sumo logic

Cloud SOAR Fundamentals

Student Lab Guide

Rev 04.23.25.K

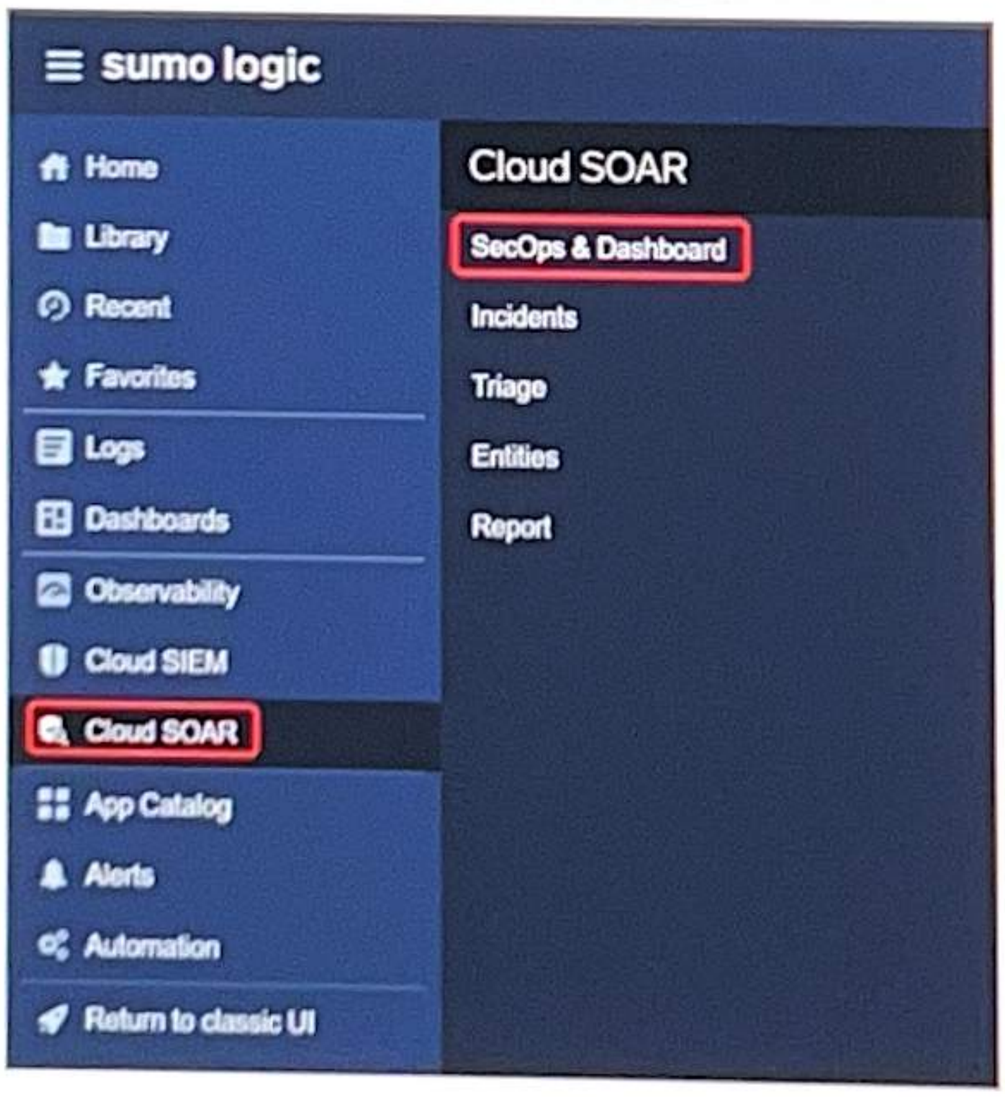
sumo logic

Table of Contents

sumo logic

Lab 0: Log in to the training environment

The training lab environment is separate from your other accounts. To access the training lab environment:

1. Open a new browser tab.
2. Go to https://service.sumologic.com.
3. Enter **training+analyst###@sumologic.com** in the **Email** field. Replace ### with a three digit number between 000 and 999.
4. Enter the **Password** provided to you by your instructor or listed on the front page of the Sumo Logic training site.
   Note: The password changes monthly.
5. In the left navigation menu, click **Cloud SOAR > SecOps & Dashboard** to go to the Cloud SOAR training environment.
6. 

Note: The training environment is a **shared, dynamic environment.** The data is refreshed and cleaned periodically. Other students can see the comments you make, so be careful what information you share. The dynamic updates and activities of other students may affect the data you see. Your experience will vary from one session to the next.

sumo logic

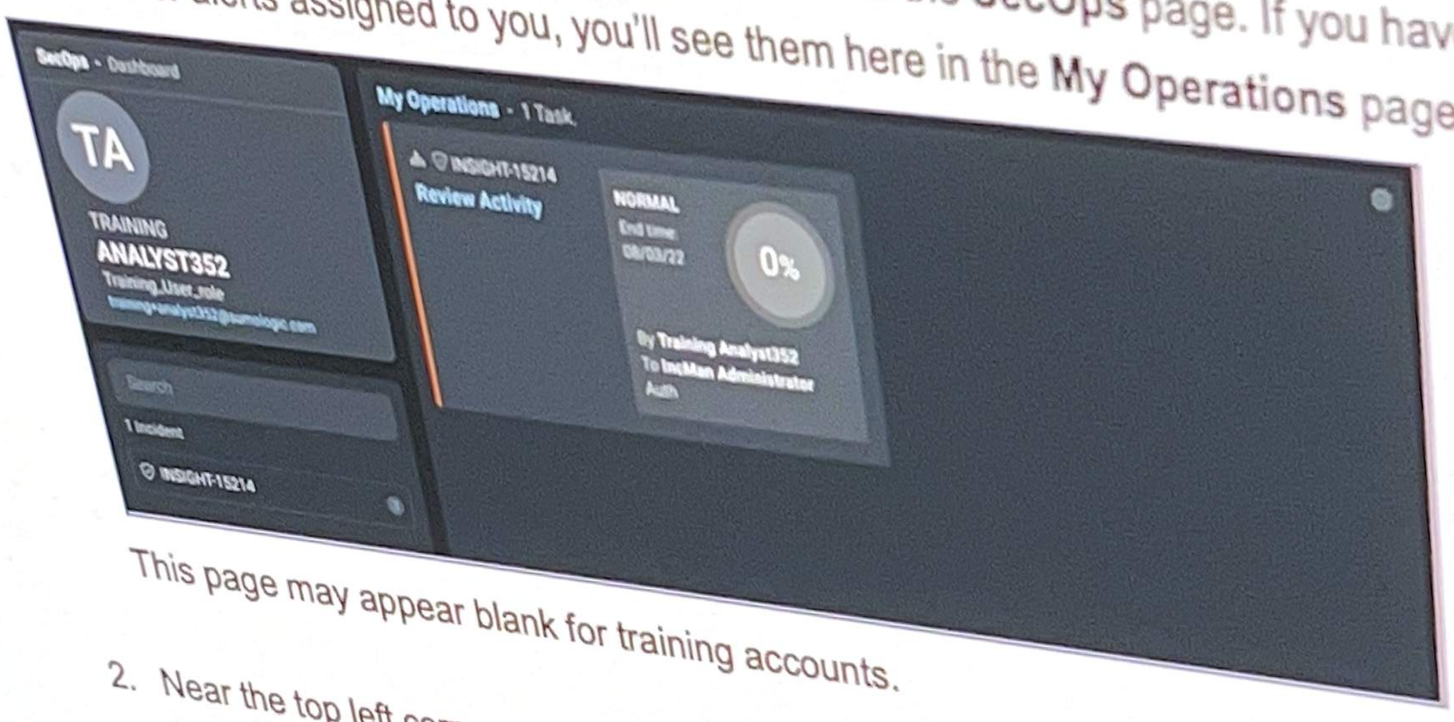
sumo logic

Lab 1: Explore the Cloud SOAR UI

In this lab, you'll get to know the different parts of the Cloud SOAR UI.

Navigate to the Cloud SOAR UI if you're not already there. Refer to Lab 0 if you need help.

