Prospectus public

NIIN
National Industry
Innovation Network

Partnering to Build Australia's Cyber Resilience and Global Leadership

Expression of Interest for Potential Members
of the New NIIN Cyber Alliance

Context

Cyber resilience has become one of Australia's greatest challenges and is critical to the nation's economic prosperity and security. Australia is the most attacked country in the world per capita from a cyber security perspective and needs to be particularly vigilant. The frequency, scale and severity of attacks are intensifying, as are the sophistication and resourcing of attackers. The Australian Cyber Security Centre received nearly 94,000 cybercrime reports in the last financial year, an annual increase of 23 per cent. This equates to a report every six minutes.[1]

The scale and impact of rising cyber security threats is significant. Successful attacks have the potential to cost the Australian economy billions of dollars, with the biggest costs stemming from loss of business continuity. The disruption to a single port, for example, is estimated to potentially cost as much as $100 million per day. A national disruption could displace up to 163,000 jobs and cost $30 billion over four weeks.[2]

Australia's Cyber Landscape at a Glance

A rise in the average cost per cybercrime report to over $46,000 for small business, $97,200 for medium business, and over $71,600 for large business

An average increase of 14 per cent.

A 20 per cent increase in the number of publicly reported software vulnerabilities

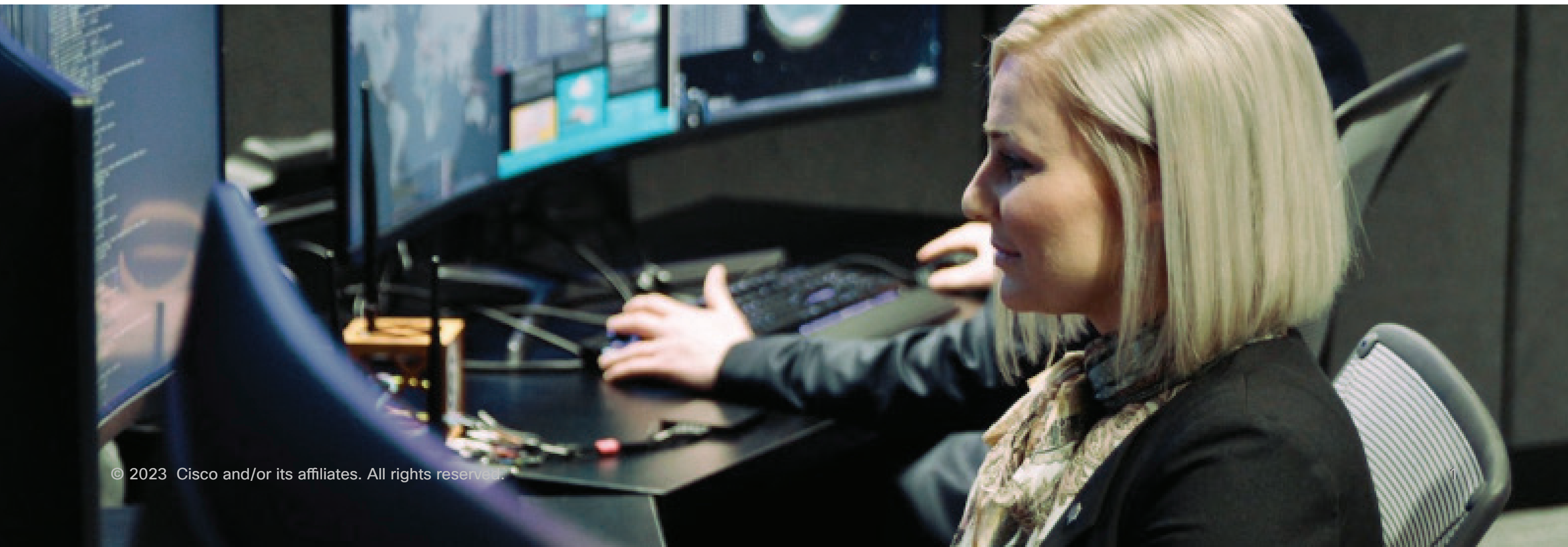
Common Vulnerabilities and Exposures worldwide.

Almost 94,000 cybercrime reports

An increase of 23 per cent from the previous financial year.

A cybercrime report every 6 minutes on average

Compared with every 7 minutes the previous financial year.



Compelling Event: A New National Strategy and Cyber Intel Partnership

Australian Cyber Security Strategy

The Commonwealth Government recently released the 2023-2030 Australian Cyber Security Strategy. The strategy follows an extended period of industry consultation which included formal responses from both Aus3C and Cisco, drawing on existing collaborations they have with university partners through the National Industry Innovation Network (NIIN).

The new Cyber Security Strategy commits more than $586 million to protecting government, individuals and businesses from cyber criminals. Major priorities include:

1. Investing in cyber awareness programs to educate businesses and individuals
2. Growing Australia's cyber security workforce and skills pipeline
3. Developing playbooks to respond to cyber incidents
4. Working with international partners to deter malicious cyber activity
5. Investing in the local cyber security ecosystem

National Cyber Intel Partnership

A number of Australian corporations and government agencies have agreed to work together on threat blocking measures as part of a new partnership. The Partnership forms a key plank of the governments cybersecurity strategy and aims to coordinate systems to block attacks (initially focusing on bank phishing scams with potential to expand).

