Ransomware Shield - enable Audit mode and exclude an application from detection (7.x)

Anish | ESET Nederland - 2019-12-30 - Reacties (0) - 7.x

Issue

ESET business products (version 7 and later) include **Ransomware Shield**. This new security feature is a part of HIPS and protects computers from ransomware. When ransomware is detected on a client computer, you can view the detection details in ESMC Web Console in **Threats**.

By default, Ransomware Shield blocks all applications with potential ransomware behavior. If there is a legitimate application or script automatically running on the managed computer and performing operations that are evaluated as ransomware behavior (moving files across folders, encrypting files and folders), you may want to exclude it from being blocked by ESET business product.

Solution

ESMC Web Console Policy settings for ESET business products include **Audit mode**. When Audit mode is enabled, applications with ransomware behavior are allowed to run and are only logged in ESMC Web Console in **Threats**. The administrator can decide to block the potential detected threat or allow it permanently by adding it to exclusions.

Follow these steps to exclude applications on a managed computer from being detected as ransomware:

1. Open the ESET Security Management Center (ESMC) Web Console.
2. Click **Policies**, select the policy for ESET business product, and then click **Policies → Edit**.

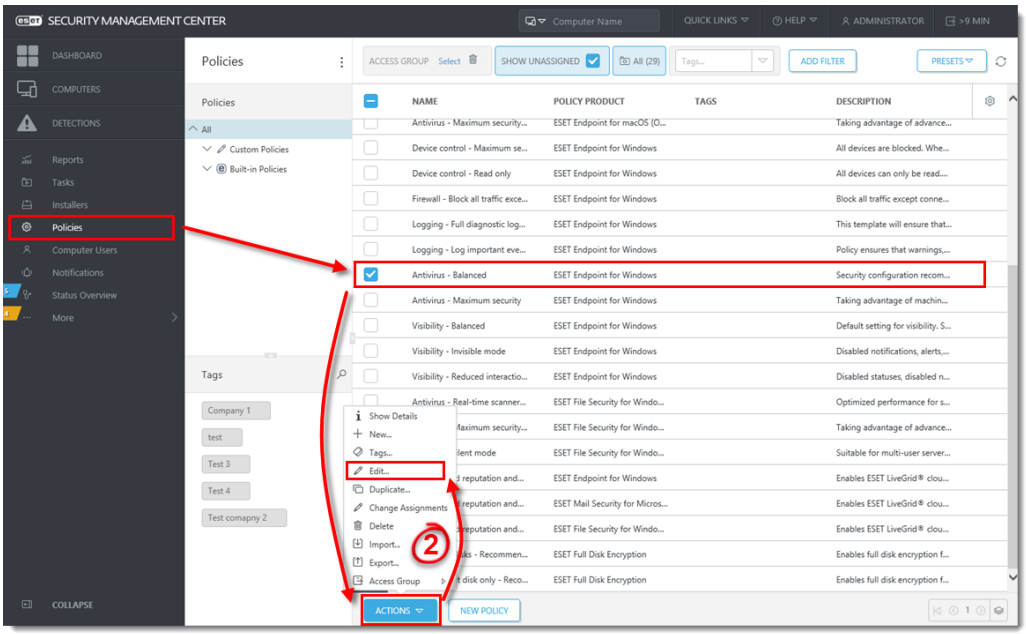


Figure 1-1
Click the image to view larger in new window

3. Click **Settings → Detection Engine → HIPS**.

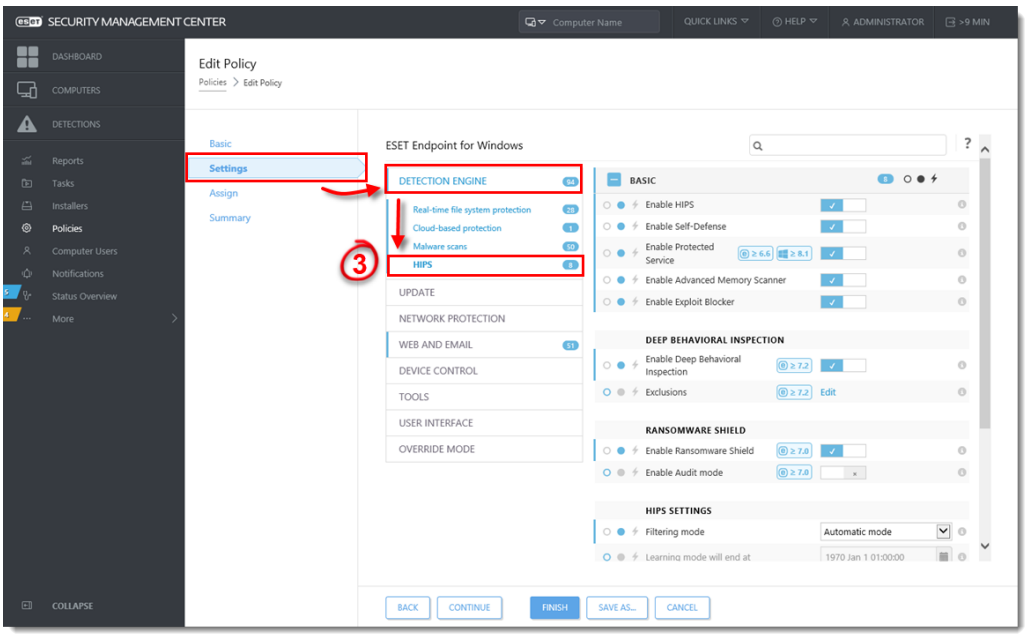


Figure 1-2
Click the image to view larger in new window

4. Click the slider bar next to **Enable Audit mode** to enable this setting and click **Finish** to apply the Policy settings.

Use Enable Audit Mode with care

When you apply **Enable Audit mode**, automatic ransomware protection is turned off and the managed computer is not protected against ransomware.

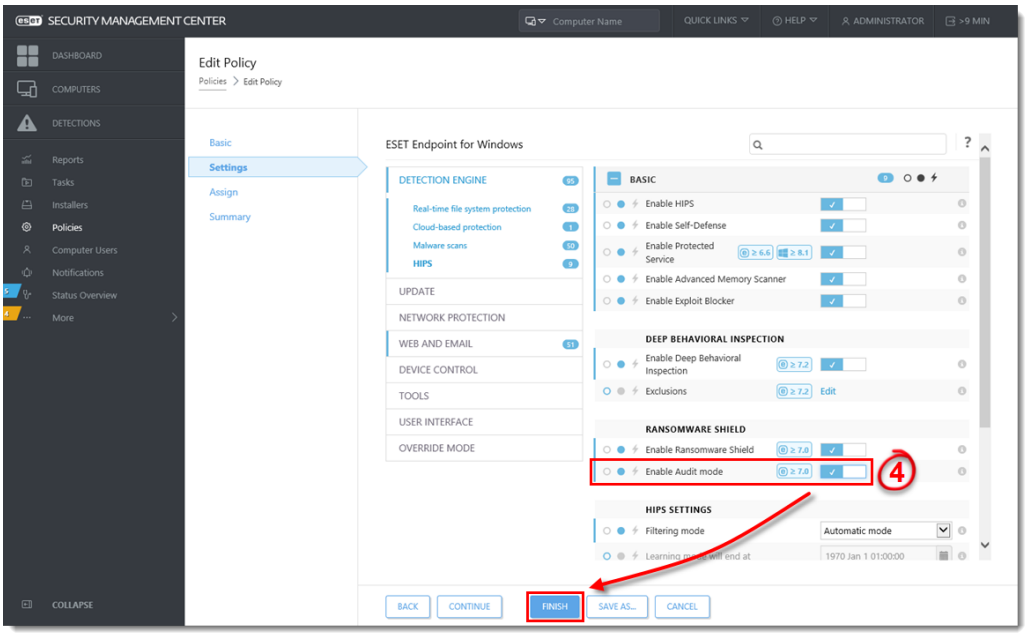


Figure 1-3
Click the image to view larger in new window

5. On the managed computer, run the application with ransomware behavior.

6. Return to ESMC Web Console and click Detections. You can see the information about the potential ransomware application detected on the client computer. In the **Action** column, there is a note **allowed by audit**.