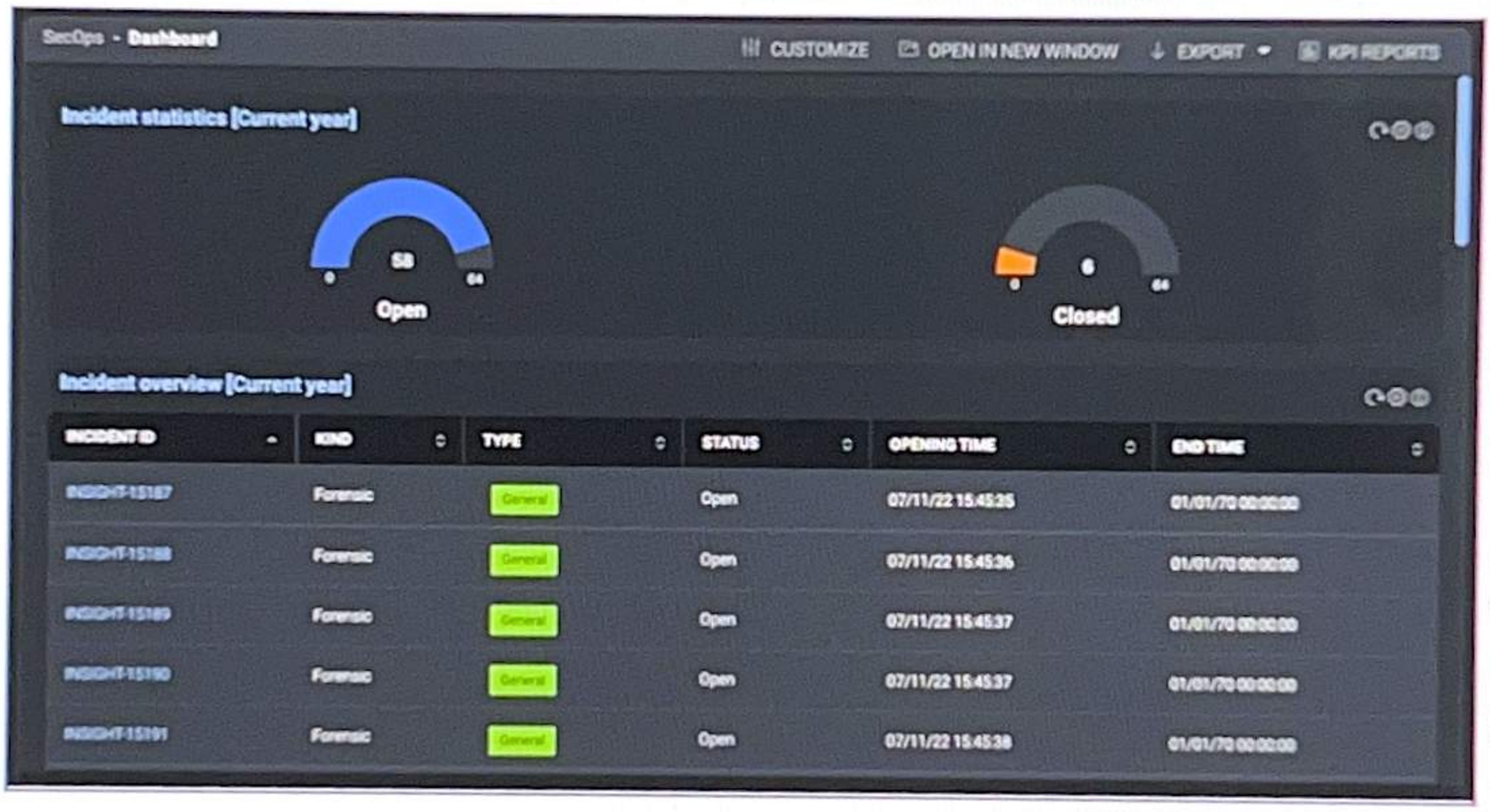
1. When you first log in to Cloud SOAR, you'll be taken to the **SecOps** page. If you have any tasks or alerts assigned to you, you'll see them here in the **My Operations** page.



This page may appear blank for training accounts.

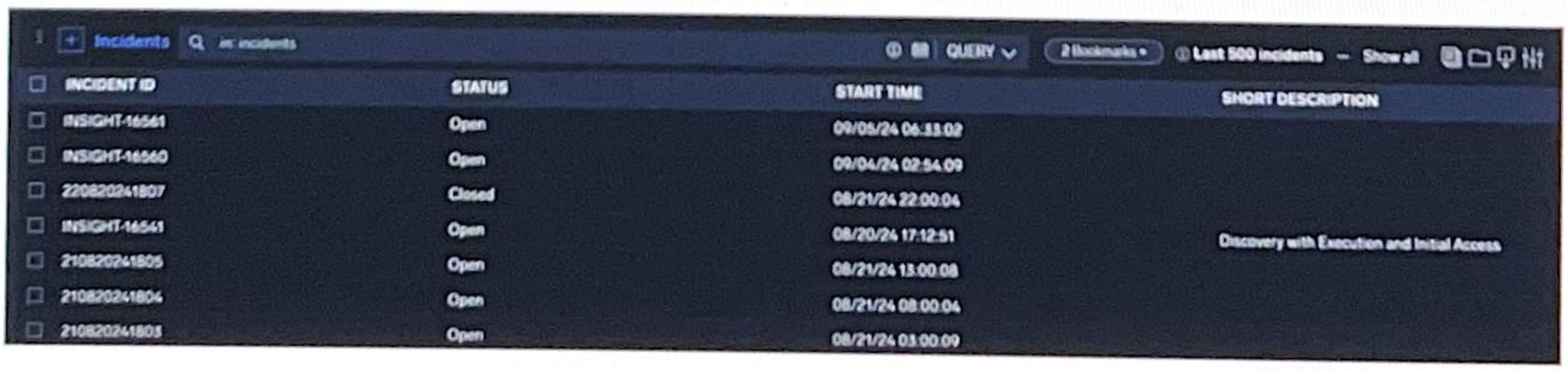
2. Near the top left corner, above your user name, click **Dashboard**.

This will take you to your main dashboard page for your organization.



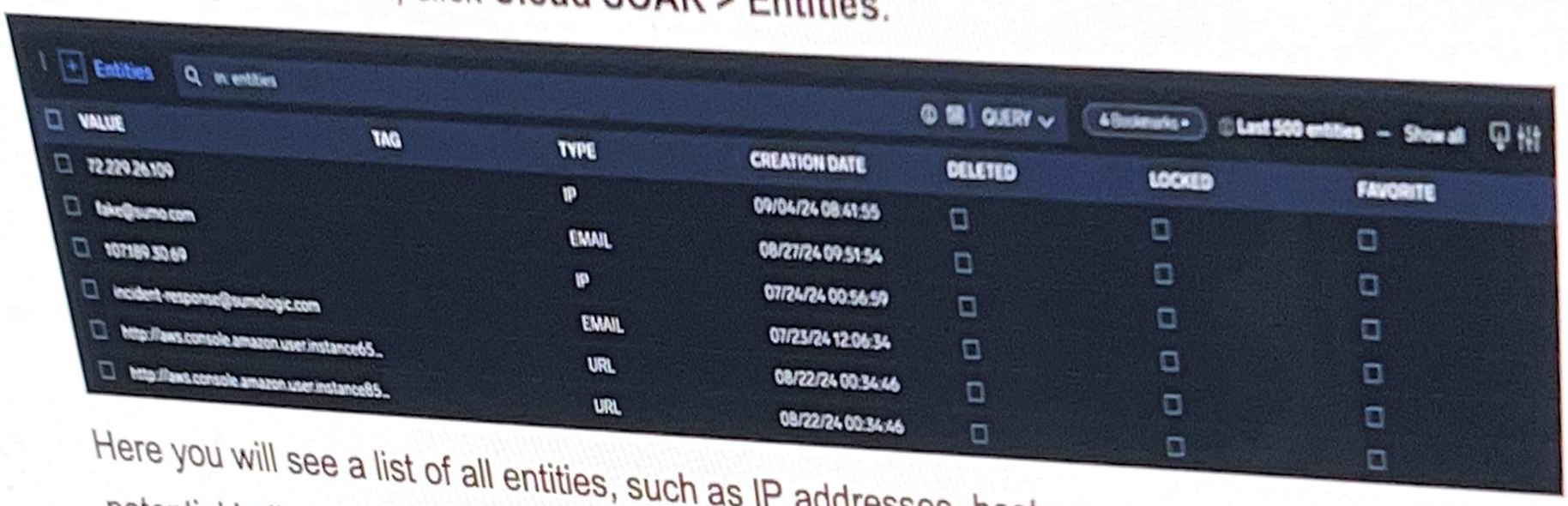
Here you'll see a custom dashboard composed of individual "widgets" with system data in graph or table form. For instance, you may see an overview of current active incidents as well as statistics for all recent incidents. If your default dashboard is empty, that just means the training account you are using doesn't have any default dashboard widgets defined. We'll learn how to create widgets and customize this area in a later lab.

3. In the left navigation menu, click **Cloud SOAR > Incidents**.



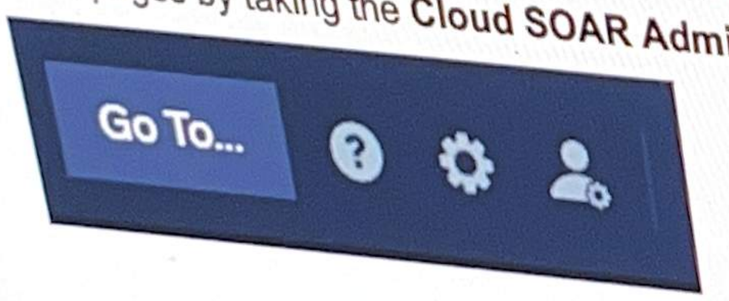
Here you'll see a list of all incidents for your organization. You can filter by various categories and search terms. For example, if you click **Mine** (under the **Bookmarks** button in the upper right) you'll only see incidents that have been assigned to you specifically. (Note that by default the training accounts will likely have no assigned incidents so the Mine view will be blank)

4. In the left navigation menu, click **Cloud SOAR > Entities**.



Here you will see a list of all entities, such as IP addresses, host names, and other potential indicators of compromise. **Entities** are unique identifiers that can help you figure out who the potential threat actors are. Like the Incidents page, you can use filters and queries to sort through the Entities in Cloud SOAR.

