DRAGOS

Operational Technology Cybersecurity

An Industry Perspective

Chuck Weissenborn
Public Sector CTO

What is industry concerned about?

AL ALANITE	Co COVELLITE	Ch CHRYSENE	Cv CHERNOVITE	Dy DYMALLOY	EL ELECTRUM	Er ERYTHRITE
Hx HEXANE	Ka KAMACITE	Ko KOSTOVITE	Ma MAGNALLIUM	Pv PETROVITE	Pi PARISITE	Ra RASPITE
St STIBNITE	Ta TALONITE	Va VANADINITE	Wa WASSONITE	Xt XENOTIME	Vz VOLTZITE	

VOLTZITE

Active Since 2023

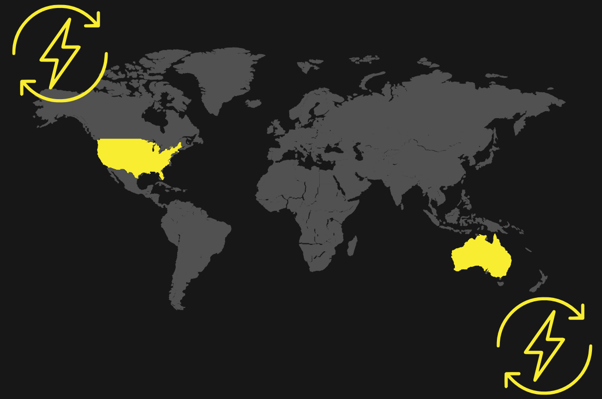
Focused on the Energy sector, and potentially other industrial infrastructure sectors in the United States

Conducts offensive operations with a major focus on detection evasion and sophisticated operational security tradecraft

Frequently utilizes living off the land (LOTL) techniques, and often tunnels C2 traffic through compromised SOHO routers

KOSTOVITE

Active Since 2021



Targets **renewable energy operations** in North America and Australia

KOSTOVITE

SINCE 2021

ADVERSARY:

- High level of operational discipline & network device knowledge
- Lives off land with stolen sys/net-admin creds

CAPABILITIES:

- Zero-day exploits
- Pulse Secure PCS
- QNAP

VICTIM:

- Global renewable energy company based in South Asia
- North America, Australia

INFRASTRUCTURE:

- Dedicated per target
- Compromised home and small business QNAP NAS devices exposed to internet
- Commercial Ivanti VPN appliances

ICS IMPACT:

- Stage 2 of ICS Kill Chain
- Intrusion into OT networks and devices

STAGE 02	Develop
STAGE 02	Test
STAGE 02	Deliver
STAGE 02	Install / Modify
STAGE 02	Execute ICS Attack

Reached Stage **2 of ICS Kill Chain capabilities** with a confirmed intrusion into an operations and maintenance (O&M) firm's OT networks and devices

Commercial Industry Perspectives

What Do Our Commercial Customers Ask Dragos?