The Opportunity for NIIN Universities

Universities will have a major role to play in the government's cyber activities. The University Foreign Interference Taskforce – established in 2019 – has reflected a proactive and collaborative approach to building the resilience of Australian universities. The new national strategy – and sustained government action – will build on the progress already made by the sector and create a framework for government policy and investment into research, skills development, collaboration and innovation. Australian universities have three major interests in the new Cyber Security Strategy:

1. Protecting their own operations

Australia's higher education sector is a major target for attack. According to data from the Australian Cyber Security Centre, 6.2% of cyber security incidents during the period of 2021-2 were reported by education and training providers.[3] Universities are a particular target for state-sponsored or state-based actor attacks given their high compute resources, links to national security, and underpinning of the nation's sovereign research capability.[4] The new strategy acknowledges universities as owners of critical infrastructure, reinforcing the Security Legislation Amendment (Critical Infrastructure) Act 2021, which imposed mandatory reporting obligations on sectors such as higher education.

2. The impact on research, skills development and industry engagement

Universities have a critical role to play in helping Government implement its new strategy. This includes:

a. Fundamental and applied research into technical, human and organisational factors

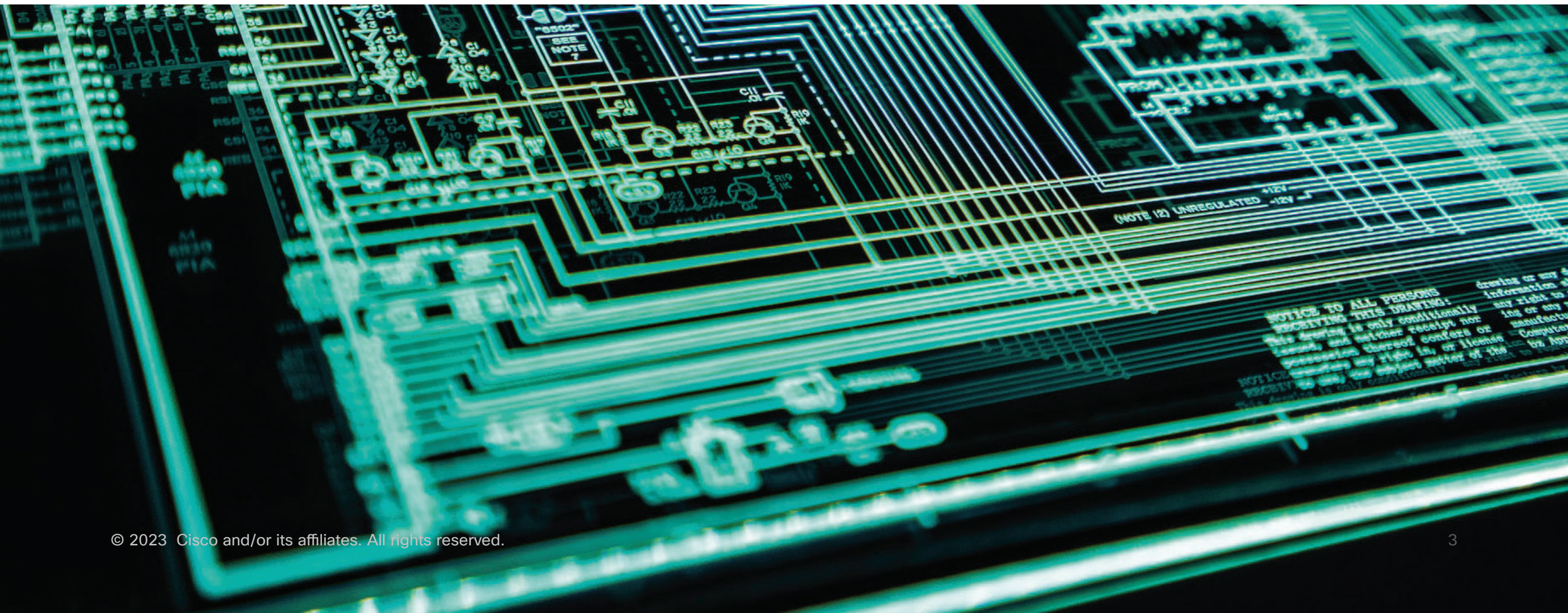
b. Identification, development and delivery of cyber security education and training ranging from specialist skills to basic cyber literacy. Australia is estimated to need an additional 650,000 tech workers by the end of the decade (requiring an uplift of 186,000 above business-as-usual forecasts). By far the greatest skills shortages are technical professionals, particularly cyber security specialists.[5]

c. Engagement with industry to translate emerging concepts and technologies into practice. Universities are instrumental in bridging the gap between theoretical cyber security advancements and practical applications. This not only fuels innovation within industry but also ensures that graduates are equipped with the latest knowledge and skills that are directly relevant to the needs of the workforce.

3. The guidance it provides to build resilience against emerging threats

In the face of complex and sophisticated cyber threats, the strategy's focus on improving national cyber defences directly influences universities' approach to protecting their own networks and data. The strategy sets out a plan to build on guidelines prepared by the University Foreign Interference Taskforce and offer strategic direction for universities to develop robust cyber security postures, ensuring they can not only withstand but also anticipate and respond to cyber threats.

