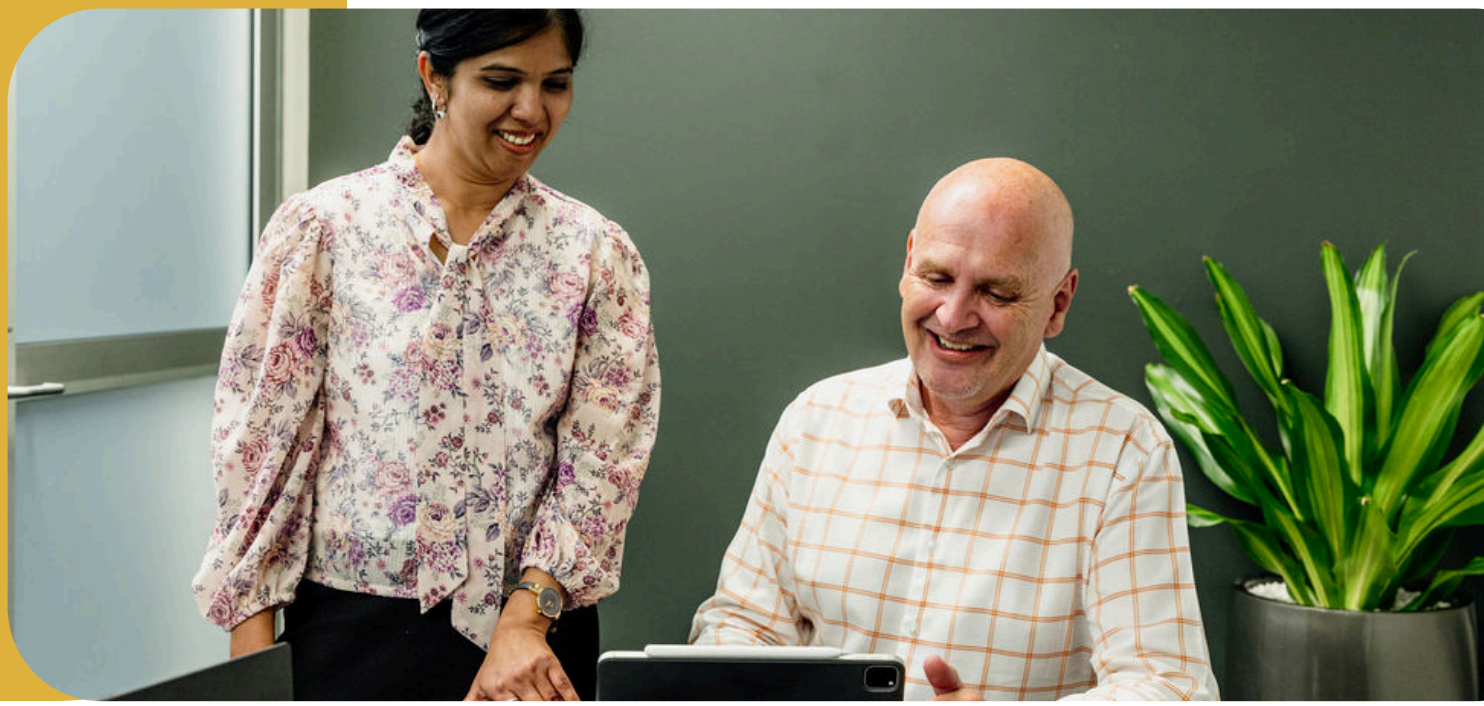
AUSCERT

Allies in Cyber Security

20 May 2024

Year in Review 2023



Forward

For the observant amongst you, you may notice that we skipped the Year in Review 2022. I would love to say nothing much happened, and we all got a chance to take leave, “kick back” and prepare ourselves for the next wave of cyber attacks.....but no! The reality is that, like many of you, we are a small cyber team, with limited resources that more often than not, punch above our weight. AUSCERT is a not-for-profit organisation with a group of very dedicated people who look to bring safety and security to you and your organisation at a very affordable price. And other than continuing to be members, the only thing we ask is that you look hard at our unique services and engage with them as much as possible.

Now when we talk about cyber, either in professional circles, with work colleagues or even friends and family, I’m concerned there is a new feeling going about. So let’s take a word popularised in The Simpsons....."meh". I fear this may be, or at least becoming, the cultural default to cyber. But let me make myself clear.....I truly believe all cyber people are dedicated and passionate about protecting their communities from the threats.

