DRAGOS®

YOU ARE NOT ALONE!
EFFECTIVE OT INCIDENT RESPONSE

Safeguarding Civilization

INTRODUCTION

Tim Ennis

- Senior Industrial Incident Responder
- Based in UK
- 10+ years of industrial experience including safety system engineering

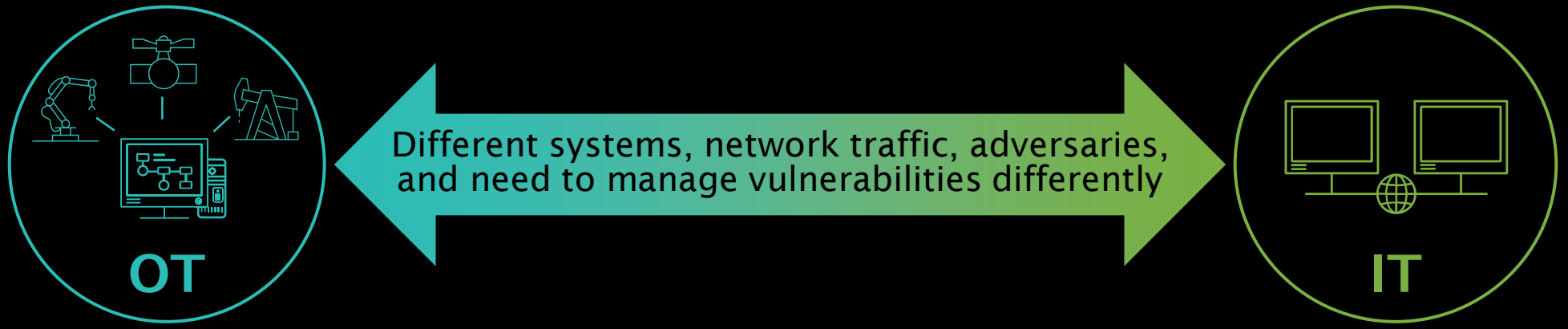
Jan Hoff

- Principal Industrial Incident Responder
- Based in Germany
- 10+ years in the energy sector as an offensive and defensive cyber security expert

DRAGOS

CYBER RISK

Operational Technology (OT) vs. Information Technology (IT)



OT

- Loss of electrical grid, water systems, safety systems, pipeline, or plant operations
- Loss of revenue generating operations for industrial companies

Impact From a Major Cyber Security Incident

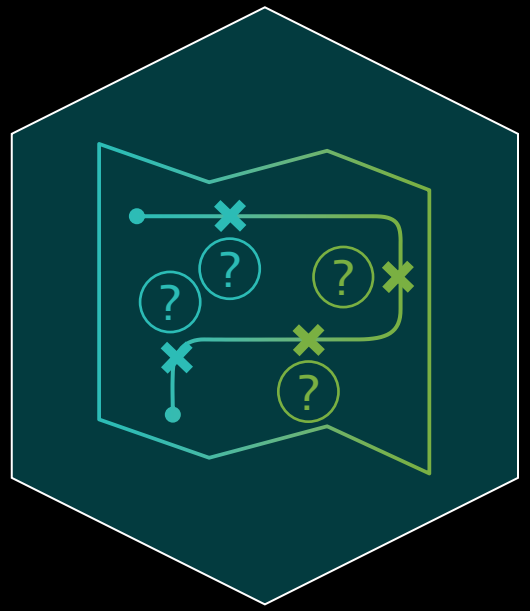
IT

- Loss of data, intellectual property, network services
- Loss of revenue generation for services, financial, & technology companies

COMMON QUESTIONS

What are you trying to defend? What are your OT “crown jewels”?

What are you trying to defend against?



Where are you in your OT security journey?