In summary, alignment with the strategy will allow universities to generate research income from government and industry, grow cyber security enrolments / support career transitions in cyber security fields and simultaneously protect their own security interests.



Why a New, National Cyber Alliance is Needed

The priorities outlined in the national strategy cannot be solved by a single university in isolation. In fact, many of the priorities directly talk to the importance of collaborative action and an ecosystem-based approach. The formation of a new Cyber Alliance will help:

1. Demonstrate that universities are willing to go above and beyond their individual contributions as part of the University Foreign Interference Taskforce: Australia's universities have been working together to deepen resilience against foreign interference. The sector has collectively developed guidelines that build on risk management policies and security practices already implemented by Australian universities. The Alliance will further demonstrate universities' commitment to working collaboratively to build cyber resilience.

2. De-risk Universities' Own Operations: The Alliance will create a forum for universities to share cyber security data and practice. By pooling knowledge and resources, universities can mitigate risk and build their defences through collective intelligence and action.

3. Build Australia's Global Cyber Security Leadership: The Alliance is aimed at positioning Australia as a regional and global leader in cyber security. It provides a unique model to tackle the security challenges and opportunities at a national level, and potential for global recognition.

4. Attract International Cyber Security Talent: The Alliance has potential to enhance Australia's global reputation as a centre for academic research in cyber security. This strengthened reputation can increase the country's appeal to international cyber security academics and professionals looking for a vibrant and supportive research community including opportunities for joint projects. Members of the Alliance are likely to have an advantage in securing and retaining this talent through leveraging existing international collaborations and partnerships.

5. Provide Early Visibility into Cyber Security Risks and Opportunities: The value of early insight into industry cyber security priorities, such as those set by leaders like Cisco, is the ability to anticipate and prepare for emerging cyber practice and technologies. Understanding these trends enables universities to plan and align their cyber security strategies accordingly, ensuring they remain at the forefront of cyber defence and education. This foresight is key to adapting to new threats and opportunities in a timely manner.

6. Strengthen Research Funding Submissions and Improve Grant Conversion: Access to an ecosystem of other universities and industry partners through the Alliance enhances the weight and relevance of research funding submissions. Grant applications grounded in industry collaboration are consistent with current government policy and will likely lead to better conversion rates and more funding for cyber security research projects.

7. Enable Joint University-Industry Delivery of Cyber Security Education: The Alliance offers opportunities for universities to pool resources in developing joint cyber security curricula that can be scaled across multiple institutions. Utilising foundational elements from established programs like Cisco's Networking Academy (which has trained 20.5 million students globally since inception in areas such as IoT security, network security and CyberOps), there are opportunities to streamline the development process but also ensure that the education provided is grounded in industry practice. This is a potentially attractive value proposition to international students given the priority they place on practical, industry-based skills. The use of curriculum developed by Cisco and industry partners adds considerable value to the international cohort and provides them with a pathway to professional recognition and opportunities that are respected by employers worldwide.

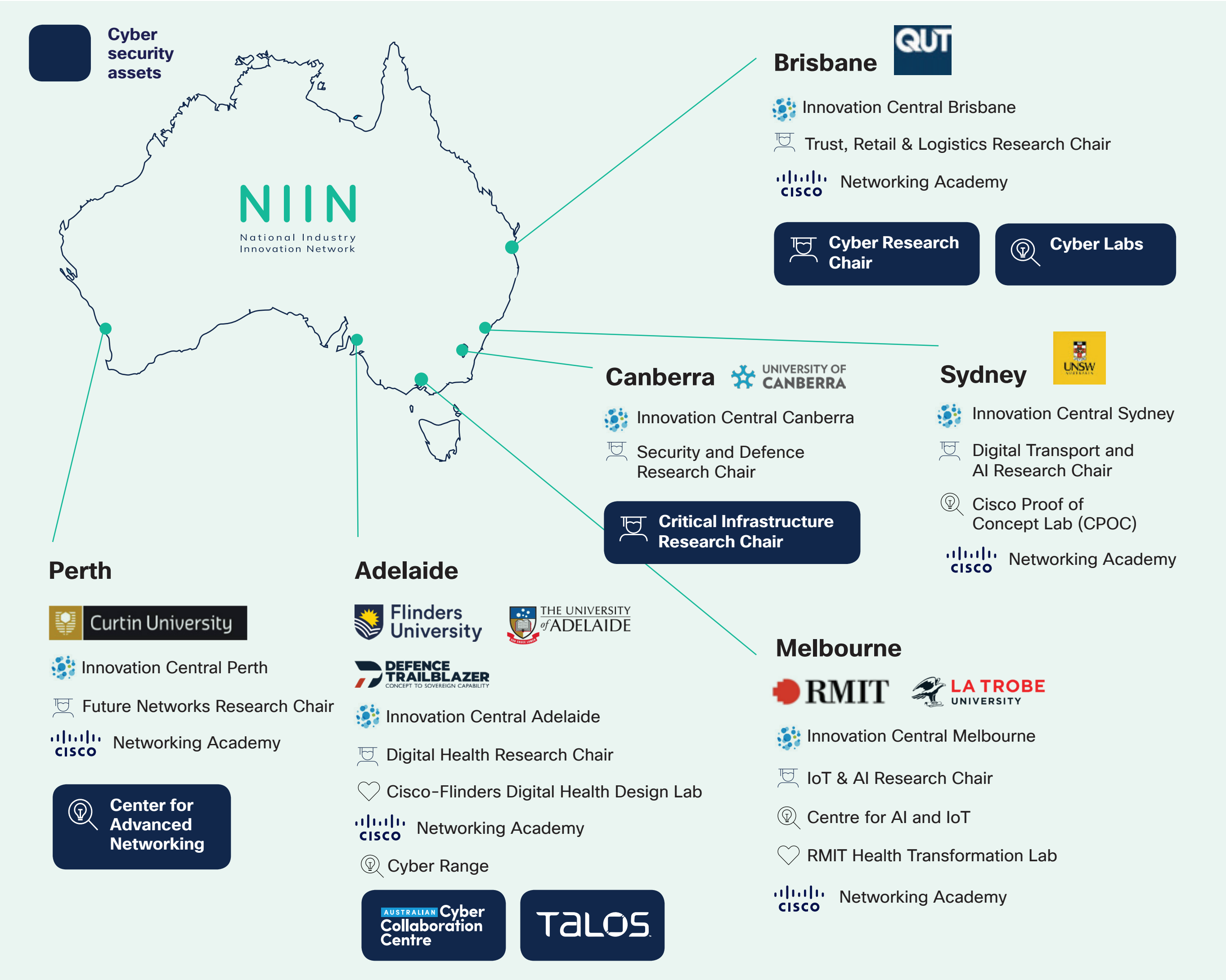
8. Improve Policy and Standards: A collective voice to governmental and standards-setting bodies is likely to be more effective in informing future policy and regulation relating to cyber security obligations for critical infrastructure assets. This can steer policy to benefit the educational sector while simultaneously solving for the national interest.

