DRAGOS®

Webinar Series: Incident Response for OT Environments

OT INCIDENT RESPONSE IS DIFFERENT

Safeguarding Civilization

INTRODUCTION

Vern McCandlish

- Principle Industrial Incident Responder
- Based in the United States
- 20+ years of industrial cybersecurity experience including law enforcement and forensics

Hussain Virani

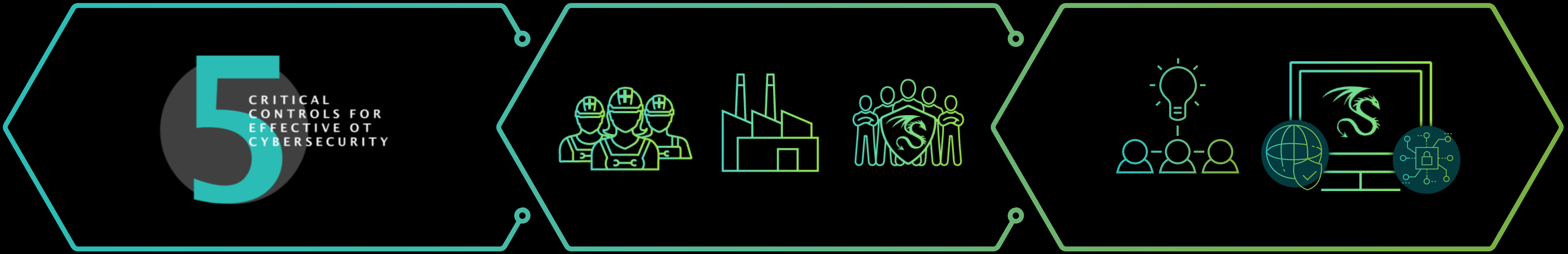
- Senior Industrial Incident Responder
- Based in Canada
- 10+ years in the oil and gas sector as an investigator and forensic analyst

THREE-PART SERIES ON OT IR

Webinar 1
You are not alone

Webinar 2
OT IR is different

Webinar 3
Effective IR – be prepared



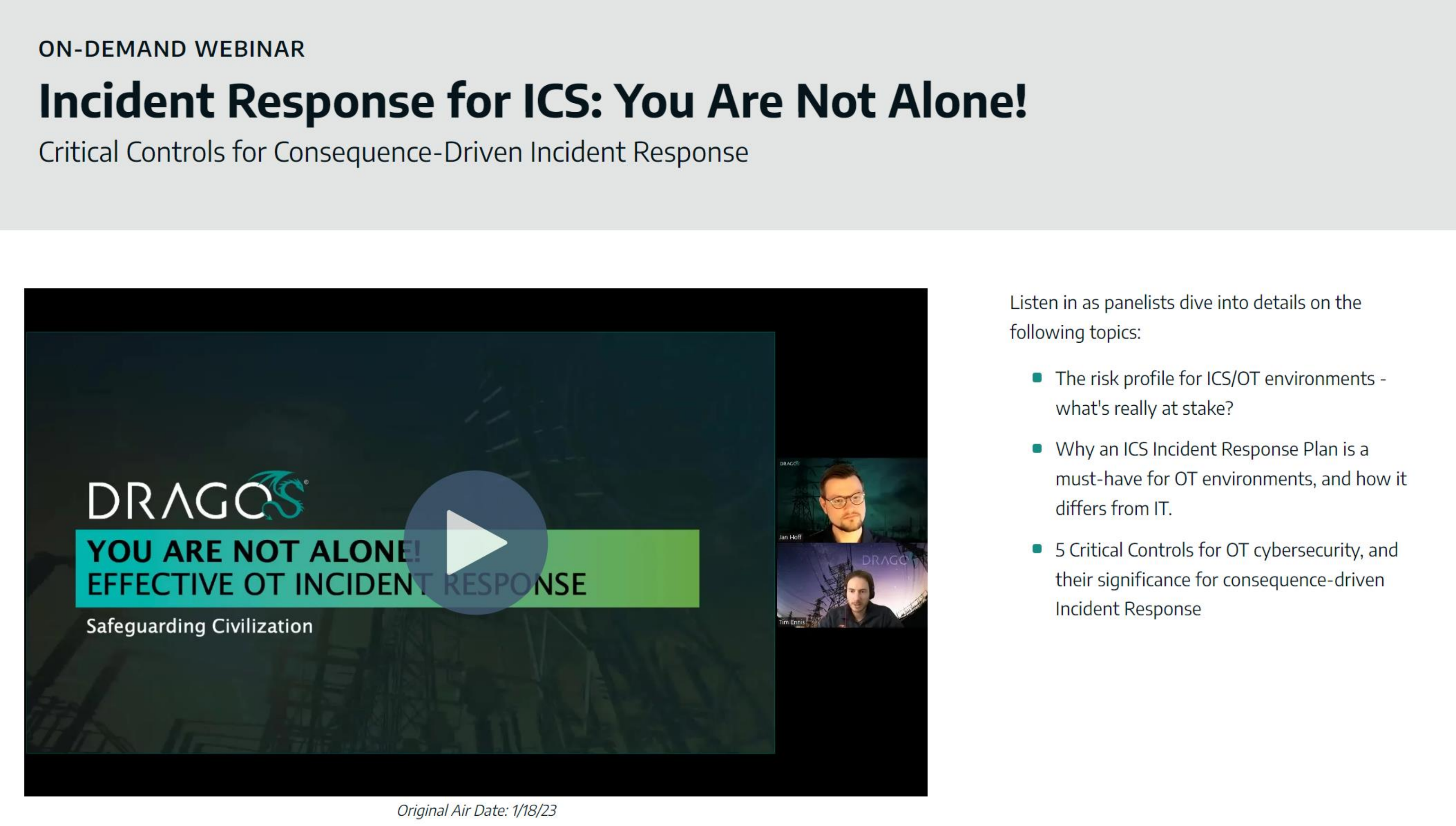
- 5 Critical Controls as a foundation for any OT cybersecurity program
- Establishing an Incident Response Plan

