Australian Critical Infrastructure and SOCI Regulations

Darktrace Compliance

DARKTRACE

Implementing the SOCI Act

The SOCI (Security of Critical Infrastructure) Act was first passed by the Australian Government in 2018, with amendments passed in 2021 and 2022.

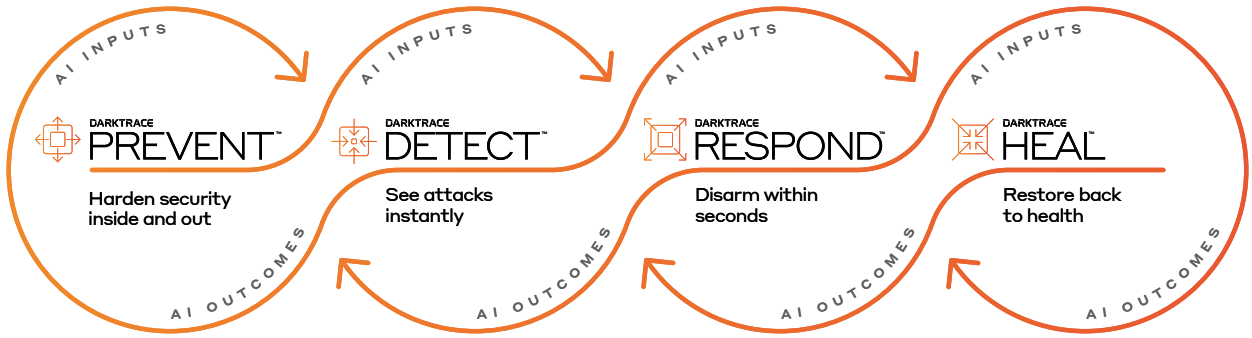
As of April 2023, the legislation covers eleven critical infrastructure sectors including healthcare and medical, food and grocery, and higher education and research.

A significant portion of the SOCI Act and its amendments can be described by three Positive Security Obligations (PSOs) which aim to strengthen resilience of critical infrastructure assets. They require Critical Infrastructure organisations to report ownership and operational information of their critical assets, to notify Government entities when a cyber-attack occurs, and to adopt and maintain a Risk Management Program (RMP).

In addition, a subset of organisations covered by the SOCI Act are defined by SoNS (Systems of National Significance). SoNS are required to fulfil an enhanced list of cyber requirements, including incident response planning and cyber tabletop exercises. While a list of SoNS is not publicly available, the impacted organisations have been or will be notified by the Federal Government in private.

Darktrace Products

The Darktrace Cyber AI Loop creates a feedback system in which each capability continuously and autonomously hardens the entire system. The Cyber AI Loop augments human performance with AI coverage of digital ecosystems at a scale far beyond the capabilities of security staff. Additionally, explainable AI natural language processing delivers clear reports and frames information for decisions made by humans across the entire Cyber AI Loop. Darktrace is committed to uplifting the security of Australian Critical Infrastructure to meet their security goals.



Darktrace PREVENT

The PREVENT product family consists of two products: PREVENT/Attack Surface Management (or ASM), which continuously monitors your attack surface for known and unknown external risks, and PREVENT/End-to-End (E2E), which hardens defenses internally, testing and prioritizing the most critical attack paths in your organization.

Darktrace DETECT

Powered by a bespoke, continuously evolving understanding of you, Darktrace DETECT delivers instant visibility of threats – even those using novel malware strains or new techniques.

Darktrace RESPOND

Darktrace RESPOND works around the clock to take targeted action and disarm threats without disrupting day to day business operations. Being fully autonomous, RESPOND is also fully customizable and allows users to set boundaries for AI actions.

Coverage Areas

Darktrace technology works for organizations of all sizes and can be brought to any environment, protecting email and cloud services, endpoints, zero trust technologies, and IT/OT networks.

Darktrace and SOCI PSOs

Darktrace Cyber AI is used by organisations across all 11 CI sectors to uplift their cyber security posture. In Australia, Darktrace empowers security teams in line with SOCI Act requirements.

Register of Critical Infrastructure Assets PSO 1: Information Provision

Under Part 2, the Australian Government must keep a register of critical infrastructure assets. Responsible entities are required to provide ongoing information about these assets and must notify the government of events that impact their operation.

- Darktrace DETECT can provide ongoing information about the status of critical infrastructure assets, including their operational status and performance.
- The Darktrace/OT coverage area fully maps and monitors the digital aspects of a critical infrastructure asset, as it passively identifies devices from centralised locations.
- Darktrace PREVENT/ASM continuously monitors Internet-facing assets associated with an organization.