The Cyber Alliance Extends the NIIN's Capability

The NIIN is a collective of industry and university partners committed to advancing the use of digital technology. Six innovation centres anchor the NIIN, with eight Research Chairs (including one focused on cyber security), two specialist labs and a number of specialised technology centres. The NIIN helps industry (including government and industry) to solve critical challenges using digital innovation in collaboration with researchers and students. The NIIN represents a low-risk mechanism for government and industry to engage in cyber security innovation and skills-building activities.

The NIIN includes resources available to industry and government, such as:

- Dedicated assets and capability for driving cyber security at scale, including Aus3C
- Specialist centres with an industry or technology focus, including Advanced Networking, Critical Infrastructure, IoT and AI, and Digital Transport
- Innovation centres in Perth, Adelaide, Melbourne, Canberra, Sydney and Brisbane.



■ Cyber security assets

NIIN
National Industry
Innovation Network

Brisbane QUT

- Innovation Central Brisbane
- Trust, Retail & Logistics Research Chair
- CISCO Networking Academy
- **Cyber Research Chair**
- **Cyber Labs**

Sydney UNSW

- Innovation Central Sydney
- Digital Transport and AI Research Chair
- Cisco Proof of Concept Lab (CPOC)
- CISCO Networking Academy

Canberra University of Canberra

- Innovation Central Canberra
- Security and Defence Research Chair
- **Critical Infrastructure Research Chair**

Melbourne RMIT, La Trobe University

- Innovation Central Melbourne
- IoT & AI Research Chair
- Centre for AI and IoT
- RMIT Health Transformation Lab
- CISCO Networking Academy

Perth Curtin University

- Innovation Central Perth
- Future Networks Research Chair
- CISCO Networking Academy
- **Center for Advanced Networking**

Adelaide Flinders University, The University of Adelaide, Defence Trailblazer Concept to Sovereign Capability

- Innovation Central Adelaide
- Digital Health Research Chair
- Cisco-Flinders Digital Health Design Lab
- CISCO Networking Academy
- Cyber Range
- **Australian Cyber Collaboration Centre**
- **Talos**

The NIIN Cyber Alliance will extend the NIIN's capabilities and existing cyber security assets by providing a new, dedicated mechanism to collaboratively solve cyber security challenges.

How the NIIN Cyber Alliance Will Work

The NIIN Cyber Alliance is industry-driven but university-enabled. The anchor industry partner is Cisco, with specialist capability in:

Cyber Security Technology

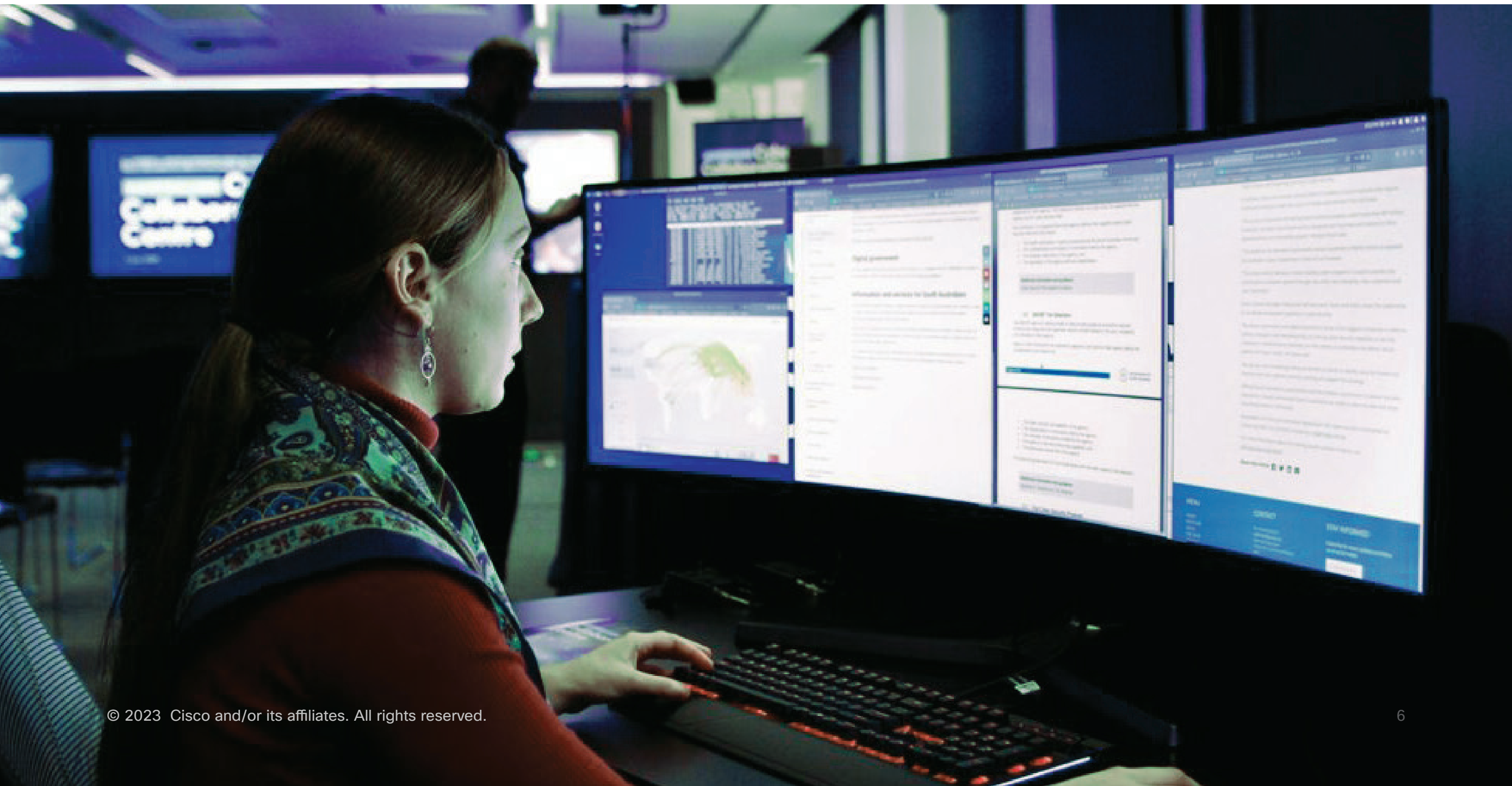
Cisco invests over US$7 billion in R&D annually. Cisco's cyber security technologies range from firewalls and secure network access to cloud security solutions and endpoint protection. Cisco is also a global driver of standards for cyber security technology including frameworks such as Zero Trust.

Cyber Security Research

Cisco's own cyber threat research group, Talos, protects organisations' people, data and infrastructure. Talos researchers, data scientists and engineers collect information about existing and developing threats, and deliver protection against attacks and malware. Talos underpins the entire Cisco security ecosystem and blocks billions of cyber threats a day.

Cyber Security Talent Development

Cisco offers a range of stand-alone and partnership courses teaching security concepts, security monitoring, host-based analysis, network intrusion analysis and security policies procedures.



Cisco is a Global and National Leader in Cyber Security

Security Technology

>85% of the world's internet traffic goes through Cisco

Recognised global leader in cyber security.

Cisco is repeatedly recognised as a global leader in cyber security by Gartner, Forrester and Frost & Sullivan.

Security Research

Cyber security research Leading Australian research

Developer of an industry-leading threat intel system.

Talos Security Intelligence and Research Group (Talos) detects, analyses and protects against threats. Talos can detect and correlate threats across networks spanning web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions.

Security Skills/Talent

Cisco Networking Academy Certifying the world's security professionals

Proud partner to Australian universities delivering world-class training.

Networking Academy's courses and tools are provided for free to 11,800 educational partners, including schools, universities, training centres, nonprofit organisations and even prisons. Since 1997, 12.67 million people in 180 countries have participated.

Security Policy & Standards

Thought leader for the highest levels of government

Active contributor to policy development.

Cisco was invited to provide industry insights to inform the Australian Prime Minister's 2015 Cyber Security Policy & Strategy Review. Cisco's regular threat, trends and benchmarking studies inform policymakers on the state of the threat landscape and Australia's cyber readiness.

Security Advisor

Trusted advisor to Australia's most sensitive agencies and companies

Cyber provider of choice for government and major companies.

Securing the Digital Economy

Driving standards

Cisco remains committed to driving new standards in education and supporting a standards-based approach.

