Custom XDR Rules

Custom XDR Rules let you create XDR alerts from SIEM events. There are three ways to create new rules:

1. Create a rule from a specific event in the events list on the **SIEM Events** page.
2. Create a rule based on the current filters on the **SIEM Events** page.
3. Create a blank and completely configurable rule from either the **SIEM Events** page or **Custom XDR Rules** page.

The **New XDR Alert Policy** wizard that runs is mostly the same for all three, regardless of where it is run from.

Create a rule from an event when there is a specific event that caught your attention. Mandatory detection logic fields are automatically populated, based on the details of the event, and you can select additional fields to add to the detection logic. All fields from the log of that specific event are available to be selected as part of the detection logic.

Create a rule based on current filters when you've applied specific filters to the events list and you want the detection logic fields to be automatically populated based on your filters (for example, a specific source type and one or more different operations).

Creating a blank rule allows you to set all of your own conditions without any parameters being automatically populated. It gives you the most freedom, but also requires you to set all of the rule parameters manually.

Note: Since Custom XDR Alerts are configured and managed by your organization, they are not monitored or managed by the CyOps team.

Note: The **Custom XDR Rules** page is currently in Beta with certain limitations. Additional enhancements are planned for inclusion before the page's General Availability release.
To request access to the **Custom XDR Rules** page during the Beta period, contact your Cynet Representative and request to be added to the Beta.

Before you begin

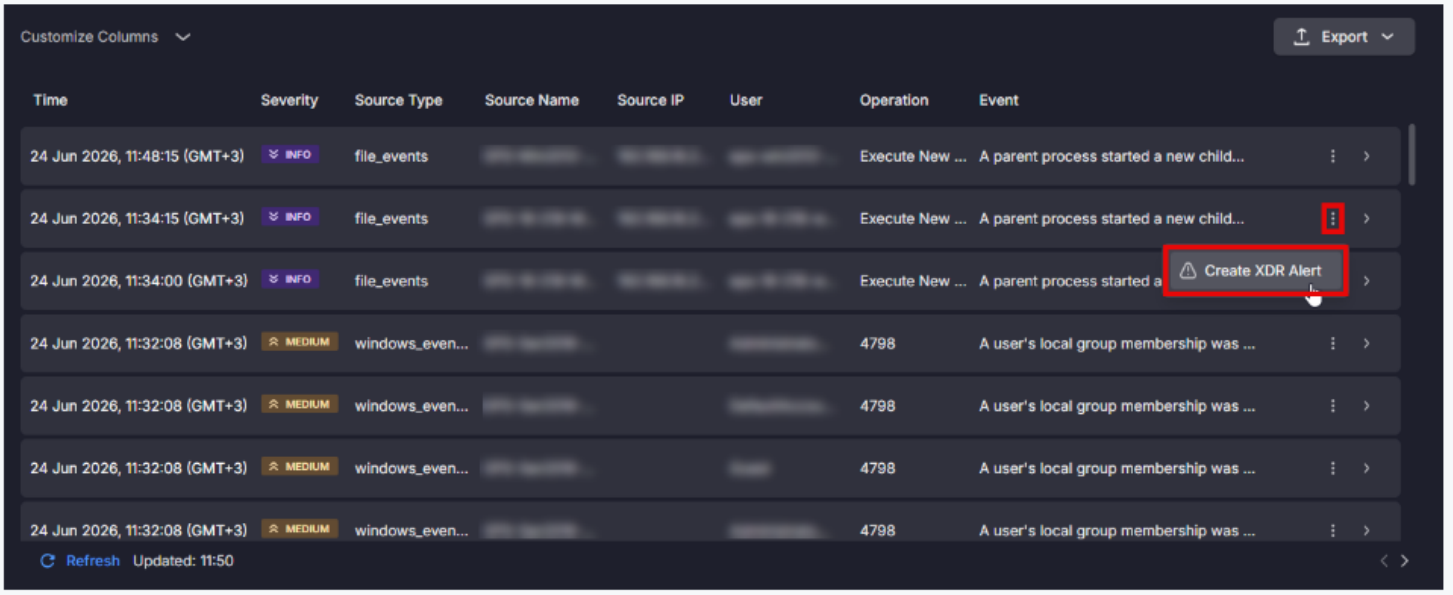
- Make sure you have access to the SIEM module.
- If you want to create a rule from filtered results, apply the relevant filters in the SIEM Events page before you start.

Notes:

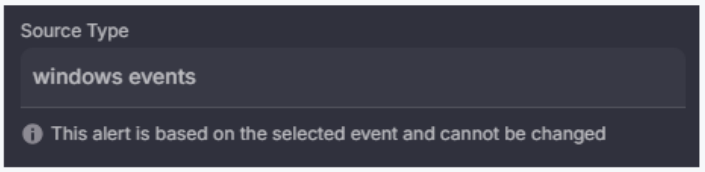
- The the **Rules Detection Logic** uses **AND** when you specify the conditions. This means that in order for the rule to trigger an alert, **all** of the conditions specified in the rule must be met.
- Custom XDR rules only trigger alerts when the conditions are met by data that was ingested **after** the rule was created.

Create a Rule from a SIEM Event

1. Go to **SIEM > SIEM Events**.
2. Locate the event you want to use.
3. Open the event actions menu.

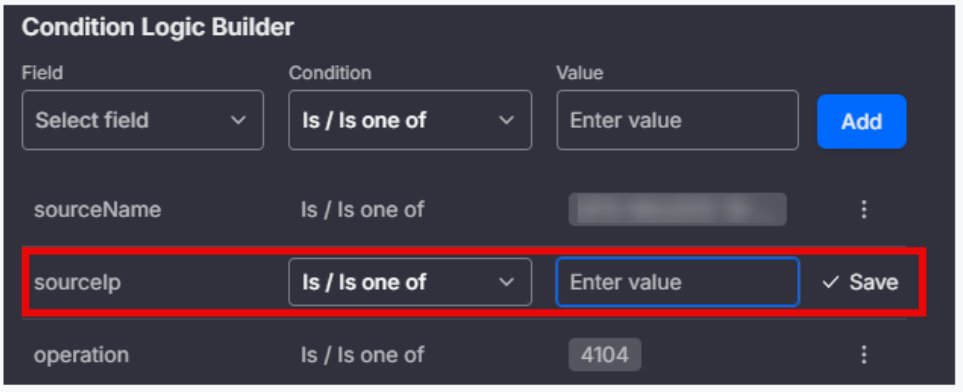


4. Click **Create XDR Alert**.
   The rule wizard opens with information from the selected event already populated.
5. On the **Alert Details** screen, add a name and optional description for the policy.
6. Review the **Detection Scope**, then click **Next**.



Important! The **Category** and **Source Type** are prepopulated and cannot be changed.

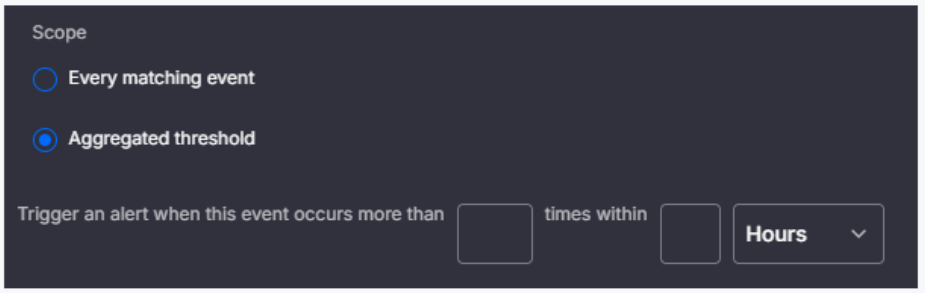
7. Modify the **Rules Detection Logic** as needed:
   Mandatory fields are prepopulated with data from the selected event. Most fields already contain the Condition and Value, but some may need these completing.
   a. For any mandatory fields that need completing, select the **Condition** and enter the **Value**, then click **Save**.



   b. If there are any fields you want to add in addition to those automatically populated from the event data, select the **Field**, **Condition** and **Value** for each, and click **Add**.

Note: When creating a rule from a specific event, any field shown in the event log of the event from which you created the rule can be selected as a field for the Rules Detection Logic.

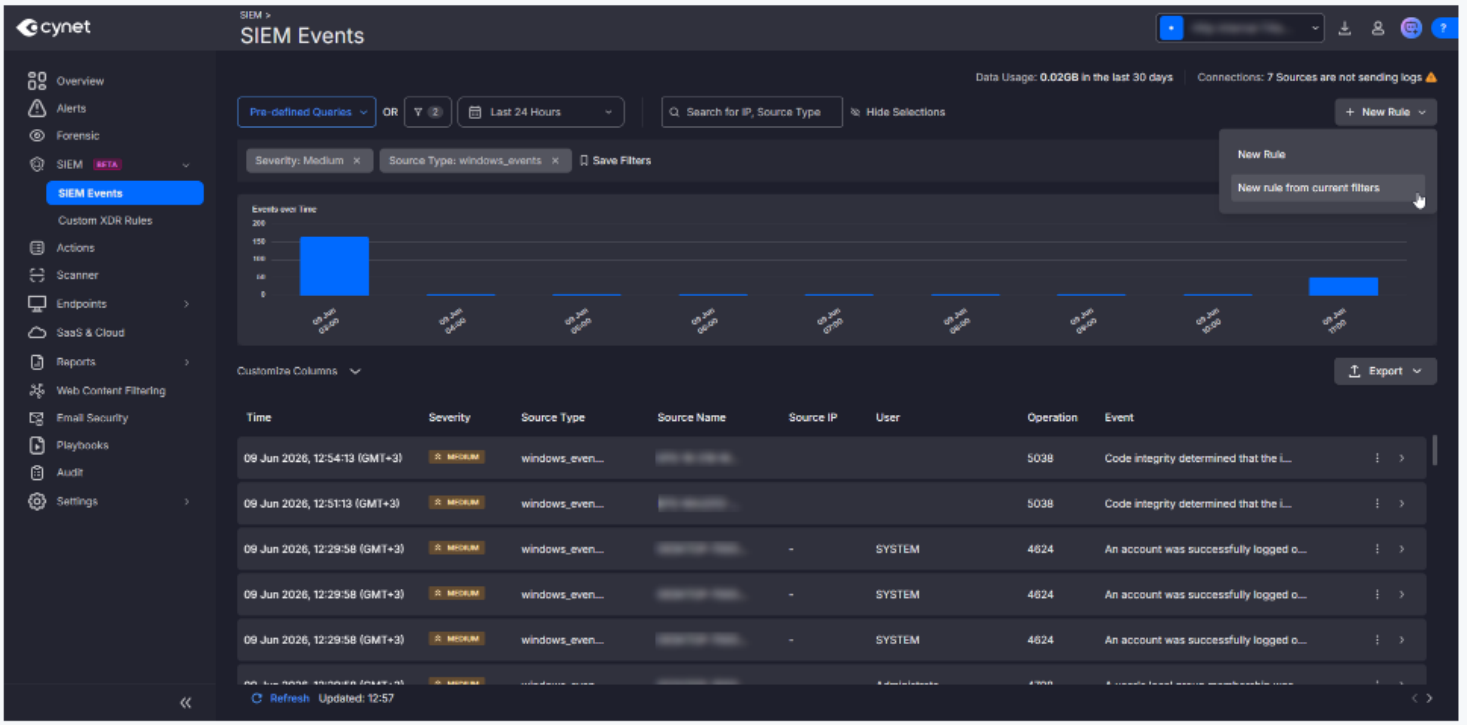
8. Click **Next**.
9. Configure the **Aggregation & Threshold** settings.
    a. Select the severity from the dropdown.
    b. Select the **Scope**:
        - **Every matching event:** Creates an alert for every event that matches the rule conditions.
        - **Aggregated threshold:** Creates an alert only when the event occurs more than the specified number of times within the selected time period.



    c. If you selected **Aggregated threshold**, configure:
        - Number of occurrences
        - Time window
10. Click **Next**.
11. Review the **Summary** page and if needed, go back to make changes.
12. Click **Create Policy**.

