A Day in the Life: OT **Analyst**

How AI Can Improve Your xOT Security Workflows



© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

Welcome to the Dragos Webinar Series

A Day in the Life:



IT Analyst

JUST INHERITED AN OT NETWORK

Knows security. Everything about the environment is new.



OT Analyst

COVERING MORE GROUND THAN ONE PERSON SHOULD

Knows the environment. The work outpaces hours in the day.



Executive

EXPLAINS OT RISK UPWARD

Owns the risk. Needs it in terms the business accepts.



New to Environment

ACCELERATE TIME TO PRODUCTIVITY

Knows the work. Doesn't know this environment or tools yet.

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

Speakers



Mary Korus

Product Marketing
Dragos Platform



Drew Hutcheon

Product Management
Dragos EmberAI

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

MONDAY MORNING

30+ water utilities lose visibility and control

CISA urges utilities to remove exposed controllers from the public internet. Similar intrusions are confirmed across multiple states.

Dragos, Water Under Attack: A Decade of Warnings, August 2026;
CISA advisory AA26-097A

Your Phone Rings....

QUESTION 1

Are we operational?

Is anything in our environment behaving the way theirs did?

QUESTION 2

Are we exposed?

Do we have those controllers, versions, and connections?

QUESTION3

What is the action plan?

If a risk, what do we do first, and what can wait?

How fast can you answer?

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

Most Investigations Start With a Feeling

30%

IR cases began with unexplained operational issues; irregular events asset owners couldn’t diagnose.

1 The alert must fire

In most of those cases, the data needed to determine whether cyber was involved had never been collected. OT network telemetry is transient. If it isn't recorded when it happens, it's gone.

2 An alert isn’t an incident

Knowing something fired is not the same as knowing what it means, which assets it touched, or what you can safely do about it.

3 The clock is running

Threat groups now work in paired models, one team developing access and handing off to a team with ICS capability, compressing compromise to operational readiness from weeks to days.

Source: Dragos 2026 OT/ICS Cybersecurity Year in Review

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

THE FOUNDATION

xOT Cybersecurity Foundation



Asset Visibility

SEE YOUR ENVIRONMENT

Discover every xOT asset, connection, and protocol — no agents, no disruption.



Threat Detection

CATCH WHAT OTHERS MISS

Detect adversary behaviors using intelligence from frontline ICS investigations.



Vulnerability Management

FIX WHAT MATTERS

Prioritize what actually matters with Now, Next, Never guidance for OT.



Investigation & Response

RESPOND WITH CONFIDENCE

Move from alert to action with guided playbooks authored by OT responders.

DRAGOS

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

Activate AI Powered Workflows

Expert-built OT Actionability

Guided, repeatable workflows built and validated by Dragos, encoding the expertise our team applies during proactive services, investigations, and incident response. Ready to run, continuously expanded.

DRAGOS EmberAI

01 Intelligence-driven query engine

02 Contextual correlation

03 Adversary-informed guidance

04 Workflow acceleration

05 Continuous learning

DRAGOS INTELLIGENCE FABRIC

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

THE FOUNDATION

A Day in the Life



IT Analyst

JUST INHERITED AN OT NETWORK

Knows security. Everything about the environment is new.



OT Analyst

COVERING MORE GROUND THAN ONE PERSON SHOULD

Knows the environment. The work outpaces hours in the day.



Executive

EXPLAINS OT RISK UPWARD

Owns the risk. Needs it in terms the business accepts.



New to Environment

ACCELERATE TIME TO PRODUCTIVITY

Knows the work. Doesn't know this environment or tools yet.

DRAGOS

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

Dragos EmberAI Customer Outcomes

Alert to Action

Get clear, guided next steps for notifications and alerts. EmberAI can take approved action on your Platform data, like tagging Crown Jewel assets, once you sign off.

Improve Efficiency

Filter the noise that has no impact, accelerate investigative steps with context, and draw on an expanding library of Dragos-built Skills for guided, repeatable workflows.

Increase Resilience

EmberAI gives analysts the context to act before a line stops or a grid segment goes offline.

Accelerate Decisions

Contextual, intelligence-backed answers in seconds instead of hours, days, or weeks. Reduce both MTTD and MTTR.

Scale Expertise

New employees and less-experienced analysts operate at the level of your most seasoned specialist, accelerating productivity and confident decision-making.

Fluent in your Context

Set your role, industry, and regulatory framework once. Every answer is grounded in your job, your sector, and your compliance posture.

Every analyst on the team gets to operate at the level of your senior OT expert.

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.

INTRODUCING



DRAGOS EmberAI

© 2026 Dragos, Inc. All Rights Reserved. Proprietary & Confidential.