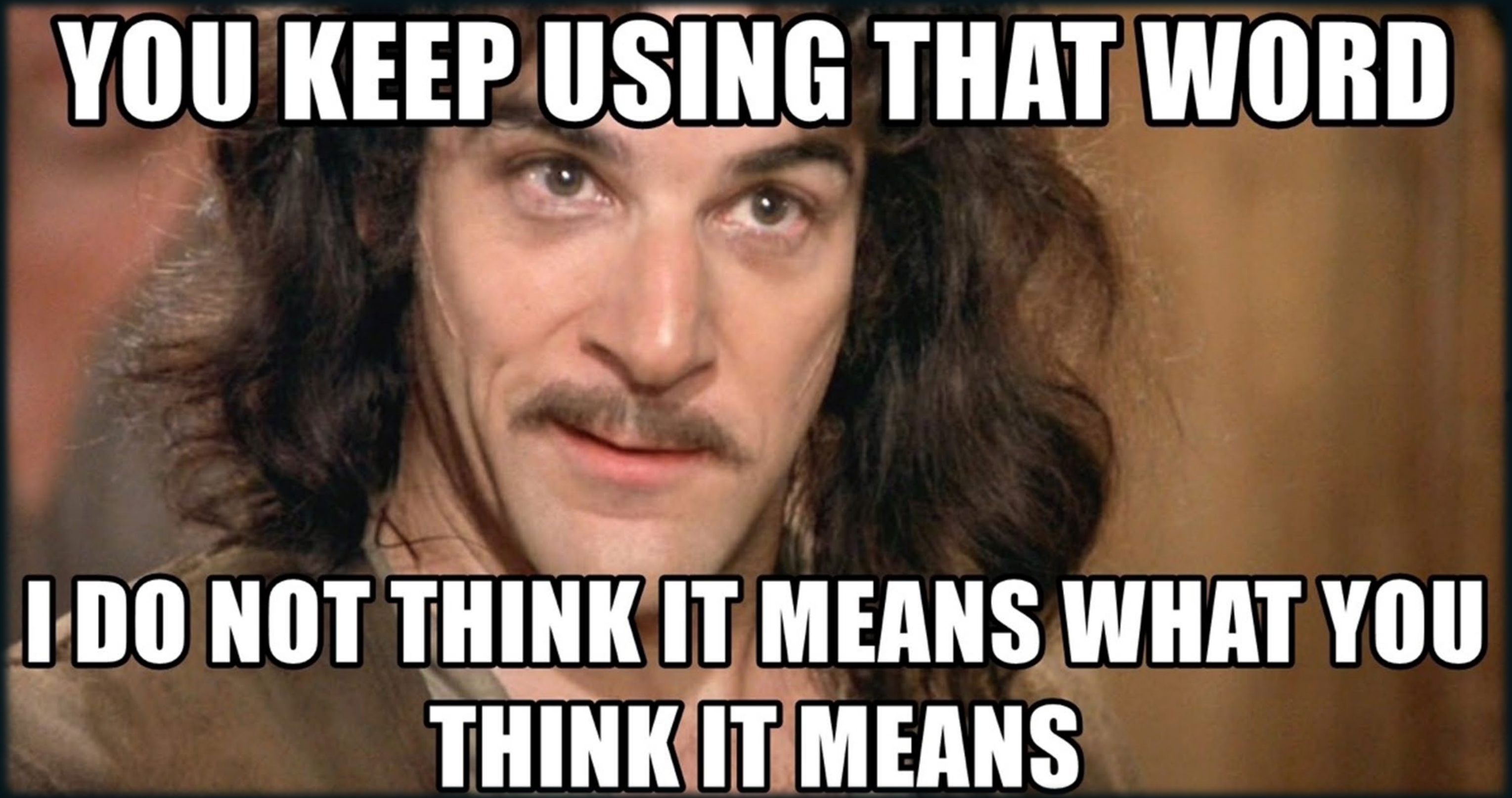
ISA GLOBAL CYBERSECURITY ALLIANCE

DRAGOS

SETTING THE STAGE

- A PROPER PERSPECTIVE OF ASSET VISIBILITY
- HOW ASSET VISIBILITY HELPS IN RISK MANAGEMENT
- WHERE DO I GO FROM HERE

WHAT IS "ASSET VISIBILITY"



WHAT IS AN "ASSET"

IT

OT

WHAT IS “VISIBILITY”

