DRAGOS

OT ASSET VISIBILITY IN ACTION

April 28, 2021

TODAY'S PRESENTERS

JOSH CARLSON

Senior Manager
Business Development

JIMMY GRAHAM

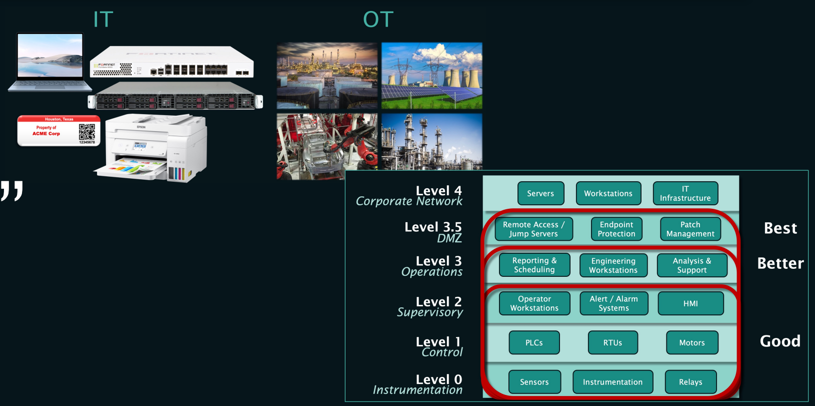
Senior Director
Product Management

DRAGOS

WEBINAR #1 RECAP

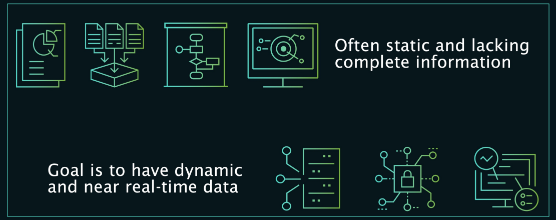
In case you missed it…

- What actually is ”Asset Visibility”



Level 4 *Corporate Network*	Servers	Workstations	IT Infrastructure	
Level 3.5 *DMZ*	Remote Access / Jump Servers	Endpoint Protection	Patch Management	Best
Level 3 *Operations*	Reporting & Scheduling	Engineering Workstations	Analysis & Support	Better
Level 2 *Supervisory*	Operator Workstations	Alert / Alarm Systems	HMI	
Level 1 *Control*	PLCs	RTUs	Motors	Good
Level 0 *Instrumentation*	Sensors	Instrumentation	Relays	

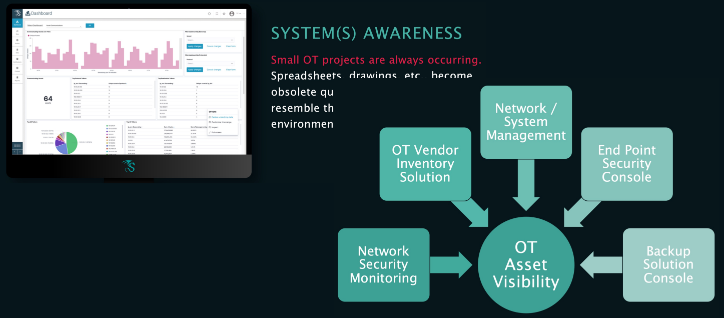
- Why having a proper perspective is important



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.

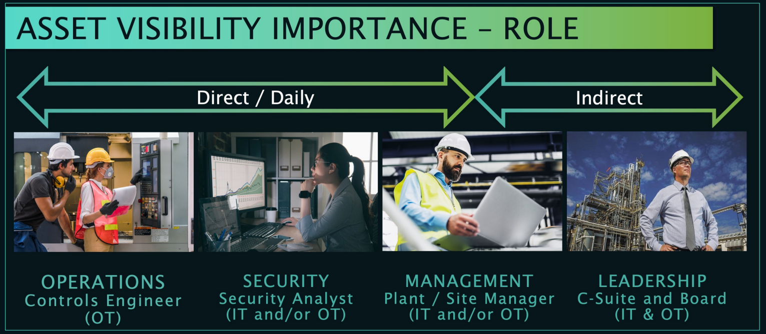
Spreadsheets, drawings, etc., become obsolete qu
resemble th
environmen

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

WEBINAR #2 RECAP

In case you missed it…

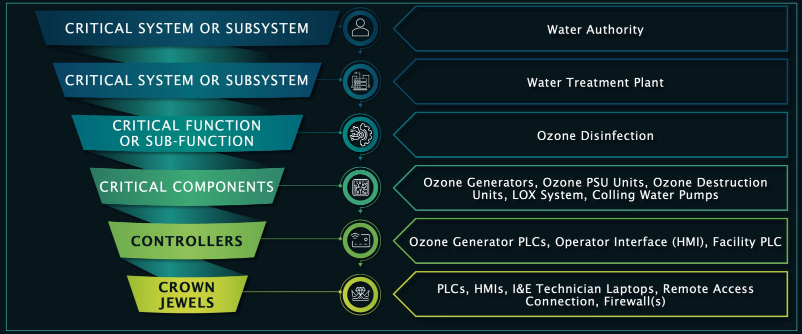
- Asset Visibility is applicable for all roles



ASSET VISIBILITY IMPORTANCE – ROLE

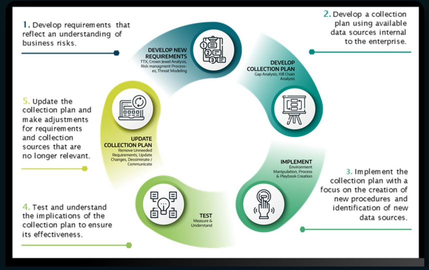
OPERATIONS Controls Engineer (OT)	SECURITY Security Analyst (IT and/or OT)	MANAGEMENT Plant / Site Manager (IT and/or OT)	LEADERSHIP C-Suite and Board (IT & OT)

- Prioritize Asset Visibility around identified Crown Jewels



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)

- Using Collection Management Framework (CMF) to mature an asset visibility strategy



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

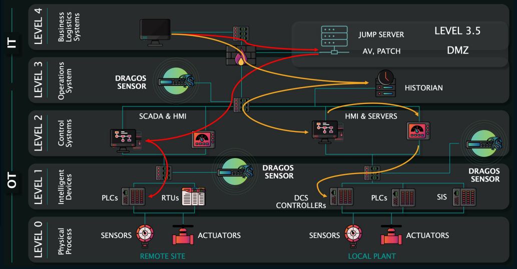
2. Develop a collection plan using available data sources internal to the enterprise.

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



ASSET VISIBILITY POLL

COMMUNITY FEEDBACK

How does your organization’s asset visibility compare in IT versus OT environments?

- IT has better visibility
- OT has better visibility
- They are about equal
- I have no idea!

SETTING THE STAGE

- Identify and organize your most critical assets – give your crown jewels the visibility they deserve
- Track devices and their communication paths over time leveraging historical data
- Quickly drill down into vital device details to assist with investigations and compliance

ASSET VISIBILITY & DRAGOS PLATFORM

KEY TAKEAWAYS

1. Obtaining real-time data within the environment is foundational for true asset visibility

2. Understanding connectivity and communication paths improves your team’s efficiency during their (incident) response

3. Organizations with cyber-operations with mature asset visibility are better positioned to have a sustained competitive advantage

RESOURCES

DRAGOS WHITEPAPERS

DRAGOS

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

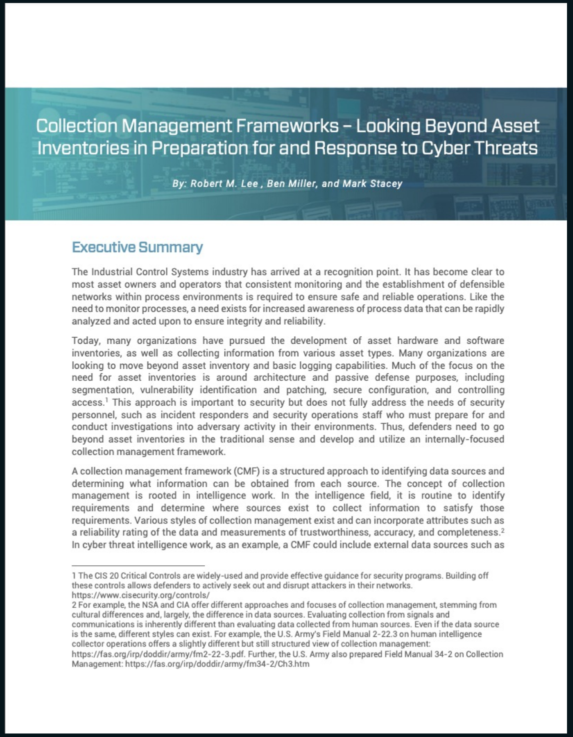
Abstract

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

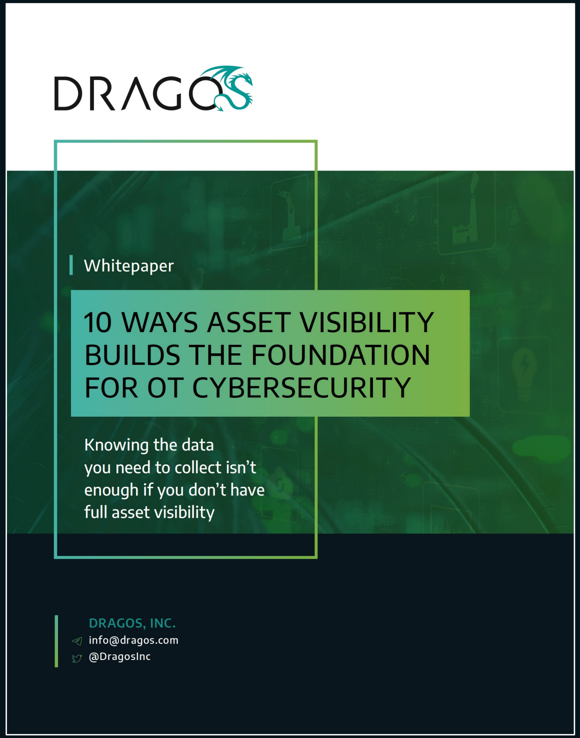
The Industrial Control Systems industry has arrived at a recognition point. It has become clear to most asset owners and operators that consistent monitoring and the establishment of defensible networks within process environments is required to ensure safe and reliable operations. Like the need to monitor 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



DRAGOS

Whitepaper

10 WAYS ASSET VISIBILITY BUILDS THE FOUNDATION FOR OT CYBERSECURITY

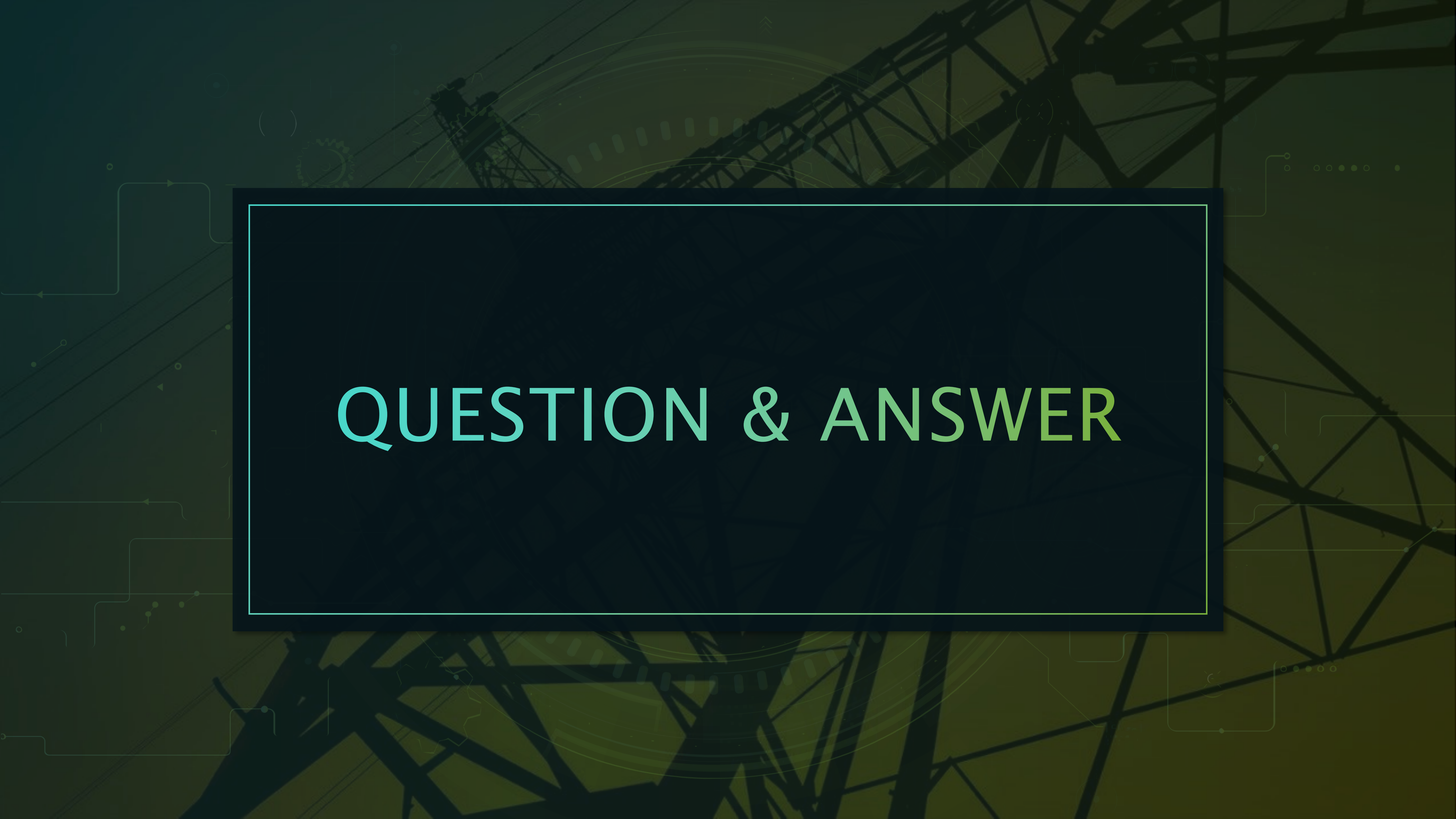
Knowing the data
you need to collect isn't
enough if you don't have
full asset visibility

DRAGOS, INC.
info@dragos.com
@DragosInc

+ Crown Jewel Analysis

+ Collection Management Framework

+ Asset Visibility – 10 Considerations



QUESTION & ANSWER

THANK YOU

DRAGOS