DRAGOS

SOLIDIFYING ASSET VISIBILITY IN YOUR ENVIRONMENT

2nd in our 3-part series

MIKE HOFFMAN

Principal Industrial Consultant

@ICSSecurityGeek

linkedin.com/in/mjhoffman7

- 20 Years in O&G with roles in downstream, upstream, and global technical leadership
- 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

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

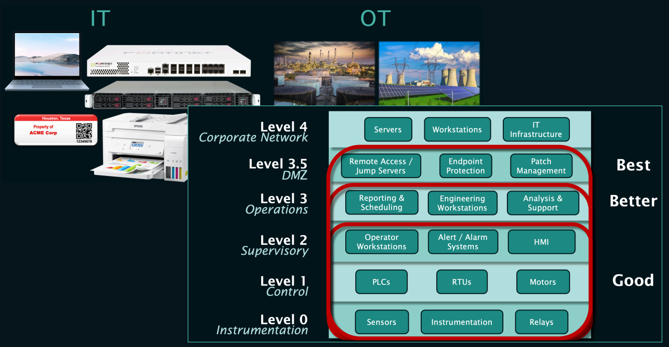
- Representative in ISA Global Cybersecurity Alliance seeking to improve Industrial Control Systems safety and security through guidelines / standards adoption and implementation

ISA GLOBAL CYBERSECURITY ALLIANCE

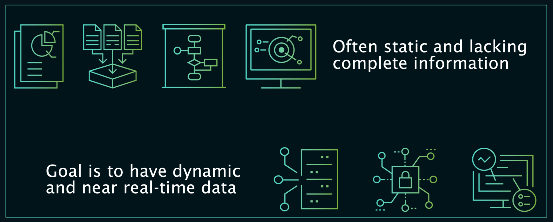
WEBINAR #1 RECAP

In case you missed it…

- What actually is ”Asset Visibility”



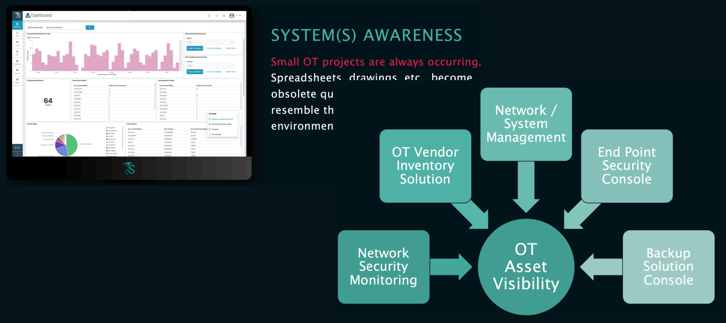
- Why having a proper perspective is important



Often static and lacking complete information

Goal is to have dynamic and near real-time data

- Ways that Asset Visibility helps in Risk Management efforts



SYSTEM(S) AWARENESS

Small OT projects are always occurring.

Spreadsheets, drawings, etc., become
obsolete qu
resemble th
environmen

Dashboard
64
Network / System Management
OT Vendor Inventory Solution
End Point Security Console
Network Security Monitoring
OT Asset Visibility
Backup Solution Console

SETTING THE STAGE

- What’s In It For You – Applying This To Your Role
- Crown Jewel Analysis (CJA) – *There’s Gold In Them Their Zones!*
- The Collection Management Framework (CMF) – *Taxes Before Axes!*

POLL

COMMUNITY FEEDBACK

What is your role?

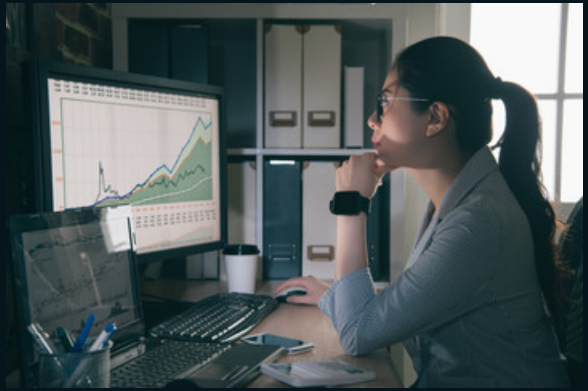
- Operations
- Security
- Management
- Consultant
- Jedi Master

ASSET VISIBILITY IMPORTANCE – ROLE

Direct / Daily

Indirect

OPERATIONS
Controls Engineer
(OT)



SECURITY
Security Analyst
(IT and/or OT)

MANAGEMENT
Plant / Site Manager
(IT and/or OT)

LEADERSHIP
C-Suite and Board
(IT & OT)

WHY EFFECTIVE ASSET VISIBILITY MATTERS?

OPERATIONS – CONTROL ENGINEERS

Primarily responsible for the safe and reliable operation of an ICS environment

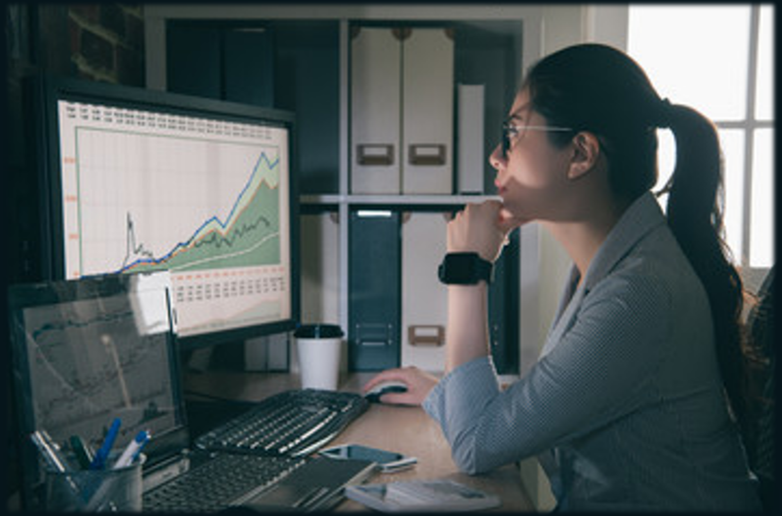
- Supports the need to understand how the ICS components are communicating
- Trust but verify third party access & modification
- Security controls deployment & monitoring
- Provide relevant vulnerability identification and potential impact

WHY EFFECTIVE ASSET VISIBILITY MATTERS?

SECURITY ANALYSTS

Primarily responsible for the security of the ICS environment

- Supports IT/OT staff on security elements within the ICS components
- Analyzes intel reports on threats targeting ICS environments
- Effective leverage for detection notifications
- Participate in assessments and incident response



WHY EFFECTIVE ASSET VISIBILITY MATTERS?

MANAGEMENT – PLANT / SITE

Primarily responsible for overall safe and efficient operation of the entire plant / site

- Requires prompt access to information about the ICS environment
- Supports intel report analysis
- Life-Cycle Management (hardware and software)
- Reports risk elements to leadership
- Participate in assessments and incident response

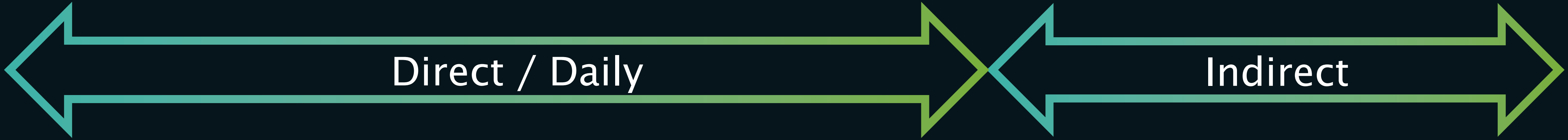
WHY EFFECTIVE ASSET VISIBILITY MATTERS?

LEADERSHIP – C-SUITE & BOARD

Primarily responsible for the overall business supported by ICS environment(s)

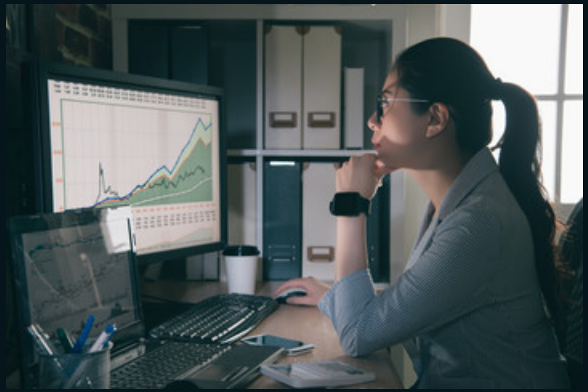
- Require prompt access to information about the ICS environment
- Provide access to additional resources as necessary
- Reports risk elements to share holders / regulators
- Participate in incident response

ASSET VISIBILITY IMPORTANCE – ROLE



Direct / Daily

Indirect



OPERATIONS
Controls Engineer
(OT)

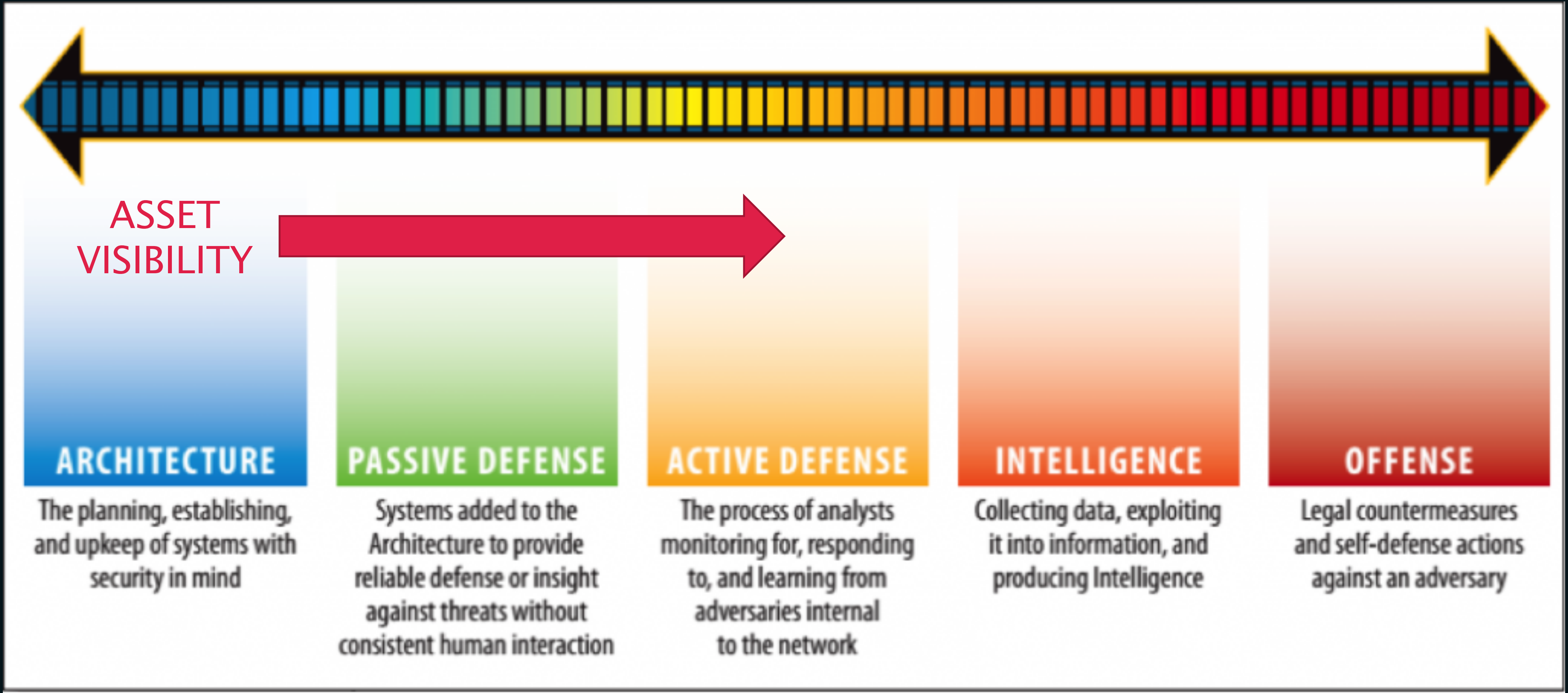
SECURITY
Security Analyst
(IT and/or OT)

MANAGEMENT
Plant / Site Manager
(IT and/or OT)

LEADERSHIP
C-Suite and Board
(IT & OT)

ASSET VISIBILITY & CROWN JEWEL ANALYSIS

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

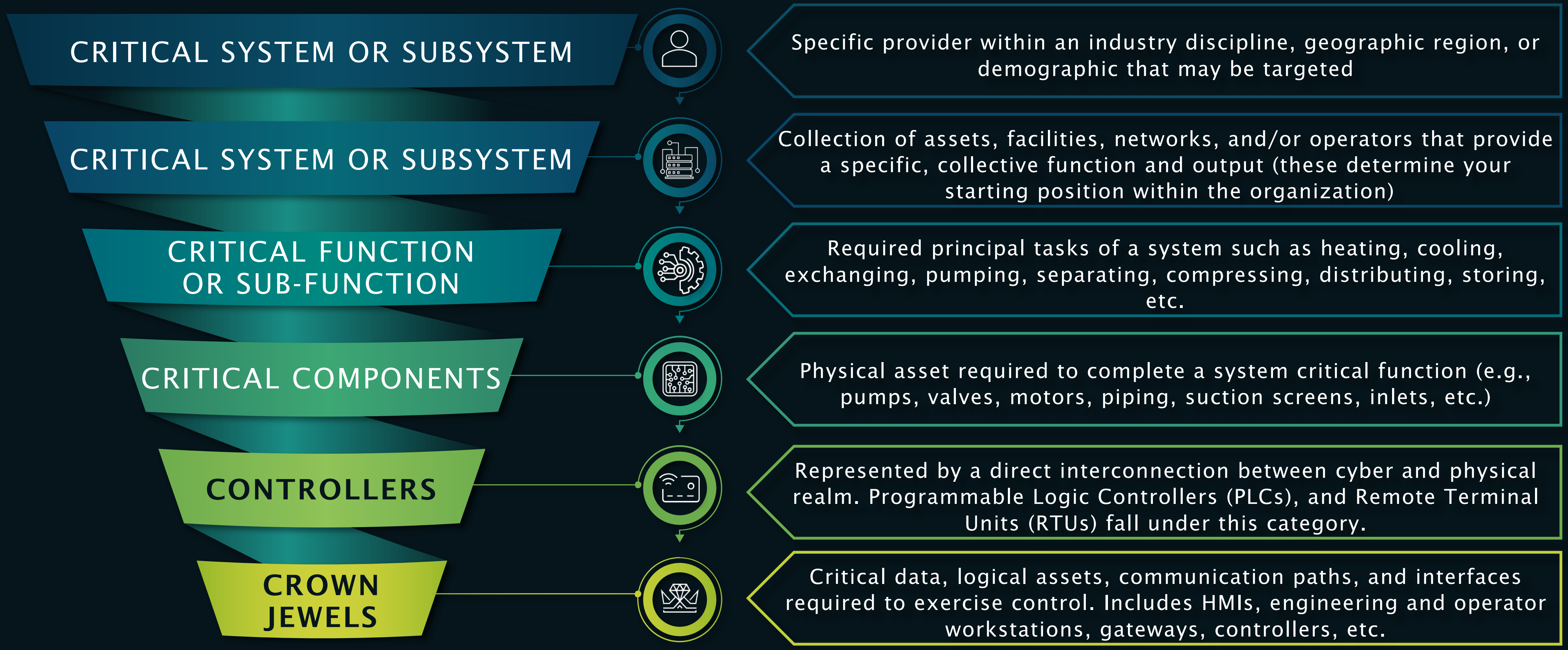
CROWN JEWEL ANALYSIS

UNDERSTANDING WHAT REALLY MATTERS

- Not all ICS devices and systems are the same
- Each may have different levels of criticality based on process impact
- Higher levels of criticality require additional security countermeasures
- Going through the CJA processes requires a multidiscipline team
- Results in identifying key systems and components that need enhanced prevention, detection, and recovery capabilities

CROWN JEWEL ANALYSIS

OVERVIEW OF THE PROCESS



CRITICAL SYSTEM OR SUBSYSTEM

Specific provider within an industry discipline, geographic region, or demographic that may be targeted

CRITICAL SYSTEM OR SUBSYSTEM

Collection of assets, facilities, networks, and/or operators that provide a specific, collective function and output (these determine your starting position within the organization)

CRITICAL FUNCTION OR SUB-FUNCTION

Required principal tasks of a system such as heating, cooling, exchanging, pumping, separating, compressing, distributing, storing, etc.

CRITICAL COMPONENTS

Physical asset required to complete a system critical function (e.g., pumps, valves, motors, piping, suction screens, inlets, etc.)

CONTROLLERS

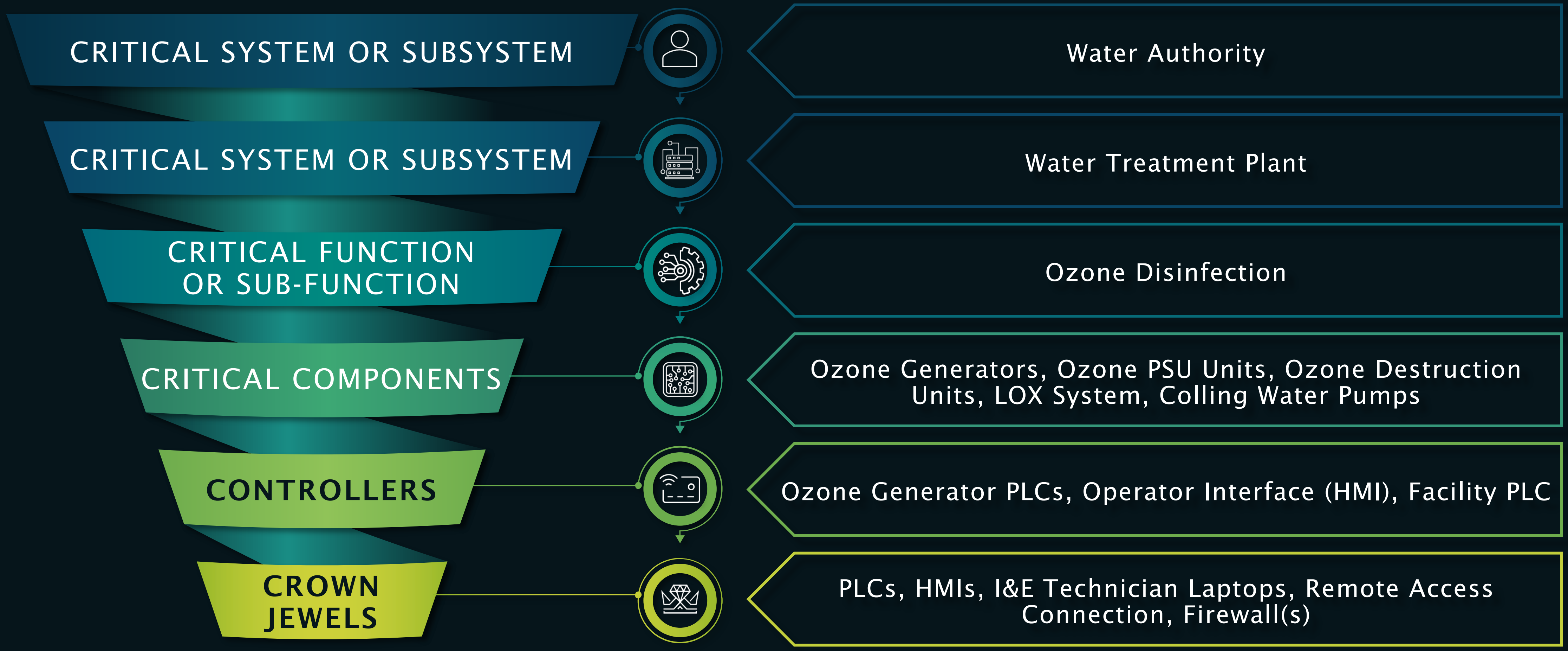
Represented by a direct interconnection between cyber and physical realm. Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) fall under this category.

CROWN JEWELS

Critical data, logical assets, communication paths, and interfaces required to exercise control. Includes HMIs, engineering and operator workstations, gateways, controllers, etc.

CROWN JEWEL ANALYSIS

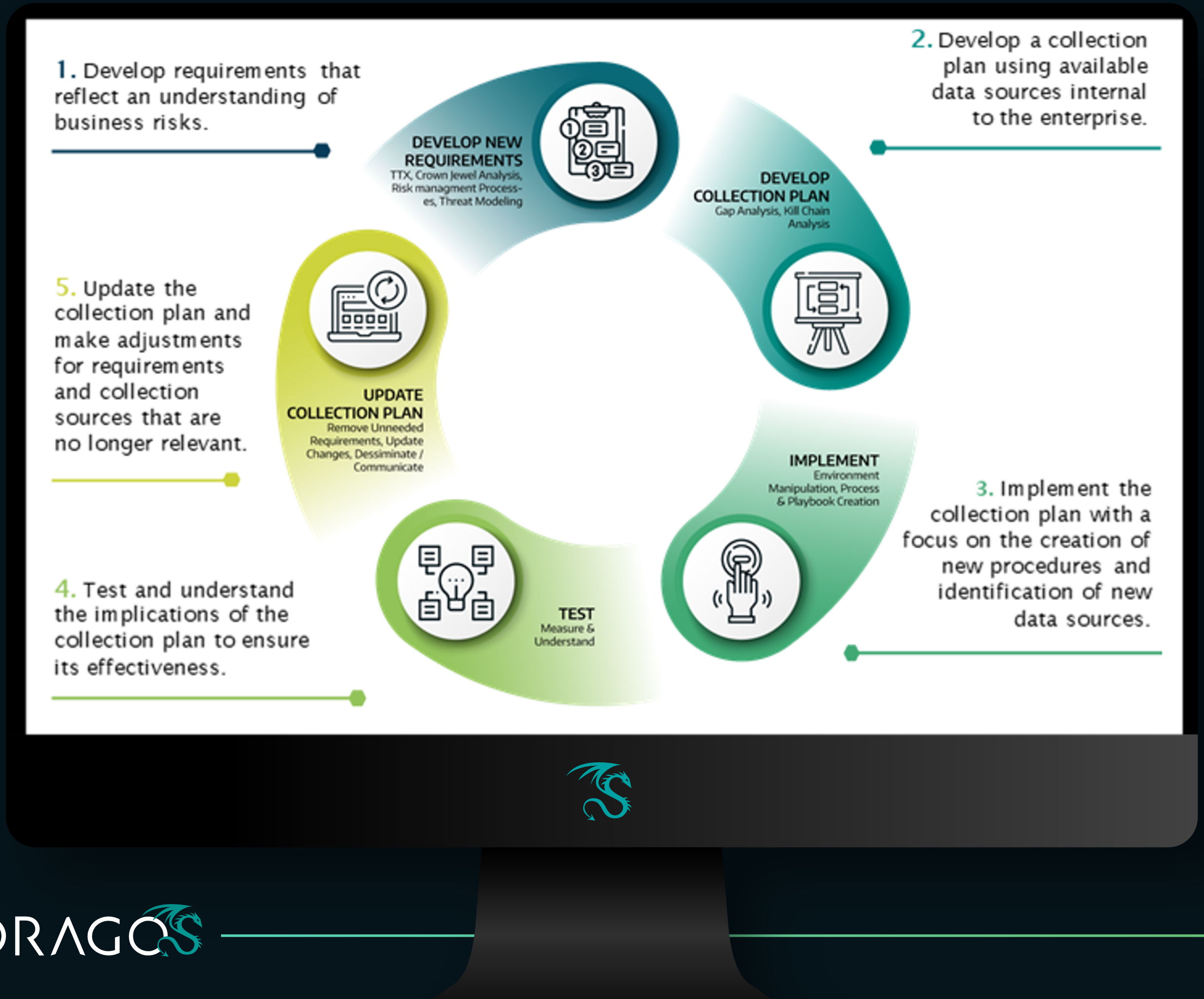
ASSET VISIBILITY IS REQUIRED FOR CJA



CRITICAL SYSTEM OR SUBSYSTEM	Water Authority
CRITICAL SYSTEM OR SUBSYSTEM	Water Treatment Plant
CRITICAL FUNCTION OR SUB-FUNCTION	Ozone Disinfection
CRITICAL COMPONENTS	Ozone Generators, Ozone PSU Units, Ozone Destruction Units, LOX System, Colling Water Pumps
CONTROLLERS	Ozone Generator PLCs, Operator Interface (HMI), Facility PLC
CROWN JEWELS	PLCs, HMIs, I&E Technician Laptops, Remote Access Connection, Firewall(s)

