DRAGOS®

Webinar Series: Incident Response for OT Environments

EFFECTIVE IR – BE PREPARED

Safeguarding Civilization

INTRODUCTION

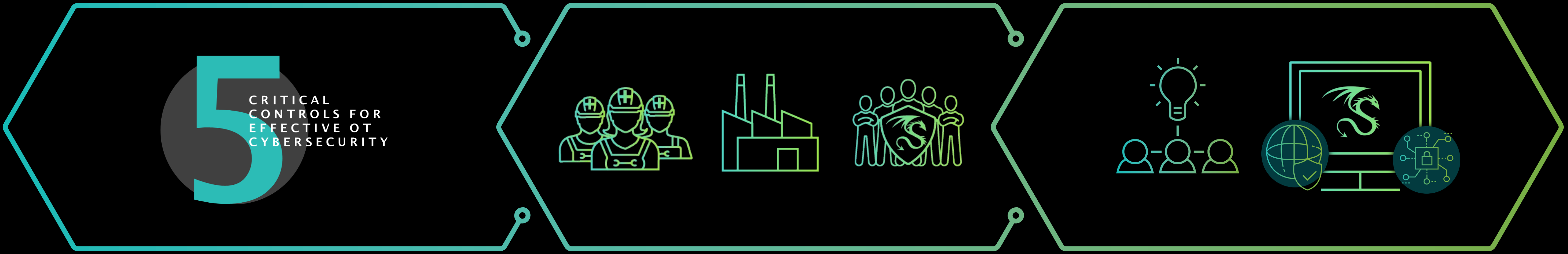
Jan Hoff

- 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

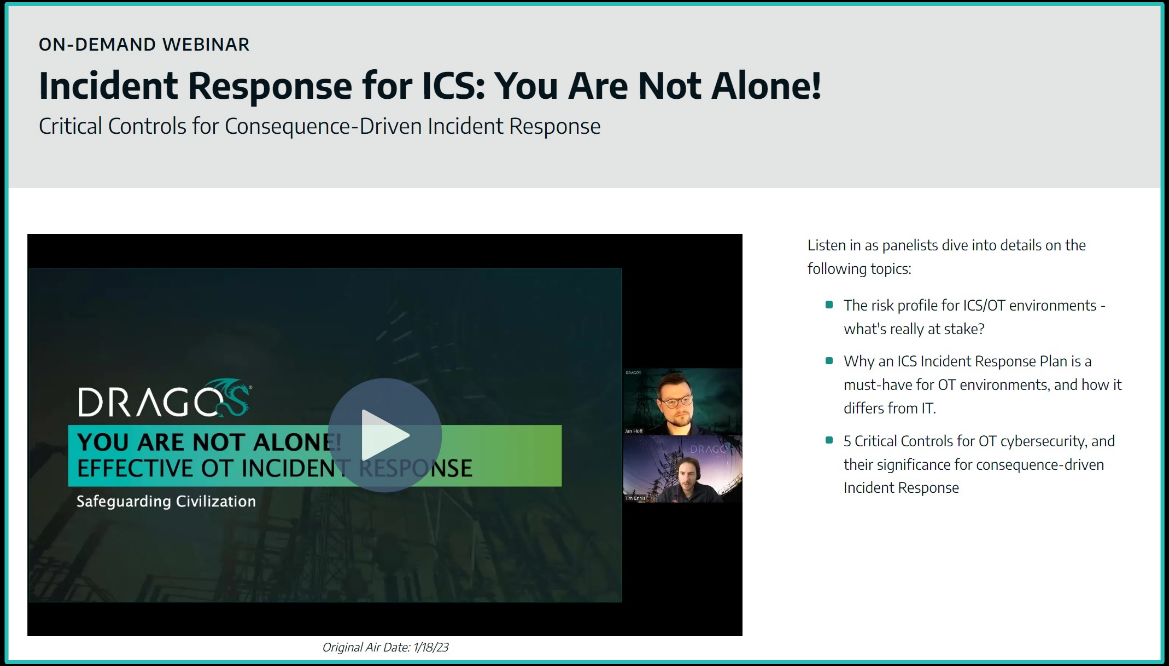
- Difference of incident response in OT and IT
- Incident Management
- IR Data Collection

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 TWO WEBINARS ARE AVAILABLE ON-DEMAND



ON-DEMAND WEBINAR

Incident Response for ICS: You Are Not Alone!