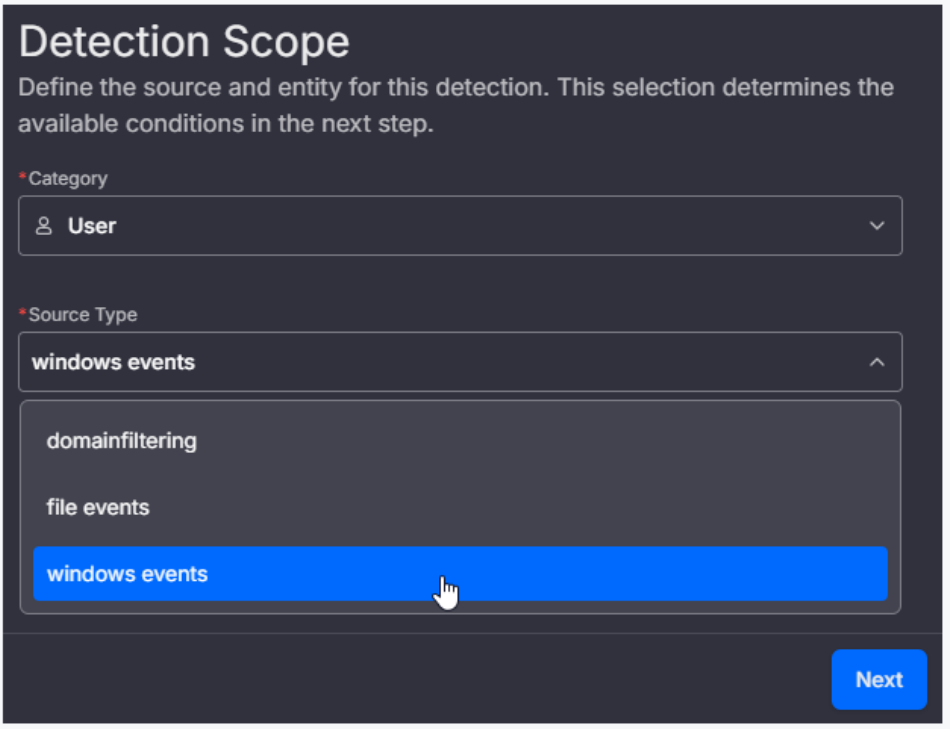
Create a New Rule (Blank or Based on Filters)

1. Go to **SIEM > SIEM Events**.
2. Click **New Rule**.



3. Select one of the following options:
    - **New Rule** to create a rule manually.
    - **New rule from current filters** to create a rule based on the filters currently applied to the SIEM Events table.
4. On the Alert Details screen, enter a **Policy Name**.
5. Optionally, enter a **Description**.
6. Click **Next**.

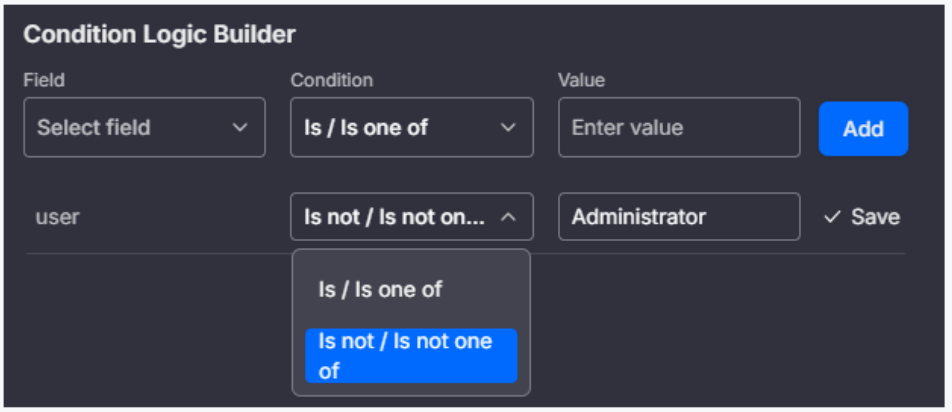
7. Under Detection Scope, select the **Category**.



8. Select the **Source Type** (or review it if you chose to create a rule from the filters).

> **Note:** Different source types are available, depending on the selected category. For example, when you select the **Host** category, only the **File Events** and **Windows Events** source types are available.

