

# Teams webhook requests for Mezmo Alerts

## Mezmo Webhook configuration

Content-Type: application/json

```
{
  "title": "Mezmo - User account alert",
  "summary": "{{ matches }} line(s) matched in {{ name }}",
  "view": "{{ name }}",
  "matches": "{{ matches }}",
  "line": "{{ line }}",
  "lines": "{{ lines }}",
  "level": "{{ level }}",
  "url": "{{ url }}",
  "query": "{{ query }}",
  "app": "{{ app }}",
  "host": "{{ host }}",
  "tag": "{{ tag }}"
}
```

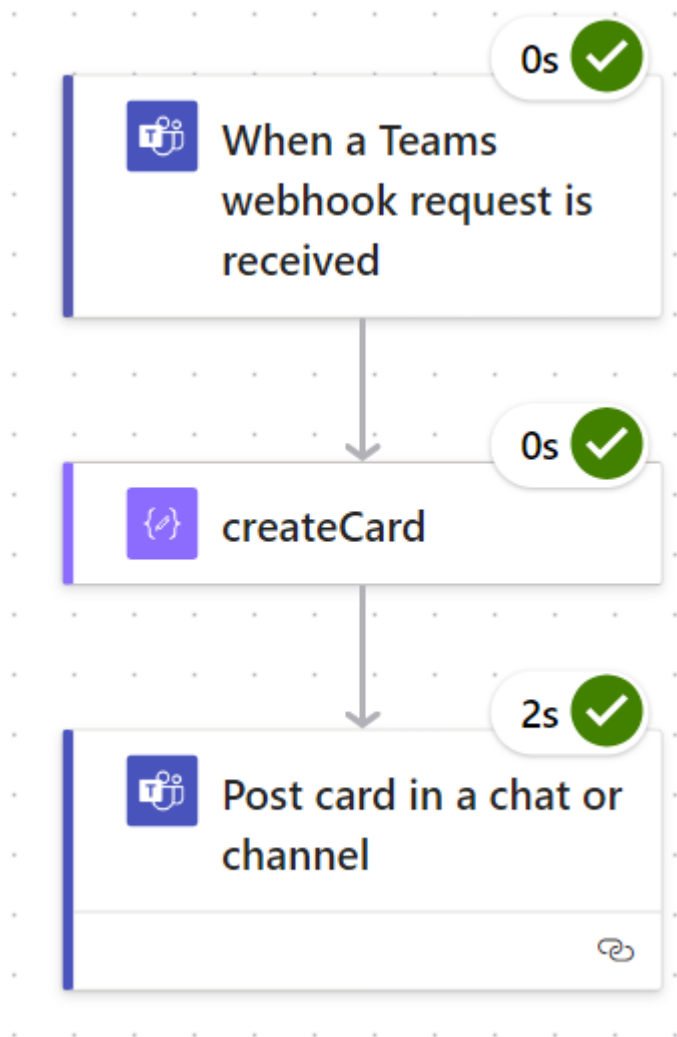
## Teams Workflow

Using the default Teams Workflow that was created failed because evidently the suggested content from Mezmo wasn't correct. I'm sure there's a way to craft the message properly straight from the Mezmo configuration so you can use the default Teams Workflow, but I haven't figured it out yet.

Instead, I went down the path of customizing the workflow in Power Automate and leveraging Compose to create the card I wanted (or at least as close as I've been able to get so far) with the data I'm sending from Mezmo via the Webhook.

## Power Automate Workflow Edit

The screenshot below is the basic workflow.



## Compose: createCard

JSON Parameters

```
{
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
  "version": "1.4",
  "type": "AdaptiveCard",
  "body": [
    {
      "type": "TextBlock",
      "size": "Medium",
      "weight": "Bolder",
      "id": "Title",
      "text": "@{triggerBody()?['title']}"
    },
    {
```

```
"type": "FactSet",
"facts": [
  {
    "title": "Summary",
    "value": "@{triggerBody()?['summary']}"
  },
  {
    "title": "View",
    "value": "@{triggerBody()?['view']}"
  },
  {
    "title": "Host",
    "value": "@{triggerBody()?['host']}"
  },
  {
    "title": "Query",
    "value": "@{triggerBody()?['query']}"
  },
  {
    "title": "Severity",
    "value": "@{triggerBody()?['level']}"
  }
],
{
  "type": "TextBlock",
  "id": "Line",
  "text": "Line: @{triggerBody()?['line']}",
  "wrap": true
},
{
  "type": "Container",
  "items": [
    {
      "type": "TextBlock",
      "text": "Click to see all lines",
      "weight": "Bolder",
      "size": "Medium",
      "color": "Accent"
    },
  ],
}
```

```

{
  "type": "ActionSet",
  "actions": [
    {
      "type": "Action.ToggleVisibility",
      "title": "Show Details",
      "targetElements": [
        "AllLinesExpanded"
      ]
    }
  ],
},
{
  "type": "Container",
  "id": "AllLinesExpanded",
  "isVisible": false,
  "items": [
    {
      "type": "TextBlock",
      "text": "@{triggerBody()?['lines']}",
      "wrap": true
    }
  ]
}
],
},
{
  "type": "TextBlock",
  "id": "URL",
  "text": "[Link to logs](@{triggerBody()?['url']})",
  "wrap": true
}
]
}

```

## Resulting Teams Card



via Workflows 3:55 PM

### Mezmo - User account alert

Summary: 1 line(s) matched in Test View. Security level: info

**View** Test View

**Host** Test View

**Query** Test View

Line: After matching at least 1 line in a 30 second period, we'll send an alert to this email with all the matched lines

[Click to see all lines](#)

Show Details

[Link to logs](#)

-end

Revision #4

Created 10 October 2024 20:58:24 by bluecrow76

Updated 10 October 2024 21:25:19 by bluecrow76