- Difference of incident response in OT and IT
- Incident Management
- IR Data Collection

- Empower people
- Improve processes
- Train to win
- Defeat the threat

THREE-PART SERIES ON OT IR

FIRST WEBINAR IS AVAILABLE ON-DEMAND



ON-DEMAND WEBINAR

Incident Response for ICS: You Are Not Alone!

Critical Controls for Consequence-Driven Incident Response

Original Air Date: 1/18/23

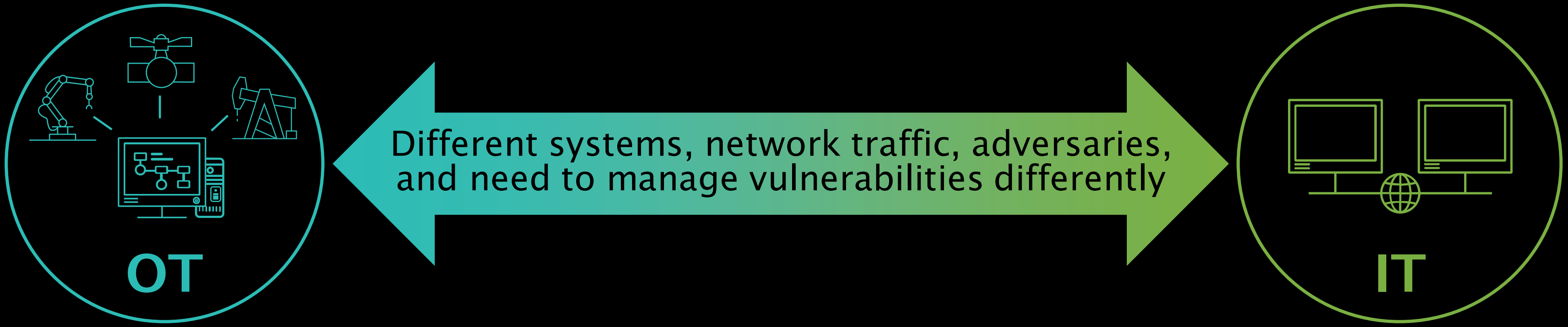
Listen in as panelists dive into details on the following topics:

- The risk profile for ICS/OT environments - what's really at stake?
- Why an ICS Incident Response Plan is a must-have for OT environments, and how it differs from IT.
- 5 Critical Controls for OT cybersecurity, and their significance for consequence-driven Incident Response

