WHITE PAPER

NAVIGATING AUSTRALIA'S SECURITY OF CRITICAL INFRASTRUCTURE (SOCI) ACT: A COMPREHENSIVE GUIDE

LEVERAGING INFOBLOX FOR ENHANCED NETWORK SECURITY AND COMPLIANCE

Infoblox Product Marketing

TABLE OF CONTENTS

INTRODUCTION

The Security of Critical Infrastructure (SOCI) Act of 2018 is a cornerstone of Australia's cybersecurity landscape, designed to safeguard critical infrastructure assets from many threats, ranging from cyberattacks to natural disasters. By understanding the act's provisions and compliance requirements, organizations can bolster their cybersecurity posture, mitigate risks and contribute to the overall resilience of Australia's critical infrastructure. This white paper reviews the SOCI Act's objectives and implications for regulated organizations and shows how Infoblox can be an important partner in addressing the requirements of SOCI.

AUSTRALIA'S RISING TIDE OF CYBERCRIME CREATED A COMPELLING NEED FOR SOCI

Australia is grappling with an escalating wave of cybercrime, which includes ransomware, data breaches and targeted attacks on critical infrastructure. This includes a significant rise in cybercrime, with data breaches increasing by 26% in 2023, as reported by the Australian Institute of Criminology. Critical infrastructure continues to be a prime target, with the ACSC's 2022-2023 Cyber Threat Report noting a significant increase in attacks, revealing vulnerabilities within these networks. Ransomware remains a major threat, with several high-profile attacks causing substantial disruptions and financial losses, including a 2021 attack on a major logistics company and a 2022 attack on a local government agency.

CRITICAL INFRASTRUCTURE SECTORS UNDER THE SOCI ACT

The SOCI Act in Australia targets specific sectors[1] crucial to the nation's economy, security and society. If disrupted, these sectors are categorized as critical infrastructure due to their potential impact on public safety, economic stability, and national security. Critical infrastructure is those physical facilities, supply chains, information technologies and communication networks, which, if destroyed, degraded or rendered unavailable for an extended period of time, would significantly impact the social or economic well-being of Australia or affect the country's ability to conduct national defense and ensure national security.

The SOCI Act covers the following 11 sectors:[2]

1. **Communications:** Includes telecommunications networks, data centers and broadcasting infrastructure. This includes broadcasting, Domain Name Systems (DNS) and telecommunications.
    a. Critical **DNS** are defined in section 12KA of the SOCI Act and in the Definitions Rules. To be considered a critical DNS asset, your asset must be managed by an entity that is critical to the administration of an Australian DNS, be used in connection with the administration of an Australian DNS, and be critical to the administration of an Australian DNS. In this case, the asset would then be a critical DNS within the communications sector.
    b. The Definitions Rules prescribe the following assets within the .au country code top-level domain (ccTLD) system as critical to the administration of an Australian domain system:
        i. Registry database

1 *Critical Infrastructure Asset Class Definition Guidance*, Cyber and Infrastructure Security Centre, Australian Government, Home Affairs. April 2023.

2 *Security of Critical Infrastructure Act 2018 (SOCI)*, Cyber and Infrastructure Security Centre, Australian Government, Home Affairs.

ii. Public WHOIS service (https://whois.auda.org.au/)
iii. .au top-level authoritative DNS name servers
iv. The following second-level authoritative DNS name servers:
    - .com.au, .asn.au, .edu.au, .net.au, .id.au, .giv.au

2. **Data Storage and Processing:** Covers data centers, cloud services and data storage facilities.
3. **Defense Industry:** Involves defense-related manufacturing, research and development.
4. **Energy:** Encompasses electricity generation, transmission and distribution, as well as gas and petroleum infrastructure.
5. **Financial Services and Markets:** Includes banking, insurance and financial market infrastructure.
6. **Food and Grocery:** Covers food production, processing, distribution and retail.
7. **Healthcare and Medical:** Includes hospitals, medical facilities and pharmaceutical manufacturing.
8. **Higher Education and Research:** Covers universities, research institutions and scientific infrastructure.
9. **Space Technology:** Involves satellite systems, ground stations and space-related infrastructure.
10. **Transport:** Includes air, rail, road and maritime transportation, as well as ports and airports.
11. **Water and Sewerage:** Covers water treatment, distribution and wastewater management.

These sectors were selected based on their criticality to the Australian economy and society, and their potential vulnerability to disruptions. A disruption in any of these sectors could have cascading effects on other sectors and the broader community.

How Does Prudential Standard CPS 234 Interoperate with SOCI?

SOCI and CPS 234 share the important goal of fortifying cybersecurity and safeguarding critical infrastructure. While CPS 234 specifically targets the financial sector, mandating robust security measures for institutions like banks and insurers, SOCI adopts a broader scope, encompassing multiple critical infrastructure industries. Both frameworks underscore the importance of resilience against cyber threats, the maintenance of system stability and the imperative of swift responses to security breaches. In some ways, CPS 234 is similar to the European Union's (EU) Digital Operational Resilience Act (DORA) regulation in its focus on financial sector cybersecurity, while SOCI is also similar to the EU's NIS2 Directive in its comprehensive approach to critical infrastructure protection inclusive of cybersecurity considerations.

ROLE OF DNS IN SECURITY AND COMPLIANCE

DNS is the only infrastructure element in networks that is universal. Everything on the network needs DNS to connect. DNS also has information on which users/devices are accessing which resources at any given point in time, and historically as well. DNS is also the first hop from an end host before it does anything–access a website, send an email or access an application. DNS is closest to endpoints–not just laptops, but printers, infrastructure, smart thermostats, all of it. From a threat detection perspective, with DNS, you can not only watch the end-user devices, but the infrastructure as well. For example, new DNS beacons that connect to malware command-and-control (C2) infrastructure, could come from network infrastructure and not just end-user devices. All of this makes DNS a ubiquitous security control point that can be used to protect the entire network, including on-premises devices, remote users and cloud environments. You can turn something you use every day into a powerful security tool.

HOW INFOBLOX CAN HELP WITH SOCI COMPLIANCE

As a leading provider of DNS, DHCP and IP address management (DDI) solutions and DNS detection and response, Infoblox can play a pivotal role in enhancing network architecture and security, both of which are critical components of SOCI compliance. Let's explore how Infoblox addresses these key areas:

Network Design and Architecture

- **Zero Trust Architecture (ZTA):** While not a direct ZTA solution, Infoblox provides foundational elements for ZTA implementation. Infoblox offers granular control over DNS and IPAM, which facilitates the policy-based access controls required for ZTA.
- **Integration with Other Security Solutions:** Infoblox's solutions can integrate with other security technologies, such as firewalls, gateways, vulnerability management, and security information and event management (SIEM) solutions. This can enhance an organization's overall security posture and help meet the SOCI Act's requirements for a comprehensive approach to security.

Network Security Controls

- **DNS Detection and Response:** Infoblox's DNS-level security features provide enterprise-wide protection against threats, such as ransomware, phishing, botnets, lookalike domains, high-risk/suspicious domains, Zero Day DNS threats, domain generation algorithms and data exfiltration, reducing the risk of unauthorized access and data breaches.
- **IPAM:** IPAM prevents IP address conflicts and unauthorized IP assignments, while providing user and device context for security events, which helps significantly speed up incident response.
- **Dynamic Host Configuration Protocol (DHCP) Management:** Secure DHCP services protect against DHCP spoofing and unauthorized IP address allocation, and gather fingerprint information on devices as they join the network. This helps identify what type of assets are on the network for better visibility
- **Threat Intelligence:** Infoblox Threat Intel applies unique DNS analytics and tracks threat actor domains, identifying them as high risk and blocking them long before those domains are weaponized, proactively protecting organizations against emerging attacks before they occur. This can be particularly useful for meeting the SOCI Act's risk identification and mitigation requirements.

Network Monitoring and Management

- **Network Discovery:** Infoblox's network discovery capabilities provide visibility into network devices, aiding in identifying vulnerabilities and potential threats.
- **IPAM:** IPAM helps track IP address utilization, identify unused IP addresses and prevent IP address exhaustion.
- **DNS Analytics:** Provides valuable insights into DNS traffic patterns, helping to detect anomalies and potential threats.
- **Automation and Orchestration:** Infoblox's automation capabilities and integrations with IT and security tools can help organizations respond more quickly to security incidents, and reduce the time and effort required for routine tasks. This can be particularly useful for meeting the SOCI Act's incident response and risk management requirements.

Network Security Testing and Assessments

- While Infoblox doesn't directly offer penetration testing or red-teaming services, it provides essential data for these activities. For example, accurate IP address information and DNS records are crucial for vulnerability assessments and penetration testing.

Supply Chain Security

- Infoblox can indirectly contribute to supply chain security by providing visibility into network devices, their associated IP addresses and any potential malicious activity from those devices. This information can be used to assess potential vulnerabilities introduced by network equipment. In addition, Infoblox can be used as part of defense-in-depth security for threat detection and containment.
- Infoblox provides a managed domain monitoring service that can be used to monitor supplier domains to ensure that a lookalike domain is not being used to exploit the trust you may have in any given vendor.

Infoblox and Cloud-Based Networking

- Infoblox supports cloud-based networking by providing DDI services in hybrid and multi-cloud environments. This ensures consistent network management and security across different cloud platforms.
- Infoblox is vital in enhancing network architecture and security, which are fundamental to SOCI compliance. By providing granular control over DDI, Infoblox empowers organizations to build more resilient and secure networks.

Risk Management and Incident Response

- **Risk Management:** Infoblox provides the necessary tools to identify and manage DNS-related risks, a critical component of SOCI compliance.
- **Incident Response:** Infoblox can aid in rapid incident response and investigation by offering visibility into DNS traffic and device and user information.
- **Compliance Reporting:** Infoblox can provide valuable data for compliance reporting. This includes information about network activity, security incidents and the effectiveness of security controls. This can help organizations demonstrate their compliance with the SOCI Act.
- **AI-Powered security operations center (SOC) Insights:** Infoblox presents a unique industry-first AI-driven security operations solution, SOC Insights. This solution utilizes the DNS detection and response (DNSDR) tool, BloxOne Threat Defense, to analyze a broad range of security events. It empowers security analysts to expedite investigations and reduce response time by transforming extensive data from security events, network activities, ecosystem interactions and unique DNS intelligence into a manageable set of immediate, actionable insights. This process helps reduce alert fatigue for security analysts.
- Infoblox makes security analysts more efficient by maintaining a database of Microsoft users with IP and MAC addresses over time. In addition, this can be shared automatically via API into SIEM and security orchestration, automation and response (SOAR) solutions to help reduce investigation times.
- Infoblox's Dossier, an online domain investigative tool, allows security analysts to get valuable context about Indicators of Compromise, including domains, IPs and URLs, helping them make informed decisions much faster than would otherwise be possible, saving valuable research time.

By leveraging Infoblox technology, organizations can significantly enhance their ability to comply with the SOCI Act's requirements, particularly in areas related to DNS security, network visibility, and IP address management.

INFOBLOX PROTECTION BY THE NUMBERS

Infoblox Threat Intel:

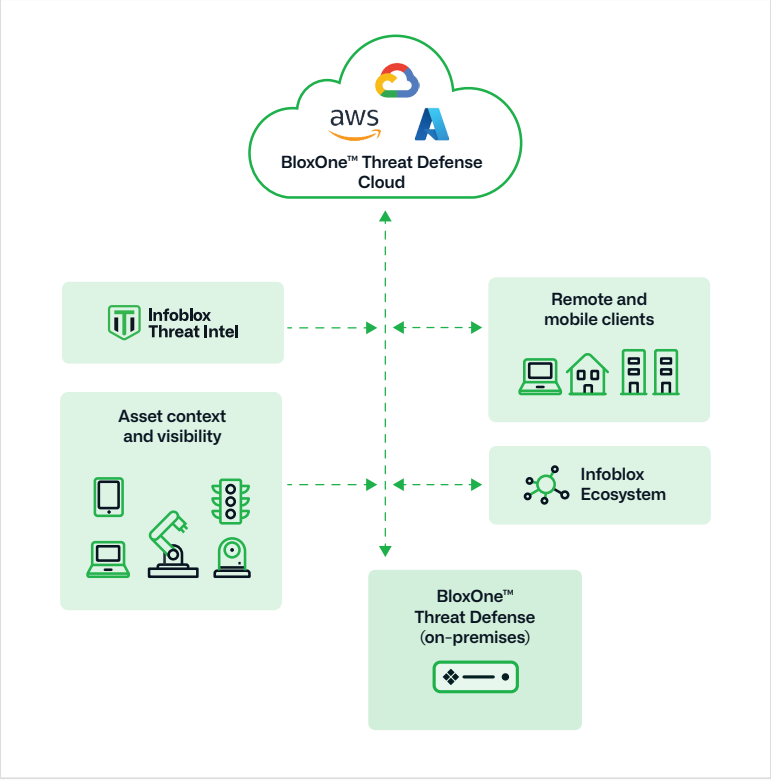
- Detects 60 percent of threats before the first DNS query and 82 percent within 24 hours of the first query
- Blocks attacks an average of 63 days earlier
- Has a 0.0002 percent false positive rate
- Adds close to 4 million new malicious and suspicious domains monthly
- Analyzes 70 billion DNS events daily

INFOBLOX BUSINESS VALUE

Infoblox provides quantifiable business value to its customers including:

- 34 percent reduction in security operations total effort
- 47 percent reduction in security-related endpoint downtime
- 50 percent reduction in endpoint detection and response (EDR) and firewall (FW) alerts
- $400,000 in productivity savings per year

DNS Detection and Response with BloxOne Threat Defense



HOW INFOBLOX ENHANCES CYBERSECURITY IN CRITICAL INFRASTRUCTURE

Organizations that provide critical infrastructure services are confronted with the demanding task of complying with regulations such as SOCI and CPS 234. These regulations present a significant challenge: the need for real-time, accurate tracking and monitoring of critical network assets, a requirement underscored by standards like NIST Essential 8 and APRA.

Traditional tools often fail to detect all types of network devices, leading to difficulties in data logging and increased alert fatigue for security specialists. The complexity is further amplified with the advent of multi-cloud environments and the rapidly evolving threat landscape.

The Visibility Challenge

Traditional tools struggle to detect all types of network devices connected to networks. While it's relatively straightforward for devices like Windows machines, tablets and smartphones, it becomes exceedingly difficult for proprietary operational technology (OT), IoT, Supervisory Control and Data Acquisition (SCADA) and third-party devices.

The Data Logging Challenge

Once assets are identified, data logging becomes a challenge as the volume of data increases with the number of devices. This creates a challenge for SIEM ingestion, generally charged by volume (GB) and the high cost of skilled personnel monitoring alerts.

The Alert Fatigue Challenge

With the increase in data volume, false-positive alert rates are at an all-time high, leading to alert fatigue for SOC/security specialists. There is a general shortage of security-skilled personnel in the market.

The Multi-Cloud Complexity

The advent of multi-cloud environments has added another layer of complexity for visibility, integration and control. There is a desire to consolidate vendors/tools to simplify operations and ensure better integration.

The Threat Landscape

The threat landscape is rapidly evolving with the advent of AI, weaponization, rogue/shadow IT and the use of unapproved AI. This fast-evolving threat landscape necessitates robust security measures.

How Infoblox Can Help with SOCI Today

Infoblox, with its advanced solutions, directly addresses these requirements. It provides the necessary tools and capabilities to overcome these challenges, enabling organizations to accurately track and monitor their critical network assets in real-time, thereby aligning with the compliance and risk management obligations of SOCI and CPS 234. Infoblox's solutions are designed to handle the complexities of today's network environments, making it a valuable ally in the quest for robust cybersecurity in critical infrastructure services.

Infoblox bolsters security by modernizing network services, offering near-real-time data on all network assets. This enhancement reduces SIEM ingestion costs and allows SOC analysts to prioritize critical tasks. Infoblox safeguards existing security stack investments through tight integration, creating an automated defensive shield with proactive threat-hunting capabilities. This comprehensive approach forms the foundation of security and visibility, which is crucial for SOCI compliance.

Infoblox Integrates with the Entire Cybersecurity Ecosystem

Infoblox's suite of solutions, including asset discovery, threat intelligence, logging assessment, DDI services and SOC insights, provide real-time visibility and control over network connections. This enables organizations to construct safer, more resilient environments, significantly boosting their ability to comply with SOCI requirements.

Acting as your network's GPS, Infoblox ensures smooth and secure network operations. It serves as a gatekeeper, filtering out threats and unwanted content before they reach end users, making it an indispensable component of a comprehensive cybersecurity strategy.

CONCLUSION AND RECOMMENDATIONS

The SOCI Act is a significant step in safeguarding Australia's critical infrastructure. By understanding the act's provisions and diligently fulfilling compliance obligations, organizations can enhance their cybersecurity posture, protect against disruptions and contribute to the overall resilience of the nation's critical assets. As the threat landscape evolves, ongoing vigilance and adaptation will be essential to maintaining a robust defense against cyber threats.

Infoblox is an essential cybersecurity partner in your SOCI compliance journey. We aim to unite security and networking teams, empowering businesses to elevate and enhance their security posture. We help organizations turn common, ubiquitous services (such as DDI) into a more powerful capability that provides an integrated, automated defensive shield with proactive offensive threat-hunting capability.

Our existing clients are invited to take advantage of a complimentary, no-obligation health check. This service is designed to confirm that your current environment is equipped to meet your compliance requirements.

Talk to our team: Reach out to us via https://www.infoblox.com/company/contact/.

ABOUT INFOBLOX

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network so your organization runs faster and stops threats earlier. Visit Infoblox.com, or follow us on LinkedIn or Twitter.

For More on SOCI and CPS 234

For more on SOCI and CPS 234 please refer to their websites for the most current versions of the regulations:

SOCI - https://www.legislation.gov.au/C2018A00029/latest/text

CPS 234 - https://www.apra.gov.au/sites/default/files/Draft-CPS-234.pdf

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240731v1