CIS Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why is this CIS Control Critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes, audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes but rarely analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems and take less configuration to turn on. Audit logs typically include user-level events -- when a user logs in, accesses a file, etc. -- and takes more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remains undetected for a long period of time.

8.1: Establish and Maintain an Audit Log Management Process

Establish and maintain a documented audit log management process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- None

Inputs

1. GV26: Enterprise's audit log management process
2. Date of the last review of the audit log management process

Operations

1. Check if `GV26` the audit log management process exists:
    1. If it exists, M1 = 1
    2. If it does not exist, M1 = 0
2. Review `GV26` for elements of the process and, at a minimum, address the collection, review, and retention of audit logs for enterprise assets:
    1. For each element that exists, assign a value of 1. Sum the values of existing elements. (M2)
    2. Identify and enumerate vulnerability scanners not properly configured to scan every 30 days or less (M6)
3. Compare the date from Input 2 and the current date. Capture the timeframe in terms of months. (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of elements included in the audit log management process
- M3 = Timeframe since the last review of the audit log management process

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve, this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	**The percentage of elements included in the audit log**
Calculation	`M2 / 3`

8.2: Collect Audit Logs

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Asset Type	**Security Function**	**Implementation Groups**
Data	Detect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

- Safeguard 8.1: Establish and Maintain an Audit Log Management Process

Inputs

1. GV1: Enterprise asset inventory
2. GV3: Configuration standards
3. GV26: Enterprise's audit log management process

Operations

1. Use GV1 to identify and enumerate assets capable of supporting logging GV27 (M1):

2. Use GV26 and GV3 as guides to determine, for each asset identified in Operation 1, if it is configured to log events as outlined by the enterprise's process

    1. Identify and enumerate assets properly configured to log events per the process (M2)
    2. Identify and enumerate assets not properly configured to log events per the process (M3)

Measures

- M1 = Count of assets capable of supporting logging
- M2 = Count of properly configured assets to log events per the audit log management process
- M3 = Count of assets not properly configured to log events per the audit log management process

Metrics

Coverage

Metric	**The ratio of logging-capable assets properly configured per the audit log management process.**
Calculation	M2 / M1

8.3: Ensure Adequate Audit Log Storage

Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV27`: Assets capable of supporting logging
2. `GV26`: Enterprise's audit log management process

Assumptions

- It is assumed that if an asset is properly configured to meet the retention policy, that would include log rotation, maximum storage size, etc.

Operations

1. For each asset in `GV27`, collect the asset's logging configuration.

2. Compare the output of Operation 1 and the retention portion of `G26`:

    1. Identify and enumerate assets configured to comply with the retention portion of the process (M2).

    2. Identify and enumerate assets not configured to comply with the retention portion of the process (M3).

Measures

- M1 = Count of `GV27` assets capable of supporting logging
- M2 = Count of assets properly configured to meet retention requirements
- M3 = Count of assets not properly configured to meet retention requirements

Metrics

Logging Storage Coverage

Metric	**The percentage of assets compliant with the organization's logging policy**
Calculation	`M2 / M1`

8.4: Standardize Time Synchronization

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV27`: Assets capable of supporting logging
2. List of approved network time sources/NTP servers

Operations

1. Using `GV27`, identify and enumerate assets capable of supporting time synchronization (M1):

2. Check the configurations of the assets identified in Operation 1:

    1. Identify and enumerate the assets configured using at least two approved time sources from Input 2 (M2)
    2. Identify and enumerate the assets configured using time sources not on the approved list (M3)
    3. Identify and enumerate the assets not configured using time sources (M4)

Measures

- M1 = Count of logging-capable assets that support time synchronization
- M2 = Count of properly configured assets using at least two approved time sources
- M3 = Count of assets configured using non-approved time sources
- M4 = Count of assets not configured to use time sources

Metrics

NTP Compliance Coverage

Metric	**The percentage of assets properly configured with at least two approved synchronized time sources**
Calculation	`M2 / M1`

8.5: Collect Detailed Audit Logs

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV18`: Enterprise assets storing, processing, and transmitting sensitive data
2. `GV26`: Enterprise's audit log management process
3. `GV3`: Configuration standards

Operations

1. Review `GV26` for detailed logging requirements such as event source, date, username, timestamp, source addresses, and destination addresses.
    1. For each detailed logging requirement included, assign a value of 1. Sum all requirements included. (M2)
2. For each asset in `GV18` check configuration using `GV3` as a guide
    1. Identify and enumerate assets properly configured to collect detailed logging requirements (M3)
    2. Identify and enumerate assets not properly configured to collect detailed logging requirements (M4)

Measures

- M1 = Count of assets capable of supporting logging `GV27`
- M2 = Count of detailed logging requirements included in the log management process
- M3 = Count of assets properly configured to collect detailed logs
- M4 = Count of assets not properly configured to collect detailed logs

Metrics

Completeness of Process

Metric	**The percentage of detailed logging requirements included in the logging management process**
Calculation	`M2 / 6`

Logging Coverage

Metric	The percentage of assets properly configured to collect detailed logs
Calculation	`M3 / M1`

8.6: Collect DNS Query Audit Logs

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

Assumptions

The enterprise maintains its own internal DNS Servers.

Operations

1. Use Input 1 `GV1` to identify and enumerate internal DNS Servers (M1)

2. Check the configurations `GV3` of each DNS Server identified in Operation 1

    1. Identify and enumerate DNS servers properly configured to collect logs (M2).
    2. Identify and enumerate DNS servers not properly configured to collect logs (M3).

Measures

- M1 = Count of internal DNS servers
- M2 = Count of properly configured DNS servers
- M3 = Count of DNS servers not properly configured DNS servers

Metrics

DNS Configuration Coverage

Metric	**The percentage of properly configured DNS servers to meet logging requirements**
Calculation	`M2 / M1`

8.7: Collect URL Request Audit Logs

Collect URL request audit logs on enterprise assets, where appropriate and supported.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

Operations

1. Use `GV1` to identify and enumerate assets that support URL logging (M1)

2. For each asset identified in Operation 1, use `GV3` to check configurations for URL logging

    1. Identify and enumerate assets properly configured for logging (M2)
    2. Identify and enumerate assets not properly configured for logging (M3)

Measures

- M1 = Count of assets capable of supporting URL logging
- M2 = Count of assets properly configured for URL logging
- M3 = Count of assets not properly configured for URL logging

Metrics

Configuration Coverage

Metric	The percentage of assets properly configured for URL logging
Calculation	`M2 / M1`

8.8: Collect Command-Line Audit Logs

Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

Operations

1. Use `GV1` to identify and enumerate assets that support command-line auditing of command shells (M1)

2. For each asset identified in Operation 1, use `GV3` to check configurations for command-line auditing of command shells

    1. Identify and enumerate assets properly configured (M2)
    2. Identify and enumerate assets not properly configured (M3)

Measures

- M1 = Count of assets capable of supporting command-line auditing of command shells
- M2 = Count of assets properly configured for command-line auditing of command shells
- M3 = Count of assets not properly configured for command-line auditing of command shells

Metrics

Configuration Coverage

Metric	**The percentage of assets properly configured for command-line auditing of command shells**
Calculation	`M2 / M1`

8.9: Centralize Audit Logs

Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations include leveraging a SIEM tool to centralize multiple log sources.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV27`: Assets capable of supporting logging
2. `GV5`: Authorized software inventory

Operations

1. Use the software inventory `GV5` to identify and enumerate log aggregating software `GV28`

2. For each asset capable of supporting logging, check if asset is covered by at least one log aggregating software

    1. Identify and enumerate assets covered by at least one aggregating software (M2)
    2. Identify and enumerate assets not covered by at least one aggregating software (M3)

Measures

- M1 = Count of `GV27`
- M2 = Count of assets covered by at least one aggregating software
- M3 = Count of assets not covered by at least one aggregating software

Metrics

Log Aggregating

Metric	The percentage of log-producing assets covered by aggregating software
Calculation	`M2 / M1`

8.10: Retain Audit Logs

Retain audit logs across enterprise assets for a minimum of 90 days.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 8.9: Centralize Audit Logs

Inputs

1. `GV28`: Log aggregating software
2. `GV3`: Configuration standards

Operations

1. For each log aggregating software `GV28` use `GV3` to check configuration standards

    1. Identify and enumerate aggregating software configured to retain logs for 90 days or more (M2)
    2. Identify and enumerate aggregating software configured to retain logs for less than 90 days (M3)

Measures

- M1 = Count of log aggregating software `GV28`
- M2 = Count of aggregating software properly configured to retain logs for 90 days or more
- M3 = Count of aggregating software configured to retain logs for less than 90 days

Metrics

Compliance

Metric	**The percentage of aggregating software properly configured to retain logs for 90 days or more**
Calculation	`M2 / M1`

8.11: Conduct Audit Log Reviews

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Asset Type	Security Function	Implementation Groups
Data	Detect	2, 3

Dependencies

- None

Inputs

1. Timestamp for two consecutive log reviews

Assumptions

Log reviews are conducted at regular and consistent intervals

Operations

1. Compare each timestamp to determine the timeframe between log reviews in days (M1)

Measures

- M1 = Timeframe between log reviews

Metrics

- If M1 is greater than seven, this Safeguard is measured at a 0 and receives a failing score.

8.12: Collect Service Provider Logs

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

Inputs

1. `GV29`: Inventory of service providers
2. `GV3`: Configuration standard

Operations

1. For each service provided in `GV29` identify and enumerate service providers that support logging (M1)

2. Use service provider identified in Operation 1, use `GV3` to check configurations

    1. Identify and enumerate service providers properly configured to collect logs (M2)
    2. Identify and enumerate service providers not properly configured to collect logs (M3)

Measures

- M1 = Count of service providers that support logging
- M2 = Count of service providers configured to collect logs
- M3 = Count of service providers not configured to collect logs

Metrics

Coverage

Metric	The percentage of service providers properly configured to collect logs
Calculation	`M2 / M1`