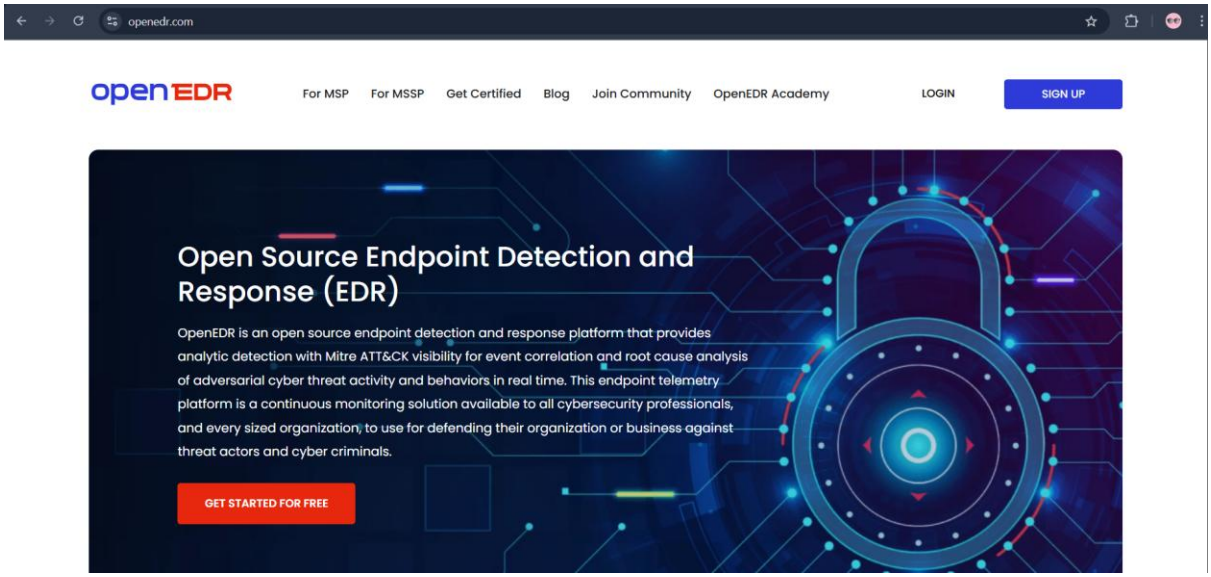
OpenEDR

Task 1: Set up open-source version of Xcitium Cloud Manager

1. Open your browser and enter

2. Select Get Started for Free.

https://openedr.com/



3. Enter your information to create a free account.

4. After creating your account, Xcitium will prompt you to set up multifactor authentication (MFA) using the authenticator app on your mobile device. If you don't have an authenticator app, you can download one from Google Play or the Apple Store.

5. Use the authenticator app to scan the onscreen QR barcode to generate a six-digit verification code. Type or enter this code in the Enter Verification Code field on your browser window, and then select Pair Authenticator.

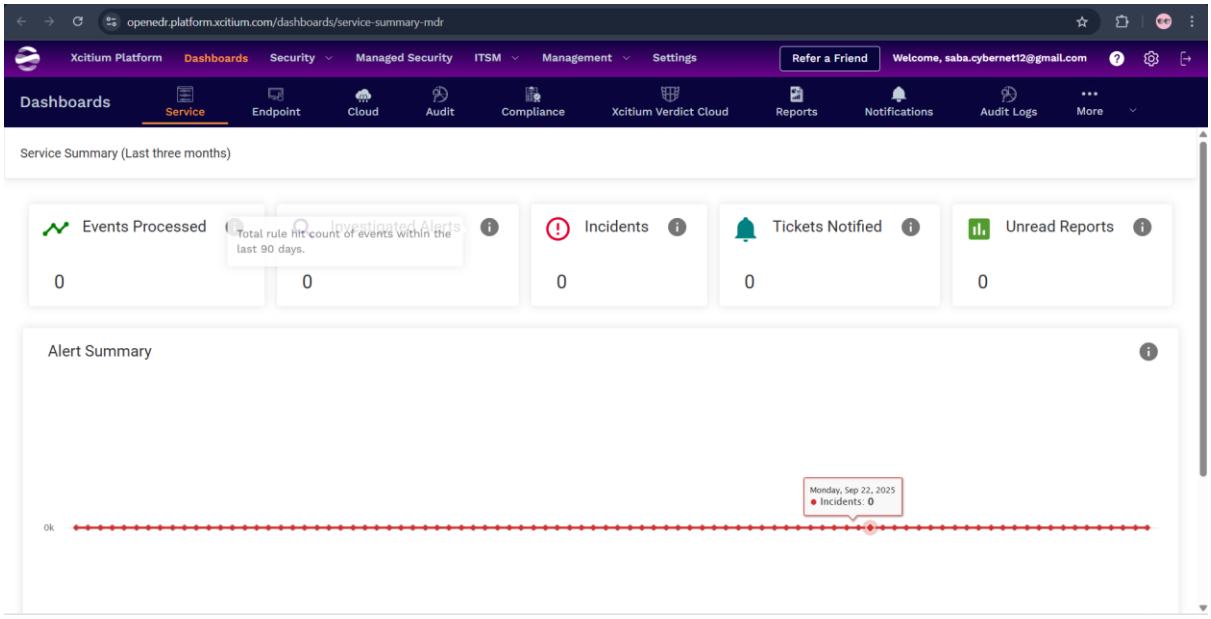
Note: You might see an optional, Set Secret Questions window. This lab does not require that you complete this task. Select the Skip option to bypass this task.

6. The Welcome screen opens. Select Next.

7. On the Enroll Devices screen, select Finish.

8. Next, select Close on the That's It! page.

9. The Dashboard screen appears.



Task 2: Add an endpoint device to the OpenEDR system

Now you've set up the OpenEDR Cloud Manager. In this task, you'll add endpoints to the Cloud Manager.

1. On the ITSM menu, select Device Management to open the Enrollment Wizard page. Next, select Enroll Device.

2. Select the operating system for your device.

3. From the Select Enrollment Type list, select Enroll and Protect.

4. Now, select your preferences from the Set Reboot Options list.

5. Keep the default values unchanged, scroll to the end of the page and select Next.

6. Enter the enrollment link into your browser's address bar or access the link on the device.

7. Select Finish.

8. The Open EDR Cloud Manager is now active on your device. Next, install the client program, or agent, on the device.

9. Open the enrollment link to get the Enrollment Wizard.

10. Follow the installment instructions on the Enrollment Wizard page. Depending on your device, you will be prompted to download either an installer or an app.

Note: The agent name will vary depending on the device.

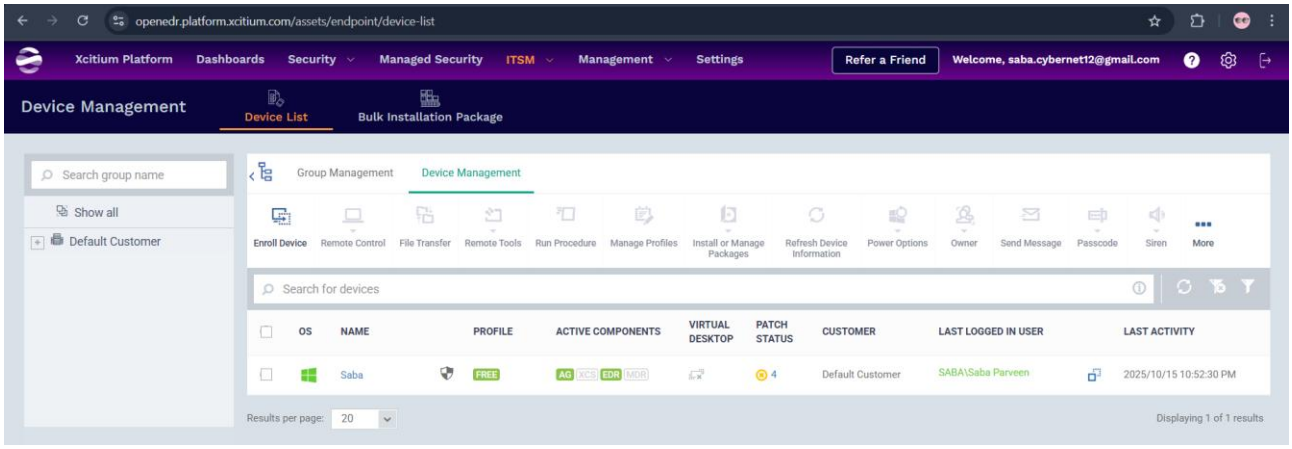
11. Now open the installer and restart your device to finish the agent setup process.