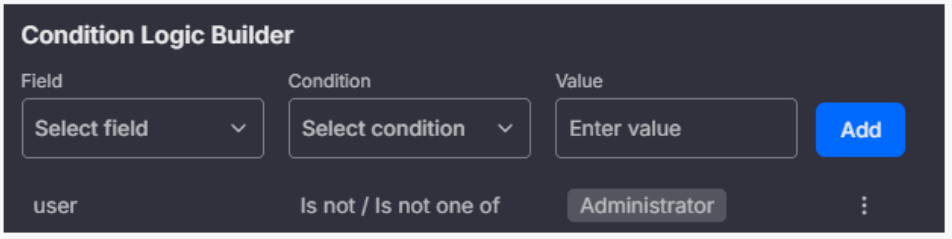
9. Click **Next**.
10. In the **Condition Logic Builder**, define the conditions that must occur for the policy to be triggered.
    Note that each category has different mandatory fields.
    a. For each mandatory field, select the **Condition**. The selected **Condition** determines whether the alert triggers when the specified value/s **are** present or when they are **not** present.



    b. For each mandatory field, enter the **Value**. Multiple values can be entered by adding a comma between them (for example: user1,user2,user3).

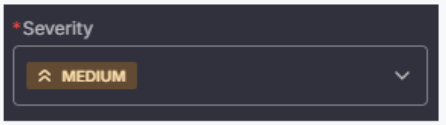
> **Note:** Only an **exact match** to a value will trigger an alert.

    c. Click **Save** for each mandatory field.
    d. Optionally add additional fields, selecting the conditions and values for each, then click **Add**, to finish building the rule logic.

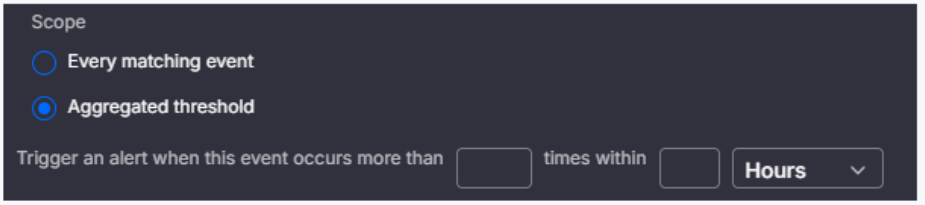


    e. Click **Next**.

11. On the **Aggregation & Threshold** screen, set the severity and scope:
    a. Select the alert **Severity** from the dropdown list.



    b. Under **Scope**, select one of the following options:

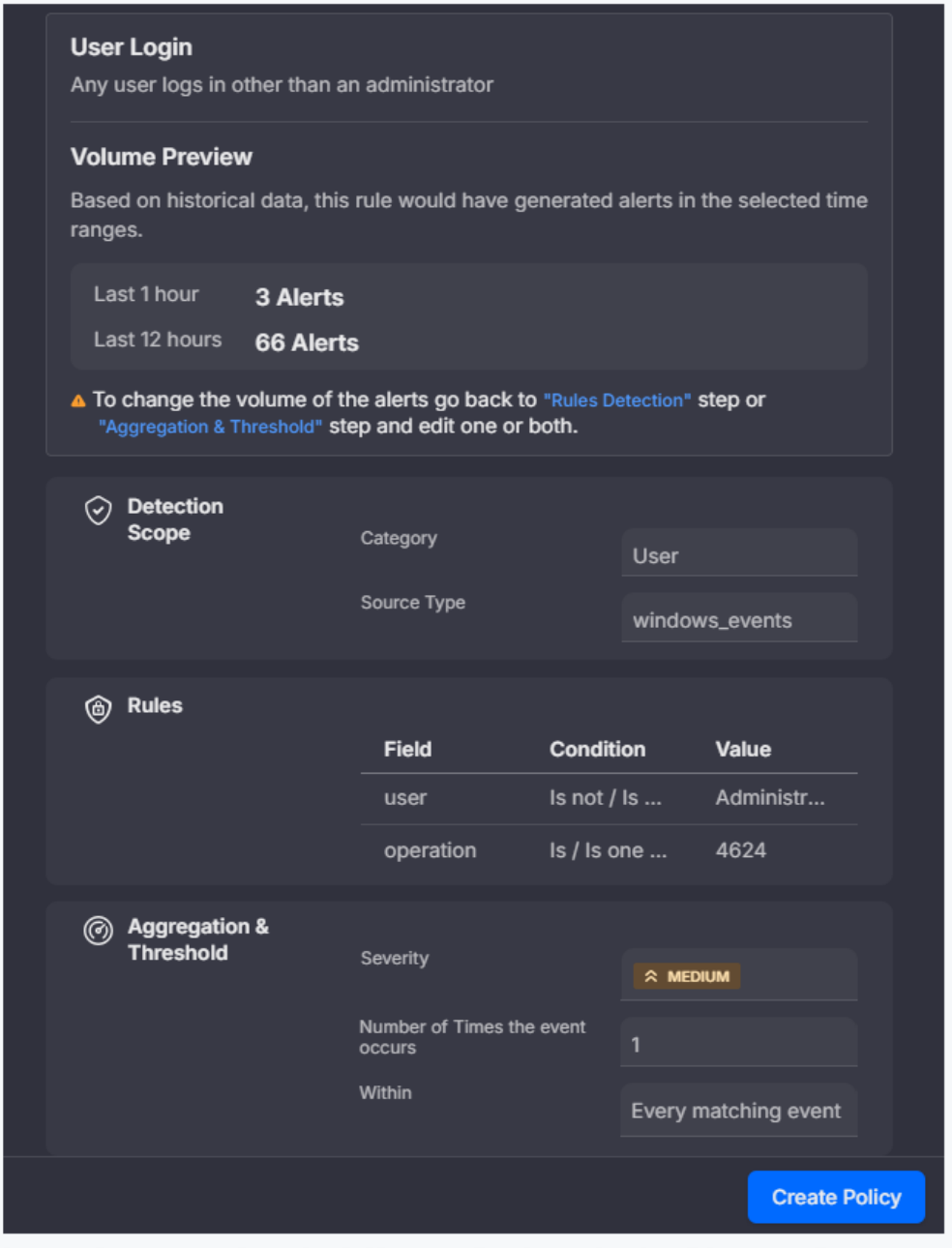


    - **Every matching event:** Creates an alert for every event that matches the rule conditions.
    - **Aggregated threshold:** Creates an alert only when the event occurs more than the specified number of times within the selected time period.

    c. If you selected **Aggregated threshold**, configure:
    - Number of occurrences
    - Time window

    d. Click **Next**.

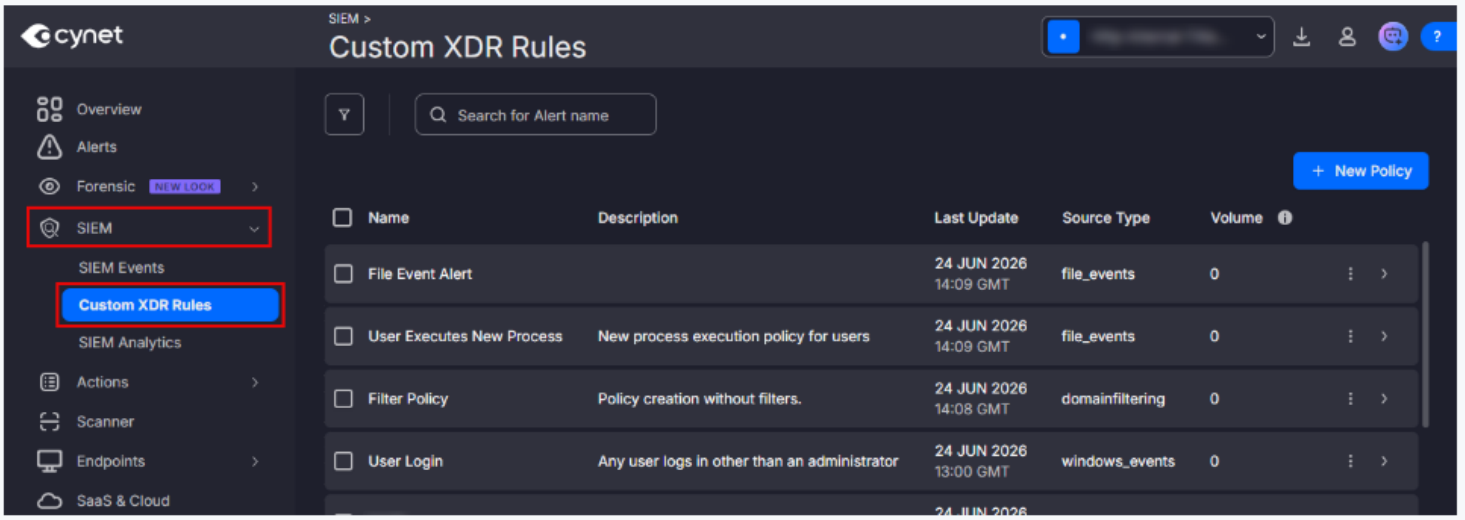
12. On the **Summary** screen, review the policy configuration and **Volume Preview**.



