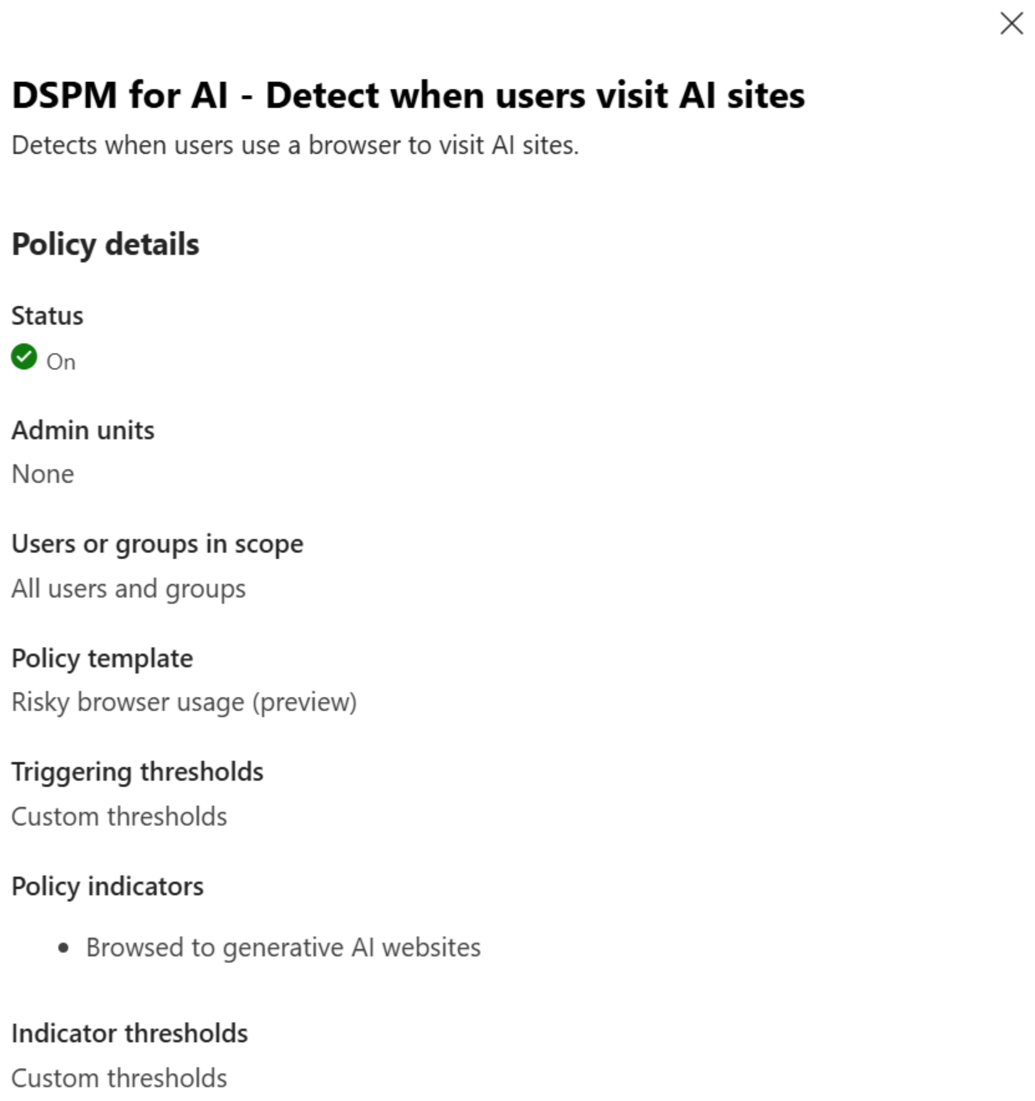
Example policy that isn't behaving as we'd expect:

IRM:
DSPM for AI - Detect when users visit AI sites



DSPM for AI - Detect when users visit AI sites

Detects when users use a browser to visit AI sites.

Policy details

Status

✓ On

Admin units

None

Users or groups in scope

All users and groups

Policy template

Risky browser usage (preview)

Triggering thresholds

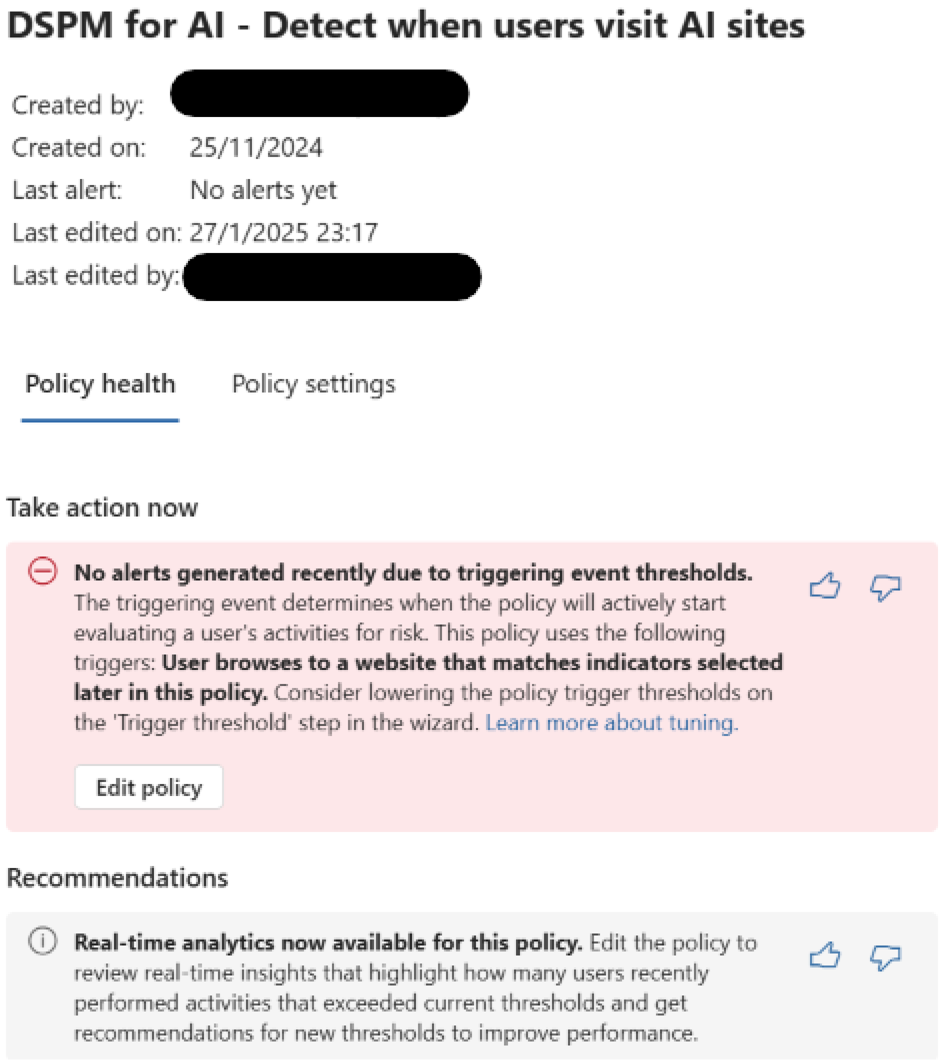
Custom thresholds

Policy indicators

- Browsed to generative AI websites

Indicator thresholds

Custom thresholds



DSPM for AI - Detect when users visit AI sites

Created by: [redacted]
Created on: 25/11/2024
Last alert: No alerts yet
Last edited on: 27/1/2025 23:17
Last edited by: [redacted]

