AUSCERT

– AUSTRALIAN PIONEER CYBER EMERGENCY RESPONSE TEAM

# MEMBERSHIP SERVICES AND BENEFITS

# MEMBERSHIP SERVICES

AUSCERT provides members with proactive and reactive advice and solutions to current threats and vulnerabilities. We'll help you prevent, detect, respond and mitigate cyber-based attacks.

As a not-for-profit security group based at The University of Queensland, AUSCERT provides a range of comprehensive services to strengthen your cyber security strategy.

AUSCERT services are split across three capability pillars: Incident Support, Vulnerability Management and Threat Intelligence. These services are all included in AUSCERT Membership.

## INCIDENT SUPPORT

The AUSCERT team is here to support you, whether you're facing a cyber incident or in need of guidance and direction. Our dedicated team is readily available to provide assistance, ensuring you have the help you need to resolve the situation or obtain the necessary guidance to move forward.

An incident is any event or activity compromising the confidentiality, integrity, or availability of your computer systems, networks, or data.

**SERVICES INCLUDED:**

- ✓ **Incident Support**
- ✓ **Phishing Takedown**

**DESCRIPTION:**

- The AUSCERT Incident Support service aids your organisation in assisting, understanding, and addressing incidents and attacks from across the globe.
- The AUSCERT team offers support in incident response, actively gathering information from diverse channels to locate data that is relevant to you. We take immediate action and follow well-defined protocols in order to obtain a resolution and satisfactory outcome.
- AUSCERT is a trusted intermediary, coordinating communication about incidents between affected parties.
- Incident support also includes AUSCERT's Phishing Takedown service, which assists your organisation by managing the takedown process of malicious sites and domains. If your organisation is targeted or affected by phishing or malicious websites, our team can analyse the situation and take appropriate action.

**WHAT'S INCLUDED:**

**Response support & assistance**

AUSCERT offers up to three hours of support per incident. If the incident requires further assistance, we assess the scope of the issue to determine if an analyst can be allocated (at cost). Should the team be unable to provide further direct assistance (due to the nature of the incident), AUSCERT offers unbiased recommendations or referrals to trusted providers.

**Dedicated skilled resource pool**

Access to our highly skilled team of analysts and developers who possess various certifications, including SANS GIAC, and are available to assist you through email, Slack, or our 24/7 telephone support hotline.

**Phishing takedown management**

AUSCERT's Phishing Takedown service is designed to assist your organisation from a multitude of phishing 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 the removal of the malicious website.

**Malware & Log Analysis**

Malware and log analysis support is available for your organisation through AUSCERT via our toolkits and analysis platforms. This entails identifying threats, recommending best practices and mitigation approaches against the threat.

## VULNERABILITY MANAGEMENT

Vulnerability management involves identifying, assessing, and mitigating weaknesses in computer systems, applications, and networks to enhance overall security. It includes applying measures such as patches and best practices to minimise the risk of exploitation.

**SERVICES INCLUDED:**

- ✓ **Security Bulletins**
- ✓ **Member Security Incident Notifications (MSINs)**
- ✓ **Critical MSINs**
- ✓ **Early Warning SMS Alerts**

**DESCRIPTION:**

- AUSCERT specialises in vulnerability research to deliver members a consistently formatted feed of bulletins across major platforms and vendors streamlining security patching.
- Security Bulletins provide concise summaries of content, enabling readers to quickly grasp essential information. They facilitate easy determination of severity and aid in prioritizing organizational security patching efforts.
- Using the Common Vulnerability Scoring System (CVSS) as the industry standard, AUSCERT identifies and references vulnerabilities through Common Vulnerabilities and Exposures (CVE) identifiers. Accompanying each vulnerability is a suggested resolution, including patching/upgrading and mitigation recommendations.
- Security Bulletins are published by AUSCERT each business day with content curated and checked to ensure up-to-date information is provided to our members.
- Member Security Incident Notifications (MSINs) are customised security reports for each member's organisation, based on your IPs and

domains. Tailored MSINs will inform you of vulnerabilities impacting your organisation.

- Critical MSINs can be issued detailing serious vulnerabilities that have been discovered with domains/IPs registered with us that are using the vulnerable product, software, or service.
- Receive SMS notifications for the most critical security vulnerabilities.

**WHAT'S INCLUDED:**

**Security Bulletin Email Subscriptions**

Members can create multiple customised email subscriptions to the Security Bulletins service for specific operating systems and environments that are relevant to your organisation. Bulletins are sent via email immediately as they are published by AUSCERT.

Security Bulletins are also available via an RSS Feed which is provided in the same consistent format.

**Security Bulletin Daily Bulletin Digest**

Alternatively, members can subscribe to receive the Daily Bulletin Digest. This is a single email issued at the end of each business day that summarises all the bulletins published by AUSCERT that day, with hyperlinks to view each bulletin.

**MSINs**

MSINs provide daily notifications about vulnerabilities, incidents, and recommended mitigation strategies. Members only receive an MSIN if there is at least one incident report related to their IPs/domains within the past 24 hours. If no incidents are detected, no MSIN is sent. Members have the option to mute specific reports for a particular IP/domain if they no longer wish to receive notifications about them.

