THE CHALLENGE OF NEW REGULATIONS

Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act)

Security of industrial systems is becoming increasingly critical to the well-being of society as a whole. The continuous function of mining operations, oil and gas, chemical plants, manufacturers, power, and water are critical to the economy – and life itself.

Protecting the world of ICS/OT is a deeply complex mission. To ensure that operators are focused on that mission, the Australian Government passed the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) which went into effect on 2 April 2022.

> “The reforms in the SLACIP Act seek to make risk management, preparedness, prevention and resilience, business as usual for the owners and operators of critical infrastructure assets... These reforms will give Australians reassurance that our essential services are resilient and protected.”
>
> Australian Government
> Department of Home Affairs

What Is In The **SLACIP Act**?

The challenge as an asset owner and operator is to clearly understand the requirements of the new regulations, to identify resources to help achieve compliance, and do the work. In summary, the SLACIP Act amends the Security of Critical Infrastructure Act 2018 in the following ways:

- It expands the list of covered industries from four in 2018 to eleven in 2022.
- Adds requirements for adopting a critical infrastructure risk management program - or a reporting obligation for assets not covered by a risk management program
- Adds definition for “Systems of National Significance” (SoNS) – a not-yet-specifically defined criteria of assets that would have significant consequence if a hazard were to occur that had a significant relevant impact on the asset
- Enhanced cyber security obligations for assets declared / registered as SoNS. Those obligations include an incident response planning, cyber security exercises, vulnerability assessments, and access to system information.

A key issue to note is that, while the SLACIP Act has passed, specifics of the requirements – risk management program, definition of SoNS, enhanced cyber security obligations – are in draft form, subject to review, amendment, and finalization.

DRAGOS – Helping You Develop Effective Security Program For Critical Infrastructure – And Simplify Compliance With The SLACIP Act

Dragos 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:

- 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, cyber security exercises, vulnerability assessments, and maintaining up to date system and asset information.
- 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.

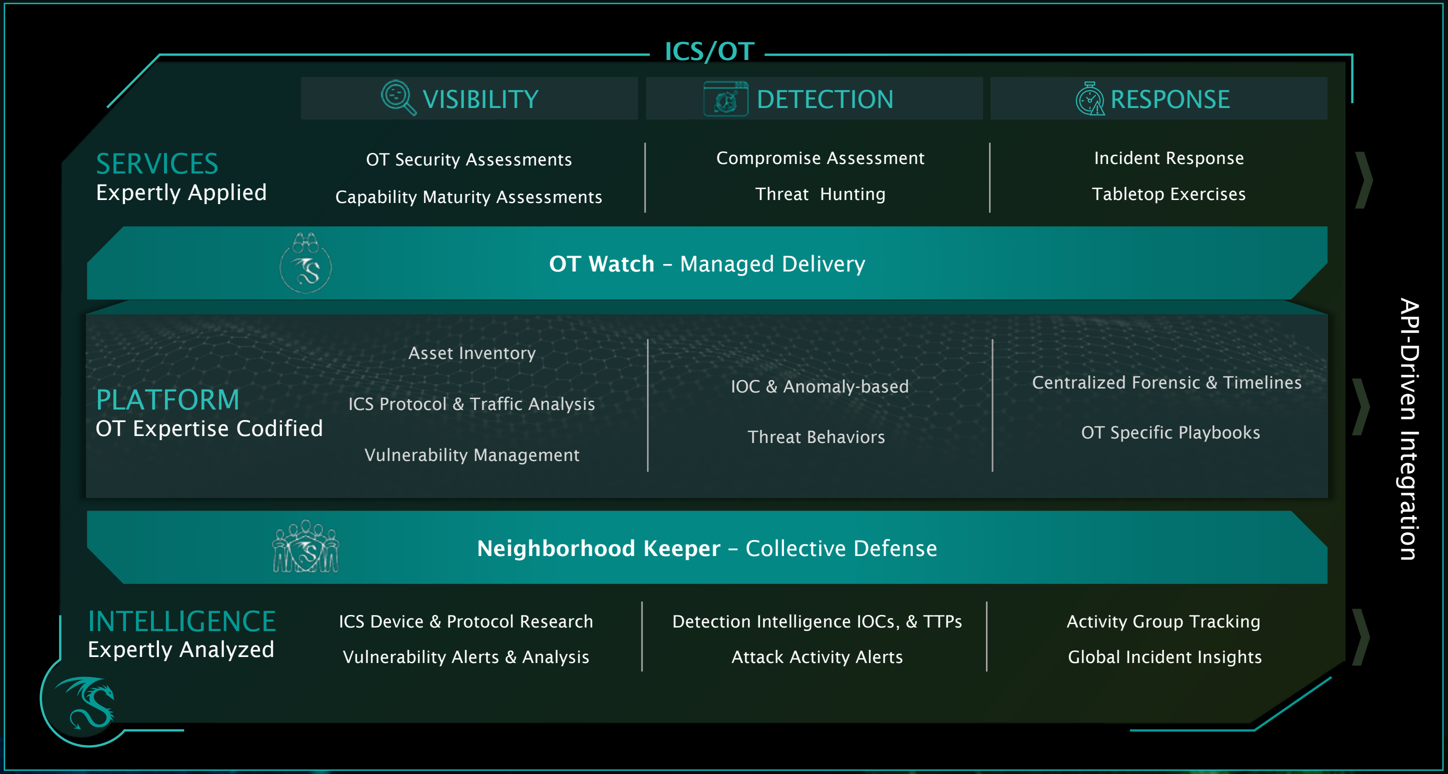
Mapping SLACIP Act Requirements to Dragos

