ESET Tech Center

How do I create a HIPS rule and enforce it on a client workstation? (5.x)

Ondersteuning | ESET Nederland - 2024-08-28 - Reacties (0) - 5.x

https://support.eset.com/kb3573

Solution

Advanced users only!

By default, the Host-based Intrusion Prevention System (HIPS) is pre-configured to ensure maximum protection of your system. While the creation of a HIPS rule may be needed to resolve an issue in certain infrequent cases, the manipulation of HIPS rules requires advanced knowledge of applications and operating systems and, as such, is not recommended.

Create a HIPS rule from the ESET Remote Administrator Console

If you do not use ESET Remote Administrator to manage your network

Perform these steps on individual client workstations.

1. Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.

2. Click **Tools → Policy Manager**.

3. Select the policy you want to edit and click **Edit Policy**.

Figure 1-1

Click the image to view larger in new window

4. Expand **Windows desktop v5 → HIPS → Settings**, click **Rules and advanced options** and then click **Edit**.

Figure 1-2

Click the image to view larger in new window

5. Click **New**.

Figure 1-3

Click the image to view larger in new window

6. Configure your rule. In the following example, we will demonstrate how to restrict unwanted behavior of certain applications:

    a. Name the rule and select **Block** from the **Action** drop-down menu.

    b. Click the **Target applications** tab (leave the **Source applications** tab blank to apply your new rule to all applications).

    c. Select the check box next to **Modify state of another application** and then click **Add**.

Figure 1-4

Click the image to view larger in new window

    d. Type the path of the application you want to apply this rule to into the **Value** field, or click **Select file** or **Select folder** to navigate to the application and exclude it that way. When you are finished, click **OK**.

Figure 1-5

Click the image to view larger in new window

    e. Select the check box next to **Notify user** to display a user

notification whenever the rule is applied. When you are finished making changes, click **OK** → **OK** to save this rule.

Figure 1-6

Click the image to view larger in new window

Information about important HIPS operations

Source applications tab: Rules set here will only be used if the event is triggered on the source machine by the application(s) added to this list.

Target files tab:

Delete file: An application on the source machine is asking for permission to delete the target file.
Write to file: An application on the source machine is asking for permission to write to the target file.
Direct access to disk: An application on the sourche machine is trying to read from or write to the disk in a non-standard way, one that will circumvent common Windows files being modified without the application of corresponding rules. This operation may be caused by malware that is trying to evade detection, backup software trying to make an exact copy of a disk, or a partition manager trying to reorganize disk volumes.
Install global hook: Refers to calling the *SetWindowsHookEx* function from the MSDN library.
Load driver: Installation and loading of drivers onto the system on the source machine.

Target applications tab:

Debugging another application: Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified, and its data can be accessed.
Intercept events from another application: The source application is attempting to catch events targeted to a specific application (for example, a

keylogger trying to capture browser events).
Terminate/suspend another application: Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes pane).
Start new application: Starting of new applications or processes.
Modify state of another application: The source application is attempting to write to the target application's memory, or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

Target registry tab:

Modify startup settings: Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for "Run key" in the Windows Registry.
Delete from registry: Deleting a registry key or its value on the source machine.
Rename registry key: Renaming registry keys on the source machine.
Modify registry: Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or or group rights for registry keys on the source machine.

7. Click **Console** → **Yes** to save your changes. Click **OK** to exit Policy Manager. Changes will take effect after the Windows operating system is restarted.

- How do initiate a remote reboot of a client workstation?

Create a HIPS rule on individual client workstations

1. Open ESET Endpoint Security or ESET Endpoint Antivirus. How do I open my ESET product?

2. Press **F5** to access Advanced setup.

3. Expand Computer, click **HIPS** → **Configure rules**.

Figure 2-1

Click the image to view larger in new window

4. Click **New**.

Figure 2-2

Click the image to view larger in new window

5. Configure your rule. In the following example, we will demonstrate how to restrict unwanted behavior of applications:

    a. Name the rule and select **Block** from the **Action** drop-down menu.

    b. Click the **Target applications** tab (leave the **Source applications** tab blank to apply your new rule to all applications).

    c. Select the check box next to **Modify state of another application** and then click **Add**.

Figure 2-3

Click the image to view larger in new window

    d. Type the path of the application you want to apply this rule to into the **Value** field, or click **Select file** or **Select folder** to navigate to the application and exclude it that way. When you are finished, click **OK**.

Figure 2-4

    e. Select the check box next to **Notify user** to display a user notification whenever the rule is applied. When you are finished making changes, click **OK** → **OK** to save this rule.

Figure 2-5

Click the image to view larger in new window

Information about important HIPS operations

Source applications tab: Rules set here will only be used if the event is triggered on the source machine by the application(s) added to this list.

Target files tab:

Delete file: An application on the source machine is asking for permission to delete the target file.
Write to file: An application on the source machine is asking for permission to write to the target file.
Direct access to disk: An application on the sourche machine is trying to read from or write to the disk in a non-standard way, one that will circumvent common Windows files being modified without the application of corresponding rules. This operation may be caused by malware that is trying to evade detection, backup software trying to make an exact copy of a disk, or a partition manager trying to reorganize disk volumes.
Install global hook: Refers to calling the *SetWindowsHookEx* function from the MSDN library.
Load driver: Installation and loading of drivers onto the system on the source machine.

Target applications tab:

Debugging another application: Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified, and its data can be accessed.
Intercept events from another application: The source application is attempting to catch events targeted to a specific application (for example, a keylogger trying to capture browser events).
Terminate/suspend another application: Suspending, resuming or terminating a process (can be accessed directly from Process Explorer

or the Processes pane).
Start new application: Starting of new applications or processes.
Modify state of another application: The source application is attempting to write to the target application's memory, or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

Target registry tab:

Modify startup settings: Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for "Run key" in the Windows Registry.
Delete from registry: Deleting a registry key or its value on the source machine.
Rename registry key: Renaming registry keys on the source machine.
Modify registry: Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or or group rights for registry keys on the source machine.

6. Click **OK** to save your changes and exit Advanced setup. Changes will take effect after the Windows operating system is restarted.

Related articles:

[Create a HIPS rule and enforce it on a client workstation (6.x)]

Tags
ERA 5.x
HIPS