SOLUTION BRIEF

OT Cybersecurity Solutions for Successful Implementation of ISA/IEC 62443

Helping You Develop a Comprehensive, Effective Security Program – and Simplify Implementation of ISA/IEC 62443

The mission of Dragos is to safeguard civilization by providing the platform, services, and intelligence to protect operational technology and critical infrastructure. Our technology supports numerous industry standards and regulations, empowering our customers to adopt best practices and exceed compliance requirements. As a founding member of the ISA Global Cybersecurity Alliance, we are committed to supporting and expanding the adoption of ISA/IEC 62443. The ISA/IEC 62443 series of standards and technical reports specifies requirements for the security of industrial automation and control systems.

ISA/IEC 62443: The World's Only Consensus-Based Series of OT Cybersecurity Standards

The goal of the ISA/IEC 62443 series is to improve the safety, reliability, integrity, and security of automation and control systems using a risk-based, methodical process. The benefits of using a standards-based approach include reducing the likelihood of a successful cyber attack, the use of a common set of requirements among stakeholders, security throughout the lifecycle, and a reduction in overall lifecycle cost.

The series describes a set of common terms and requirements used globally by asset owners, product suppliers, and service providers to secure their control systems and the equipment under control, outlining a comprehensive framework for the design, planning, integration, and management of secure systems.

ISA/IEC 62443 is a functional standard – the series sets objectives for security performance but does not define how these objectives should be met.

Mapping Dragos Capabilities to Simplify Adoption of ISA/IEC 62443

Dragos offers technology, infrastructure, and professional services support to translate the objectives within ISA/IEC 62443 into actionable pieces of your cybersecurity plan, customized for your environment and risk profiles.

DRAGOS OFFERING	HOW IT HELPS DRAGOS CUSTOMERS	WHAT IT CAN DO TO HELP YOU ADOPT AND APPLY ISA/IEC 62443
The Dragos Platform	The Dragos Platform automates the delivery of visibility into asset inventory, asset vulnerabilities, and network traffic. It detects cyber threats to OT assets and provides contextual, practical advice to mitigate each threat. It features response capabilities to streamline investigation, root cause analysis, mitigation, repair, and reporting of incidents.	A few examples of the ISA/IEC 62443 objectives that can be met or exceeded by using Dragos Platform include: • ISA/IEC 62443-3-3 SR 1.13 The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted network. • ISA/IEC 62443-3-3 SR 2.8 The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, con figuration changes, potential reconnaissance activity and audit log events. • ISA/IEC 62443-3-3 SR 6.2 The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. Monitoring can be achieved through a variety of tools and techniques such as IDS, IPS, network monitoring mechanisms, etc. • ISA/IEC 62443-3-3 SR 7.8 The control system shall provide the capability to report the current list of installed components and their associated properties.

DRAGOS OFFERING	HOW IT HELPS DRAGOS CUSTOMERS	WHAT IT CAN DO TO HELP YOU ADOPT AND APPLY ISA/IEC 62443
Professional Services	Global services resources help you establish and maintain a risk management program. Dragos industry-specific experts assist in the development and resourcing of incident response plans, cyber security exercises, vulnerability assessments, and more. Our team can help your company maintain up-to-date system and asset information to enable compliance with regional and industry-specific regulations.	A few examples of the ISA/IEC 62443 objectives that can be met or exceeded by using Dragos professional services include: • ISA/IEC 62443-3-2 ZCR 2.1 The organization shall perform a high-level cybersecurity risk assessment of the SuC in order to identify the worst-case unmitigated cybersecurity risk that could result from the interference with, disruption of, or disablement of mission critical IACS operations. • ISA/IEC 62443-3-2 DRAR 12 The results of the cyber risk assessment shall be documented and reported. Documentation that was instrumental in performing the cyber risk assessment (such as architecture diagrams, vulnerability assessments and source of threat information) shall be recorded and archived along with the cyber risk assessment. • ISA/IEC 62443-3-3 SR 5.1 The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks. • ISA/IEC 62443-3-2 ZCR 3.1 The organization shall establish zones and conduits by grouping IACS and related assets. Grouping shall be used upon the results of the high-level cybersecurity risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access or responsible organization. • ISA/IEC 62443-3-3 SR 5.2 The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zone and conduits model.

DRAGOS OFFERING	HOW IT HELPS DRAGOS CUSTOMERS	WHAT IT CAN DO TO HELP YOU ADOPT AND APPLY ISA/IEC 62443
Threat Intelligence	Dragos threat intelligence services alert you to OT adversary campaigns, providing detailed detection TTPs. The Dragos intelligence team delivers easy-to-implement, practical vulnerability mitigation advice. We publish valuable reports and alerts with insights from key threats and incidents.	A few examples of the ISA/IEC 62443 objectives that can be met or exceeded by using Dragos threat intelligence include: • ISA/IEC 62443-3-3 SR 3.2 The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software transported by electronic mail, Internet access, removable media, network connections, infected lap tops or other common means. • ISA/IEC 62443-3-2 DRAR 1 A list of threats that could affect the assets contained within the zone or conduit shall be developed. A threat description shall include a description of the threat source, threat vectors and potentially affected assets. • ISA/IEC 62443-3-2 DRAR 2 The zone or conduit shall be analyzed in order to identify and document the known vulnerabilities in the assets contained within the zone or conduit including the access point. • ISA/IEC 62443-3-2 ZCR 5.4 The Cybersecurity Requirements Specification shall include a description of the threat environment that impacts the SuC. The description shall include the source(s) of threat intelligence and include both current and emerging threats.

About Dragos, Inc.

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

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.