Microsoft Sentinel new incident UI

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

Link to a great demo : https://youtu.be/dCn-FfU0Mtg

- Toggle to another version of the incident page

1. The customer would like to revert to the previous page / new page.
2. There's a toggle in the banner at the upper side of the incident page. It's persistent.
3. If customer can't find the banner to toggle between experiences - ask customer to refresh / clear cache
4. It's very important for us to know why customers would like to use the old page. It'll help with migration

- Comments

1. Comments can't be found (in the previous incident page they had their own tab) - comments can be found in the activity log, triggered by the "activity log" button right next to "tasks". To see only comments, the customer can filter in the log.

2. When comments are typed very fast, the page sometimes returns to resources page. This is a known bug. Happens only in rare occasions.
   Raise CRI if happens.

- Tasks

1. Tasks is a different feature, please refer to documentation - Work with incident tasks in Microsoft Sentinel | Microsoft Learn

- Activity log

1. The customer made a change to the incident, but it doesn't yet appear in the activity log.

2. It may take up to 30 seconds for the log to update due to LA query time.

3. validation of base64 img not working as expected - Known bug. Raise ICM.

4. Customer can't delete a comment - Due to user's insufficient permissions or Workspace lock. Appears in documentation.

5. Links in comments try to open inside Sentinel and get an error - Customers should make sure the following parameter is part of the link: target="_blank". Example:

https://www.bing.com
This also applies to existing playbooks. Appears in documentation.

- Delete incident

1. Incident can't be deleted - Might be permissions, Workspace lock or Defender M365D incident. Refer to the delete incident documentation - Work with incident tasks in Microsoft Sentinel | Microsoft Learn

- Pivot to entity pages

1. How to pivot to an entity page? (change from current experience)

To pivot to the entity page, the customer needs to select the entity in the entities tab and choose “view full details”, or click the entity’s name in the grid.

- Entity actions

1. Customer doesn’t have an option to add an entity to TI.

Only specific entities can be added to TI. For others, the option won’t exist. Appears in feature’s documentation.

2. Customer doesn’t have an option to run a playbook on an entity.

There are no playbooks deployed in the workspace for this type of entity.

- Entity selection

1. When I click an entity in the entities widget in the overview, the customer is sent to the entities tab but the entity is not selected in the entities grid.

Known bug.

When the entity is lower in the entities grid’s list, and scroll is needed, it might seem it’s not selected. It is selected however, and the right panel will show its details in the entities tab. If the customer will scroll down they will see it.

- Timeline

1. Customer can’t delete an alert from the incident. Alerts from M365D can’t be deleted.

Refer to delete incident documentation - [Work with incident tasks in Microsoft Sentinel | Microsoft Learn]

- Timeline

1. Dark mode issues in the filter - Known bug.

- Similar incidents

1. Can’t change columns width sometimes. Known bug. Hover over the field to see the entire text of the column

2. The link in the info balloon in the similarity reason sometimes loses focus when it's clicked. So after one click somewhere in the tooltip, the link click is closing the tooltip and not triggering the link button. Ask customer to refresh. This is a Know bug.

- Top insights

1. An error message in top insights - This means that two things happened simultaneously:

1.1. No top insights.

1.2. One of the tables required for the top insight (usually UEBA) isn’t activated in the workspace.

If this is not the use case, open a CRI.

2. Customer has entity insights in the entity page but no top insights.

The timeframe for entity page insights is different (in the incident page, it's 24 hours prior to first alert until last alert). Exists in documentation.

3. Columns is chart can't be resized sometimes. This is a Known bug.

4. Entities tab shows entity insights with no results and the top insights panel doesn't.

By design. Top insights are only ones with results.

Appears in documentation.

- Entities tab

1. Customer has entity insights in the entity page but no entity insights in the entities tab

The timeframe for entity page insights is different (in the incident page, it's 24 hours prior to first alert until last alert).

Appears in documentation.

2. Entity timeline is different than entity page.

The time frame is different. Timeline in entities tab is 7 days.

Appears in documentation.

Time frame appears in the entity's timeline in the entities tab.

3. Columns in insights charts can't be resized sometimes.

Known bug.

- Incident actions

1. Customer can't find incident actions (run playbook on incident, create automation rule, create Team, view Team details).

They are now located in the "incident actions" menu at the top right, above top insights.

Appears in documentation.

Used to be in the details panel.

- Incident workbook

1. Some rare edge cases when it doesn't open properly.

Please raise CRI with configurations of Sentinel and browser so we can investigate.

- Logs in context experience

1. No export table

Known.
exists in the full-page experience.

Please raise FR.

2. No “open in a new tab”

Known.
exists in the full-page experience.

Please raise FR.

3. Bookmark is created but doesn’t appear in the incident

When creating a bookmark in the Logs panel, there are two buttons: “create bookmark” and “create bookmark in current incident”. Customer needs to select the correct option.