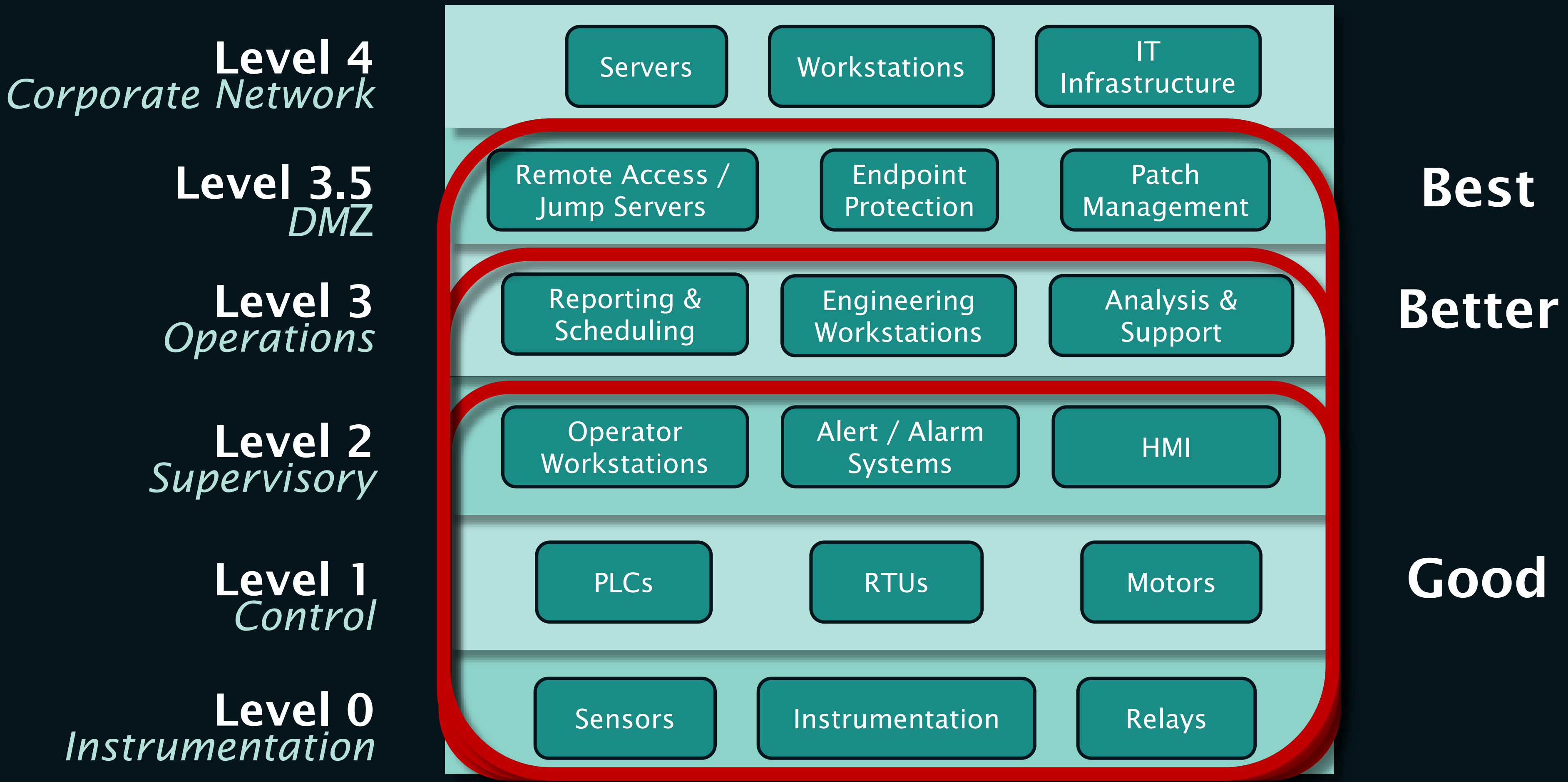
DEPENDS ON YOUR PERSPECTIVE…

Often static and lacking complete information

Goal is to have dynamic and near real-time data

ASSET VISIBILITY SCOPE

HOW MUCH DO I NEED?



Level 4 *Corporate Network*: Servers · Workstations · IT Infrastructure

Level 3.5 *DMZ*: Remote Access / Jump Servers · Endpoint Protection · Patch Management

Level 3 *Operations*: Reporting & Scheduling · Engineering Workstations · Analysis & Support