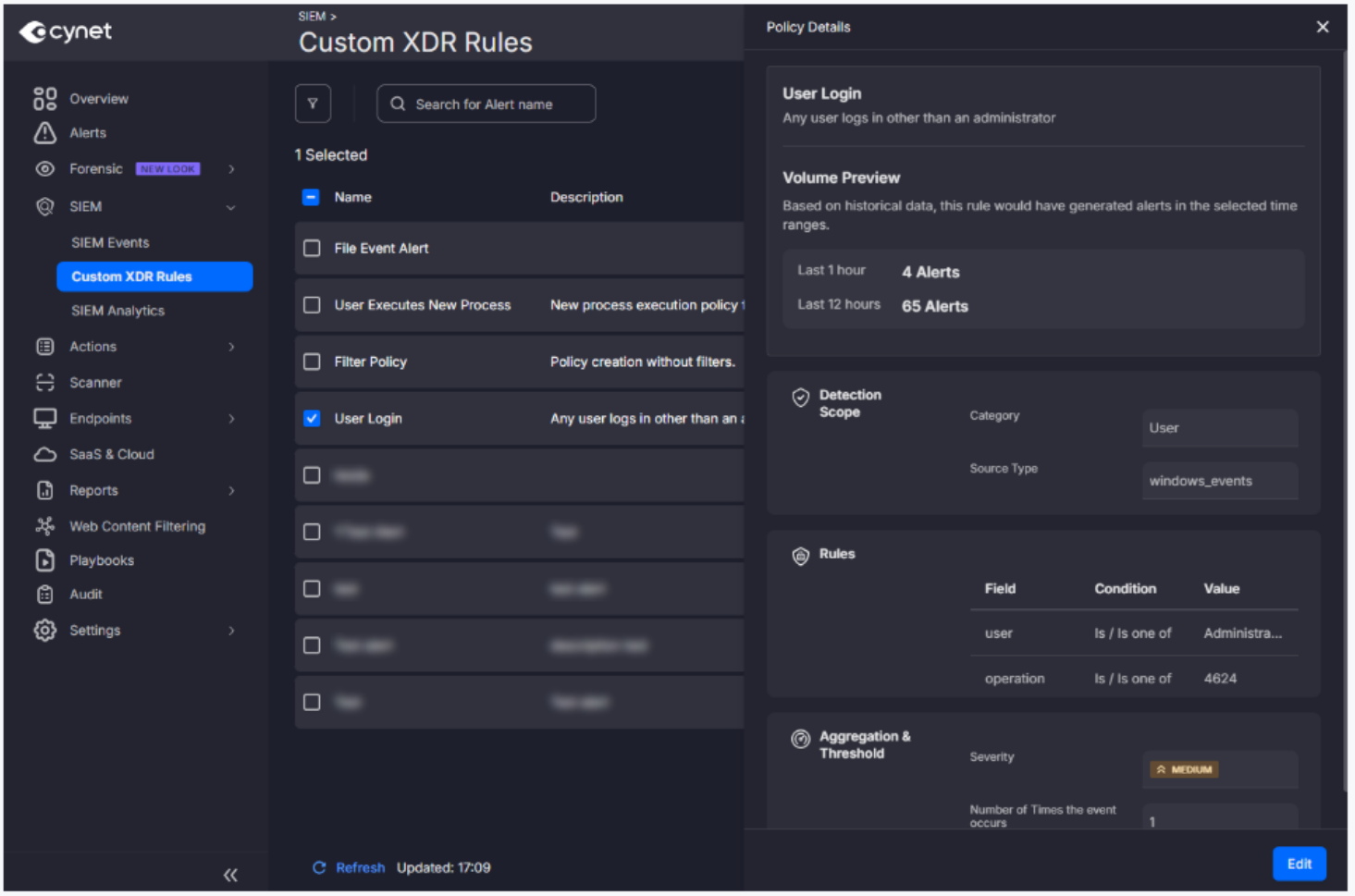
13. If needed, return to the **Rules Detection** or **Aggregation & Threshold** step to adjust them. Otherwise, click **Create Policy**.