COLLECTION MANAGEMENT FRAMEWORK

BUILDING YOUR VISIBILITY STRATEGY



1. Develop requirements that reflect an understanding of business risks.

2. Develop a collection plan using available data sources internal to the enterprise.

3. Implement the collection plan with a focus on the creation of new procedures and identification of new data sources.

4. Test and understand the implications of the collection plan to ensure its effectiveness.

5. Update the collection plan and make adjustments for requirements and collection sources that are no longer relevant.

DEVELOP NEW REQUIREMENTS
TTX, Crown Jewel Analysis, Risk managment Process-es, Threat Modeling
DEVELOP COLLECTION PLAN
Gap Analysis, Kill Chain Analysis
IMPLEMENT
Environment Manipulation, Process & Playbook Creation
TEST
Measure & Understand
UPDATE COLLECTION PLAN
Remove Unneeded Requirements, Update Changes, Dessiminate / Communicate

QUESTIONS

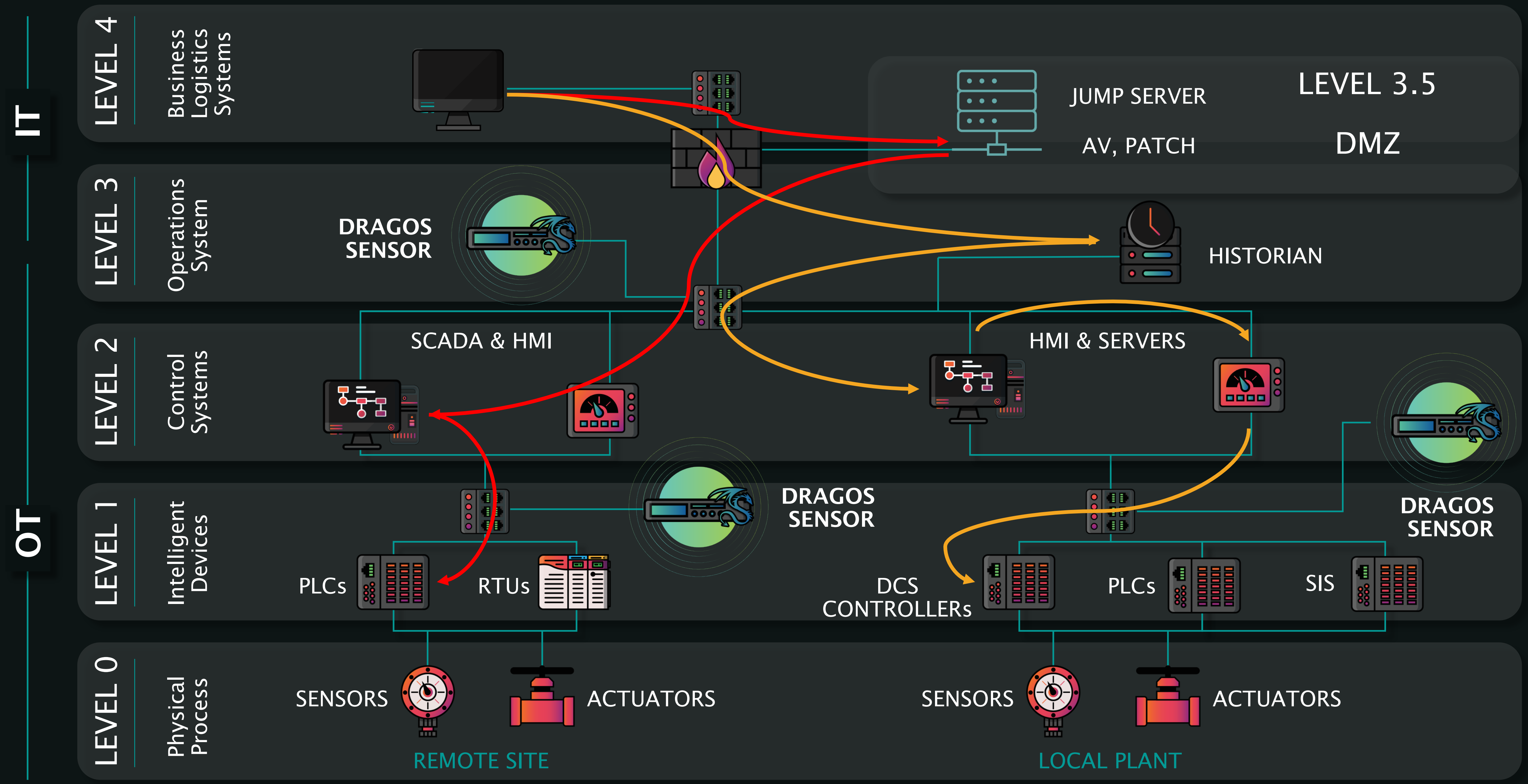
- Are the Crown Jewels properly monitored?
- Am I logging the right settings/levels?
- How long are the logs stored?
- Can I detect both network and device level activity?

