How Dragos Supports Singapore CCoP for Critical Information Infrastructure

Dragos provides industrial organisations with the expert technology, intelligence, and consulting services to help protect OT Critical Information Infrastructure (CII OT), helping fulfil CCoP compliance requirements.

The Cybersecurity Act of 2018 provided the Commissioner of Cybersecurity powers to investigate cybersecurity threats and incidents, to determine their impact, & to prevent further harm. Thus, the Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure (CII) was established, last updated in December 2022. The CCoP provides detailed guidelines for protecting critical infrastructure, including Operational Technology (OT).

Dragos specialises in cyber security for OT. We help industrial organisations in electric, oil & gas, transportation, water, mining, & manufacturing to protect their OT systems. Dragos' unique combination of a technology platform, OT-specific threat intelligence, and consulting services provide the key resources to build an effective OT threat defence.

Audit, Governance, & Training for OT

Dragos Services provides OT Cybersecurity Assessments, Pen Testing, Incident Response, Training & other services delivered by skilled OT cyber consultants to help evaluate & recommend key steps to build cybersecurity maturity.

Identify OT Assets, Detect & Hunt Threats

Dragos Platform automates OT asset inventory, with risk-based vulnerability management & threat detection for OT systems. Continuous monitoring prioritises notifications, while detailed logging enables fast investigation & hunting. Optional OT Threat Hunting services are available via OT Watch.

Response & Recovery from Cyber Events

Incident Responders experienced in OT cyber event investigation and recovery are available via Rapid Response Retainer. Retainer hours can be used for Assessments, Pen Tests, & Tabletop Exercises & more, to help optimise response plans and protection posture for OT.

DRAGOS – SPECALISING IN OT CYBERSECURITY

Dragos was founded in 2016 by the practitioners who created the ICS cyber mission for US Government agencies.

The founders saw the problem of persistent OT cyber-attacks by a growing number of adversaries were not being addressed. So, they hired the most experienced team of ICS/OT security practitioners – threat hunters, researchers, and incident responders - to help build the Dragos

Requirements of Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure (CII)

The CCoP provides detailed requirements for protecting Critical Information Infrastructure (CII). Dragos focuses exclusively on Operational Technology (OT) cybersecurity, and here map our capabilities against the CCoP.

MAPPING OF DRAGOS CAPABILITY TO CCOP

SECTION	DESCRIPTION	DRAGOS CAPABILITYRELATING TO OPERATIONAL TECHNOLOGY (OT)
1. PRELIMINARY	*Glossary of terms and high-level applicability of the framework*	Dragos supports a wide range of capabilities that help fulfil CCoP requitements for CII OT.
2. AUDIT	*Requirements for remediating findings from audits performed by CIIOs to ensure compliance*	Dragos provides audits of OT cyber architecture, including Vulnerability Assessments, Compromise Assessments, evaluation of network topology and other elements of the architecture. We include prioritised recommendations for remediation. All can be used to help fulfil the Audit requirements for CII OT.
3. GOVERNANCE REQUIREMENTS	*Establishing and maintaining frameworks to ensure cybersecurity strategies are aligned with its business objectives. It also provides guidance to the CIIO in evaluating, defining, and directing efforts to manage cybersecurity risks.*	Dragos provides program reviews to help evaluate the cyber program for OT (3.2.1). Dragos Services directly align with Risk Identification, Analysis, & Evaluation (3.2.2 a, b, c) with OT Cybersecurity Assessment (OTCA) that includes identification of assets, compromise, vulnerabilities; and scenario-based risk analysis for OT crown jewels,; we deliver threat hunting services; we provide Incident Response services that include post incident reviews. All include reports with prioritised recommendations that can be utilised by the CIIO for Risk Response and Risk Registers relating to 3.2.4 & 3.2.5. **Dragos Platform provides continuous identification of assets and changes, threat detection, vulnerability management, and data sets that aid in incident investigations. Optional OT Watch augments that with Continuous Threat Hunting Services.** Dragos provides program reviews to help evaluate the cyber program that include Policies, Standards, Guidelines & Procedures relevant to OT cyber for Section 3.3. Dragos OT Cybersecurity Assessment (OTCA) helps to evaluate Cybersecurity Design Principles in 3.5 as well as evaluating Use of Cloud Computing in Section 3.7. Program reviews can be scoped to include review of Change Management processes in Section 3.6. Dragos can also perform above services of OT systems for related to Section 3.8 Outsourcing and Vendor Management.

