censys

Securing the AUKUS Supply Chain

Addressing Cyber Vulnerabilities in a Complex Digital Ecosystem

Table of Contents

Introduction

The AUKUS trilateral security pact, established between Australia, the United Kingdom and the United States, represents a pivotal alliance to promote a free, open, and secure Indo-Pacific region. As these three nations work together to ensure stability and deter potential threats, the integrity of the supply chain supporting AUKUS becomes a critical concern. The supply chain, comprising a vast network of vendors, suppliers, and service providers, plays a foundational role in the success of AUKUS. However, it also introduces a significant risk: the potential for cyber threats that could be exploited by adversarial nation-states or other malicious actors opposed to the mission of AUKUS.

Recognizing this risk, Censys, as the author of this white paper, sees an urgent need to address the potential cybersecurity risks within the supply chain. Through its expertise in internet-wide scanning and monitoring, Censys has identified how exposed infrastructure can serve as entry points for attackers, thereby jeopardizing the security of the entire AUKUS initiative. This white paper seeks to underscore the importance of understanding and securing the supply chain's attack surface, with a particular focus on the risks posed by internet-exposed systems and devices. By doing so, the member states can better safeguard the AUKUS mission and contribute to a stable and secure Indo-Pacific region.

The AUKUS Supply Chain: An Expanding Attack Surface

The AUKUS supply chain represents a complex and expansive network of vendors, suppliers, and service providers, all of which play a critical role in supporting the strategic objectives of the United States, the United Kingdom, and Australia. However, this intricate web of interconnected entities also significantly expands the attack surface, creating numerous entry points for potential cyber threats. The proliferation of internet-exposed systems and devices within this supply chain further exacerbates the risk, as each connected asset could potentially serve as a gateway for adversarial actors to infiltrate the broader network. Cybersecurity vulnerabilities such as unpatched software, weak authentication protocols, and unsecured IoT devices are particularly concerning, as they can be exploited by nation-states or other malicious actors seeking to undermine the AUKUS mission. As the supply chain grows in complexity and scale, so too does the challenge of securing it against these ever-evolving cyber threats. Understanding the full extent of this attack surface is essential for effectively mitigating the risks and ensuring the continued success of the AUKUS initiative.

Supply Chain Cyber Threats to AUKUS

The AUKUS supply chain faces significant cyber threats, particularly from nation-state actors with the capability and intent to disrupt the alliance's strategic goals. These adversaries may seek to exploit vulnerabilities within the supply chain to gain unauthorized access to sensitive information, disrupt operations, or insert malicious code that could compromise the integrity of the entire AUKUS initiative. The tactics, techniques, and procedures (TTPs) employed by these threat actors are increasingly sophisticated, ranging from supply chain poisoning and the introduction of hardware or software backdoors to the exploitation of third-party access points. Historical examples of such attacks demonstrate the devastating impact that compromised supply chains can have on national security, underscoring the urgency of addressing these risks within the context of AUKUS. By understanding these threats and the methods used by adversaries, AUKUS members can better protect their supply chain from infiltration and ensure that the alliance remains resilient in the face of evolving cyber challenges.

Censys, and more specifically the Censys Platform, provides a way forward in addressing key risks that include:

Supply Chain Attacks

- **Compromise of Suppliers:** Adversaries may target smaller suppliers within the AUKUS supply chain, exploiting weaker security measures to gain access to sensitive information or introduce malicious software into the supply chain.

- **Hardware and Software Vulnerabilities:** Inserting vulnerabilities into hardware and software components during the manufacturing process is a significant risk. This can allow adversaries to manipulate or sabotage critical defense systems.

Intellectual Property (IP) Theft

- **Cyber Espionage:** State-sponsored actors may attempt to steal classified or sensitive technologies, designs, and other intellectual properties related to defense capabilities.

Data Breaches

- **Sensitive Data Exposure:** Due to the nature of defense cooperation, the supply chain will handle a significant amount of classified information. Any breach could lead to severe consequences, including the exposure of military strategies and technologies.

Third-Party Risks

- **Reliance on External Vendors:** The use of third-party vendors and contractors increases the risk of these entities being compromised, which can affect the integrity and security of the supply chain.

Supply Chain Interdependencies

- **Complexity and Interconnectedness:** The interdependencies between various components and suppliers in the AUKUS supply chain create opportunities for adversaries to exploit weaknesses at any point in the chain.