**Critical MSINs**

These will be distributed as they emerge and will be flagged accordingly for urgent attention to mitigate potential high-priority risks. For example, zero-day and other critical vulnerabilities.

**Early Warning SMS Alerts**

The analyst team sends Early Warning SMS alerts to designated contacts listed on your membership account for critical vulnerabilities requiring immediate action to protect a member's security. These alerts provide details of the relevant security bulletin containing potential advice or solutions.

## THREAT INTELLIGENCE

Threat Intelligence is knowledge and information about potential or known cyber threats which pose risks to an organisation's data, systems, and networks.

This includes collecting, analysing, and interpreting information from various sources to gain insights into the Tactics, Techniques, and Procedures (TTPs) employed by threat actors.

By leveraging this intelligence, organisations can strengthen their security posture, enhance their threat detection capabilities, and respond effectively to cyber threats, subsequently reducing the risk of successful attacks and minimising the potential impact on their systems and data.

**SERVICES INCLUDED:**

- ✓ **AusMISP**
- ✓ **Malicious URL Feed**
- ✓ **Sensitive Information Alert**
- ✓ **AUSCERT Daily Intelligence Report (ADIR)**

**DESCRIPTION:**

- The AUSCERT MISP service provides members with threat indicators acquired from trusted communities and organisations. It includes AUSCERT's examination of captured malware and other threat samples, as well as dependable third-party sources and members.
- AusMISP serves as a tactical threat Intelligence tool, empowering you to obtain and share timely cyber threat intelligence, including indicators of compromise, attack patterns, and other cyber security-related data. This collaborative intelligence enhances your cyber security posture and helps members better defend against cyber threats and attacks.
- The AUSCERT Malicious URL Feed can be added to your firewall's blocklist, web proxy, content filters, IDS/IPS, and SIEM, to prevent or detect compromises to your network. AUSCERT encounters numerous phishing and malware attacks which are analysed and curated into this Australian-based feed.
- Daily and weekly intelligence reports are available from AUSCERT based on the latest verified cyber security news.
- Sensitive Information Alerts provide notification via email when sensitive material is found online by our analyst team which specifically targets your organisation. The sensitive material typically consists of leaked credentials such as a username in the form of an email address and an authentication string (hash or passwords). We process data from a variety of sources including the dark web, ransomware leak sites, international CERTs, and our trusted partners. These alerts are based on the domains that are registered to your organisation which is nominated and verified on your membership account.

**WHAT'S INCLUDED:**

**AusMISP**

Members who opt into AusMISP will be given access to our MISP instance, which is a shared feed of curated threat intelligence, including the ACSC CTIS (Cyber Threat Intelligence Sharing) data.

Utilise the provided threat indicators to enhance your network security by integrating them into defensive controls like SIEMs, firewalls, IDS/IPS, ACLs, web proxies, and mail filters.

AusMISP enables the sharing of diverse security-related data from members. This includes a comprehensive database that stores both technical and non-technical information about malware, incidents, attackers, and intelligence, such as:

- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)
- Threat actor information

- Network intrusion data
- Vulnerabilities
- Malware characteristics
- Threat intelligence
- Phishing data
- Financial fraud information.

AusMISP can help you identify relationships between attributes and indicators from malware, previous attack campaigns, or analysis through its correlation engine. This aids in connecting campaigns and understanding the techniques used in incidents.

**ADIR**

The AUSCERT Daily Intelligence Report is a daily summary of cyber security news curated by our analysts from multiple reliable sources that enables you to stay up to date with current news and alerts. Each Friday we issue a "Week in Review" (WIR) summary with AUSCERT announcements, essential security bulletins, and key news articles from the week.

**Malicious URL Feed**

This is a live feed and content is frequently added and removed based upon ongoing AUSCERT analysis and intelligence. It is available for two different time periods:

- Previous 24-hour feed
- Previous 7 days feed

It's an all-inclusive feed, for Phishing and Malware in both txt and xml formats.

**Sensitive Information Alert**

Members are issued with a Sensitive Information Alert if leaked credentials or sensitive material are found by our analyst team. Sensitive Information Alerts are issued via email and will include an encrypted file containing the data for your organisation to analyse and action.

# ADDITIONAL BENEFITS

✓ Member benefits for the annual **AUSCERT Cyber Security Conference**, Australia's longest running information security conference.
  - Reduced registration price (available to all members)
  - 50% off one conference registration (small members)
  - One or more conference registrations (medium members and above).

  The next conference will be held on 21-24 May 2024 at The Star Gold Coast. Further details are available here: https://conference.auscert.org.au/

✓ Member pricing for AUSCERT's range of **cyber security training courses**. Course information, pricing and calendar are available here: https://auscert.org.au/services/auscert-education/

✓ Access to AUSCERT member meetups, workshops and events.

AUSCERT.ORG.AU

## QUESTIONS ABOUT OUR SERVICES OR HOW TO BECOME A MEMBER?

membership@auscert.org.au

AUSTRALIA'S PIONEER
CYBER EMERGENCY RESPONSE TEAM