INCIDENT COMMAND AND MANAGEMENT

CYBER RISK

OPERATIONAL TECHNOLOGY (OT) VS. INFORMATION TECHNOLOGY (IT)



Different systems, network traffic, adversaries, and need to manage vulnerabilities differently

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

TALKING ABOUT IMPACT

CONSIDERING CONSEQUENCES IN OT

POTENTIAL CONSEQUENCE	EXAMPLES	CYBER INCIDENT EXAMPLE
Plant damage	• Damage to control system equipment • Excessive wear on final elements (such as actuators) • Over-pressurization of vessels and pipework • Fire or explosion	• TRISIS • CrashOverride
Loss of production	• Plant trips (opening of circuit breakers, activation of shutdown measures). • Manual shutdown of plant as a conservative decision. • Manual shutdown of plant due to loss of billing, production, shipping data from ERP systems.	• CrashOverride • TRISIS • Colonial Pipeline • Norsk Hydro • Honda • Mariposa Botnet at Electric Utility (2012)

TALKING MORE ABOUT IMPACT

CONSIDERING CONSEQUENCES IN OT

POTENTIAL CONSEQUENCE	EXAMPLES	CYBER INCIDENT EXAMPLE
Impact on product quality	• Contamination of product. • Changes to logic sequences. • Delay in sealing/packaging/chilling product.	• Oldsmar Water treatment facility attack
Industrial safety event	• Loss of limb, livelihood, life to an onsite worker or member of the public • Exposure to hazardous substances	• No known public record of cyber-attack leading to injury or death of onsite worker or member of the public.
Environmental safety event	• Uncontrolled release to the environment • Discharge of untreated effluent • Loss of containment	• Maroochy Shire Sewage Spill

INCIDENT MANAGEMENT (IM)

The National Fire Protection Association provides a definition of Incident Management (IM): “the combination of facilities, equipment, personnel, procedures and communications operating within a common organizational structure, designed to aid in the management of resources during incidents”.

https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

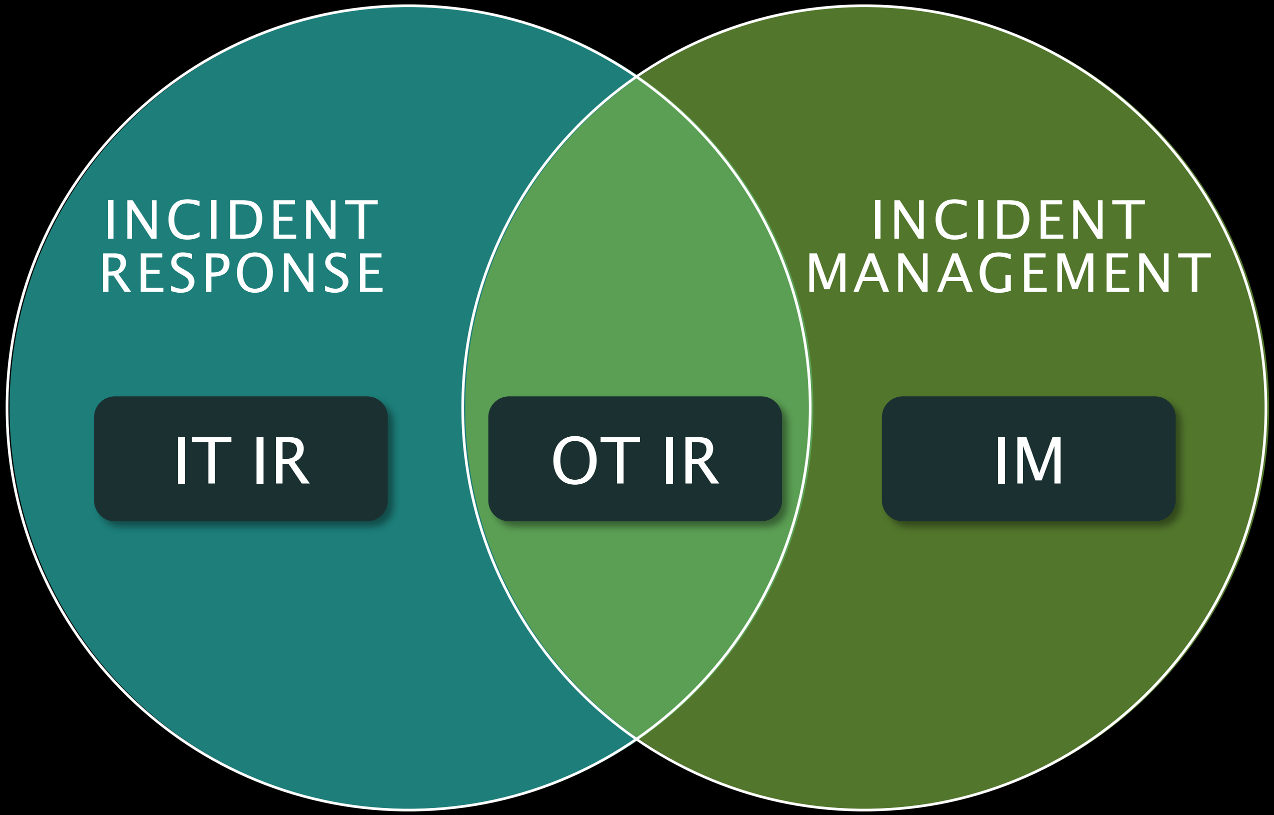
INCIDENT MANAGEMENT (IM)

