CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why is this CIS Control Critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use "zero-day exploits", which take advantage of previously unknown vulnerabilities that have yet to have a patch released by the software vendor. These software design flaws provice zero days for developers to fix these issues before attackers are able to exploit them. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review their software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

2.1: Establish and Maintain a Software Inventory

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Identify	1, 2, 3

Dependencies

- None

Inputs

1. `GV5`: The authorized software inventory with detailed information including: timestamp indicating both last updated and last verified values, timestamp indicating installation date, operating system, software name, software version, software publisher, authorization status, business purpose, supported/unsupported. Where applicable, additionally include URL, app store(s), deployment mechanism, and decommission date.
2. `GV6`: The date of the last update to the authorized software inventory.

Operations

1. Check `GV5` for completeness of detailed information.
    1. Note items that have complete detailed information (M2).
    2. Note items that have missing or incomplete information (M3).
2. Compare the current date to `GV6` and note timeframe in months (M4).

Measures

- M1 = Count of `GV5`
- M2 = Count of items in `GV5` with complete information
- M3 = Count of items in `GV5` with incomplete or missing information
- M4 = Timeframe in months since last update `GV6`

Metrics

- If M1 is not provided or available, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M4 is greater than six months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Accuracy Score

Metric	What percentage of the current enterprise asset inventory contains necessary detailed information?
Calculation	`M2 / M1`

2.2: Ensure Authorized Software is Currently Supported

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Identify	1, 2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV5`: The authorized software inventory with detailed information. deployment mechanism, and decommission date.
2. Authoritative source of information indicating supported/unsupported details by product.
3. Exception documentation for unsupported software that is necessary for the fulfillment of the enterprise's mission.
4. `GV6`: Date of last update to the authorized software inventory

Assumptions

1. Authorized software inventory with detailed information exists for the enterprise.

Operations

1. For each item in `GV5`, perform a lookup in Input 2 to verify the supported/unsupported status.

    1. Enumerate each item labeled "unsupported" but "supported" based on Input 2 (M2)
    2. Enumerate each item labeled "supported" but "unsupported" based on Input 2 (M3).

2. Identify and note truly "unsupported" items from Input 1 after conducting Operation 1 (M4).

3. For each unsupported item identified in Operation 2, conduct a check using Input 3.

    1. Note items that do not have appropriate exception documentation (M5).
    2. Note items that do have appropriate exception documentation (M6).

4. Compare the date of `GV6` to the current date and note the timeframe in weeks (M7).

Measures

- M1 = Count of Input 1
- M2 = Count of items in Input 1 that are mislabeled as unsupported
- M3 = Count of items in Input 1 that are mislabeled as supported
- M4 = Count of unsupported items
- M5 = Count of items in Input 1 that are no longer supported but exception documentation exists

- M6 = Count of items in Input 1 that are no longer supported and exception documentation does not exist
- M7 = Timeframe in weeks of the last update to the authorized software inventory

Metrics

- If M7 is greater than four, then this safeguard is measured at a 0 and receives a failing score. The other metrics don\'t apply.

Percentage of Unsupported Software in Use

Metric	**What percentage of authorized software inventory in use is unsupported?**
Calculation	`M4 / M1`

Rate of False Positives

Metric	**What percentage of software listed as supported is actually not supported?**
Calculation	`M3 / M1`

Rate of False Negatives

Metric	**What percentage of software listed as unsupported is actually supported?**
Calculation	`M2 / M1`

Percentage of unsupported software with exception documentation

Metric	**What percentage of software listed as unsupported but appropriate exception documentation exists?**
Calculation	`M5 / M4`

2.3: Address Unauthorized Software

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Respond	1, 2, 3

Dependencies

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

Inputs

1. `GV5`: Authorized software inventory
2. `GV1`: Enterprise asset Inventory
3. Enterprise defined timeframe for scanning of enterprise assets.
4. Enterprise defined allowable timeframe for resolution of discovered unauthorized software (recommend at least monthly)

Assumptions

1. The scanning schedule timeframe is greater than the enterprise-defined allowable timeframe for the resolution of discovered unauthorized software.

Operations

1. Identify the software capable enterprise assets in `GV1` (`GV7`)
2. Scan the assets identified in Operation 1 and note software present on each asset (M1)
3. Compare the scan results to the authorized software list in `GV5`
    1. Enumerate unauthorized software identified on assets (M2)
4. Conduct a subsequent scan of assets identified in Operation 1 as dictated by the timeframe in Input 3
    1. Compare to a list generated in Operation 3 (M2)
5. For each software still present in Operation 4, check the authorized software list in `GV5`
    1. Software that remains installed and is not listed in `GV5` is placed on the unaddressed software list (M3) for that asset.

Measures

- M1 = The count of software installed on a given asset
- M2 = The count of unauthorized software installed on a given asset
- M3 = The count of unaddressed software installed on a given asset, identified by follow-up scan.
- M4 = Timeframe for resolution of discovered unauthorized software in weeks

Metrics

- If M4 is greater than four weeks, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Unauthorized software Per Asset

Metric	Ensure unauthorized software installations are addressed
Calculation	`(M2-M3) / M3`

Unauthorized software for the enterprise

- The enterprise metric is calculated by averaging the results calculated above per asset.

