Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

Guidelines for system monitoring

Event logging and auditing

Event logging strategy

By developing an event logging strategy, an organisation can ensure the accountability of all user actions on a system and improve their chances of detecting malicious behaviour.

Security Control: 0580; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.

Centralised logging facility

A centralised logging facility can be used to correlate event logs from multiple sources. This functionality may be provided by a Security Information and Event Management solution.

Security Control: 1405; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A centralised logging facility is implemented and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs.

Security Control: 0988; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.

Events to be logged

The following list of events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Security Control: 0584; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
For any system requiring authentication, logon, failed logon and logoff events are logged.

Security Control: 0582; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The following events are logged for operating systems:

- *access to important data and processes*
- *application crashes and any error messages*
- *attempts to use special privileges*

- *changes to accounts*
- *changes to security policy*
- *changes to system configurations*
- *Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP) requests*
- *failed attempts to access data and system resources*
- *service failures and restarts*
- *system startup and shutdown*
- *transfer of data to external media*
- *user or group management*
- *use of special privileges.*

Security Control: 1536; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The following events are logged for web applications:

- *attempted access that is denied*
- *crashes and any error messages*
- *search queries initiated by users.*

Security Control: 1537; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The following events are logged for databases:

- *access to particularly important information*
- *addition of new users, especially privileged users*
- *any query containing comments*
- *any query containing multiple embedded queries*
- *any query or database alerts or failures*
- *attempts to elevate privileges*
- *attempted access that is successful or unsuccessful*
- *changes to the database structure*
- *changes to user roles or database permissions*
- *database administrator actions*
- *database logons and logoffs*
- *modifications to data*
- *use of executable commands.*

Events log details

For each event logged, sufficient detail needs to be recorded in order for the event log to be useful.

Security Control: 0585; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
For each event logged, the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.

Event log protection

Effective event log protection and storage ensures the integrity and availability of captured event logs.

Security Control: 0586; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Event logs are protected from unauthorised access, modification and deletion.

Event log retention

Since event logs can contribute to investigations following cyber security incidents, they should ideally be retained for the life of a system, and potentially longer. However, the minimum retention requirement for these records under the National Archives of Australia's ***Administrative Functions Disposal Authority*** publication is seven years.

Security Control: 0859; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
*Event logs are retained for a minimum of 7 years in accordance with the National Archives of Australia's **Administrative Functions Disposal Authority** publication.*

Security Control: 0991; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
DNS and proxy logs are retained for at least 18 months.

Event log auditing

Auditing of event logs is an integral part of maintaining the security posture of systems. Such activities can help detect and attribute any violations of security policy, including cyber security incidents.

Security Control: 0109; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Event log auditing procedures are developed and implemented covering the scope and schedule of audits, what constitutes a violation of security policy, and actions to be taken when violations are detected, including reporting requirements.

Security Control: 1228; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Events are correlated across event logs to prioritise audits and focus investigations.

Further information

Further information on event logging associated with a cyber security incident can be found in the ***Guidelines for cyber security incidents***.

Further information on retaining event logs can be found in the National Archives of Australia's ***Administrative Functions Disposal Authority*** publication at http://www.naa.gov.au/information-management/records-authorities/types-of-records-authorities/AFDA/index.aspx.

Vulnerability management

Vulnerability management strategy

Vulnerability management activities can assist organisations to be proactive in identifying, prioritising and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide organisations with a wealth of valuable information about their exposure to cyber threats, as well as assisting them to determine security risks associated with the operation of systems. Undertaking regular vulnerability management activities is important as cyber threats will change over time.

Security Control: 1163; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A vulnerability management strategy is developed and implemented that includes:

- *conducting vulnerability assessments and penetration tests for systems throughout their life cycle to identify security vulnerabilities*
- *analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls*
- *using a risk-based approach to prioritise the implementation of identified mitigations or treatments*
- *monitoring information on new or updated security vulnerabilities in operating systems, software and ICT equipment as well as other elements which may adversely impact the security of a system.*

Conducting vulnerability assessments and penetration tests

A vulnerability assessment can consist of a documentation-based review of a system's design, an in-depth hands-on assessment or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible. A penetration test however is designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical business information or services.

Conducting a vulnerability assessment and penetration test prior to systems being deployed, and after significant changes, can allow an organisation to establish a baseline for system monitoring activities. In addition, conducting a vulnerability assessment and penetration test annually can ensure that the latest cyber threats are being addressed.

Overall, a vulnerability assessment or penetration test should be conducted by suitably skilled personnel independent of the system being assessed. Such personnel can be internal to an organisation or a third party. Where possible, it is advisable that system managers do not conduct such activities themselves. This ensures that there is no conflict of interest, perceived or otherwise, and that the activities are undertaken in an objective manner.

Security Control: 0911; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Vulnerability assessments and penetration tests are conducted by suitably skilled personnel before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner.