# Dragos 2026 OT Cybersecurity Report

## Year in Review, Manufacturing Focus

DRAGOS

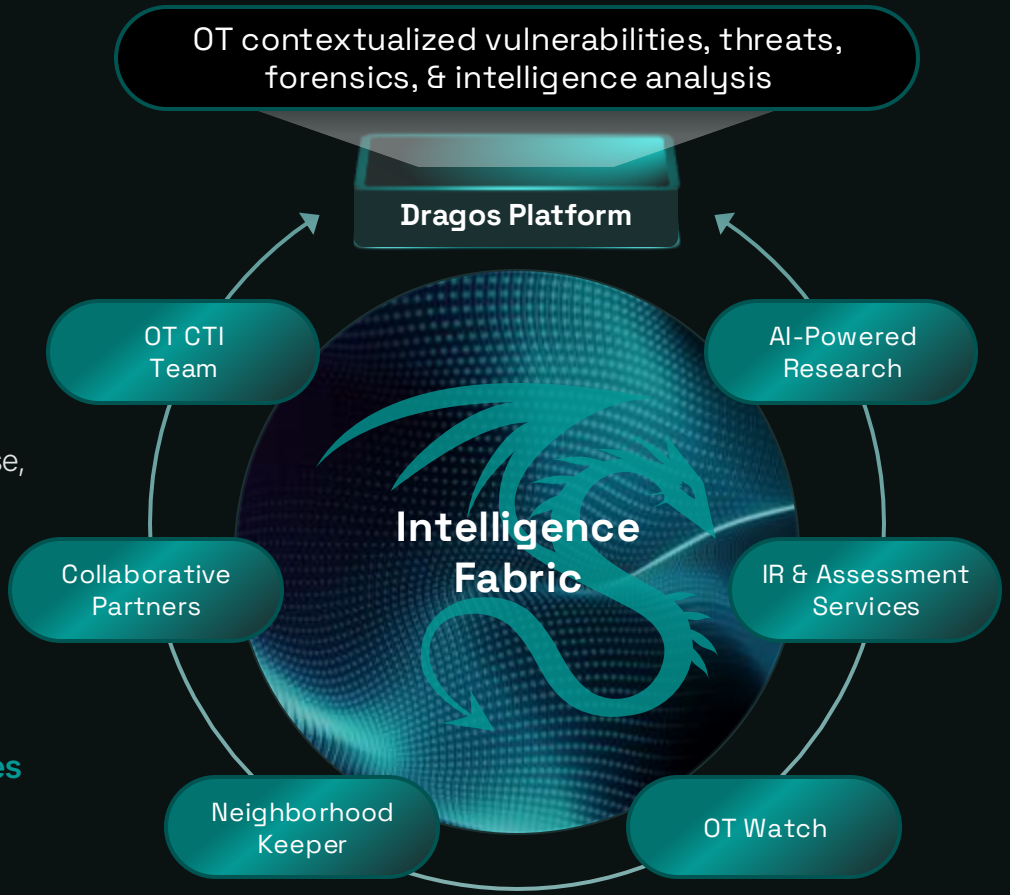
# The Dragos Intelligence Fabric

Powers the Platform, informs our services, and differentiates Dragos from competitors

**Expansive Knowledge Base of OT Cyber Insights**
A decade of frontline adversary research, incident response, vulnerability analysis, and 5 petabytes of daily telemetry

**Builds Continuously with Research and Real-World Feedback**
New telemetry, fresh investigations, expert-driven hunt hypotheses, analyst validation, and partner collaboration.

**Delivering Clear OT Context and Actionable Priorities**
Flows directly into the Dragos Platform, providing context, relevance, and prioritization.



# Middle East Developments

## Cyber Attacks

### What is going on

- Considerable amount of GPS attacks around the Strait of Hormuz
- Reported Adversarial activity and data exfiltration in LNG companies
- BAUXITE claimed Jordanian wheat silo compromise
- MuddyWater increased activity against the US. Israel (historically targeting the EU, but it's shifting focus to the US and Israel)
- Hacktivism is on the rise (claims have doubled since the start of the war)

### How to be ready

- Expect Stage1 Activity
  - Primary Operational Risk
- Adversaries Will Target Exposed ICS/OT Assets
  - Eliminate or lock down internet-facing devices
- Prepare for Manual Operations
  - Ensure you have offline tested backups
- Expect & Accept Hacktivist Noise
  - DDoS campaigns, exaggerated claims of operational disruption

# Background

Point 1

Kinetic Attacks begin in Iran on Feb 28, 2026

Point 2

How cyber was used during the operations

Point 3

Internet degradation in Iran

Point 4

Retaliation attacks


# 9th Annual Dragos Year in Review

**New specialized threat groups** with diverse approaches lower the barrier for established groups to achieve OT impact

Control loop mapping demonstrates **adversaries understand industrial operations at the process level**