Censys Findings: Exposed Devices in the AUKUS Supply Chain

Censys conducted its enumeration of internet-exposed devices within the AUKUS supply chain by leveraging both its Censys Search and Attack Surface Management (ASM) platforms. The process began with Censys Search, which is designed to continuously scan the global internet, collecting data on all accessible hosts and devices, resulting in the Censys dataset which is leveraged by both platforms. This dataset provides real-time visibility into the digital assets of organizations worldwide. For the AUKUS supply chain, Censys identified the vendors and service providers involved and then used Censys Search to locate any internet-exposed devices associated with these entities. The data collected included details such as IP addresses, open ports, services running, SSL certificates, and potential vulnerabilities.

Following this initial data collection, Censys employed its Attack Surface Management platform to provide a more comprehensive and organized view of the findings. The ASM platform allowed Censys to map out the entire digital footprint of each vendor, highlighting exposed assets that could pose security risks. The platform's automated workflows and risk prioritization features enabled Censys to quickly identify and categorize the most critical vulnerabilities within the supply chain. By correlating the data from both platforms, Censys was able to produce a detailed enumeration of internet-exposed devices, revealing potential entry points for adversarial actors. This methodology not only provides a clear understanding of the current threat landscape but also offers actionable insights for mitigating risks within the AUKUS supply chain.

Examples of Exposed Devices

U.K. + Australian Submarine Fabricators

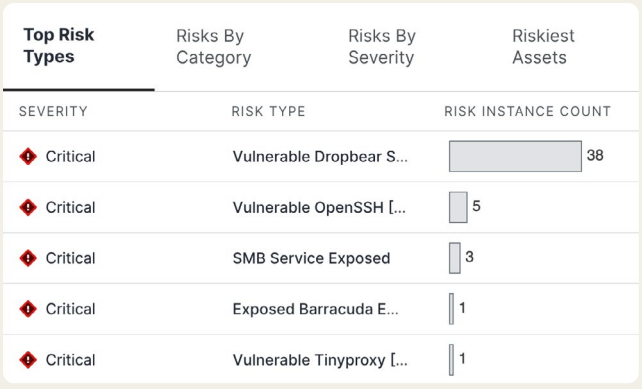
BAE Systems Synopsis

Censys found 3,000+ active cybersecurity risk instances associated with BAE Systems' publicly exposed infrastructure. These cybersecurity risks vary by category. Censys initial analysis showed large amounts of misconfigurations, exposures, vulnerabilities, information leakage, and compliance risks.

Potential Impact

One critical cybersecurity risk identified associated with the Dropbear SSH service allows remote attackers to execute arbitrary code via format string specifiers in the username or host argument.

BAE Systems:
Current External Attack Surface Top Risks



U.K. + Australian Submarine Fabricators

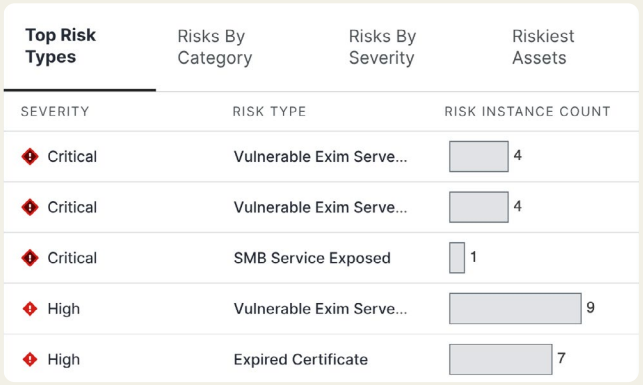
BAE Systems Supply Chain Partners Synopsis

Censys found 1,000+ active cybersecurity risk instances associated with the supply chain partners of BAE Systems publicly exposed infrastructure. These cybersecurity risks vary by category. Censys initial analysis showed misconfigurations, exposures, vulnerabilities, and compliance risks.

Potential Impact

One critical cybersecurity risk identified associated with the Exim mail server is running a version that is vulnerable to a heap overflow. If not resolved this would result in data corruption or unexpected behavior by any process that accesses the affected memory area.

BAE Systems Supply Chain Partners
Current External Attack Surface Top Risks



U.K. + Australian Submarine Fabricators

Rolls Royce Synopsis

Censys found 80+ active cybersecurity risk instances associated with Rolls Royce's publicly exposed infrastructure. These cybersecurity risks vary by category. Censys' initial analysis showed service misconfigurations, software vulnerabilities, service/interface exposure, compliance risk, and web app security vulnerabilities.