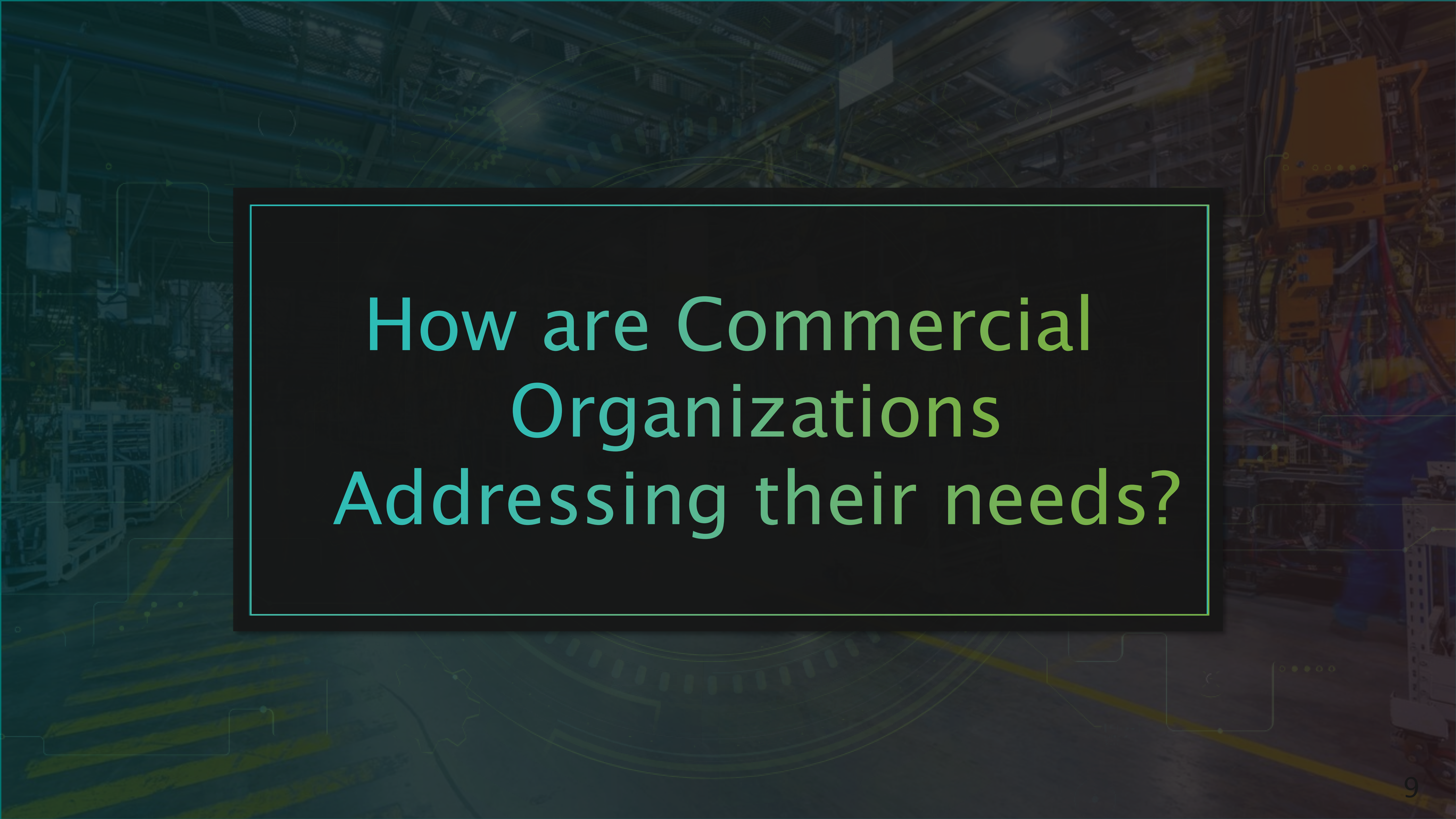
- Is my environment compromised by a threat actor?
- What are the dependencies of my critical functions and assets?
- Are things operating as expected?
- Should I care about *{vulnerability}* that is present in my environment?
- Is my OT cybersecurity program effective?

Are these the right questions?

- Must understand what commercial companies are focused on:
  - Safety
  - Reliability (Availability)
  - Productivity
- THEN
  - Confidentiality
  - Integrity

Additional Commercial Drivers

- Insurance requirements
- Government regulations
- Government contracts
- Profit



How are Commercial Organizations Addressing their needs?

