SOLUTION BRIEF

Kingdom of Saudi Arabia National Cybersecurity Authority (NCA) Operational Technology Cybersecurity Controls (OTCC-1: 2022)

How Dragos Technology & Solutions Can Help to Meet NCA OTCC-1:2022 Requirements

Security of industrial systems is becoming increasingly critical to the well-being of society as a whole. The continuous function of oil and gas infrastructure, refineries, manufacturing, power, and water are critical to the economy – and life itself. Protecting industrial control systems (ICS) and operational technology (OT) is a deeply complex mission. To ensure that operators are focused on that mission, the Kingdom of Saudi Arabia (KSA) National Cybersecurity Authority (NCA) issued Operational Technology Cybersecurity Controls (OTCC-1:2022).

What Is In OTCC-1:2022?

The OTCC-1:2022 regulations build from Compliance with Essential Cybersecurity Controls (ECC 1:2018), which remain as core prerequisites. The challenge as an asset owner and operator is to understand clearly the requirements of the OTCC regulations, to identify resources to help achieve compliance, and do the work. In summary, the OTCC-1:2022 provides guidelines for:

Cybersecurity Governance

The people, process, and technology requirements defining operational technology (OT) cybersecurity programs.

Cybersecurity Resilience

Proactive risk analysis, architecture, and incident response planning to assure continued operations minimize the impacts on OT environments from disasters caused by cybersecurity incidents.

Cybersecurity Defense

The controls used to secure the OT environments to maintain the production uptime, safe operations, confidentiality, integrity, and availability of OT assets.

