ONAPSIS TURNKEY

Solution Brief

RESPONDING TO AUSTRALIA'S CRITICAL INFRASTRUCTURE CYBERSECURITY REFORMS

Meeting Positive Security Obligations
Integrating application layer security into your risk management program.

Visibility
Rapid identification and alerting of vulnerabilities and monitoring for unusual activity.

Management
Integration of application security information into SIEM, threat intelligence, development and workflow platforms.

Advice and Prioritisation
Assessing threats and vulnerabilities according to their impact and likelihood, advising on best practice action and prioritising remediation.

Automation
Rapidly meeting information gathering directives with automated vulnerability register, evidence collection, testing and validation of IT controls against security policies.

8 minutes
*one report of a cyber attack every 8 minutes**

25%
*cyber incidents associated with critical infrastructure or essential services**

* ACSC Annual Cyber Threat Report 2020-21

EXPANDED COVERAGE OF SOCI ACT

Under recent amendments to the Security of Critical Infrastructure (SOCI) Act, cybersecurity obligations now cover communications, data storage or processing, financial services and markets, water and sewage, energy, health care and medical, higher education and research, food and grocery, transport, space technology and the defence industry.

POSITIVE SECURITY OBLIGATIONS

Mandatory requirements include establishing, maintaining, and complying with a risk management program: identification of threats, mitigation of risks, minimisation of impact, governance and oversight. Critical infrastructure organisations also must undertake vulnerability assessments and provide access to system information as directed.

COMPLEX ECOSYSTEM TO SECURE

Mission-critical SAP applications are typically maintained by a combination of in-house teams and third-party developers and service providers, and hosted in a hybrid of cloud, hosted and on-premises infrastructure. Critical SAP vulnerabilities are being weaponised in under 72 hours, and new unprotected SAP applications provisioned in the cloud are being discovered and compromised in less than three hours.

ARE YOU COMPLIANT?

- Can your organisation demonstrate compliance with its positive security obligations for core business applications?
- Does your cybersecurity team have visibility and control on vulnerabilities and risks at the application layer?
- Do your current security providers and solutions go deep enough into the code base of your critical systems?

To better understand how Onapsis can assist you in complying with the SOCI Act, or to get a firsthand look at the capabilities of The Onapsis Platform, request a meeting now at https://onapsis.com/request-a-demo.