March 2025

AUSCERT

Allies in Cyber Security

Year In Review 2024

TABLE OF CONTENTS

Foreword

Over the past month, Southeast Queensland experienced a tropical cyclone. For those living or raised in regions where this is not a once in fifty-year occurrence, you could be forgiven for wondering why all the fuss, the media coverage, the seemingly extensive doomsday preparation. However, roughly two weeks earlier, Mike Burgess, Director-General of ASIO, delivered the **2025 Annual Threat Assessment.** At first glance, these two events may seem unrelated. What does a cyclone have in common with a national security briefing? And what does either have to do with the **AUSCERT Year in Review**?

The answer is simple: **Preparedness.**

In this year's **Threat Assessment Report**, Burgess took a forward-looking approach, focusing on emerging threats rather than reviewing the past year. His report is sobering, and I strongly encourage anyone in cybersecurity to read the transcript or watch the address. Burgess describes how Australia is facing multifaceted, merging, intersecting, concurrent, and cascading threats. While some, like terrorism and online radicalization, may not directly concern cybersecurity professionals, others should be at the forefront of our focus.

Foreign interference, cyber espionage, and cyber-enabled sabotage are rapidly increasing. As cybersecurity professionals, we must start viewing these as strategic threats. Given that nearly all organisations operate within **interconnected supply chains**, these risks extend beyond individual businesses—they impact the broader Australian economy. In some industries, efforts are already underway to improve intelligence sharing. We at AUSCERT are also working on strategies to introduce more **tactical and strategic intelligence** to support cybersecurity functions within businesses.

Burgess' address wasn't just about threats—it was also about **preparation**. For years, organisations have implemented **strong technical controls** and aligned process controls with frameworks such as **NIST** and **ISO 27001**. However, one area still lagging is **education and awareness**. While the Director-General emphasised public awareness, this is equally critical at all levels within businesses. A strong **cyber-aware culture** helps organisations not only mitigate threats but also strengthens supply chain security and, ultimately, protects the Australian economy.

Whilst this Year in Review looks back at 2024, it also looks forward and outlines AUSCERT's expanding **GRC** capabilities. We aim to assist businesses with preparedness planning with incident response plans and offer **affordable tabletop exercises (TTXs)**. These exercises can be eye-opening and engaging, often revealing process gaps that need to be addressed. However, they should never be viewed as mere **box-ticking** exercises. Instead, they provide a vital opportunity to refine **incident response processes** and strengthen **cross-functional relationships**—which will be crucial in an actual crisis. When conducting these exercises, **remember that real-world crises often present unforeseen challenges.** By practicing and internalising responses to known threats, organisations can free up cognitive bandwidth to adapt to unexpected scenarios.

And as for that cyclone—perhaps it serves as a reminder that preparedness isn't just about anticipating the obvious. It's also about being ready to adapt for the **unforeseen.**

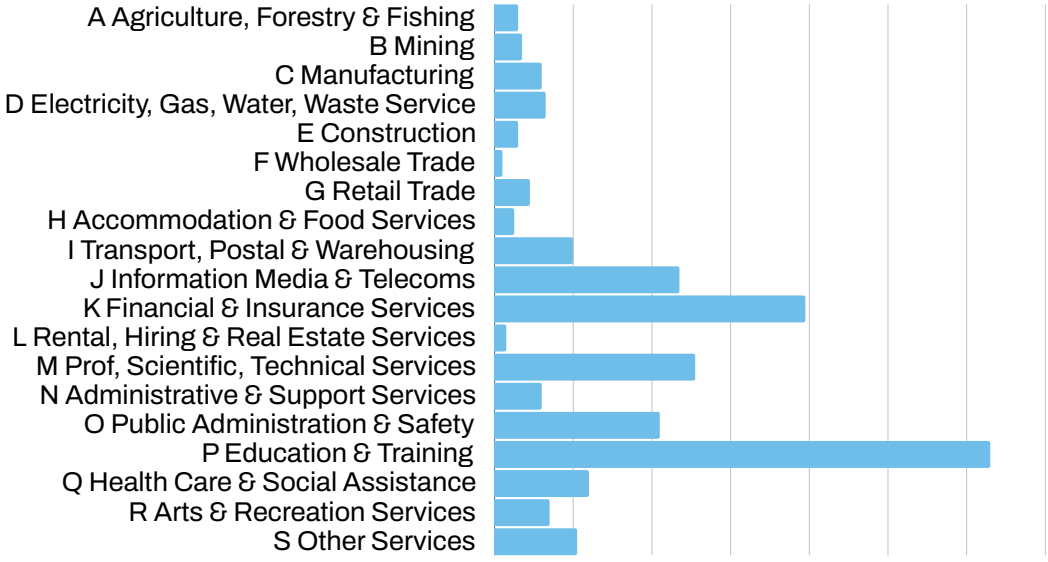
Dr David Stockdale
Director, AUSCERT

Membership Overview

AUSCERT's membership spans a diverse range of industries, from small businesses to large enterprises. The **Education & Training** sector remains our largest, encompassing a significant number of universities and schools. The **Financial & Insurance Services** sector follows closely as our second-largest, including a wide range of financial institutions and banks. In 2024, the **Professional, Scientific & Technical Services** sector has emerged as our third-largest industry, reflecting growing cyber security needs in these fields.

We have also seen increased membership from the **Transport, Postal & Warehousing** sector, as well as **Public Administration & Safety.** This growth is likely driven by rising cyber security threats and stricter regulatory and compliance requirements. Despite these shifts, AUSCERT continues to maintain strong representation across all major industries, reinforcing our role as a trusted cyber security partner.

2024 AUSCERT Members
ANZ Standard Industrial Classification



In 2024, we continued to see substantial growth among **small and medium-sized organisations.** Our members span various regions across Australia, with **Queensland, Victoria, and New South Wales** emerging as the top three states. Additionally, we have a smaller group of international members, primarily from the **South Pacific region,** as well as **Fiji, India, Liechtenstein, Papua New Guinea, the Netherlands, and the USA.**

AUSCERT

Allies in Cyber Security

2024 Overview

8,364 Incidents Handled

8,037 Security Bulletins Distributed

37,700 Member Security Incident Notifications Sent

6,992 Sensitive Information Alerts Sent

10,170 Phishing Takedowns Handled

AUSCERT
Allies in Cyber Security

Incident Support

Incident by Classification

Last year, our analyst team managed **10,170** incidents. Each incident is identified and classified based on its characteristics to help determine the most common threats impacting our members.

Top Incidents

- Phishing
- Spam
- Malicious Code

1) Fraud: Phishing

Phishing is the largest threat category our team handles, encompassing various attack types. Response involves identifying and shutting down fraudulent websites, email accounts, and infrastructure used by cyber criminals to deceive victims. Tackling phishing requires close collaboration between cyber security teams, domain registrars and hosting providers to minimise its impact. Phishing remains the most common cyber attack due to its low cost, high effectiveness, and easy scalability, making it a persistent threat across all industries.

2) Abusive Content: Spam

Spam is the second-largest category affecting member organisations due to its persistence, automation, and connection to broader cyber threats, making it a significant challenge. Events with this classification indicate that a system was likely involved in sending unsolicited bulk email, meaning the recipient did not provide verifiable consent, and the message was distributed as part of a larger batch with similar content.

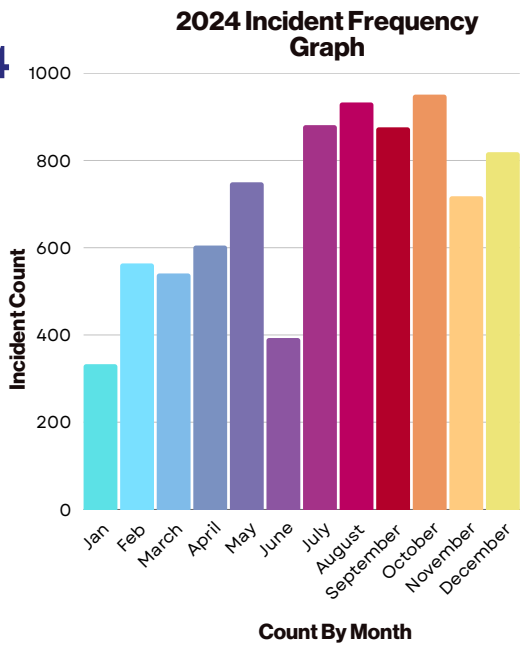
3) Malicious Code: Malware

Malware is the third-largest category affecting member organisations due to its widespread distribution methods, evolving sophistication, and severe security implications. Events with this classification indicate a system distributing malicious software. Infections typically occur when a user accesses a compromised URL via a web browser. However, this does not necessarily mean the malware is hosted directly on the system or URL—it may be loaded from another server

Incident Frequency Throughout 2024

Cyber incidents peaked around the end of the financial year (EOFY), as businesses become more vulnerable to attacks due to increased financial activity. With a surge in payments, invoicing, and accounting processes, fraudsters take advantage of this period to exploit financial workflows.