Potential Impact

One cybersecurity risk identified associated with this service transmits data in plaintext, which allows an attacker to intercept or modify the data if on the same network. FTP servers can also be targets of password spraying and credential stuffing attacks.

Rolls Royce
Current External Attack Surface Top Risks

Top Risk Types | Risks By Category | Risks By Severity | Riskiest Assets

SEVERITY	RISK TYPE	RISK INSTANCE COUNT
High	Expired Certificate	20
High	EOL Microsoft IIS Software	1
High	FTP Service Exposed	1
Medium	Outdated TLS Version	24
Medium	No Trusted Path Certificate	23

U.S. Submarine Fabricators

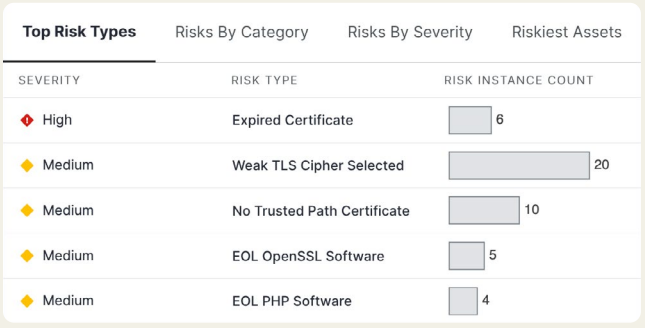
General Dynamics Electric Boat (GDEB) Synopsis

Censys found 50+ active cybersecurity risk instances associated with GDEB's publicly exposed infrastructure. These cybersecurity risks vary by category. Censys initial analysis showed service misconfigurations, software vulnerabilities, service/interface exposure, and web app security vulnerabilities.

Potential Impact

One cybersecurity risk identified associated with the services presenting expired certificates will be flagged as unsafe by modern browsers, which can result in business interruption. Additionally, expired certificates make it easy to launch a man-in-the-middle attack and hijack any requests made to the web application, allowing the attacker to intercept and steal all data sent to it.

GDEB
Current External Attack Surface Top Risks



U.S. Submarine Fabricators

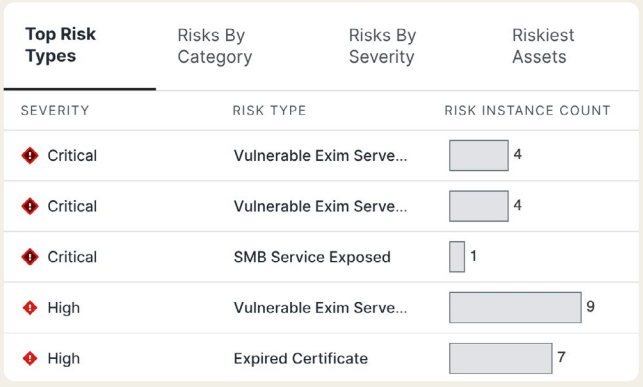
GDEB SMB Supply Chain Partners Synopsis

Censys found 70+ active cybersecurity risk instances associated with GDEB SMB supply chain partners' publicly exposed infrastructure. These cybersecurity risks vary by category. Censys initial analysis showed device exposure, name infrastructure misconfiguration, compliance risk, services misconfigurations, service/interface exposure, and web app security vulnerabilities.

Potential Impact

One cybersecurity risk identified was an RDP service which is designed to enable remote management, a capability that attackers often target. Several vulnerabilities, including remote code execution, exist for this service. It also accepts NTLM credentials and has been targeted by ransomware groups in password spraying and credential stuffing attacks.

GDEB SMB Supply Chain Partners
Current External Attack Surface Top Risks



U.S. Submarine Fabricators

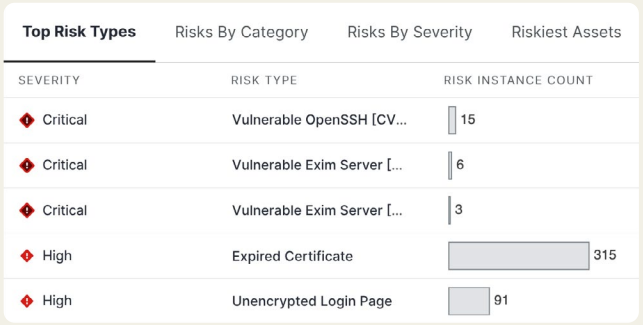
Raytheon Synopsis

Censys found 8,000+ active cybersecurity risk instances associated with Raytheon's publicly exposed infrastructure. These cybersecurity risks vary by category. Censys initial analysis showed large amounts of service misconfigurations, service/interface exposures, web app security vulnerabilities, software vulnerabilities, name infrastructure misconfiguration, device exposure, evidence of compromise, name infrastructure, information leakage, and compliance risks.