Shift from reconnaissance to **attempted operational effects throughout 2025**

**Ransomware incidents are OT** by consequence despite frequent oversimplification and mislabeling

**Organizations still struggle to implement basic controls**, preventing an effective response when attacks occur

# Dragos Identifies 3 New Threat Groups

Of the 26 threat groups tracked by Dragos, 11 were active in 2025

# New: SYLVANITE

Rapid exploitation broker enabling VOLTZITE access to critical infrastructure

SINCE 2025

Sy

- Exploited Ivanti VPN vulnerabilities within 48 hours of disclosure
- Extracted Active Directory credentials
- Installed persistent web shells on F5 devices
- Handed off access to VOLTZITE or deeper intrusions

## Targets:

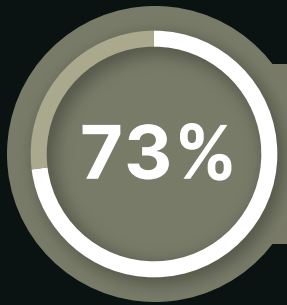

Electric Power


Water


Oil & Gas


Manufacturing


Public Administration




of Dragos IR cases involved active exploitation or credential reuse of VPN/jumphosts

**Overlaps with:** UNC5221, UNC5174, UNC5291, UNC3236, HOUKEN, Red Dev 61, CL-STA-0048, UTA0178

# New: AZURITE

Theft of operational information, long-term access enablement

SINCE 2021

Az

## What Dragos Observed in 2025

- Compromised SOHO routers to build proxy infrastructure across multiple countries
- Exfiltrated OT network diagrams and operational data
- Accessed engineer workstations through compromised edge devices
- Maintained persistent access for extended periods using living off the land techniques

## Targets:

Manufacturing | Defense | Automotive | Electric | Government | Oil & Gas

**Overlaps with:** Flax Typhoon, Ethereal Panda, UNC5923, Raptor Train, Red Dev 54

# New: PYROXENE

Cross-domain access enabling movement from IT into OT networks

SINCE 2025

Py

## What Dragos Observed in 2025

- Created fake LinkedIn profiles posing as aerospace recruiters
- Used stolen credentials to access Citrix and VMware systems
- Compromised defense contractor websites to target employees
- Moved from corporate IT into operational technology networks

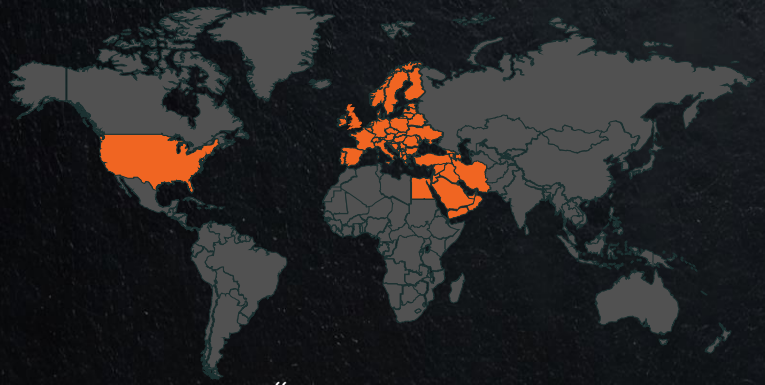
## Targets:

Transportation | Logistics | Aerospace | Aviation | Utilities | Manufacturing

**Overlaps with:** APT35, Tortoiseshell, UNC1549, Imperial Kitten, assessed by the U.S. Government to be aligned with the Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC)

# THREAT GROUP: BAUXITE (associated with CyberAv3ngers)

## ICS ACTIONS AGAINST EASY-TO-ACCESS TARGETS



"Between November 2023 and January 2024, CyberAv3ngers targeted U.S.-based Unitronics PLC devices used in multiple critical infrastructure industries, including the WWS Sector, likely in four separate waves of cyberattacks. The actors compromised at least 75 devices, including at least 34 in the WWS Sector in the United States."

***-- Cybersecurity & Infrastructure Security Agency***

- Oil & Natural Gas
- Electric
- Water & Wastewater
- Food & Beverage
- Chemical Manufacturing

# BAUXITE

Direct ICS manipulation and destructive operations targeting internet-exposed operational technology

2023

Bx

## What Dragos Observed in 2025

- Threatening email campaign targeting cybersecurity vendors, ICS researchers, and media
- Deployed two wiper malware variants against Israeli targets during Iran-Israel conflict
- Continued Stage 2 activity: Direct manipulation of internet-exposed HMIs, PLCs, and industrial devices

## Targets:

Critical infrastructure globally, with focus on organizations with internet-exposed OT devices