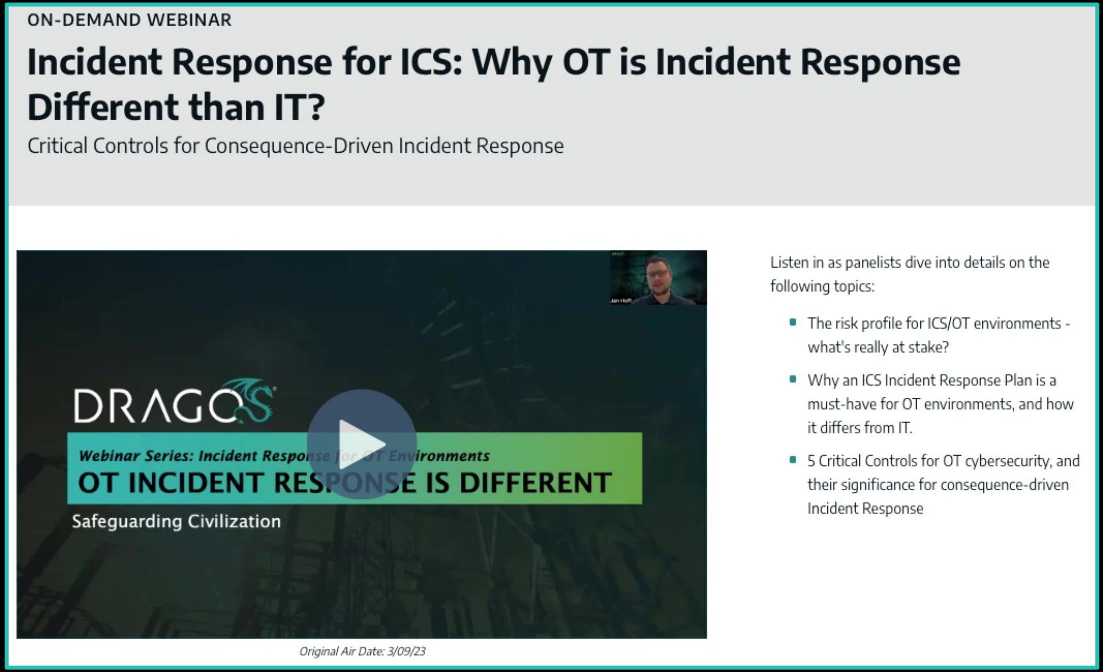
Critical Controls for Consequence-Driven Incident Response

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

Original Air Date: 1/18/23

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


DRAGOS
Webinar Series: Incident Response for OT Environments
OT INCIDENT RESPONSE IS DIFFERENT
Safeguarding Civilization

ON-DEMAND WEBINAR

Incident Response for ICS: Why OT is Incident Response Different than IT?

Critical Controls for Consequence-Driven Incident Response

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

Original Air Date: 3/09/23

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

IR WHITEPAPERS

EXISTING AND NEW THIS MONTH

An Executive's 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

incident response whitepaper

Out Now!

AN EXECUTIVE'S GUIDE TO OT CYBER INCIDENT RESPONSE

DRAGOS

OT Cyber Incidents on the R

Operational technology (OT) risks are on th
threat actors and incidents targeting indus
by the day. Even when organizations inves
OT cybersecurity controls, cybersecurity in
inevitability. Coupled with emerging policy
regulations calling for increased executive
more corporate transparency in reporting c
an appropriate incident response has never
to industrial cyber resilience.

Unfortunately, many ICS/OT organizations stru
recover quickly from incidents in their environ
show that most organizations who tested their
preparedness faced at least some challenges in
response capabilities. What's more, 86% of organ
of visibility across OT networks, that make dete
response incredibly difficult at scale.[1]

As industrial organizations seek to improve thos
the most important considerations they need to k
OT cyber incident response is not a simple add-o
incident response program. The unique nature of
requires an incident response plan and program t
tailored to OT risks.

It takes thoughtful and OT-specific planning, cons
significant expertise to develop an effective and r
response capability.

How Cyber Incident Response i Different in OT

While some of the basics of incident response are u
IT and OT environments, the truth is that OT incide
a whole other level of preparation and readiness con
because OT incident response is called to respond to
with a different approach, and with different experti

[1] Dragos "2021 ICS/OT Cybersecurity Year in Review" Report, dragos.com/

DRAGOS

An Executive's Guide to ICS/OT Incident Response

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

WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Incident Response for Operational Technology (OT)

Preparing for and Responding to OT Security Incidents in Industrial Environments

OT INCIDENT RESPONSE PROCESS

RECAP: INCIDENT REPONSE PROCESS IN OT

PREPARATION	INCIDENT RESPONSE TEAM
IDENTIFICATION	INCIDENT RESPONSE TEAM
CONTAINMENT	OT OPERATORS
ERADICATION	OT OPERATORS
RECOVERY	OT OPERATORS
LESSONS LEARNED	JOINT ACTIVITY