Potential Impact

One critical cybersecurity risk identified associated with ***This service is running a vulnerable version of OpenSSH susceptible to CVE-2024-6387*** which is a reoccurrence of **CVE-2006-5051**. This vulnerability allows an unauthenticated attacker to execute code with root privileges.

Raytheon
Current External Attack Surface Top Risks



Implications of Exposed Devices

The identification of exposed infrastructure and their associated cybersecurity risks within the AUKUS supply chain carries significant implications for the security and stability of the entire initiative. These exposed assets, whether they are unpatched servers, vulnerable IoT devices, or improperly secured cloud services, represent potential entry points for cyber adversaries. When such vulnerabilities are left unaddressed, they can be exploited by nation-states or other malicious actors to gain unauthorized access to sensitive information, disrupt operations, or even sabotage critical systems. The presence of these exposed devices within the supply chain underscores the urgent need for continuous monitoring and remediation efforts to prevent exploitation.

The broader implications of these findings extend beyond individual incidents, as they highlight the systemic risks posed by interconnected and often overlooked components of the supply chain. It is crucial for the member states of AUKUS to recognize that the security of their mission is only as strong as the weakest link in their supply chain. Proactively addressing these vulnerabilities is essential to safeguarding the overarching goals of a free, open, and secure Indo-Pacific region.

Censys is a powerful tool for internet-wide scanning, asset discovery, and vulnerability management, which helps visualize your cyber terrain by offering insights into your attack surface. By providing a real-time, comprehensive view of your entire digital infrastructure, Censys allows organizations to visualize their cyber terrain in a way that highlights risks, prioritizes response actions, and enables proactive defense planning.

Here's how it contributes:

Historical View of Cyber Terrain

- With Censys' historical data, you can see how your infrastructure has changed over time. This can help track asset exposure trends, identify outdated software, and understand the impact of changes in your network.
- This historical context helps visualize how the cyber terrain has evolved and where persistent security gaps may exist.

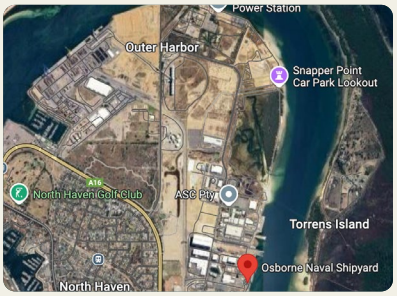
Threat Landscape Monitoring

- Censys monitors the global threat landscape, offering intelligence on trends like open ports or the rise of new vulnerabilities. This information can be visualized against your infrastructure, helping you to proactively adjust your defense based on emerging threats.

Geolocation and Clustering

- Censys enables visualizing assets based on geolocation, clustering assets based on specific regions or networks. This helps with understanding where assets are physically located and if they align with your security policies.