**Overlaps with:** CyberAv3ngers (hacktivist persona)

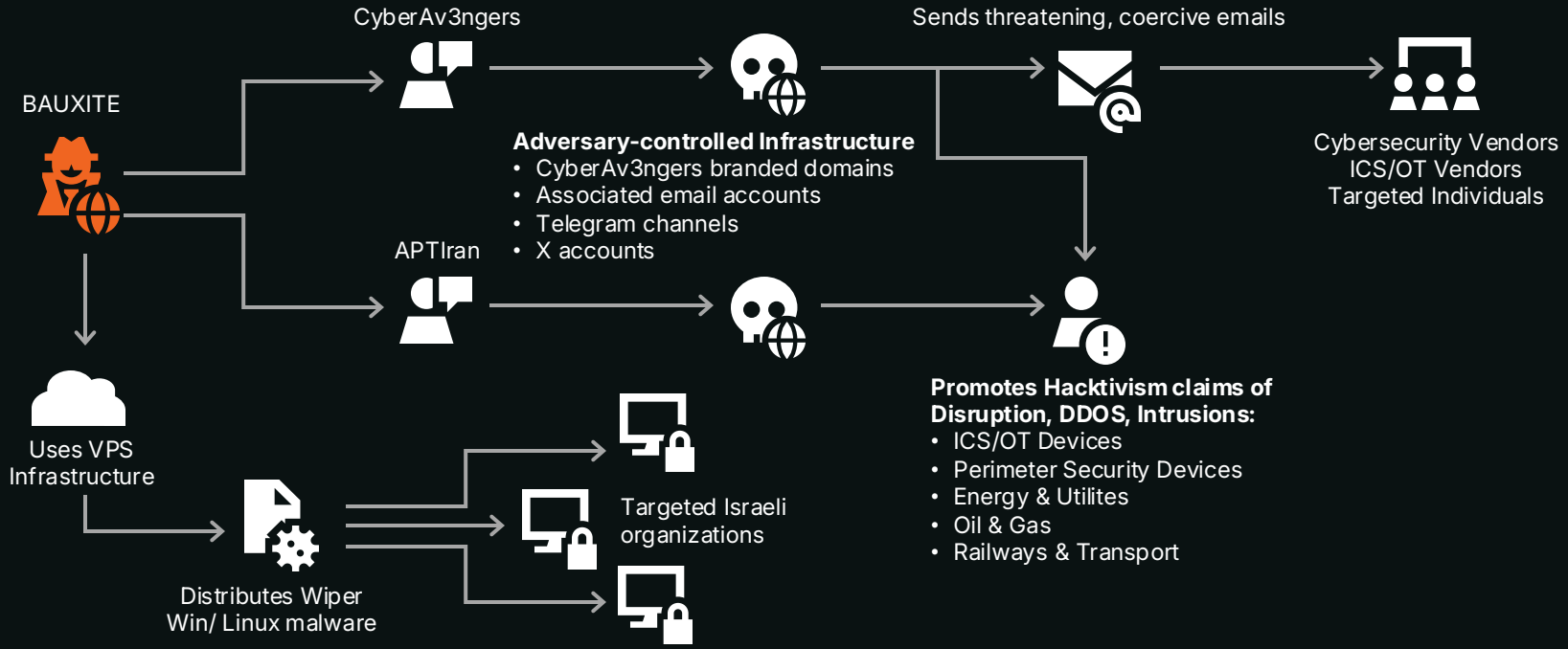
# BAUXITE 2025 Activity

01

Psychological, Influence Operations

02

Destructive attacks against Israeli targets



# Root Cause Analysis Problem

You can’t determine root cause if you lack monitoring BEFORE the incident.

**30%**

of IR cases began with “something is wrong”

**82%**

lack criteria for when operational anomalies trigger cyber investigation

*Is it cyber?*
*Is it mechanical?*
*Is it operator error?*

## Many attacks don’t look like cyber

They’re just operational misuse of legitimate equipment

**VOLTZITE** config dumping looks like troubleshooting

**KAMACITE** VFD scanning looks like standard system enumeration

# AI Compounds the Visibility Problem

Establish visibility BEFORE deploying AI or risk creating exponentially greater blind spots.