5. The Configuration and Administration icons in the upper right of the interface contain other menu options that are generally used by administrators. You can learn more about these pages by taking the **Cloud SOAR Administration** course.



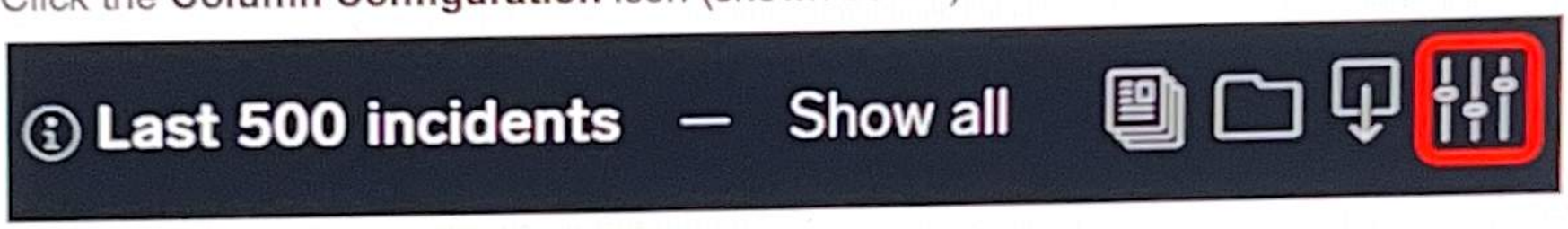
sumo logic

Lab 2: Investigate an incident

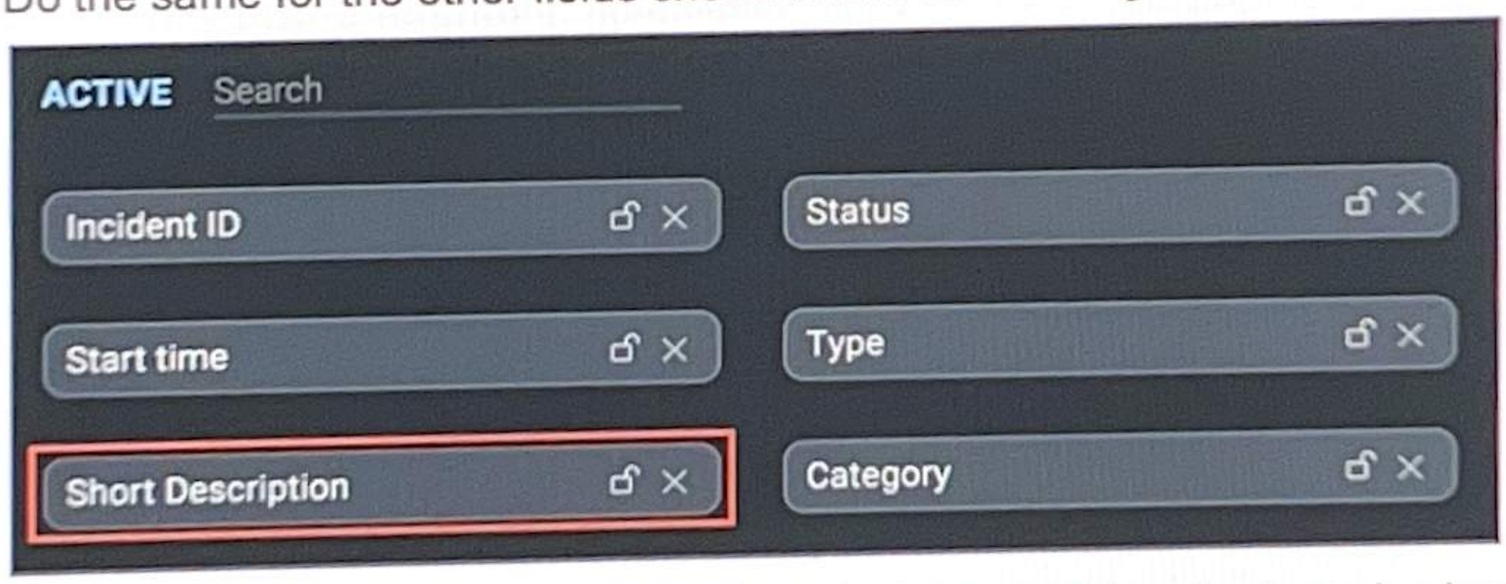
In this lab, you'll investigate an alert, gather information, and decide what to do in response to it.

Navigate to the Cloud SOAR UI if you're not already there. Refer to Lab 0 if you need help.

1. In the left navigation menu, click **Cloud SOAR > Incidents**.
2. Click the **Column Configuration** icon (shown below).

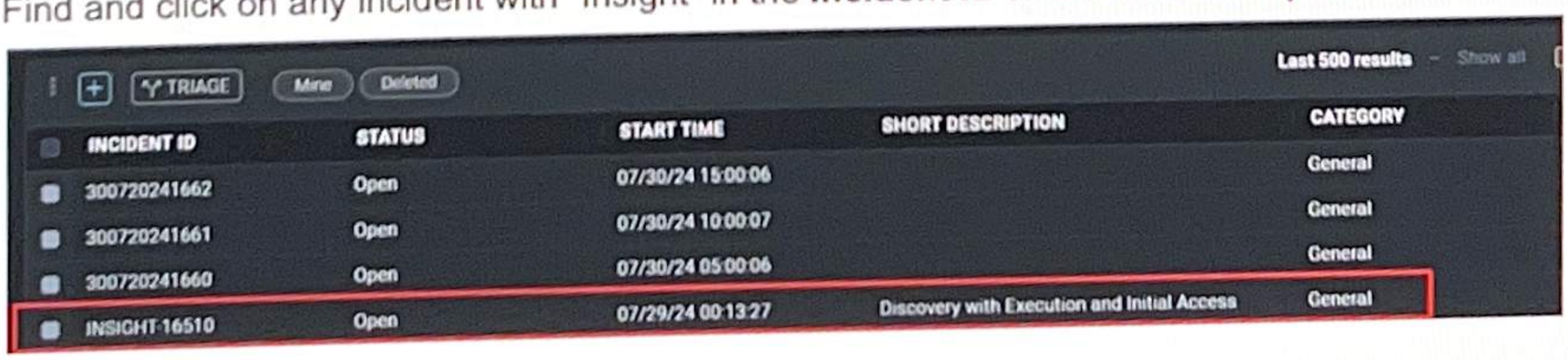


3. In this view, you can adjust the display to show the data fields you are interested in. Check whether **Short Description** is listed on the left side under the **Active** column. If it isn't, click the **+** next to **Short Description** in the **Available** column.
4. Do the same for the other fields shown in the below image. Then click **Apply**.

