SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Maritime Cybersecurity Regulations

How Dragos Helps You Meet Unified Requirements E26 and E27

The International Association of Classification Societies (IACS) has introduced two new cyber security regulations, Unified Requirements (URs) E26 and E27, which will be enforced for all classed vessels launched in 2024. These regulations aim to enhance vessel cyber resilience and protect the maritime industry from emerging cyber threats, following the introduction of other industry standards like IASME's Maritime Cyber Baseline in 2022.

UR E26 focuses on the secure integration of Operational Technology (OT) and Information Technology (IT) equipment into a ship's network, emphasizing cyber resilience through identification, protection, detection, response, and recovery. UR E27 focuses on securing third-party equipment suppliers and strengthening the integrity of onboard equipment and systems. These regulations apply to vessels built on or after January 1, 2024, and represent a significant milestone in IACS' efforts to ensure safer shipping in the face of evolving technological developments.

Unified Requirement E26 (UR E26)

UR E26 focuses on ensuring the secure integration of OT and IT equipment into the ship's network throughout its lifecycle.

REQUIREMENTS	DRAGOS SOLUTIONS

Identification:
• Identification of cyber threats and vulnerabilities specific to the ship's OT and IT equipment.
• Establishing a comprehensive inventory of cyber assets, including:
  • a functional description of Computer Based Systems (CBS)
  • a block diagram of connections
  • inventory/register of hardware and software
  • documentation of features, protocols, data flows, and networks connecting CBSs
	Dragos Platform:
	Asset Inventory Use Case
	A comprehensive and real-time understanding of all assets in your environment is essential for network monitoring, threat correlation, and effective vulnerability management. Our customers use the Dragos Platform to identify crown jewel assets, create asset inventories, and identify unusual activity across thousands of devices. The Dragos Platform's asset inventory and visibility capabilities include:
	• Comprehensive inventory of all assets, devices, and details
	• Faster triage of incidents through timeline analysis
	• Group assets by zone to identify unexpected traffic
	
	Dragos Platform:
	Vulnerability Management Use Case
	OT cybersecurity teams are overwhelmed by hundreds of vulnerabilities that potentially need to be remediated. Dragos customers use the Platform to simplify compliance and reporting, prioritize vulnerabilities that matter most, and maximize remediation resources.

Protection:
• Implementation of protective measures to secure OT and IT equipment against cyber threats, including:
  • Security zones
  • Antivirus, antimalware, and antispam processes
  • Regulations on the use of wireless communication and mobile devices
• Application of access controls and security measures to prevent unauthorized access.
	OT Cybersecurity Assessment
	The OT Cybersecurity Assessment includes a full program review, creation of a collection management framework, crown jewel analysis, topology review, standards and regulations review, indicators of compromise sweep, threat discovery, asset inventory, network vulnerability assessment, and asset vulnerability assessment.
	
	OT Network Vulnerability Assessment
	An OT Network Vulnerability Assessment helps your company close gaps in network defense by evaluating protection, detection, and response capabilities that currently exist in your environment. The assessment identifies exploitable vulnerabilities and provides action items to strengthen OT cybersecurity posture.
	
	OT Penetration Testing
	OT Penetration Testing prevents severe breaches by leveraging real-world attacker tactics, techniques, and procedures (TTPs) gained from intelligence. Penetration testing identifies devices that could allow unauthorized access to critical OT assets and demonstrates how attackers can move through OT environments.

REQUIREMENTS	DRAGOS SOLUTIONS
Attack Detection: • Implementation of mechanisms and tools to detect cyber attacks and incidents promptly. • Monitoring and analyzing network traffic for signs of abnormal behavior. • Diagnostic functions for system health.	**Dragos Platform:** **Detection Use Case** Adversaries evolve their tactics, techniques, and procedures with subtle behaviors that are easily lost in the noise of your environment. Our platform customers immediately see any unauthorized IT-OT traffic across complex networks, analyze file downloads quickly and easily, and detect potential adversaries in the environment in real time. **OT Watch** With Dragos OT Watch, our OT cybersecurity experts become part of your team, performing high severity notification triage and proactive threat hunting with the Dragos Platform to ensure threats don't get overlooked. Our elite team of analysts proactively hunt for and report on threat activity in your OT environment using the latest threat intelligence exclusive to Dragos customers. We work alongside your team to triage and investigate high severity notifications to reduce the burden on internal resources.