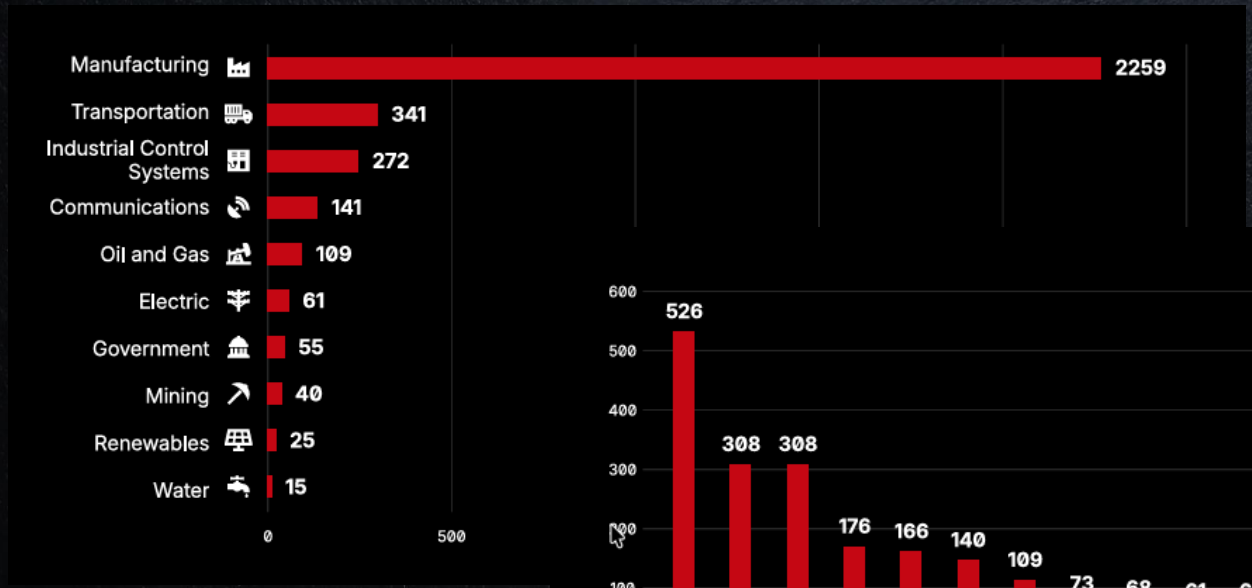
Organizations are deploying

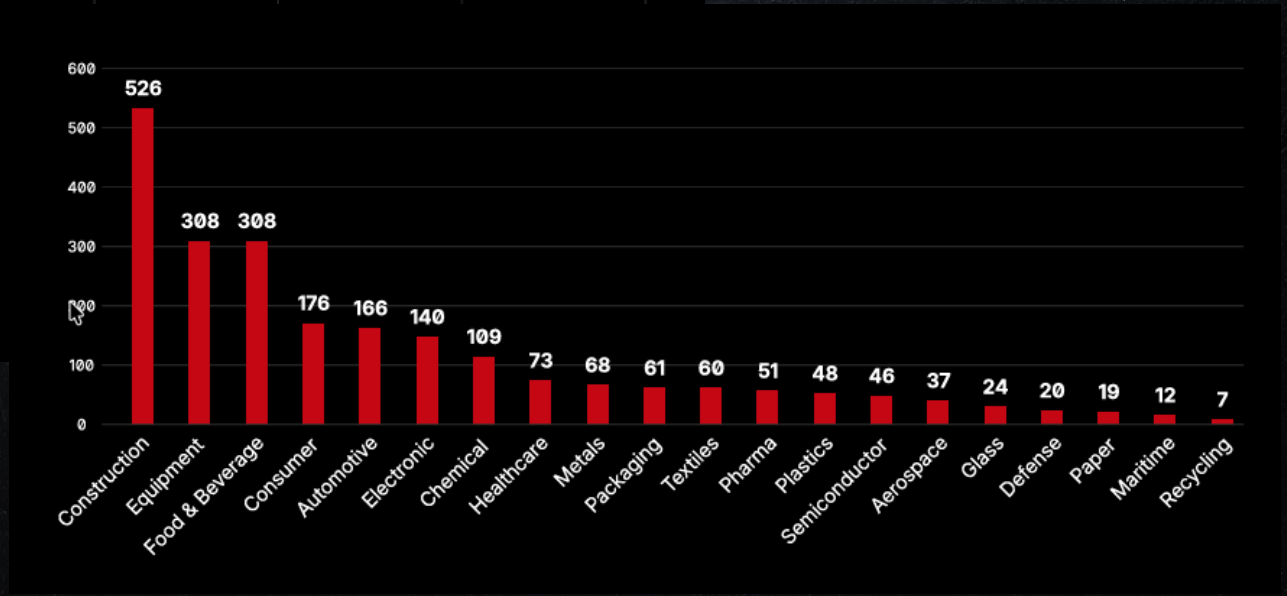

in operational environments without first establishing visibility.

"Was this cyber, equipment failure, AI error, or authorized change?"

Impossible to answer without OT visibility & foundational telemetry already in place beforehand

# RANSOMWARE OVERVIEW, MANUFACTURING, 2025



# Ransomware in OT is Mislabeled as IT Problem

Don’t call it an IT breach if OT stops working

If you classify by operating system, you miss the operational impact.

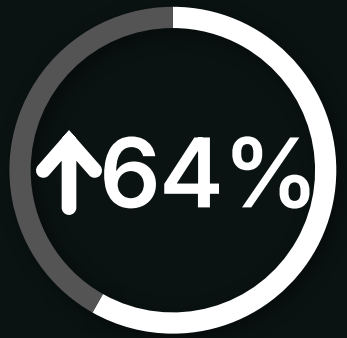
If you classify by network segment, you miss IT/OT dependencies.