It's no surprise that the **Financial & Insurance Services** industry is the most impacted among our members. Cyber criminals often target sectors that handle high-value data and critical services, making financial institutions prime targets for fraud, identity theft, and business email compromise (BEC).

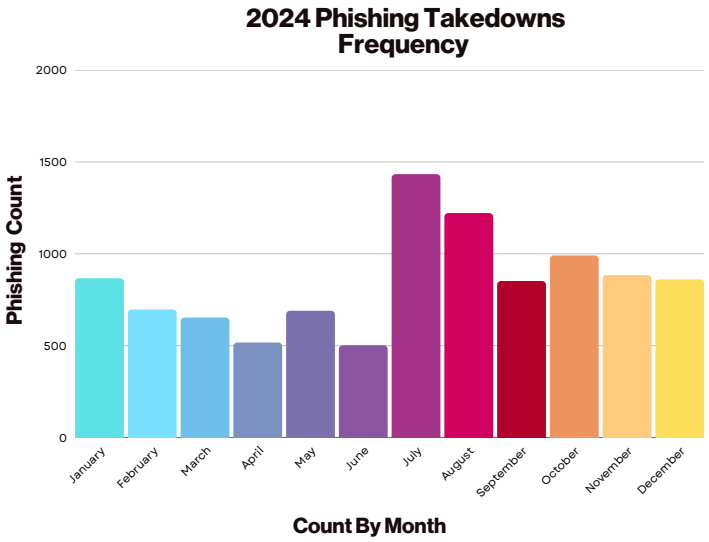


AUSCERT
Allies in Cyber Security

Incident Support

Phishing Takedown

Phishing takedown trends are evolving as attackers use AI, deepfakes, and advanced social engineering to bypass security. The rise in takedown requests has driven AUSCERT to enhance its infrastructure for more efficient processing. Phishing attacks **peaked around the end of the financial year (EOFY)**, exploiting the urgency of tax filings and financial transactions. Another surge occurred towards year-end, coinciding with holiday shopping, bonus payouts, and increased digital transactions.



Emerging Trends

Brand Impersonation Tactics

AUSCERT has detected a significant increase in phishing scams impersonating government and taxation agencies during tax season. Reports of tax-related phishing emails and scams jumped from **1,100 in 2022 to 2,500 in 2023 & 2,960 in 2024.** These phishing emails typically impersonate official entities and may contain convincing logos and language to deceive recipients and urge users to click on a link, scan a QR code or download an attachment. The emails also claim that urgent action is required to avoid account suspension, try to trick users about a pending tax refund, highlight issues with a tax return or demand immediate action to avoid penalties.

Quishing Attacks

AUSCERT has **observed a surge in incidents of "quishing", also known as QR code phishing**. This is a type of social engineering attack which involves tricking someone into scanning a QR code using a mobile device to obtain sensitive information or lead users to malicious content. Appearing legitimate, it can be difficult to identify intent as users can't easily see the URL the code is leading to.

AI-Generated Attacks

AI-generated phishing attacks are transforming cyber crime, allowing cyber criminals to craft highly personalised, scalable, and convincing scams. By **leveraging artificial intelligence, attackers can automate and refine phishing campaigns**, making them more deceptive and harder to detect. Additionally, AI has significantly enhanced social engineering tactics, making manipulation easier and more effective than ever before.

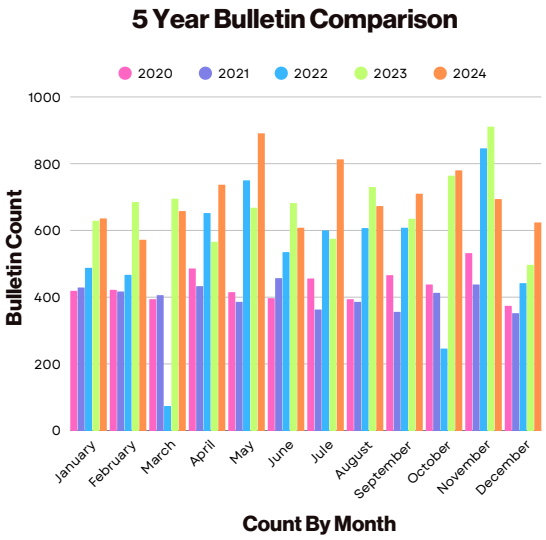
Fake CAPTCHA

Cyber criminals are increasingly using fake CAPTCHA verifications in phishing attacks to create a false sense of legitimacy. Once users "complete" the fake CAPTCHA, they are **redirected to malicious sites designed to steal credentials or deliver malware like Lumma Stealer.** This tactic helps bypass automated security scans, making phishing attempts more effective. As AI-driven attacks grow more sophisticated, users and organisations must stay vigilant by verifying URLs, avoiding suspicious sites, and implementing strong security measures to mitigate phishing risks, such as engaging cyber security awareness training.

Vulnerability Management

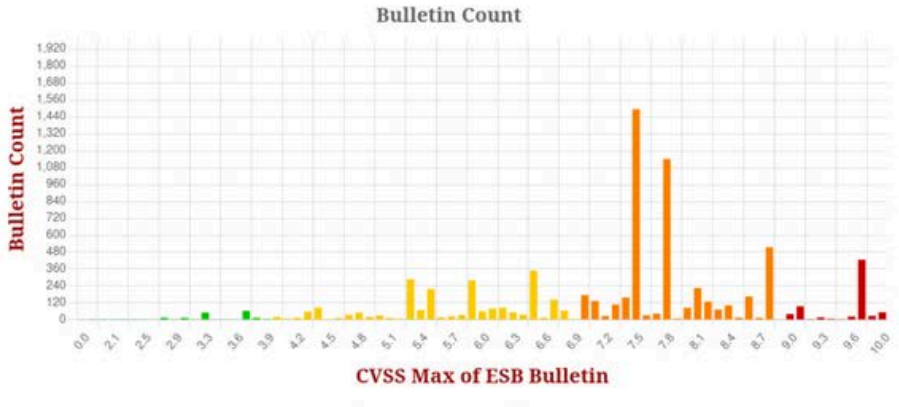
Bulletins

In 2024, AUSCERT issued **8,037 Security Bulletins**, marking a significant rise over the past five years. This increase is driven by **enhanced internal processes** and a **broader industry focus** on vulnerability discovery and proactive threat mitigation. Last year AUSCERT incorporated the **Exploitation Prediction Scoring System (EPSS)** within our Bulletins and Critical MSINs to assist members effectively manage prioritisation in vulnerability management.



Bulletins by CVSS Score

The **Common Vulnerability Scoring System (CVSS)** is an industry-standard framework for assessing and communicating the severity of security vulnerabilities. It helps organisations prioritise threats based on their potential impact. AUSCERT identifies and references vulnerabilities using **Common Vulnerabilities and Exposures (CVE)** identifiers. Each vulnerability bulletin includes a recommended resolution, such as patching, upgrading, or applying mitigation measures.



2024 CVSS Score Severity Ratings

0.0: None
0.1 – 3.9: Low
4.0 – 6.9: Medium
7.0 – 8.9: High
9.0 – 10.0: Critical

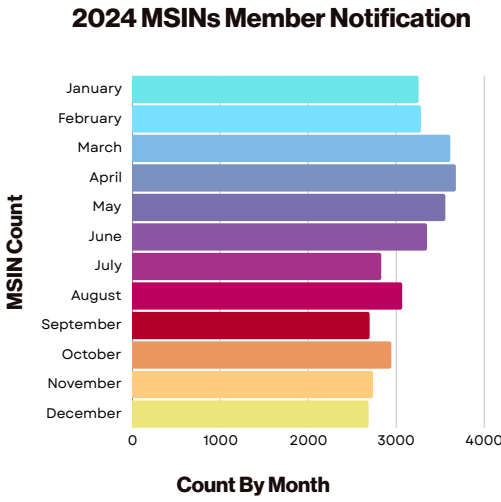
Understanding vulnerability severity is crucial for organisations to manage cyber security risks and allocate resources efficiently. In 2024, most reported bulletins fell into the **High Severity category**, highlighting the rising threat of data breaches, financial losses, and operational disruptions. With organisations overwhelmed by patching demands, **prioritising high-severity vulnerabilities** in conjunction with the criticality of the relevant system and its degree of internet exposure is essential to mitigate risks. Focusing on critical threats first helps reduce cyber incidents, improve regulatory compliance, optimise IT resources, and minimise financial losses. In today's evolving threat landscape, a proactive vulnerability management strategy is key to maintaining security and business continuity.