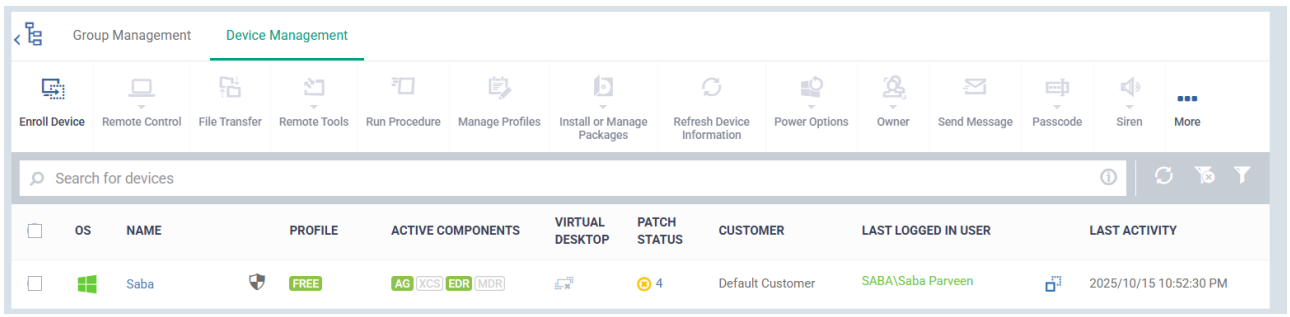
12. After completion of the agent installation, you will verify that the agent can communicate with the Cloud Manager.

13. Visit

https://openedr.com/ and log into the OpenEDR Cloud Manager. Select Get Started.

14. Select ITSM and then Device Management to view the connected devices. Check for your listed device



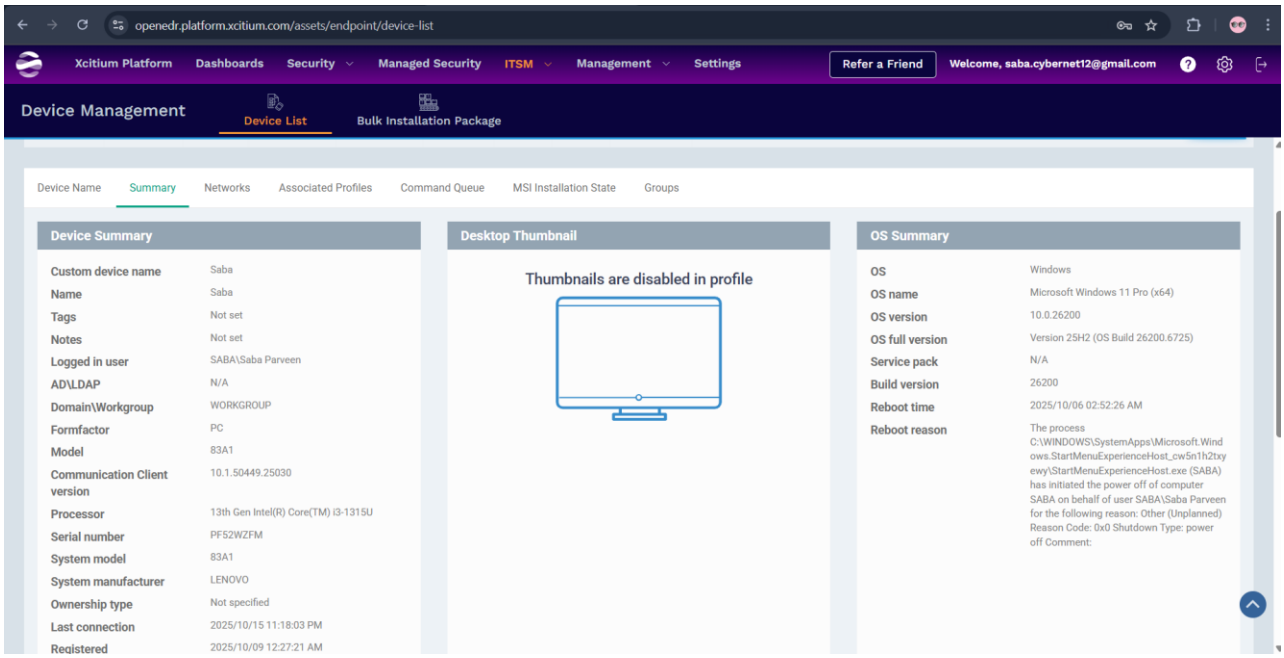


Task 3: Locate endpoint data in the Cloud Manager

Now that agent and the cloud manager are communicating well, let's look at the steps to analyze the data collected by the Cloud manager to manage endpoint protection.

1. Select your device on the Device Management pane.

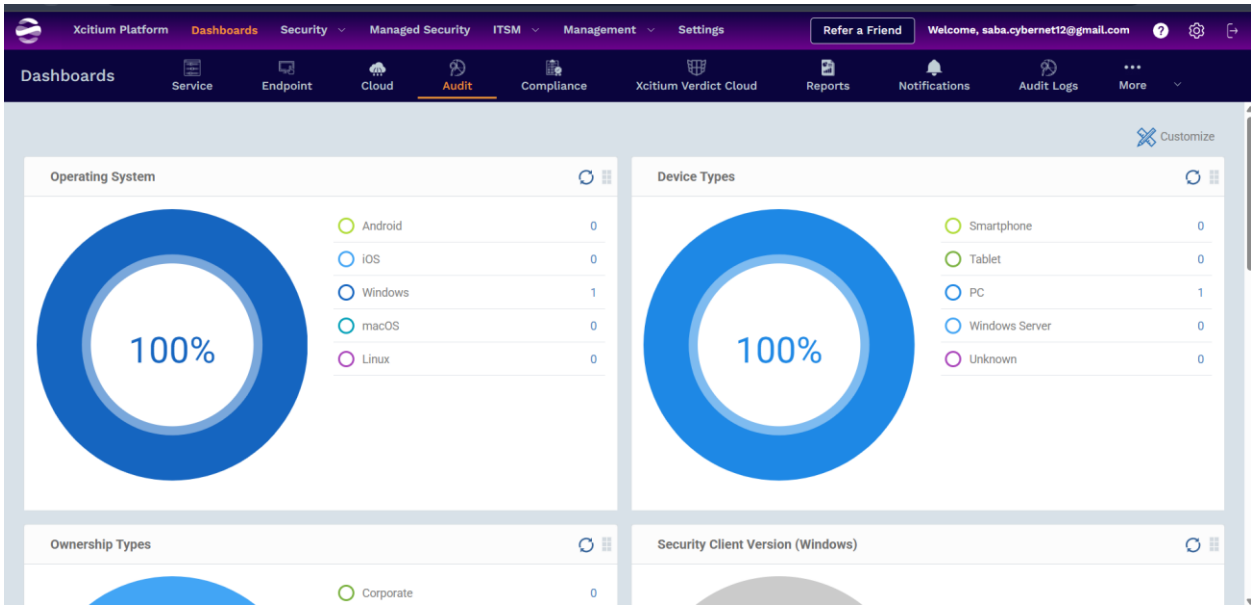
2. Review the detailed information on the Summary page for device's hardware, operating system, security software, and performance metrics, including CPU, RAM, and network usage.



3. Navigate to the Software Inventory tab to access a detailed list of all applications installed on the device.

4. Navigate away from the Device List to explore additional information captured from endpoints. Explore the Audit pane.

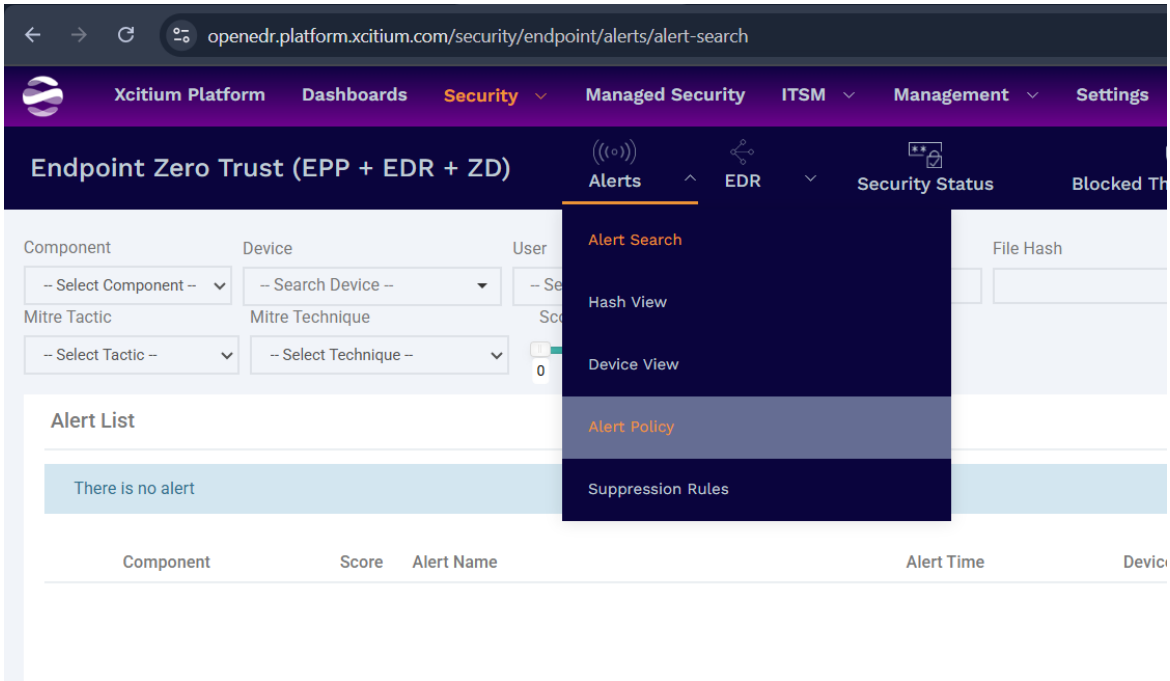
Select the Dashboard tab. → Select the Audit tab to get an overview of the endpoints managed by OpenEDR.