**Classify by consequence:**
Did operations stop? It's an OT incident.

> **“It only hit Windows systems.”**
>
> *Engineering workstations run Windows. HMIs run Windows. Historians run Windows.*

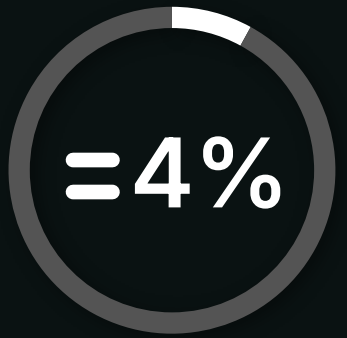
# The State Of ICS/OT Vulnerabilities

15% of vulnerabilities Dragos assessed in 2025 had incorrect CVSS data




More Severe CVSS


Less Severe CVSS

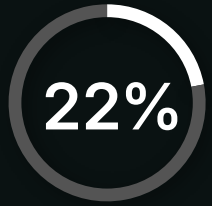



The Same

**52% of advisories** required Dragos to provide mitigations vendors didn't

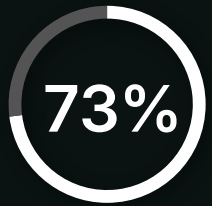
# Where Vulnerabilities Reside

**VULNERABLE ASSETS BORDERING THE ENTERPRISE ARE EXPLOITED FOR INITIAL ACCESS**

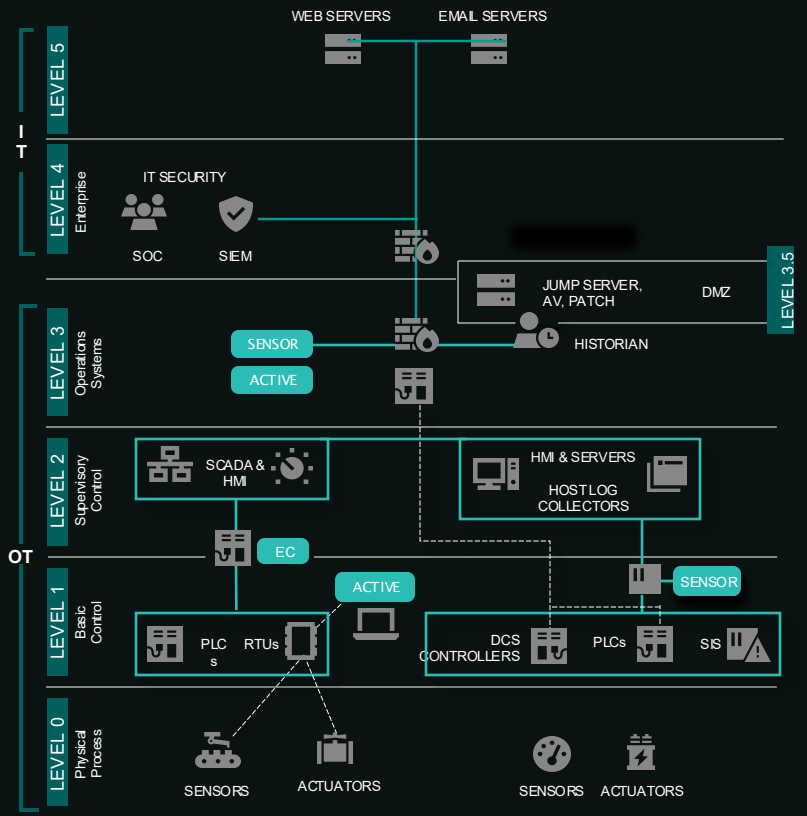



LEVELS
3.5 | 4 | 5

**VULNERABLE ASSETS DEEP WITHIN ICS NETWORKS ARE CLOSE TO CRITICAL PROCESSES**




LEVELS
0 | 1 | 2 | 3

# Necessity of Risk-Based Decision

Only some vulnerabilities need immediate action


of ICS/OT vulnerabilities

needed to be addressed

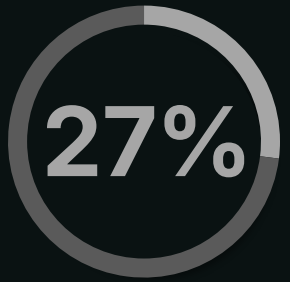
**NOW**


are network exploitable with no direct operational impact

These need to be addressed

**NEXT**

Mitigate through network monitoring, segmentation & MFA




pose a possible threat but rarely require action

They likely never need to be addressed

**NEVER**

Monitor these for signs of exploitation

# Defenders Can’t Keep Up

Findings from pentests, tabletop exercises, assessments, and incident response

## Can't **See** Fast Enough


have no OT visibility, impeding root cause analysis


detected ANY red team activity below IT/OT boundary

## Can’t **Respond** Fast Enough


TTX struggled to detect & respond before process impact


recovery times

# Insights From Dragos Intelligence Fabric

- Dragos incident response teams observed an increase in cases involving compromised credentials and unauthorized access to VMware ESXi during ransomware events.
- Exploitation of trusted third-party relationships is frequently observed in incidents involving leaked credentials from external partners.
- 5 days is the average dwell time for Dragos OT Ransomware Cases in 2025, all time is 42 days for Ransomware.
- Dragos Incident Response observed significant operational disruption in all OT ransomware cases in 2025.
- 54 percent of Dragos Services Architecture Reviews conducted revealed appropriate levels of ICS network monitoring deployed.
- 88 percent of Dragos TTXs reported degraded detection capabilities.
- 3 percent of Network Penetration Tests reported lack of monitoring - customer's do not often request a Network Penetration Tests if they lack monitoring. They are almost certainly past the initial implementation stages of monitoring and are now progressing towards operationalizing or optimizing their visibility.
- 56 percent of Dragos Network Penetration Tests included findings related to LOTL activity.
- 3 percent of services engagements identified use of default credentials.
- 53 percent of services reports identified public or internet facing assets.
- 49 percent of services engagements revealed remote access weaknesses.