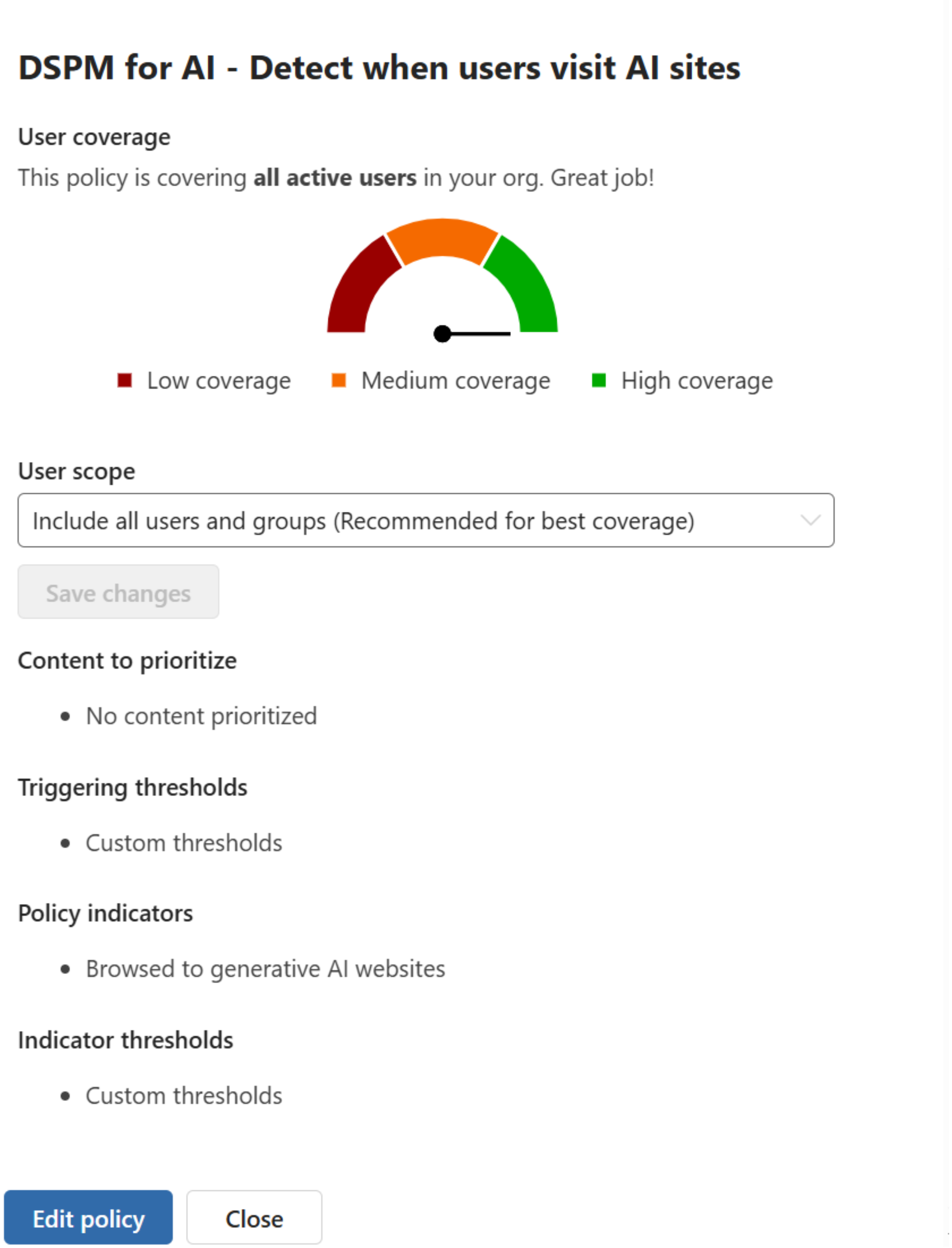
Policy health | Policy settings

Take action now

No alerts generated recently due to triggering event thresholds. The triggering event determines when the policy will actively start evaluating a user's activities for risk. This policy uses the following triggers: **User browses to a website that matches indicators selected later in this policy.** Consider lowering the policy trigger thresholds on the 'Trigger threshold' step in the wizard. Learn more about tuning.

Recommendations

Real-time analytics now available for this policy. Edit the policy to review real-time insights that highlight how many users recently performed activities that exceeded current thresholds and get recommendations for new thresholds to improve performance.



