DRAGOS®

Webinar Series: Incident Response for OT Environments

OT INCIDENT RESPONSE IS DIFFERENT

Safeguarding Civilization

INTRODUCTION

Jan Hoff

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

Tim Ennis

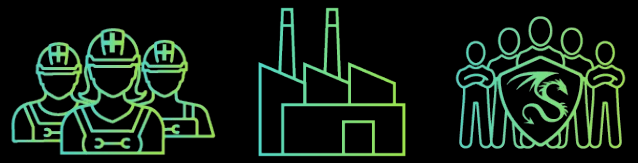
- Senior Industrial Incident Responder
- Based in UK
- 10+ years of industrial experience including safety system engineering

THREE-PART SERIES ON OT IR

Webinar 1
You are not alone

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

Webinar 2
OT IR is different



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

Webinar 3
Effective IR – be prepared

- OT IR Process in depth
- Incident Management Tools and Techniques
- IR Checklist

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

https://hub.dragos.com/on-demand/incident-response-for-ics

IR WHITEPAPERS

EXISTING AND NEW THIS MONTH

- An Executives Guide to OT Cyber Incident Response
  - https://hub.dragos.com/guide-an-executives-guide-to-ot-cyber-incident-response
- Many more resources on
  - https://www.dragos.com
- Incident Response for OT
  - Out Now!

IR FOR OT WHITEPAPER

RELEASED ON 1ST MARCH

- Convergence of IR and IM principles
- Why OT IR is different to IT response
- How to prepare for effective IR for OT

Incident Command and Management

Thinking about non-cyber for a moment

Think of an example of emergency management arrangements being put into action (non-cyber)…

Example: Loss of containment leading to explosion at fuel storage and distribution terminal

Response team coordination, planning, and exercises

https://www.icheme.org/media/14090/buncefield-incident-summary-11-dec-05.pdf

CONVERGENCE OF PRINCIPLES

INCIDENT MANAGEMENT (IM)

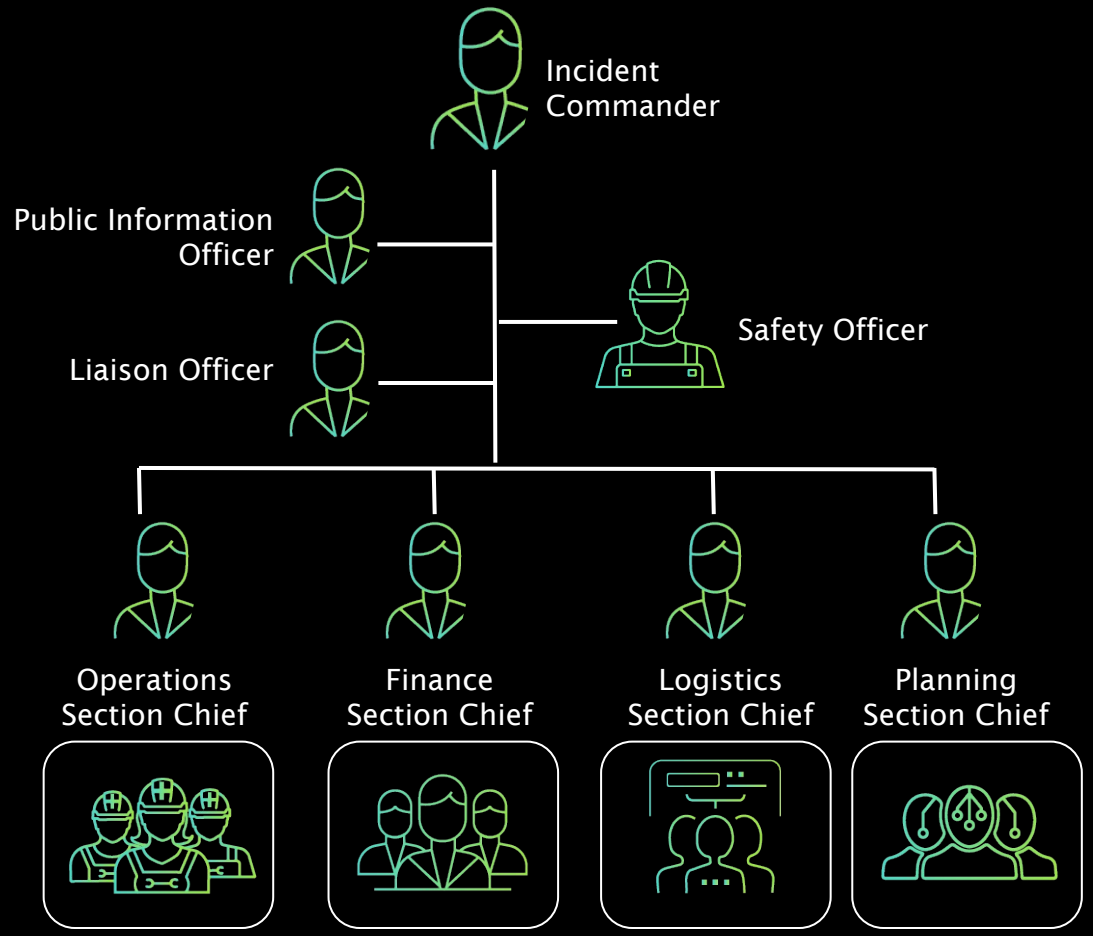
The National Fire Protection Association provides a definition of Incident Management (IM): “the combination of **facilities, equipment, personnel, procedures and communications** operating within a common organizational structure, designed to aid in the management of resources during incidents”.