# TAKEAWAYS

Adversaries Are Mapping Control Loops to Cause Physical Impact

Exploits Are Weaponized Rapidly, But Mitigation Takes Longer

Ransomware Shutdowns Are OT Incidents Being Mislabeled as IT

Gap Between Adversary Capability and Defender Visibility Is Widening

OT Security Fundamentals Remain the Most Effective Defense


THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

# RECOMMENDATIONS

01 ICS Incident Response Plan

02 Defensible Architecture

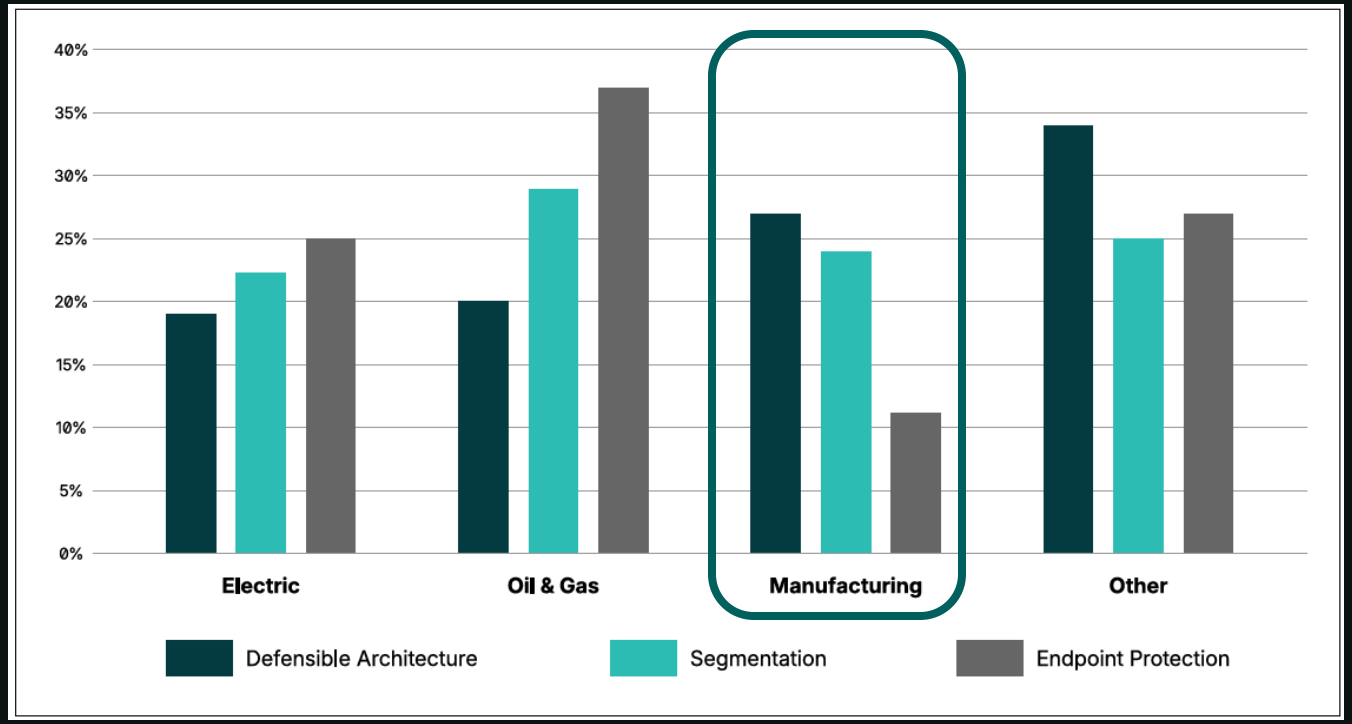
03 ICS Network Monitoring Visibility

04 Secure Remote Access

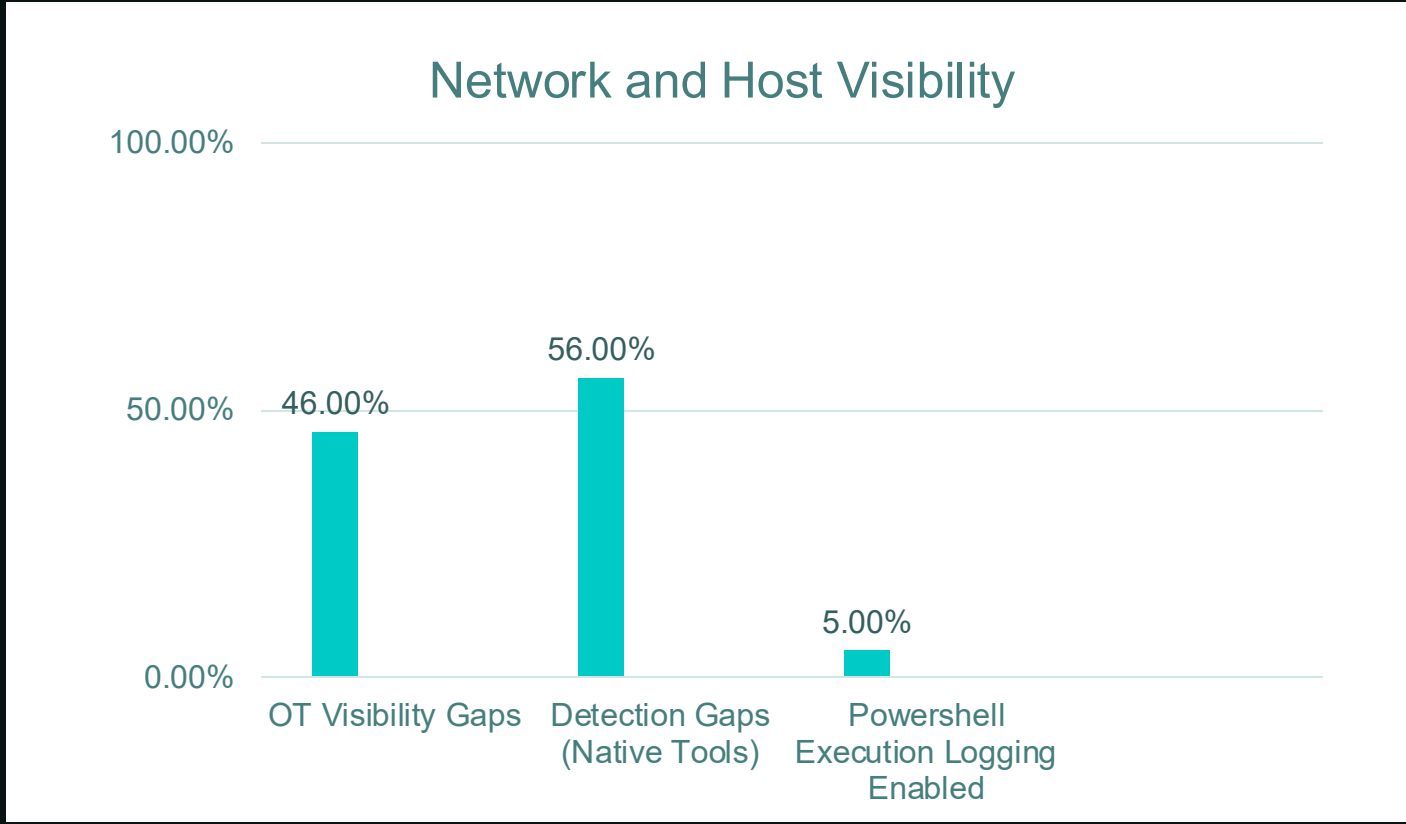
05 Risk-based Vulnerability Management

# Field Data, Defensible Architecture Stats

⚠ O&G is still struggling with basic controls