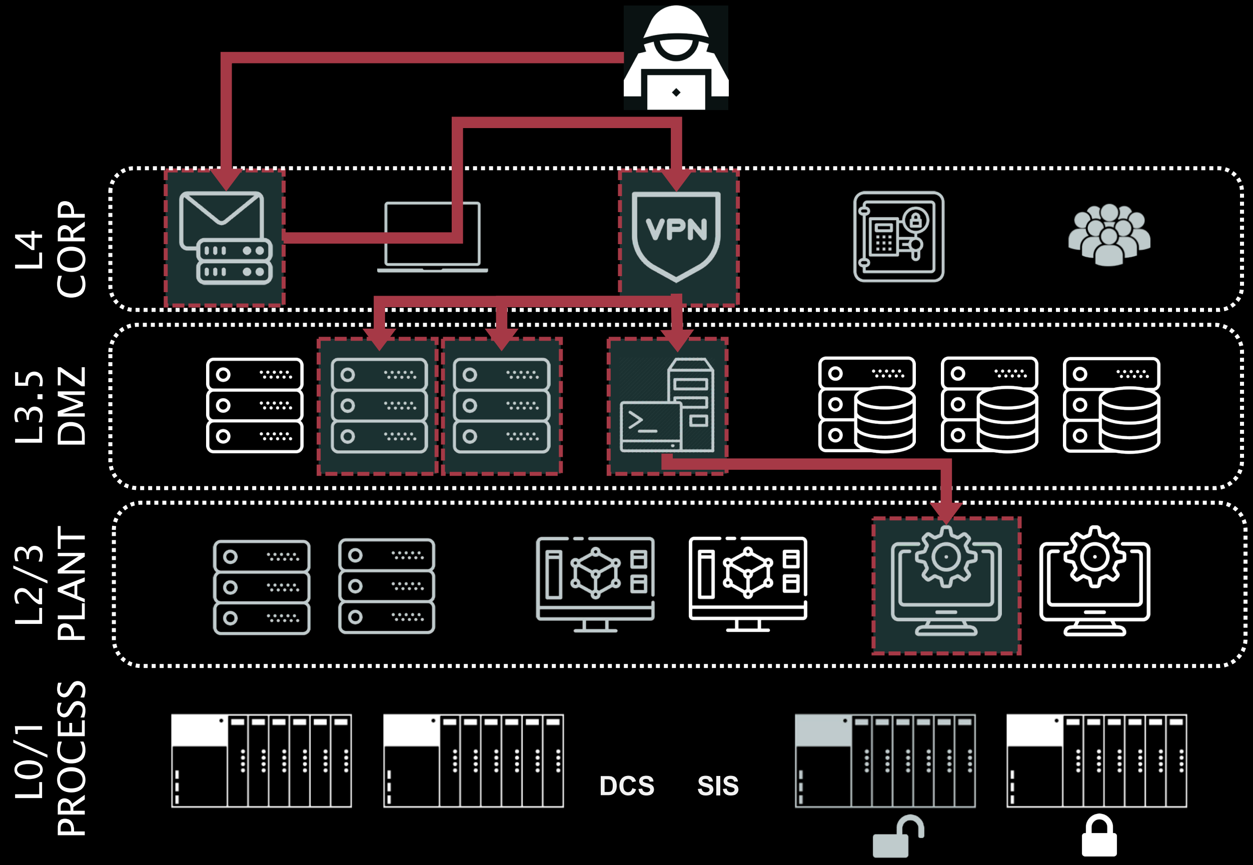
IT Incident Response workflow needs OT consideration

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

Containment and Eradication might be continuous

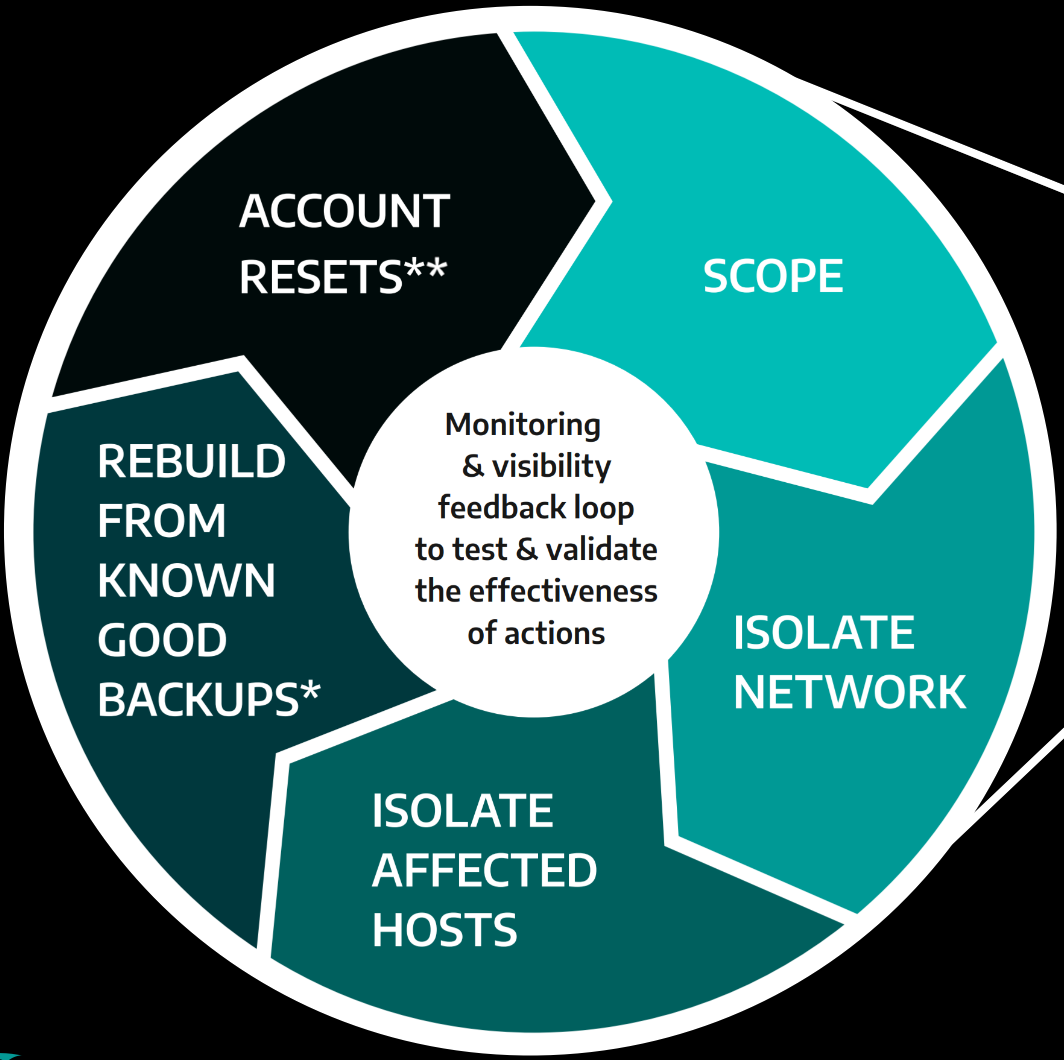
PHASES OF PICERL

PROCESSES OWNED BY INCIDENT RESPONSE



PICERL PHASE	OWNERSHIP
PREPARATION	INCIDENT RESPONSE TEAM
IDENTIFICATION	INCIDENT RESPONSE TEAM
CONTAINMENT	OT OPERATORS
ERADICATION	OT OPERATORS
RECOVERY	OT OPERATORS

OT IR ERADICATION PROCESS


ACCOUNT RESETS**
SCOPE
ISOLATE NETWORK
ISOLATE AFFECTED HOSTS
REBUILD FROM KNOWN GOOD BACKUPS*
Monitoring & visibility feedback loop to test & validate the effectiveness of actions

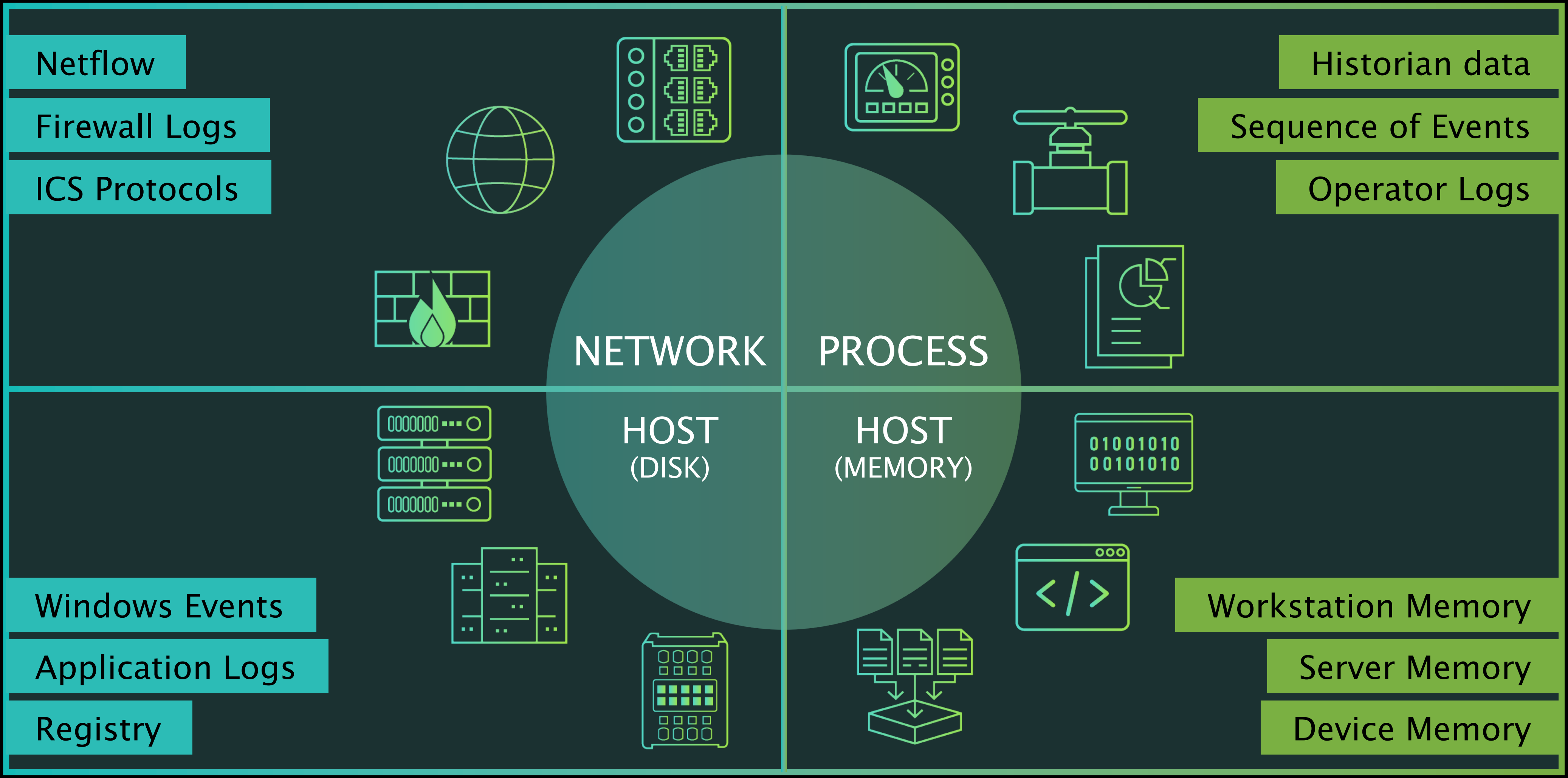
PREPARATION	INCIDENT RESPONSE TEAM
IDENTIFICATION	INCIDENT RESPONSE TEAM
CONTAINMENT	OT OPERATORS
ERADICATION	OT OPERATORS
RECOVERY	OT OPERATORS
LESSONS LEARNED	JOINT ACTIVITY

* Consider restoring from backups instead of only removing malware/adversary artefacts

** Site-/plant-wide account resets likely require careful consideration, planning and third-party support

PREPARING FOR COLLECTION IN OT ENVIRONMENTS

RECAP: COLLECTION DATA SETS FOR OT



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

COLLECTION MANAGEMENT FRAMEWORK (CMF)

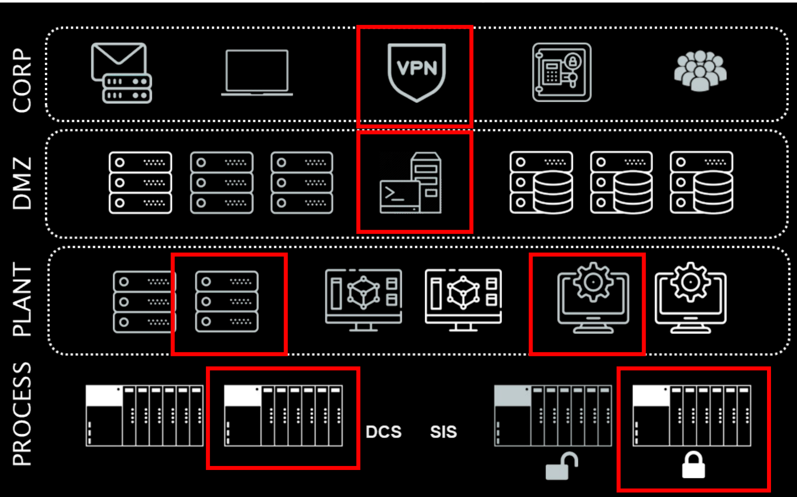
SUSTAINED VISIBILITY INTO YOUR ENVIRONMENT

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

CREATING A CMF (EXAMPLE)

Location / Zone	Asset Type	Data Type	Data Storage duration	Data Storage Location
CORP	Firewall/VPN	Authentication Logs	30 days	IT SIEM
DMZ	Jumphost	EDR logs	10 days	OT SIEM
PLANT	Network Management Appliance	DHCP Logs	180 days / 365 days	Appliance and Dragos Platform
PLANT	Engineering Workstation	Event Logs (Sysmon)	1 day / 365 days	EWS and Log Server
PROCESS	PLC	Syslog	unknown	Device Only
PROCESS	SIS Controller	Passive Network Data	365 days	Dragos Platform



PREPARING FOR IR IN OT ENVIRONMENTS

RECAP – INCIDENT MANAGEMENT COMPONENTS

SITUATION COMPONENT	OT CYBERSECURITY INCIDENT	FIRE	CHEMICAL SPILL
Facilities	• ?	• Control center	• Spill kits • Eye wash stations • Control center
Equipment	• ?	• Fire extinguishers • Fire blankets • Risers	• PPE • Absorbent materials
Personnel	• ?	• Fire crews • Duty officer	• First aid team
Procedures	• ?	• Evacuation, muster	• Containment • Clean-up • Reporting
Communications	• ?	• Fire alarm • All clear • Call to fire Brigade	• Emergency contact number

