Support for CISC Risk Assessments to Achieve SOCI Compliance

Dragos provides the expert technology and skills needed to help industrial organisations be SOCI compliant and reduce cyber risk of critical systems

SOCI legislation introduced key compliance requirements for industrial companies in Australia. The Australian Critical Infrastructure Resilience Strategy (CISC) provides a framework for industrial organisations and government to collaborate to achieve SOCI compliance. The CISC Risk Assessment Methodology outlines steps to assess and address that cyber risk.

Dragos can assist owners and operators of critical infrastructure achieve the outcomes described in the CISC Risk Assessment Advisories and, in doing so, improve their ability to Prevent, Detect, Respond and Recover from incidents.

Our OT cybersecurity technology and solutions offer:

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.

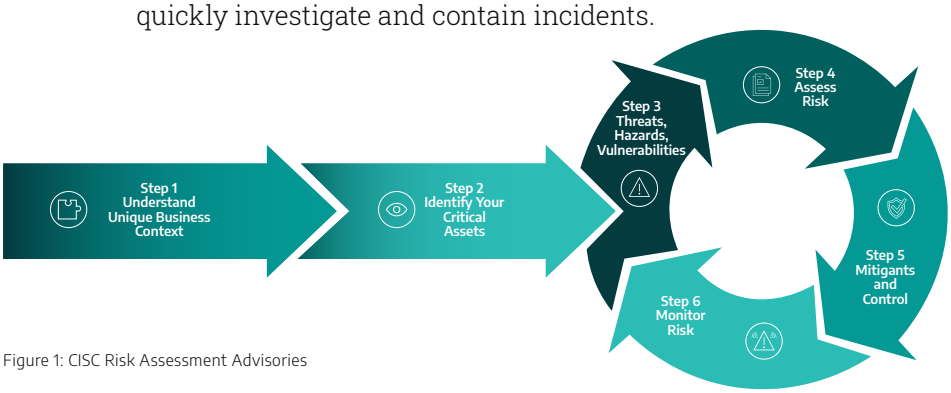

Figure 1: CISC Risk Assessment Advisories

CISC RISK ASSESSMENT

As part of Australia's Critical Infrastructure Resilience Strategy, amendments to the SOCI introduced mandatory Risk Management (CIRMP) reporting obligations for owners and operators.

CISC has provided the CISC Risk Assessment Advisories which propose a six-step process for assessing and managing cybersecurity risks.

Mapping Dragos Capabilities to the CISC Risk Assessment Advisories

STEP	DESCRIPTION	DRAGOS CAPABILITY
Step 1	Understand business & sector landscape	Dragos experts are drawn from across a wide range of critical infrastructure sectors. Collectively we have first-hand experience and insights into the full range of Australian critical infrastructure verticals.
Step 2	Identify your critical assets	The Dragos Platform identifies critical assets by monitoring and analysing OEM systems network traffic and provides visual maps and monitors for changes. Our Professional Services consultants work with you to review asset topology and identify crown jewel assets to help prioritise risk mitigation.
Step 3	Threats, hazards & vulnerabilities	Dragos Threat Intelligence tracks threat groups, monitors active campaign activities, and analyses TTPs for adversaries that target infrastructure. We identify vulnerabilities and analyse CVEs issued by other parties, often correcting risk scores and adding mitigation steps suitable for OT networks. The Dragos Platform compiles vulnerability and threat intelligence and applies it to your asset base to create an active risk assessment of threats, hazards, and vulnerabilities in your environment, enabling you to evaluate hazards like open ports, remote access connections, vulnerable protocols and much more. Dragos Professional Services works with numerous organisations to actively investigate adversaries and their tactics for those that have been targeted.
Step 4	Assess risk	Dragos Professional Services help customers assess risk by identifying crown jewel assets, analyse threat scenarios that evaluate consequences of successful attacks, including the likelihood of attacks. They evaluate the architecture and security controls, creating recommendations for stepwise improvement. Dragos Threat Intelligence is critical to assessing cyber risk, evaluating new vulnerabilities, threat groups, active campaigns for insight into the probability of attack.

Step 5	Identify mitigations and implement controls	Dragos Platform continuously monitors your OT asset networks. It analyses traffic and systems to identify vulnerabilities and hazards that drive changes to architecture to PREVENT threats. It analyses threat behaviors to allow you to DETECT potential attacks, providing the detailed forensics and prescriptive playbooks to quickly investigate and RESPOND to events. Dragos Professional Services helps to assess your OT cyber architecture, OT security program, and Incident Response plans. We provide Incident Response Services in case of an event, and tabletop exercises to help improve your plans.
Step 6	Monitor risk	The Dragos Platform provides continuous monitoring for both vulnerability risk, hazards, and active threats to your systems. Dragos Threat Intelligence allows you to monitor campaign activity, threat groups, vulnerabilities, and TTPs particular to your OT environments.

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.

Copyright ©2023 Dragos, Inc. | All Rights Reserved. | Last updated October 2023