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

INCIDENT COMMAND SYSTEM

ESTABLISH STRUCTURE PRE-INCIDENT

- 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
- Parties involved in OT incident response are significantly different to IT IR



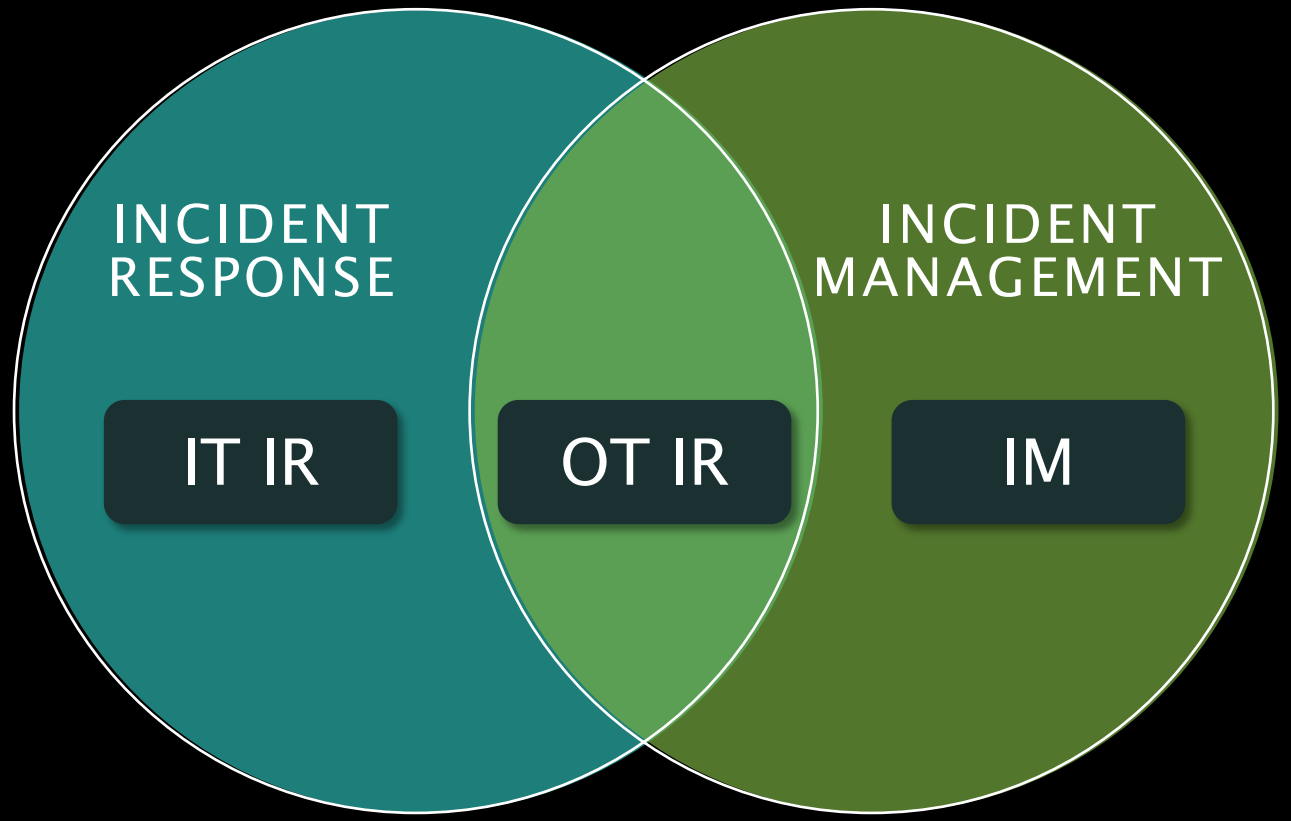
INCIDENT MANAGEMENT (IM)