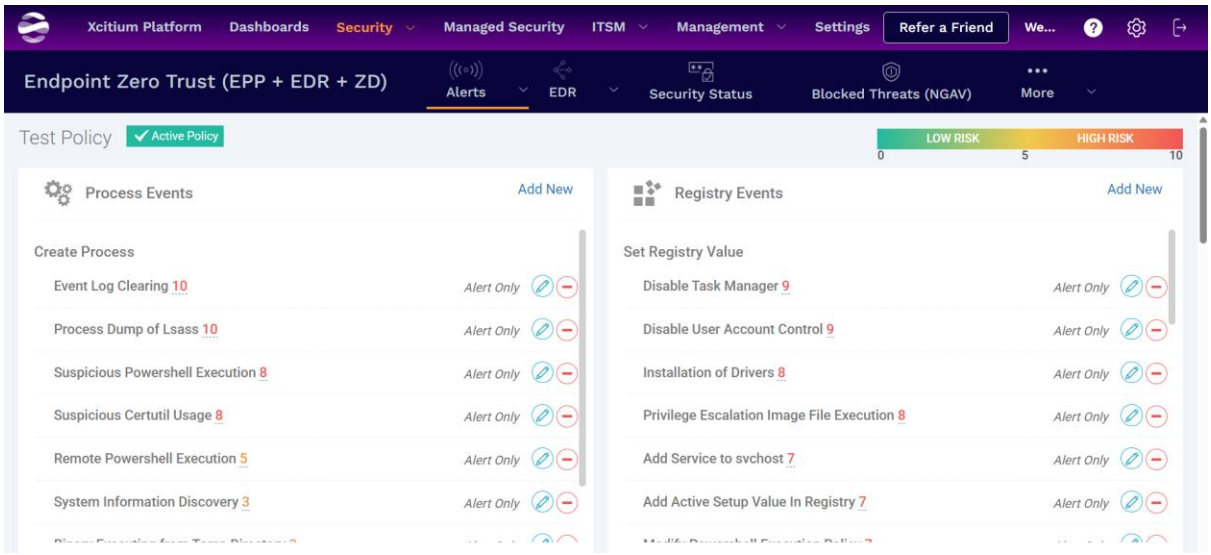
5. Select Security tab to view endpoint threat alerts. Next, select Endpoint Zero Trust (EPP + EDR + ZD) from the drop-down list.

The Endpoint Security pane displays all EDR alerts based on severity levels. Events with a score from 0 to 5 are at the low risk, and those with a score from 6 to 10 are at the high risk.