Level 2 *Supervisory*: Operator Workstations · Alert / Alarm Systems · HMI

Level 1 *Control*: PLCs · RTUs · Motors

Level 0 *Instrumentation*: Sensors · Instrumentation · Relays

Best

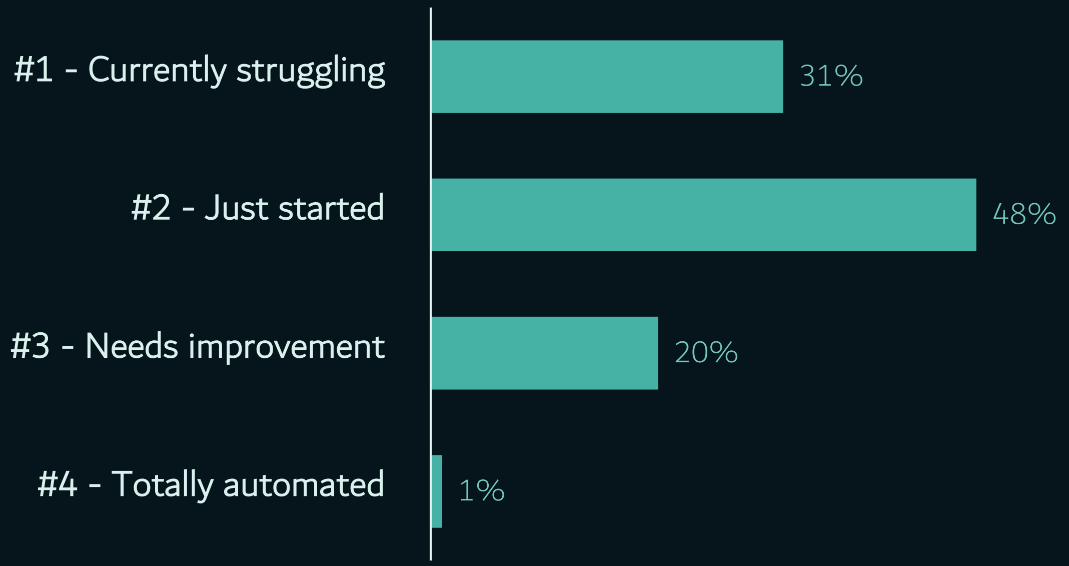
Better

Good

POLL

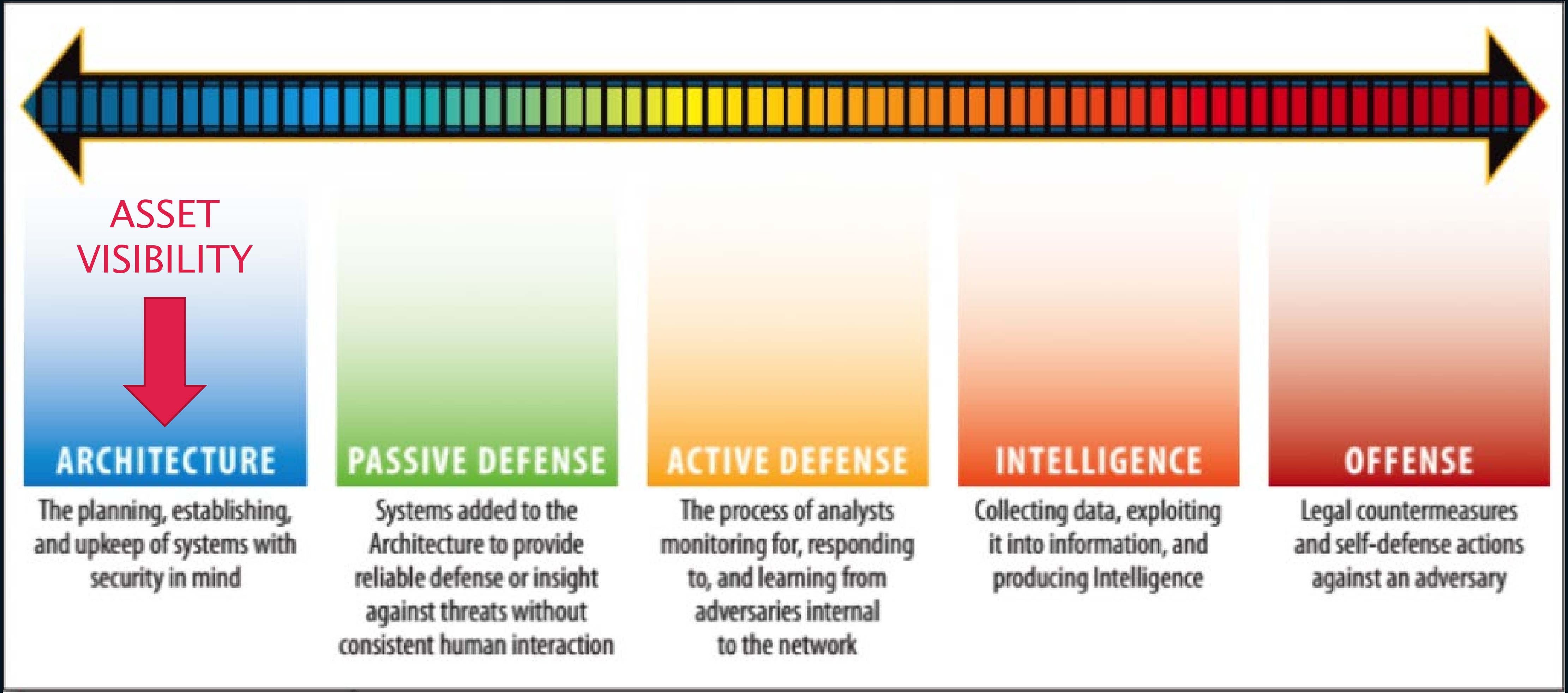
COMMUNITY FEEDBACK

How would you rate your current OT asset visibility?



ASSET VISIBILITY & RISK MANAGEMENT

SLIDING SCALE OF CYBER SECURITY



ASSET VISIBILITY

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

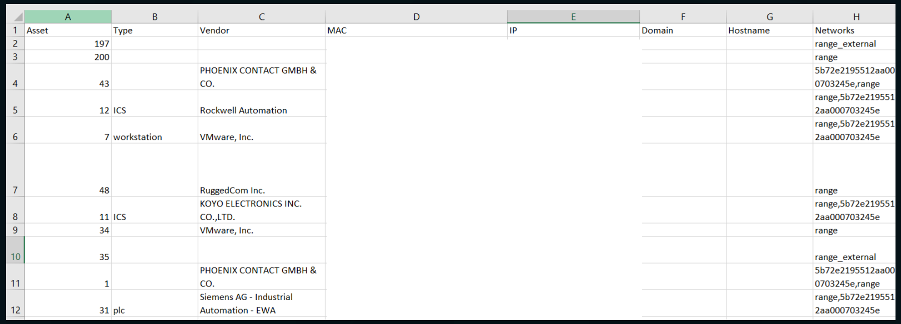
INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

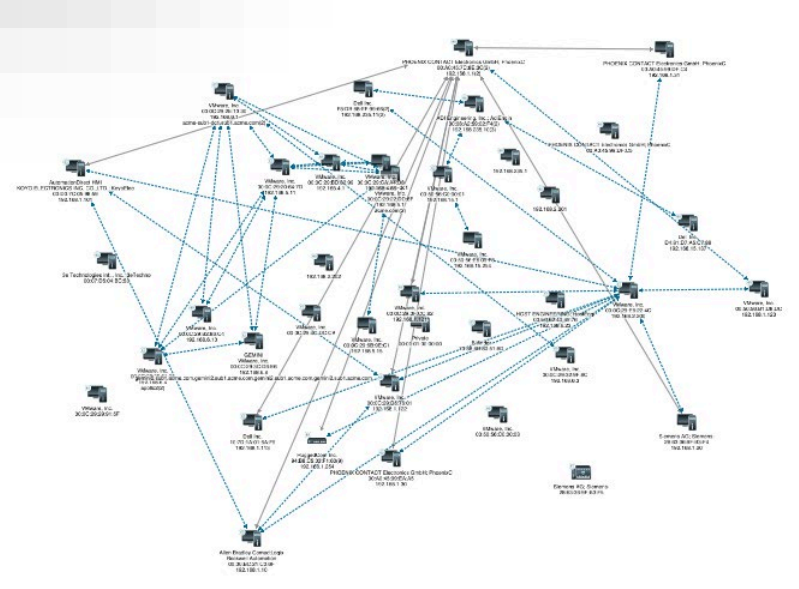
OFFENSE

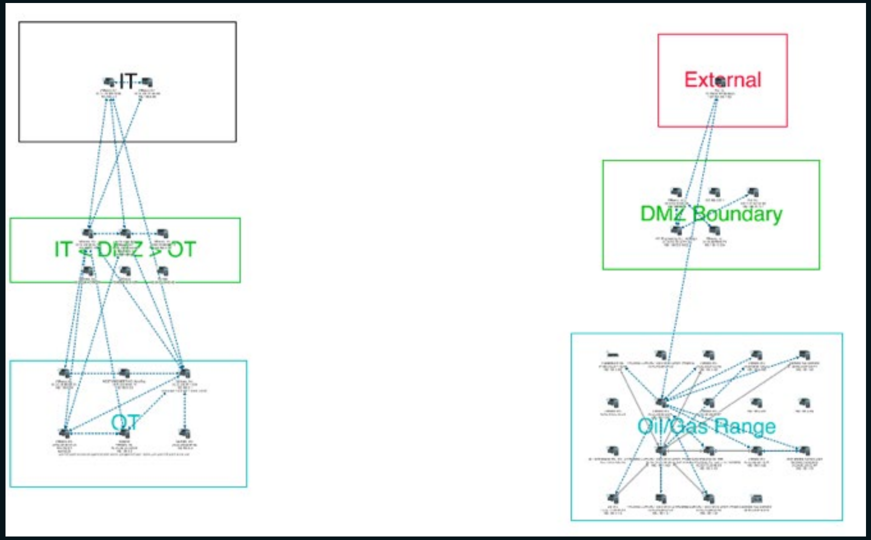
Legal countermeasures and self-defense actions against an adversary

WHY MATURE ASSET VISIBILITY?



	A	B	C	D	E	F	G	H
1	Asset	Type	Vendor	MAC	IP	Domain	Hostname	Networks
2	197							range_external
3	200							range
4	43		PHOENIX CONTACT GMBH & CO.					5b72e2195512aa000703245e,range
5	12	ICS	Rockwell Automation					range,5b72e2195512aa000703245e
6	7	workstation	VMware, Inc.					range,5b72e2195512aa000703245e
7	48		RuggedCom Inc.					range
8	11	ICS	KOYO ELECTRONICS INC. CO.,LTD.					range,5b72e2195512aa000703245e
9	34		VMware, Inc.					range
10	35							range_external
11	1		PHOENIX CONTACT GMBH & CO.					5b72e2195512aa000703245e,range
12	31	plc	Siemens AG - Industrial Automation - EWA					range,5b72e2195512aa000703245e





Understanding the environment is first for any workflow

STANDARDS AND REGULATIONS

REFERENCE INVENTORIES AS PRIMARY STARTING POINT

- ISA/IEC-62443
- NIST Cyber Security Framework
- SANS Top 20/CIS Critical Security Controls
- NERC CIP