AUSCERT
Allies in Cyber Security

Vulnerability Management

Member Security Incident Notifications

Member Security Incident Notifications (MSINs) deliver **customised daily threat intelligence** encompassing vulnerabilities, incidents, and recommended mitigation strategies. These reports provide daily updates on vulnerabilities, incidents, and recommended mitigation strategies. Members receive an MSIN only if there has been at least one incident report related to their IPs/domains in the past 24 hours; if no incidents are detected, no MSIN is sent. Additionally, members can mute notifications for specific IPs or domains if they choose to stop receiving updates.

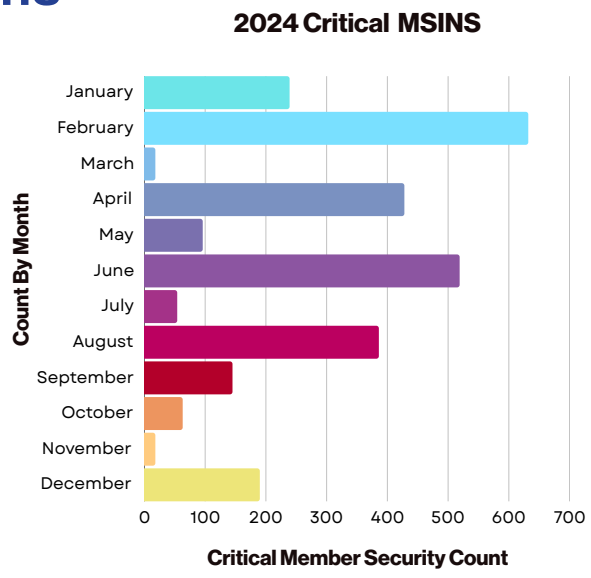


Over the past year, the industries with the highest MSIN reception were Education & Training, Information Media & Telecommunications, and Professional, Scientific & Technical Services. MSINs were consistently sent each month, reaching a total of **37,700 for the year**—an average of 3,141 per month. This reflects our commitment to keeping all members informed with relevant and timely notifications.

Critical Member Security Notifications

We issue alerts as serious vulnerabilities emerge, detailing risks in domains/IPs registered with us that use affected software or services. These notifications, including zero-day and other critical threats, highlight internet-exposed vulnerabilities that attackers could exploit, ensuring urgent attention to high-priority risks.

In 2024, **885 Critical MSINs** were issued across **70 products** impacting AUSCERT members. Persistent vulnerabilities were notably observed in Ivanti's Connect Secure and Policy Secure, Confluence Data Center and Server, various WordPress plugins, and Kibana, highlighting ongoing security challenges and the need for proactive vulnerability management.



Opt into our Early Warning SMS Alerts

SMS Alerts will be sent whenever AUSCERT issues a **Critical Member Security Incident Notification (MSIN).**

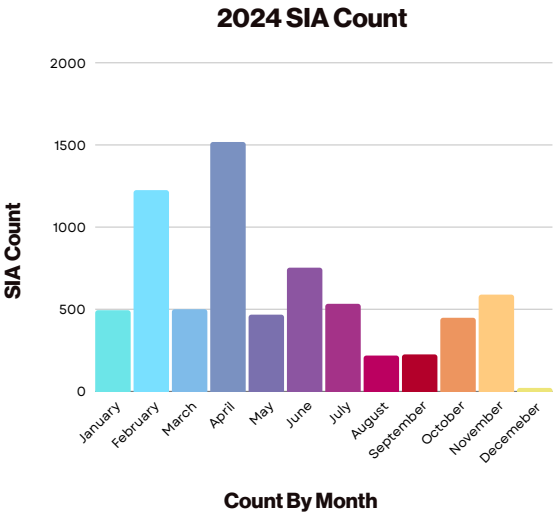
Only contacts who are subscribed to receive SMS Alerts and have a mobile number listed will receive these notifications. To review who is subscribed within your organisation, please visit the 'Manage Contacts' section of the Member Portal.

***Only available for Australian mobile numbers (+61)**

Threat Intelligence

Sensitive Information Alert (SIAs)

Sensitive Information Alerts (SIAs) are issued when our analysts detect **leaked credentials or sensitive data related to members**. Delivered via email, these alerts provide details of the exposure, enabling organisations to assess and take prompt action.



The graph shows a spike in alerts at the start of the year, followed by a decline towards year-end. This trend suggests data exposures may be more frequent during certain periods, highlighting the need for continuous monitoring.

January typically experiences a spike in reported data breaches, often due to organisations uncovering incidents that occurred over the holiday season when staff were on leave. This underscores the importance of phishing-resistant authentication and proactive security measures to mitigate data leaks and enhance cyber resilience.

Emerging Trend

A growing concern, based on AUSCERT member feedback, is the presence of non-existent accounts in some SIAs derived from information stealer malware logs and credentials exposed in multiple breaches. Informal sources suggest cybercriminals may be using AI-generated data to create realistic yet fabricated credentials, deceiving buyers and complicating the analysis of credential-based attacks. Further research and formal reporting are needed to assess the scale and impact of this emerging trend

Hear from our Members!

"AUSCERT's connection to a wider set of industries and partnerships [rather] than cyber security silos is their most significant drawcard.

AUSCERT collates a broader view of the threats that are out there and what's happening in general."

Mark Jackson

Security Services Lead, MYOB

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

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, incorporates the **ACSC CTIS (Cyber Threat Intelligence Sharing) data,** 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.

Hear from our Members!

"We use the Malware Information Sharing Platform (MISP) a lot, and we've learned to automate from there. When I graduated there was a lot of talk about the intel and IOCs that came from AUSCERT. We would be looking for them in our environment and acting on them if needed"

Trace Borrero

Senior Cyber Security Engineer
University of Southern Queensland

AUSCERT
Allies in Cyber Security

Governance, Risk & Compliance

Maturity Assessment

AUSCERT's Maturity Assessments help organisations **evaluate their security posture** against critical controls, identifying gaps and risk exposures across people, processes, and technology. The service includes a **comprehensive assessment**, detailed gap and risk reports, and an executive summary with a strategic roadmap. An optional follow-up is also available to track and document improvements.

Package includes the following:

- Comprehensive Assessment
- Maturity Gap Report
- Risk Scenario Assessment Report
- Executive Summary & Roadmap
- Optional Follow up

Client Success Story

"The AUSCERT Maturity Assessment, based on a subset of NIST CSF controls, was an effective and efficient engagement to obtain an independent assessment of UniQuest's Cyber Security program. The benefits we obtained from the process include:

1. Identifying Security Posture: The assessment helped identify our current security posture with a clear understanding of our maturity level.
2. Risk Management: The assessment facilitates the identification of key risks and establishing a plan to mitigate the most likely or impactful ones.
3. Stakeholder Assurance: The assessment reports provide transparency to UniQuest's stakeholders on cyber security maturity.
4. Breach Prevention: The assessment reports help in identifying the greatest risks of a breach and recommendations for elevating the security controls that prevent these.
5. Maintaining Best Practice: The assessment helps in benchmarking UniQuest's security maturity compared to industry averages and developing an improvement program that grows and maintains our security posture over time."

Elliot Larard
UniQuest
AUSCERT Member

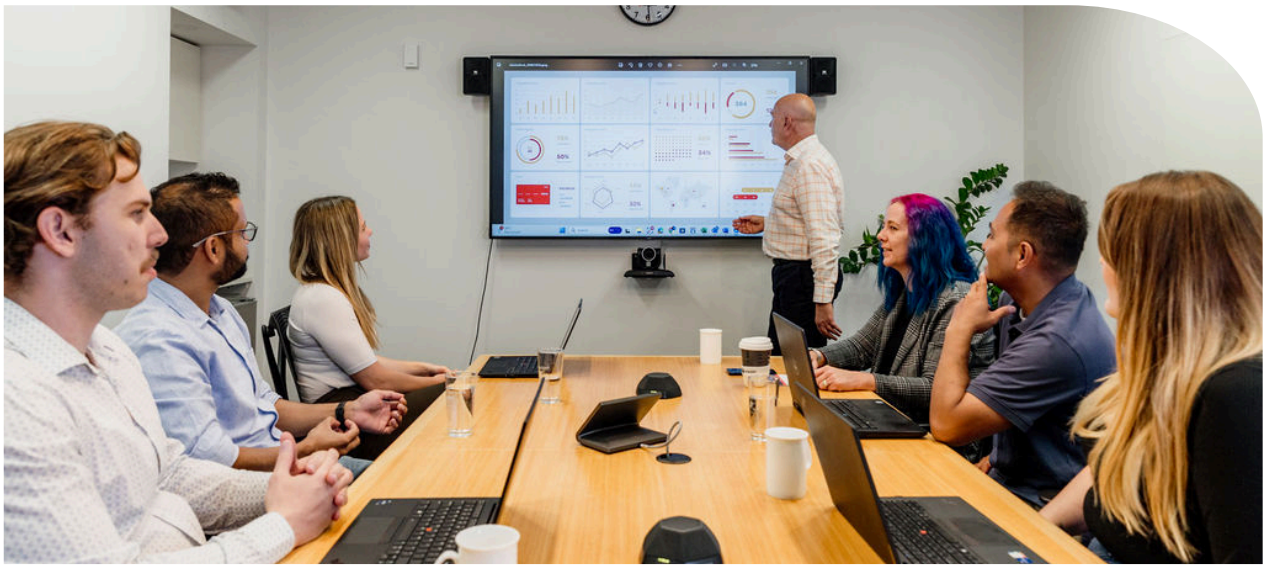
AUSCERT
Allies in Cyber Security

Cyber Incident Response Plans (CIRP)

After launching our Maturity Assessments and gathering customer feedback, we identified a common need for **Cyber Incident Response Plans (CIRP)** to enhance preparedness and resilience. Subsequently, we established this service to help strengthen organisations' security postures. A robust CIRP is essential for ensuring an effective response and swift recovery when security defences are breached. Whether you need a custom-built CIRP or a thorough review of your existing plan, we're here to help strengthen your organisation's resilience.

