AI Defense Events

The Events section offers a comprehensive view of activities and interactions within your AI Defense environment. It includes detailed event logs capturing AI-related activities such as detected prompts, responses, and rule matches. Advanced filtering options allow you to refine data by time period, application, or event type, enabling targeted monitoring and efficient analysis of AI events.

- The Event logs has the following details:
  - **Event Time**: Timestamp indicating when the event occurred, enabling precise tracking and analysis.
  - **Rule Action**: Specifies the action taken by the system, such as block, allow, or alert, based on the guardrail or policy applied.
  - **Message Type**: Identifies whether the captured message is a prompt, response, or both, providing context to the event.
  - **Application**: The associated application where the event originated, offering insight into usage patterns and activity sources.
  - **Model**: Specifies the AI model involved in the interaction, helping to pinpoint the source of the AI activity.
  - **Rule Name**: The name of the policy or guardrail rule that triggered the event, aiding in understanding the enforcement mechanisms.

Filter Events List

You can filter the events log list view by clicking the settings icon on the right top corner of the table. You can select

Click **Apply.** This changes the columns displayed in the table.