Whether those threats are cyber-criminal or foreign state driven activity, I think this state of "meh" could be a survival response to the constant bombardment of cyber-attacks, successful breaches, large-scale events that occupy the front pages. And don't forget the avalanche of new tech that will either save us (or possibly trigger our demise!).

Dr David Stockdale
Director, AUSCERT

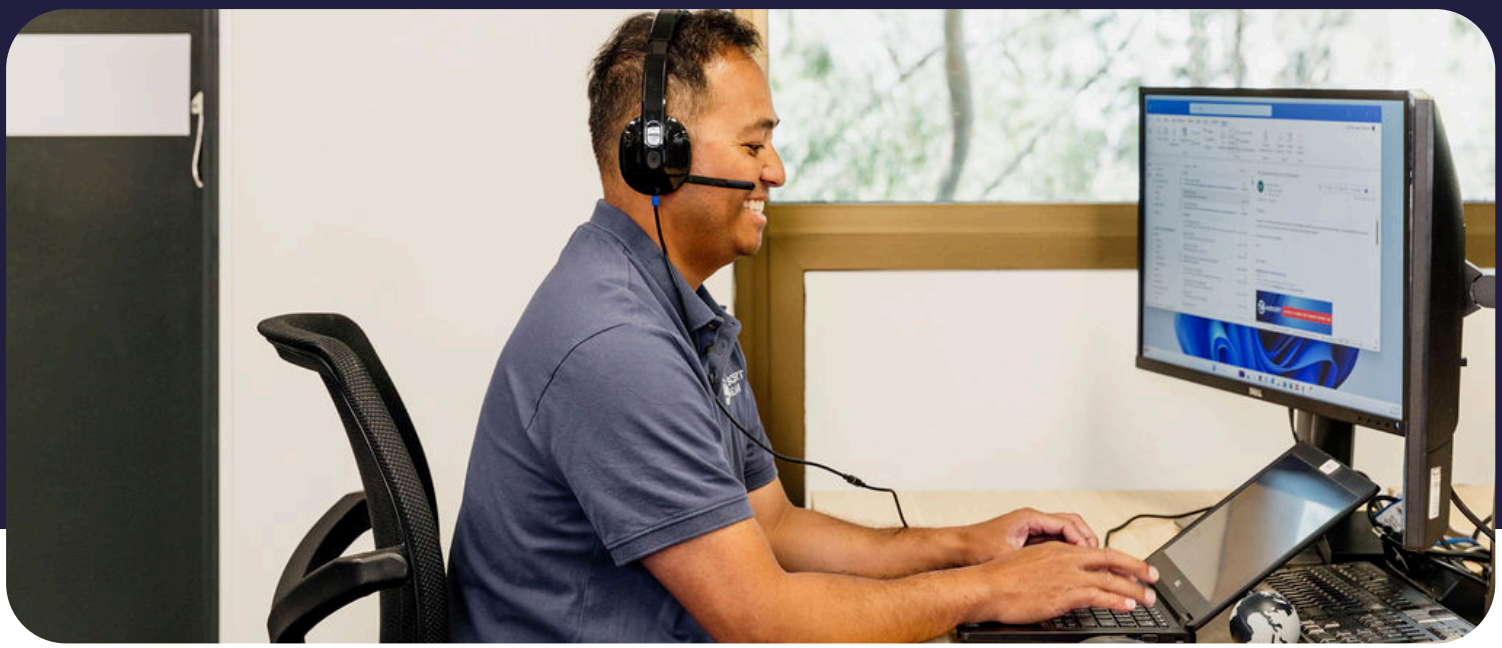
I actually had to google what the top 10 cyber events of 2023 were, not because I don't pay attention but because there seems to be an endless stream of news. And a number of these events were against some of the world's biggest companies that have big budgets and well-structured approaches to cyber security.

The challenge we face as cyber professionals is not only to keep our communities safe but also keep them engaged at just the right level that does not trigger a shutdown response through fear or fatalistic apathy. Changing the conversation and the culture to a “we’re all in this together” needs to come to the forefront.

