Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Stakeholder kit

Event logging

Table of contents

About this kit

Lose the blind spots – use event logging.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has identified 4 priority actions which are key to bolstering the cyber security of any organisation.

We urge executives, business owners, and IT and cyber security professionals to take action on the second of these priorities – event logging.

What is event logging and why does it matter?

Event logs are records of system occurrences, which can include malicious or unauthorised activity.

Event logging supports the continued delivery of operations and improves the security and resilience of critical systems by enabling network visibility.

Without logs, you're flying blind. You won't have insight into system behaviour, application issues or user actions – giving malicious threat actors the upper hand.

Implementing a threat detection strategy takes event logging to the next level, and improves an organisation's chances of detecting malicious behaviour in their systems and networks.

Event logging and threat detection are key components in any organisation's cyber defence arsenal.

How can you help?

You can use the key messages and resources in this kit to raise awareness of ASD's ACSC's event logging advice and messaging, by:

- ✓ Ensuring your organisation understands the importance of event logging and takes action to implement best-practice advice.
- ✓ Telling your technical audiences, stakeholders, staff and customers about the importance of implementing effective event logging and share the key messages.
- ✓ Featuring content and information about event logging in internal and external newsletters and on your website.
- ✓ Forwarding to your communications team to repurpose this content across your internal and external communications channels.
- ✓ Sharing content from this kit on social media and encouraging your audiences to take action.
- ✓ Providing talking points to your managers, senior leaders and executive for meetings, events and engagements to start the conversation about prioritising event logging practices.
- ✓ Directing people to cyber.gov.au/eventlogging to take action.

Key messages

For organisations

- Cyber incidents are on the rise, but you can't defend against what you can't see.
- Event logs keep a record of what's happening in your networks – helping you spot suspicious activity and stop threats sooner.
- Without logs, you're flying blind and malicious cyber actors can move within your networks undetected.
- Without event logging you can't see anomalies when they occur.
- Poor logging gives attackers places to hide in your networks.
- Event logging can help you monitor better, detect sooner, and remain cyber resilient.

For executives

- Time is money. Respond to threats sooner with event logging.
- Find threats on your networks sooner rather than later with event logging.
- Missing logs give malicious threat actors the upper hand. Don't wait for your data and networks to be exposed.

For IT and cyber security professionals

- Malicious cyber actors can compromise devices and leverage legitimate system tools to maintain a presence in networks and avoid detection.
- Use best practice logging techniques to mitigate against this including:
    - Develop and implement an enterprise approved logging policy.
    - Implement a centralised event logging facility such as a secured data lake to enable log aggregation and then forward select, processed logs to analytic tools, such as security information and event management (SIEM) solution and extended detection and response (XDR) solutions.
    - Store detailed logs in a secure, central location that is write-once, read-many to avoid the risk of attackers changing or deleting event logs.
    - Maintain baselines of network, user, administrative, and application activity.
    - Build or acquire automation (such as machine learning models) to continually review all logs to compare current activities against established behavioural baselines and alert on specified anomalies Leverage user and behaviour analytics to better identify suspicious activity.

Calls to action

- Lose the blind spots. Use event logging. Take action now with our event logging guidance.
- You can't defend against what you can't see. Take action now with our event logging guidance.
- Visit cyber.gov.au/eventlogging for best-practice advice and publications on event logging.

Editorial content

Use this content across your communication channels, newsletters, staff intranet pages, website news, and customer or stakeholder emails.

Lose the blind spots. Use event logging

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is urging organisations to take action and implement effective event logging practices.

Event logging is a critical element of any cyber security strategy, helping to answer who did what, when, and how in your systems?

Without effective event logging, malicious actors can move through networks undetected. So, how can you defend against something you can't see?

At its core, effective event logging and threat detection aims to alert network defenders when cyber security events occur and support incident response by revealing the scope and extent of a compromise.

Setting up event logging enables defenders to detect, defend and respond to events or incidents. The types of events that logging captures can vary; these could be user application logs, firewall logs or anti-virus software logs.

ASD's ACSC has seen an increase in instances of malicious actors employing 'living off the land' (LOTL) techniques, again highlighting the importance of taking action to implement and maintain an effective event logging solution.

Organisations should also take action in the form of threat detection.

Threat detection best practices include:

- Develop and implement an enterprise approved logging policy.
- Implement a centralised event logging facility such as a secured data lake to enable log aggregation and then forward select, processed logs to analytic tools, such as security information and event management (SIEM) solution and extended detection and response (XDR) solutions.
- Establish and continuously maintain baselines of network, user, administrative, and application activity and least privilege restrictions.
- Build or acquire automation (such as machine learning models) to continually review all logs to compare current activities against established behavioural baselines and alert on specified anomalies.
- Reduce alert noise by fine-tuning via priority (urgency and severity) and continuously review detections based on trending activity.
- Leverage user and behaviour analytics to better identify suspicious activity.

When used effectively, event logging and threat detection helps defenders spot cyber security incidents early and detect malicious activity on the network.

Learn how to take action on event logging now at cyber.gov.au/eventlogging.

Further resources

Get social

Join the conversation by following ASD's social media channels and share our content with your followers. By sharing ASD's social content you can help your followers improve their cyber security.

ASD will post regularly over the campaign period. Make sure to share using the hashtags #EventLogging, #CyberSecurity and #InfoSec.

@ASDGovAU

Australian Signals Directorate

asd.gov.au

Australian Signals Directorate

Become an ASD Partner

Join ASD's Cyber Security Partnership Program as a Business or Network Partner to receive cyber security alerts, advisories and up-to-date advice, and initiatives to uplift the cyber resilience of Australian organisations.

Responding to cyber incidents

For immediate assistance during a cyber incident, **call the 24/7 Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).**

ASD is not a regulator; we are here to help you respond to and recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call our 24/7 hotline.

If you request support, we can provide you with immediate advice and assistance, which may include:

- information on how to contain and remediate an incident
- intelligence and advisory products to help you with your incident response
- linking you to Australian Government entities that may further support your response.

Every report helps us build a national cyber threat picture and informs the development of our advice and guidance.

About ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security.

Who we help

Our advice and assistance is for the whole economy, including:

- critical infrastructure and systems of national significance
- federal, state and local government
- small and medium businesses
- academia
- charities and not-for-profit organisations
- the Australian community.

What we do

ASD brings together capabilities to improve Australia's national cyber resilience. Its services include:

- providing the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, on 1300 CYBER1 (1300 292 371)
- publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- monitoring cyber threats and intelligence sharing with partners
- helping Australian entities respond to cyber security incidents
- enhancing the cyber security resilience of Australian entities with exercises and uplift activities
- enabling Australian organisations and individuals to engage with the ASD's ACSC and fellow partners through ASD's Cyber Security Partnership Program.

The most effective cyber security is collaborative and our partnerships are key. We thank contributors to the development of our guidance and the organisations who help uplift Australia's cyber security by sharing the latest cyber security advice, alerts and guidance.

Further assistance

ASD is not a regulator; we are here to help you recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call 1300 292 371 (1300 CYBER1).

Your report helps us build a national cyber threat picture and informs the development of our advice and guidance.

Get in touch

If you would like to subscribe to receive future stakeholder kits from ASD's ACSC or have any questions, please email our Public Communication team at asd.publiccomms@defence.gov.au.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre