CIS Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this CIS Control Critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to enterprises' networks. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web or email-based malware; and adversaries can leverage weak security configurations for traversing the network, once they are inside.

Additional assets that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks, etc.) should be identified and/or isolated, in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex, dynamic enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" our enterprise assets at very large scale in order to support their opportunities.

Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines can be difficult to track in asset inventories when they are shut down or paused. Another benefit of complete enterprise asset management is supporting incident response. Both when investigating the origination of network traffic from an asset on the network, and to be able to identify all potentially vulnerable, or impacted, assets of similar type or location during an incident.

1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud

environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

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

Dependencies

- None

Inputs

1. `GV1`: Detailed Enterprise Asset Inventory - The enterprise's list of current approved inventory to include all assets as outlined in the safeguard. This list is a mix of manual and tool-generated endpoints that includes information such as authorized, non-authorized, IP address, device type, and any other information as defined by the enterprise.

2. Aggregate Enterprise Asset Inventory - The enterprise's list of all devices detected, manually or through automated scans, since the last update to `GV1`.

3. Date of last update to the Detailed Enterprise Asset Inventory

Assumptions

1. Devices belonging to the organization, but not connected to the organization's network, require manual discovery in order to be included in the aggregate inventory.

Operations

1. Calculate the intersection of `GV1` and Input 2

    1. Enumerate items in `GV1` that are not in Input 2 (M4)
    2. Enumerate items in Input 2 not in Input 1 (`GV2`: M5). These assets are considered unauthorized.

2. Check items in Input 1 for complete or missing detailed information

    1. Enumerate items that have complete information (M6)
    2. Enumerate items that do not have complete information or missing information (M7).

3. Calculate the time (in months) since the last update to Input 1 by using the current date and Input 4 (M8).

Measures

- M1 = `GV1`
- M2 = Count of items in Input 2

- M3 = Count of items in the intersection of `GV1` and Input 2
- M4 = Count of items in `GV1` not found in Input 2
- M5 = `GV2`
- M6 = Count of items in `GV1` that contain all necessary detailed information
- M7 = Count of items in `GV1` that do not contain detailed information
- M8 = Months since the last update to `GV1`

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 M8 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 aggregate endpoint inventory is accounted for in the current enterprise asset inventory?**
Calculation	`M3 / M2`

Completeness Score

Metric	**What percentage of the current enterprise asset inventory contains necessary detailed information?**
Calculation	`M8 / M1`

Procedural Review

Manual review/rating of the inventory procedures, to include adding and removing assets, and the time allowable or expected, after the acquisition or disposal of assets.

1.2: Address Unauthorized Assets

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

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

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. GV1: Detailed Enterprise Asset Inventory
2. GV2: Unauthorized Assets
3. The enterprise-defined time frame for removing unauthorized assets (weekly or more often).

Assumptions

1. If the item is not reachable, it may be reasonable to assume it has been removed from the network and, therefore, dealt with.

Operations

If the optional disposition list is provided, the checks would be tailored to those dispositions. For the following, assume no disposition list is available:

1. At the time frame specified by Input 3, for each unauthorized asset in GV2, check to see if the asset is present in the updated asset inventory from GV1.

2. For those items in GV2 that are not in GV1, scan the network to determine if the item is still reachable on the network.

    1. Enumerate the items from GV2 that are unreachable (M4)
    2. Enumerate the items from GV1 that are unreachable (M5)

Measures

- M1 = GV1
- M2 = Count of GV2
- M3 = Timeframe in days for Input 3
- M4 = Count of items from GV2 that are unreachable after scan
- M5 = Count of items from GV1 that are unreachable after scan

Metrics

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

Coverage

Metric	**The ratio of unaccounted for, unauthorized assets, to the total assets in the asset inventory.**
Calculation	If the value of M4 is 0, there are no unauthorized assets that remain unaccounted for. In this case, the value of the metric is 1. Otherwise, the value is `(M2 - M4) / M2`.

1.3: Utilize an Active Discovery Tool

Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. The list of active discovery tool(s) used by the enterprise
3. List consisting of the union from scan results conducted using all active asset discovery tool(s) within the enterprise (discovered assets).
4. Timeframe between two active asset discovery tool scans.
5. `GV3`: Configuration Standard

Assumptions

1. The asset discovery tools on the provided list are active asset discovery tools, as opposed to passive asset discovery tools (verification of this is not performed during the following operations).

Operations

1. Identify enterprise assets not discovered by the active discovery tools by comparing Input 1 and Input 3 (M2).

2. Identify the configurations for active asset discovery tools that interface with `GV1` by using `GV3`

3. Using the configuration information in `GV3`, check the approved configurations to verify that the tools are capable of interfacing with the asset inventory to make automatic updates.

    1. Enumerate those tools that are compliant (M3)
    2. Enumerate those that are not compliant (M4).

Measures

- M1 = Count of all discovered assets from Input 3
- M2 = Count of undiscovered assets
- M3 = Count of properly configured tools
- M4 = Count of improperly configured tools
- M5 = Count of Input 2
- M6 = Count of `GV1`
- M7 = Timeframe in hours for Input 4

Metrics

- If M7 is greater than 24 hours, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M5 is 0, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Asset Discovery Coverage

Metric	Asset Discovery Coverage
Calculation	`M1 / M6`

Tool Compliance Ratio

Metric	Tool Compliance Ratio
Calculation	`M3 / M2`

1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. List of DHCP servers
2. `GV41`: List of Change Management Database (CMDB) servers

Assumptions

1. CMDB servers are configured to pull from DHCP logs

Operations

1. For each DHCP server, enumerate those where DHCP logging is enabled (M2)
2. For each CMDB server, enumerate those where DHCP logs are used to update IP addresses (M4)

Measures

- M1 = Count of Input 1
- M2 = Count of DHCP servers with logging enabled
- M3 = Count of Input 2 `GV41`
- M4 = Count of CMDB servers configured to use DHCP logs to update IP addresses
- M5 = Count of devices in the DHCP server logs that are not included in the CMDB servers
- M6 = Count of devices in the DHCP server logs that are included in the CMDB servers

Metrics

- M4 > 0 indicates a non up-to-date asset inventory

DHCP Logging Quality

Metric	**Ratio of appropriately configured DHCP logging enabled to known DHCP servers**
Calculation	`M2 / M1`

CMDB Configuration Quality

Metric	**Ratio of appropriately configured CMDB servers using DHCP logging to update IP addresses**
Calculation	`M4 / M3`

1.5: Use a Passive Asset Discovery Tool

Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

Asset Type	**Security Function**	**Implementation Groups**
Devices	Detect	3

Dependencies

- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Inputs

1. `GV4`: Enterprise network architecture documentation
2. List of passive asset discovery tools in use by the organization. For each, include the location of the tool's configuration information and which networks it covers.
3. `GV3`: Approved configuration(s) for each passive asset discovery tool. Configurations should include the settings necessary for the tool to be able to update the enterprise's asset inventory

Operations

1. Identify approved configurations for passive asset discovery tools using `GV3`

2. For each passive asset discovery tool provided in Input 2, check the tool's configuration against the appropriate approved configuration from `GV3`

    1. Enumerate those tools that are properly configured (M1)
    2. Enumerate those tools that are improperly configured (M2) noting the deviations from proper configuration

3. Identify and enumerate the enterprise's networks (M5) using Input 1, check to see if at least one properly configured passive asset discovery tool from M1 covers that network.

    1. Create a list of the enterprise's networks that have coverage from at least one properly configured passive asset discovery tool (M3)
    2. Create a list of the enterprise's networks that do not have coverage from any properly configured passive asset discovery tools (M4)

Measures

- M1 = Count of properly configured passive asset discovery tools
- M2 = Count of improperly configured passive asset discovery tools
- M3 = Count of organization's networks that are covered by properly configured passive discovery tools
- M4 = Count of organization's networks that are not covered by properly configured passive discovery tools
- M5 = Count of enterprise's networks.

Metrics

Coverage

Metric	**The ratio of the organization's networks with coverage from at least one properly configured passive asset discovery tool to the total number of networks**
Calculation	`M3 / M5`