And for those who also don’t remember the list of 2023 major events, this is what Google came back with;

- Hamas’ kinetic cyberattack against Israel
- Supply chain attack against ION Derivatives
- Data breaches caused by vulnerability in MoveIT software
- LockBit ransomware attack against ICBC
- “Scattered Spider” ransomware group attacks against Caesars and MGM Casinos
- Marina Bay Sands data breach incident
- Credit card data interception attack against Air Europa
- LockBit ransomware attack against UK Royal Mail
- LockBit ransomware attack against Boeing
- Largest DDoS attack ever recorded against Google
- Let's look at what our dedicated AusCERT team members dealt with in 2023. And I hope this will help provide positive conversations to drive back the possibility of “meh”.

Membership Overview

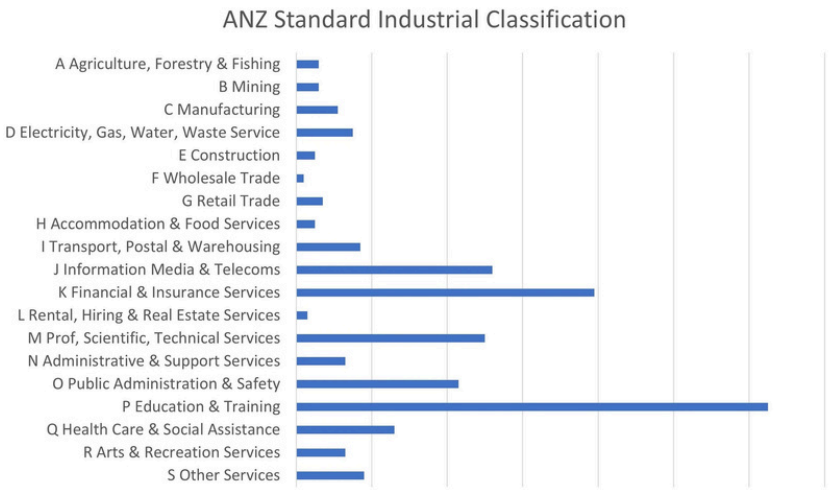


AUSCERT members represent a diverse array of industries. Predominantly, our members are concentrated within the Education & Training sector, which encompasses a significant portion of higher education institutions, including universities and schools. Our second-largest market is the Financial & Insurance Services sector, inclusive of numerous banks. The Information, Media & Telecoms industry closely follows as our third-largest sector. We maintain a good representation of members across all major markets.

Member Demographics

Our members are classified into different tiers based on their sizes, ranging from small, medium, large, to enterprise levels. We've witnessed substantial growth in small and medium-scale organisations.

Our members hail from various regions across Australia, with Queensland, Victoria, and New South Wales emerging as the top three states. Additionally, we have a smaller cohort of international members, primarily from the South Pacific region.



AUSCERT
Allies in Cyber Security

Incident Support

Cyber criminals often target industries that hold valuable data or provide critical services. Financial institutions are prime targets for financial fraud and identity theft, while Education and Training organisations may be targeted for intellectual property theft or ransomware attacks. Public Administration and Safety agencies may face attacks aimed at disrupting government operations or compromising sensitive information.

Top 3 Industries Most Affected

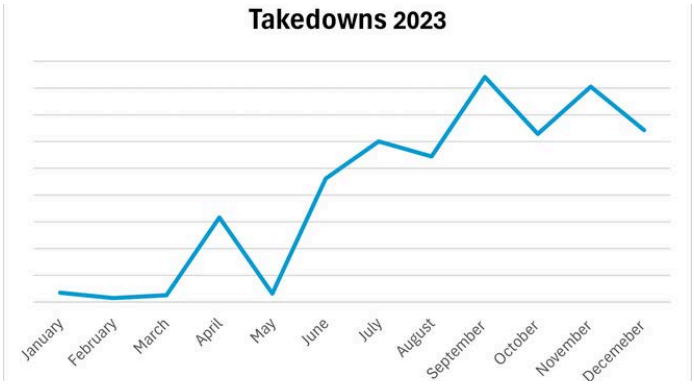
1. Financial & Insurance
2. Education & Training
3. Public Administration & Safety

Phishing Takedown

AUSCERT's Phishing Takedown service is designed to assist member organisations with targeted phishing, spear phishing and whaling attacks. If your organisation's brand is used on a phishing web site, or if spear phishing targets your organisation, AUSCERT can utilise its worldwide contact network to request removal of the fraudulent web site.

Our team will either request a site takedown, if it is an individual web site being used for malicious purposes, or a domain revocation, if the whole domain is used for malicious intent. Drawing on our strong relationships with international CERTs, we have a high success rate in delivering phishing takedowns.