DSPM for AI - Detect when users visit AI sites

User coverage

This policy is covering **all active users** in your org. Great job!

🟥 Low coverage 🟧 Medium coverage 🟩 High coverage

User scope

Include all users and groups (Recommended for best coverage)

Content to prioritize

- No content prioritized

Triggering thresholds

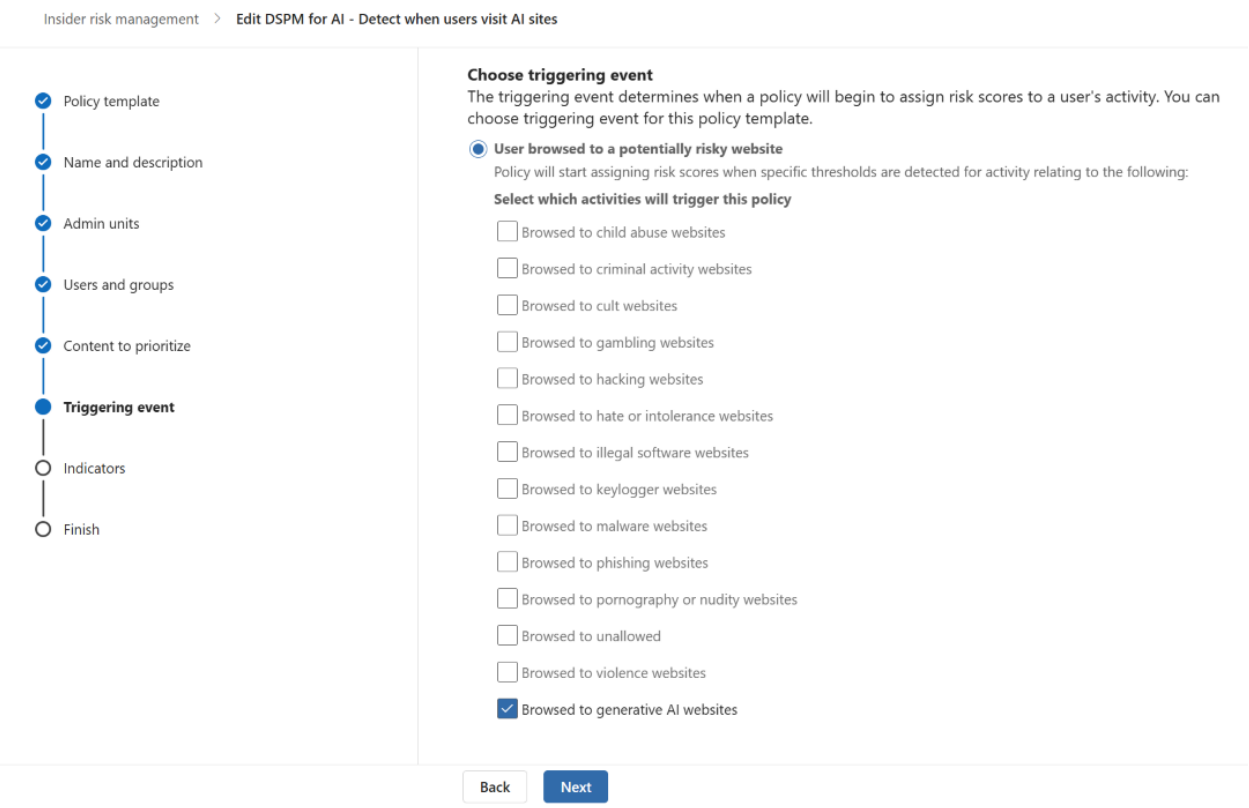
- Custom thresholds

Policy indicators

- Browsed to generative AI websites

Indicator thresholds

- Custom thresholds



Choose triggering event

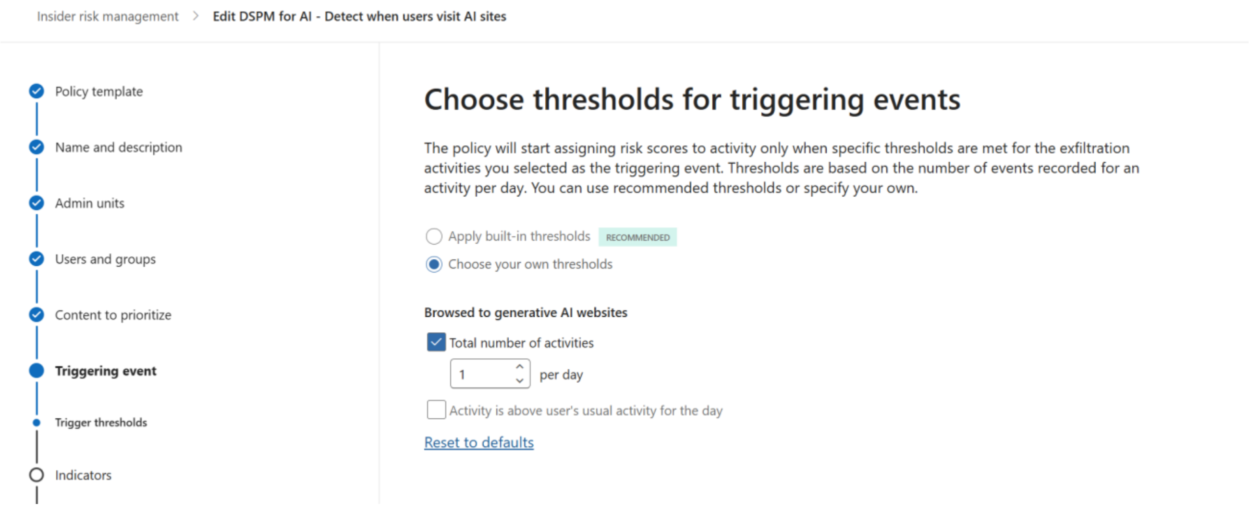
The triggering event determines when a policy will begin to assign risk scores to a user's activity. You can choose triggering event for this policy template.

● **User browsed to a potentially risky website**

Policy will start assigning risk scores when specific thresholds are detected for activity relating to the following:

Select which activities will trigger this policy

- □ Browsed to child abuse websites
- □ Browsed to criminal activity websites
- □ Browsed to cult websites
- □ Browsed to gambling websites
- □ Browsed to hacking websites
- □ Browsed to hate or intolerance websites
- □ Browsed to illegal software websites
- □ Browsed to keylogger websites
- □ Browsed to malware websites
- □ Browsed to phishing websites
- □ Browsed to pornography or nudity websites
- □ Browsed to unallowed
- □ Browsed to violence websites
- ☑ Browsed to generative AI websites



Choose thresholds for triggering events

The policy will start assigning risk scores to activity only when specific thresholds are met for the exfiltration activities you selected as the triggering event. Thresholds are based on the number of events recorded for an activity per day. You can use recommended thresholds or specify your own.

