CIS Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts to enterprise assets and software.

Why is this CIS Control Critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including weak passwords account still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an an online account that has been compromised (in a public password dump), social engineering a user to give their password or using malware to capture passwords or tokens in memory or over the network.

Administrative or highly privileged accounts are a particular target, because they allow attackers to add other accounts or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in CIS Control 8 (Audit Log Management) is important in the development of a comprehensive Identity and Access Management (IAM) program.

5.1: Establish and Maintain an Inventory of Accounts

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

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

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV5`: Authorized software inventory
2. `GV22`: Inventory of accounts
3. Date of last review of the inventory of accounts

Operations

1. Check if the enterprise maintains an inventory of user and administrative accounts (Input 2):

    1. If the inventory exists, M1 = 1
    2. If the inventory does not exist, M1 = 0

2. Using the inventory of accounts `GV22`, determine if the inventory captures the following elements: person's name, username, start/stop dates, and department:

    1. Each element is assigned a value of 1 if it exists and 0 if it does not. Total the number of elements that exist (M3).

3. Using `GV22`, check each account for elements: person's name, username, start/stop dates, and department:

    1. Identify and enumerate accounts with all elements (M4)
    2. Identify and enumerate accounts missing or with incomplete elements (M5)

4. Use `GV5` to identify authentication systems or other software that manages accounts `GV23`.

5. Using the output of Operation 4, enumerate all current user and administrative accounts throughout the enterprise (M6)

6. Compare the output of Operation 5 with `GV22`:

    1. Identify and enumerate accounts that are supposed to be active/enabled (M7)
    2. Identify and enumerate accounts that are supposed to be disabled/removed (M8)

7. Compare the current date to the date provided in Input 3 and enumerate the timeframe in months (M9)

Measures

- M1 = Does the account inventory exist (Output of Operation 1)
- M2 = Count of accounts in `GV22`
- M3 = Count of elements provided in the inventory
- M4 = Count of accounts in inventory with complete information
- M5 = Count of accounts in inventory with missing or incomplete information
- M6 = Count of current accounts identified through Operation 5
- M7 = Count of authorized accounts
- M8 = Count of unauthorized accounts
- M9 = Timeframe of the last update in months

Metrics

- If M1 is 0, this Safeguard receives a failing score, and other metrics don't apply.
- If M9 is greater than three, this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	**The percentage of minimum elements included in the inventory.**
Calculation	`M3 / 4`

Metric	**The percentage of accounts with complete information.**
Calculation	`M4 / 2`

Accuracy of Inventory

Metric	**The percentage of accurately listed accounts in the inventory.**
Calculation	`M8 / M6`

5.2: Use Unique Passwords

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

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

Dependencies

- None

Inputs

1. `GV20`: Unique password policy for the enterprise

Operations

1. Check if the enterprise has a unique password policy:
2. If the policy is available, M1 = 1
3. Otherwise M1 = 0
4. Review the policy and determine whether it includes password guidance for accounts without MFA:
5. If guidance is included, M2 = 1
    1. Does guidance, at a minimum, require a fourteen-character password:

1. If password guidance is fourteen characters or longer, M3 = 1
2. Otherwise M3 = 0

6. Otherwise M2 = 0

7. Review the policy and determine whether it includes password guidance for accounts with MFA:

8. If guidance is included, M4 = 1

    1. Does guidance, at a minimum, require an eight-character password:

    2. If password guidance is eight characters or longer, M5 = 1
    3. Otherwise M5 = 0

9. Otherwise M4 = 0

Measures

- M1 = Does a password policy exist?
- M2 = Does guidance exist for accounts without MFA?
- M3 = Does guidance for accounts without MFA meet minimum guidance?
- M4 = Does guidance exist for accounts with MFA?
- M5 = Does guidance for accounts with MFA meet minimum guidance?

Metrics

- If M1 is 0, the Safeguard receives a failing score. Other metrics don't apply.

Completeness of Password Policy

Metric	**The percentage of completeness of the unique password policy**
Calculation	`(M2 + M4) / 2`

Strength of Policy

Metric	**The percentage of password guidance that meets minimum character length standards**
Calculation	`(M3 + M5) / 2`

5.3: Disable Dormant Accounts

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

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

Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Inputs

1. `GV22`: Inventory of accounts
2. Enterprise-defined policy for dormant threshold

Assumptions

- The list of accounts for the enterprise includes OS-level, database, internal and external application accounts.
- A query interface is assumed to enable the collection of a “last activity” timestamp, such as the last login, as well as a status indicating if the account is enabled or disabled.

Operations

1. Review Input 2 and note the dormant threshold in terms of days (M2).

2. For each account in `GV22`, query the interface and collect:

    1. The date of the last activity for each account.
    2. Whether the account is disabled or not.

3. Using the output of Operation 2.1 and Input 2:

    1. Identify and enumerate accounts that have exceeded the dormant threshold (M3).
    2. Identify and enumerate accounts that are still within the dormant threshold (M4).

4. Use the output of Operation 2.2 and 3.1 (M3):

    1. Identify and enumerate accounts that are disabled (M5).
    2. Identify and enumerate accounts that are still enabled (M6).

