



Webinar Series: Incident Response for OT Environments

EFFECTIVE IR – BE PREPARED

Safeguarding Civilization

INTRODUCTION



Hussain Virani

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



Noah Hemker

- Senior Industrial Incident Responder
- Based in U.S.
- 6+ years of experience safeguarding critical infrastructure and incident response



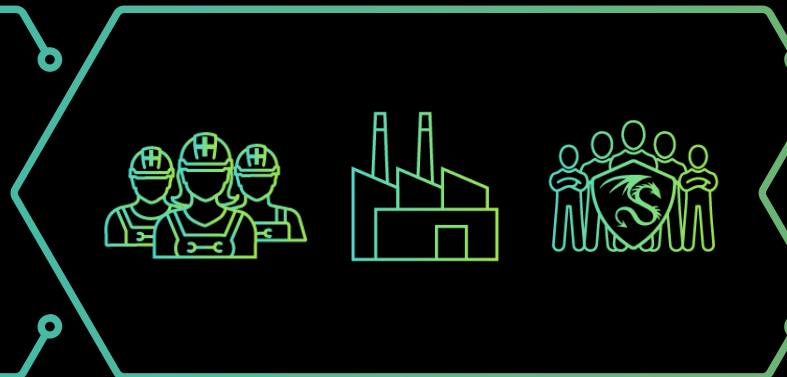
THREE-PART SERIES ON OT INCIDENT RESPONSE

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 INCIDENT RESPONSE

AVAILABLE ON-DEMAND AT DRAGOS.COM

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

[ON DEMAND | YOU ARE NOT ALONE!](#)

ON-DEMAND WEBINAR

Why is OT Incident Response Different than IT?

Part II: Incident Response for ICS Webinar Series



Original Air Date: 3/1/23

Listen in on Part II of our Incident Response for ICS webinar series, where we explore the differences between incident response for OT environments vs IT environments.

In this webinar, Vernon McCandlish, Principal Industrial Incident Responder and Hussain Virani, Senior Industrial Incident Responder, outlines what incident command looks like across the globe, and dives into an in-depth discussion on exactly what's different about incident response in OT environments, and why an ICS incident response plan is a critical step for OT cybersecurity preparedness.

[ON DEMAND | WHY IS OT IR DIFFERENT THAN IT?](#)

EXECUTIVE'S GUIDE TO ICS/OT INCIDENT RESPONSE

DOWNLOAD AT THE LINK BELOW

An Executive's Guide to OT Cyber Incident Response

<https://hub.dragos.com/guide-an-executives-guide-to-ot-cyber-incident-response>

Explore what it takes to build a consequence-driven plan to ensure OT Incident Response readiness

Discover the value of an OT Incident Response Retainer, and how it differs from IT



INCIDENT RESPONSE FOR OT WHITEPAPER

NOW AVAILABLE

Incident Response for Operational Technology







[Incident Response for Operational Technology](#)

Explore the convergence of Incident Response
and Incident Management principles

Which phases of Incident Response are
different in industrial environments, and how
to prepare accordingly