Darktrace's self-learning asset identification provides teams with full visibility of all devices communicating within a digital estate and updates the list as the business evolves, equipping teams with accurate asset information.

Notification of Cyber Security Incidents PSO 2: Mandatory Cyber Incident Notifications

Under Part 2B, responsible entities must notify the Australian Government of cyber incidents which impact critical assets.

Darktrace DETECT autonomously investigates and reports upon cyber incidents in real time with Cyber AI Analyst:

- Cyber AI Analyst provides a complete view of an incident, with a plain English summary alongside technical details such as time stamps and IP addresses.
- Cyber AI incidents can be printed in PDF format for distribution or exporting to other security tools such as a SIEM or SOAR.
- Cyber AI incidents enable teams to confidently determine the location and extent of a cyber attack, reducing response times and uplifting IR teams should they be needed.

Darktrace RESPOND autonomously contains a threat, disrupting an attacker and buying time for the defenders.

More on Darktrace's AI Analyst and Compliance

Darktrace DETECT provides the real-time visibility required to make intelligent decisions in live situations, while enabling in-depth investigations into historical activity using Cyber AI Analyst.

A list of what is included in an AI Analyst incident:

- A high-level Summary of the incident and associated Model Breaches.
- A detailed timeline highlighting relevant events related to the incident.
- Attack phases involved in the incident (e.g. Initial infection, established foothold, privilege escalation, etc.)
- A list of Related Breaches and Breached Devices.
- Summary details around connections, endpoints, files, beaconing activity, etc.
- The ability to create a shareable report of the incident in a PDF that can be shared with the relevant stakeholders.
- The ability to acknowledge the incident and remove it from the incident tray.
- The ability to drill down into more detailed windows and different sets of data for purposes of threat hunting and focused incident response.
- Can conduct on-demand investigations around individual devices as determined by the security team.

Darktrace is already helping organizations in the United States comply with national security requirements. For example, on March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law. Like the Australian SOCI act, this legislation requires critical infrastructure owners and operators to quickly notify the Cyber and Infrastructure Security Agency (CISA) of ransomware payments and significant cyber-attacks.

Darktrace/OT extends Darktrace's comprehensive coverage to OT assets and networks, empowering organizations to:

- Identify all OT assets communicating on an IP-connected network including serial-connected devices.
- Detect reprogram events and firmware updates.
- Track CVEs associated with OT devices.
- Threat hunting across a wide range of supported OT protocols, such as S7, Modbus, DNP3, CIP and OPC-UA.
- Visibility into network topography and IT/OT communication patterns.

Cyber and Information Security Hazards PSO 3: Risk Management Plans (RMPs)

Under Part 2A, responsible entities must create and adhere to RMPs that address risks to critical infrastructure assets. For each asset, the RMP must identify and minimise material risks, and mitigate the impact of realised incidents.

Identifying material risks to cyber and information security:

- Darktrace PREVENT assesses which external (ASM) and internal (E2E) assets are susceptible to being used in a cyber incident and in what ways.
- E2E intelligently prioritises technical risks within a digital estate before an incident has taken place, such as the use of outdated protocols or insecure remote access solutions.

Minimising cyber and information security risks to prevent incidents:

- PREVENT provides a list of recommended actions to reduce cyber risk within a digital environment.
- PREVENT outputs are used by DETECT and RESPOND to identify and disrupt cyber attacks using a 'defence in depth' approach to further minimise cyber risk.

Mitigate the impacts of realized incidents:

- Darktrace/OT extends visibility and risk management to operational technology, including SCADA, ICS and IIoT.
- RESPOND is focused on containing incidents to reduce the spread and damage of malicious or unwanted cyber events.
- HEAL assists in recovering from cyber incidents and return systems to a trusted operational state.

SOCI Act PSO	Description	Darktrace Coverage
Information Provision	A requirement for most Critical Infrastructure organisations to report operational information, such as asset lists and control information, to the Department of Home Affairs.	PREVENT/ASM Darktrace DETECT Darktrace/OT
Cyber Incident Notifications	The Mandatory Cyber Incident Notifications obligation requires organisations to notify government entities when a cyber-attack has occurred.	Darktrace DETECT Darktrace RESPOND Cyber AI Analyst
Risk Management Programs	Responsible entities must identify and take steps to minimise or eliminate "material risks" that could have a "relevant impact" on the critical asset.	PREVENT/E2E Darktrace RESPOND Darktrace/OT

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,200 organizations globally from advanced cyber-threats.

Scan to LEARN MORE