Measures

- M1 = Count of accounts in `GV22`
- M2 = Timeframe of dormant threshold in days
- M3 = Count of dormant accounts
- M4 = Count of active accounts
- M5 = Count of dormant accounts that have been disabled
- M6 = Count of dormant accounts still enabled

Metrics

Dormant Accounts

Metric	**The percentage of dormant accounts still included in the inventory.**
Calculation	`M6 / M1`

Enabled Dormant Accounts

Metric	**The percentage of dormant accounts still enabled.**
Calculation	`M6 / M3`

5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

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

Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Inputs

1. `GV22`: Inventory of accounts
2. List of users identified as administrators

Assumptions

- For the purpose of this control, it is assumed that users identified as administrators that have active administrative and non-administrative accounts have properly dedicated accounts for administrative privileges.

Operations

1. Using `GV22` and Input 2:

1. Identify and enumerate users identified as administrators with active administrator accounts (M1).
2. Identify and enumerate users identified as administrators without active administrator accounts (M2).
3. Identify and enumerate users not identified as administrators with active administrator accounts (M3).

2. Using `GV22` and the output of Operation 1.1:

    1. Identify and enumerate users identified as administrators that have an active non-administrative user account (M4).
    2. Identify and enumerate users identified as administrators that do not have an active non-administrative user account (M5).

Measures

- M1 = Count of authorized administrative users with active administrator accounts
- M2 = Count of authorized administrative users without active administrator accounts
- M3 = Count of non-administrative users with active administrator accounts
- M4 = Count of authorized administrative users with an active administrative and non-administrative account
- M5 = Count of authorized administrative users without an active administrative and non-administrative account
- M6 = Count of Input 2

Metrics

Administrative User Accounts

Metric	**The percentage of administrative users with both an administrative account and a non-administrative account.**
Calculation	`M4 / M6`

Unauthorized Administrative Accounts

Metric	**The percentage of unauthorized administrative accounts.**
Calculation	`M3 / (M1 + M3)`

5.5: Establish and Maintain an Inventory of Service Accounts

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain the department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized on a recurring schedule at a minimum quarterly, or more frequently.

Asset Type	Security Function	Implementation Groups
Users	Identify	2, 3

Dependencies

- Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Inputs

1. `GV23`: Authentication and Authorization System Inventory
2. Inventory of service accounts
3. Date of last review of the inventory of service accounts

Operations

1. Check if the enterprise maintains an inventory of service accounts (Input 2):
    1. If the inventory exists, set M1 = 1.
    2. If the inventory does not exist, set M1 = 0.
2. Using the inventory of accounts (Input 2), determine if the inventory captures the following elements: department owner, review date, and purpose:
    1. Each element is assigned a value of 1 if it exists and 0 if it does not. Total the number of elements that exist (M3).
3. Using Input 2, check each account for elements: department owner, review date, and purpose:
    1. Identify and enumerate accounts with all elements (M4).
    2. Identify and enumerate accounts missing or with incomplete elements (M5).
4. Use `GV23` to identify authentication systems or other software that manages service accounts.
5. Using the output of Operation 4, enumerate all current service accounts throughout the enterprise (M6).
6. Compare the output of Operation 5 with Input 2:
    1. Identify and enumerate accounts that are supposed to be active/enabled (M7).
    2. Identify and enumerate accounts that are supposed to be disabled/removed (M8).
7. Compare the current date to the date provided in Input 3 and enumerate the timeframe in months (M9).

Measures

- M1 = Does the account inventory exist (Output of Operation 1)

- M2 = Count of accounts in Input 2
- M3 = Count of elements provided in inventory
- M4 = Count of accounts in inventory with complete information
- M5 = Count of accounts in inventory with missing or incomplete information
- M6 = Count of current service accounts identified through Operation 5
- M7 = Count of authorized accounts
- M8 = Count of unauthorized accounts
- M9 = Timeframe of last update in months

Metrics

- If M1 is 0, this Safeguard receives a failing score and other metrics don't apply.
- If M9 is greater than three, this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	**The percentage of minimum elements included in the inventory.**
Calculation	`M3 / 4`

Metric	**The percentage of accounts with complete information.**
Calculation	`M4 / 2`

Accuracy of Inventory

Metric	**The percentage of accurately listed accounts in the inventory.**
Calculation	`M8 / M6`

5.6: Centralize Account Management

Centralize account management through a directory or identity service.

Asset Type	Security Function	Implementation Groups
Users	Govern	2, 3

Dependencies

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

Inputs

1. `GV1`: Enterprise asset inventory

Operations

1. Using `GV1` identify and enumerate centralized authentication points (M1)

2. For each centralized authentication point identified in Operation 1, determine whether it is necessary or can be consolidated:

    1. Identify and enumerate authentication points that are unnecessary or can be consolidated (M2)
    2. Identify and enumerate authentication points that are necessary and cannot be consolidated (M3)

Measures

- M1 = Count of centralized authentication points in the enterprise
- M2 = Count of unnecessary centralized authentication points
- M3 = Count of necessary centralized authentication points

Metrics

Coverage

Metric	**Percentage of properly centralized authentication points.**
Calculation	`M3 / M1`