DRAGOS PLATFORM

Expertise Integrated Into Software to Reduce OT Risk

OT WATCH Dragos Managed Vulnerability Response, Hunting, & Incident Triage

VISIBILITY
Assets, Traffic, & Vulnerabilities

DETECTION
Compromises & Threat Behaviors

RESPONSE
Investigation Forensics & Playbooks

NEIGHBORHOOD KEEPER Community-Wide Threat Visibility & Collective Defense

EFFECTIVE OT SECURITY

CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

01
ICS incident response

02
Defensible architecture

03
ICS network visibility & monitoring

04
Secure remote access

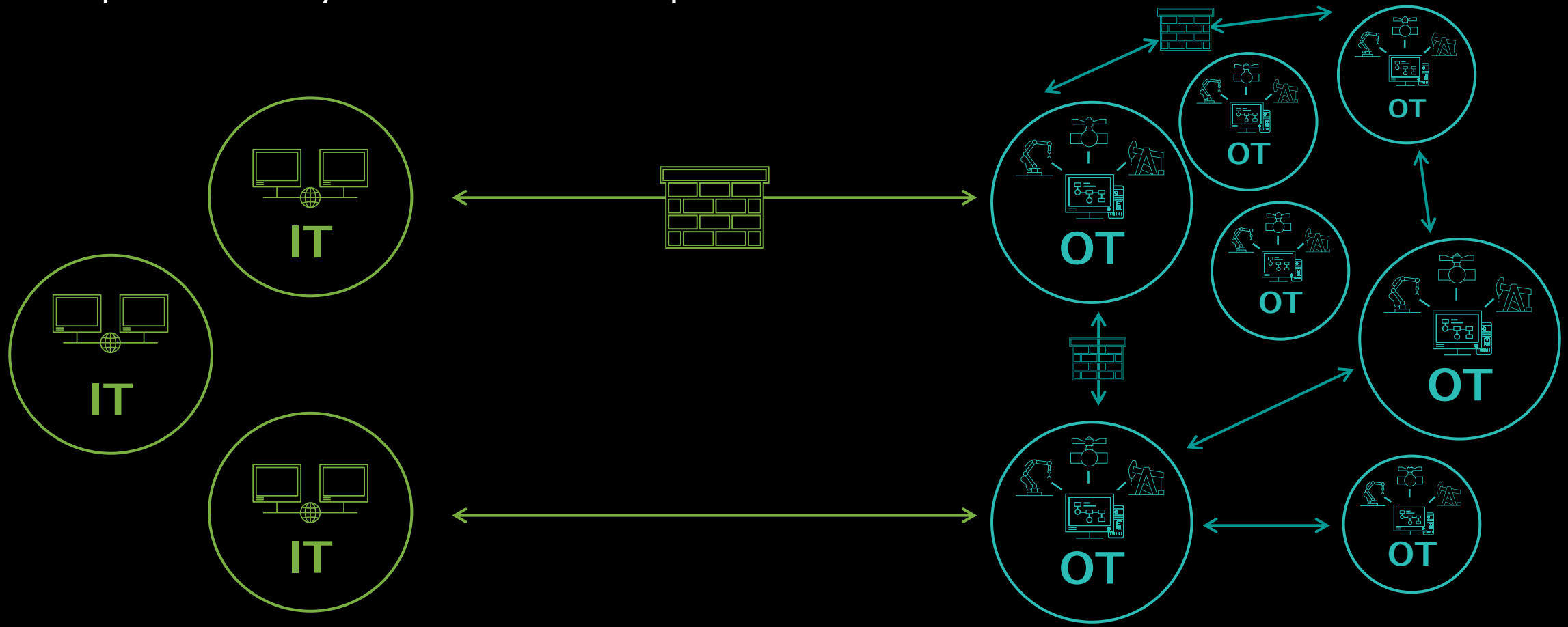
05
Risk-based vulnerability management

YOUR SYSTEMS ARE NOT ALONE

Defensible architectures and prioritization

SYSTEMS OF SYSTEMS

Architectures contain multiple interconnected and interdependent systems and components

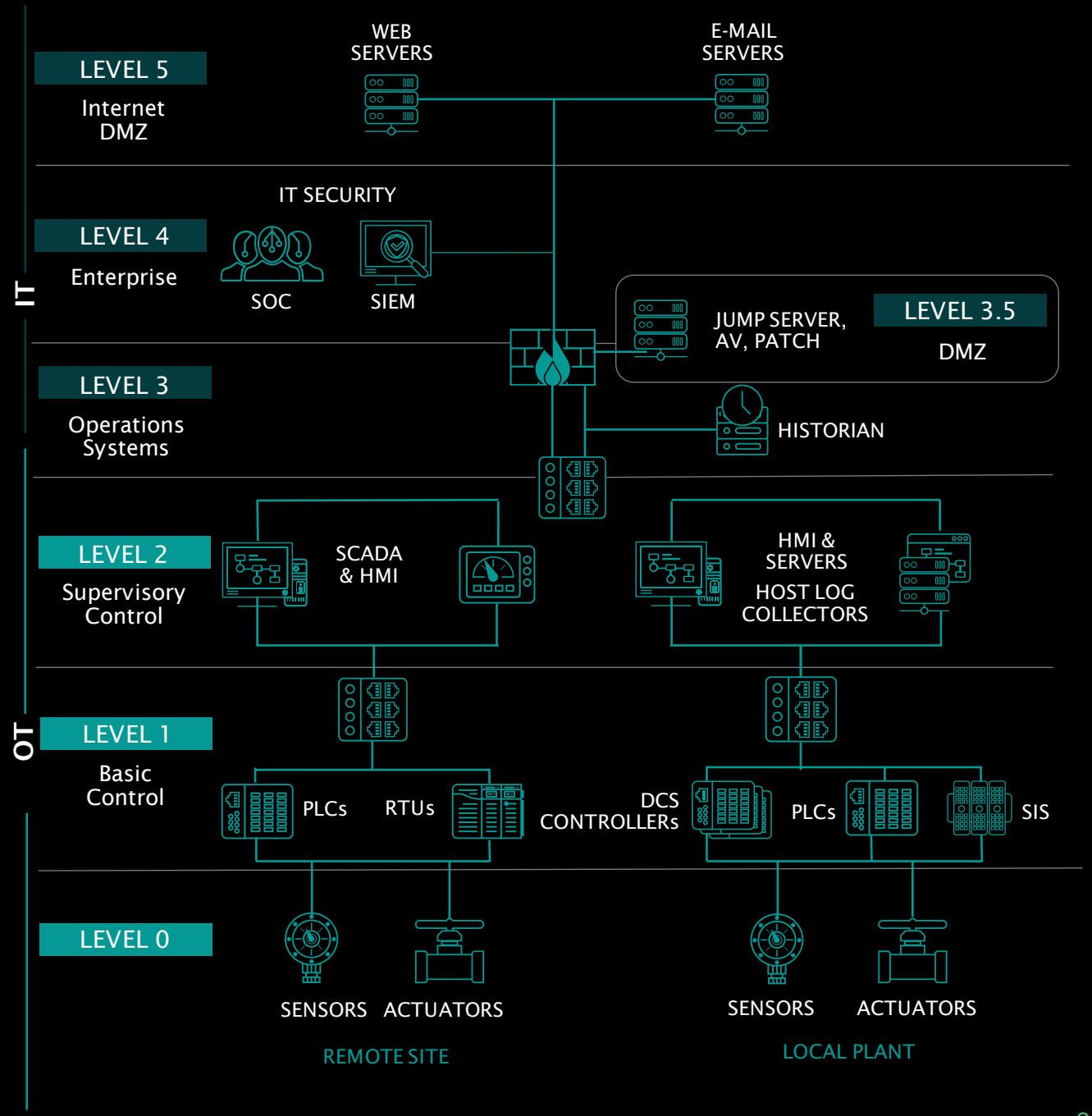


TYPICAL OT ARCHITECTURE

What does **your network look like?**

Is your **system architected properly?**

Do you have a current **asset inventory?**



COLLECTION MANAGEMENT FRAMEWORK (CMF)