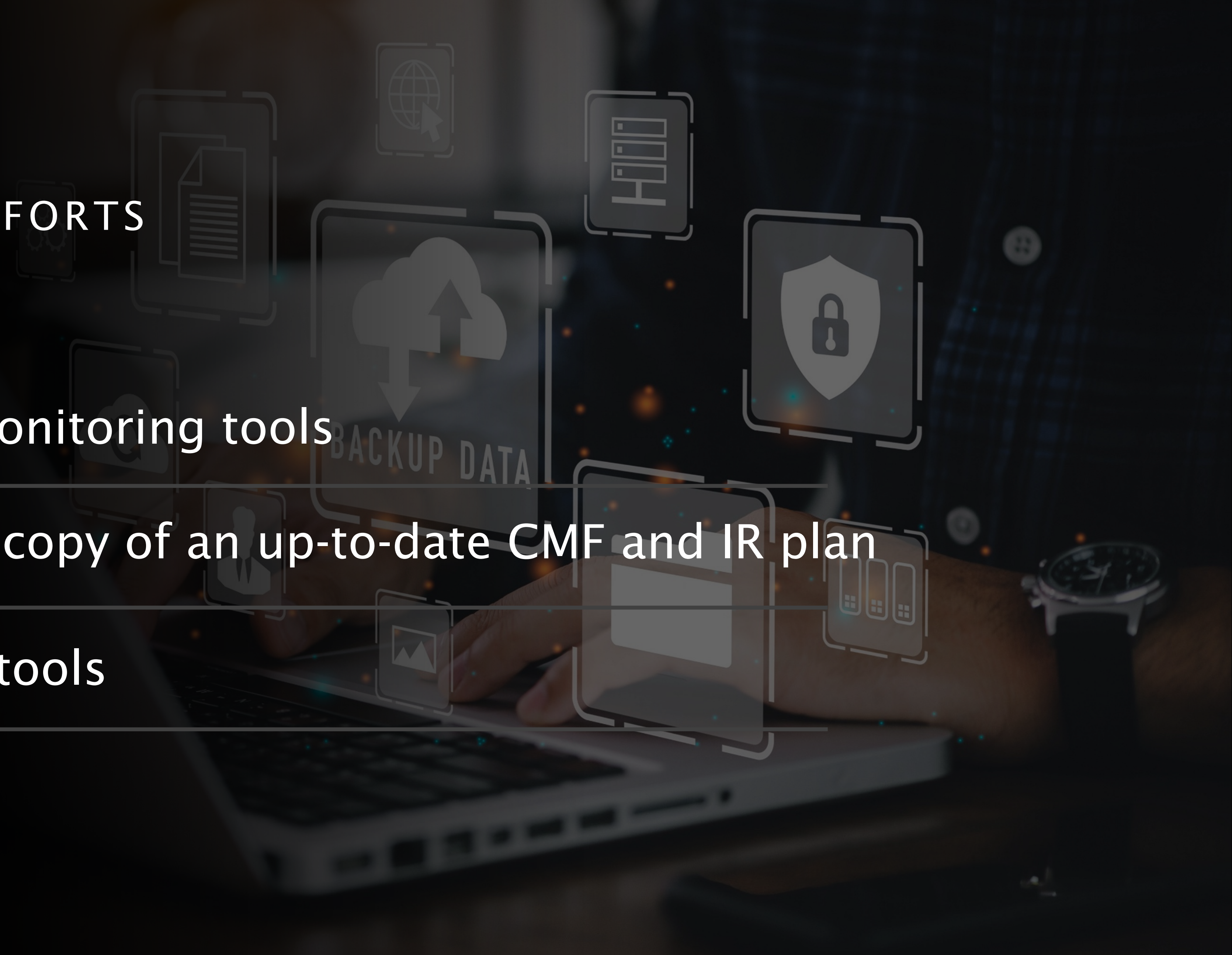
FACILITIES

PHYSICAL LOGISTICS OF OPERATIONALIZING THE TEAMS

1. Collaboration space for Incident Response providers and support teams
2. Incident response line and out-of-band communications
3. IR room with whiteboards
4. Virtual war rooms as required for multinational organizations or remote teams

EQUIPMENT

SUPPLYING RESPONSE EFFORTS



1. Network Security monitoring tools
2. Grab bag including copy of an up-to-date CMF and IR plan
3. Forensic collection tools

PERSONNEL

DEFINING ROLES & RESPONSIBILITIES

1. Defined Incident Response team size and structure
2. Incident Command structure
   (Dedicated Incident Commander appointed, site champions)
3. Relevant training, site, and professional certifications
4. Personal Protection Equipment (PPE)

PROCEDURES

DEFINED, DOCUMENTED, AND REPEATABLE

1. Forensic Collection procedure
2. OT network containment procedure
3. Host isolation procedure
4. Predefined eradication strategies
5. Predefined recovery processes and procedures