Available Plans

- **Custom CIRP Development**
- **CIRP Review & Optimisation**
- **Testing & Validation**



Tabletop Exercises

Our tabletop exercises (TTXs) are designed to explore and improve your organisation's preparedness in managing and responding to various cyber incidents. These exercises help identify critical gaps in your incident response strategies and decision-making under pressure, improving organisational cyber resilience.

Information Gathering > **Simulation Exercise** > **Post TTX Report** > **Debrief Meeting**

Members receive a 15% discount on all GRC services!

Contact us for a quote today!

grc@auscert.org.au

AUSCERT
Allies in Cyber Security

Training

We have observed a shift in training preferences, with fewer individuals enrolling and more organisations opting for in-house training for their employees. This trend highlights a growing demand for **customised, in-house solutions tailored to an organisation's unique needs** and workforce, rather than general public courses. AUSCERT is happy to adapt our training offerings to align with an organisation's specific objectives and coordinate in-house courses to better serve their needs.

To make our training courses more accessible to the broader community, AUSCERT has **opened them to all individuals and organisations in 2025**, extending beyond just its members. To ensure members continue to receive exclusive benefits, they will enjoy a **15% discount on all courses**. These training programs are essential for strengthening cyber security resilience, equipping workforces with the critical knowledge and skills needed to stay secure.

Hear from our Trainers!

"AUSCERT's training courses offer hands-on, practical experience, catering to all levels of industry knowledge, from foundational concepts to advanced technical topics.

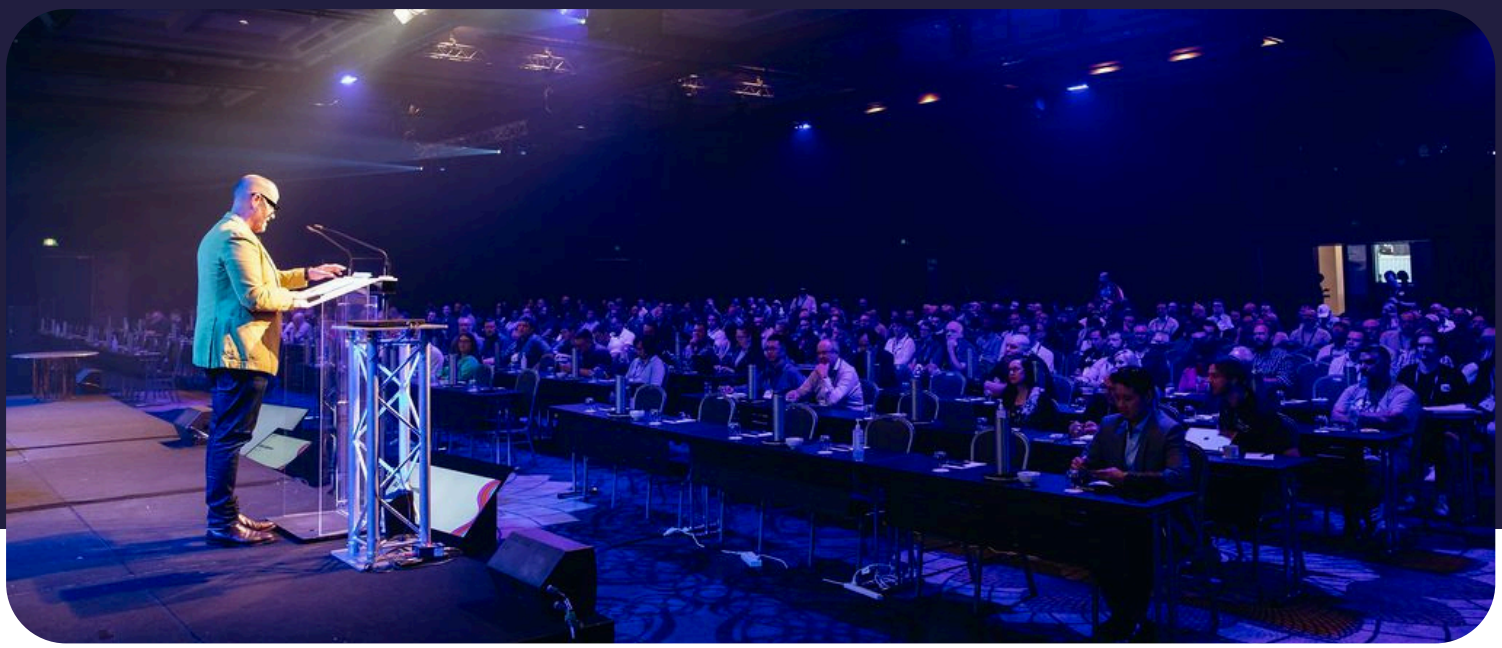
Led by experienced practitioners, our interactive courses go beyond self-paced online learning, providing engaging, industry-relevant training that helps participants build valuable knowledge and confidence in their skills."

Mark Carey-Smith

AUSCERT Principal Analyst & Trainer

AUSCERT
Allies in Cyber Security

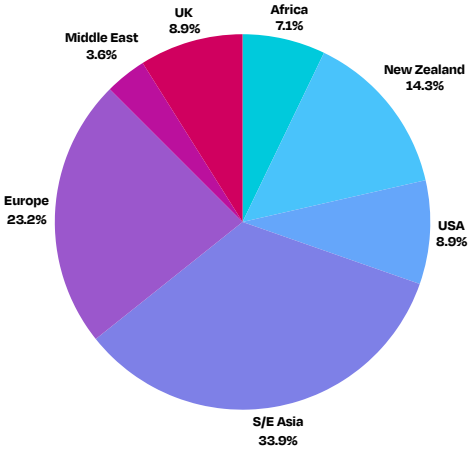
AUSCERT Conference



AUSCERT2024 empowered participants to amplify their impact in cyber security. The theme highlights the far-reaching influence of individual actions within the broader cyber community, promoting a "pay it forward" mindset—demonstrating how shared knowledge and collaboration create a ripple effect that strengthens the entire industry.

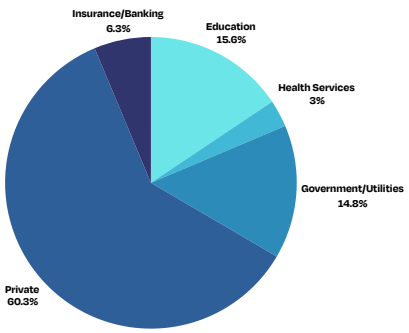
AUSCERT's Cyber Security Conference continues to grow each year, earning increased international recognition. Attendees now join us from across the globe, including **New Zealand, the USA, and Southeast Asia.**

Demographics by Region

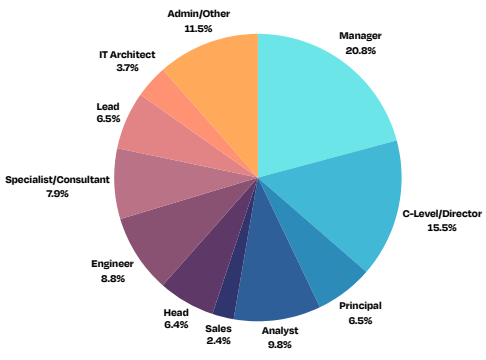


Over the years, we have built a strong community spanning diverse industries and roles. Our data shows that **private enterprises** make up the largest attendee segment, followed by the **education sector** and then **government/utilities**. Most participants are **managers or directors,** reflecting a network of experienced professionals and industry leaders driving cyber security forward.

Demographics by Industry



Demographics by Position



Community Outreach

Community engagement is essential for building connections, sharing knowledge, and strengthening the cyber security industry. This involves active collaboration with global partners to exchange intelligence, provide support, and share resources. By fostering these relationships, AUSCERT enhances the global cyber security ecosystem and improves its ability to counter cross-border cyber threats.