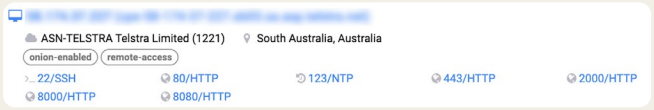
Results for South Australia

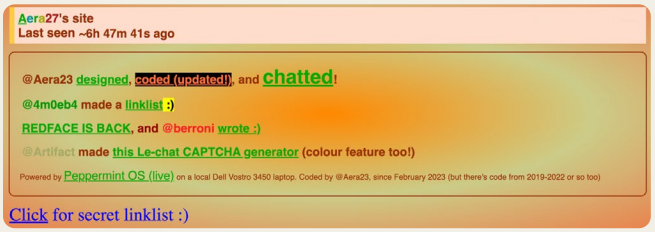


South Australian Cyber Terrain Stats

Publicly Exposed Assets	Supporting Censys Platform Query
~250k Publicly exposed assets in South Australia	-
~200 Critical Infrastructure (ICS/SCADA/HMI)	`location.province: 'south australia' and labels:ics`
~20 Cameras with critical, known, and easily exploited vulnerabilities	`(location.province: 'south australia' and cves.cvss.score: [9 to *] and cves.cvss.components.attack_complexity: low) and cves.kev.source=`CISA` and labels: camera`
~20 Internet of Things (IOT) with critical, known, and easily exploited vulnerabilities.	`(location.province: 'south australia' and cves.cvss.score: [9 to *] and cves.cvss.components.attack_complexity: low) and cves.kev.source=`CISA` and labels: iot`
~2400 Publicly exposed assets in South Australia, with critical, known, and easily exploited vulnerabilities.	`(location.province: 'south australia' and cves.cvss.score: [9 to *] and cves.cvss.components.attack_complexity: low) and cves.kev.source=`CISA``
Server utilizing Onion Services	`location.province: 'south australia' and labels:onion`

Example of search query and result





Mitigation Strategies for Securing the AUKUS Supply Chain

Securing the AUKUS supply chain against cyber threats requires a multifaceted approach that incorporates robust vendor risk assessments, continuous monitoring, and the adoption of advanced security frameworks. One of the key strategies is to implement thorough vendor risk assessments, which involve conducting comprehensive security audits of all vendors and suppliers within the supply chain. These audits should evaluate the vendors' cybersecurity practices, adherence to industry standards, and overall risk posture. It is essential to ensure that all parties involved in the supply chain are following stringent cybersecurity protocols to minimize the likelihood of introducing vulnerabilities.

In addition to risk assessments, continuous monitoring of the supply chain is crucial. By leveraging threat intelligence and real-time data analysis, AUKUS members can detect and respond to potential threats as they emerge. Continuous monitoring allows for the identification of new cybersecurity risks, changes in the attack surface, and suspicious activity that could indicate a breach. Incorporating automated tools and platforms, such as those provided by Censys, can enhance the effectiveness of this monitoring process.

Another critical strategy is adopting cybersecurity frameworks and models, such as the NIST Cybersecurity Framework 2.0 and Zero Trust. Within the supply chain, a Zero Trust architecture operates on the principle that no entity—whether internal or external—should be trusted by default. This model enforces strict authentication and verification for all devices, users, and systems seeking network access. By implementing Zero Trust principles, AUKUS member states can significantly reduce the risk of unauthorized access and lateral movement within the supply chain.

Finally, collaboration among the AUKUS member states is essential for securing the supply chain. Joint exercises, shared threat intelligence, and coordinated incident response efforts can significantly enhance the collective security posture of the alliance.
By working together, the United States, United Kingdom, and Australia can more effectively address the complex and evolving cyber threats that target the supply chain, ensuring the success and resilience of the AUKUS mission.