There are a number of specifics not yet resolved with components of the SLACIP Act. Accordingly, we will provide a high-level mapping of Dragos capabilities. Dragos serves the industrial side of critical infrastructure, focusing on operational technology for industries covered by SLACIP that include Water and Sewage, Energy, Transportation, Food & Beverage Manufacturing, Space, and Defense. We provide a subset of capability for Data Storage & Processing, Communications, and Health Care / Medical. Below is a high-level analysis of where we can help.

SLACIP ACT COMPONENT	DRAGOS CAPABILITY	DESCRIPTION
Risk Management Program • Identify hazards that could have a relevant impact to assets • Minimize or eliminate risk of hazard occurring • Mitigate relevant impact of hazard on asset	Dragos Global Services Compromise Assessment or OT Program Assessment Dragos Platform Asset Inventory & Vulnerability Mgt	Dragos Global Services provides an in depth OT Program Assessment with a comprehensive review and recommendations for a risk management program; a subset of that capability is offered as Compromise Assessment. Dragos Platform provides automation of asset inventory and vulnerability management to identify risks and mitigate impacts
Register Systems of National Significance (SoNS) - criteria TBD	Dragos Services Crown Jewel Analysis (part of OT Program Assessment)	Dragos Global Services can help identify your critical OT assets and consequences of hazards that can be useful in submitting to the Minister.
Enhanced cyber security obligations for SoNS • Incident response planning, • cyber security exercises, • vulnerability assessments, • access to system information	Dragos Global Services Incident Response Plan/Retainer, Tabletop Exercises, Compromise Assessment / Vulnerability Assessments Dragos Platform Asset Inventory	Dragos Global Services have deep experience in helping to develop OT incident response plans, provides a retainer model and resources to assist in incidents. Table Top test and refine those plans; Dragos Compromise and Vulnerability Assessments are core offerings. Dragos Platform provides detail information base for incident instigation & reporting.

DRAGOS SOLUTIONS

Dragos 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.



ICS/OT

	VISIBILITY	DETECTION	RESPONSE
SERVICES Expertly Applied	OT Security Assessments Capability Maturity Assessments	Compromise Assessment Threat Hunting	Incident Response Tabletop Exercises
OT Watch – Managed Delivery			
PLATFORM OT Expertise Codified	Asset Inventory ICS Protocol & Traffic Analysis Vulnerability Management	IOC & Anomaly-based Threat Behaviors	Centralized Forensic & Timelines OT Specific Playbooks
Neighborhood Keeper – Collective Defense			
INTELLIGENCE Expertly Analyzed	ICS Device & Protocol Research Vulnerability Alerts & Analysis	Detection Intelligence IOCs, & TTPs Attack Activity Alerts	Activity Group Tracking Global Incident Insights

