From OT to xOT

What is Extended Operational Technology?

Danielle Gauthier

Senior Product Marketing Manager, Intelligence

DRAGOS

The Operational Environment Has Changed

Isolation has been replaced by interconnected operational dependencies.

Environment Expanded

Operations now extend beyond traditional OT.

- More connected systems
- More operational dependencies
- More complexity

Visibility Challenged

Security teams lose operational context.

- Incomplete inventories
- Unknown relationships
- Blind spots

More Operational Risk

More dependencies mean more opportunities for disruption.

- Larger attack surface
- Cascading operational impact
- Greater business risk

Adversaries Are Adapting Just as Quickly

Recent threat activity shows:

Adversaries invest in understanding how operations work before acting.

VOLTZITE (Volt Typhoon) has maintained access and stolen OT-relevant data – including GIS information, network diagrams, and operating instructions – to build detailed knowledge of U.S. critical infrastructure.

More connected operational environments create new pathways to critical processes.

When EDR blocked its Windows ransomware, Akira compromised an unsecured webcam and used the unmonitored Linux device to deploy ransomware across the network of a manufacturing facility.

Operational dependencies have become targets for achieving operational impact.

FrostyGoop malware altered heat meter values through ENCO controllers, causing the district heating system to make incorrect operational decisions based on manipulated process data.

The xOT Mindset Shift

From…	To…
• Protect assets	• Safeguard physical processes
• Inventory devices	• Inventory operational influence
• Prioritize CVEs	• Prioritize operational risk
• Monitor communications	• Understand operational dependencies

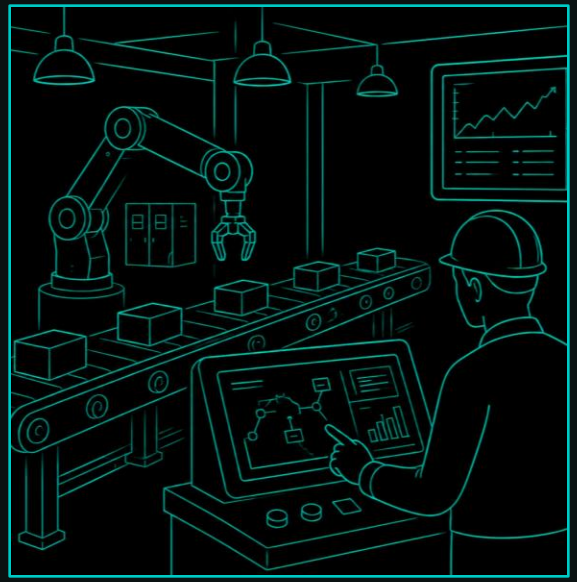
What is xOT?

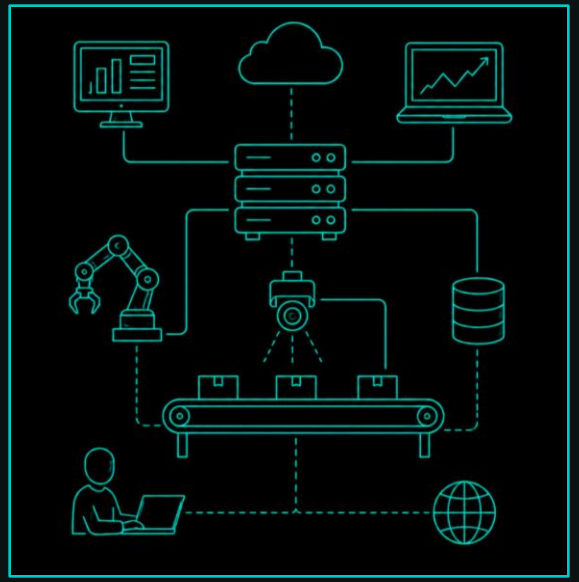
Extended Operational Technology (xOT) is the interconnected operational environment that collectively influences physical outcomes.

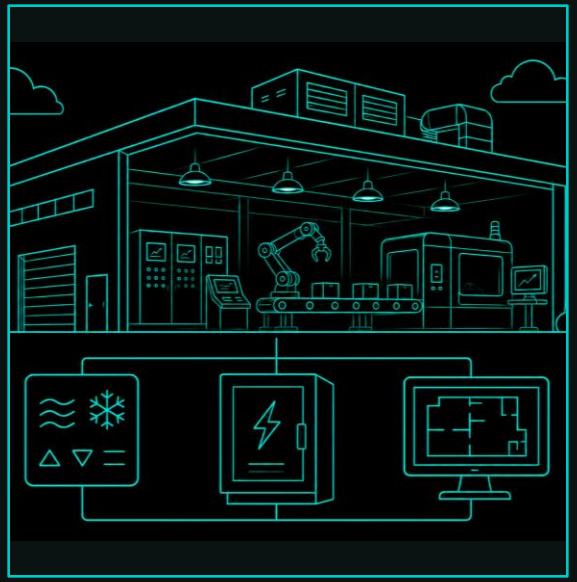
If it influences physical outcomes, it is a part of the xOT environment.

What xOT Looks Like

Every system influencing production is part of the operational environment.







Every Sector Has a Different Mix

All industries share a common OT foundation – PLCs, SCADA, Safety Controllers, etc.
Specialized operational technology meets sector-specific operational outcomes.