The other key member of the NIIN Cyber Alliance is:

AUSTRALIAN Cyber
Collaboration
Centre

Aus3C is a member-based, independent not-for-profit, with government and industry partners such as Cisco. Its mission is to build cyber capacity to secure Australia's digital future, which it does by enhancing the nation's cyber ecosystem through increased collaboration between research, industry and government. Aus3C will serve as the primary delivery vehicle within the Alliance and will be responsible for coordinating activities between Alliance members.

Operating Model for the Alliance

The operating model has been organised to provide light-touch governance that recognises members have their own obligations / interests in this area. Importantly, the Australian Cyber Collaboration Centre (Aus3C) would act as the Alliance Operator including responsibility for overall co-ordination, member services and staging of events. It would also be responsible for co-ordinating access to a range of assets and capabilities for members of the Alliance (e.g. cyber range, cyber curriculum / credentials, cyber focused research chairs and specialist centres, and threat intelligence services).

In performing this role Aus3C will develop a number of key functions:

The NIIN Cyber Alliance Advisory Group

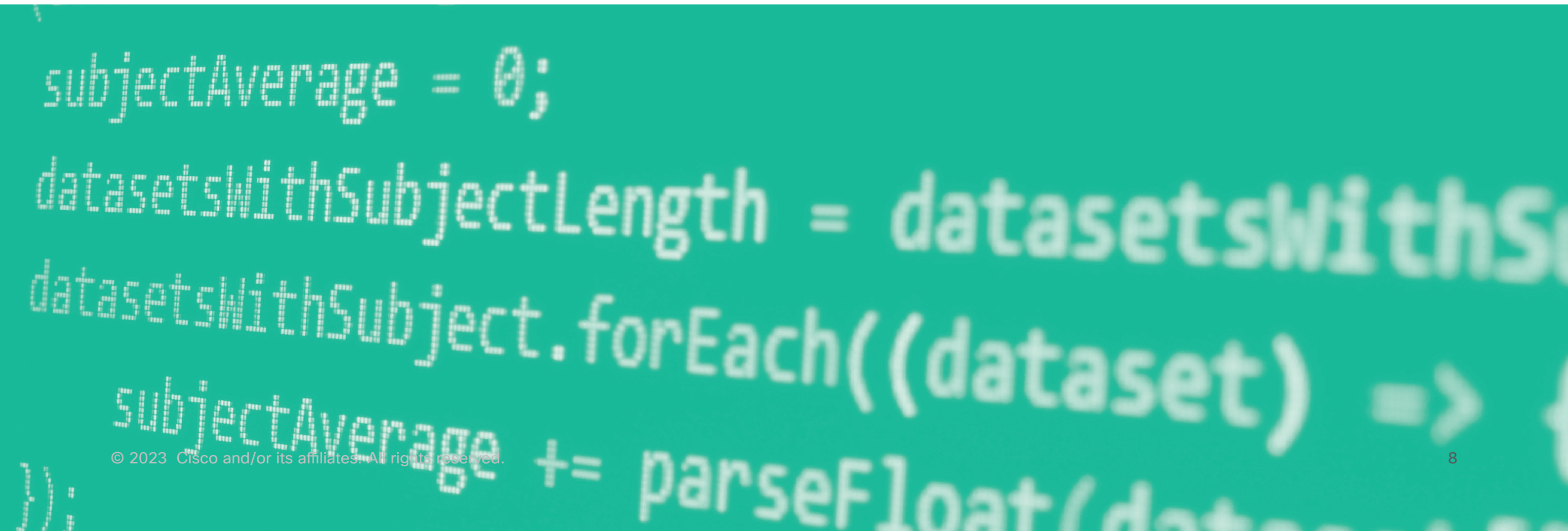
This group provides guidance and strategic advice to the alliance, ensuring the initiatives align with the broader objectives of the NIIN. Membership of this group is still being considered.

Cyber Alliance Members

This includes university and industry members of the Alliance wanting to create value from partnerships and monetise assets that have been assembled (for research and education purposes).