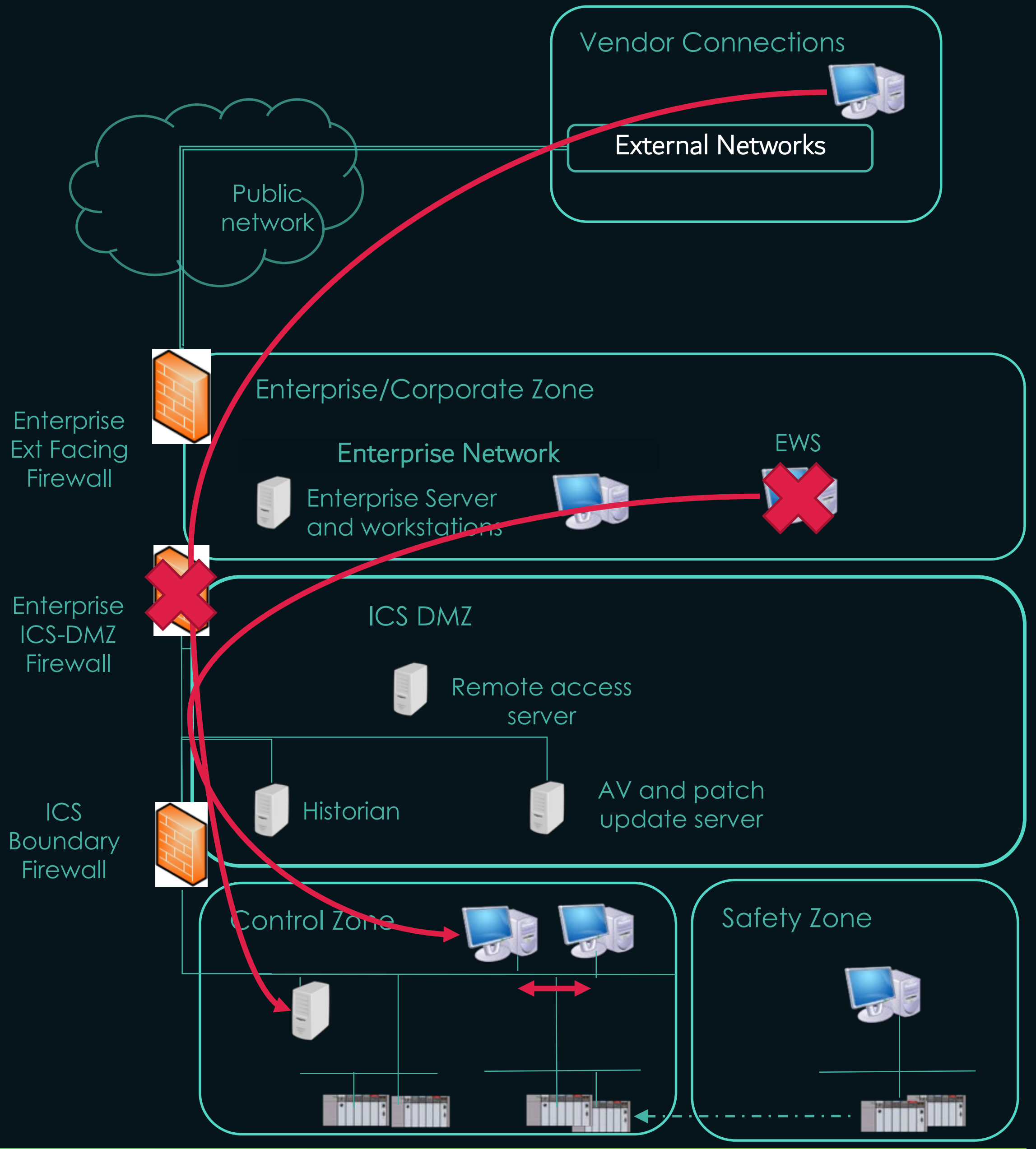
WHY EFFECTIVE ASSET VISIBILITY MATTERS?

SUPPORTS THE FOLLOWING EFFORTS

- Architecture Reviews
- Incident Response
- Crown Jewel Analysis
- Collection Management Framework
- Threat Hunting
- Vulnerability identification and remediation
- Life-Cycle Management (hardware and software)
- Hardening and security controls deployment
- SIEM detection and enrichment

VISIBILITY SUPPORTS FURTHER ANALYSIS

- Third-Party Remote Access
- ICS on Corporate Network
- Firewall with overly permissive ruleset
- Lack of ICS DMZ
- Horizontal Communication Between Zones



ONE OPTION ...*

FREE PASSIVE TOOLS

- Sophia
- NetworkMiner
- Wireshark
- Tshark
- TCPDump

* *Requires in-house expertise and OT “know-how”*

WHAT IS CONTAINED WITHIN ASSET VISIBILITY?

Automated Entries

- MAC address
- IP address(s)
- Firmware version
- Operating System
- Applications
- Ethernet/TCP/UDP ports, protocols in use
- Service Versions
- Communications with other systems, devices, networks

Manual Entries

- Backup Frequency
- Device Owner
- Location
- → Function
- → Network ID
- → Criticality level

THESE CAN BE AUTOMATED

IMPACT TO OPERATIONS

BE CAREFUL: TEST, TEST, AND TEST AGAIN

- Know thy tools! It’s important to be able to articulate how a tool functions to establish trust with operations
- It’s their shop, they run the show
- Respect the rules of engagement
- Only use active methods (NMAP, for example) on lab environments or low impact systems