COMMUNICATIONS

INFORMED ACTIONS

1. Severity Matrix incorporated into the OT specific IRP

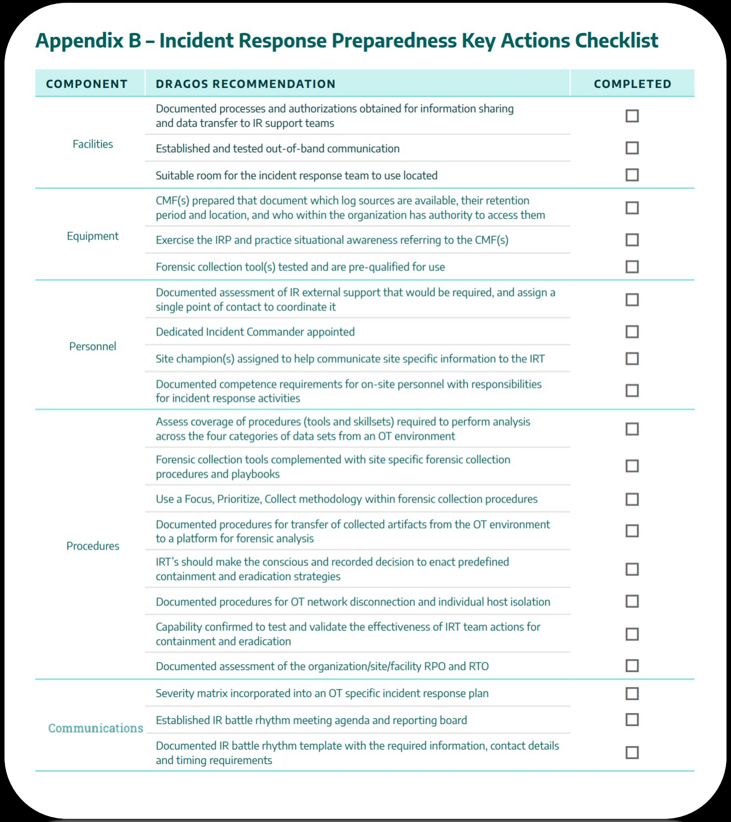
2. Incident Dashboards & Reporting Templates
   Battle rhythm agenda items including orientation to ICS Kill Chain and/or MITRE ATT&CK

3. Templates for incident reporting to external stakeholders

EXAMPLE INCIDENT ACTION TRACKING BOARD

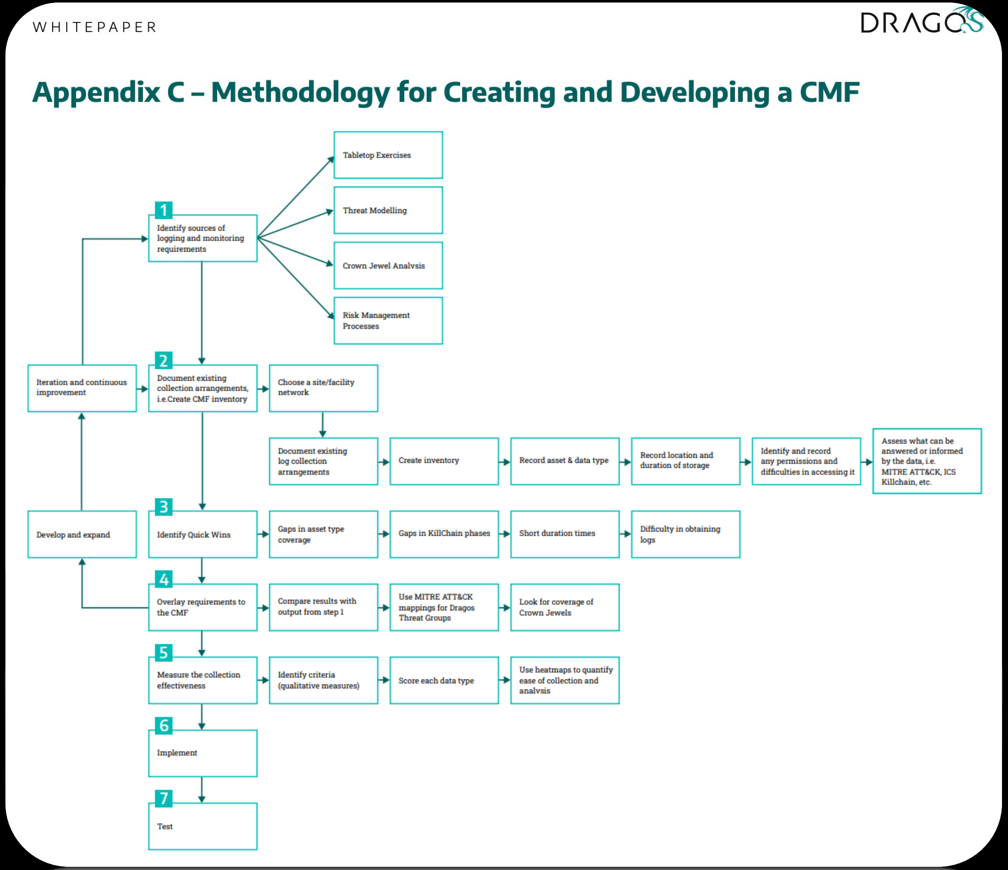
Response Tracking								
Information Received			Actions Assigned				Actions Completed	
Information	Source	Date – Time received	Action	Assigned to	Priority	Date-Time assigned	Action & Result	Date-Time completed
Notification of suspected organizational breach	Government Agency	2022-04-22 1400 UTC	Assemble Incident Response Team	Incident Commander	High	2022-04-22 1530 UTC	IRT comms stood up, incident status report logged in dedicated comms channel	2022-04-22 1730 UTC
n/a	n/a	n/a	Investigate network traffic for new or suspicious connections	OT Security Analyst	High	2022-004-22 1730 UTC	Updated incident status report – no new connections identified from initial analysis. Continuing to analysis of available logs	2022-04-22 2000 UTC
Plant operating status reported as normal.	Ops manager	2022-04-23 0800 UTC	Update incident status report	Duty incident information handler	Low	2022-04-23 0830 UTC	Incident status report updated	2022-04-23 0900 UTC
Threat intelligence report states that vendor X devices are being targeted	Threat Intelligence provider & Information sharing portal	2022-04-23 0900 UTC	Contact vendor and establish communications	System Owner	Medium	2022-04-23 0930 UTC	Vendor contacted and agent assigned to provide support as per SLA.	2022-04-23 1430 UTC