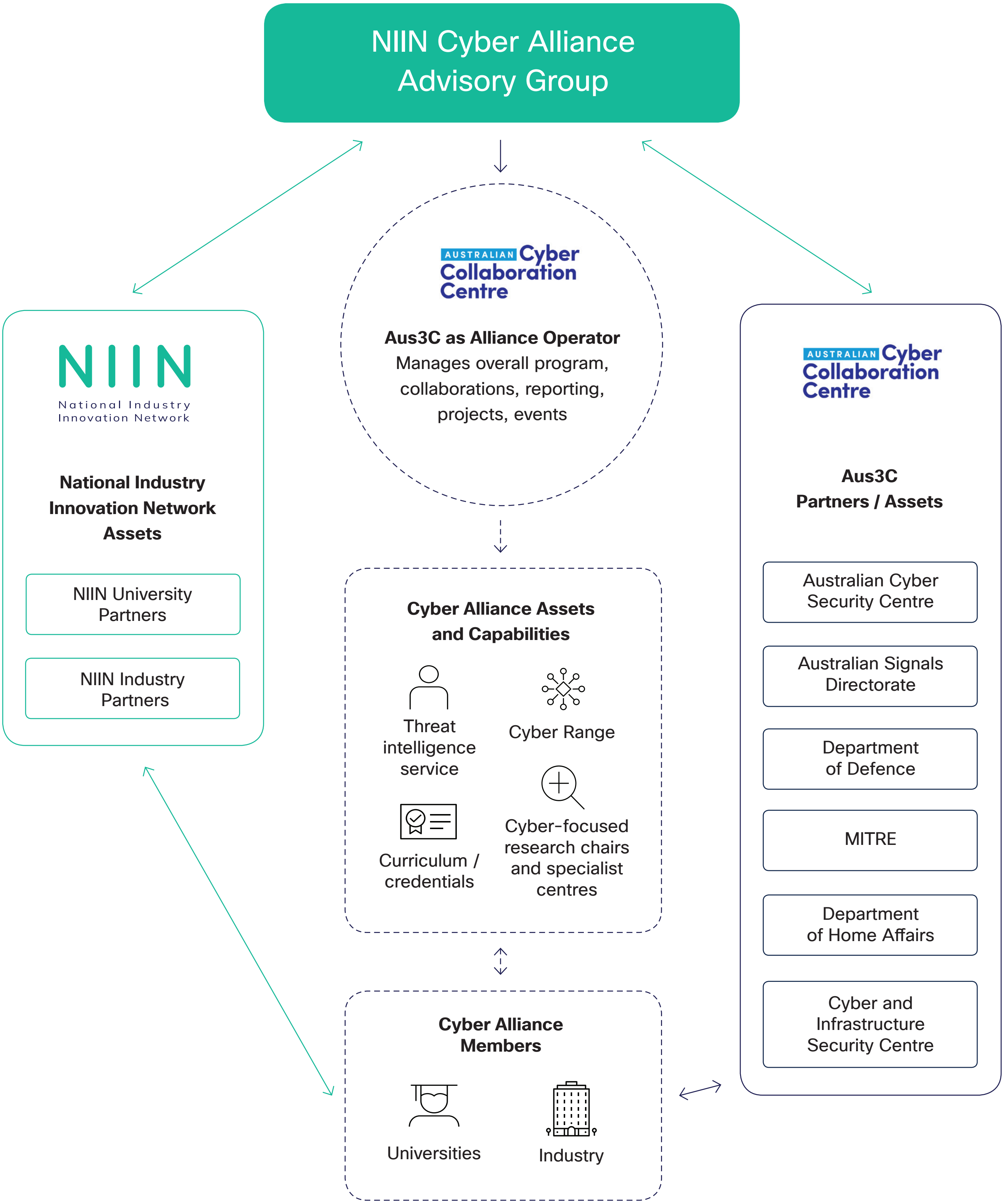
The broader NIIN and Aus3C partner ecosystems

Aus3C will broker and maintain relationships with individual partners and the collective to create value for Alliance members.



```
subjectAverage = 0;
datasetsWithSubjectLength = datasetsWithS
datasetsWithSubject.forEach((dataset) =>
  subjectAverage += parseFloat(data
});
```

NIIN Cyber Alliance Operating Model



NIIN Cyber Alliance Advisory Group

Aus3C as Alliance Operator
Manages overall program, collaborations, reporting, projects, events

National Industry Innovation Network Assets

- NIIN University Partners
- NIIN Industry Partners

Cyber Alliance Assets and Capabilities

- Threat intelligence service
- Cyber Range
- Curriculum / credentials
- Cyber-focused research chairs and specialist centres

Cyber Alliance Members

- Universities
- Industry

Aus3C Partners / Assets

- Australian Cyber Security Centre
- Australian Signals Directorate
- Department of Defence
- MITRE
- Department of Home Affairs
- Cyber and Infrastructure Security Centre

AUSTRALIAN Cyber Collaboration Centre
NIIN National Industry Innovation Network
AUSTRALIAN Cyber Collaboration Centre

Direct Benefits of the Alliance to University Members

There are a number of direct benefits to universities joining the NIIN Cyber Alliance:

- Access to a bank of cyber security industry partners with whom they can collaborate on industry research, skills and internship projects
- Access to the TALOS threat intelligence services
- Access to cyber training tools and facilities including the Cisco Cyber Range facility at Aus3C and existing curriculum content including cyber security micro-credentials and programming offered by the Cisco Networking Academy
- Access to thought leadership from the NIIIN research chairs and Aus3C's partner community including international collaborators
- Access to an annual Cyber Security Trends report, which will be published by the Alliance, that also outlines specific opportunities and roles for universities
- Early exposure to emerging technologies and trends in cyber security including access to a network of research chairs within the NIIN focused on the role of cyber security at different parts of the technology stack and in different industry domains.