COMPLEXITIES OF IDENTIFYING SYSTEMS

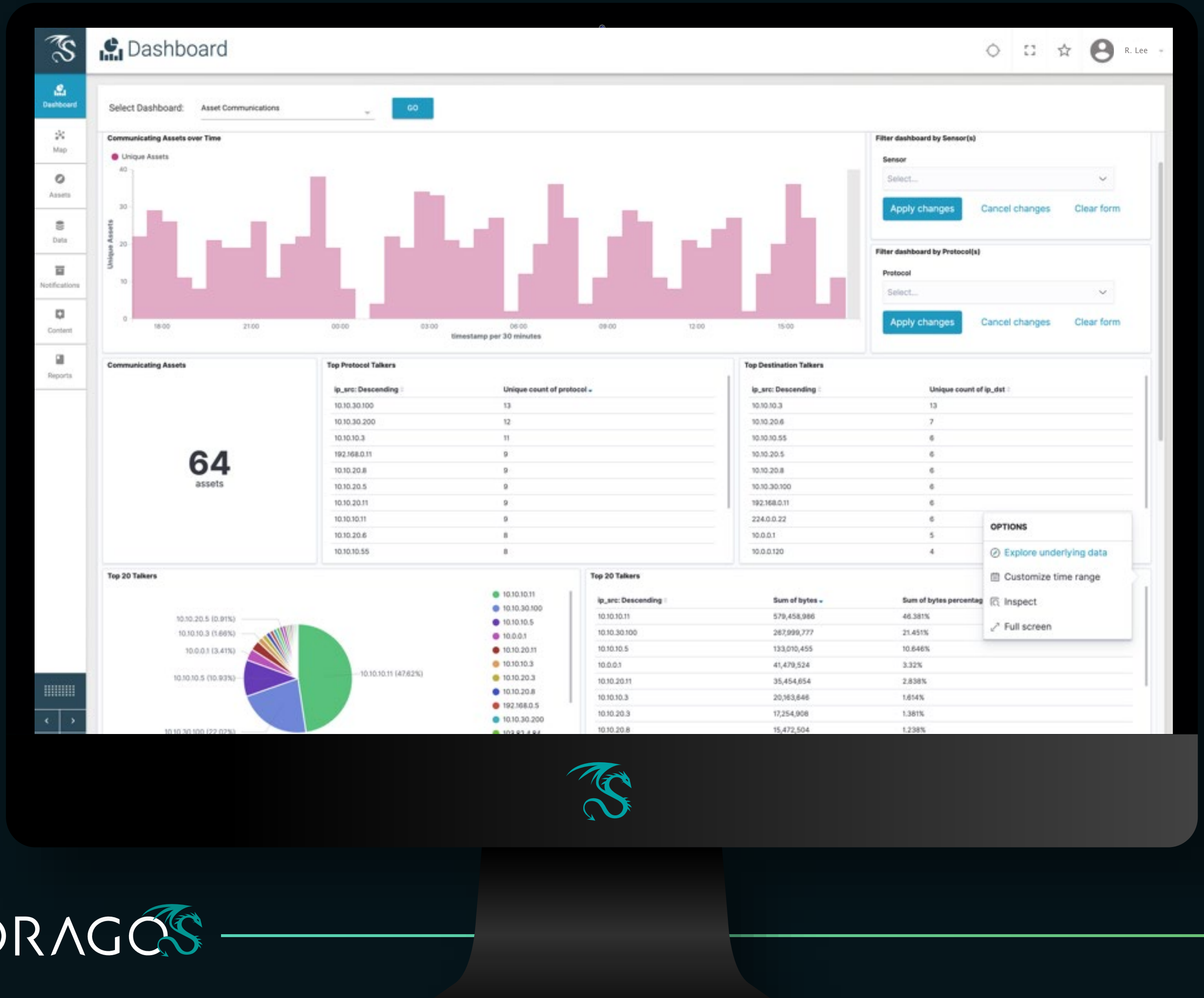
HOW DO YOU UNIQUELY IDENTIFY A DEVICE?

+ IP address / NAT / DHCP
+ Multiple networks
+ Redundant network paths
+ MAC address may change (VMs)
+ Infrequent OT device communications
+ Limited OT protocol dissectors

Image by Ernie Hayden

IMPORTANCE OF AUTOMATED ASSET VISIBILITY

YES, THE OT ENVIRONMENT DOES CHANGE!



Select Dashboard: Asset Communications

Communicating Assets

64
assets

Top Protocol Talkers

ip_src: Descending	Unique count of protocol
10.10.30.100	13
10.10.30.200	12
10.10.10.3	11
192.168.0.11	9
10.10.20.8	9
10.10.20.5	9
10.10.20.11	9
10.10.10.11	9
10.10.20.6	8
10.10.10.55	8

Top Destination Talkers

ip_src: Descending	Unique count of ip_dst
10.10.10.3	13
10.10.20.6	7
10.10.10.55	6
10.10.20.5	6
10.10.20.8	6
10.10.30.100	6
192.168.0.11	6
224.0.0.22	6
10.0.0.1	5
10.0.0.120	4