As a CERT supporting all industries in Australia and neighbouring regions, AUSCERT maintains strong partnerships with numerous CERTs/CSIRTs worldwide. These relationships are vital for enabling timely information sharing, coordinated incident response, and the development of cyber security best practices.

Hear from our Members!

"In these ever-changing times, I have faith that integrity means something. When I think of AUSCERT I think of integrity, leadership, collaboration, community, and future.

Australia needs AUSCERT and AUSCERT needs Australia to support it because the future of our children rests in the hands of entities like AUSCERT, its membership base and those who support it every year."

Brian Hay

Co-Founder and Executive Director, Cultural Cyber Security Director at Cybernation

Asia-Pacific Computer Emergency Response Teams (APCERT)

AUSCERT collaborates with APCERT to enhance cyber security across the Asia Pacific, fostering global cooperation among CERTs and CSIRTs. We actively participate in working groups and cyber exercises to strengthen incident response. In 2024, an APCERT initiative trained Hong Kong CERT in using Machine Learning for phishing domain prediction and improving threat detection. Additionally, AUSCERT began sharing weekly Cyber Threat Intelligence (CTI) with APCERT, reinforcing regional cyber security efforts.

FIRST

We are proud to maintain a strong partnership with FIRST, a leading global organisation for Incident Response and Security Teams. As active members, we strengthen our ability to respond swiftly and effectively to security incidents while fostering collaboration within the global cyber security community. This year, we began working with Ethio-CERT to support the deployment of CERT/CSIRT tools, enhancing their cyber security capabilities and incident response readiness.

Australian 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.

IDCARE

This year, AUSCERT and the University of Queensland collaborated with IDCARE to deliver the Cyber and Critical Tech Co-operation Program, providing tailored cybercrime and online scam response assistance to microbusinesses and individuals in Papua New Guinea and Fiji. This initiative evaluates the applicability of proven Australian cyber security capabilities within the Indo-Pacific, aiming to strengthen community response and build long-term resilience against cyber threats. AUSCERT is proud to partner with IDCARE and the University of Queensland in supporting our Indo-Pacific neighbours and enhancing cyber security across the region

AUSCERT
Allies in Cyber Security

AUSCERT PODCAST

Share Today Save Tomorrow

Our podcast brings you engaging insights, compelling stories, expert knowledge, and personal journeys from across the industry, offering valuable lessons that can be applied in any workplace. By fostering a connected community and facilitating meaningful discussions, we provide a platform for diverse voices committed to advancing cyber security.

With a steadily growing audience, we remain dedicated to our mission—sharing relevant insights today to help build a stronger, more resilient community for the future.

In 2024, we released nine episodes covering a wide range of topics and featuring exceptional guest speakers. Explore them below!

1. **Episode 30: Security Culture** - Featuring Daisy Wong, FlyBuys
2. **Episode 31: Cybercrime** - Featuring Nigel Phair, Monash University
3. **Episode 32: Behaviour change to reduce threats** - Featuring Jane O'Loughin, CERTNZ
4. **Episode 33: The world of AI** - Featuring Luke Zaphir, University of Queensland
5. **Episode 34: Wireless in an undiscovered country** - Featuring Edward Farrell, Mercury ISS
6. **Episode 35: Introducing Ivano** - Featuring Ivano Bongiovanni
7. **Episode 36: Changing face of Incident Response** - Featuring Kylie Watson, DXC
8. **Episode 37: Conference MC Extraordinaire, Adam Spencer** - Featuring Adam Spencer
9. **Episode 38: Security Awareness + Education culture = Behaviour change** - Featuring Kelsy Luengen, Seek

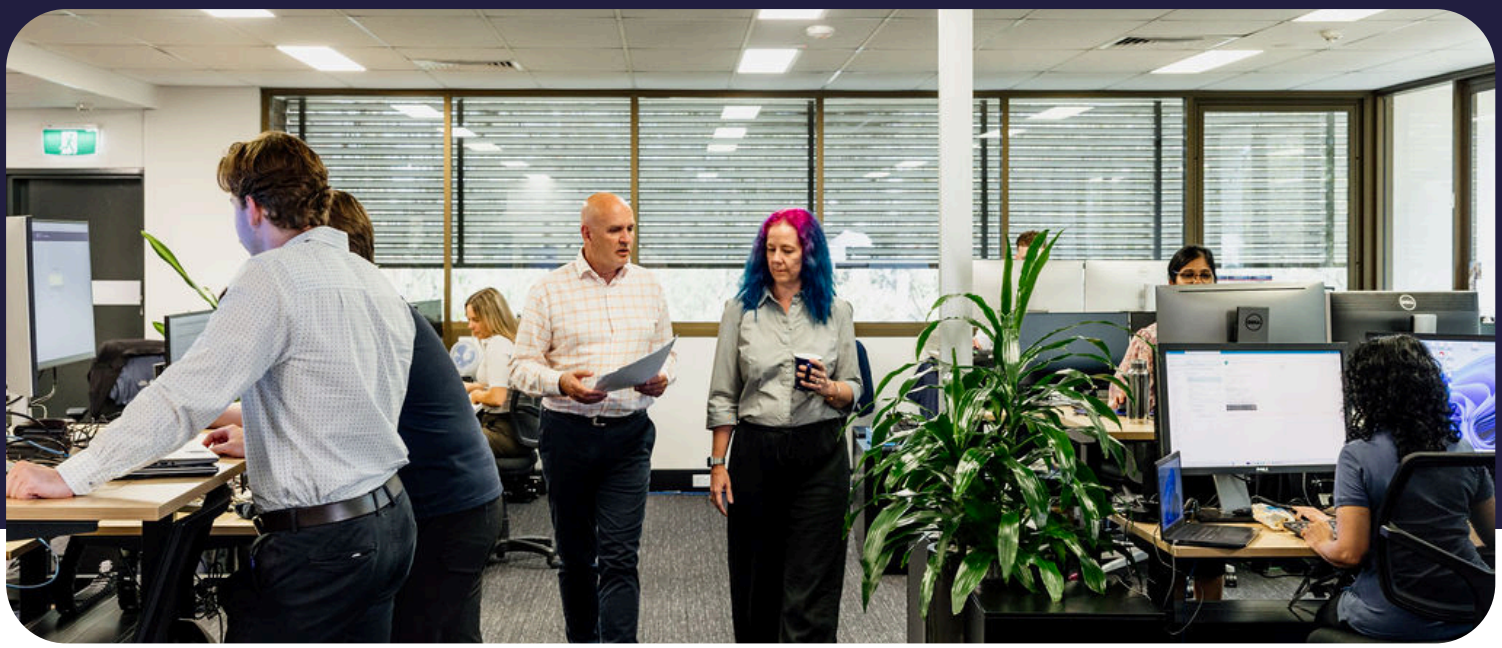
2,433 plays in the last 12 months

Most Plays Per Country



AUSCERT
Allies in Cyber Security

Infrastructure Updates



Member Service Updates

In 2024 we rolled out a new look for the Member portal which followed a pipeline of improved functionality across services, complete with an enhanced member portal and exciting new features!

MSINS

We've updated our MSINs to include the severity level in the subject line. For example:[Severity: CRITICAL] AUSCERT Member Security Incident Notification (MSIN) for “Member Name” Individual events in MSINs are now categorised into severity levels.

MSINS Dashboard

The beta version of our new MSINs dashboard is now available on the AUSCERT Member Portal. The dashboard provides a completely new way to view and interact with your organisation’s **Member Security Incident Notifications (MSINs)**. The dashboard enables us to share more data about your organisation and features search, filter, and query options; plus a more detailed view of each alert. An API with two GET endpoints is available for automating workflows, you’ll find documentation linked on the portal. We’ve included some graphs to illustrate data relevant to your organisation as well as an Australian overview for comparison. MSIN email subscriptions remain unchanged and the original calendar view is still accessible via a button in the header of the MSIN dashboard homepage.

Early Warning SMS Alerts

We have enhanced the **Early Warning SMS** service to ensure members are promptly informed about critical vulnerabilities. SMS Alerts are sent whenever AUSCERT issues a **Critical Member Security Incident Notification** (MSIN).

Sensitive Information Alerts (SIAs)

Previously, SIA emails included an encrypted file attachment and a link to retrieve the symmetric key from the Member Portal for decryption. With this update, emails will now contain a unique URL directing members to the portal, where they can generate a temporary download link—eliminating the need for decryption and streamlining access. Future enhancements will introduce API access and a Member Portal dashboard for even greater convenience.

Documentation Hub

The **Documentation Hub in our member portal,** designed to centralise all technical resources, including user guides, API documentation, and other vital materials. While the hub is currently in its early stages, our aim is to migrate existing documentation and will continue to expand it with fresh resources. As part of its features, the hub offers both light and dark mode options for an optimal viewing experience. Notably, all API and user guides for the new MSINs service are already available, making it the go-to destination for members seeking up-to-date technical support.