COMPAIRSON OF DIFFERENT INCIDENT

COMPONENT / SITUATION	FIRE	COMPONENT / SITUATION	INCIDENT RESPONSE
Facilities	• Control center	• Spill kits • Eye wash stations • Control center	• Helpdesk • SOC • Forensics Lab
Equipment	• Fire extinguishers • Fire blankets • Risers	• PPE • Absorbent materials	• Security tools • Hard drive write-blockers • Evidence bags
Personnel	• Fire crews • Duty officer	• First aid team	• Analysts • DFIR specialists
Procedures	• Evacuation, muster	• Containment • Clean-up • Reporting	• IR plan • BCP
Communications	• Fire alarm • All clear • Call to fire Brigade	• Emergency contact number	• Report an event • Comms to employees • Press releases

CONVERGENCE OF IR AND IM

OT INCIDENT REPONSE NEEDS INCIDENT MANAGEMENT



Safety and OT often have a strong incident management focus

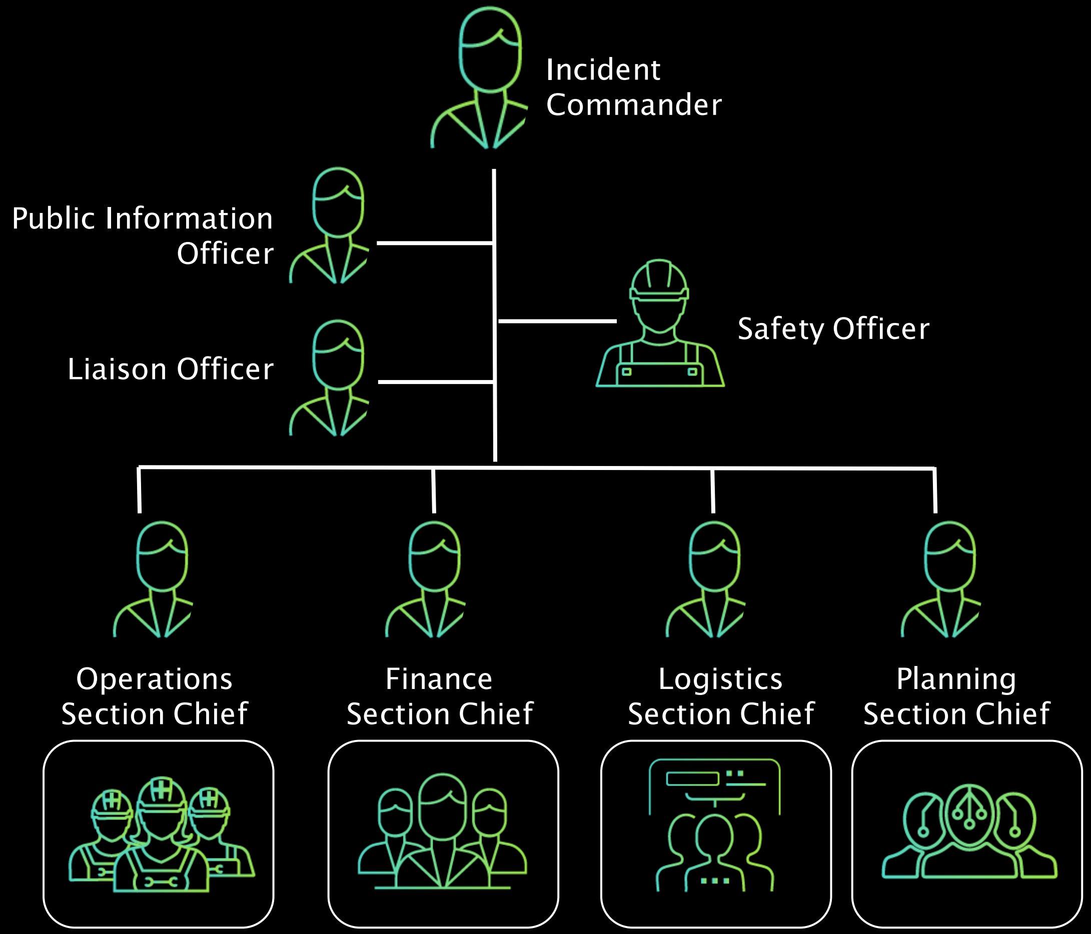
Historically incident response has been part of the IT domain