Top 20 Talkers

Top 20 Talkers

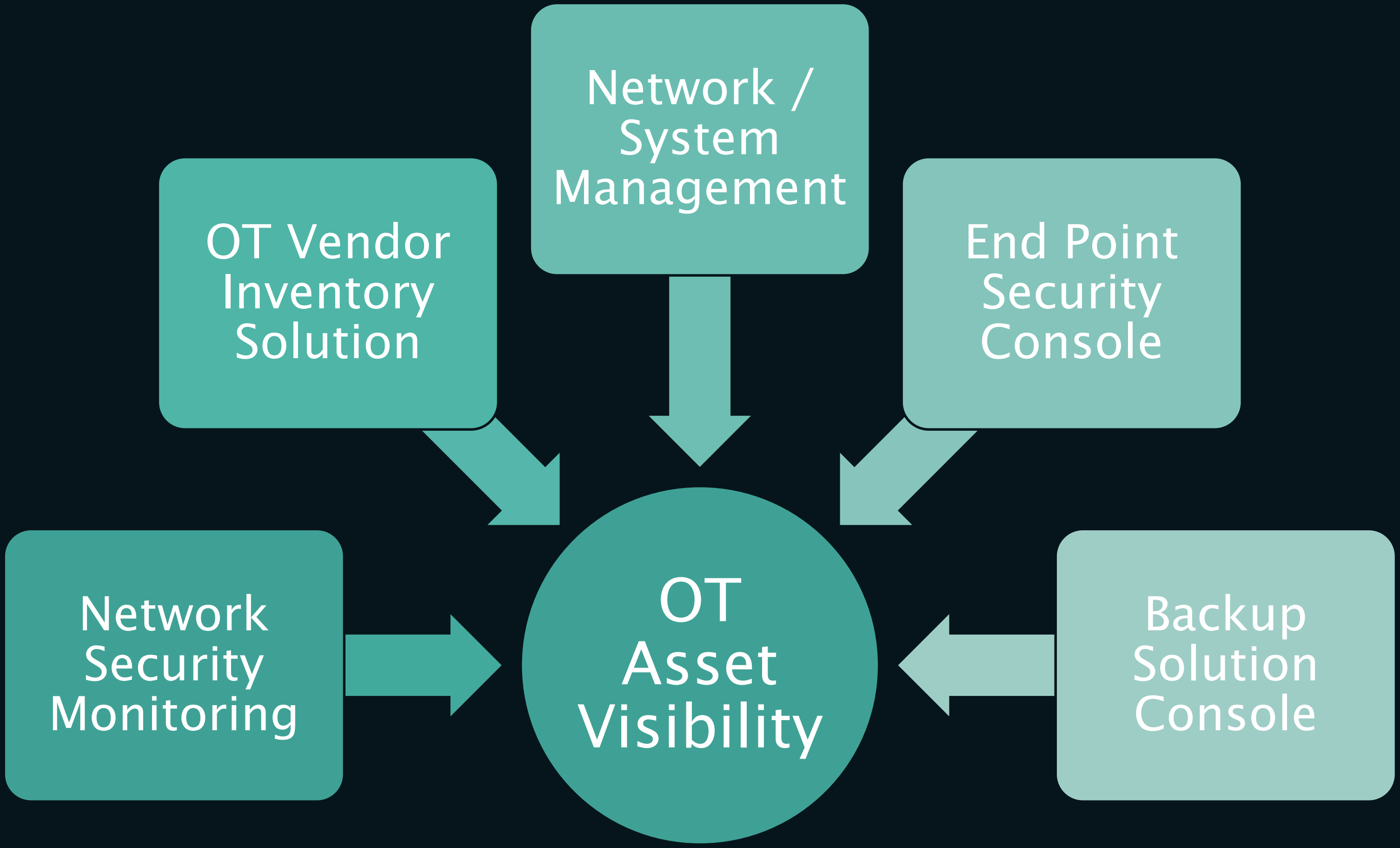
ip_src: Descending	Sum of bytes	Sum of bytes percentag
10.10.10.11	579,458,986	46.381%
10.10.30.100	267,999,777	21.451%
10.10.10.5	133,010,455	10.646%
10.0.0.1	41,479,524	3.32%
10.10.20.11	35,454,654	2.838%
10.10.10.3	20,163,646	1.614%
10.10.20.3	17,254,908	1.381%
10.10.20.8	15,472,504	1.238%

SYSTEM(S) AWARENESS

Small OT projects are always occurring. Spreadsheets, drawings, etc., become obsolete quickly and almost never resemble the "true state" of the environment.

AUTOMATED OT ASSET VISIBILITY

SOURCES? THEY ARE MANY!



Network / System Management

OT Vendor Inventory Solution

End Point Security Console

Network Security Monitoring

OT Asset Visibility

Backup Solution Console

WHERE TO GO FROM HERE

PIVOT PATH ANALYSIS

AN ATTACKER'S PERSPECTIVE

Identify Assets

- Passive analysis to identify assets in use
- Record ports and protocols as well

Identify Topologies

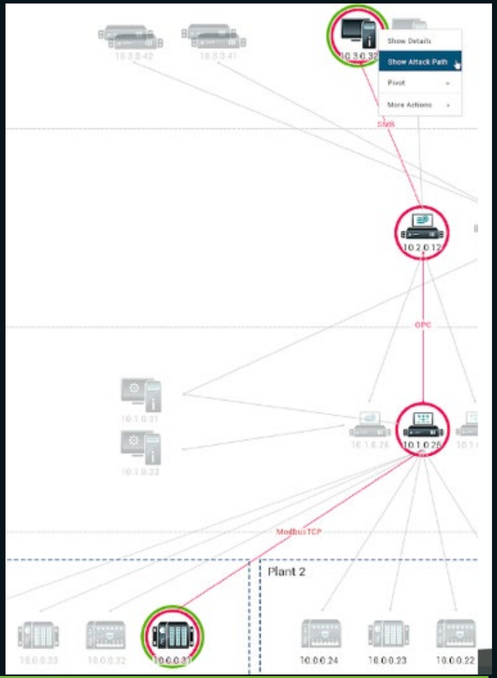
- Visually map out the interconnections between assets
- Record the protocols on the links between