Feedback Feature

Thank you to all who have already been putting our **Feedback Feature** to good use and sharing your thoughts and ideas. Whether you have a suggestion, a question, or a concern, you can now provide feedback on service improvements and changes directly through the portal. This streamlined feature ensures your voice is heard, enabling us to continuously enhance your experience and address your needs effectively.

Bulletins Updates

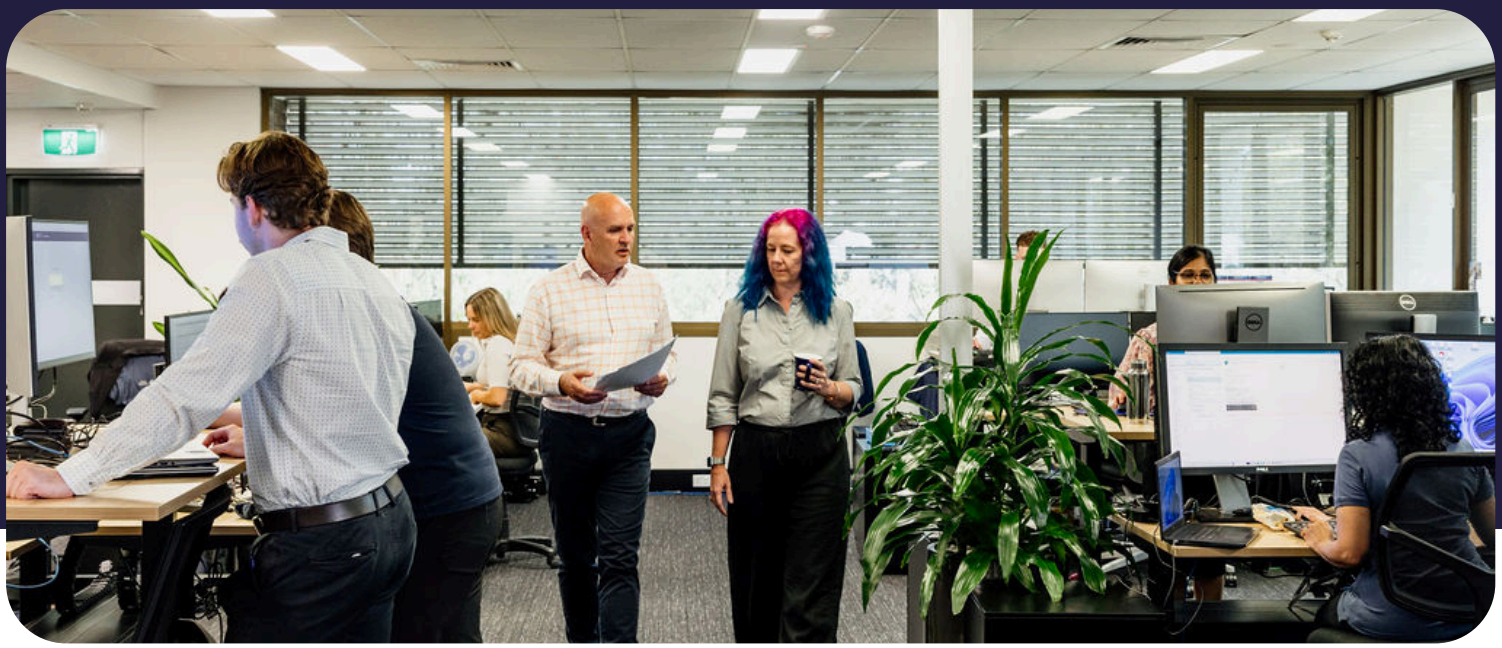
We have updated our system that produces AUSCERT Security Bulletins to ensure members receive the most benefits.

- **Introduction of advanced filtering options**, empowering users to merge filters and search parameters for smoother navigation
- **Consolidated OS Categories:** Some end-of-life operating system categories have been consolidated for data consistency. Existing email subscriptions remain unchanged. We recommend reviewing your subscriptions to ensure you receive Bulletins for your chosen operating systems and familiarise yourself with the updated options. You can update your preferences through the Member Portal.
- **Digital Signature Removal:** Bulletins will no longer be digitally signed. Previously, they were wrapped with a GPG signature; however, feedback indicated this was not a priority.
- **Daily Digest Option:** Members can opt to receive AUSCERT Bulletins as a daily digest issued at the end of each business day. Subscribe now through the Member Portal.

Bulletins - Exploitability Index & Exploitation Predication Scoring System

Bulletins now feature **Exploitability Index (EI) for its Microsoft AUSCERT Security Bulletins (ASB)**. The Exploitability Index forecasts which vulnerabilities are likely to be exploited within 30 days of an advisory's release, helping organisations to prioritise their vulnerability management. AUSCERT has also introduced **Exploitation Prediction Scoring System (EPSS)** within our bulletins and Critical MSIN.

Conclusion



Having been at AUSCERT for almost a year, I've had the privilege of witnessing a truly transformative period for the organisation. From refreshing our brand identity to making key infrastructure upgrades to our member portal and services, it has been an exciting journey of growth and innovation.

It is not an understatement to say that our industry is going through some seismic changes. It's encouraging, and exciting, to see how much the overall maturity has improved. At the same time, there's still so much work to do.

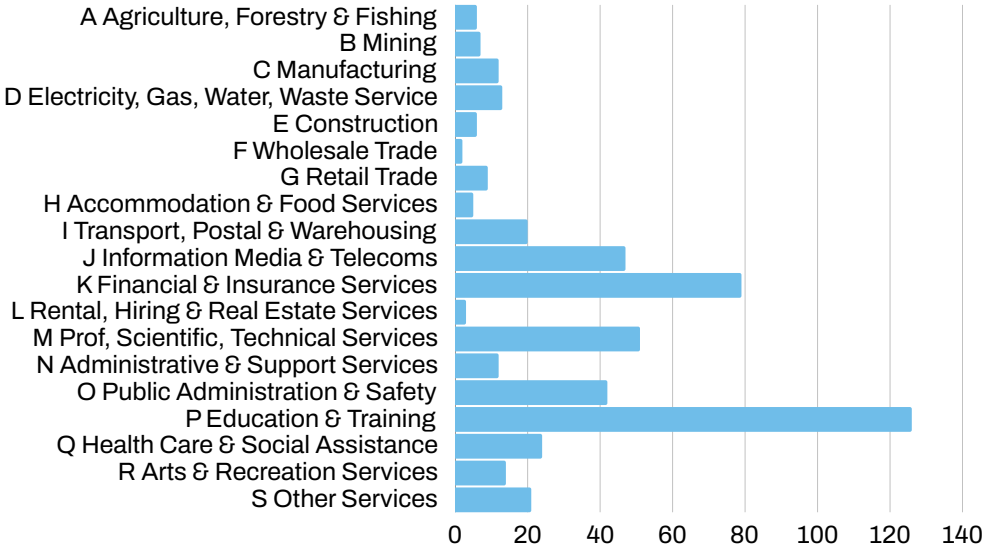
AUSCERT wants to skate to where the pack is going to be, not where it has been. Our team is focused on automating more processes, allowing us to dedicate more time to our members while prioritising critical projects and services. I'm excited for what's to come and the continued evolution of AUSCERT in supporting the cyber security community.