○ Apply built-in thresholds RECOMMENDED

● Choose your own thresholds

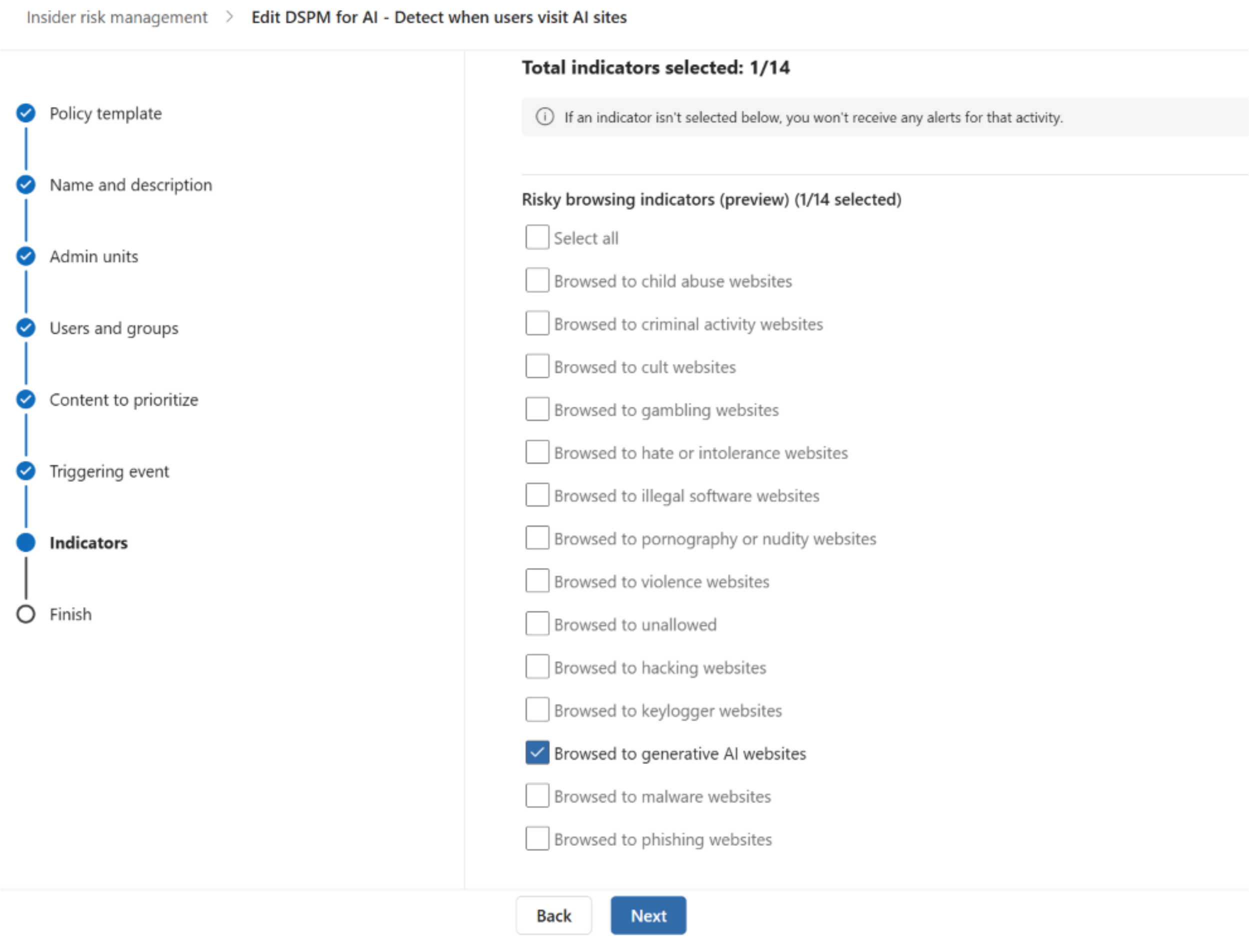
Browsed to generative AI websites

☑ Total number of activities

1 per day

□ Activity is above user's usual activity for the day

Reset to defaults



Insider risk management > Edit DSPM for AI - Detect when users visit AI sites

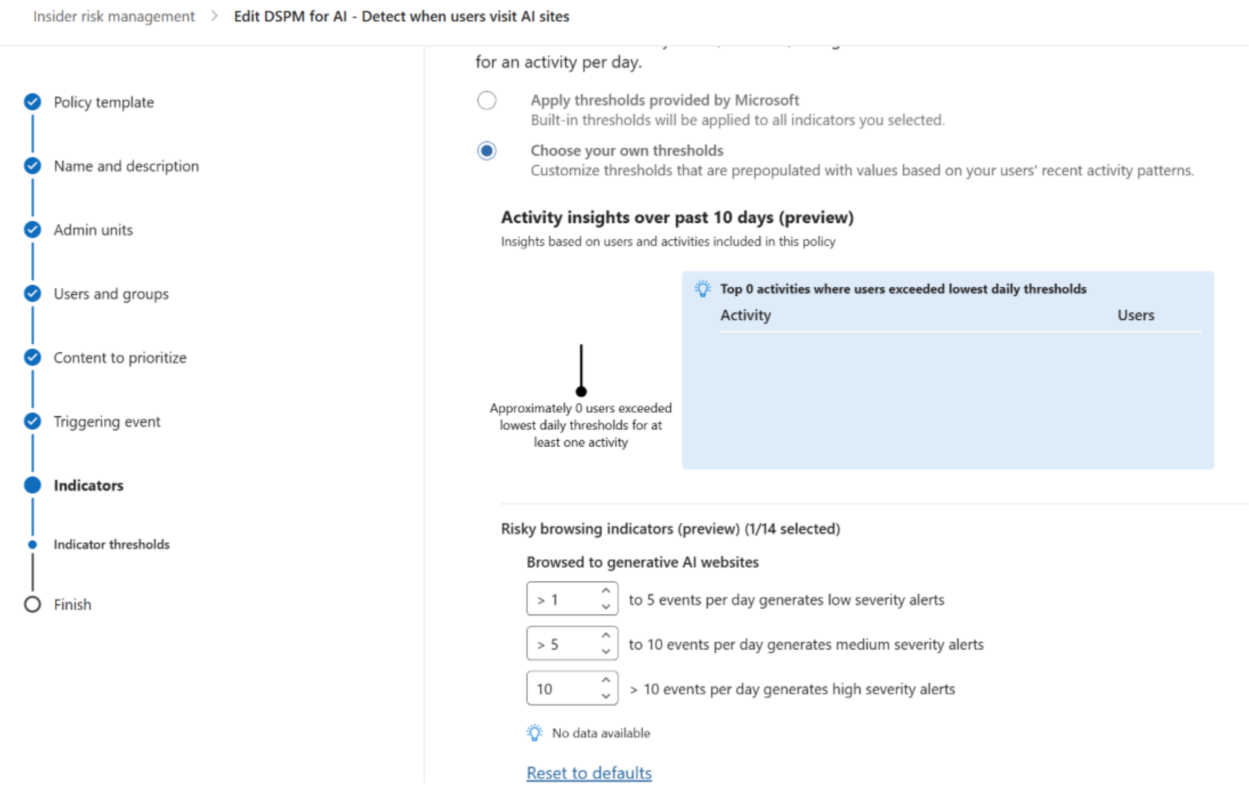
- ● Policy template
- ● Name and description
- ● Admin units
- ● Users and groups
- ● Content to prioritize
- ● Triggering event
- ● **Indicators**
- ○ Finish

Total indicators selected: 1/14

ⓘ If an indicator isn't selected below, you won't receive any alerts for that activity.

Risky browsing indicators (preview) (1/14 selected)

- □ Select all
- □ Browsed to child abuse websites
- □ Browsed to criminal activity websites
- □ Browsed to cult websites
- □ Browsed to gambling websites
- □ Browsed to hate or intolerance websites
- □ Browsed to illegal software websites
- □ Browsed to pornography or nudity websites
- □ Browsed to violence websites
- □ Browsed to unallowed
- □ Browsed to hacking websites
- □ Browsed to keylogger websites
- ☑ Browsed to generative AI websites
- □ Browsed to malware websites
- □ Browsed to phishing websites



for an activity per day.

○ Apply thresholds provided by Microsoft
Built-in thresholds will be applied to all indicators you selected.

● Choose your own thresholds
Customize thresholds that are prepopulated with values based on your users' recent activity patterns.

Activity insights over past 10 days (preview)

Insights based on users and activities included in this policy

Approximately 0 users exceeded lowest daily thresholds for at least one activity

Top 0 activities where users exceeded lowest daily thresholds

Activity	Users

Risky browsing indicators (preview) (1/14 selected)

Browsed to generative AI websites

> 1 to 5 events per day generates low severity alerts

> 5 to 10 events per day generates medium severity alerts

10 > 10 events per day generates high severity alerts

No data available

Reset to defaults