COMPARISON OF DIFFERENT INCIDENTS

COMPONENT / SITUATION	FIRE	CHEMICAL SPILL	CYBERSECURITY INCIDENT
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

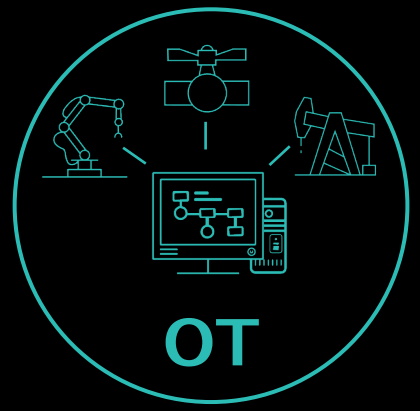
---

OT incident response must consider both domains

DIFFERENCES OF OT IR IN THE SPOTLIGHT

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

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)

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 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

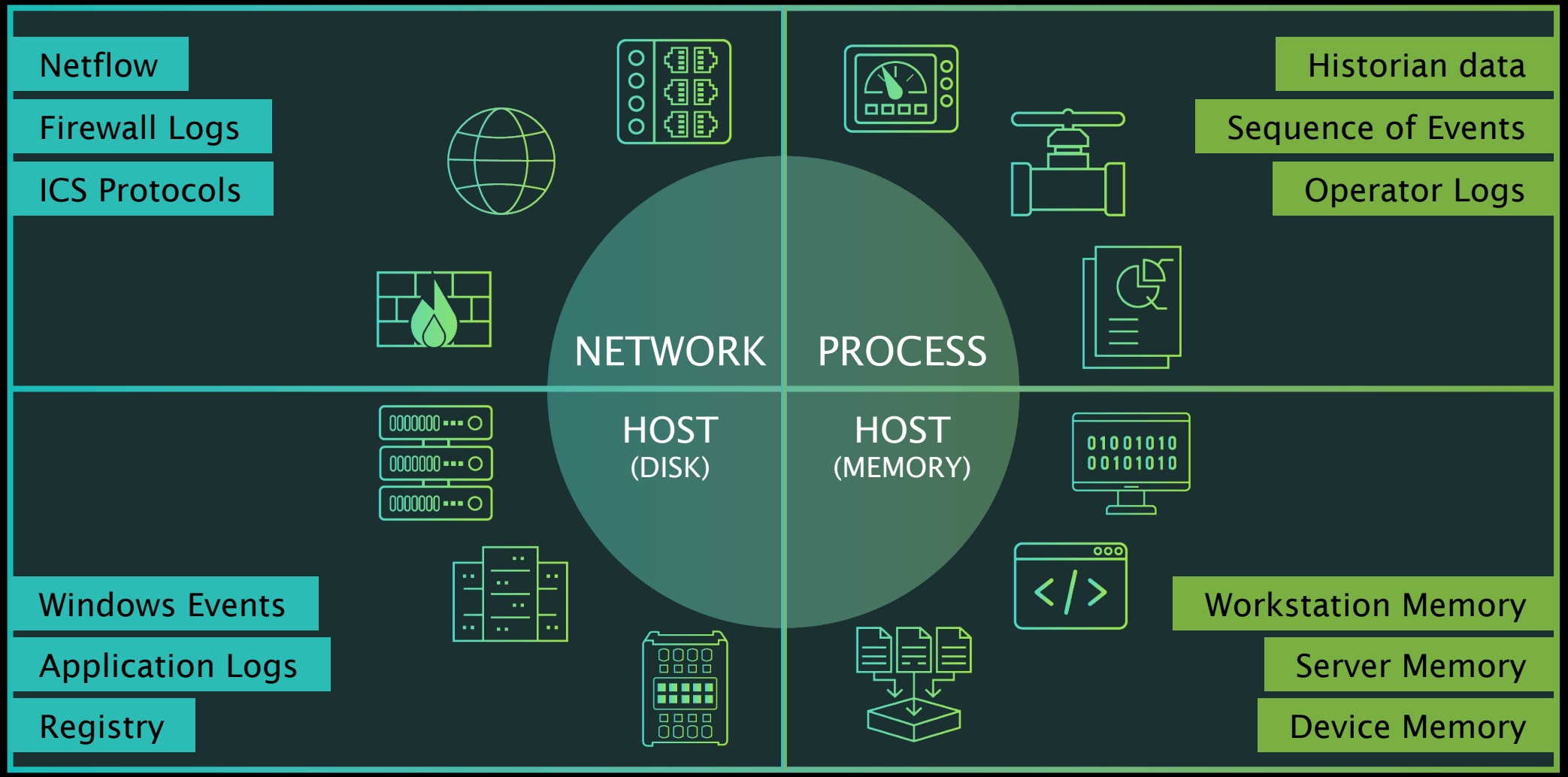
COLLECTION MANAGEMENT FRAMEWORK (CMF)