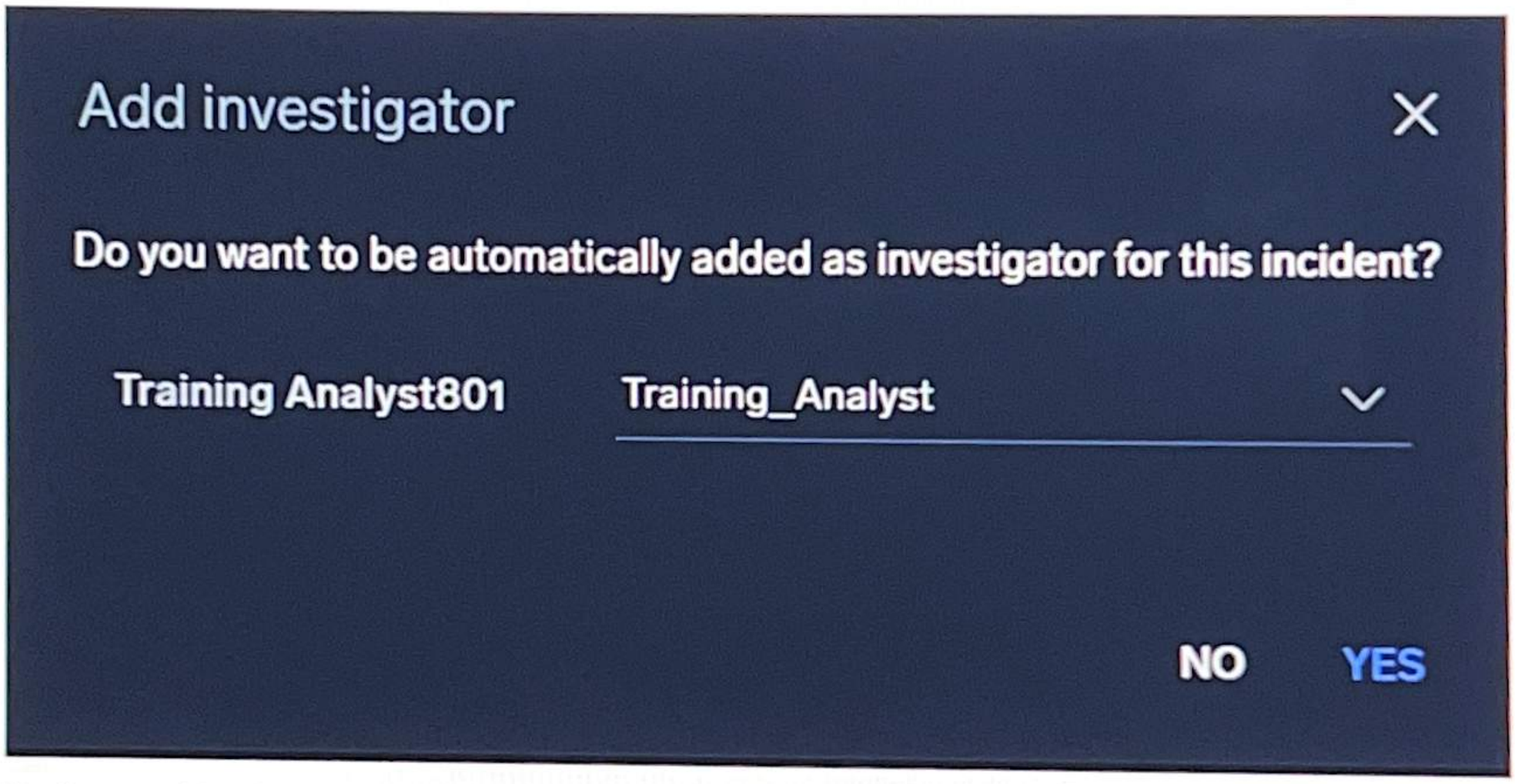


You'll now see incident records displayed with the additional selected columns visible. Some incidents will now show a short description based on the MITRE ATT&CK framework along with a category and type.

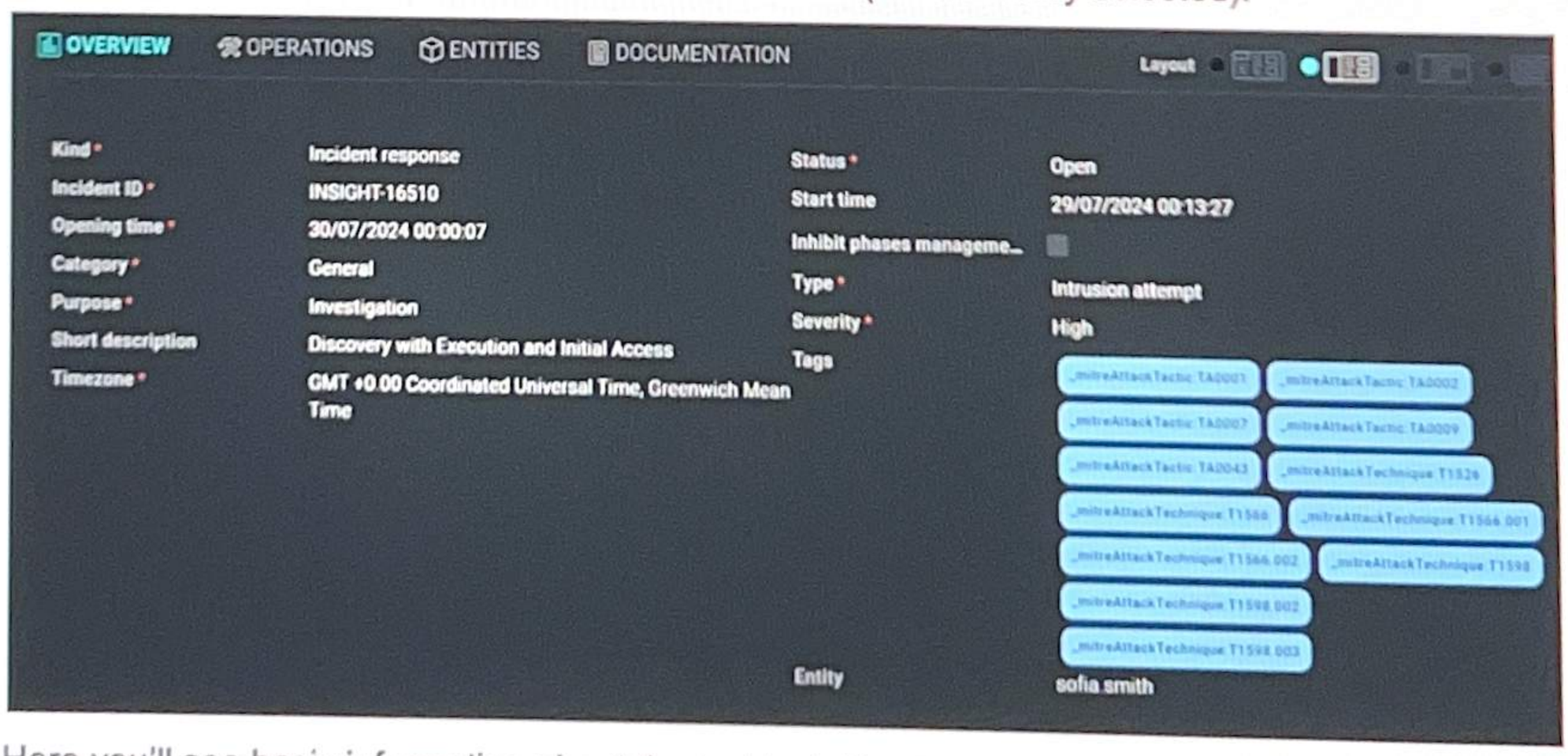
5. Find and click on any incident with "Insight" in the **Incident ID** and a status of **Open**.



6. When you select the incident, a popup will appear asking to add a user as an "investigator". Select **Training_Analyst** from the drop-down, then click **Yes** to add yourself as an investigator.



7. On the resulting incident view, click the **Overview** tab (if not already selected).

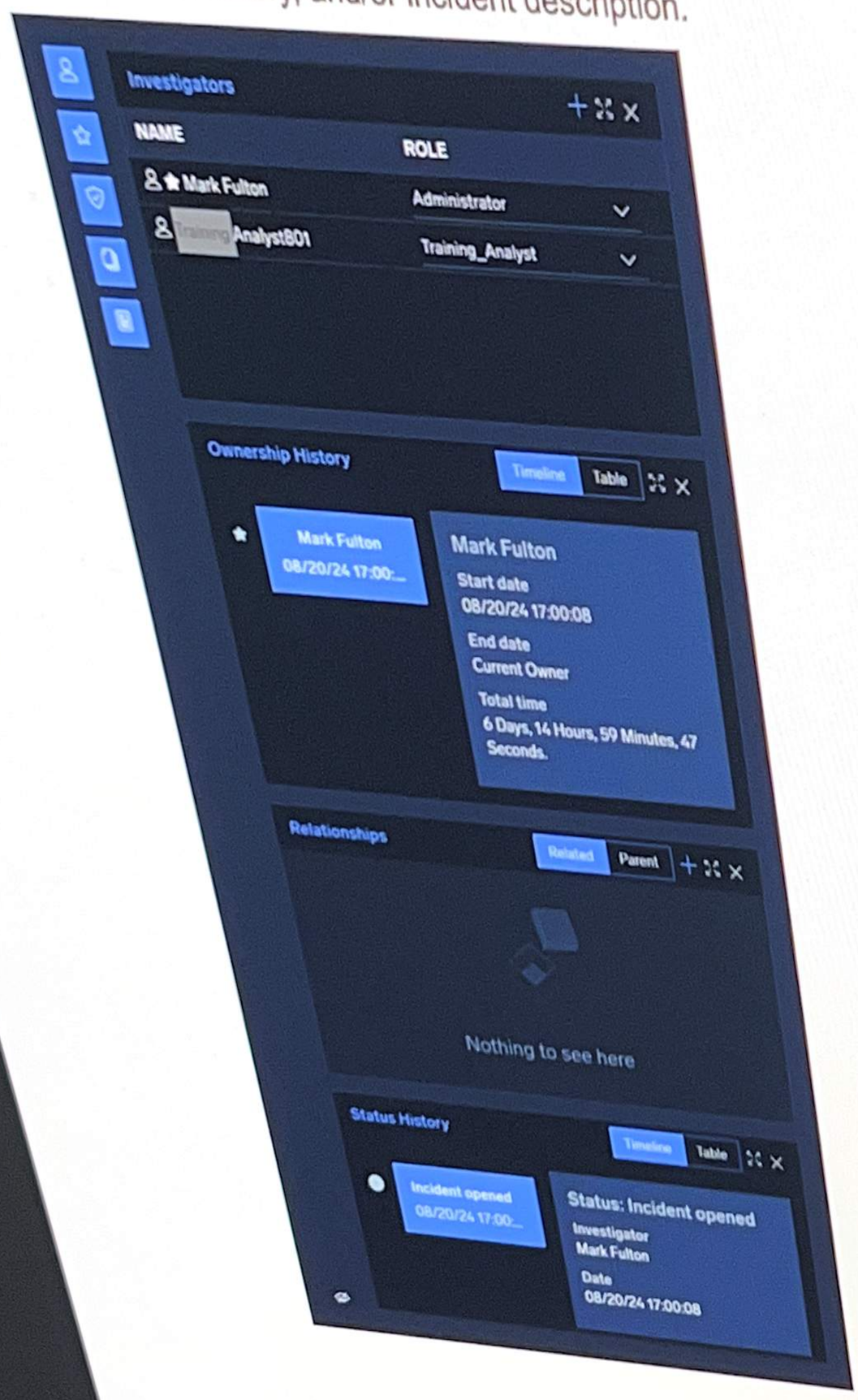


Here you'll see basic information about the incident, like the entities involved in the incident and the time the incident was opened. This incident was imported from Sumo