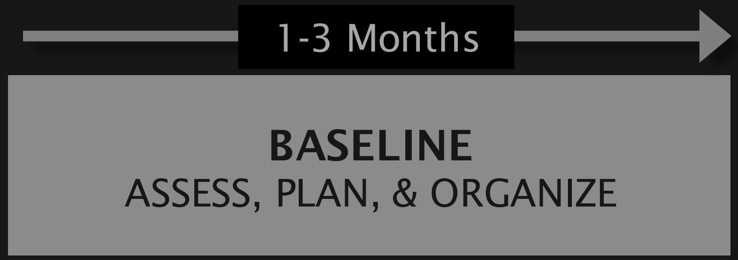
ICS/OT Cyber Security Journey

BASELINE
ASSESS, PLAN, & ORGANIZE

OPERATIONALIZE
OT-SPECIFIC
RISK CONTROLS

OPTIMIZE
MATURE OT RISK
REDUCTION PROGRAM

ICS/OT Cyber Security Journey



1-3 Months

BASELINE
ASSESS, PLAN, & ORGANIZE

Establish Baseline

Create an Incident Response Plan

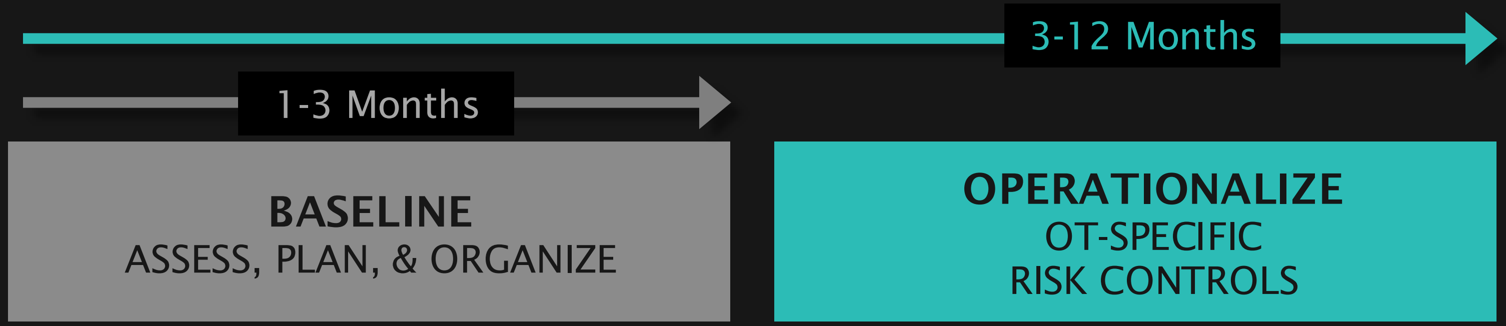
- Assess Your OT Cyber Security Architecture
- Organize your assets inventory & collection management framework

Implement MFA

Global organizations with multiple sites struggle with this phase more so than any other.

Organizations MUST acknowledge they cannot centralize all functions, and that each site must have its own people, plans, and procedures nested underneath higher echelon guidance.

ICS/OT Cyber Security Journey



3-12 Months

1-3 Months

BASELINE
ASSESS, PLAN, & ORGANIZE

OPERATIONALIZE
OT-SPECIFIC
RISK CONTROLS

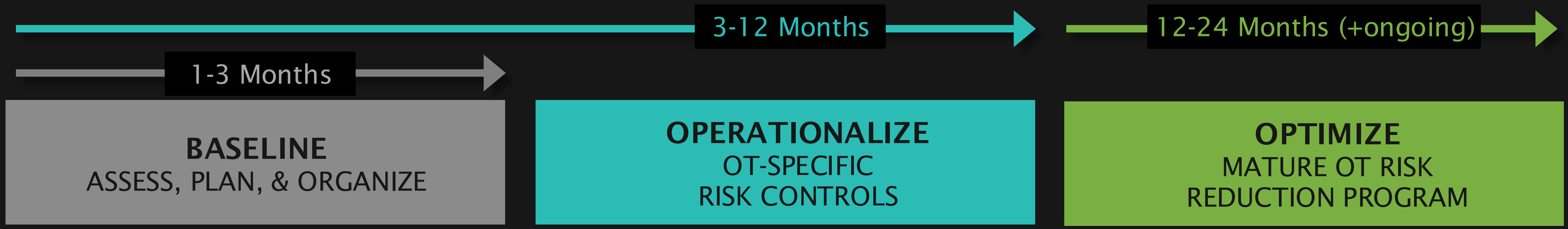
Operate Dragos Platform

- Monitor OT assets & network traffic in Crown Jewel sites
- Identify & manage key OT vulnerabilities
- Detect & respond to OT incidents

The actions during this phase are similar in nature to that of mission analysis during the military decision making process.

Global organizations may have many interconnected sites; establishing visibility and having *people* who understand how processes work across boundaries is key to success in this phase.