Sustained visibility into your environment

A CMF is the practice of documenting all the potential sources of data that could be used by incident responders and investigators

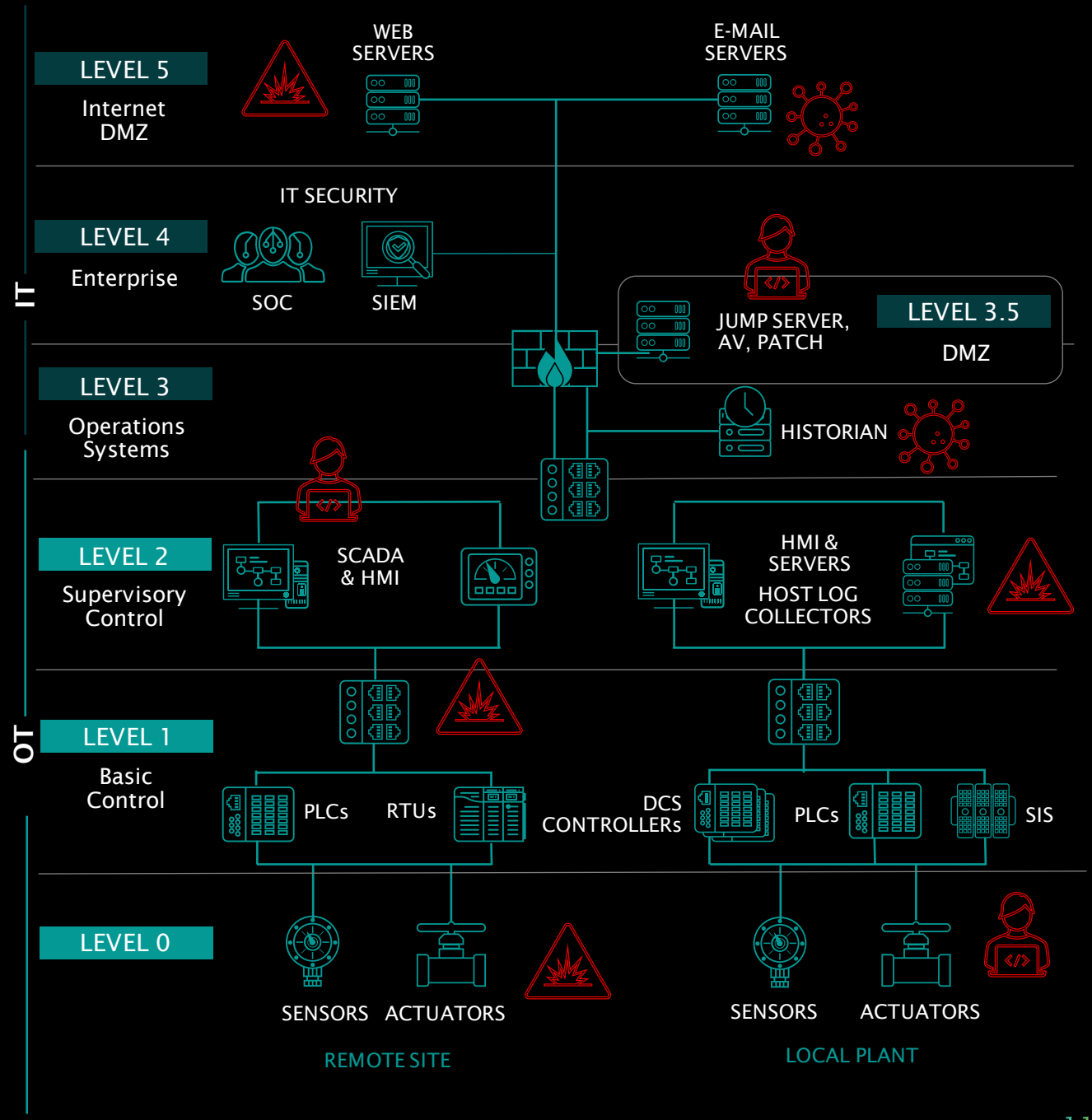
- Includes all digital assets such as computers, data loggers, network equipment, PLCs
- Anything that contains logging or forensic information that could inform an analyst during an investigation is valuable

TYPICAL OT ARCHITECTURE

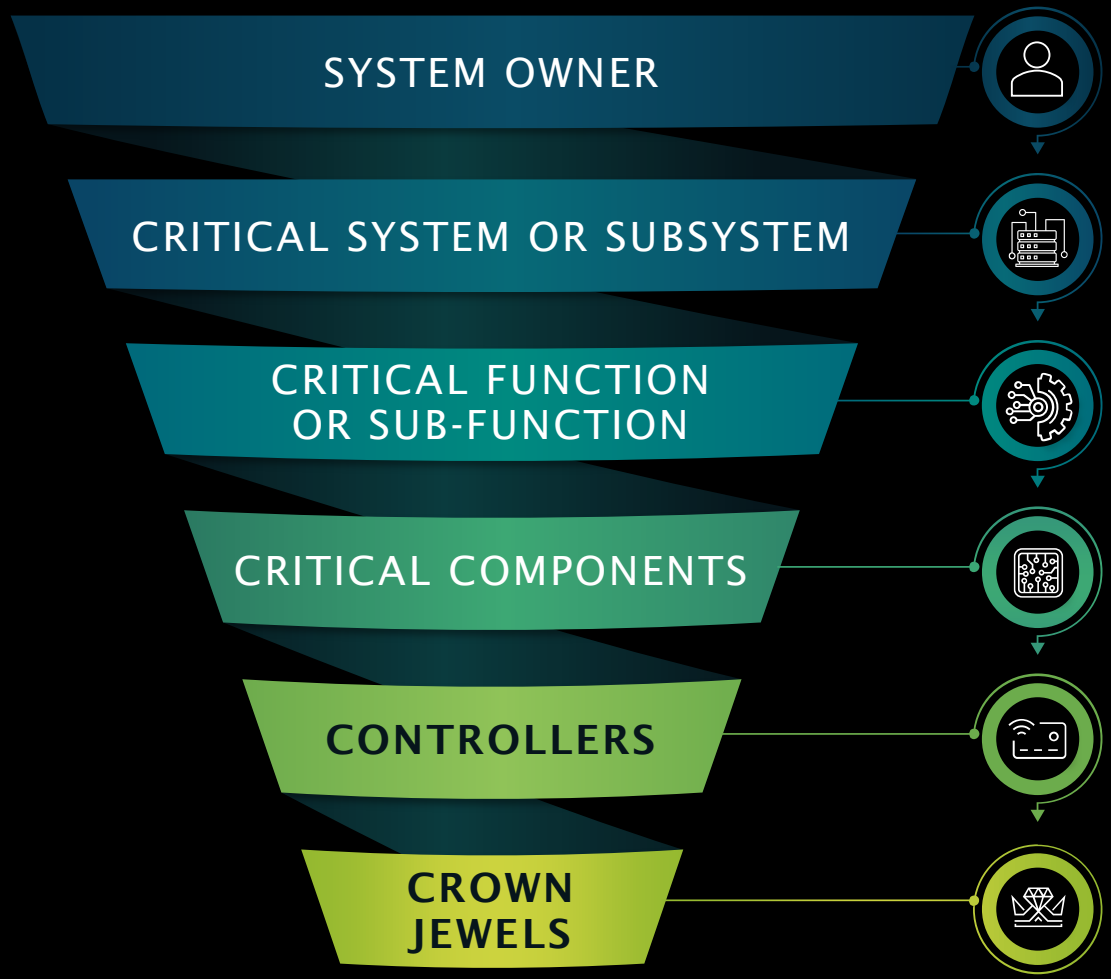
What does a **bad day look like** in your environment?