sumo logic

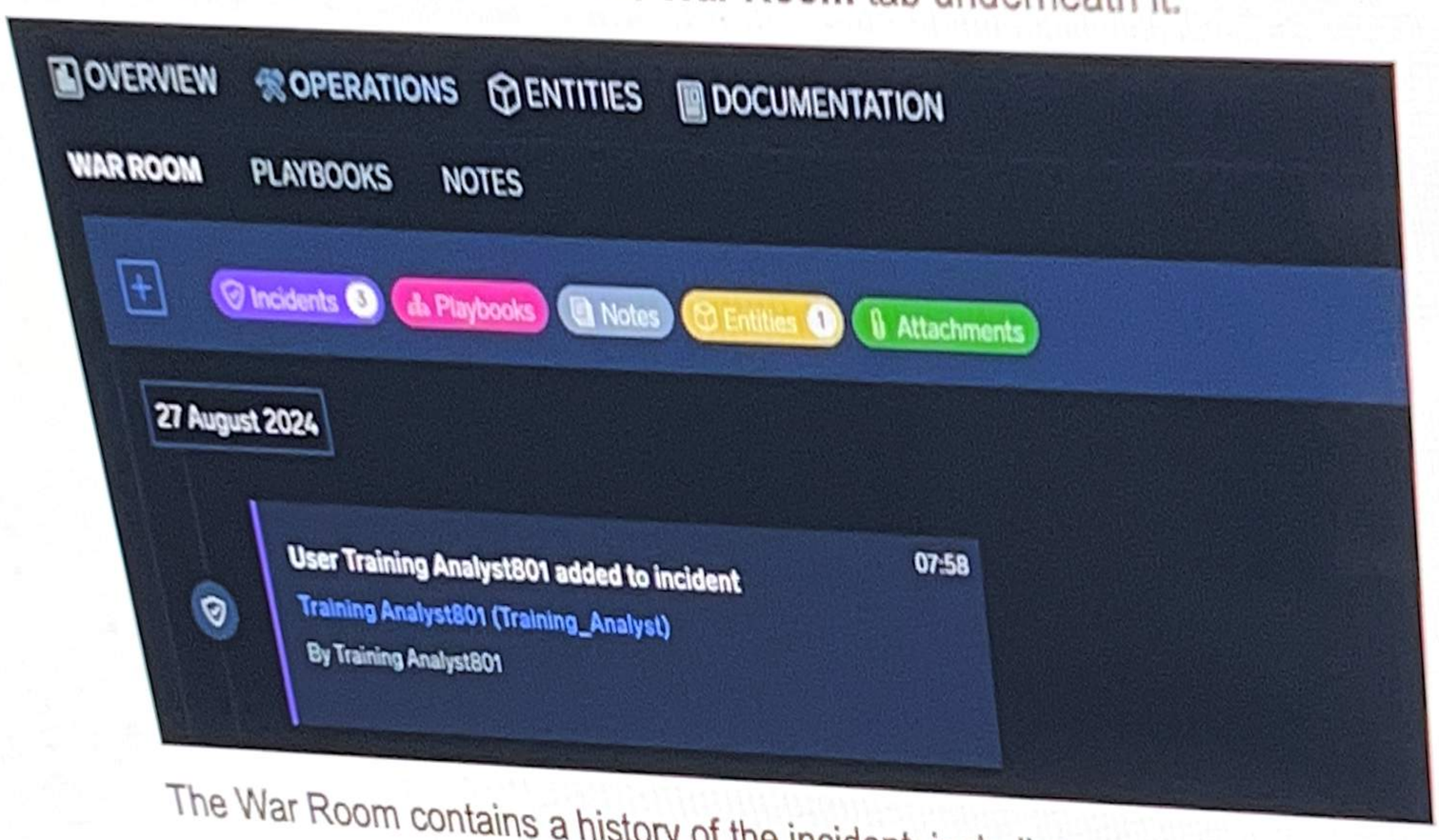
Logic Cloud SIEM, so it contains the Cloud SIEM incident ID as well as a short description and tags based on the MITRE ATT&CK framework.

8. On the right side of the Overview tab you can click on any icon to open up a sidebar with various widgets, showing the list of investigators, ownership history, relationships, incident status history, and/or incident description.



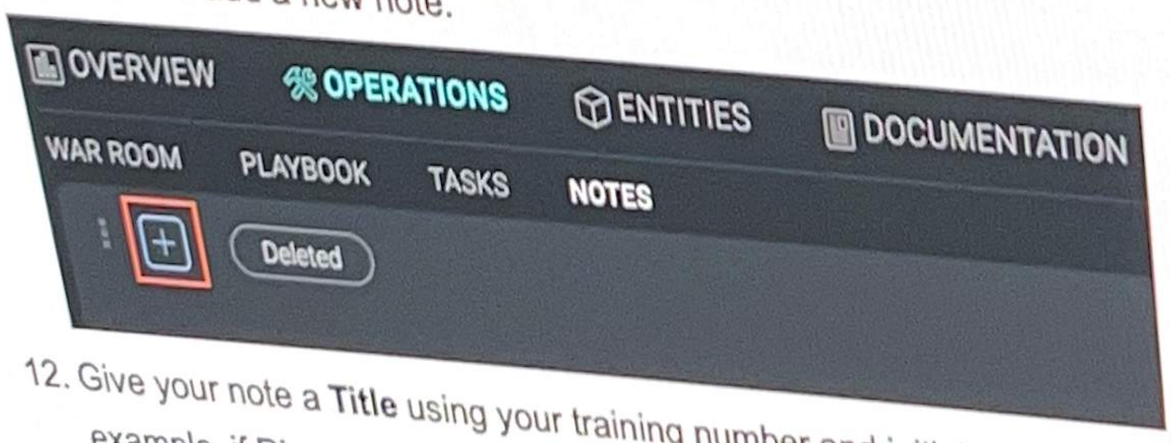
sumo logic

9. Click the **Operations** tab, and click the **War Room** tab underneath it.



The War Room contains a history of the incident, including any tasks and investigators that have been assigned, playbooks that have been executed, entities that are being tracked, and any other notes or attachments.

10. Under the **Operations** tab, click **Notes**.
11. Click the **+** to add a new note.



12. Give your note a **Title** using your training number and initials as a unique identifier. For example, if Riya Singh used account training+analyst321, she would use "RS 321" as a unique identifier.
13. You can optionally add one or more tags in the **Tag** field. Add a **Date of creation** using the date picker. You can choose today's date.
14. Type a few sentences in the **Description** field. You can describe the event in detail, and/or make suggestions about the next steps to resolve the incident.
15. Click **Create** to save your note.