Dr Ivano Bongiovanni

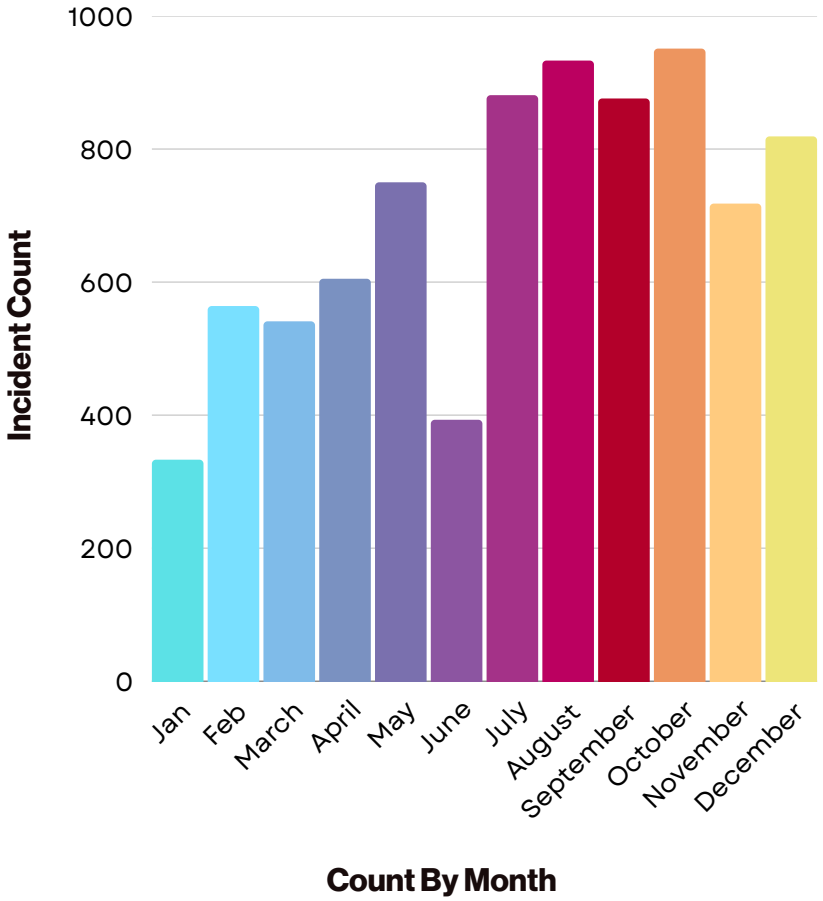
General Manager , AUSCERT

Appendix

2024 ANZ Standard Industrial Classification

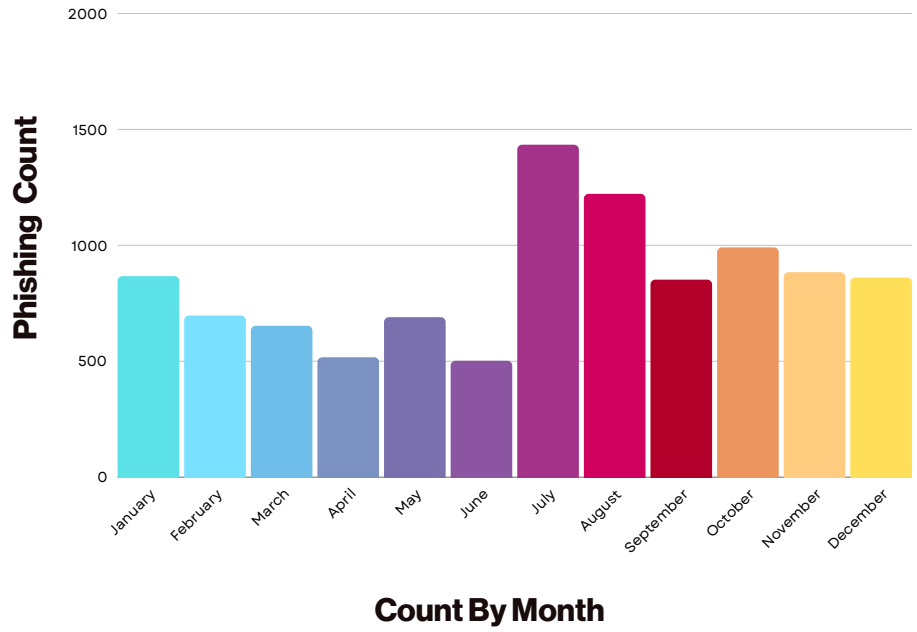


2024 Incident Frequency Graph

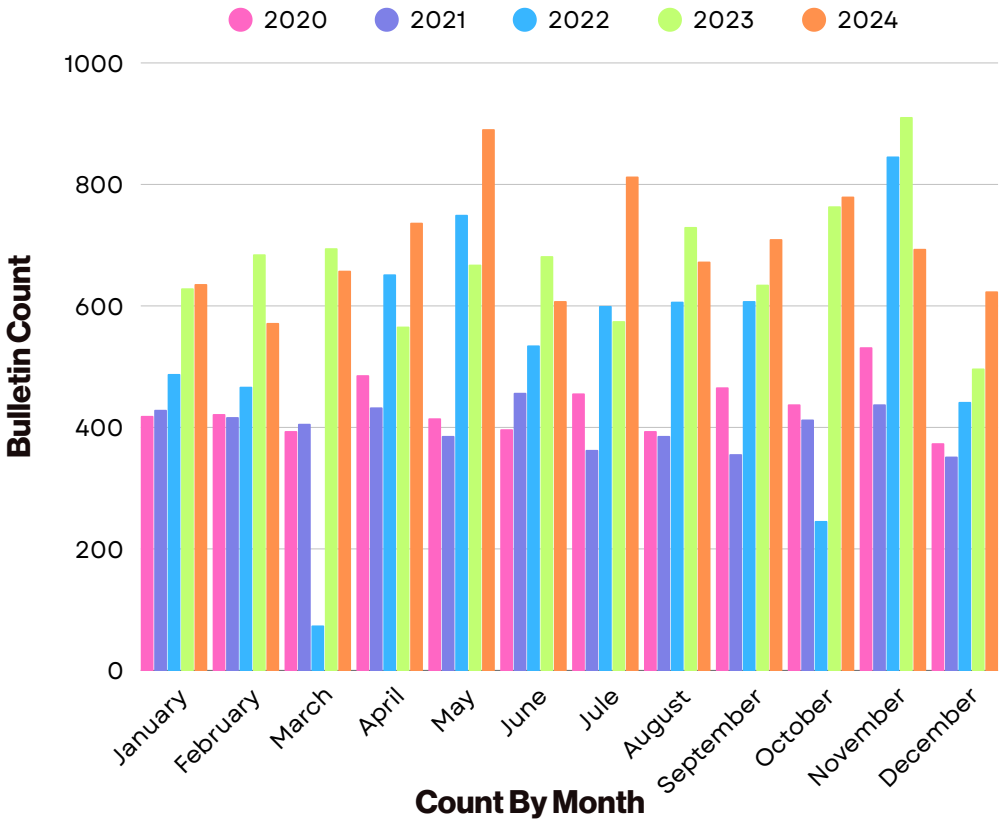


Appendix

2024 Phishing Takedowns

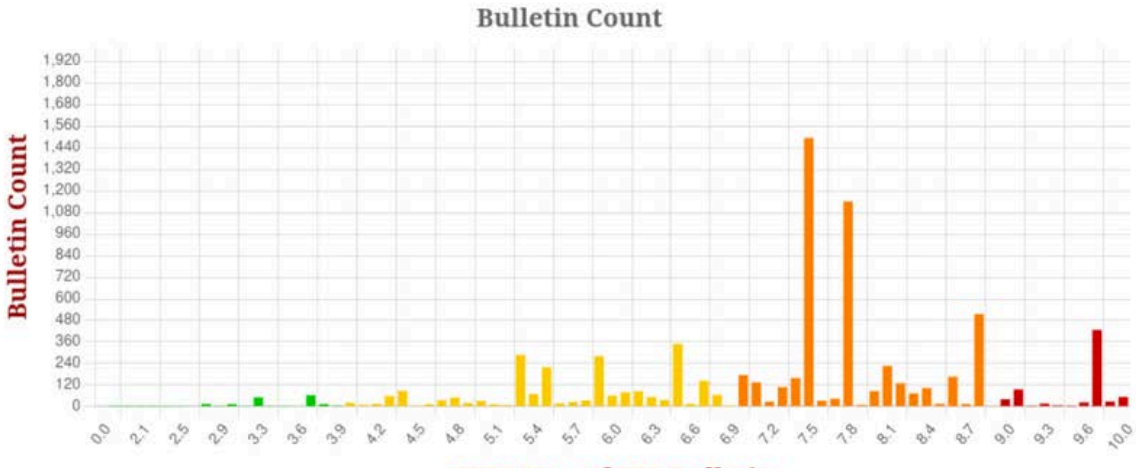


5 Year Bulletin Comparison

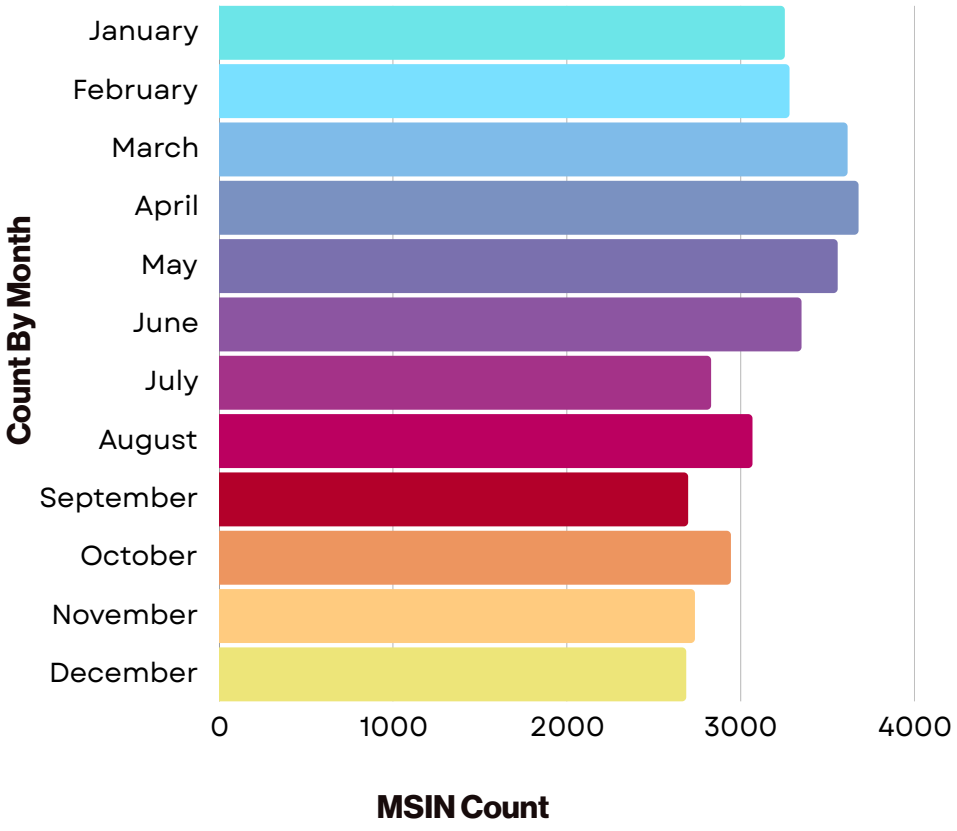


Appendix

2024 CVSS Max of ESB Bulletin