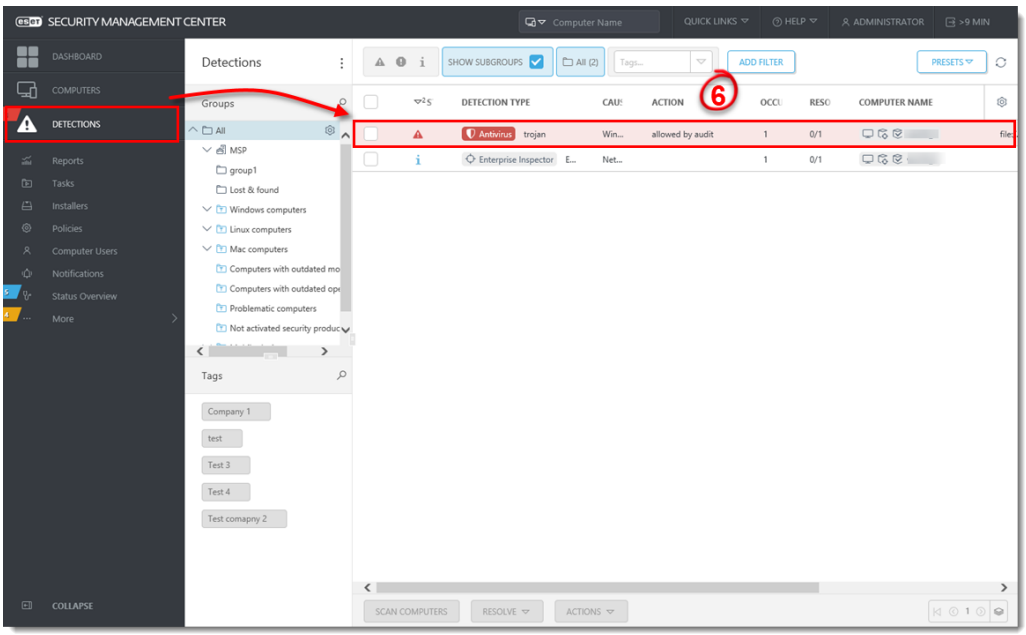


Figure 1-4
Click the image to view larger in new window

7. Click the threat and click **Show Details**. Verify the path to the application in **Object URI** and make sure that you want to exclude the threat from detection. Then click **Close**.

Use Exclusions with caution

Exclusions increase the exposure of managed computer to malware.

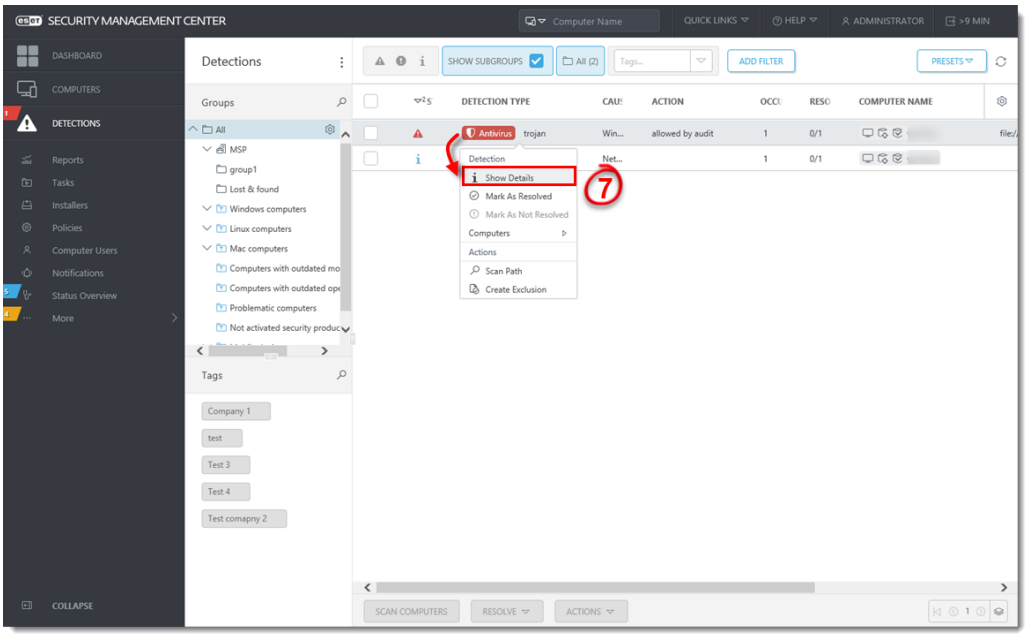


Figure 1-5
Click the image to view larger in new window

8. Click the detection and select **Create exclusion**.

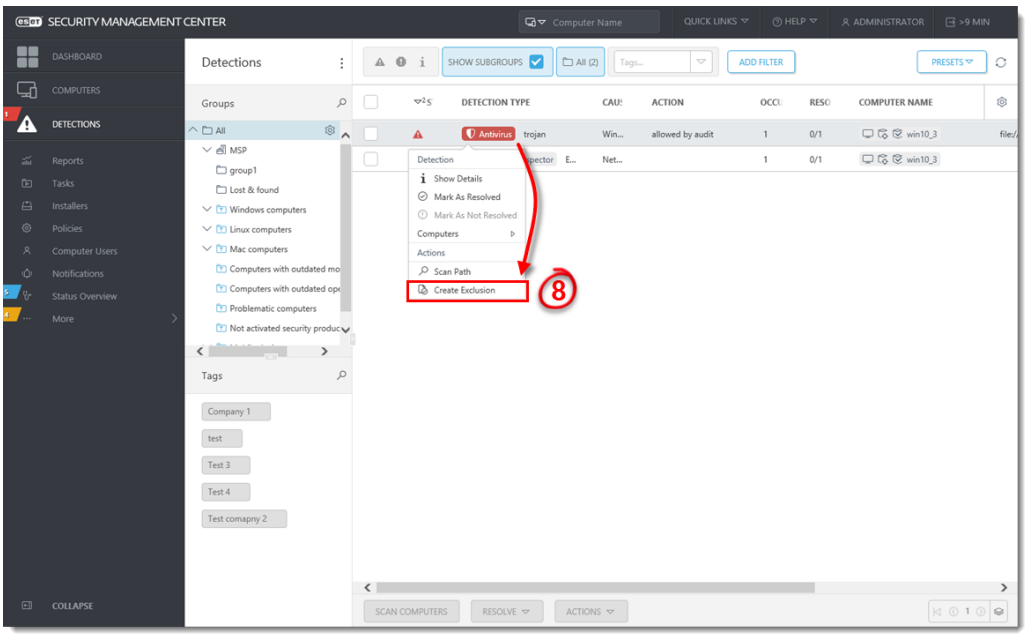


Figure 1-6
Click the image to view larger in new window

9. Select the **Exclusion criteria**. The recommended option is pre-selected based on the detection type. Select the check box **Resolve matching alerts** to automatically resolve the alerts covered by the exclusion. Optionally, you can add a **Comment**.

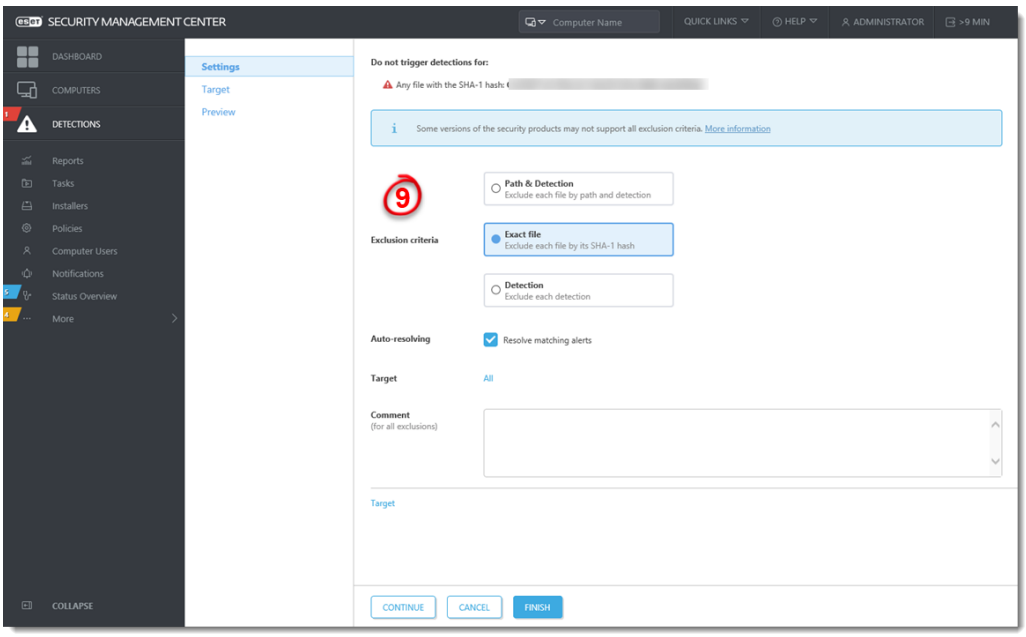
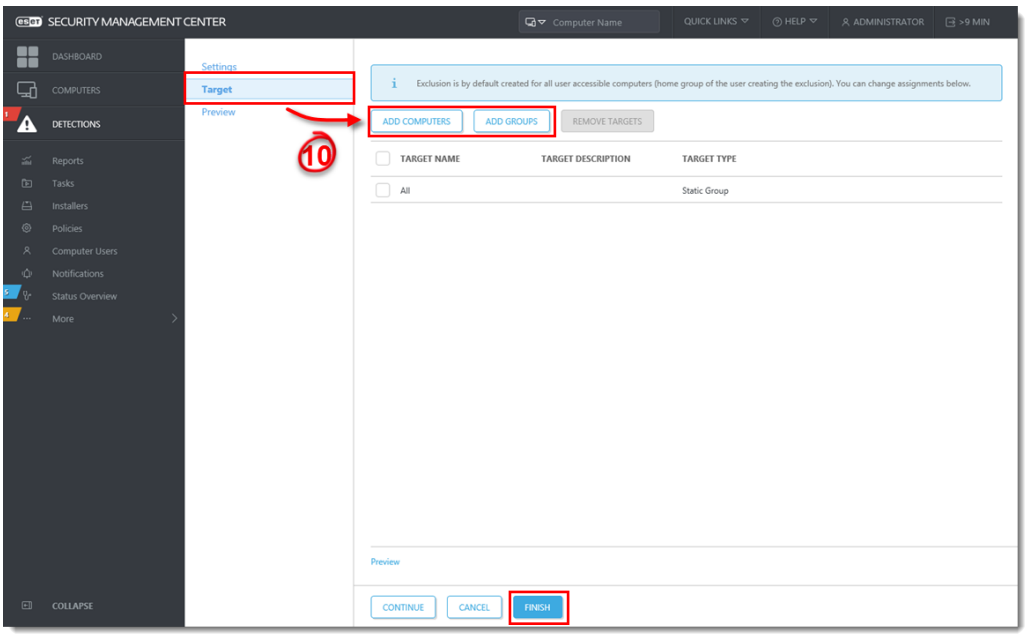


Figure 1-7
Click the image to view larger in new window

10. Click **Target** and select computer(s) or group(s) where the exclusion will be applied and click **Finish**



11. Ransomware Shield no longer detects the excluded application.

12. Edit the Policy for ESET business product and click the slider bar next to **Audit mode** to turn it off and ensure the automatic ransomware protection of the managed computer.

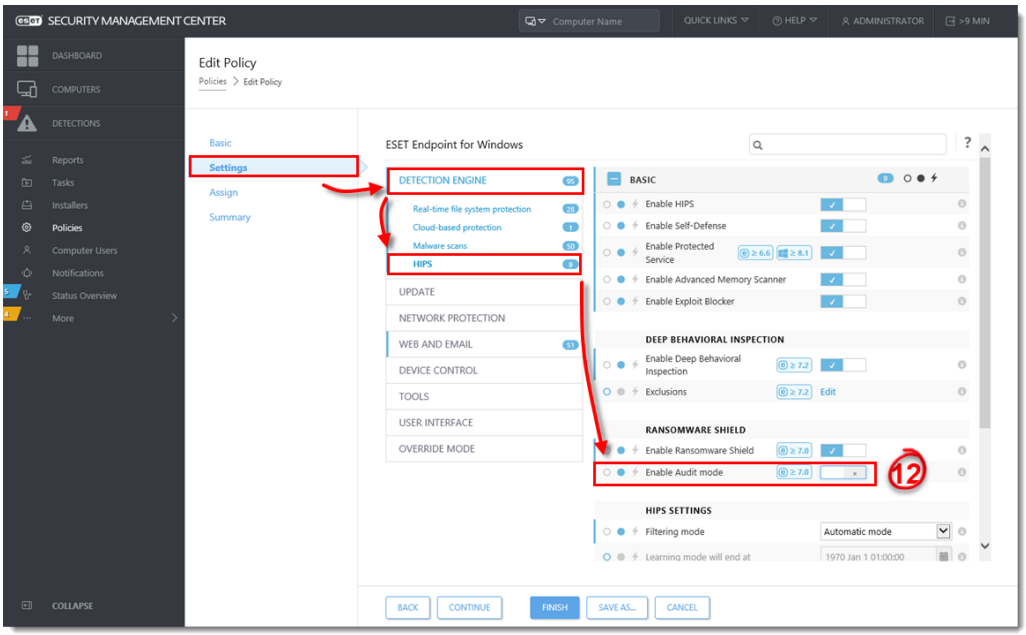


Figure 1-8
Click the image to view larger in new window

Reacties (0)