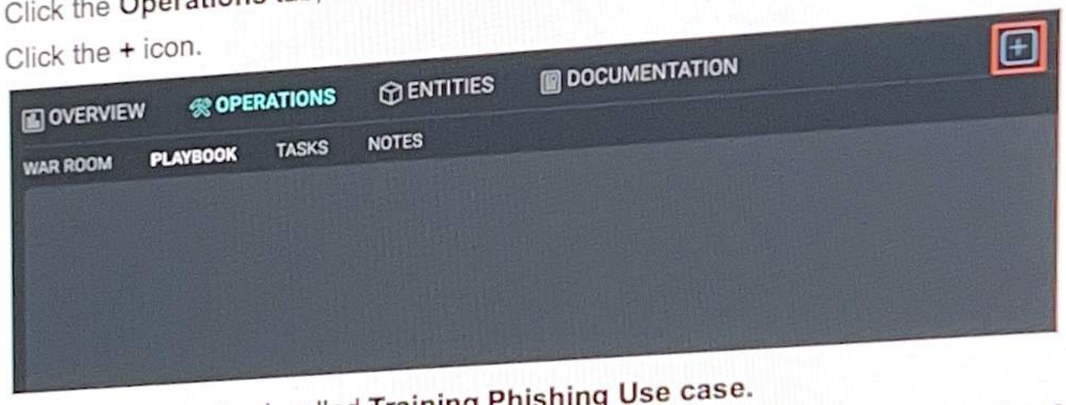
sumo logic

Lab 3: Respond to an incident

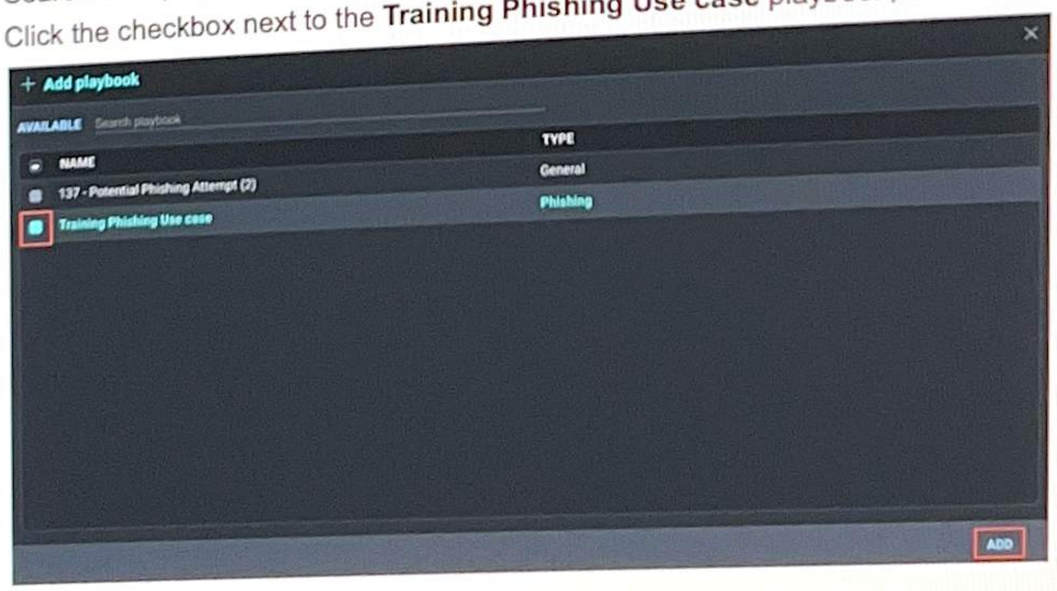
In this lab, you'll respond to the incident you investigated in Lab 2.

Navigate to the Cloud SOAR UI, if you're not already there. Refer to Lab 0 if you need help.

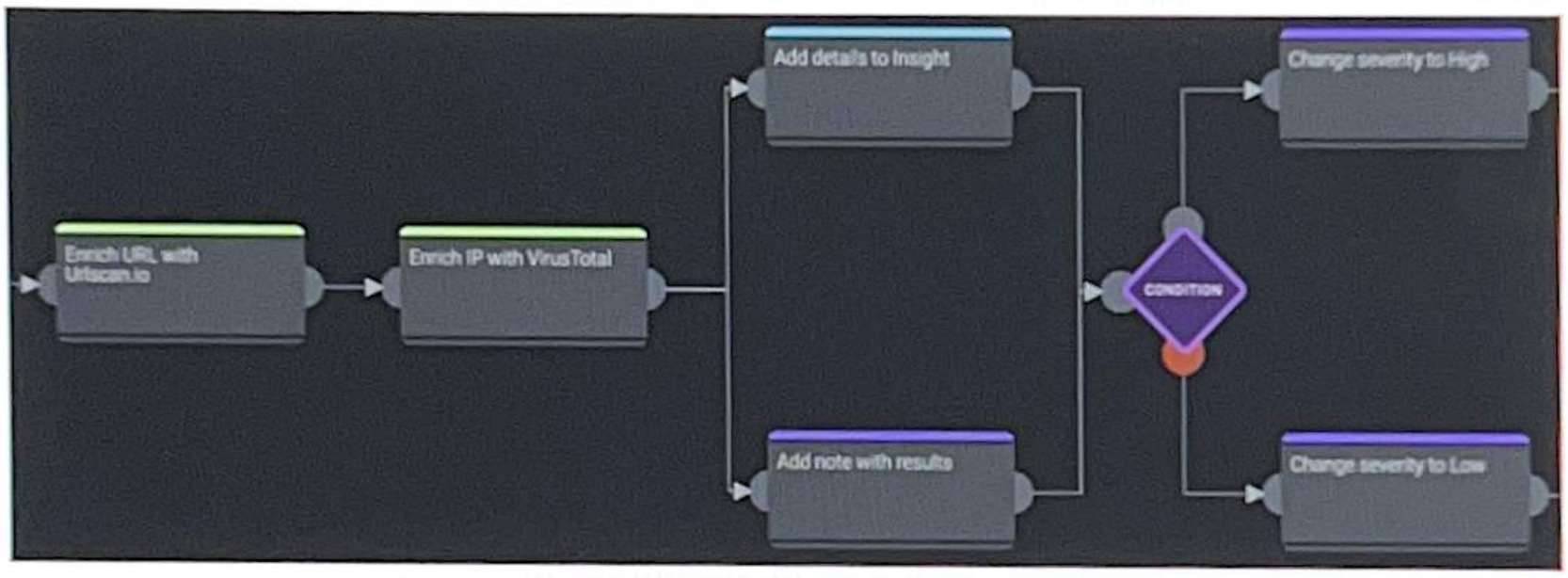
1. Return to the incident details view for the incident you chose from Lab 2.
2. Click the **Operations** tab, then click **Playbook**.
3. Click the **+** icon.



4. Search for a playbook called **Training Phishing Use case.**
5. Click the checkbox next to the **Training Phishing Use case** playbook, then click **ADD**.



6. You can drag the playbook flowchart around and use scroll to zoom in and out on the different pieces. You can also click each node to find out more about it. Take a moment to explore the playbook and familiarize yourself with it.

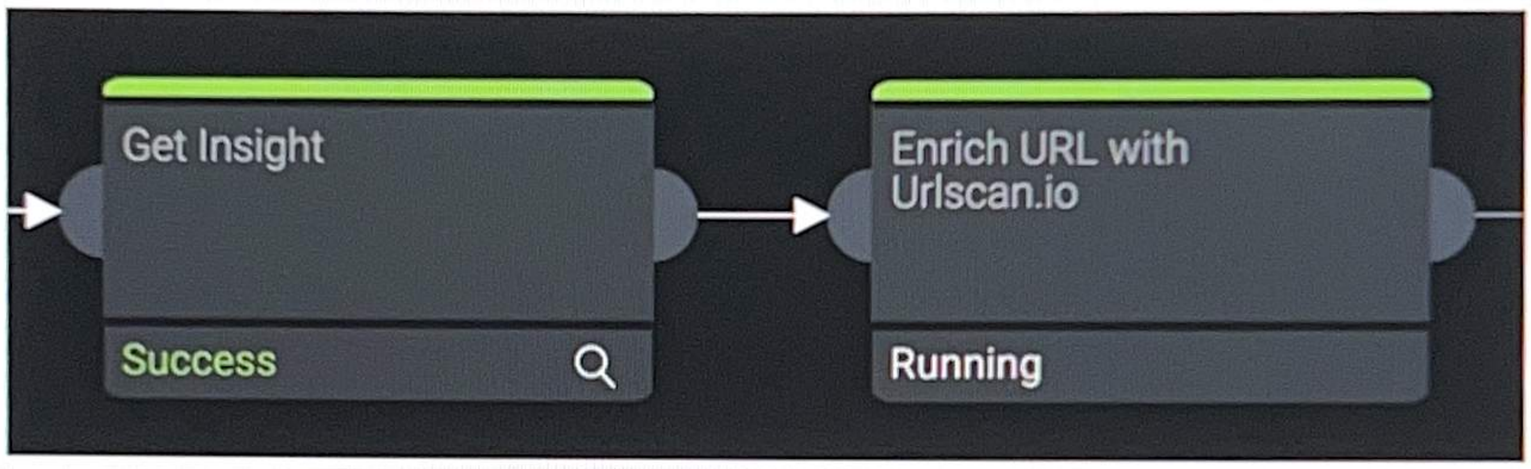


This playbook checks information from the Cloud SIEM Insight, then enriches it with threat intelligence information from Urlscan.io and VirusTotal. Then, it adds notes with the results of these enrichments to both the Cloud SIEM Insight and the Cloud SOAR Incident. Next the playbook uses a condition based on the score of the scan: if the score is above 0, the severity is changed to High and a task to review is assigned to a SOC Analyst. If the score is 0, the severity is changed to Low and the incident is closed.

7. Click **Run (play button icon)** at the bottom.

Note: If you do not have the option to add or run a playbook, the Incident may be closed. Click **Reopen Incident** in the bottom left of the Incident page. Once the Incident is open again, you should be able to run the playbook.