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

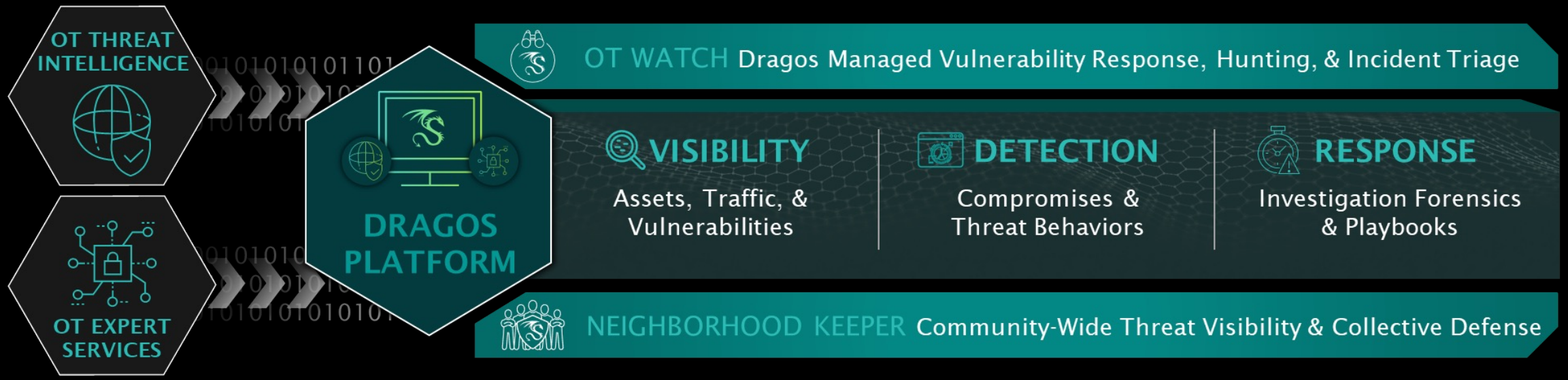


NETWORK COLLECTION

- Network data is not limited to full packet captures
- Identification of anomalies (devices, traffic, volumes, ...)
- Classification and dissection of traffic required
- Passive network collection allows for baselining and investigations
- Encrypted traffic can significantly hinder collection (consider interception)

