DRAGOS®
SAFEGUARDING CIVILIZATION

Support for CISC Enhanced Cyber Security Obligations (ECSOs) for Industrial Systems

> **Dragos provides the expert technology and solutions needed to fulfill the cyber protections required for Systems of National Significance (SoNS)**

Enhanced Cyber Security Obligations (ECSOs) are defined by SOCI legislation for Systems of National Significance (SoNS). The ECSO's are brief and represent core elements of effective cyber protections for industrial systems identified as "systems of national significance." To fulfill these obligations requires deep expertise in industrial control systems (ICS) and operational technology (OT) incident response, vulnerability analysis, and threat detection.

Dragos specializes in ICS/OT cybersecurity solutions and support. We combine a scalable technology platform, insightful threat intelligence, and an ecosystem of expert consulting services that you can leverage to fulfill SOCI ECSOs. We work across industrial sectors – power generation and distribution, transportation, mining, oil and gas, building automation and data centers, and manufacturing - protecting hundreds of customers and hundreds of thousands of assets every day.

Our portfolio of OT cybersecurity solutions includes:

Clear View of Assets, Hazards, & Vulnerabilities
The Dragos Platform streamlines the discovery and monitoring of OT assets, matching those systems to vulnerabilities with a "now, next, never" risk-based prioritisation for mitigating vulnerability risk.

Know Your Risk & Plan Mitigation Controls
Dragos Professional Services experts help to evaluate cyber risk and defensive posture, helping you chart a path to more effective risk mitigation and lessen the impact from potential cyber incidents.

Monitor Systems & Respond to Potential Threats
Ongoing monitoring of critical assets is key to reducing cyber risk. Intelligence-driven threat detection provides fast warning to attacks, while response playbooks and IR experts can help you quickly investigate and contain incidents.

DRAGOS AUSTRALIA

Protecting Australian critical infrastructure has long been a Dragos priority. Dragos's APAC Headquarters is in Melbourne, Australia with a 30-seat capacity ICS/OT cybersecurity training facility. We now have over 20 local team members, that include:

- Expert solution architecture & relationship management

- ICS threat intelligence analysts and threat hunters

- OT incident responders and professional services team

- Cybersecurity partners and resellers

Mapping Dragos Capabilities to the CISC SoNS Enhanced Cyber Security Obligations

SONS ECSO REQUIREMENT	DRAGOS CAPABILLITY	DRAGOS CAPABILITY DESCRIPTION
Developing **cyber security incident response plans** to prepare for a cyber security incident	Dragos Incident Response Services & Rapid Response Retainer (RRR)	Our experienced OT incident responders will guide you through the process of developing and maturing your incident response plans. A Rapid Response Retainer (RRR) provides access to analysis, investigation, and remediation advice for incidents, while our onboarding workshop review your incident response plans and maturity, offering best practice enhancements from our experience.
Undertaking **cyber security exercises** to build cyber preparedness	Tabletop Exercises (TTX) & Architecture Reviews	Dragos Tabletop Exercises (TTX) test response plans based on threat scenarios from real-world adversary TTPs. We help you evaluate response, identify weaknesses, and refine your incident response plans. Dragos OT Cybersecurity Assessments (OTCA) assesses vulnerabilities and topologies, and other aspects of your architecture, identifies your crown jewels and makes recommendations for better cyber defense.
Undertaking **vulnerability assessments** to identify vulnerabilities for remediation	Vulnerability Assessments & Risk-Based Vulnerability Management	A Dragos Vulnerability Assessment, available also through RRR burn down, inventories OT assets and matches them against our vulnerability database. We provide a prioritised analysis for remediation, including alternative mitigations suitable for OT. The Dragos Platform is used to maintain up-to-date view of assets and vulnerabilities, with risk-based "now, next, never" guidance to manage asset inventories and vulnerabilities continuously.
Providing system information to **develop and maintain a near-real-time threat picture**	Dragos Platform	The Dragos Platform provides continuous monitoring of OT systems and networks, creating real-time asset inventories and capturing network and event logs, system telemetry, and alerts/threat behaviors in real time. Dragos can support SoNS entities to provide this information in a timely fashion.

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