Electric & Utilities	*EMS (Energy Management System) · ADMS (Advanced Distribution Management System) · DERMS (Distributed Energy Resource Management) · Protective Relays · IEDs (Intelligent Electronic Devices)*
Oil & Gas	*Pipeline Management · Compressor Stations · Leak Detection · Flow Computers*
Manufacturing	*MES (Manufacturing Execution System) · Robotics · Machine Vision · AMRs*
Mining	*Fleet Management · Drilling Control · Blasting Systems*
Water & Wastewater	*Treatment Controls · Chemical Dosing · Distribution Telemetry*

Operational Influence Extends Beyond Traditional OT

Physical outcomes depend on technologies that extend beyond the traditional control system.

Building & Facility Systems

BMS

HVAC

Power Monitoring

Environment Controls

Remote Operations

Vendor Access

Remote Operations Centers

Engineering Workstations

Operational Data & Decisions

Historians

Cloud Platforms

Operational Analytics

Artificial Intelligence

Connected Devices

Industrial IoT

Environmental Sensors

Smart Instrumentation

Wireless Field Devices

How Do You Operationalize xOT?

Operationalizing xOT requires four foundational capabilities.

Visibility & Asset Intelligence

Know what influences your operations.

Operational Context

Understand how systems work together.

Detection & Monitoring

Detect operational change as it happens.

Operational Expertise

Turn operational insight into confident decisions.

Technology, intelligence, and expertise work together to secure the operational environment.

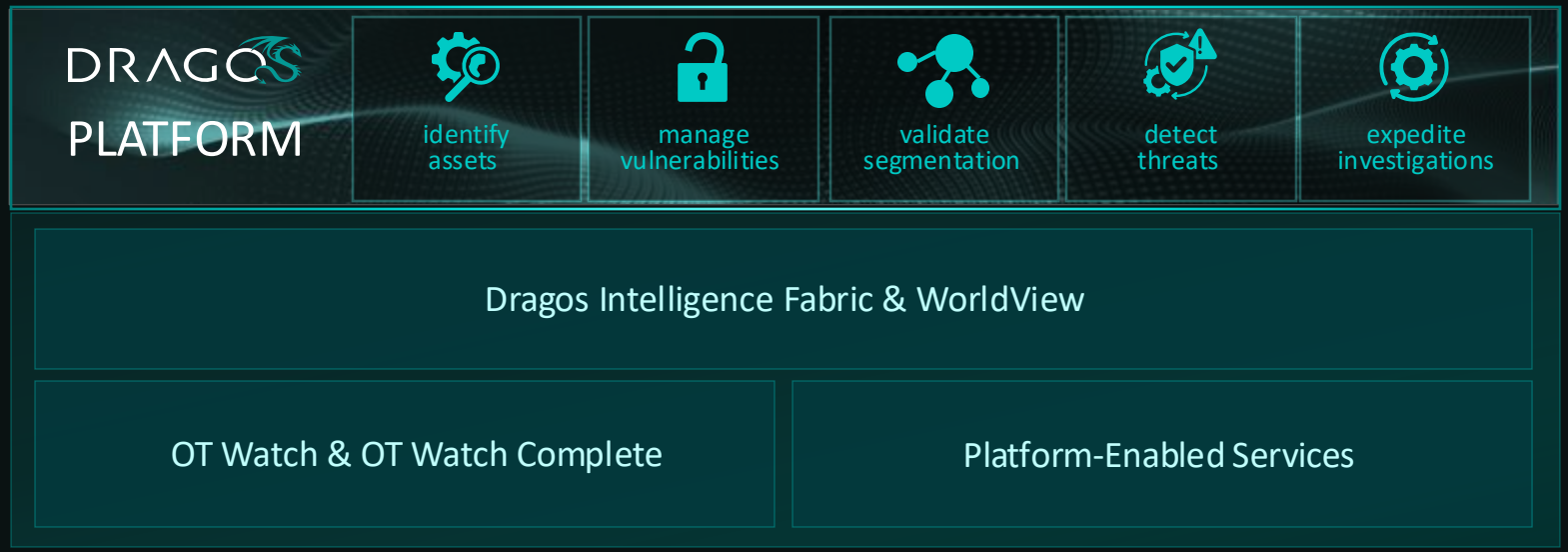
How Dragos Enables xOT

Visibility
Across OT Environments

OT Context
to Prioritize Action

Monitoring
to Prioritize Action

Expertise
to Extend Your Team



How to Start

First: See What You Have

Inventory your operational environment. Find every system that influences physical outcomes. Document dependencies and relationships. Understand what normal looks like.

Next: Understand What Matters

Map critical pathways to operational impact. Identify which systems you'd notice if they failed. Validate your inventory against reality. Understand threat surface in your specific context.

Ongoing: Stay Current

Monitor for change in your operational environment. Update your understanding as systems evolve.

Bringing It All Together

xOT expands what matters.

Security must account for every system that can influence physical outcomes, not just traditional OT assets.

Operational context drives better decisions.

Understanding relationships and operational dependencies is essential for prioritizing risk and responding effectively.

Operationalizing xOT requires an integrated approach.

Technology, intelligence, continuous monitoring, and expertise work together to secure the operational environment.

xOT Environments Require More Than Visibility Alone.

PROTECT

xOT Devices

DETECT

xOT Threats

RESPOND

With Confidence

Powered by the industry's richest xOT device, network, and threat intelligence.

DRAGOS | dragos.com