OT incident response must consider both domains

INCIDENT COMMAND SYSTEM

ESTABLISH STRUCTURE PRE-INCIDENT

- Parties involved in OT incident response are significantly different to IT IR
- Used by fire services, military, and law enforcement
- Scales well in real time
- Keeps individuals and teams focused on their part of response
- Includes prior planning for logistics and messaging



Incident Commander

Public Information Officer

Liaison Officer

Safety Officer

Operations Section Chief

Finance Section Chief

Logistics Section Chief

Planning Section Chief

INCIDENT DATA COLLECTION

COLLECTING FROM OT NETWORKS

FOCUS

on the most valuable hosts and datasets

PRIORITIZE

collection of volatile, time-sensitive or time-consuming datasets

COLLECT

from individual systems via removable media

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

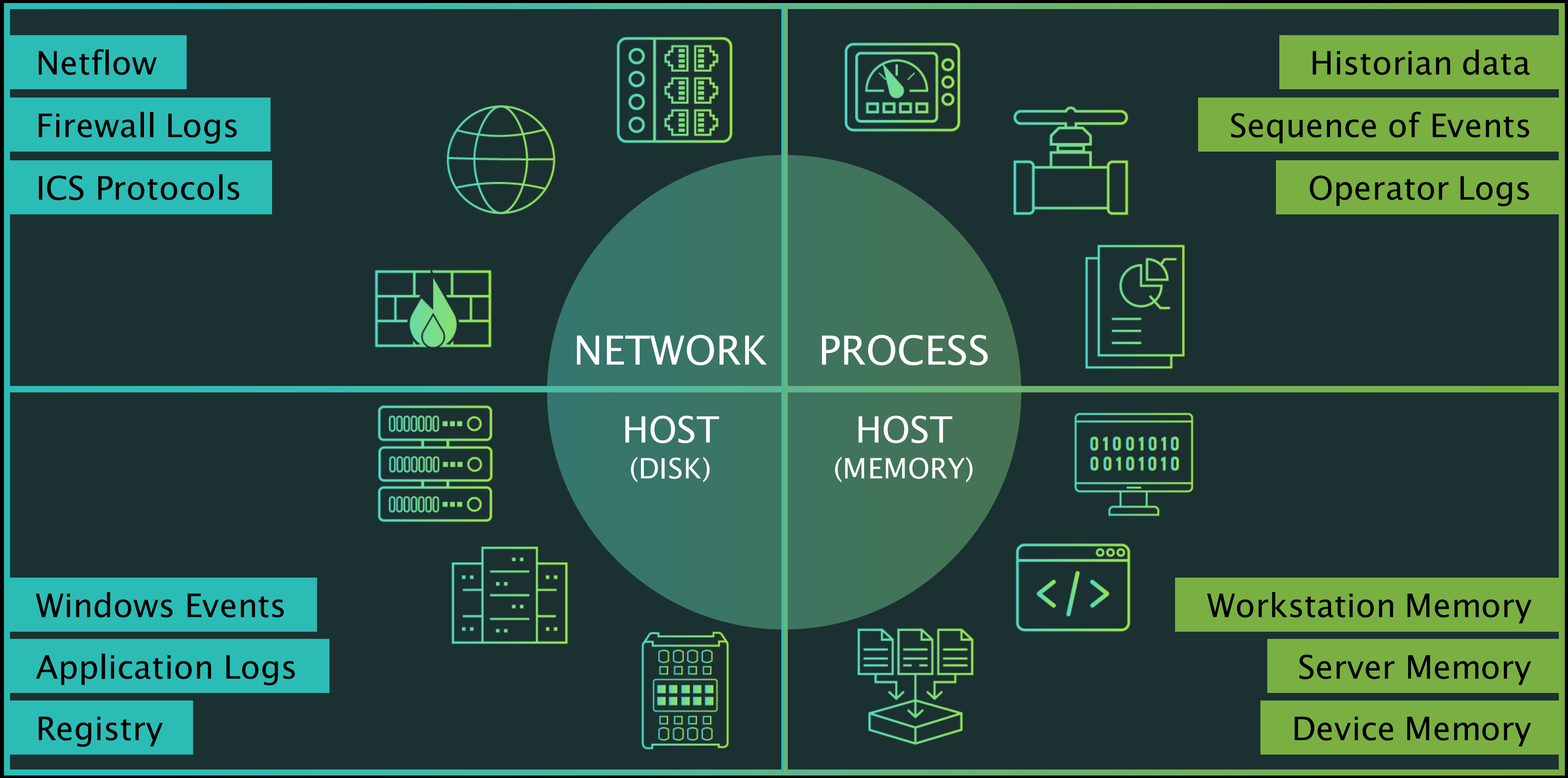
COLLECTION MANAGEMENT FRAMEWORK (CMF)

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

OVERVIEW: COLLECTION DATA SETS



NETWORK

- Netflow
- Firewall Logs
- ICS Protocols

PROCESS

- Historian data
- Sequence of Events
- Operator Logs

HOST (DISK)

- Windows Events
- Application Logs
- Registry

HOST (MEMORY)

- Workstation Memory
- Server Memory
- Device Memory

NETWORK COLLECTION

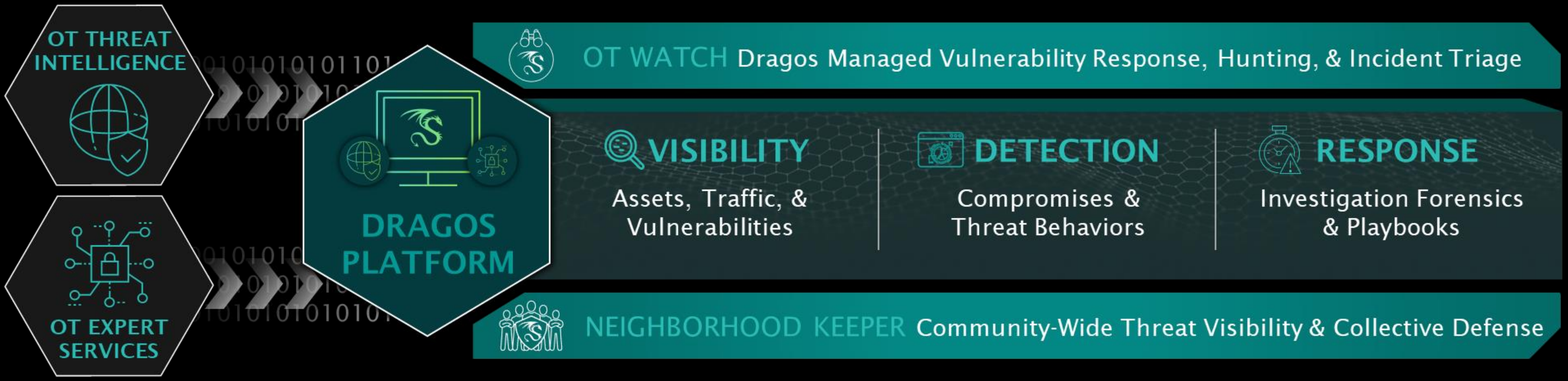
EXPLAIN EACH DATASET AND THEIR RELEVANCE FOR OT IR AND CONTRAST TO IT IR

Passive network collection allows for baselining and investigations

Netflow
Firewall Logs
ICS Protocols
NETWORK

DRAGOS PLATFORM

EXPERTISE INTEGRATED INTO SOFTWARE TO REDUCE OT RISK



OT THREAT INTELLIGENCE

OT EXPERT SERVICES

DRAGOS PLATFORM

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

VISIBILITY
Assets, Traffic, & Vulnerabilities

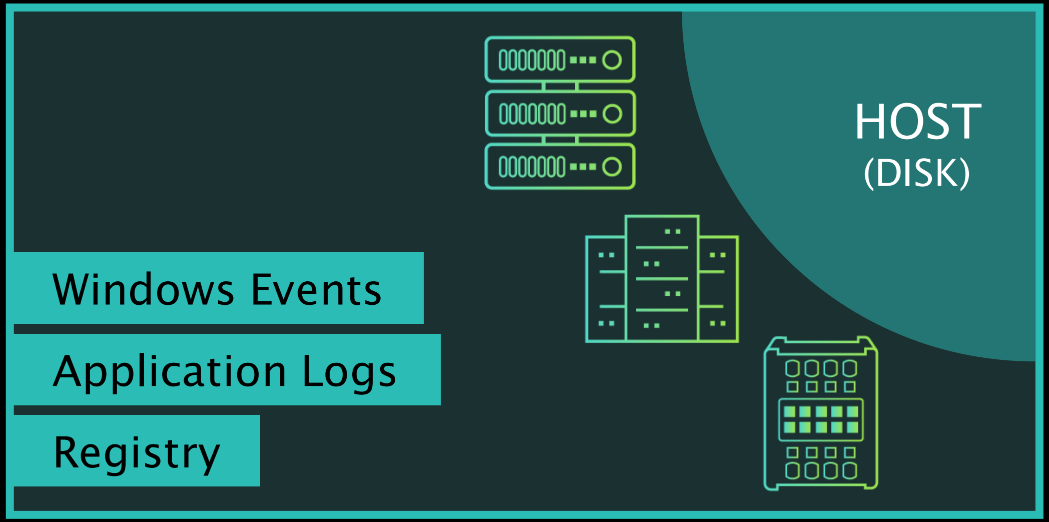
DETECTION
Compromises & Threat Behaviors

RESPONSE
Investigation Forensics & Playbooks

NEIGHBORHOOD KEEPER Community-Wide Threat Visibility & Collective Defense

HOST (DISK) COLLECTION

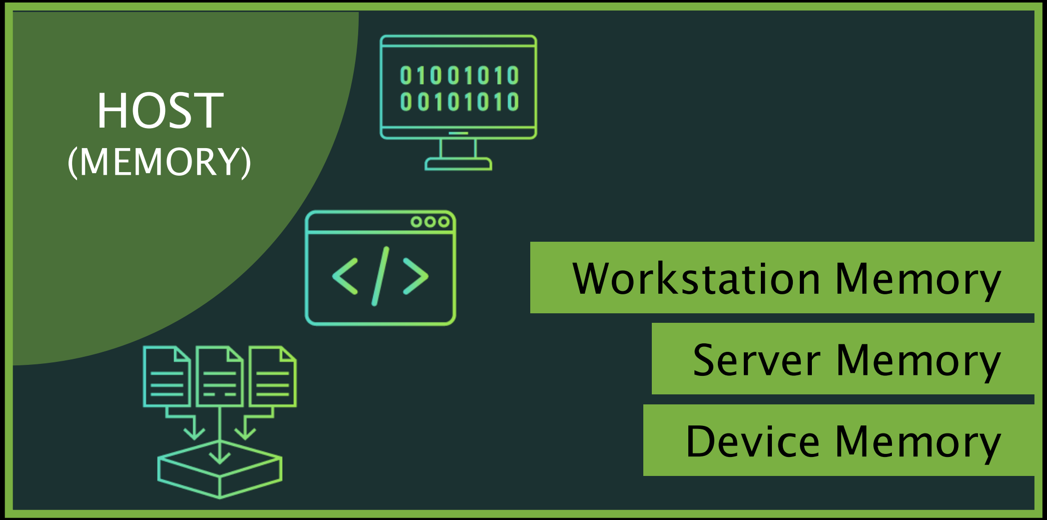
- Automated collection of initial triage data (e.g., registry, system logs)
- Disk images are likely secondary for initial triage, but may be required for forensics
- Acquire data to perform root-cause analysis