View Custom XDR Rules

1. From the Cynet toolbar, navigate to **SIEM** > **Custom XDR Rules**.



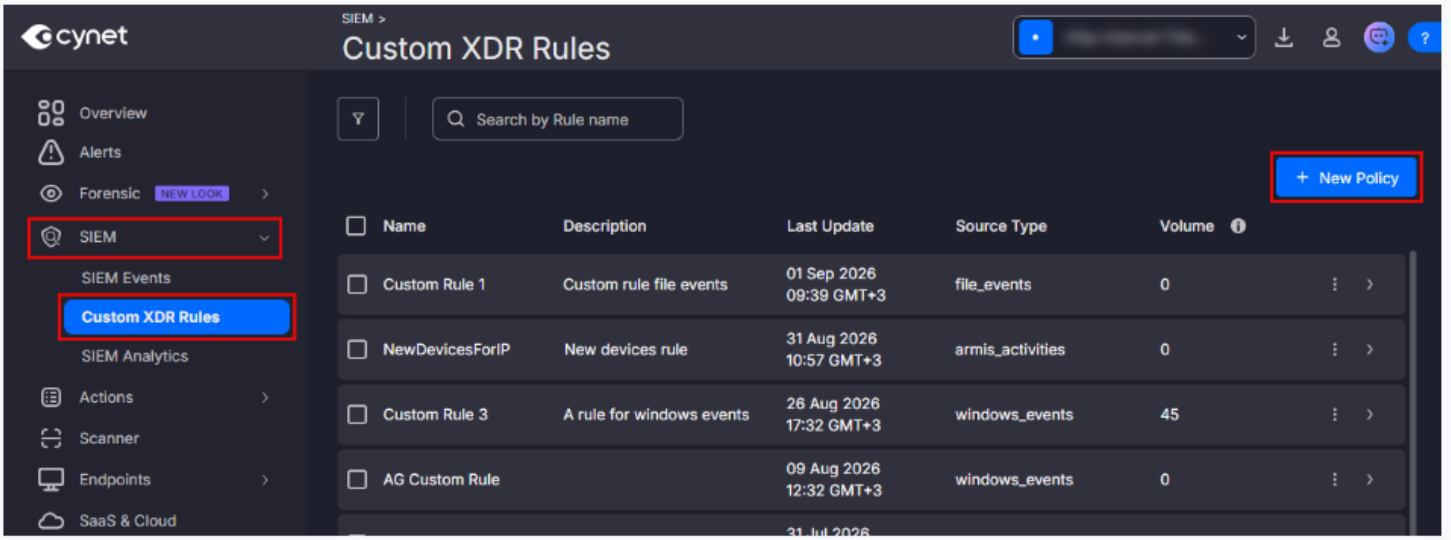
2. Optionally use the search bar or filter by Source Type to find a rule.
3. Review the information displayed in the table.
4. Select a rule to open its details.



The details page displays the **Volume Preview**, **Detection Scope**, **Rules**, and **Aggregation & Threshold** settings.

Create a Rule from the Custom XDR Rules Page

1. On the **Custom XDR Rules** page, click **New Policy**.



2. Continue from step 4 of **Create a New Rule (Blank or Based on Filters)** above.

Last updated: Oct 8, 2026

Did this article help solve your problem?

YES NO

Copyright © 2026 Cynet Security Ltd. All rights reserved.