INCIDENT REPOSENSE PROCESS IN OT

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

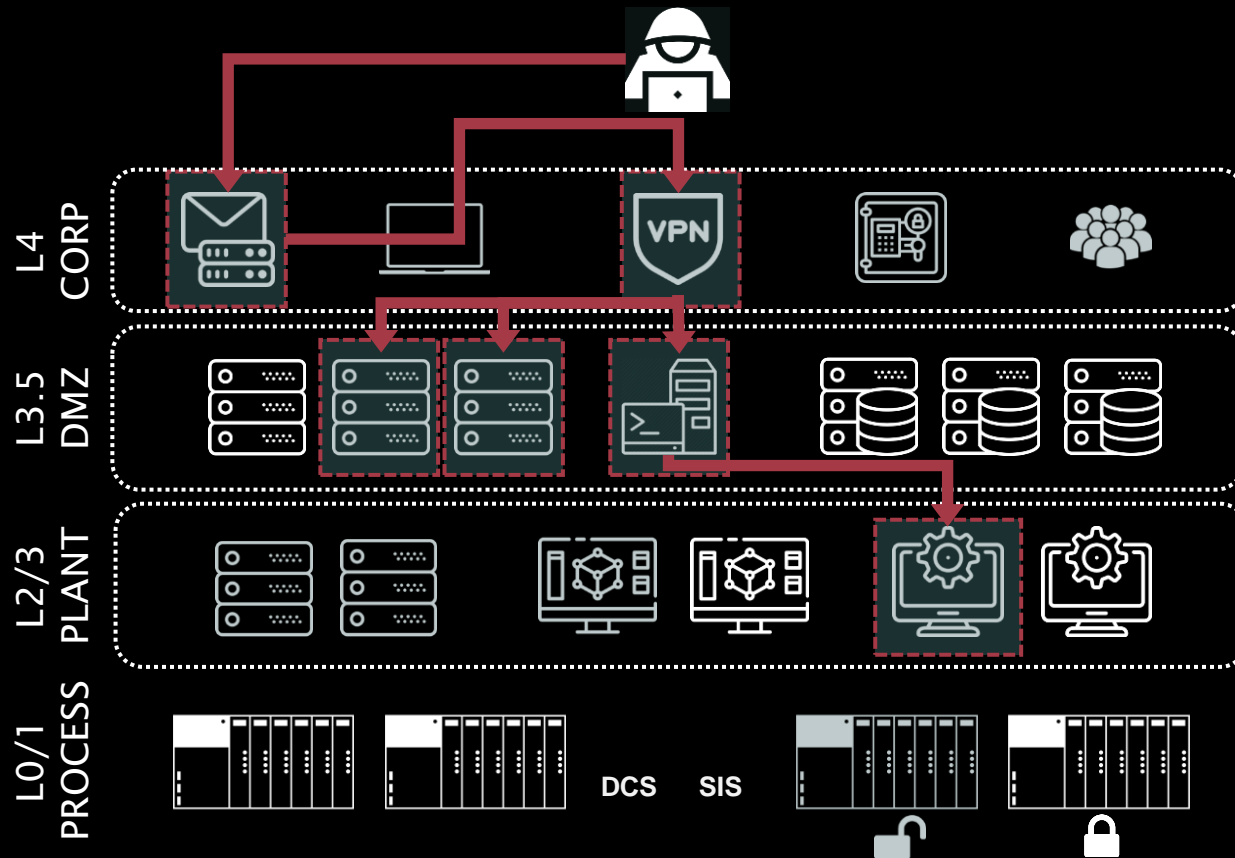
IT Incident Response workflow needs OT consideration

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

Containment and Eradication might be continuous

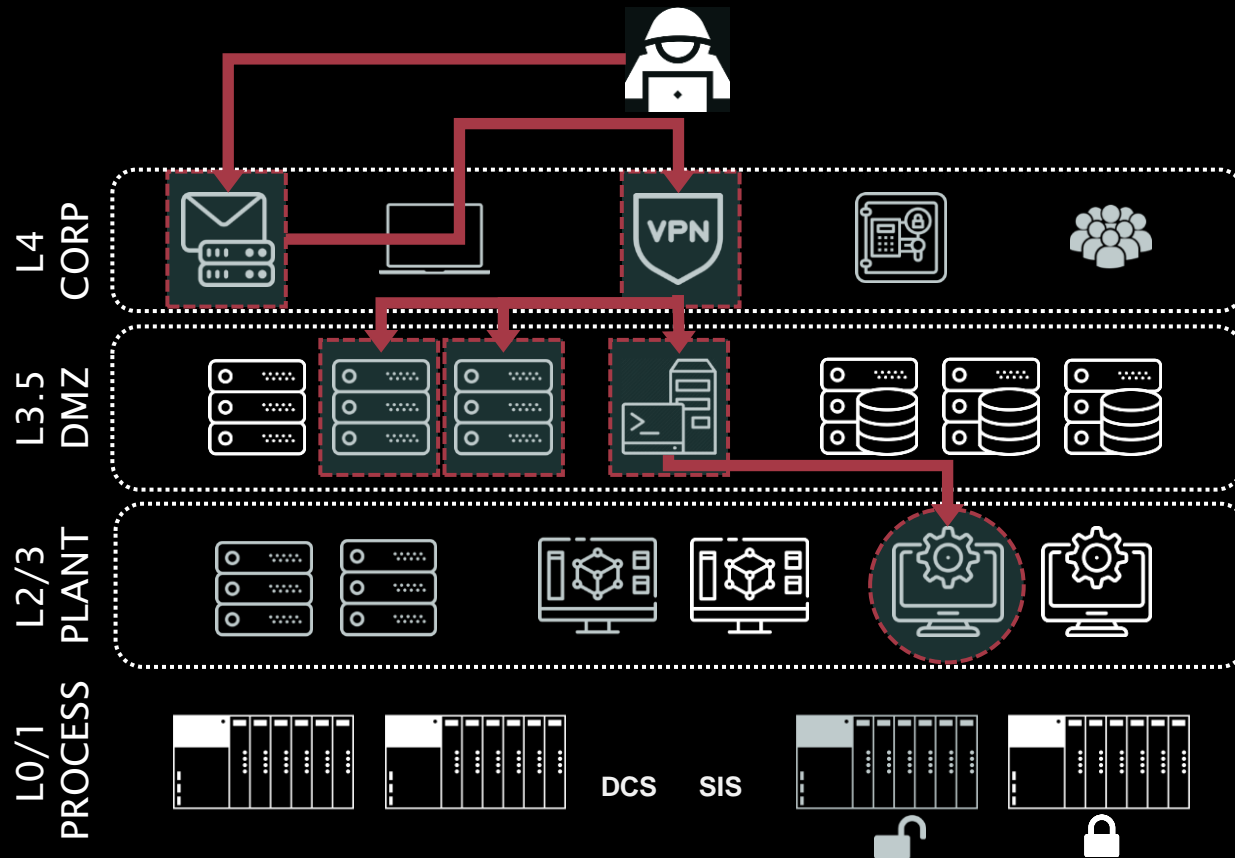
PHASES OF PICERL

PROCESSES OWNED BY INCIDENT RESPONSE



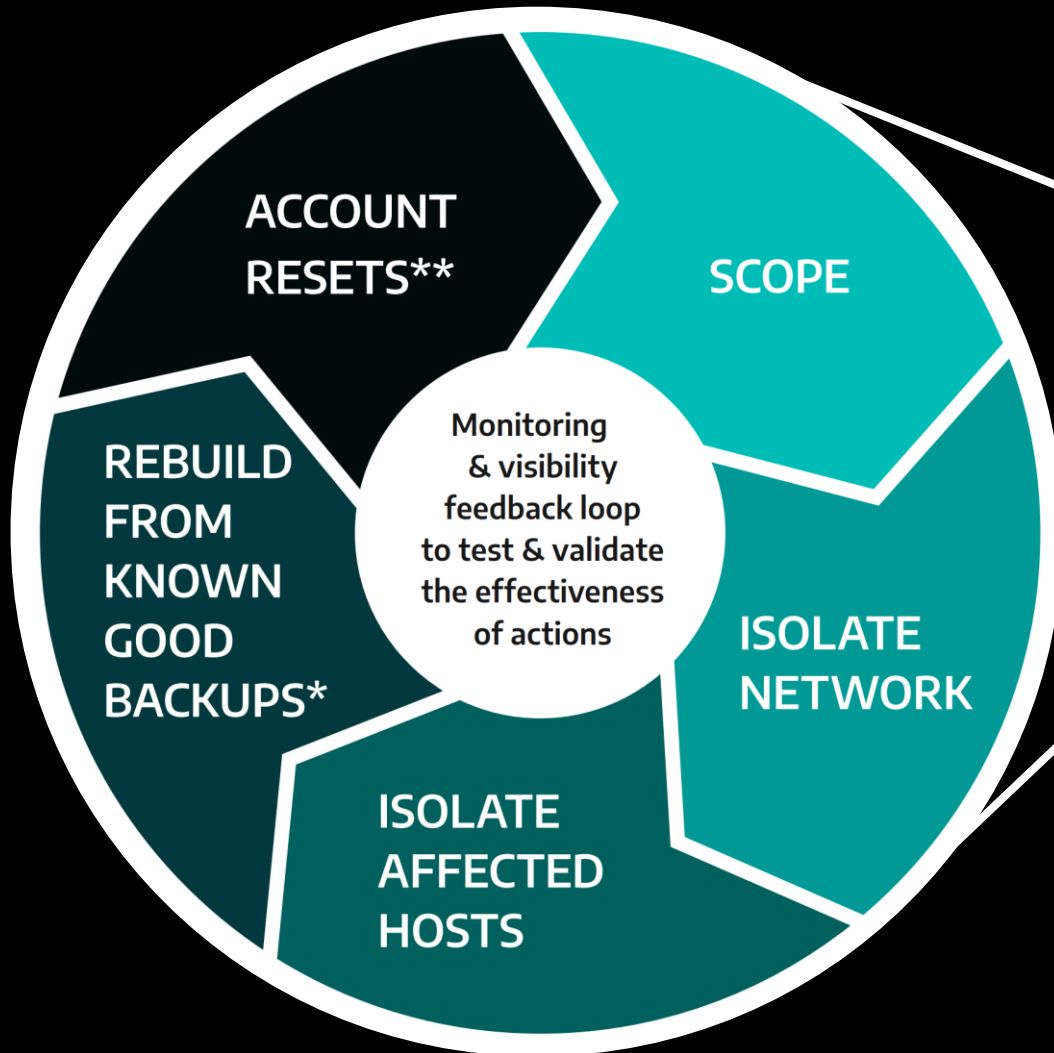
PHASES OF PICERL

PROCESSES OWNED BY ASSET OWNERS & OPERATORS



 CONTAINMENT	OT OPERATORS
 ERADICATION	OT OPERATORS
 RECOVERY	OT OPERATORS

OT IR ERADICATION PROCESS

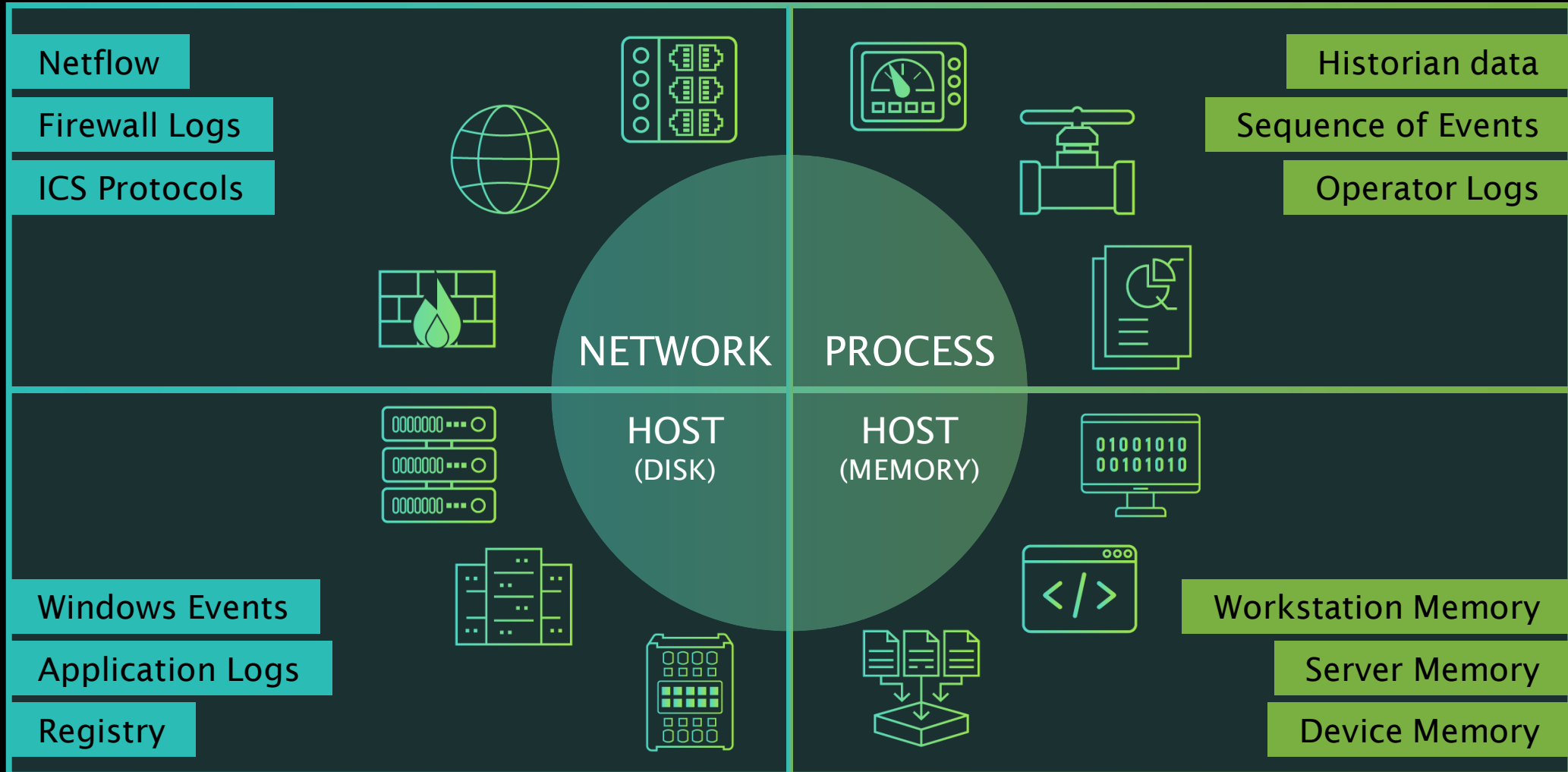


 PREPARATION	INCIDENT RESPONSE TEAM
 IDENTIFICATION	INCIDENT RESPONSE TEAM
 CONTAINMENT	OT OPERATORS
 ERADICATION	OT OPERATORS
 RECOVERY	OT OPERATORS
 LESSONS LEARNED	JOINT ACTIVITY

* 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