In the second half of 2023, we saw a particularly high trend of takedowns. Usually around the End of Financial Year we see a high trend of phishing attacks as attackers capitalise on the busy times hoping to catch people when they are distracted with other pressing deadlines. Individuals and businesses tend to engage in various financial transactions, such as tax filings, budget planning, and bonus distributions. Cyber criminals have shown great ability in exploiting this through phishing emails.



"I became an AUSCERT member in the late 90s. As an organisation, we required a partner, somebody that could help advise and mature our information security space.

It was great having an organisation that wasn't connected to a vendor, government, or any area.

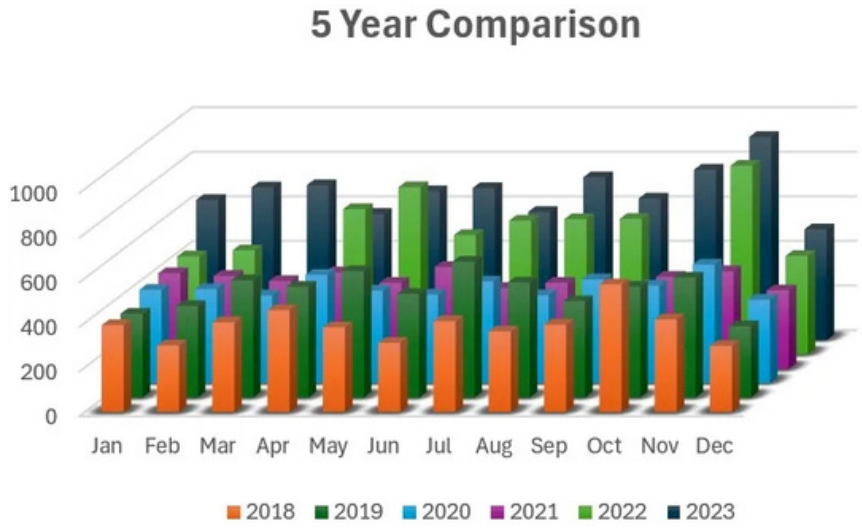
AUSCERT helped my organisation to mature in that area with guidance, as well as providing us with alerts and starting to give us broader levels of alert capability than what we could do internally."

Mikhail Lopushanski,
Chief Information Security Officer
People First Bank

Vulnerability Management

Bulletins

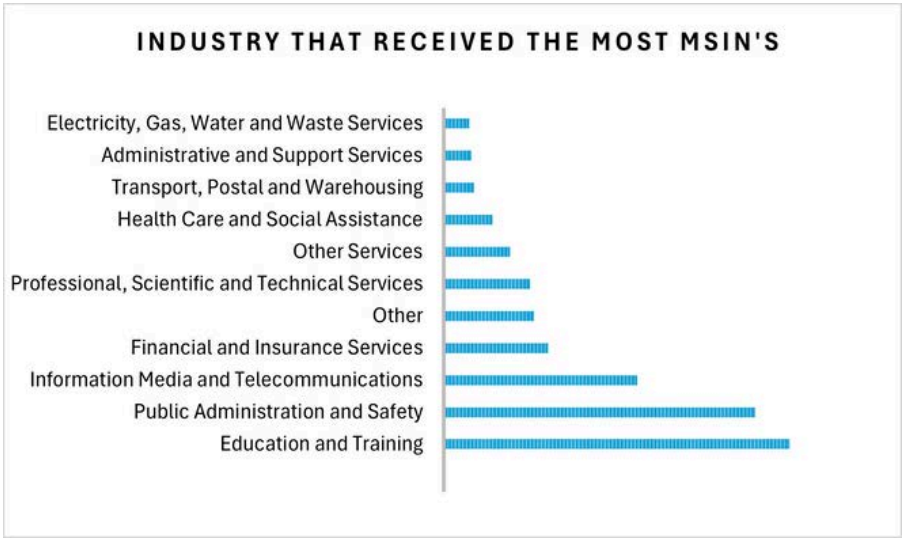
In 2023, AUSCERT distributed **7,792 External Security Bulletins (ESBs)** and **245 AUSCERT Security Bulletins (ASBs)** to its members via email. The marked increase of publications over 5 years can be attributed to AUSCERT's streamlined processes, as well as a general industry trend of increased **vulnerability discovery and awareness** over that time period.