ICS/OT Cyber Security Journey



1-3 Months

3-12 Months

12-24 Months (+ongoing)

BASELINE
ASSESS, PLAN, & ORGANIZE

OPERATIONALIZE
OT-SPECIFIC
RISK CONTROLS

OPTIMIZE
MATURE OT RISK
REDUCTION PROGRAM

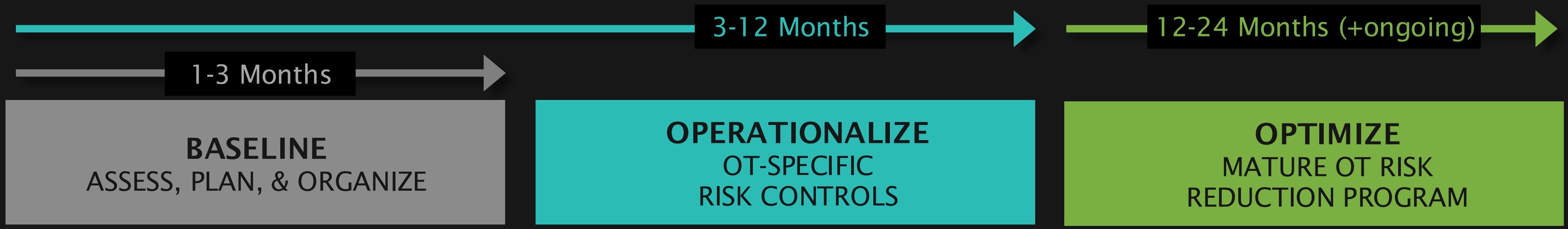
Once crown jewels and key interdependencies are monitored, continue to expand efforts at scale.

For the Public Sector, structured programs are often in place to help manage these prioritization actions.

Expand & Mature

- Expand deployment to medium & low impact OT sites
- Integrate OT incidents & intelligence with IT SOC
- Validate defensive controls

ICS/OT Cyber Security Journey



1-3 Months

3-12 Months

12-24 Months (+ongoing)

BASELINE
ASSESS, PLAN, & ORGANIZE

OPERATIONALIZE
OT-SPECIFIC
RISK CONTROLS

OPTIMIZE
MATURE OT RISK
REDUCTION PROGRAM

Establish Baseline

- Create an Incident Response Plan
- Assess Your OT Cyber Security Architecture
- Organize your assets inventory & collection management framework

Operate Dragos Platform

- Monitor OT assets & network traffic in Crown Jewel sites
- Identify & manage key OT vulnerabilities
- Detect & respond to OT incidents

