SOLUTION NOTE

ROLE OF DNS IN ADDRESSING AUSTRALIA'S SECURITY OF CRITICAL INFRASTRUCTURE (SOCI) ACT

INTRODUCTION

The Australian Security of Critical Infrastructure Act, enacted in 2018, designates certain sectors as critical infrastructure due to their vital importance to the nation's economy, security and societal structure. The SOCI Act's designated 11 critical infrastructure sectors are:

- **Communications:** This includes telecommunications networks, data centers and broadcasting infrastructure (broadcasting, Domain Name Systems (DNS) and telecommunications). Critical Domain Name Systems (defined within the Act) are those managed by entities crucial for administering Australian domain names (.au ccTLD system). These include the registry database, public WHOIS service, `.au` top-level DNS servers and specific second-level servers (`.com.au`, `.asn.au`, etc.).
- **Data Storage and Processing:** This covers data centers, cloud services and more.
- **Defense Industry:** This includes defense manufacturing, research and development.
- **Energy:** This encompasses electricity generation and gas and petroleum infrastructure.
- **Financial Services and Markets:** This includes banking, insurance and finance.
- **Food and Grocery:** This covers food production, processing, distribution and retail.
- **Healthcare and Medical:** This includes medical facilities and pharmaceuticals.
- **Higher Education and Research:** This covers universities and research institutions.
- **Space Technology:** This involves satellites, ground stations and more.
- **Transport:** This includes air, rail, road and maritime transportation, ports and airports.
- **Water and Sewerage:** This covers water treatment, distribution and waste management.

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.

DNS: YOUR NETWORK'S UNSUNG SECURITY HERO

Imagine your network as a bustling city. DNS acts like the city's central directory. Every device on the network, from laptops to printers and even smart thermostats, relies on DNS to find the resources they need–websites, applications, email servers and more.

But DNS goes beyond mere directory services. It also holds a wealth of historical and real-time information. It tracks which users and devices are accessing which resources, offering a complete picture of network activity.

Here's why this makes DNS a powerful security tool:

- **Universal Visibility:** Unlike other security measures, DNS is present at every network touchpoint. It's the first stop for any device attempting to communicate, making it ideal for monitoring activity across all endpoints–user devices, infrastructure and cloud environments.
- **Early Detection:** Traditional security often focuses on user devices. DNS, however, can also watch infrastructure for suspicious behavior. For instance, new DNS requests connecting to malware command-and-control servers could originate from compromised network equipment, not just user machines.

This unique vantage point allows DNS to function as a ubiquitous security control point, safeguarding your entire network–on-premises, remote and cloud-based. It's a familiar tool transformed into a powerful line of defense, turning everyday operations into a shield against cyber threats.

INFOBLOX: YOUR ALLY IN ACHIEVING SOCI COMPLIANCE

Infoblox provides robust network security and management solutions that empower organizations to meet SOCI compliance. Here's how we do it:

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.
	DHCP Management: Secure DHCP services protect against Dynamic Host Configuration Protocol (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 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, thus reducing 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.
Supply Chain Security	**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.
	Managed Domain Monitoring Service: 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.
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 SOC Insights: Infoblox introduces SOC Insights, an industry-first AI-powered security operations solution. Leveraging the BloxOne Threat Defense tool, it analyzes a wide array of security events. It transforms complex data from network activities, ecosystem interactions and unique DNS intelligence into actionable insights, streamlining investigations and response times. This reduces alert fatigue for security analysts.
	Infoblox's Dossier: Dossier is an online domain investigative tool that allows security analysts to get valuable context about indicators, 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 IPAM.

Benefits include:

- **34% Reduction in Security Operations Effort:** Infoblox streamlines security processes, freeing up valuable time for security operations center (SOC)/security specialists to focus on critical tasks.
- **47% Reduction in Security-Related Endpoint Downtime:** Infoblox keeps devices operational and users productive by minimizing false positives.
- **50% Reduction in Endpoint Detection and Response (EDR) and Firewall (FW) Alerts:** Infoblox drastically cuts through the noise, allowing security teams to prioritize genuine threats.
- **$400,000 in Annual Productivity Savings:** Infoblox's efficiency translates to significant business cost savings.

CONCLUSION AND RECOMMENDATIONS

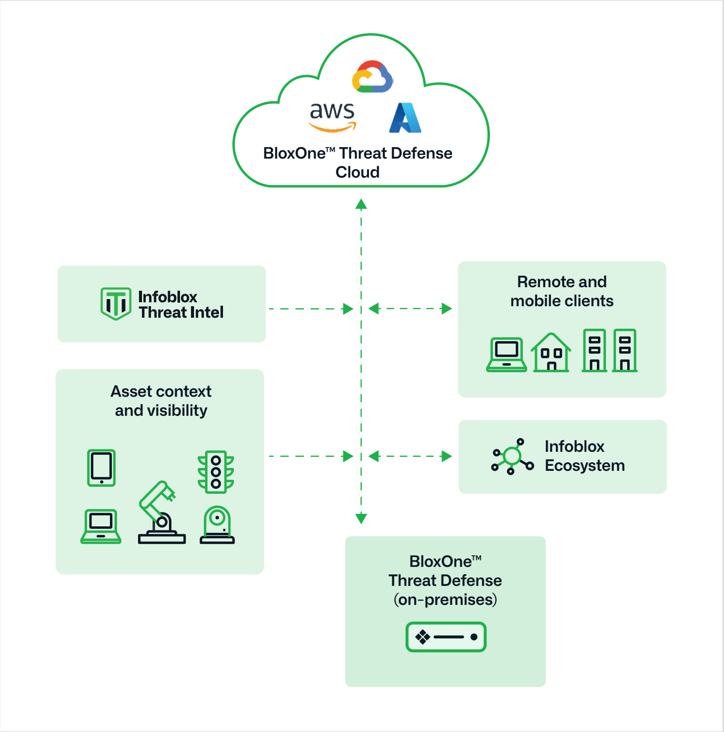
aws
BloxOne™ Threat Defense Cloud
Infoblox Threat Intel
Remote and mobile clients
Asset context and visibility
Infoblox Ecosystem
BloxOne™ Threat Defense (on-premises)

Figure 1: DNS detection and response with BloxOne Threat Defense

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.

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

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.

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

+1.408.986.4000
www.infoblox.com

Version: 20240731v1