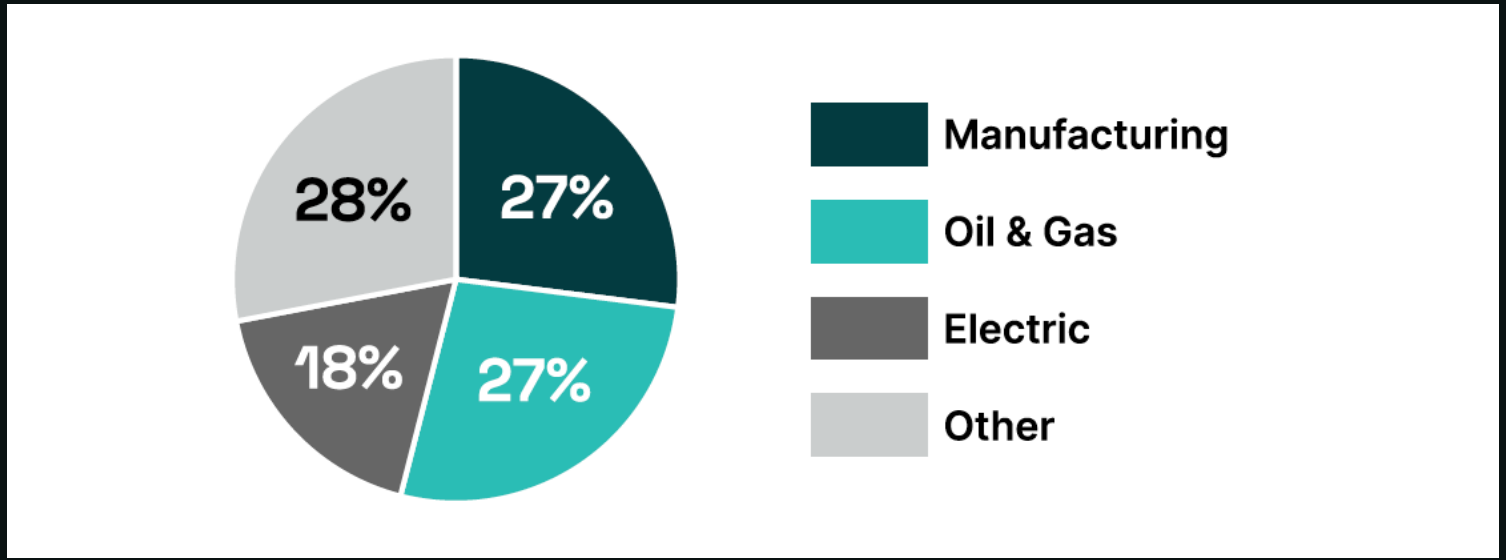


# Field Data, OT Visibility Stats (All Engagements)



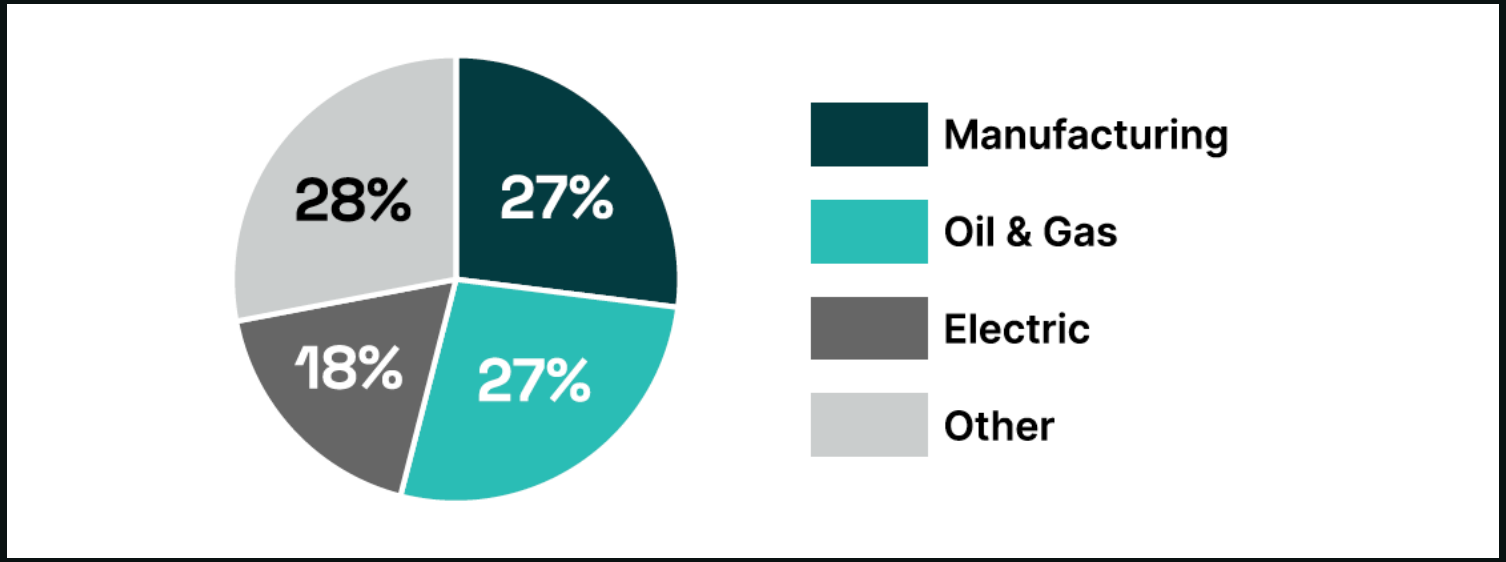
# Field Data, Secure Remote Access

⚠ 50% of engagements included SRA findings



# Field Data, Vulnerability Findings

⚠ 80% of engagements included vulnerability findings




QUESTIONS AND ANSWERS

# Thank you