RECAP: COLLECTION DATA SETS FOR OT



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

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 Ability to collect volatile media
- 3 Grab bag including copy of an up-to-date CMF and IR plan
- 4 Forensic collection tools
- 5 Write/scratch media
- 6 Proper tech and tooling

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 Common understanding of terminology
- 2 Incident Dashboards & Reporting Templates
- 3 Templates for incident reporting to external stakeholders
- 4 Cadence for communications
- 5 Knowing the intended audience
- 6 Out of band communications

EXAMPLE INCIDENT TIMELINE

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	2022-04-22 1730 UTC	Updated incident status report - no new connections identified from initial analysis. Continuing to analysis 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

KEY TAKEAWAYS

PREPARE AHEAD FOR A CRISIS

OT OPERATORS ARE VITAL FOR IR

COLLAB ACROSS BUSINESS UNITS

5 CRITICAL
CONTROLS FOR OT
CYBERSECURITY

ADDITIONAL RESOURCES:

[DRAGOS.COM/SERVICES/INCIDENT-RESPONSE/](https://dragos.com/services/incident-response/)

[5 CRITICAL CONTROLS FOR WORLD-CLASS OT CYBERSECURITY](#)



Email: hvirani@dragos.com



Email: nhemker@dragos.com

URGENT INCIDENT RESPONSE

North America
+1 410-618-0135

EU & United Kingdom
+44 14830967867

Australia
+61 3 4422 2774

For non-emergency requests, email us at ir@dragos.com