Step 8. Behavior analysis

Step 8. Behavior analysis

Introduction

Using PAM you can configure **policies and rules** in the Soffid console to detect actions or behaviors that may put your organization at risk. With this information, you will be able to analyze the behavior of the critical accounts that you have defined in your systems and configure what actions you want to run in each case.

Once you create the PAM policy, you must assign it to the proper folder on the password vault.

Step 8.1. PAM Rules

Step-by-step

1. To create a new PAM Rule, you must access the PAM Rules page in the following path:

   `Main Menu > Administration > Configure Soffid > Security settings > PAM rules`

2. To add a new PAM rule, you must click the add button (+) and Soffid will display a new window to fill in the data.

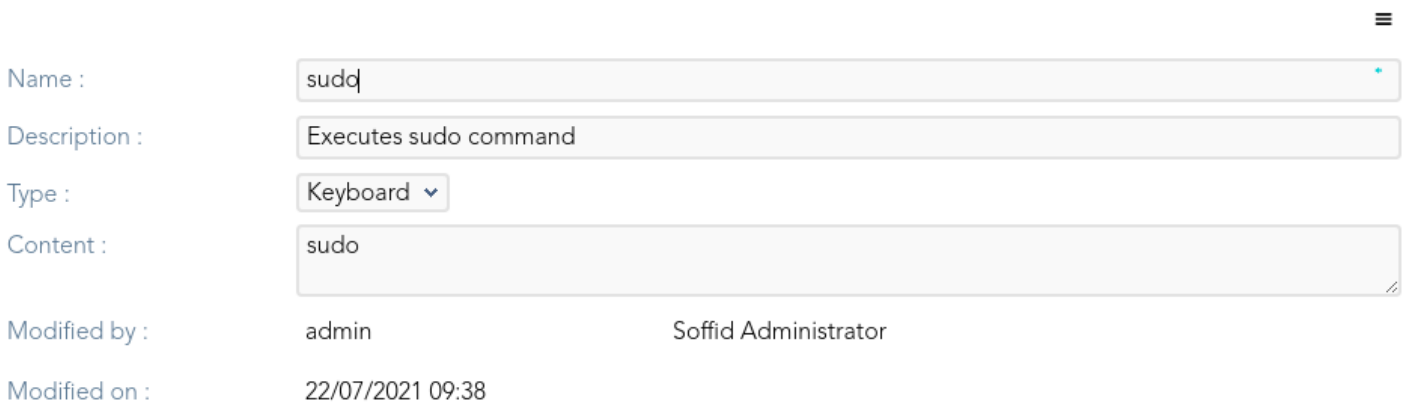
- The **Name** should be an identificative and unique rule name. That field will be mandatory.
- The **Description** should be a brief description of the rule.
- The **Type** allows you to select the rule will be a keyboard or a screen rule. That field will be mandatory.
- The **Content** should be what the rule will detect. For instance, a Linux command like *sudo* or *rm *-r*. That field will be mandatory.

3. Then you need to click on the "Apply changes" button to save the new PAM rule.

   3.1. If you click on the "Undo" button, no updates will be saved.

4. Finally you can create a PAM policy to apply the rules.

Screen overview



Step 8.2. PAM Policies

Step-by-step

1. To create a new PAM Policy, you must access the PAM Rules page in the following path:

   `Main Menu > Administration > Configure Soffid > Security settings > PAM policies`

2. To create a new PAM policy, you must click the add button (+) and Soffid will display a new window to fill in the data.

- The **Name** should be an identificative and unique policy name. That field will be mandatory.
- The **Description** should be a brief description of the rule.
- The **Rules list**: show a list of the PAM rules defined. You can check/uncheck the available options. You can choose zero, one, or several options:
  - **Close session**: if you select this option when the rule is met, Soffid will close the session opened.
  - **Lock account**: if you select this option when the rule is met, Soffid will lock the account.
  - **Open issue**: if you select this option when the rule is met, Soffid will open an issue in the ticketing system.
  - **Notify**: if you select this option when the rule is met, Soffid will send a notification about the action.

3. Then you need to click on the "Apply changes" button to save the new PAM policy.

   3.1. If you click on the "Undo" button, no updates will be saved.

4. Finally you can assign the PAM policy to the proper Password vault folder.

Screen overview

Name : default *

Description : Default Policy

Modified by : pgarcia Patricia García

Modified on : 3/6/2023 12:04

Rule	Close se…	Lock acc…	Open is…	Notify
cd .. (tenant)	☑	☐	☐	☑
Drop table	☑	☐	☐	☑
ipconfig	☑	☐	☐	☑
ls	☐	☐	☐	☐

Step 8.3. Assign PAM policy

Assign PAM policy

1. To assign the PAM policy to a Password Vault folder, you must access the Password vault page in the following path:

   `Main Menu > Administration > Resources > Password vault`

2. Then you must select the folder by clicking on the record. Soffid will display a window with the folder data.

3. You can select the password policy selecting it on the drop-down list.

4. Finally you need to click on the "Apply changes" button to save the password policy,

   4.1. If you click on the "Undo" button, no updates will be saved.

Screen overview