Response:
• Creation of incident response teams and communication protocols.
• Development of response procedures to address and mitigate cyber incidents.
• Creation of provisions in the event of an incident, including:
  • ability to operate locally, independently, and/or manually
  • ability to isolate the network
  • ability to fallback to a minimal risk condition
	Dragos Platform:
	Incident Investigation Use Case
	Dragos Platform users can analyze changes and forensic records, efficiently manage response and recovery, and leverage prescriptive playbooks with proven, tested response protocols.
	Rapid Response Retainer
	An OT-specific Rapid Response Retainer is essential for any industrial environment. Since the potential impact of a cyber attack can vary based on visibility, the ability to respond, and your organizational security posture, a dedicated OT incident response plan accounting for your needs is crucial to quickly scope, investigate, and respond to incidents. As the cornerstone of your OT cyber program, an OT-specific incident response retainer ensures you can respond quickly and recover confidently.
	Tabletop Exercises
	The Dragos Tabletop Exercise (TTX) Service is a step-by-step method that demonstrates how a realistic attack may occur within your unique OT environment based on your organization's most concerning risks. Dragos TTXs include collaboration between all stakeholders, including IT and OT security teams, to strengthen internal communication strategies and develop relationships.

REQUIREMENTS	DRAGOS SOLUTIONS

Recovery:
• Regularly testing and updating comprehensive recovery plans to ensure effectiveness.
• Establishing recovery processes to restore operations and systems affected by cyber incidents, including:
  • backup and restoration capabilities
  • controlled shutdown, reset, rollback, and restart processes
	Rapid Response Retainer: Recovery Measures
	Every Dragos Rapid Response Retainer begins with a Readiness Assessment as part of your onboarding, to assess your current incident response preparedness. With a baseline established, the Response team at Dragos can make strategic and tactical recommendations, including safe and secure shut down and restoration procedures.

Unified Requirement E27 (UR E27)

UR E27 emphasizes cyber resilience, ensuring 3rd party equipment suppliers secure and strengthen the integrity of onboard equipment and systems.

REQUIREMENTS	DRAGOS SOLUTIONS
Cyber Resilience of Systems and Equipment: • Ensuring that onboard systems and equipment are designed and maintained with cyber resilience in mind. • Implementing security controls and measures to protect critical systems.	**Dragos Platform** The Dragos Platform monitors your systems and includes up-to-date threat intelligence to identify new threats and vulnerabilities. Dragos Threat Intelligence allows you to monitor risk to your sector and asset base, providing full situational awareness.
User Interaction with Computer-Based Systems: • Providing guidelines for how users interact with computer-based systems to minimize security risks. • Promoting best practices for user authentication and access management.	**Dragos ICS-OT Cybersecurity Training** Training builds a better shared understanding of the terminologies, purpose, security goals, and technologies deployed in OT environments and security programs. Training operations staff in cybersecurity fundamentals, access management, authentication, and recovery procedures are an important part of business continuity. Cybersecurity is everyone's job, and the operations team are the front lines for preventing, identifying, and responding to incidents.

The Dragos Platform

The Dragos Platform provides comprehensive visibility of your ICS/OT assets and the threats you face, with best-practice guidance to respond before a significant compromise.

Top Five Differentiators

Why the Dragos Platform is the Best Choice for OT Environments

Largest, Most Experienced ICS Team: We bring unmatched industrial expertise to the table, ensuring your infrastructure is in the hands of true OT professionals.

Empowering Threat Response: We don't just detect threats; we arm you with deep context and actionable playbooks.

Effective Vulnerability Management: Dragos corrects and enriches CVSS scores with exclusive "Now, Next, Never" guidance, ensuring a proactive and effective approach.

Reduced Alert Fatigue: Forget about noisy alarms overwhelming your SOC. Dragos unique intelligence distills threat behavior analytics to reduce alert fatigue and false positives.

Less Dependence on Signatures: Move away from traditional signature-based detections, reducing your exposure to evolving threats.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us

info@dragos.com @DragosInc @Dragos, Inc.