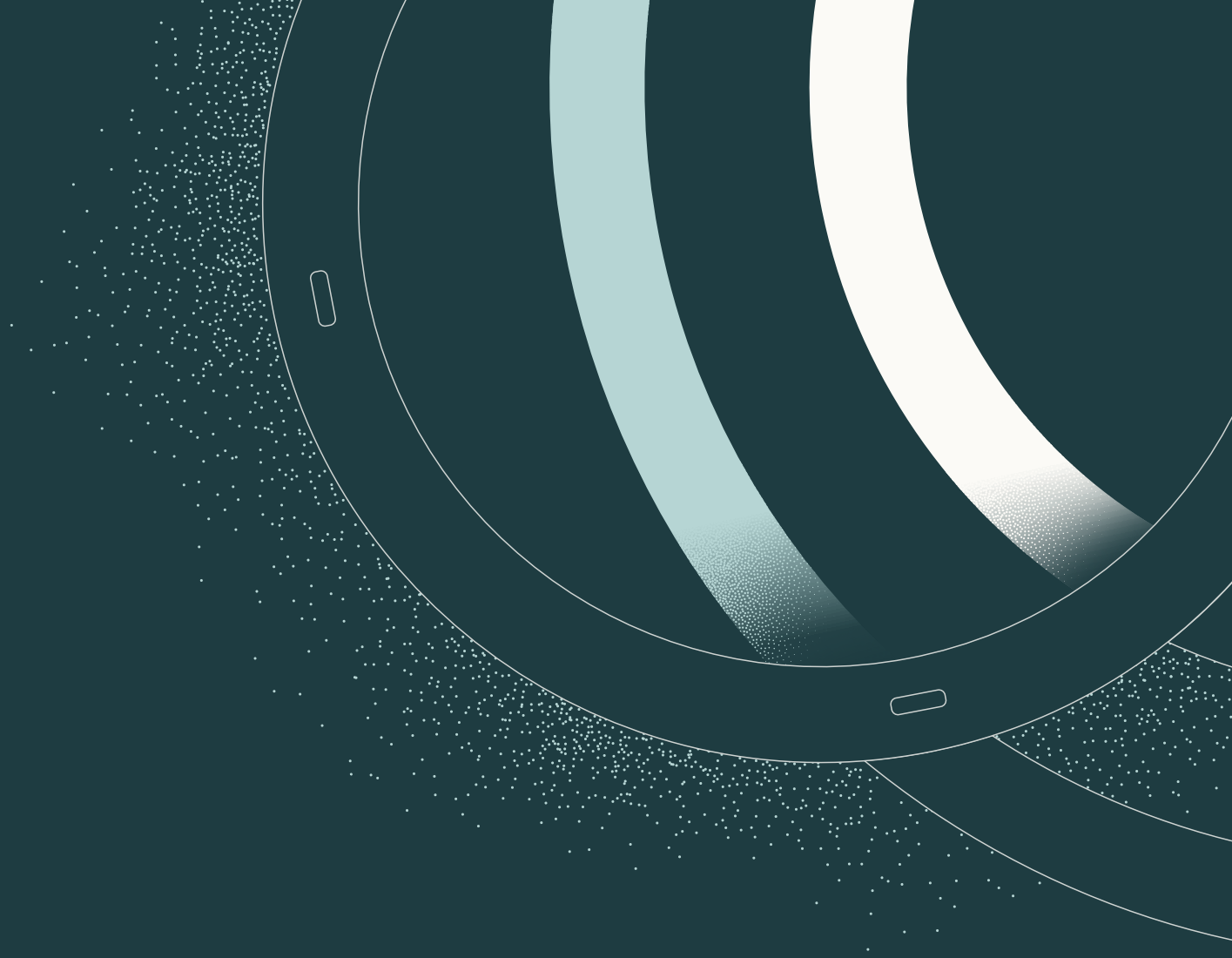
Future Considerations and Conclusion

Strengthening the AUKUS Supply Chain for Long-Term Security

In securing the AUKUS supply chain, it is essential to consider not only the current cyber threats but also emerging challenges that may arise as technology continues to evolve and threat actors' tactics become more sophisticated.

The rapid development of emerging technologies, such as quantum computing and artificial intelligence, presents new risks that could further complicate the security landscape. Addressing these potential future threats requires foresight and adaptability, ensuring that the AUKUS alliance remains resilient against not only today's cyber risks but also those of tomorrow. Additionally, the legal and regulatory frameworks surrounding supply chain security must be considered, as compliance with international agreements and standards plays a crucial role in maintaining a robust defense. The economic implications of supply chain risks, including the potential costs associated with breaches and the loss of intellectual property, also highlight the need for a comprehensive approach to risk management. Engaging stakeholders across both the public and private sectors is vital to fostering a collective approach to supply chain security. By promoting collaboration and shared responsibility, the AUKUS member states can strengthen their collective defenses against cyber threats.

In conclusion, the security of the AUKUS supply chain is integral to the success of the alliance's mission to promote a free, open, and secure Indo-Pacific region. The interconnected nature of the supply chain introduces significant risks that must be addressed through proactive measures such as vendor risk assessments, continuous monitoring, and the adoption of industry-recognized best practices i.e. NIST CSF 2.0 + Zero Trust principles. As this white paper has shown, the insights and findings provided by the Censys Internet Intelligence Platform underscore the urgent need for vigilance and collaboration. By prioritizing supply chain security and remaining adaptable to emerging threats, the AUKUS alliance can safeguard its mission and ensure the long-term stability and security of the Indo-Pacific region.



censys

Censys' mission is to be the one place to understand everything on the internet. Frustrated by the lack of trustworthy Internet intelligence, we set out to create the industry's most comprehensive, accurate, and up-to-date map of the Internet. Today, Censys delivers real-time Internet intelligence and actionable threat insights to global governments, over 50% of the Fortune 500, and leading threat intelligence providers worldwide.

VISIT
censys.com

CONTACT
hello@censys.com