DRAGOS

5 Critical Takeaways

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.

1. Regulation Drives Results, But Only with the Right Foundation

58% of organizations are now subject to mandatory OT cybersecurity compliance

~50% fewer financial losses and safety impacts from incidents experienced by regulated sites

72% increased investment in logging, monitoring, and detection due to regulations

Evidence collection remains a top pain point for compliance programs

The Dragos Solution: Dragos Platform provides compliance-ready capabilities for ISA/IEC 62443, NERC CIP, TSA SD, and emerging APAC frameworks

- Automated asset inventory and change detection for audit evidence
- Built-in logging and reporting aligned to regulatory requirements
- OT-native monitoring that proves visibility and control
- Pre-mapped controls to major compliance frameworks

THE VALUE: Turn compliance from a checkbox exercise into a force multiplier for operational resilience and cyber maturity.

2. Detection Is Strong, But Only at the Surface

1 in 8 organizations have full visibility across the ICS Cyber Kill Chain

49% have OT-specific detection, but coverage drops dramatically at lower Purdue levels

10% report full visibility at Level 2 (supervisory control)

Remote sites remain among the least protected environments

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

- Full visibility from IT to Level 0 (physical process)
- Purpose-built detection for ICS protocols (Modbus, DNP3, OPC, etc.)
- Passive monitoring that won't disrupt operations
- Unified visibility across enterprise, plant floor, and remote sites

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

3. Intelligence Integration is the Missing Multiplier

52% Organizations with threat intelligence are 52% more likely to improve monitoring and segmentation

21% deployed intelligence integration in the past year

64% report increased ransomware targeting OT environments

57% see rising nation-state-aligned threats

The Dragos Solution: Dragos WorldView threat intelligence provides

- OT-specific threat intelligence from the world's leading ICS threat hunters
- Actionable indicators tied directly to industrial adversary groups
- Pre-built detection rules that integrate seamlessly with Dragos Platform
- Context on threat actor TTPs, targeting, and capabilities

THE VALUE: Transform generic alerts into prioritized, contextual threats and adjust defenses before adversaries strike.

4. Incident Response Plans Exist But Recovery Still Lags

57% have an OT-specific incident response plan

±50% of incidents are detected within 24 hours

22% take 2-7 days to remediate, **19% take over a month**

1.7x Organizations with IR plans report 1.7x better preparedness

The Dragos Solution: Dragos Services & Support accelerates response and recovery

- 24/7/365 OT security operations center monitoring
- Incident response retainers with OT-specialized responders
- Tabletop exercises and purple team engagements
- Post-incident root cause analysis and containment guidance

THE VALUE: Cut remediation time from weeks to days - and build muscle memory through realistic OT-focused exercises.

5. Asset Visibility Is Priority #1, For Good Reason

50% invested in asset inventory and visibility in 2025

54% plan to continue investing in 2026-2027

31% have no centralized inventory of remote access points

Asset visibility is the foundation for detection, segmentation, and vulnerability management

The Dragos Solution: Dragos Platform provides comprehensive asset intelligence

- Passive discovery of every OT asset—no scanning, no disruption
- Automatic identification of device type, vendor, model, firmware version
- Backplane-level visibility into PLC configurations and logic
- Risk-based vulnerability prioritization tied to your specific environment

THE VALUE: You can't protect what you can't see - Dragos gives you a complete, always-current inventory of your OT environment

The Bottom Line

Organizations with OT-native security platforms report:

- Faster detection and containment
- Better IT-OT collaboration
- Stronger preparedness and resilience
- 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.

Ready to strengthen your OT security posture?
Learn how Dragos can help.

Book a Demo