COLLECTION MANAGEMENT FRAMEWORK

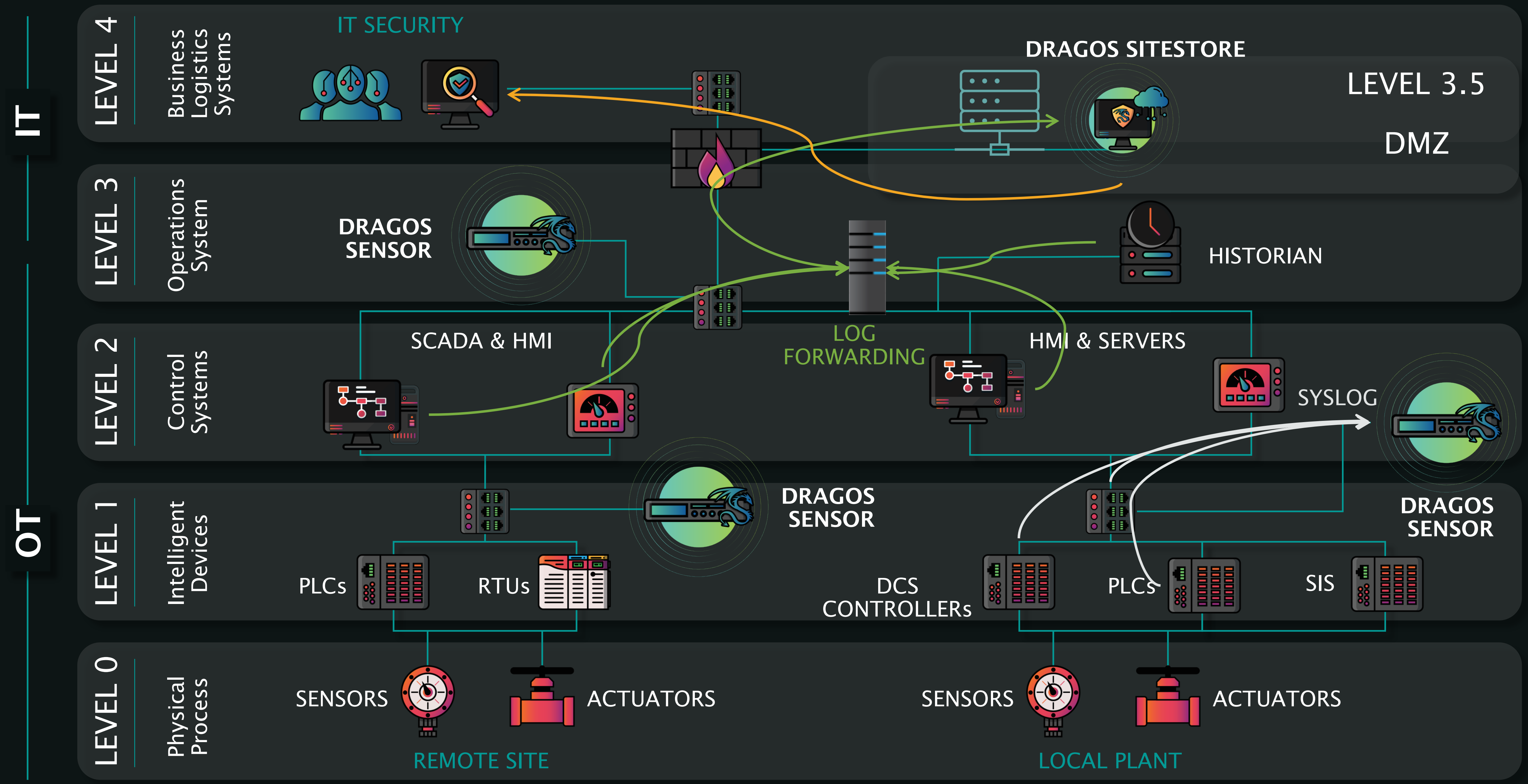
AS CONFIGURED

Site	Segment / Level	Asset	Data Type	Kill Chain Phases	Data Storage Location	Data Retention	Follow-On Collection
Plant A	DMZ	VPN Concentrator	Access Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	2 Years	Local Firewall Logs
Plant A	DMZ	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	180 Days	Firewall Ruleset
Plant A	DMZ	Jump Host	Windows Event Logs	Reconnaissance, Command and Control, Delivery	Enterprise Log Server	1 Year	Registry
Plant A	Supervisory Network	EWS	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	30 Days	Registry, Memory, MFT
Plant A	Supervisory Network	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	Local Host	15 Days	Historian Logs, Registry
Plant A	Control Network	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	Local Host	7 Days	Firewall Ruleset
Plant A	Control Network	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	7 Days	Registry, Memory, MFT
Plant A	Control Network	PLCs	Internal Logging	Installation, Actions, on Objectives	Local Host	7 Days	Controller Logic

ASSET VISIBILITY – ATTACK PATHS



ASSET VISIBILITY - LOGGING



COLLECTION MANAGEMENT FRAMEWORK

VISIBILITY STRATEGY

Site	Segment / Level	Asset	Data Type	Kill Chain Phases	Data Storage Location	Data Retention	Follow-On Collection
Plant A	DMZ	VPN Concentrator	Access Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	2 Years	Local Firewall Logs
Plant A	DMZ	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	180 Days	Firewall Ruleset
Plant A	DMZ	Jump Host	Windows Event Logs	Reconnaissance, Command and Control, Delivery	Enterprise Log Server	1 Year	Registry
Plant A	DMZ	Dragos Site Store	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	IT/OT SIEM	180 Days	Ruleset
Plant A	Supervisory Network	EWS	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	IT/OT SIEM	180 Days	Registry, Memory, MFT
Plant A	Supervisory Network	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	IT/OT SIEM	180 Days	Historian Logs, Registry
Plant A	Control Network	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	IT/OT SIEM	180 Days	Firewall Ruleset
Plant A	Control Network	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	IT/OT SIEM	180 Days	Registry, Memory, MFT
Plant A	Control Network	PLCs	Internal Logging	Installation, Actions, on Objectives	IT/OT SIEM	180 Days	Controller Logic