HOST (MEMORY) COLLECTION

VOLATILE SYSTEM DATA

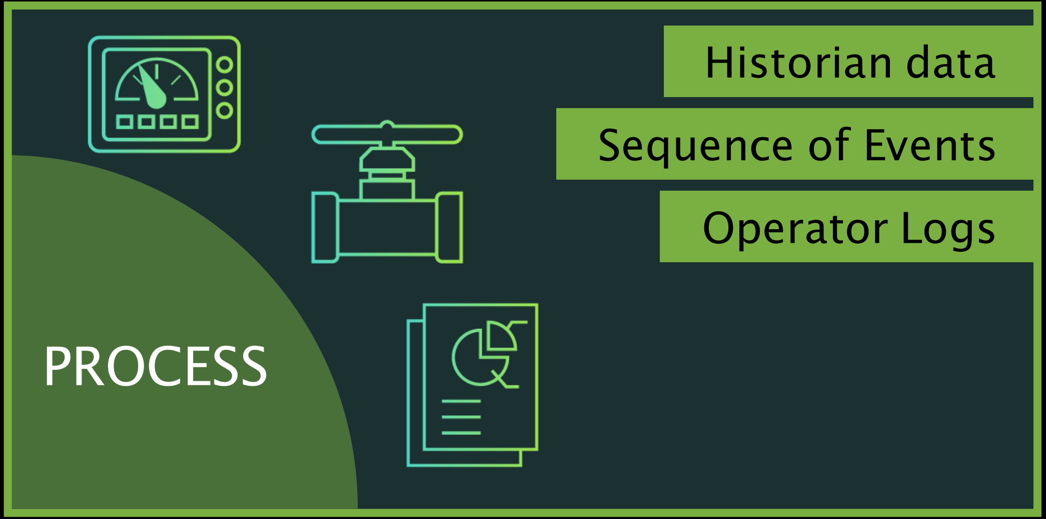
- For quick triage and incident response volatile data (memory) is a valuable source
- Malware and system behavior can be reconstructed, active communications can be captured
- Field devices may not have persistent memory and memory is the only available source
- Beware of legacy operating systems and ensure tool compatibility
- Memory acquisition might impact system operations and need to be tested before



PROCESS DATA COLLECTION

INDUSTRIAL PROCESS AND ITS LOGS

- Process data is often overlooked by IT incident responder
- Historically industrial processes generate and log data (records-keeping, legal, optimization)
- Can be digital, analog, or even verbal
- Likely non-standardized and distributed within the plant/organization
- Acquisition in collaboration with plant personnel
- Provides important information on process anomalies, normal operation and allows correlation



OT INCIDENT RESPONSE PROCESS

INCIDENT REPONSE PROCESS IN OT

PREPARE	INCIDENT RESPONSE TEAM
IDENTIFY	INCIDENT RESPONSE TEAM
CONTAIN	OT OPERATORS
ERADICATE	OT OPERATORS
RECOVER	OT OPERATORS
LESSONS LEARNED	JOINT ACTIVITY

Incident Response workflow, but differences in OT

Ownership of "Contain, Eradicate and Recover" is usually with OT operators

Containment and Eradication might be performed continuously until no further indicators of compromise are found

INCIDENT REPONSE PROCESS IN OT

- PIRCERL provides a good outline for an IRP
  - Utilize each phase as a headline
  - Preface with key information, workflow diagram and contact data
- Be aware of differences in ownership
- More details on each phase of the PICERL process on our next webinar

WEBINAR SUMMARY

SUMMARY

KEY TAKEAWAYS

1 Impact in OT environments can be different to what organizations prepare for in IT

2 Incident Response in OT requires structure and more involved parties than IT IR

3 Data collection requires special consideration and preparation

4 Network visibility and asset inventory are key success criteria for OT Incident Response

THANK YOU

Email: vmccandlish@dragos.com

Email: hvirani@dragos.com