Do you know the **hidden dependencies?**

What are **consequences of attacks** and **adverse events?**



DRAGOS CROWN-JEWEL-ANALYSIS MODEL



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

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

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

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

Represented by their direct interconnection between the logical and the physical network. Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) fall under this category.

Critical data, logical assets, and/or communication and control interfaces required to exercise control over components, and thus, functions (HMIs, DCs, gateways, controllers, etc.)


YOU ARE NOT ALONE
IN AN INCIDENT
Responding to incidents in industrial environments

INCIDENT RESPONSE

Do not respond to incidents alone

- Consider OT specific skills and personnel, use a retainer, decide on activation criteria
- Prepare all potentially involved personnel for Incident Response
- Utilize previously planned incident command systems and playbooks

Prioritize life/environment before production outages

- An incident might not be limited to a single location, process or system

Consider consequences of actions and adversaries

- Most IR activities will impact the normal operation
- Loss of visibility, loss of control, loss of productivity, …

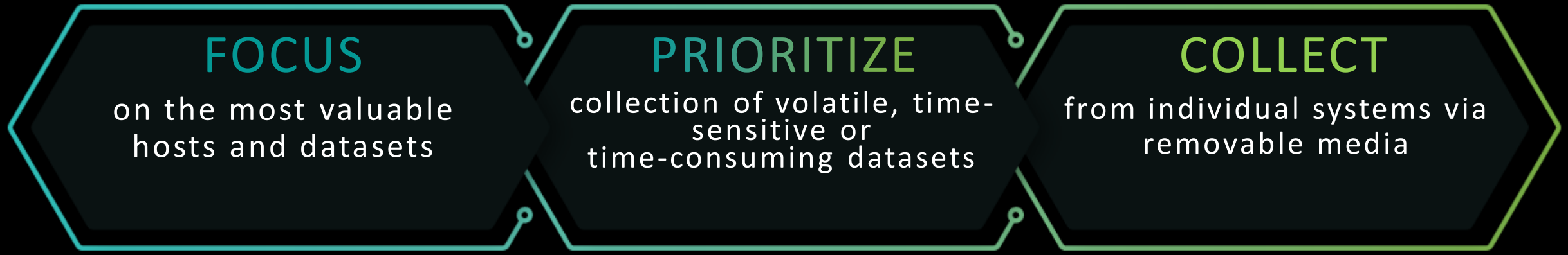
An adversary could be inside your network

- You might not be alone while handling an incident

THE ‘TAKE 5’ OF OT IR

1. Keep Calm
2. Assemble Your Team
3. Activate Third Parties Early
4. Spin Up Out-of-Band Comms
5. Collect Evidence & Scope

COLLECTING FROM OT NETWORKS



IT approaches for (forensic) data collection may fail in OT	Focus and prioritize crown jewel applications	Assess available (forensic) data and their retention time	Collection might require on-site presence	Prepare access/ removable drives and validate procedures

KICKSTARTING YOUR INCIDENT RESPONSE

Good preparation and readiness is key for effective response

Benefits of OT Monitoring & Visibility

1. Quicker investigation
2. More thorough investigations
3. Easier assurance of eradication
4. More insightful results
5. Early detection to prevent/limit incident