90 Days, Good | 180 Days, Better | 360 Days, Best

RESOURCES

DRAGOS WHITEPAPERS

Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping

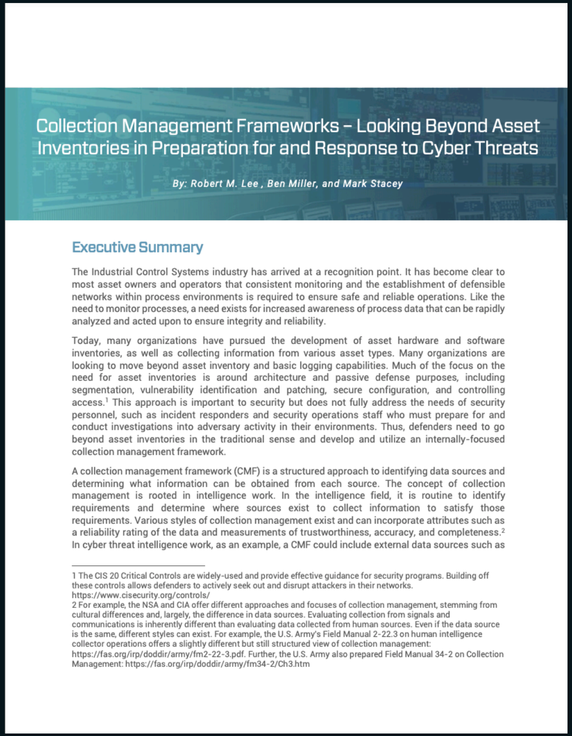
Abstract

The advent of communication networks within industrial environments has proven to effectively compress decision cycles, increase productivity, and has freed organizations of many resource constraints and increased safety and reliability of operations. The reliance of real-time operational data to drive business decisions has led to significantly increased physical asset connectivity within industrial environments. Over the last 20 years, this increase has opened the way for attackers to potentially compromise process functions through the very communication networks that are depended upon for control and safety. This fact has motivated security professionals to develop a plethora of security assessment frameworks, including frameworks specifically designed to identify vulnerabilities and mitigate the risk of cyber attacks within industrial control systems (ICS).

However, no single assessment framework allows industrial asset owners to scope and prioritize the most critical network assets and processes with their associated network dependencies--the failure of which would result in a loss of the ability to operate. This paper will introduce an easily applied and repeatable scoping model that will help security analysts identify starting points for cyber threat hunts, incident response planning, penetration/vulnerability assessments, and cyber security strategies for ICS environments. This is done through merging traditional IT risk methodologies with historically-proven engineering and process risk methodologies by aligning network assets to known risk metrics within operational environments. We describe this scoping model by laying out a foundational analytic framework that starts with system and functional analysis and leverages completed Process Hazard Analysis (PHA), Piping and Instrumentation Diagram (P&ID) reviews, and their associated control strategies within the industrial environment. We use the results of these analyses to steer and identify control network dependency of critical processes to systematically determine crown jewels, as would be determined by an attacker to affect system functions.

The analytic results involved within this model allow a security analyst to work from the starting point of identified risks to processes. Cyber attackers often assess the feasibility of affecting system functions in a similar fashion. Therefore, a key assumption must be made up front in this analytic process. The position of the highest impact to a system's functional output, which can be defined as the organization's bottom line, should be assumed when trying to determine the most impactful risk of a cyber-attack.

©2019 Dragos, Inc. All rights reserved. [Protected] Non-confidential content. January 2019



Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats

By: Robert M. Lee , Ben Miller, and Mark Stacey

Executive Summary

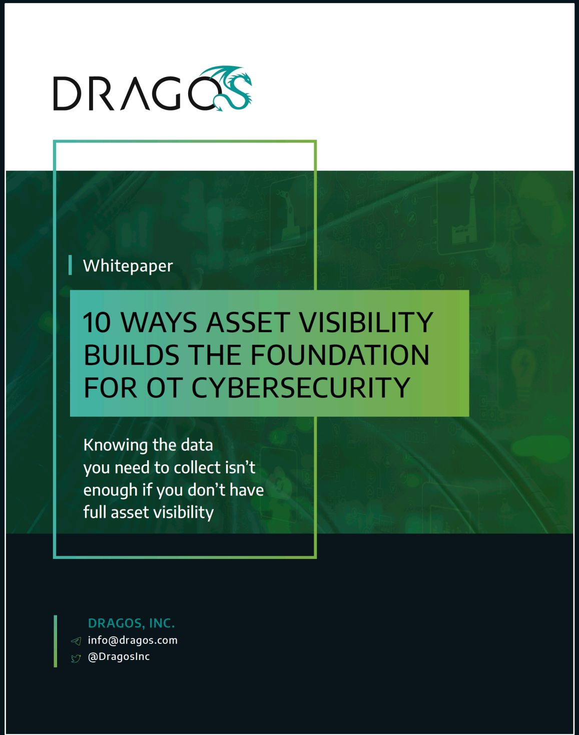
The Industrial Control Systems industry has arrived at a recognition point. It has become clear to most asset owners and operators that consistent monitoring and the establishment of defensible networks within process environments is required to ensure safe and reliable operations. Like the need to monitor processes, a need exists for increased awareness of process data that can be rapidly analyzed and acted upon to ensure integrity and reliability.

Today, many organizations have pursued the development of asset hardware and software inventories, as well as collecting information from various asset types. Many organizations are looking to move beyond asset inventory and basic logging capabilities. Much of the focus on the need for asset inventories is around architecture and passive defense purposes, including segmentation, vulnerability identification and patching, secure configuration, and controlling access.[1] This approach is important to security but does not fully address the needs of security personnel, such as incident responders and security operations staff who must prepare for and conduct investigations into adversary activity in their environments. Thus, defenders need to go beyond asset inventories in the traditional sense and develop and utilize an internally-focused collection management framework.

A collection management framework (CMF) is a structured approach to identifying data sources and determining what information can be obtained from each source. The concept of collection management is rooted in intelligence work. In the intelligence field, it is routine to identify requirements and determine where sources exist to collect information to satisfy those requirements. Various styles of collection management exist and can incorporate attributes such as a reliability rating of the data and measurements of trustworthiness, accuracy, and completeness.[2] In cyber threat intelligence work, as an example, a CMF could include external data sources such as

[1] The CIS 20 Critical Controls are widely-used and provide effective guidance for security programs. Building off these controls allows defenders to actively seek out and disrupt attackers in their networks. https://www.cisecurity.org/controls/

[2] For example, the NSA and CIA offer different approaches and focuses of collection management, stemming from cultural differences and, largely, the difference in data sources. Evaluating collection from signals and communications is inherently different than evaluating data collected from human sources. Even if the data source is the same, different styles can exist. For example, the U.S. Army's Field Manual 2-22.3 on human intelligence collector operations offers a slightly different but still structured view of collection management: https://fas.org/irp/doddir/army/fm2-22-3.pdf. Further, the U.S. Army also prepared Field Manual 34-2 on Collection Management: https://fas.org/irp/doddir/army/fm34-2/Ch3.htm



Whitepaper

10 WAYS ASSET VISIBILITY BUILDS THE FOUNDATION FOR OT CYBERSECURITY

Knowing the data
you need to collect isn't
enough if you don't have
full asset visibility