8. Watch the playbook run.
    - The playbook may take several minutes to run. You can track its progress by looking for green “Success” messages at each step.



    - Pay attention to whether the Incident is escalated to High or deescalated to Low severity after the Condition step.
9. Verify that the playbook ran successfully.
10. Click the **Notes** tab. You should see a new note based on the playbook’s results.

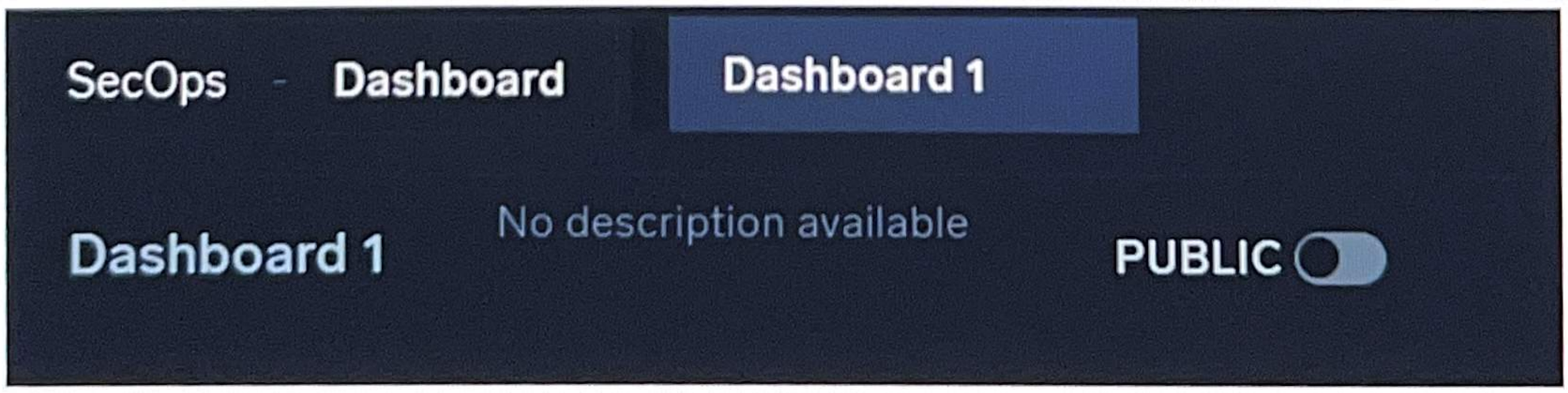
Lab 4: Customize a dashboard

In this lab, you'll create and customize a dashboard using widgets.

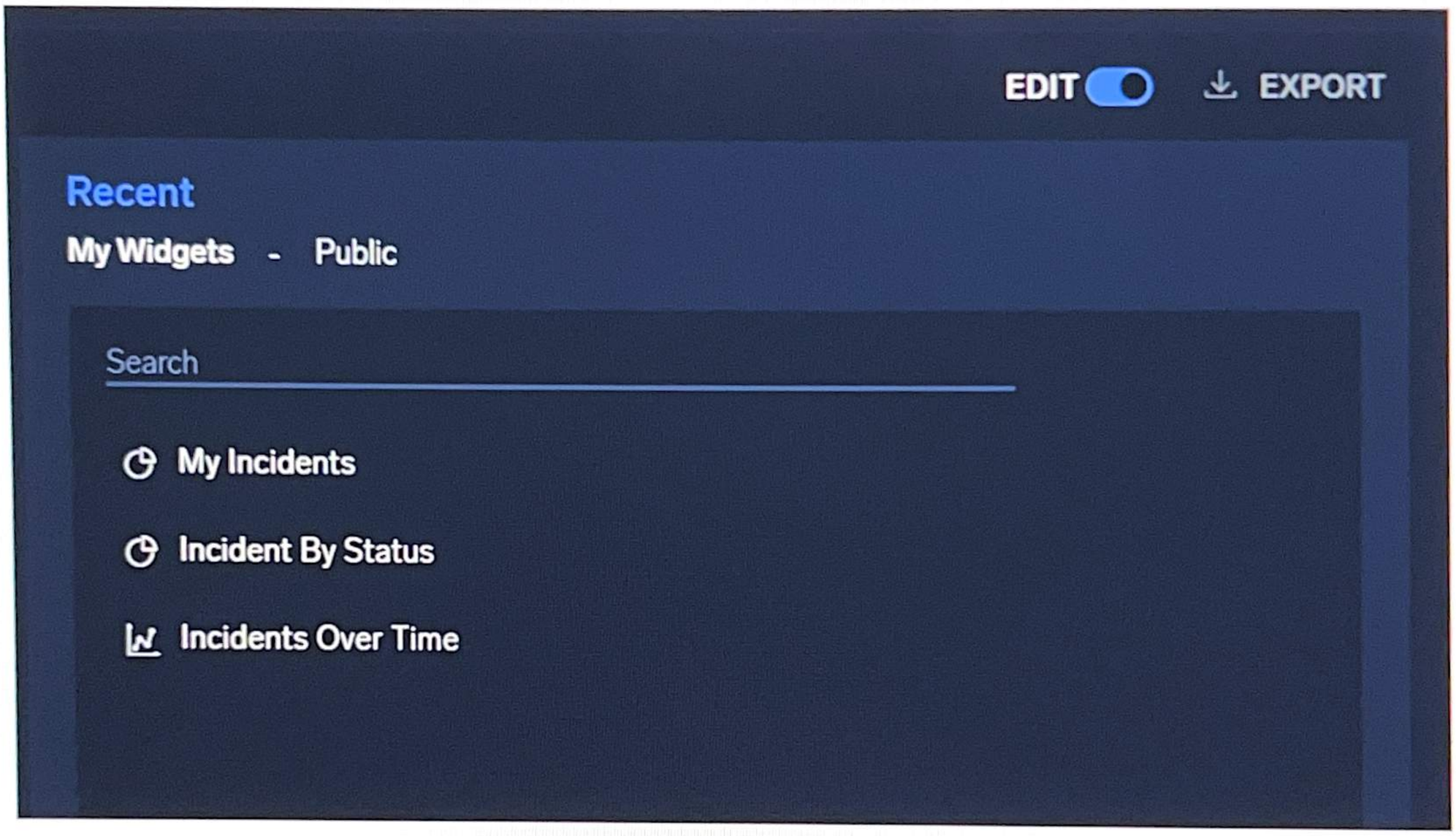
1. In the left navigation menu, click **Cloud SOAR > SecOps & Dashboard**. Then (if not already defaulted there) click the "Dashboard" link in the top left of the SecOps view.

2. Click the 'plus' icon in the upper right, then select "New Dashboard".

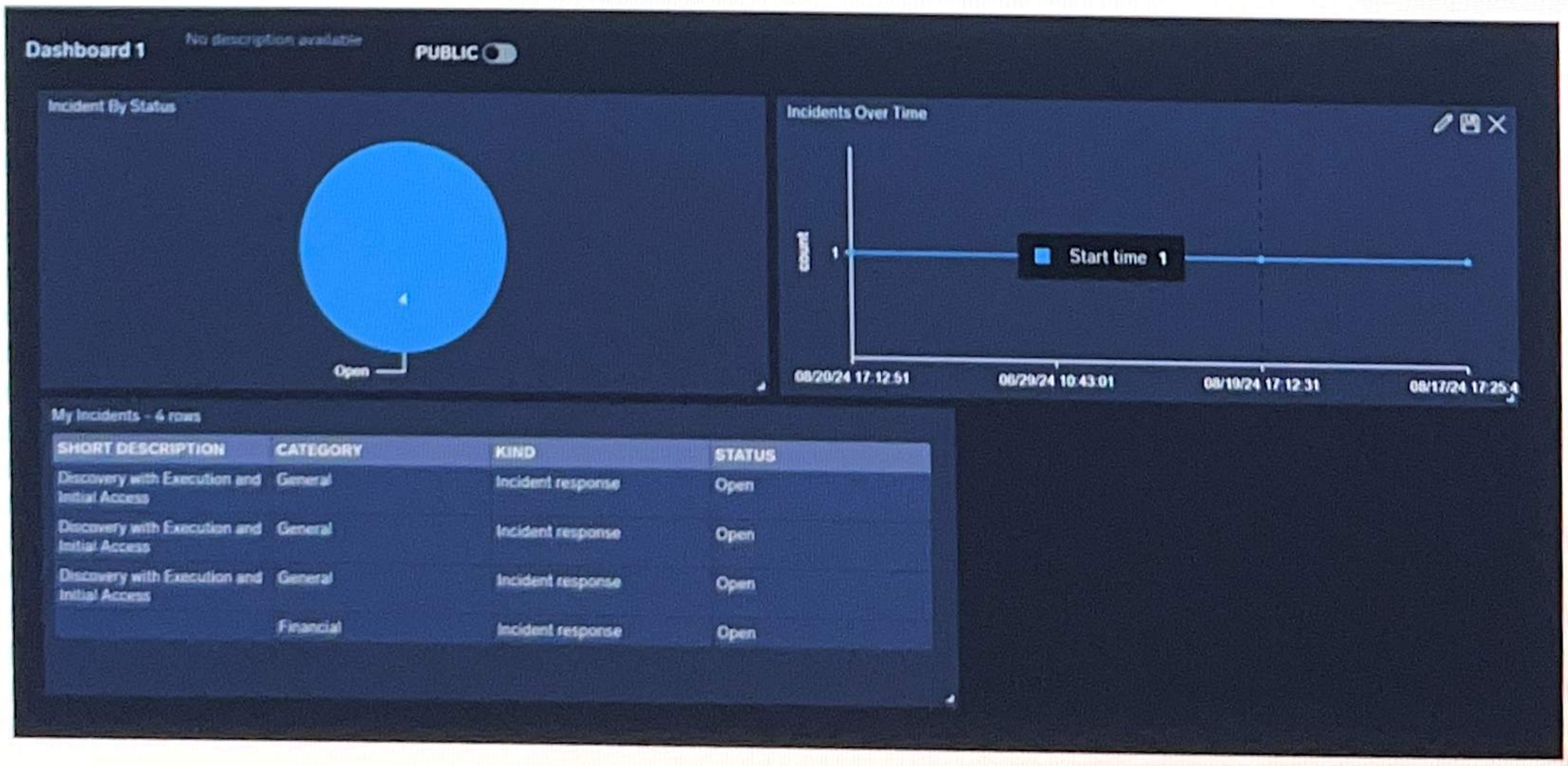
3. Click on the default dashboard name ("Dashboard #") below the tab row and change the name to include your initials or chosen ID number. Add a description if desired by clicking on the "No description available" field and adding text.