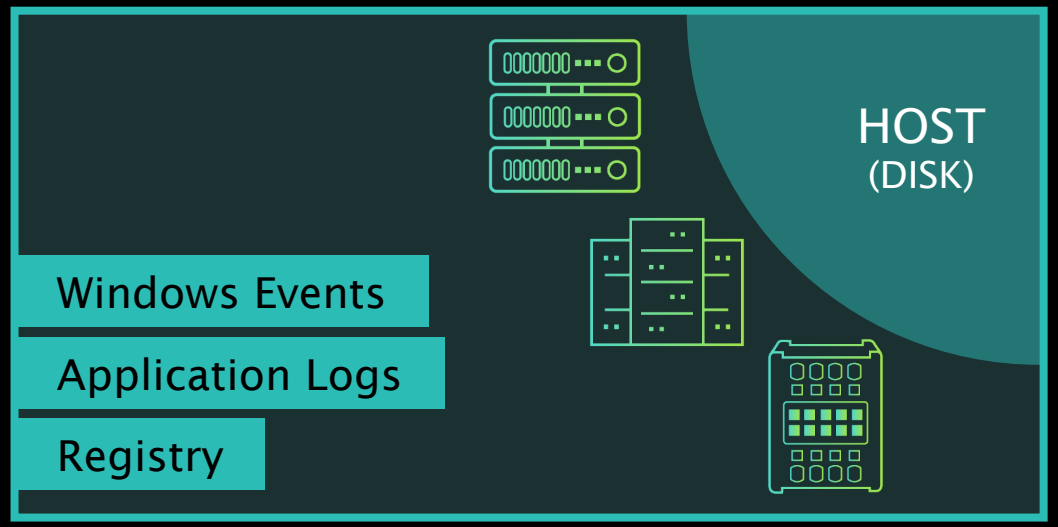
DRAGOS PLATFORM

EXPERTISE INTEGRATED INTO SOFTWARE TO REDUCE OT RISK



HOST (DISK) COLLECTION

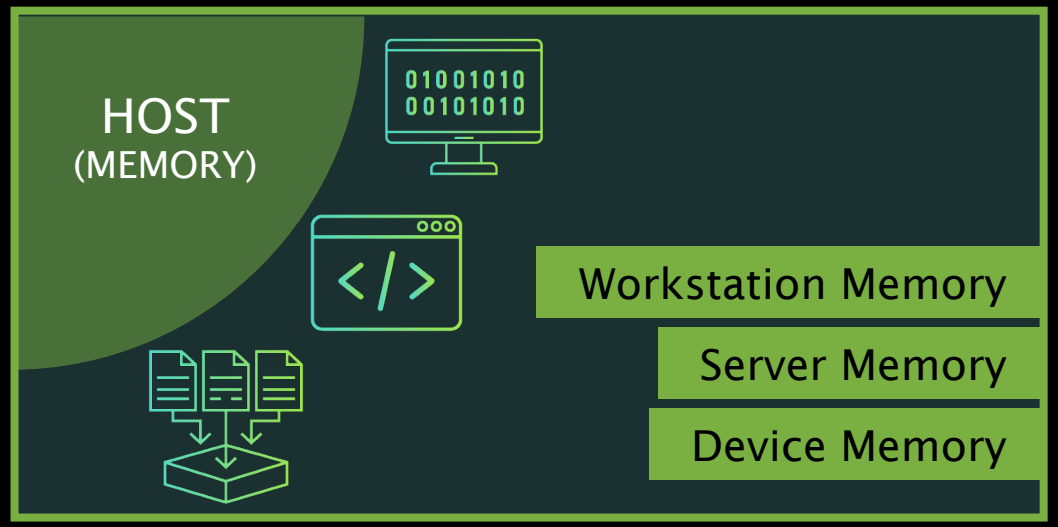
- (Automated) collection of initial triage data (e.g., registry, system logs)
- Value highly dependent on system configuration before a collection is necessary
- ICS systems might utilize proprietary or unknown filesystems and logging
- Disk images are likely secondary for initial triage, but may be required for forensics
- Acquire data to perform root-cause analysis in different phases, if disk is not readily available



HOST (MEMORY) COLLECTION

VOLATILE SYSTEM DATA

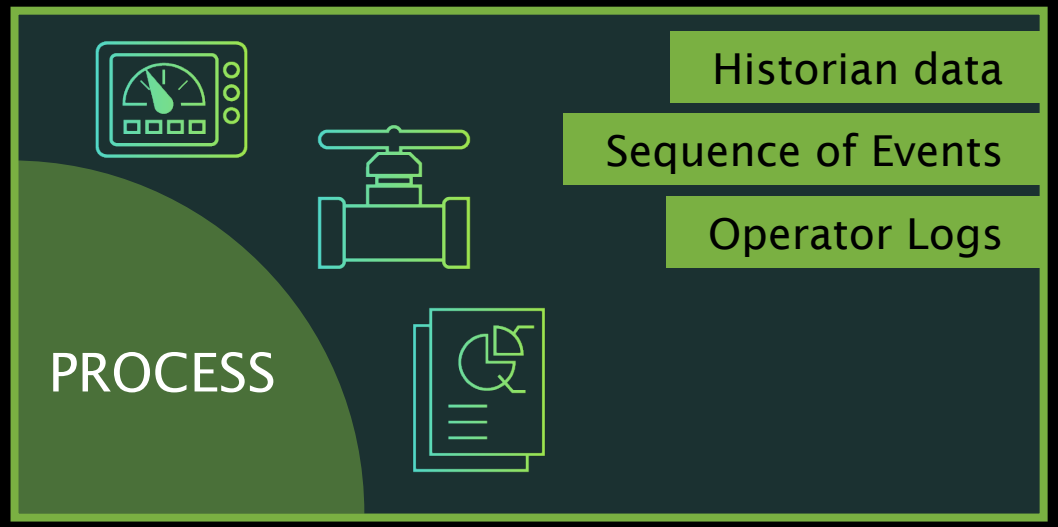
- For quick triage and incident response volatile data (memory) is a valuable source
- Malware and system behaviour can be reconstructed, active communications can be captured
- Field devices may not have persistent memory and memory is the only available source
- Beware of legacy operating systems and 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

IT Incident Response workflow needs OT consideration

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

Containment and Eradication might be continuous

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: tennis@dragos.com

Email: jhoff@dragos.com

RESOURCES

- An Executive's Guide to OT Cyber Incident Response (Whitepaper)
- Dragos Rapid Response Retainer Datasheet
- Dragos Professional Services Brochure
- OT-CERT Membership Datasheet
- Incident Response for ICS Webinar Part 1 (on-demand)