ADDITIONAL RESOURCES



Appendix B – Incident Response Preparedness Key Actions Checklist

COMPONENT	DRAGOS RECOMMENDATION	COMPLETED
Facilities	Documented processes and authorizations obtained for information sharing and data transfer to IR support teams	□
	Established and tested out-of-band communication	□
	Suitable room for the incident response team to use located	□
Equipment	CMF(s) prepared that document which log sources are available, their retention period and location, and who within the organization has authority to access them	□
	Exercise the IRP and practice situational awareness referring to the CMF(s)	□
	Forensic collection tool(s) tested and are pre-qualified for use	□
Personnel	Documented assessment of IR external support that would be required, and assign a single point of contact to coordinate it	□
	Dedicated Incident Commander appointed	□
	Site champion(s) assigned to help communicate site specific information to the IRT	□
	Documented competence requirements for on-site personnel with responsibilities for incident response activities	□
Procedures	Assess coverage of procedures (tools and skillsets) required to perform analysis across the four categories of data sets from an OT environment	□
	Forensic collection tools complemented with site specific forensic collection procedures and playbooks	□
	Use a Focus, Prioritize, Collect methodology within forensic collection procedures	□
	Documented procedures for transfer of collected artifacts from the OT environment to a platform for forensic analysis	□
	IRT's should make the conscious and recorded decision to enact predefined containment and eradication strategies	□
	Documented procedures for OT network disconnection and individual host isolation	□
	Capability confirmed to test and validate the effectiveness of IRT team actions for containment and eradication	□
	Documented assessment of the organization/site/facility RPO and RTO	□
Communications	Severity matrix incorporated into an OT specific incident response plan	□
	Established IR battle rhythm meeting agenda and reporting board	□
	Documented IR battle rhythm template with the required information, contact details and timing requirements	□



WHITEPAPER

Appendix C – Methodology for Creating and Developing a CMF

1
Identify sources of logging and monitoring requirements
Tabletop Exercises
Threat Modelling
Crown Jewel Analvsis
Risk Management Processes
2
Document existing collection arrangements, i.e.Create CMF inventory
Iteration and continuous improvement
Choose a site/facility network
Document existing log collection arrangements
Create inventory
Record asset & data type
Record location and duration of storage
Identify and record any permissions and difficulties in accessing it
Assess what can be answered or informed by the data, i.e. MITRE ATT&CK, ICS Killchain, etc.
3
Identify Quick Wins
Develop and expand
Gaps in asset type coverage
Gaps in KillChain phases
Short duration times
Difficulty in obtaining logs
4
Overlay requirements to the CMF
Compare results with output from step 1
Use MITRE ATT&CK mappings for Dragos Threat Groups
Look for coverage of Crown Jewels
5
Measure the collection effectiveness
Identify criteria (qualitative measures)
Score each data type
Use heatmaps to quantify ease of collection and analvsis
6
Implement
7
Test

WEBINAR SUMMARY

SUMMARY

KEY TAKEAWAYS

1. Preparation is key for OT IR

2. 5 Critical Controls for OT Cybersecurity

3. Develop OT-specific IR plans and procedures

4. Exercise plans, procedures and tooling

THANK YOU

Email: tennis@dragos.com

Email: jhoff@dragos.com