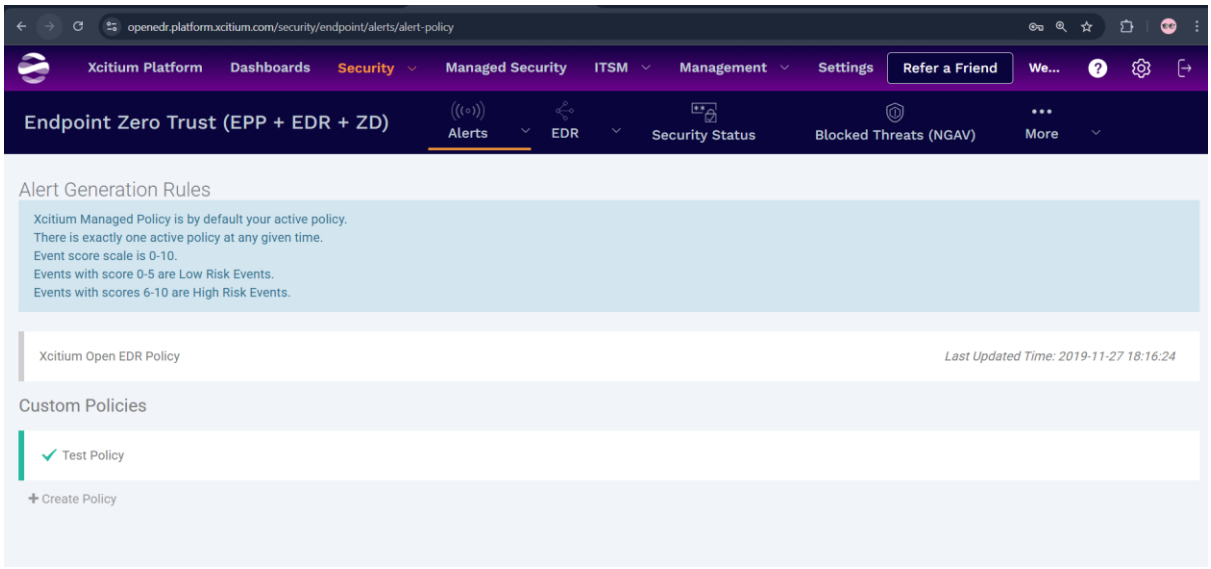
6. Next, establish new rules for monitoring potentially harmful executable downloads into the user's devices. For this, you should create a custom policy. Return to the Alert Policy page and select Create Policy to begin.



7. Type Test Policy in the Custom Policies field, and press Enter in your keyboard.



8. Click on custom policy named Test Policy, to view the various policy details.



Note: Your custom policy begins with the same rules as the Xcitium Predefined Policy. However, you have the option to add, edit, or delete rules based on custom policies.

Task 4: Manage endpoint patches from the cloud manager

Patch management stands as a critical measure for organizations to prevent malicious attacks and ensure that each endpoint has their patches consistently updated. Let's explore how to manage patches on your endpoint devices.

1. Navigate to ITSM –> Device Management –> Select your Device.

2. Your selected device page will appear. Select the Patch Management tab.

3. Ensure that all available updates for the endpoint are visible. To instruct your device to recheck for new updates, Select Check Available Updates.

4. To install patches directly from the cloud manager, select the checkbox next to the patch you wish to install, and then select Install Patch(es).

5. Uninstall the patch that impacts other applications. To do so, select the checkbox next to the patch you want to remove, and then select Uninstall Patch(es).

6. Navigate to the Third-Party Applications tab next to the Operating System to review additional installed applications that have patches or available new versions.

Practice exercises

Next, use these practice exercises to reinforce your learning.

Exercise 1: Create a new security policy in OpenEDR

> **Objective: Create and apply a new security policy to protect against suspicious file execution.**
>
> **Hint: The test file should be blocked or an alert should be generated according to the policy rules you set.**