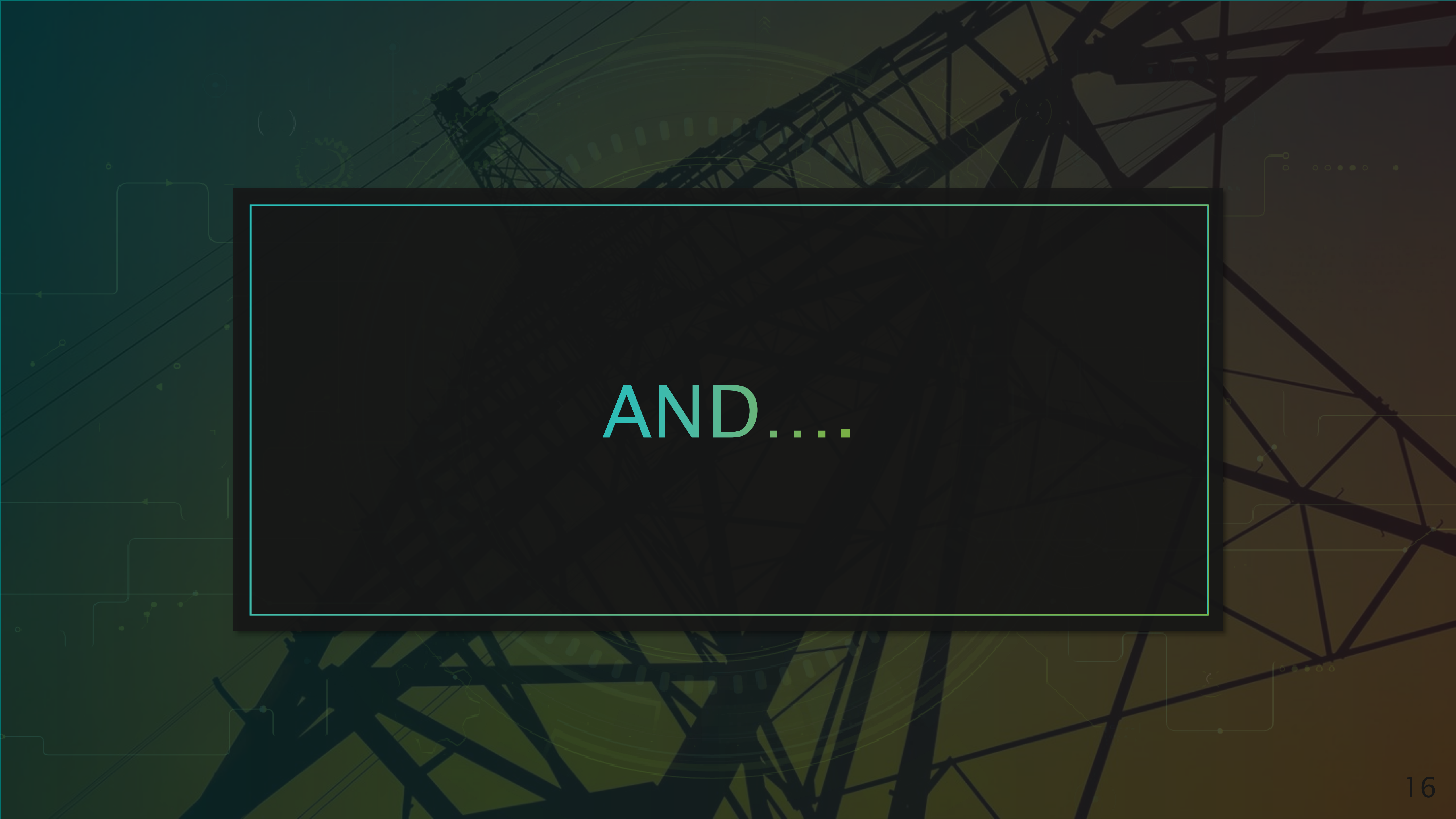
Expand & Mature

- Expand deployment to medium & low impact OT sites
- Integrate OT incidents & intelligence with IT SOC
- Validate defensive controls

HAVING PARTNERS THAT UNDERSTAND OT HELPS ORGANIZATIONS SCALE QUICKER

Key Capabilities/Resources Used by Industry

- OT-specific cyber threat intelligence
- Threat Detection
- Asset Management
- Vulnerability Management
- SIEM
- Data Historians
- Configuration Change Detection
- Endpoint Security



AND….

PEOPLE!!!

People are our #1 challenge

- OT cybersecurity requires at least fundamental knowledge in:
    - Sector-specific engineering (how things work)
    - Networking (how things communicate to work)
    - IT Systems (yes, they're within or are part of OT, too)
    - Cybersecurity (thing Purple – not just red or blue)

People are needed at all levels and locations

(Not all inclusive)

- Local to Site
  - Protect, Defend, Hunt, Initial Response
  - Cyber commissioning
- Enterprise
  - Centralized understanding of operational risk
  - Cybersecurity Service-provider functions (SOC, etc.)
  - IT-in-OT infrastructure support (IDaM, transport, etc.)
  - Security control validation
- Strategic
  - Resourcing
  - Translation of OT cyber/engineering to senior leaders
  - OT cyber governance

Call to Action

FIVE CRITICAL CONTROLS

5 CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

A Journey to safety, reliability, and productivity:
Enabled through OT Cybersecurity

01

An ICS-specific incident response plan

02

A defensible architecture

03

OT Visibility: asset inventory, vulnerability mapping, & monitoring

04

Vulnerability management program

05

Multi-factor authentication (MFA)

Community: Dragos OT-CERT

OT-CERT
OPERATIONAL TECHNOLOGY
CYBER EMERGENCY READINESS TEAM

1,600 members

60 countries

OT-CERT is the Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gaps that exist in industrial infrastructure.