DRAGOS, INC.
info@dragos.com
@DragosInc

+ [Crown Jewel Analysis]
+ [Collection Management Framework]
+ [Asset Visibility – 10 Considerations]

CONCLUSION

KEY TAKEAWAYS

1. Asset Visibility has applicability for all roles

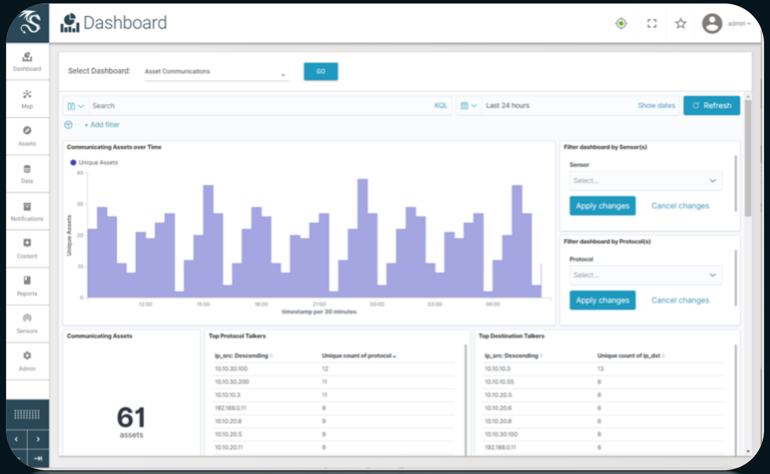
2. Prioritize asset visibility around identified Crown Jewels

3. Use a Collection Management Framework to understand visibility gaps and to develop a visibility strategy

FINAL WEBINAR FOR ASSET VISIBILITY SERIES

- Asset Visibility in Action with the Dragos Platform!

- A live walkthrough of common customer use cases exploring:
  - Baselines
  - Interactive Asset Map
  - Threat Detection



Select Dashboard: Asset Communications

Last 24 hours

Communicating Assets

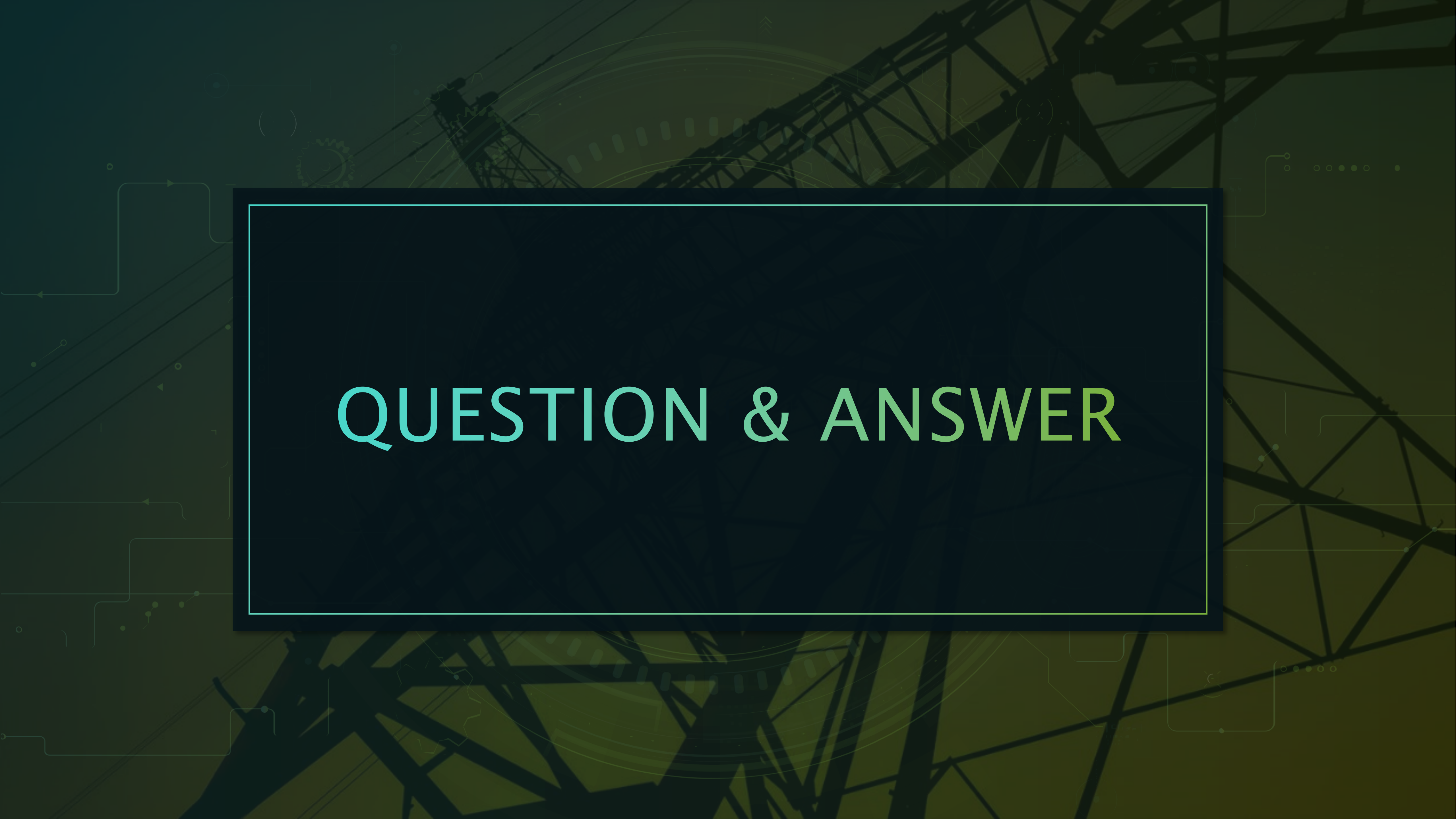
61
assets

Top Protocol Talkers

ip_src: Descending	Unique count of protocol
10.10.30.100	12
10.10.30.200	11
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

Top Destination Talkers

ip_src: Descending	Unique count of ip_dst
10.10.10.3	13
10.10.10.55	6
10.10.20.5	6
10.10.20.6	6
10.10.20.8	6
10.10.30.100	6
192.168.0.11	6



QUESTION & ANSWER

THANK YOU

DRAGOS