MSIN Member Notifications

Member Security Incident Notifications deliver **customised daily threat intelligence** encompassing vulnerabilities, incidents, and recommended mitigation strategies. Members exclusively receive an MSIN if there's been at least one report pertaining to their IPs/domains within the previous 24 hours.

Additionally, members possess the autonomy to silence specific reports for particular IPs/domains should they prefer not to receive notifications about them. Over the past year, the industries that topped the list in MSIN reception were Education & Training, Public Administration & Safety, Information Media Telecommunications, and Financial and Insurance Services.



AUSCERT
Allies in Cyber Security

Threat Intelligence

Malicious URL Feed

The AUSCERT **Malicious URL feed** contains a list of active phishing, malware, malware logging or mule recruitment websites, curated from analysis of numerous phishing and malware attacks. This feed can be incorporated into network security devices such as firewalls, content filters, IDS/IPS, and SIEM, to prevent or detect compromises to your network

AusMISP

Launched in November 2023, the AUSCERT MISP service provides members with **threat indicators acquired from trusted communities and organisations.** It includes the results of AUSCERT's analysis of captured malware and other threat samples, as well as dependable third-party sources and members.

By using the AusMISP service, members are able to receive and share timely and relevant cyber threat intelligence, including **indicators of compromise, attack patterns,** and other cyber security-related data. This collaborative intelligence enhances cyber security posture and helps members better defend against cyber threats and attacks.

"AUSCERT memberships have numerous benefits, providing access to information, people, skills, and knowledge that an organisation might not have in-house.

The membership allows for asking questions, gaining guidance, and receiving information that helps protect systems, networks, and people.

AUSCERT's training contributes to the cybersecurity maturity of an organisation."

Dave O'Loan
Head of Cyber Relations,
Australian Academic Research Network (AARNet)

Training

Last year we had 358 participants across a total of 29 training courses. Our training courses are very popular amongst our member organisations as a critical component of cyber security resilience, by ensuring their workforce is equipped with relevant knowledge and skills.

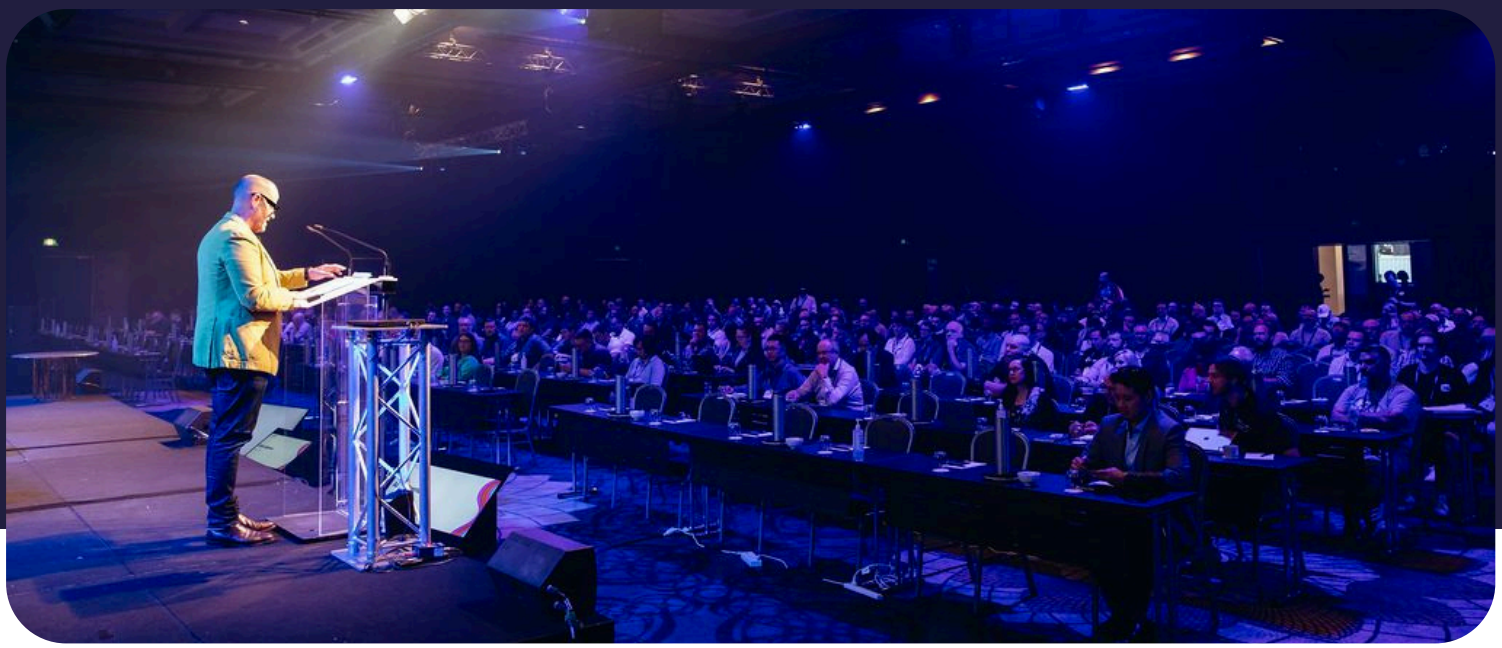
AUSCERT provides a range of cyber security training courses, suitable for cyber security, IT or risk management professionals, as well as cyber security awareness training that delivers important foundational knowledge in an engaging way that online, self-service training does not.

Hear from one of our expert practitioners, Gary Gaskell, who delivers our training courses and has been putting his skills to good use by helping many participants grow their capabilities.

"AUSCERT's training programs aim to address the skill shortages in our community. Often incidents occur due to individuals being unaware of free security features. I believe problems occur due to a lack of awareness. AUSCERT is here to rectify this. The Introduction to Cyber Security for IT Professionals course helps organisations understand the basic features available to keep companies secure. The classes are very popular and appreciated by all those who attend."

Gary Gaskell
AUSCERT Trainer

AUSCERT Conference

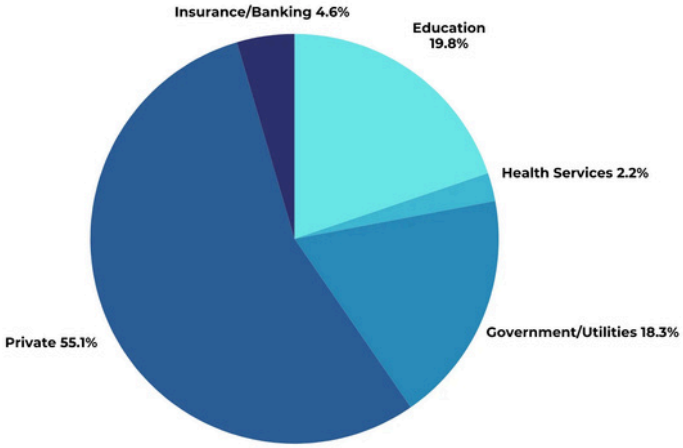


The **AUSCERT Cyber Security Conference** has firmly established itself as a cornerstone in the cybersecurity landscape, emphasizing collaboration, knowledge-sharing, and community strengthening.

Over the years, we've cultivated a robust community consisting of members from diverse industries and roles. Our data illustrates that the primary sector represented is **private enterprises**, followed by the **education sector**, with the **government/utilities sector** closely trailing behind. Attendees typically consist of managers or directors from these industries, showcasing a cohort of **industry experts and influential leaders.**

As our community continues to expand each year, we're gaining increased international recognition, with attendees joining us from around the globe, including New Zealand, the USA, and Southeast Asia.

AUSCERT2023 Attendee Demographics - Industry



Community Outreach

Community outreach serves as a vital cornerstone for nurturing connections, disseminating knowledge, and fortifying the cyber security industry. This important activity entails active engagement with diverse global partners to exchange intelligence, extend support, and pool resources. By fostering these relationships, AUSCERT strengthens the global cybersecurity ecosystem and enhances its ability to respond to cyber threats that transcend national borders.

As a CERT that covers all industries in Australia and neighbouring countries, AUSCERT maintains robust relationships with numerous **CERTs/CSIRTs** (Computer Emergency Response Teams/Computer Security Incident Response Teams) across different countries. These partnerships are crucial for facilitating timely and effective information sharing, collaboration on cyber security incidents, and the development of best practices.

Asia-Pacific Computer Emergency Response Teams (APCERT)

AUSCERT collaborates closely with APCERT to bolster Internet security across the **Asia Pacific region**, fostering global cooperation among CERTs and CSIRTs throughout this expansive area. Our shared mission is to cultivate a cyber space that is safe, clean, and reliable in the Asia Pacific Region, underpinned by robust international collaboration. AUSCERT is regularly involved in working groups and jointly coordinates cyber exercises for incident response teams across the Asia Pacific Region.

FIRST

We're proud to maintain a strong partnership with FIRST, a vital component of the global Forum for Incident Response and Security Teams. As active members, we enhance our ability to respond swiftly and effectively to security incidents. FIRST serves as a hub for computer security incident response teams across government, commercial, and educational sectors, fostering collaboration and coordination in incident prevention.

Our involvement extends to the CVSS working group, where our team contributes to the development and refinement of Common Vulnerability Scoring System standards. In September 2023, we had the privilege of attending the FIRST Conference, further enriching our knowledge and networks within the cybersecurity community.

Women in Security

The Australian Women in Security Network (AWSN) is a non-profit organisation dedicated to educating and empowering women and girls in the field of security while actively working to bolster female representation within the security community. AUSCERT proudly stands as a supporter, extending annual booth opportunities at our conference and providing unwavering support for AWSN's various initiatives year-round.

We champion diversity and we believe that defending, protecting, and educating all types of companies, Small-Medium Enterprises, Not-for-Profit organisations, education institutions, and all Australians requires different minds and types of people.

"AUSCERT has done a lot of good things relating to diversity in the industry. Firstly, the conference is always accessible. I've seen two other people in wheelchairs, and I've never had an issue getting up on the stage when presenting.

Regarding the industry, AUSCERT is highly supportive of the Australian Women Security Network. I volunteer with this network, and they've always had a booth at the conference."

Daisy Wong
Security Culture and Awareness Lead
Flybuys

AUSCERT
Allies in Cyber Security

AUSCERT PODCAST

Share Today Save Tomorrow

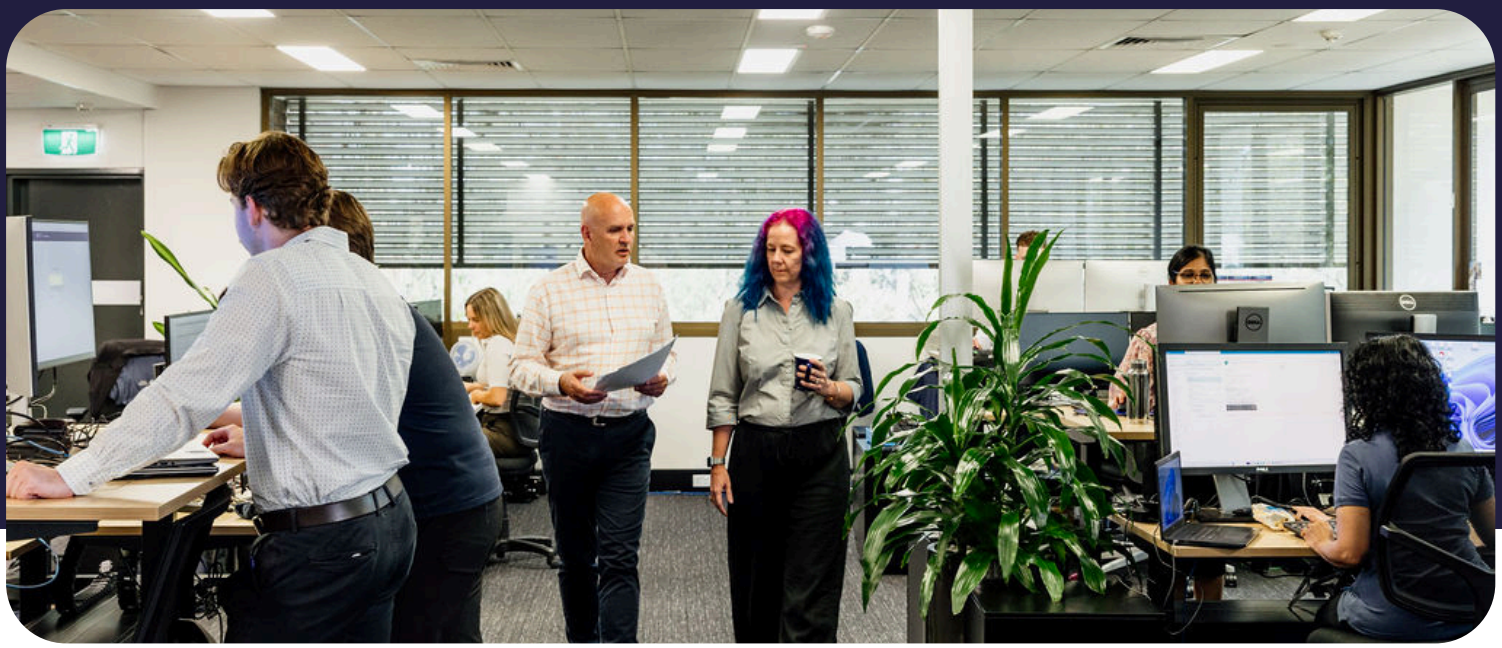
Our podcast is designed to deliver captivating insights, compelling stories, expert knowledge, and personal journeys from the industry, offering valuable lessons to apply in any workplace. With a focus on nurturing an interconnected community and exchanging valuable insights, our podcast serves as a platform for voices from all areas who are dedicated to advancing the cyber security industry.

With a growing number of listeners each episode, we are dedicated to our mission of sharing relevant information today to build a stronger more resilient community tomorrow!

Across 2023 we published 11 episodes addressing a variety of topics. Check them out below!

1. Zero Trust
2. Cyber Risk & Insurance
3. Secure Code
4. Changing behaviour in Cyber
5. Mobile Device Security & AusCERT2023 Wrap Up
6. People, People, People, Process and Technology
7. What does the future hold?
8. Communication is key
9. Celebrating Neurodiversity
10. Cyber artefacts
11. CTI – The importance of info and why context matters

Conclusion



The future of AUSCERT shines brightly with a multitude of thrilling initiatives on the horizon. We're eagerly anticipating the year ahead!

One particularly exciting development is AUSCERT's expansion into the Governance, Risk, and Compliance (GRC) domain. GRC is a vital component of cyber security that integrates governance, risk management, and compliance to help bolster an organisation's security.

We're thrilled to introduce our latest service offering: the Maturity Assessment Service. This comprehensive service provides expert guidance and consultations to assist your organisation in navigating the complexities of GRC, enhancing your cyber security posture while aligning with your business goals. We will help organisations confidently adhere to industry frameworks, standards, and benchmarks. Our maturity assessments are designed to identify and address cyber security practice gaps in your organisation. We work with you to reduce your risk exposure, thereby advancing the security and compliance standards across your organisation.

Infrastructure Updates

In the past year, our organisation has made significant strides in enhancing our technical capabilities, propelling us forward in delivering top-notch services and upgrading our internal infrastructure.

The infrastructure and development teams streamlined their processes in response to increased resources, producing a huge increase in their ability to meet both in-house and member requirements. The adoption of more modern deployment techniques has enabled the team to rapidly respond to requests from members and allowing for increased velocity in delivering projects. This will be more evident in 2024 as a number of changes roll out across our online services.

Revamped Member Services:

- **Submission Portal Enhancement:** Our Submission Portal received an update along with backend improvements, accompanied by the testing of an API submission endpoint for future automation.
- **Ransomware Report Integration:** We've added the Ransomware Report to our Member Slack Channel, which provides information on global ransoms and highlights Australian victim organisations.
- **Streamcatcher:** Streamcatcher leverages machine learning to pre-emptively identify potentially malicious websites before they are launched. The underlying technology was shared within our network of other CERTs and the system will be introduced for our members later in 2024.

Enhanced Internal Tooling & Services:

- **Security Bulletins Backend:** We have deployed a new bulletins backend service, facilitating the decommissioning of our oldest internal tool and streamlining the bulletins publishing process.
- **Decommissioning Legacy Services:** We've replaced or upgraded numerous legacy systems, including sunsetting our oldest legacy server (DAPP – if you know, you know).
- **New Takedown Application Development:** We've developed a new internal Takedown app to aid analysts in performing takedowns and analysing phishing sites.
- **New 'Gatekeeper' Application Implementation:** We've bolstered the reliability and confidence of our data feed into malicious URL feeds and MISP instances, reducing false positives and noise in our datasets.

All of these internal tooling and service upgrades have been completed to facilitate the delivery of the next generation of services for our members.

Thank you for joining us on our journey throughout 2023. We look forward to continuing this adventure with you in 2024 and beyond!

AUSCERT

Allies in Cyber Security

Thank you!