4. In the top right corner, click the **Edit** control to enter edit mode.



5. Click on one or more widgets from the edit sidebar to add the widget to your dashboard. Note that you can drag and place the dashboard widget in different places and arrangements on the dashboard screen.



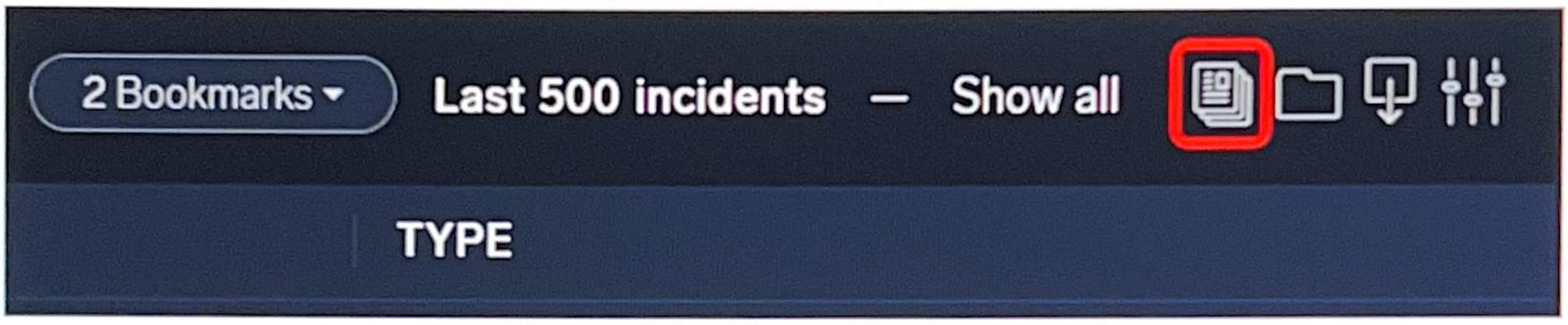
6. Click “New” in the edit sidebar to create a new widget.
7. Enter a widget name “Incidents By Type XXX”, using your initials or chosen ID in the name in place of XXX.
8. Under **Group By**, select “Type”.
9. In the left sidebar, choose the “Bar Graph” icon (second from the top).

   NOTE: If you do not see any data in your graph, you can go back and assign more incidents to your user name so your widget has more incident data to include. Or you can edit the filter on top of the widget configuration to say **"involved:false"** instead, to include incidents that are not assigned to you.
10. Click **Save** in the lower right corner.
11. Back on the **Edit** sidebar, click on your new widget to add it to your dashboard. Rearrange the rows and columns of your dashboard by dragging widgets to different locations.
12. Click **Edit** in the upper right to turn off Edit mode for your dashboard.

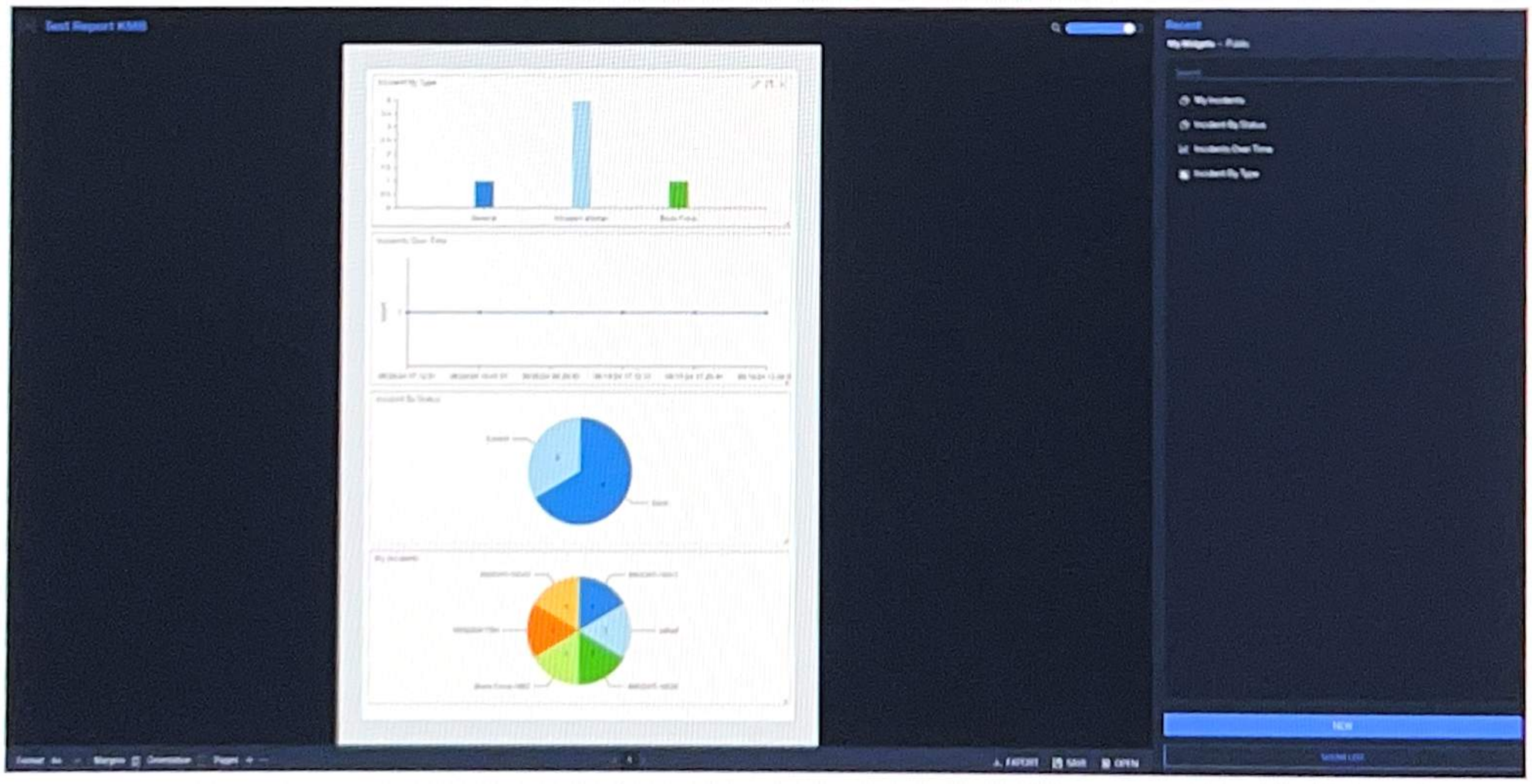
Lab 6: Create and export a report

In this lab, you'll create and export a report.

1. In the left navigation menu, click **Cloud SOAR > Incidents**.
2. Click on the "[#] Bookmarks" menu on top and select "Mine".
3. In the top right, click the **Report** icon.



4. In the Report view, you'll have a blank page view and a sidebar on the right with the available widgets (similar to the dashboard view).
5. Click on one or more of the available widgets to add them to the report. (You can create a new widget using the same process as the previous lab as well).



6. Click **Save** when you've finished creating your report. Create a name like "Test Report XXX" with your initials in place of XXX.

sumo logic

7. After saving your report, click **Export** at the bottom of the page to download your report in PDF form.