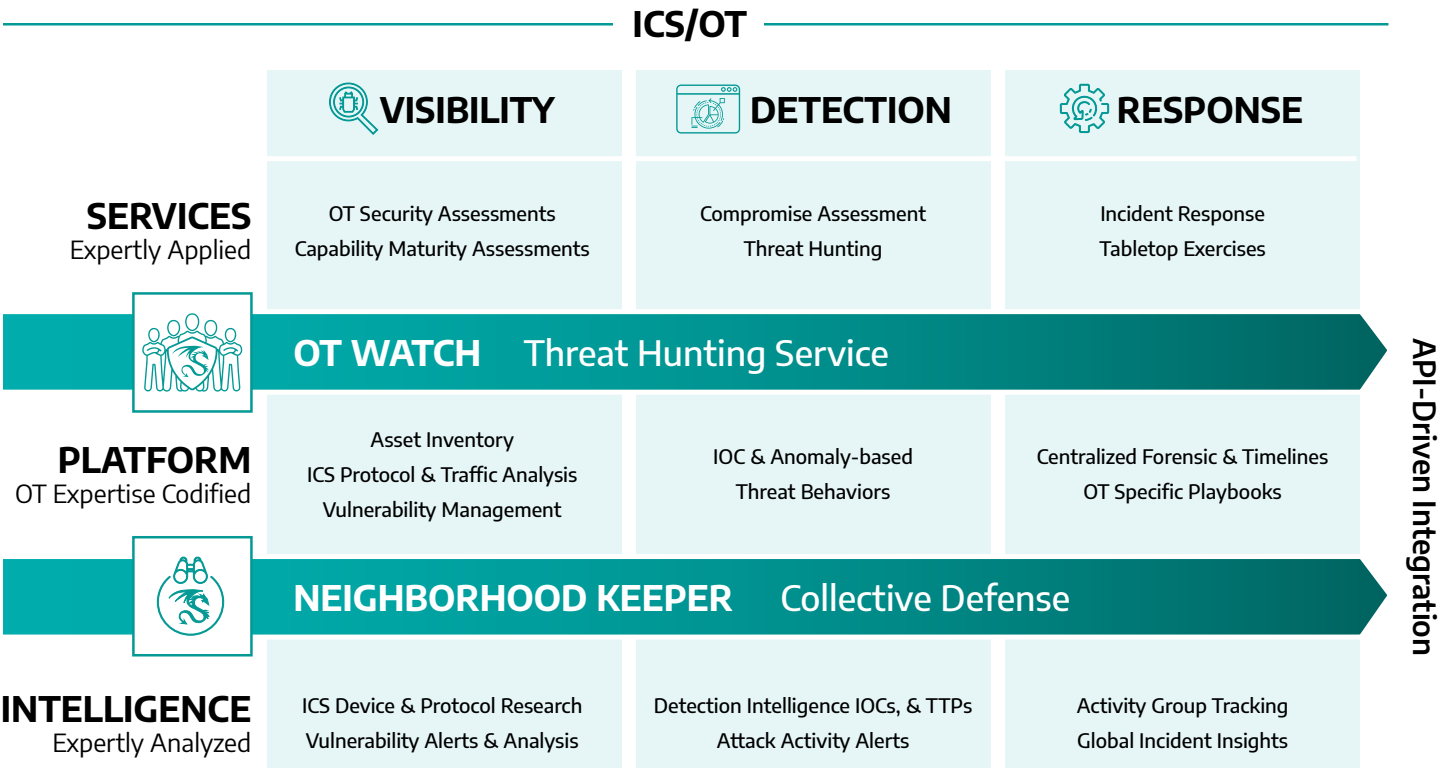
Third Party Cybersecurity

Concerned with the extension of effective OT security controls to key suppliers.

How Dragos Can Help to Develop an Effective Security Program & Simplify Compliance with OTCC-1:2022

Dragos's mission is to safeguard civilization by providing the platform, services, and intelligence to protect critical infrastructure and operational technology. We are actively focused on building the community among OT operators, security practitioners, government agencies, and key third parties. We provide:

- **The Dragos Platform,** a technology platform that automates the delivery of visibility into asset inventory, asset vulnerabilities, and network traffic; detection of cyber threats to OT assets; and response capabilities that streamline investigation, root cause analysis, mitigation, repair, and reporting of incidents.
- **Global Services** resources that help you establish and maintain a risk management program, assist in the development and resourcing of incident response plans, cybersecurity exercises, vulnerability assessments, and maintaining up-to-date system and asset information.
- **OT Cyber Threat Intelligence Services** that alert you to OT adversary campaigns, provides detailed detection TTPs, delivers practical vulnerability mitigation advice, and informs you with insights from key threats and incidents.



Mapping Dragos Technology & Services to OTCC Requirements

There are a number of specific requirements in OTCC. Dragos serves the industrial side of critical infrastructure, focusing on operational technology for industries that include water and sewage, energy, transportation, food & beverage manufacturing, space, and defence. We provide a subset of capability for data storage & processing, communications, and health care / medical. Below is a summary analysis of where we can help.

OTCC DOMAINS	DRAGOS CAPABILITIES
Cybersecurity Governance	**Dragos Global Services** provides in-depth review, best practices, and recommendations for risk management, roles and responsibilities, policies/procedures. Specifically, OT Security Program Assessment and Capability Maturity Assessments, and Incident Response Planning apply, and can be augmented with in depth risk analysis and planning workshops. While Dragos does not provide direct services for project management, change management, audit, HR, or training, the above assessment and planning services can be leveraged to assist in program design. In addition, the **Dragos Platform** can be used to provide validation of controls and information sets useful for audit purposes.

OTCC DOMAINS	DRAGOS CAPABILITIES
Cybersecurity Defense	**Dragos Platform** provides critical OT security risk controls to help build and maintain a strong industrial security posture that conforms with KSA NCA requirements. • In-depth visibility into assets, vulnerabilities, network traffic, system commands and much more, providing in depth record for forensic analysis. • Detection of threats, with IOC and anomaly-based detection, as well as behavioral threat detection driven by our Intelligence team. • Response playbooks from our in-field experts to streamline your investigation & mitigation actions. **Dragos Global Services** provides a full spectrum of capability to assist in the review and improvement of cybersecurity controls in accordance with OTCC: • OT Security and Capability Maturity Assessments to review architecture, assemble asset inventory, catalog vulnerabilities, and review your OT program, including defense controls outside of the Dragos platform. • Provide ICS-specific incident responses planning, tabletop exercises, and response resources. **Dragos Intelligence** employs specialized vulnerability management analysis to correct and enrich CVSS, as well as providing alternative mitigation strategies. That intelligence is integrated into Dragos Platform and is available as part of a separate WorldView subscription.
Cybersecurity Resilience	**Dragos Services** provides proactive risk analysis, architecture, and incident response planning (and resources) to assure continued operations minimize the impacts on industrial control systems in OT environments from disasters caused by cybersecurity incidents. **Dragos Platform** provides the protection that enhances the resiliency and reduces susceptibility of OT assets from cyber threats and vulnerabilities. **Dragos Intelligence** provides the insight into attack groups, threat activity, and TTPs that can increase response times and reduce MTTR.
Third-Party Cybersecurity	**Dragos Services** provides OT Security Program Assessment and Architecture reviews that can help facilitate design and implementation of these policies. Further, **Dragos Platform** can validate effectiveness of the controls and monitor third party interaction with OT systems for cyber risk.

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.