Dragos Community Defense Program (CDP)

Free OT cybersecurity software technology

Dragos Platform & other key resources such as Dragos Academy

For small water, electric, and natural gas providers

<$100 million revenues

To help reduce risk of cyber events

- Inventory assets
- Detect & hunt threats
- Manage vulnerabilities
- Respond to incidents

Register at:
Dragos.com/community-defense-program

Email us at:
CDPinfo@dragos.com

A Call to Action: Protecting Small Utilities is ALL our jobs

Qualifying Organizations

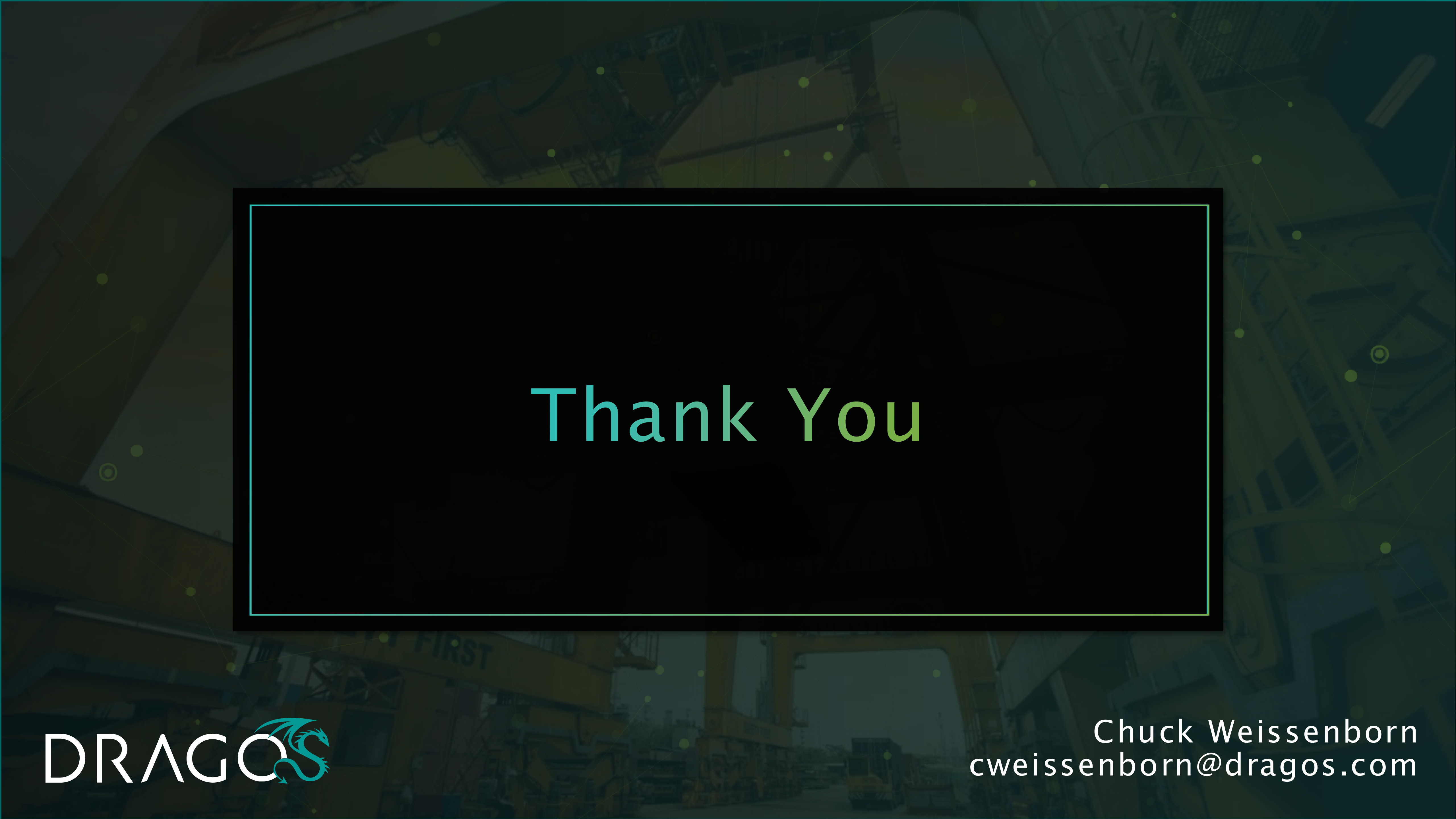
Apply now. *Dragos.com/community-defense-program* Or request more info *cdpinfo@dragos.com*

Organizations that don’t qualify, and want to improve cyber security

Contact *info@dragos* to help chart your journey and join OT-CERT at *Dragos.com/ot-cert/registration*

ISACs, other community & government organizations

Help get the word out. Send this link to qualifying organizations *Dragos.com/community-defense-program*



Thank You

Chuck Weissenborn
cweissenborn@dragos.com