5 Critical lakeawaus

from the 2025 SANS State of OT Security

Since 2017, the SANS Institute State of ICS/OT Cybersecurity Survey has been the definitive benchmark for industrial security programs worldwide, tracking how organizations secure critical infrastructure—from detection and incident response to compliance and technology investments. The 2025 survey gathered insights from over 330 cybersecurity professionals across energy, manufacturing, water, oil and gas, transportation, and other critical sectors. Respondents represent a global cross-section of practitioners from frontline OT security teams to CISOs—responsible for protecting the operational technology that powers modern society. Dragos is proud to sponsor this research alongside SANS Institute.

Regulation Drives Results, But Only with the Right Foundation 58% ~50% 72%

of organizations are now subject

to mandatory OT cybersecurity compliance

fewer financial losses and safety impacts

from incidents experienced by regulated sites The Dragos Solution: Dragos Platform provides compliance-ready capabilities for

ISA/IEC 62443, NERC CIP, TSA SD, and emerging APAC frameworks

increased investment in logging, monitoring, and detection due to

regulations



point for compliance programs

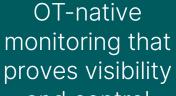


change detection for audit evidence

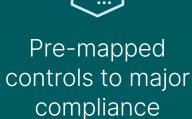
resilience and cyber maturity.



aligned to regulatory requirements **THE VALUE:** Turn compliance from a checkbox exercise into a force multiplier for operational



and control



frameworks

Detection Is Strong, But Only at the Surface 49% 10% 1 in 8

visibility across the ICS Cyber Kill Chain

organizations have full

coverage drops dramatically at lower Purdue levels

have OT-specific

detection, but

The Dragos Solution: Dragos Platform delivers OT-native threat detection

report full visibility at

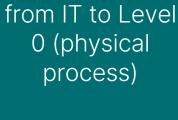
Level 2 (supervisory

control)

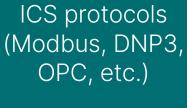


environments

Full visibility Purpose-built Passive



and process controllers.

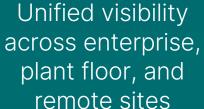


detection for

THE VALUE: See threats before they reach your most critical assets: PLCs, SCADA systems,



monitoring that



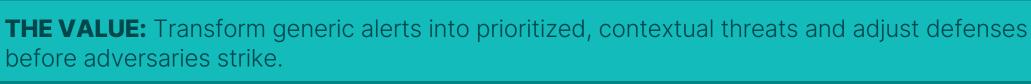
Intelligence Integration

is the Missing Multiplier 64% 21% 52% 57% Organizations with deployed intelligence report increased see rising nationthreat intelligence are integration in the ransomware targeting state-aligned threats 52% more likely to OT environments past year improve monitoring

The Dragos Solution: Dragos WorldView threat intelligence provides

and segmentation

OT-specific Pre-built Actionable Context on threat threat intelligence detection rules indicators from the world's tied directly that integrate targeting, and



leading ICS threat

hunters



to industrial

adversary groups

57% ±50% 22%

of incidents are

detected within 24

hours



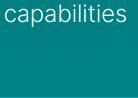
seamlessly with

Dragos Platform

take 2-7 days to

remediate, 19% take

over a month



actor TTPs,

Incident Response Plans Exist

But Recovery Still Lags

24/7/365

OT security

operations center

monitoring

50%

invested in asset

inventory and visibility

in 2025

realistic OT-focused exercises.

recovery

have an OT-specific

incident response plan

Incident response retainers with OT-specialized

responders

54%

plan to continue

investing in 2026-2027

Tabletop exercises and purple team

engagements

31%

have no centralized

inventory of remote

access points

Backplane-level

visibility into PLC

configurations

and logic

Post-incident root cause analysis and containment

guidance

Asset visibility is

the foundation

for detection,

segmentation,

1.7x

Organizations with IR

plans report 1.7x better

preparedness

THE VALUE: Cut remediation time from weeks to days - and build muscle memory through

Asset Visibility Is Priority #1,
For Good Reason

The Dragos Solution: Dragos Services & Support accelerates response and

and vulnerability management The Dragos Solution: Dragos Platform provides comprehensive asset intelligence

current inventory of your OT environment

THE VALUE: You can't protect what you can't see - Dragos gives you a complete, always-

Organizations with OT-native security platforms report:



Faster detection

and containment

Passive discovery

of every OT

asset-no

scanning, no

disruption



The Bottom Line

Better IT-OT

collaboration

Automatic

identification

of device type,

vendor, model,

firmware version



Stronger

preparedness

and resilience



Risk-based

vulnerability

prioritization tied

to your specific

environment

More effective compliance and audit readiness

Dragos delivers the only purpose-built, OT-native cybersecurity platform designed to protect industrial operations—from asset visibility and threat detection to intelligence-driven defense and expert incident response.

Copyright © 2025 Dragos, Inc. All Rights Reserved.

Ready to strengthen your OT security posture?