API-Driven Integration

Dragos Global Services Offering Details

SERVICE	DESCRIPTION		
Architecture Reviews	**Compromise Assessment**	**Architecture Review**	**OT Program Assessment**
	Utilize the Dragos Platform to look for vulnerabilities in your environment. Analyze asset maps, threat behaviors, asset and protocol vulnerabilities, insecure credentials.	Each Architecture Review is uniquely tailored to customer goals, to provide an understanding to the most critical ICS systems in your environment, and the potential consequences of a cyber-attack on those systems, and helps to shape and prioritize the protection, detection, and response efforts	Evaluate your existing cyber security program with an understanding of your existing network and security posture, and their relationship between your detection and response capabilities. Includes Program Review, CMF, Crown Jewel Analysis, and a Topology Review, and more.
Capability Maturity Assessment	Understand your OT organizational maturity using a crawl, walk, run approach. Use assessment to create a roadmap that includes reviewing your assets and incident response plans, set milestones for operationalizing your OT controls, work towards the goal of optimizing your risk reduction.		
Penetration Tests Assess Exploitable Vulnerabilities	**Network**	**Device**	**Application**
	Attempt a system compromise and privilege escalation, leveraging access to pivot within the network.	Review effectiveness of security controls, identify hardware and software vulnerabilities and device attack surface.	Identify hardware and software vulnerabilities, and get expert recommendations to strengthen your overall security posture.
Vulnerability Assessment	Identify vulnerabilities within your network, hosts, field devices, and applications		
Compromise Assessment	Evaluate for common indicators of an ongoing or prior network compromise, looking for IOCs, threat behaviors, and vulnerable assets and protocols		
Threat Hunt	A comprehensive threat hunt, tailored to your unique environment, looking for existing threats across targeted assets. Get visibility into OT systems, networks and assets, advanced threat modelling and detection, and understand the operational impact		
	Incident Response Retainer (IRR)		**Non-Retainer**
Incident Response Services	IRR provides services for planning, preparing, and responding to incidents, with experts on standby 24x7 and guaranteed response times. Burn down retainer hours on any Dragos service. Retainer customers get onboarded with a Readiness Assessment workshop, which includes a document review, IR best practices overview, and a C2M2 maturity assessment.		Non-retainer customers follow a pay-as-you-go model with best effort response time.
Tabletop Exercises Evaluate Your OT Defensive Posture	**Standard TTX**	**Custom TTX**	**Executive TTX**
	Applies to any industry, and covers a generalised threat scenario for IR teams to test capabilities, based on real-world adversary TTPs	Customised consequence-driven scenario specific to your network and threat landscape. Challenge mature incident response teams with tailored events and artifacts	Curated scenario to assess the executive management of communications, information sharing, reputational concerns, and operational impact

Dragos Platform Offer Details

DRAGOS PLATFORM		
Visibility	Asset Inventory and Profiles	Build asset inventory depth through “operations safe” passive collection and device level detail. Establish asset profile baselines for connected integrations with firewall, SIEM, and CMDB systems. Group assets in a visual map with customizable zones for easier cyber-ops management. See historical changes with timeline views to spot unexpected activity.
	ICS Protocol Analysis & Traffic Analysis	Capture, analyze, and investigate device communications to improve the accuracy and understanding of devices in your environment. Monitor for remote connections and easily search historical activity.
	Vulnerability Management	Practical OT vulnerability intelligence and mitigation strategies with industry specific analysis, correction, and enrichment of known vulnerabilities. Alternative mitigation advice, prioritized with “Now, Next, Never” guidance. Vulnerability disposition tracking for full lifecycle management and to simplify audits.
Detection	IOC & Anomaly Detection	Expertly curated Indicators of Compromise (IOCs), malicious IPs, domains, and hashes analyzed by the Dragos Threat Intelligence team. Anomalous traffic patterns and baseline deviation alerts.
	Threat Behaviors	High signal, low noise intelligence-based detections mapped against MITRE ATT&CK for ICS. Composite detections from analysis of threat group tactics, techniques, and procedures (TTPs).
Response	Centralised Forensics & Timelines	Provide responders with the tools to triage and investigate potential incidents. Centralized forensics and timeline views to coordinate across OT and IT teams.
	OT Specific Playbooks	Incident response playbooks with OT-centric guidance from industry experts. Collect evidence and organize case notes in the analyst investigation workbench.
System Deployment	Deployment	The Dragos Platform architecture is able to accommodate a full range of customer deployment requirements including on premises and cloud based. Dragos Platform appliances are available in both virtual and physical models including ruggedized sensors designed for harsh industrial environments

**To learn more about Australian SLACIP Act please,
please contact sales@dragos.com or visit dragos.com/services**