YOU ARE NOT ALONE IN THE COMMUNITY

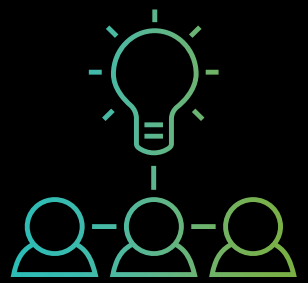
Share information and join forces

OT CERT AND ISACS

Information sharing is a key community aspect

Share OT security knowledge and best practices

Utilize and contribute to close the OT cybersecurity skills gap in the community



Share Information on adversaries and anomalies

Sharing indicators and adversary behavior allows protection and proactive hunting

Forming partnerships

Build information sharing groups (ISACs), promote shared values and jointly safeguard critical infrastructures

COMMUNITY DEFENSE

Exchanging Intel & Building Skills to Strengthen the Collective Defense

NEIGHBORHOOD KEEPER

Collective Threat Insights & Defense

A free, opt-in program for Dragos Platform customers

Collective ICS threat, asset, & vulnerability intelligence

DRAGOS OT-CERT

OT Cyber Emergency Response Team

Free resources & expertise open to asset owners & operators

Regional workshops, growing content library, vulnerability disclosures

OT-CERT

Industrial Cybersecurity Resources For The OT Community

Free Cybersecurity Resources

Free content available for OT asset owners and operators, to help you build and maintain an effective OT cybersecurity program

Open to ICS/OT Community

Beneficial for businesses of all sizes, especially those with fewer OT cybersecurity resources and expertise

New Content Monthly

Members have access to a growing library of resources such as reports, webinars, training, best practice blogs, assessment toolkits, tabletop exercises and more, available from the OT-CERT portal

Regional Workshops

Customized regional workshops to meet the needs of the community

Vulnerability Disclosures

We take a coordinated approach to the disclosure of vulnerabilities, working with vendors to better protect our customers and the ICS/OT community

DRAGOS OT-CERT

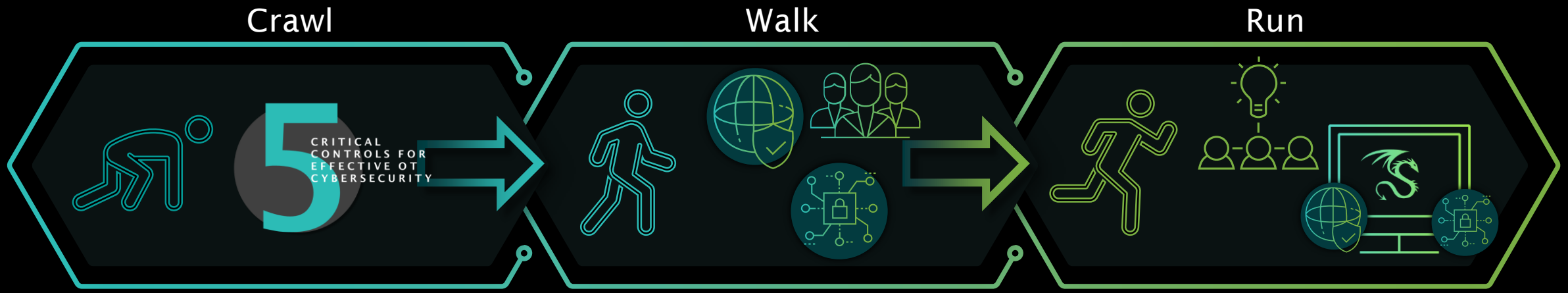
Operational Technology – Cyber Emergency Readiness Team

Register for membership at dragos.com/ot-cert/registration

ROADMAP FOR EFFECTIVE OT INCIDENT RESPONSE

Moving forward with an action plan

YOU ARE NOT ALONE ON YOUR JOURNEY!



- Implement 5 Critical Controls for Effective OT Security
- Identify Crown Jewels

- Utilize Threat Intelligence for Defense
- Increase Visibility and Resilience
- Test Plans and Control Effectiveness (TTX)

- Exercise! Exercise! Exercise! Exercise!
- Measure and improve
- Collaborate and share

THANK YOU

Email: tennis@dragos.com

Email: jhoff@dragos.com