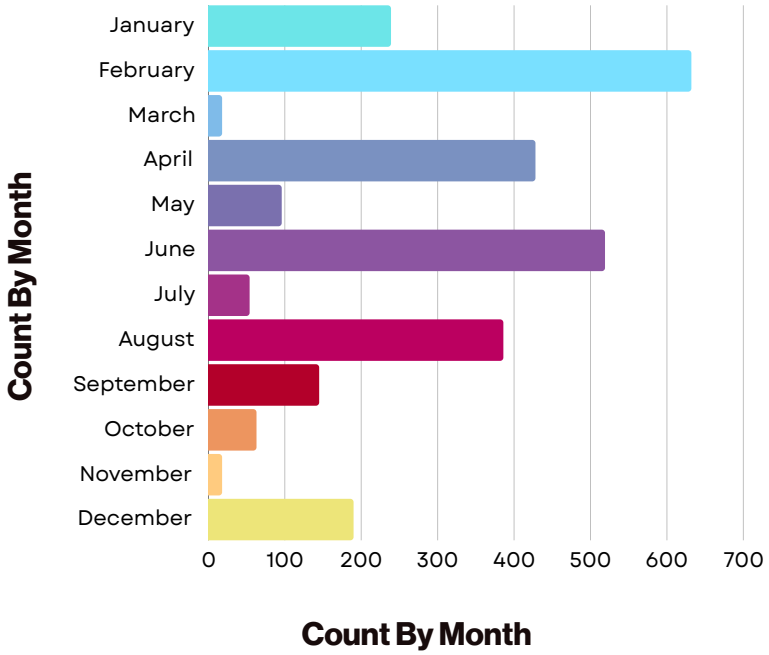


2024 MSINs

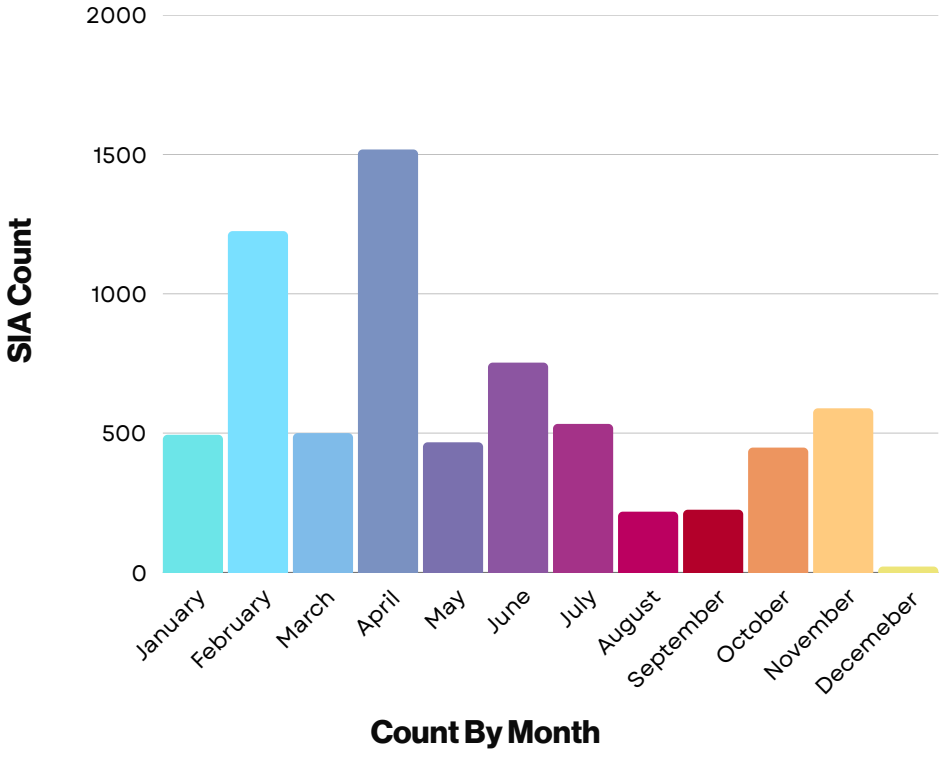


Appendix

2024 Critical MSINs

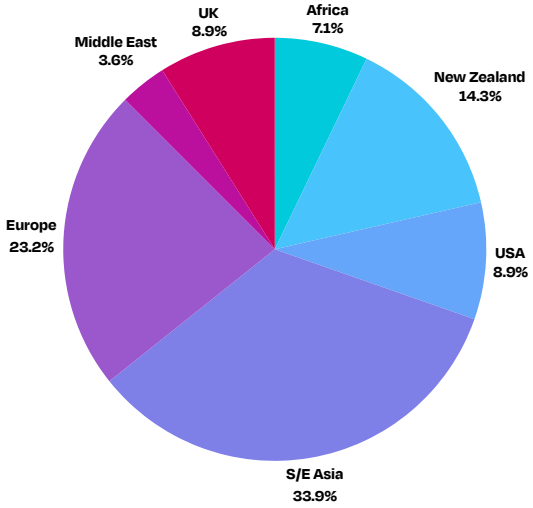


2024 SIA Frequency

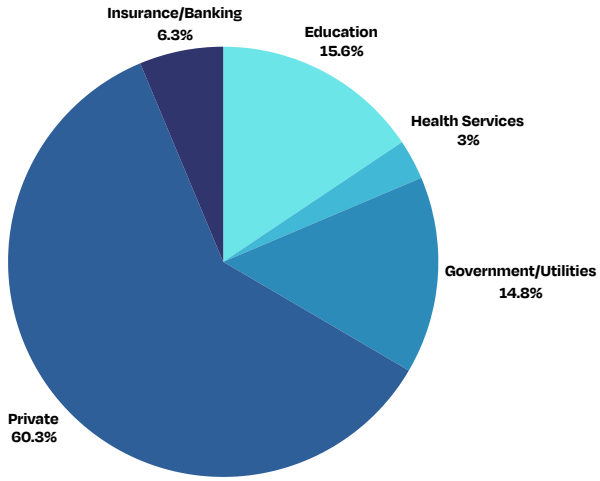


Appendix

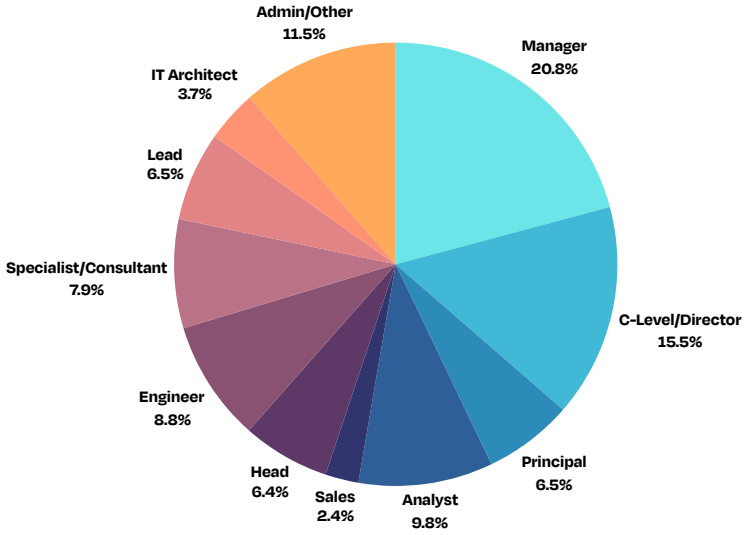
AUSCERT2024 Demographics by Region



AUSCERT2024 Demographics by Industry



AUSCERT2024 Demographics by Position



AUSCERT

Allies in Cyber Security