4. IDENTIFICATION REQUIREMENTS	*Assist the CIIO in understanding and identifying the resources and assets supporting the CIIO's critical business functions in delivering essential services, and the associated cybersecurity risks. It enables the CIIO to focus and prioritise its efforts in protecting these assets.*	Dragos Platform enables the discovery of OT assets that can provide the basis to then add other information required in Section 4.1.1. Dragos Platform tracks changes in asset inventory that can assist in Section 4.1.2.
5. PROTECTION	*help the CIIO understand and implement the required people, process, and technology controls to protect the CII and to limit and contain the impact of cybersecurity incidents.*	Dragos Services and the OTCA can help assess architectures and policies around the controls for OT systems in Section 5, while the Dragos Platform provides network monitoring to help validate controls around those same elements. Section 5.10 Patch Management: the Dragos Platform actively tracks vulnerabilities for OT assets, including status of patches as well as alternative mitigations especially useful in OT environments. That information can be used to instrument the requirements in 5.10. Section 5.14 Vulnerability Assessments, and 5.15 Penetration Testing: Dragos Services conducts Vulnerability Assessments for OT environments as well as Penetration Tests as standard service offerings. Section 5.16 Adversarial Attack Simulation may be defined as an added SOW but is not a standard service offering.
6. DETECTION	*…aim to assist the CIIO in understanding and implementing the required people, process and technology controls to detect and identify any malicious activity or vulnerability that could compromise the CII…*	Section 6.1 Logging: Dragos Services Rapid Response Retainer (RRR) onboarding helps the CIIO review the key systems and logging for OT systems, what Dragos terms Collection Management Framework (CMF) Section 6.2 Monitoring and Detection: Dragos Platform performs continuous monitoring and detection of OT system environments including scanning for IOCs, establishing baselines of behaviours, generating alerts for potential threats identified via advanced behavioural analytics, enabling analysis of events, and providing the information for reporting. Section 6.3 Threat Hunting: The Platform can be used to enable Threat Hunting in OT environments; optional OT Watch service leverages Platform to perform continuous threat hunting through both automated analytics and experienced OT threat hunters. Section 6.4 Cyber Threat Intelligence & Information Sharing: Dragos WorldView intelligence is a subscription services that provides in depth cyber threat intelligence (CTI) focused on OT as described in 6.4.1. Dragos Platform includes optional Neighborhood Keeper that provides mechanisms to share information on threats and vulnerabilities outlined in 6.4.2

7. RESPONSE AND RECOVERY REQUIREMENTS	*… seeks to minimise the impact of cybersecurity incidents through processes that include the identification, containment and eradication of cybersecurity threats, and the recovery of systems, root-cause analysis and implementation of corrective actions to prevent recurrence…*	Dragos Services provides comprehensive services for OT Incident Response. We help evaluate and recommend improvements for IR Plans outlined in 7.1 & 7.2; we provide Responders skilled in investigations for cyber events in OT. We provide Tabletop Exercises that test those plans as outlined in Section 7.3.
8. CYBER RESILIENCY REQUIREMENTS	…includes maintaining the ability of the CIIO and CII to withstand cybersecurity incidents, continue the delivery of essential services and recover from cybersecurity incidents…	Dragos Services can provide review of backup and restoration processes as part of expanded SOW in an OTCA but does not offer a standard service in this area.
9. CYBERSECURITY TRAINING & AWARENESS	*… helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cybersecurity incidents that they may encounter in their work…*	Dragos Services can provide review of Cybersecurity Awareness Program as part of expanded SOW in an OTCA but does not offer a standard service in this area. Dragos Academy provides on-demand training on OT cybersecurity concepts and skills, plus instructor-led training on OT cyber basics.
10. OPERATIONAL TECHNOLOGY (OT) SECURITY REQUIREMENTS	… apply to CII which are OT systems.	Dragos Services OTCA can help to assess network segmentation requirements outlined in Section 10.2.1, 10.2.3, 10.2.4, 10.2.6. Dragos Platform monitors data flows and triggers alerts for threat behaviours and anomalies as described in 10.2.2. Dragos does not provide any standard services that address 10.3 or 10.4.
11. DOMAIN-SPECIFIC PRACTICES	… applies only to CII which CII assets include internet-facing Domain Name System (DNS) servers	Dragos Services OT Cybersecurity Assessment can help to assess impact OT systems and networks for DNSSEC

Dragos for Full Spectrum of OT Security Capabilities

Dragos, Inc. has a global mission to safeguard civilisation. We are privately held and headquartered in the Washington, DC area with regional offices in Canada, Australia, New Zealand, Europe, and GCC.

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