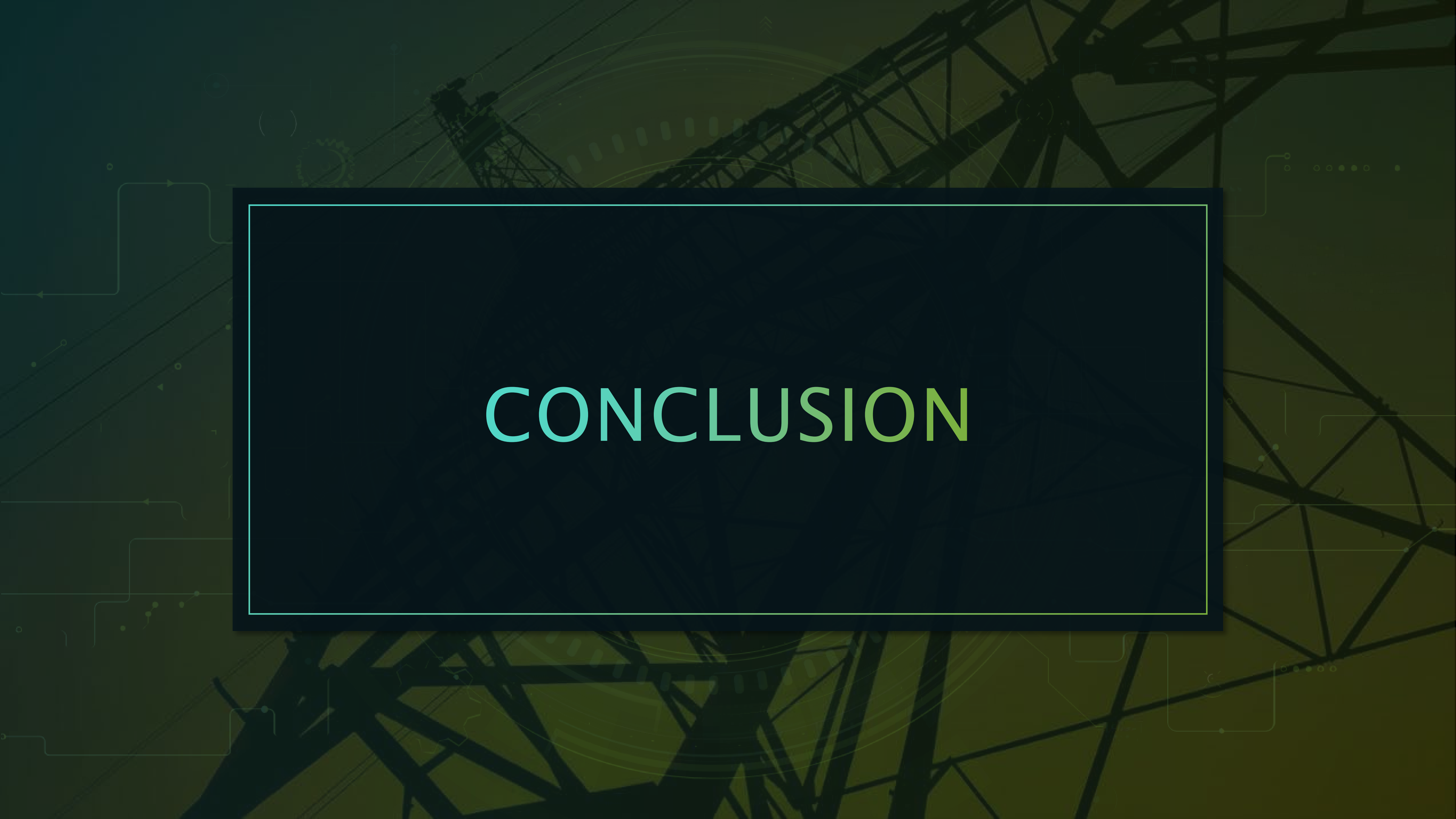
Identify Pivot Points

- Determine shortest routes possible between assets
- Determine any routes on key assets

Modify Passive Defenses

- Tailor collection for detection
- Tune network segmentation as needed





CONCLUSION

KEY TAKEAWAYS

- Why having a proper perspective of asset visibility is important

- Ways that asset visibility will help in your risk management efforts

- Some future milestones after you are satisfied with your level of asset visibility

ASSET VISIBILITY WEBINAR SERIES

February 25th – Focus on what matters

- The Collection Management Framework – taxes before axes!
- Crown Jewel Analysis – there's gold in them there zones!

Late March – A look ahead

- Tying it all together with the Dragos Platform (v1.7)
- Connection between:
  - Asset Visibility
  - Baselines
  - Threat Detection

THANK YOU

DRAGOS

dragos.com/resources