Aus3C Platinum Members

BAE SYSTEMS
CISCO
Australian Government Department of Defence
DTEX
Government of South Australia
SAAB
THE UNIVERSITY of ADELAIDE
University of South Australia
VeroGuard Systems

Aus3C Premium Members

11point2
Academy IT
ACG
ADELAIDE FRINGE
AIRLOCK DIGITAL
aizoOn
ALCHEMY
ARRPWERE
BDO
BLUERYDGE
CHECK POINT
CITADEL.IT
Comunet
Concept Data
CROWDSTRIKE
CYBER SECURITY COOPERATIVE RESEARCH CENTRE
CYBERARK
CYBER OPS
cyconsol
cynch
DCI Data Centers
DMAW LAWYERS
Escapenet
FIFTHDOMAIN
Flinders University
FORTINET
hastwell_
HutSix socially distant
insync solutions
IONIZE
KELSIAN CONNECTING PEOPLE & PLACES
LOCKHEED MARTIN
logitech
McGrathNicol
mirvac
myvenue
nbn
OPTUS

Talos

Cisco Talos stands as one of the most sophisticated threat intelligence teams in the world. This group of world-class cyber security experts works tirelessly to detect, analyse, and protect against cyber threats. Talos is the intelligence arm behind all of Cisco's security products, infusing them with up-to-date threat information to ensure strong protective measures.

Talos operates by collecting data on threats from Cisco's extensive global network. This data is analysed to understand and predict threat behaviours, which then informs the development of defence mechanisms. Their work is crucial in maintaining the security of organisational infrastructures and protecting sensitive information.

Talos highlights

- Proactive Threat Detection: Talos was instrumental in uncovering the VPNFilter malware, which affected over half a million routers worldwide. Their early detection and subsequent analysis helped mitigate a substantial threat to global internet infrastructure.
- Research Contributions: Talos regularly publishes research on the latest threats, vulnerabilities, and trends in cyber security, contributing to the community's collective knowledge.
- Community Engagement: Through initiatives like the Talos Security Intelligence and Research Group, Talos engages with the cyber security community to share knowledge, tools, and methodologies, fostering a collaborative environment for combating cyber threats.

Value for NIIN Cyber Alliance members

By accessing Talos threat intelligence, universities can significantly enhance their cyber security posture. They gain insights into the latest threat landscapes, enabling them to fortify their networks against sophisticated cyber attacks. This access is not merely about defence; it's about enabling proactive strategies to anticipate and mitigate potential breaches.

Specific Opportunities Being Explored by the Alliance

Establishment of an Insider Risk Centre of Excellence

Insider risk has grown in importance as part of business risk management processes with the increasingly interlinked nature of organisations' technology and staff. The recent Security of Critical Infrastructure Act 2018 ('SOCI') reforms require more organisations to adopt and maintain an insider risk capability as a component of their risk management program. The Australian Insider Risk Centre of Excellence (AIR CoE) has been established to build a trusted community of domestic and international practitioners in insider risk and the organisations they represent.

The AIR CoE will prioritise three key focus areas: thought leadership, training and education, and research and development. The community of practice will provide strong support to these areas, serving as the foundation for all activities, and ensuring industry relevance is driving the initiatives. Aus3C drives the AIR CoE and is establishing a global network of practitioners exploring ways to ensure insider risk is elevated in company operations.

National Network of Cisco-enabled Cyber Range Facilities anchored by Aus3C Cyber Range (at NIIN University Partners)

Aus3C Cyber Range is the country's most advanced commercially accessible range environment where cyber security professionals can simulate cyber attacks and defences to gain practical experience in a controlled setting. This facility offers an immersive learning environment for understanding complex cyber threats and testing response strategies. There is an opportunity to scale the Cyber Range capabilities by creating a network of cyber ranges at NIIN university partner facilities. The network would be anchored by Aus3C and activated through curriculum courses and training that can be standardised and shared across universities, ensuring access to consistent and high-quality capability building.

Co-funding for Cyber Security Innovation Projects / Challenges

The Alliance is a challenge network focused on identifying and solving the most pressing cyber security challenges (bringing together siloed capabilities). Industry and government members are expected to nominate potential challenges and provide input into collateral developed within the NIIN, such as white papers and thought leadership material. A particular priority will be projects that are aligned with the Universities Education Accord priorities.

International collaborations and linkages

Potential to work with global partners aligned to Five Eyes and defence alliances, including the National Center for Cyber Leadership at George Washington University and the University of Maryland, among others. There is also potential to participate in programs for international students, including students from India, focused on cyber security experiences and skills development.

[1] https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[2] https://www.cisco.com/c/dam/global/en_au/solutions/industries/government/securing-australia-critical-infrastructure.pdf
[3] https://www.campusreview.com.au/2022/07/universities-on-cyber-alert-after-deakin-breach
[4] https://cybercx.com.au/higher-education-industry-threat-report
[5] https://techcouncil.com.au/wp-content/uploads/2022/08/2022-Getting-to-1.2-million-report.pdf

How to join the NIIN Cyber Alliance

This document is seeking to elicit formal expressions of interest from universities wanting to join the alliance. Joining the Alliance involves several steps:

- Entering into a simple agreement with Aus3C (acting as the secretariat for the NIIN Cyber Alliance) outlining basic expectations and values
- Signing on as a platinum member of Aus3C (cost is $40,000 per annum) unlocking collaboration opportunities with 120+ industry, university and government members
- Active participation in key events run by the Alliance including an annual Cyber Alliance Summit and Annual International Cyber Security study tour.

How to Join as a Foundation Member

Interested organisations are encouraged to provide feedback and indicate interest in joining / knowing more about the alliance by emailing niincyberalliance@external.cisco.com