Step-by-Step Solution — Exercise 1

Step 1: Log in to the OpenEDR Cloud Manager

1. Open your web browser and navigate to

`https://openedr.com/`

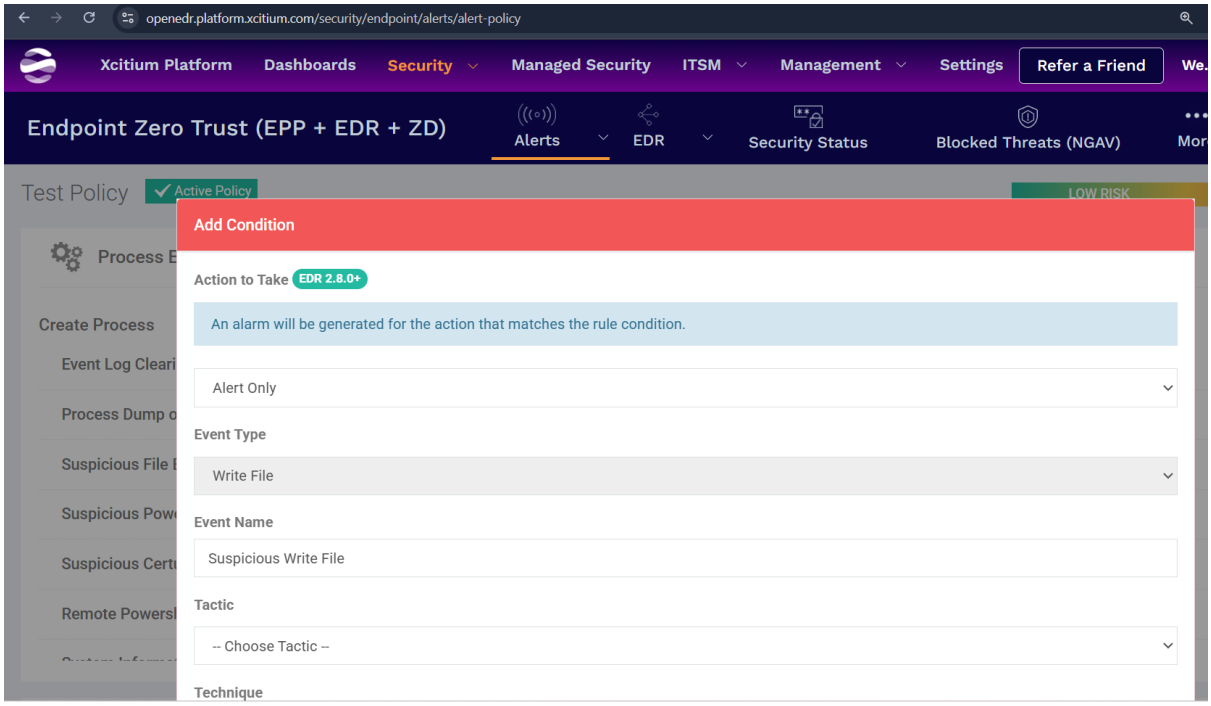
Step 2: Navigate to the Alert Policy Page

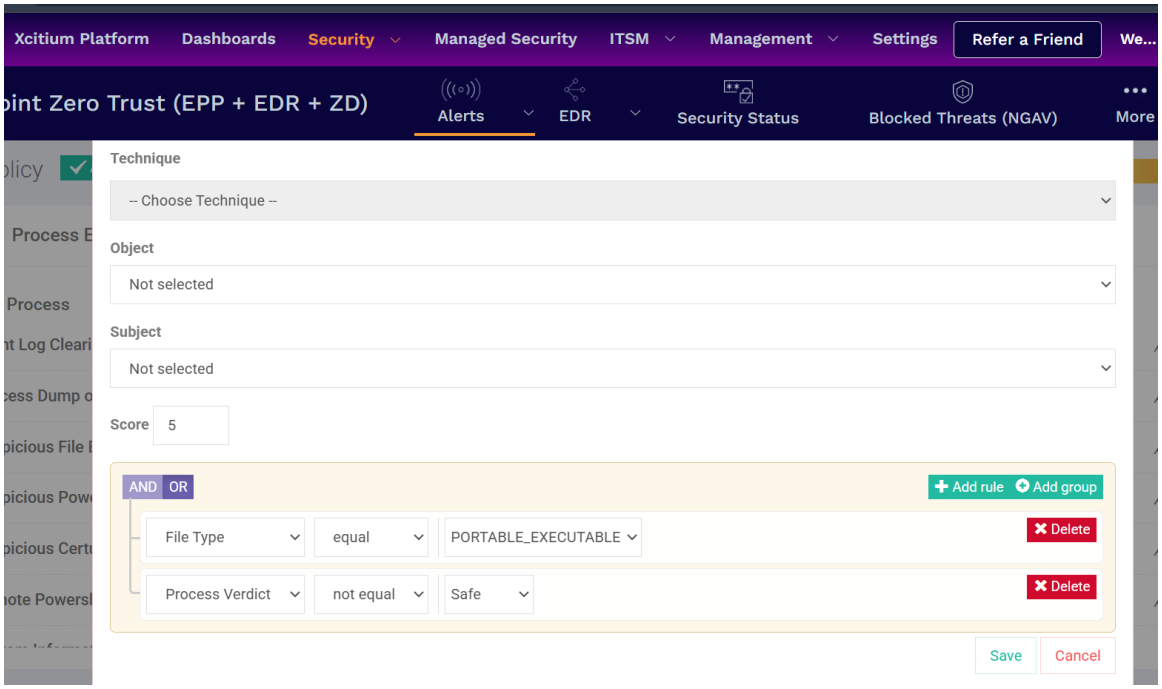
1. In the Cloud Manager's left navigation pane, go to
   Security → Alert Policy (sometimes found under *Endpoint Security*).
2. Review the **existing predefined policies** (for example, the *Xcitium Predefined Policy*).
   These contain the default detection and prevention rules applied to all devices.

Step 3: Create a New Custom Policy

1. Click **Create Policy** at the top right.
2. In the **Custom Policies** field, type a name such as
3. `Test Policy - Suspicious File Execution` and press **Enter**.
4. Your new policy appears in the list.
   Click on **Test Policy** to open its configuration screen.

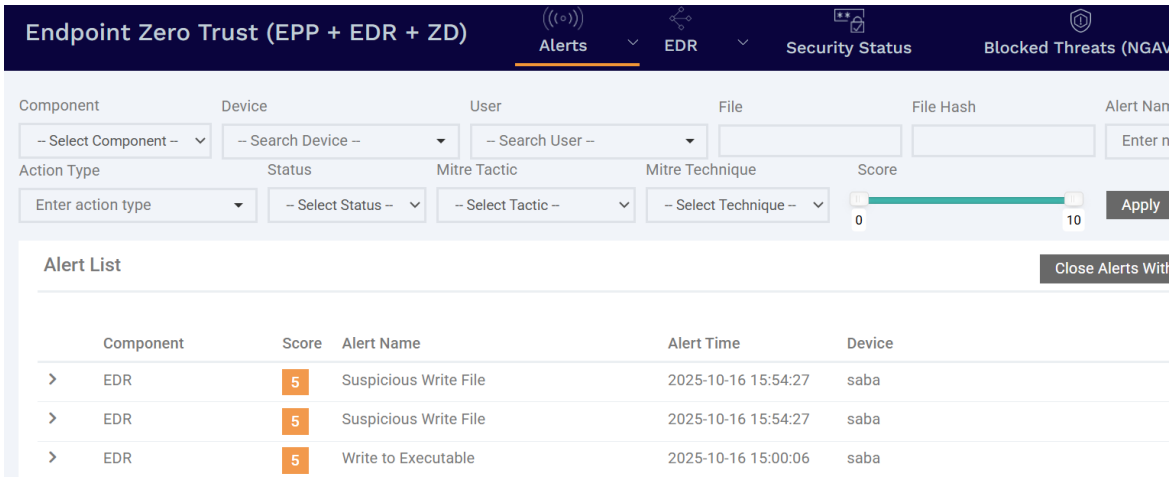
Step 5: Add New Rules for Harmful Executable Downloads

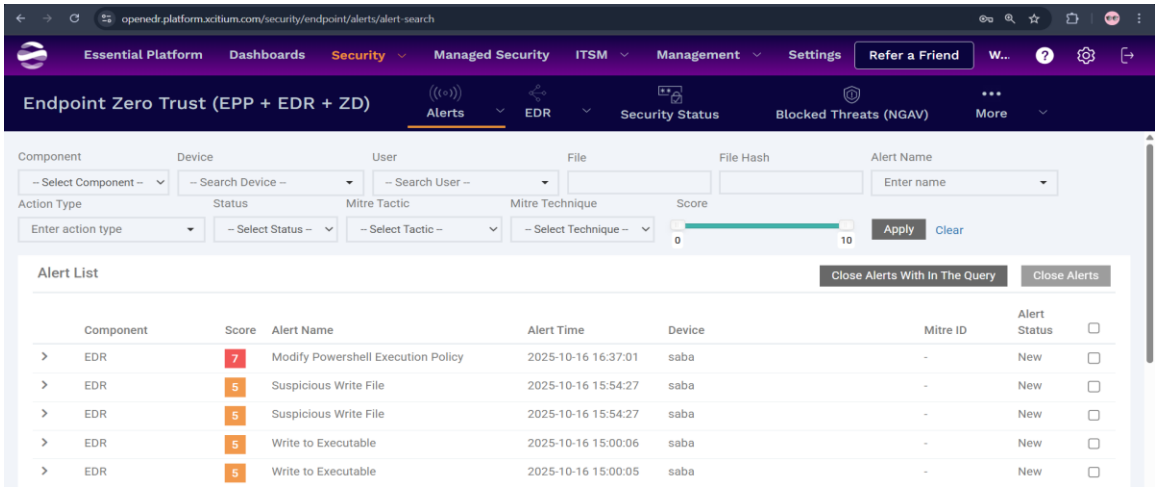




Step 6: Save and Apply the Policy

Step 7: Test the Policy





Get certified:

https://edr.comodo.com/certification/