2.4: Utilize Automated Software Inventory Tools

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Asset Type	Security Function	Implementation Groups
Software	Detect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.3: Address Unauthorized Software

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV7`: Software capable assets
3. List of software inventory tools

Operations

1. Use `GV1` and `GV7` to identify and enumerate assets unable to support sofware (M2).

2. For each software capable asset `GV7`:

    1. Identify and enumerate if the asset is covered by at least one software inventory tool (M3)

    2. Identify and enumerate if the asset is not covered by at least one software inventory tool (M4)

Measures

- M1 = Count of `GV7`
- M2 = Count of assets unable to support software
- M3 = Count of assets covered by software inventory tools
- M4 = Count of assets not covered by software inventory tools
- M5 = Count of Input 2

Metrics

- If M5 is 0 or unavailable, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Inventory Tool Coverage

Metric	The percentage of endpoints covered by software inventory tools to the total number of applicable endpoints
Calculation	:code:`M3 / M1`

2.5: Allowlist Authorized Software

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 2.3: Address Unauthorized Software
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV7`: Software capable assets
2. `GV5`: Authorized software inventory
3. `GV3`: Approved configuration Standards
4. Date of last assessment of this safeguard

Operations

1. Using `GV7` identify and enumerate assets capable of supporting allowlisting software (some assets may not enable third-party software installation or otherwise have constrained environments precluding the use of allowlisting software) (M1).

2. Using `GV5`, identify all authorized allowlisting software within the enterprise (`GV8`)

3. Using the output from Operation 1 and authorized allowlisting software `GV8`:

    1. Identify and enumerate allowlisting capable assets with allowlisting software installed (M2)
    2. Identify and enumerate allowlisting capable assets without allowlisting software installed (M3)

4. Use `GV3` to identify allowlisting software configurations (`GV9`)

5. For each asset with allowlisting software installed (M2) from Operation 2, use the output from Operation 3 to:

    1. Identify and enumerate properly configured software (M4)
    2. Identify and enumerate improperly configured software (M5)

6. Compare Input 4 to the current date and note the timeframe in months (M6)

Measures

- M1 = Count of enterprise assets capable of supporting allowlisting software
- M2 = Count of enterprise assets capable of supporting allowlisting software and have the software installed
- M3 = Count of enterprise assets capable of supporting allowlisting software and do not have the software installed
- M4 = Count of enterprise assets with allowlisting software that is properly configured
- M5 = Count of enterprise assets with allowlisting software that is properly configured
- M6 = Timeframe since the last assessment of this safeguard

Metrics

- If M6 is greater than six months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Allow listing Installation Coverage

Metric	**The percentage of enterprise assets capable of supporting allowlisting with allowlisting installed**
Calculation	`M2 / M1`

Allowlisting Configuration Coverage

Metric	**The percentage of enterprise assets with properly configured allowlisting installed**
Calculation	`M4 / M2`

2.6: Allowlist Authorized Libraries

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Protect	2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 2.5: Allowlist Authorized Software
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Inputs

1. `GV8`: Authorized allowlisting software
2. The list of authorized software libraries
3. `GV9`: Approved configuration (s) for allowlisting software
4. Date of the last assessement of this safeguard

Operations

1. For each item identified in `GV8, use the approved configurations from code: GV9` and authorized library list from Input 2:

    1. Identify and enumerate allowlisting software properly configured to allow process loading of authorized libraries (M2)
    2. Identify and enumerate allowlisting software improperly configured to allow process loading of authorized libraries (M3)

2. Compare the date from Input 4 to the current date and note the timeframe in months (M4).

Measures

- M1 = Count :code:`GV8
- M2 = Count of properly configured allowlisting software
- M3 = Count of improperly configured allowlisting software
- M4 = Timeframe since the last assessment of this safeguard

Metrics

- If M4 is greater than six months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	**The percentage of appropriately configured allowlisting software instances within the enterprise.**
Calculation	`M2 / M1`

2.7: Allowlist Authorized Scripts

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Software	Protect	3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV5`: Authorized allowlisting software
2. The list of authorized scripts
3. `GV3`: Approved configuration Standards
4. Date of last assessement of this safeguard

Operations

1. Use `GV5` to identify and enumerate all enterprise authorized software capable of executing scripts, including allowlisting software, email client applications, and web client applications (M1)

2. Use `GV3` to identify approved configurations for all software identified in Operation 1

3. For each item identified in Operation 1, use the approved configurations from Operation 2:

    1. Identify and enumerate software properly configured to allow execution of authorized and signed scripts from Input 2 (M2)
    2. Identify and enumerate software improperly configured to allow execution of authorized and signed scripts from Input 2 (M3)

4. Compare the date from Input 4 to the current date and note the timeframe in months (M4).

Measures

- M1 = Count of authorized software capable of executing scripts

- M2 = Count of properly configured software
- M3 = Count of improperly configured software
- M4 = Timeframe since the last assessment of this safeguard

Metrics

- If M4 is greater than six months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	**The percentage of appropriately configured allowlisting software instances within the enterprise.**
Calculation	`M2 / M1`