sumo logic

Cloud SOAR Administration

Student Lab Guide

Rev 10.29.24.K

sumo logic

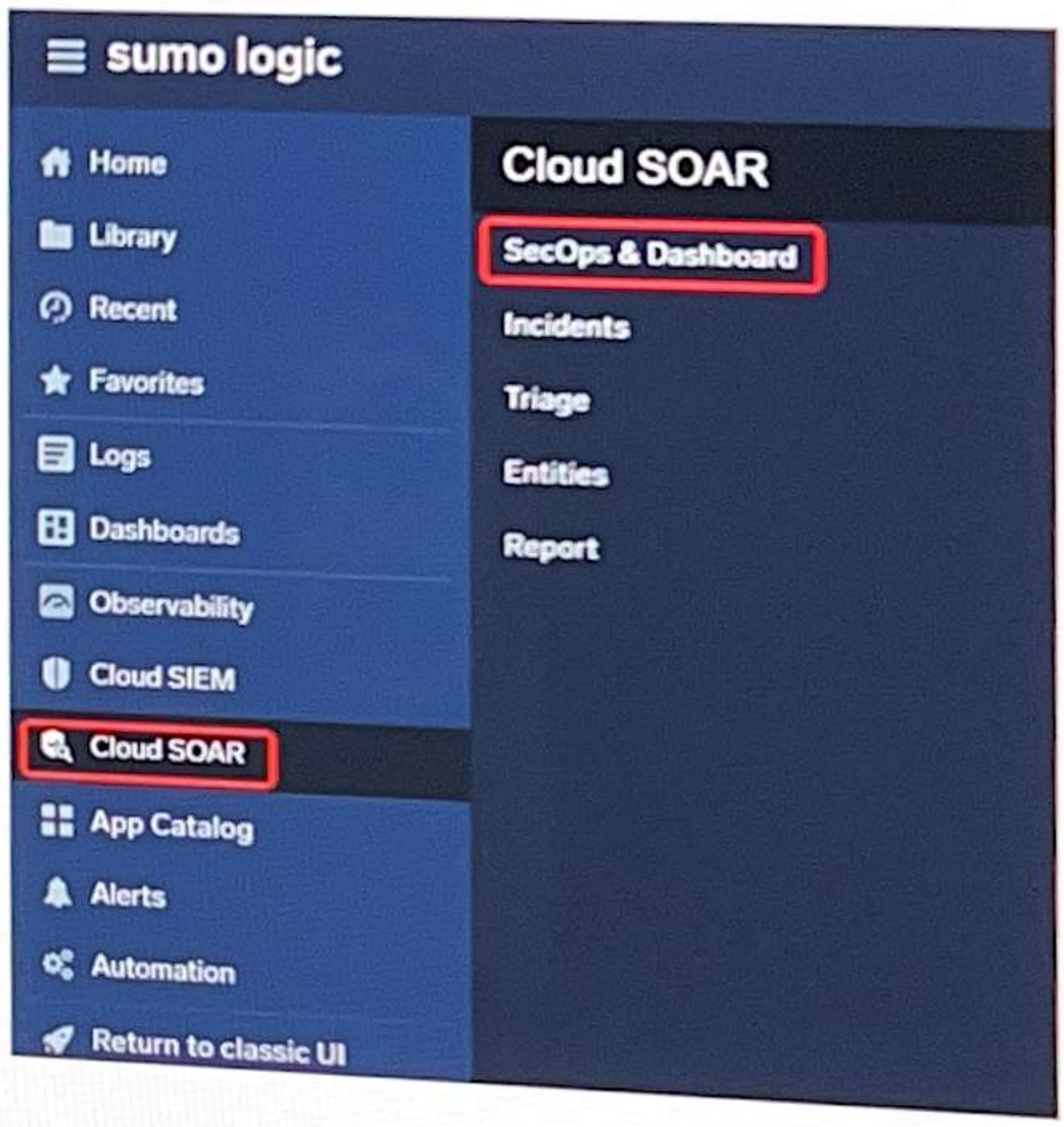
Table of Contents

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+admin###@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.
   Note: The password changes monthly.
5. In the left nav menu, click **Cloud SOAR > SecOps & Dashboard** to go to the Cloud SOAR training environment.



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

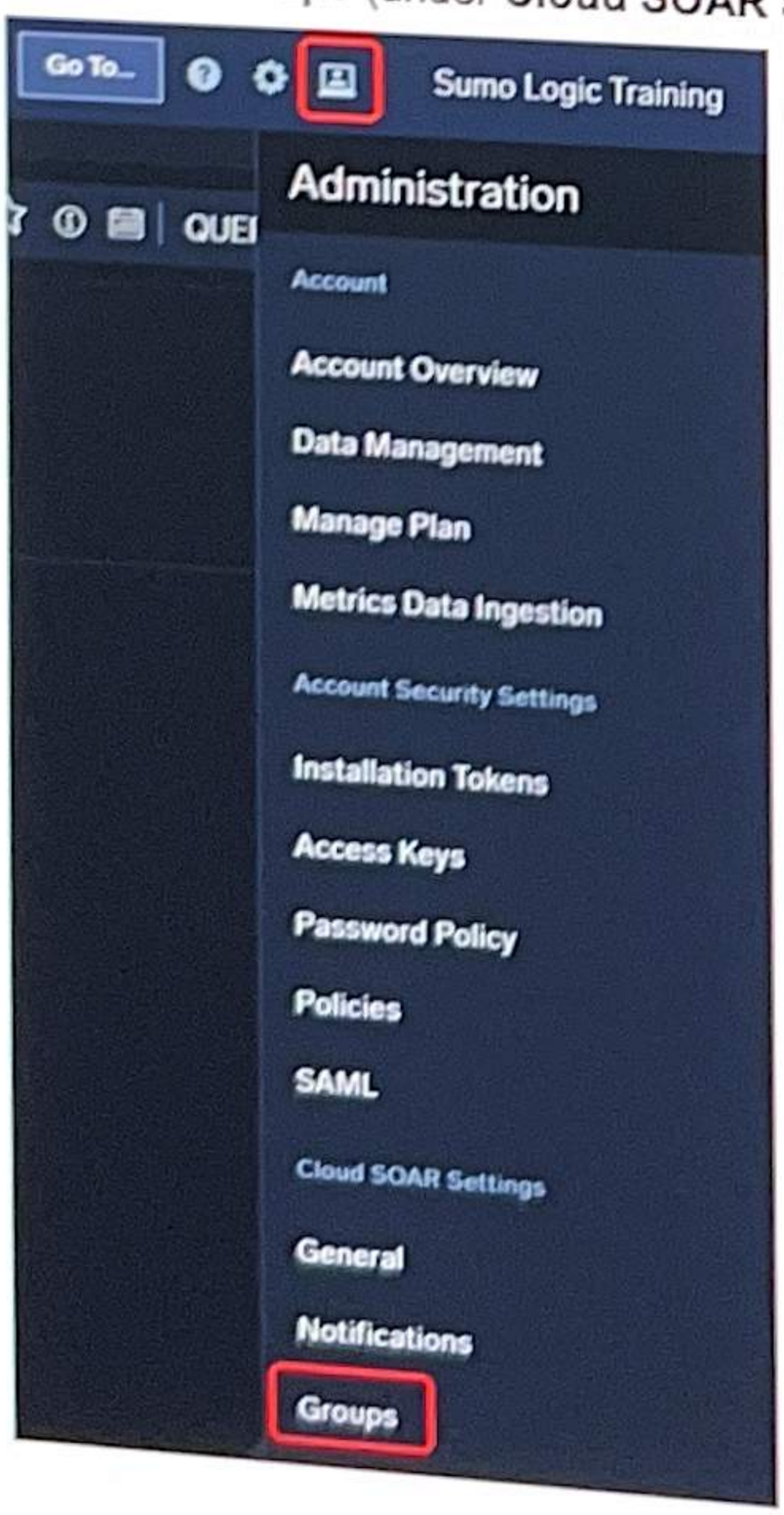
Lab 1: Explore the Cloud SOAR UI

In this lab, we'll take a quick tour of some of the basic admin features in Cloud SOAR.

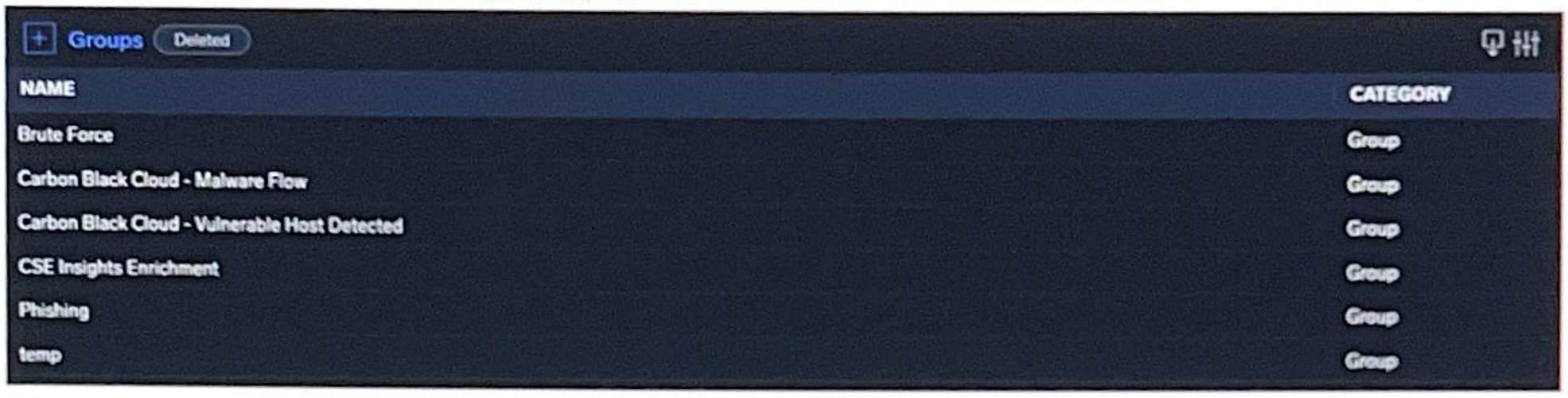
Navigate to the Cloud SOAR UI if you're not already there. Refer to Lab 0 if you need help.

In Cloud SOAR users and user privileges are controlled through the main Sumo Logic web interface, although you can create Cloud SOAR-specific user groups, making it easy to assign specialized roles to multiple users at once – for instance a group of users with different roles responsible for customer support.

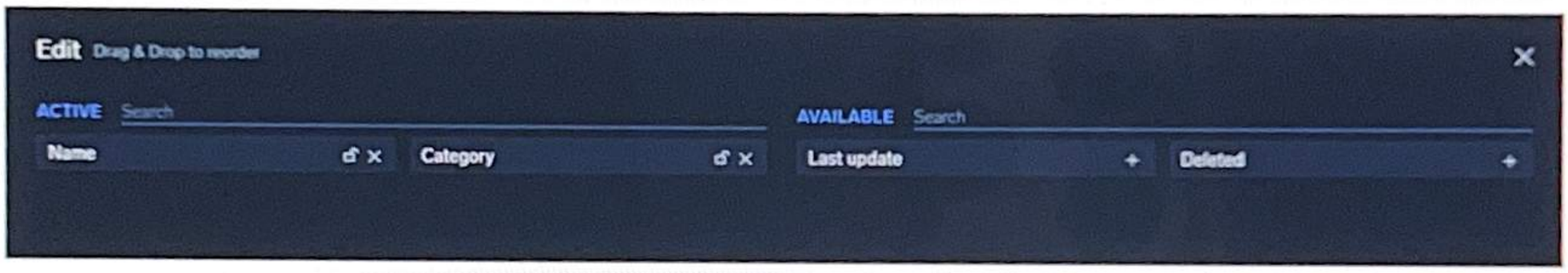
1. To create / manage user groups in Cloud SOAR, In the top right corner click the **admin** icon, then **Groups** (under **Cloud SOAR Settings**).



Here you'll be shown all the user groups in the system.

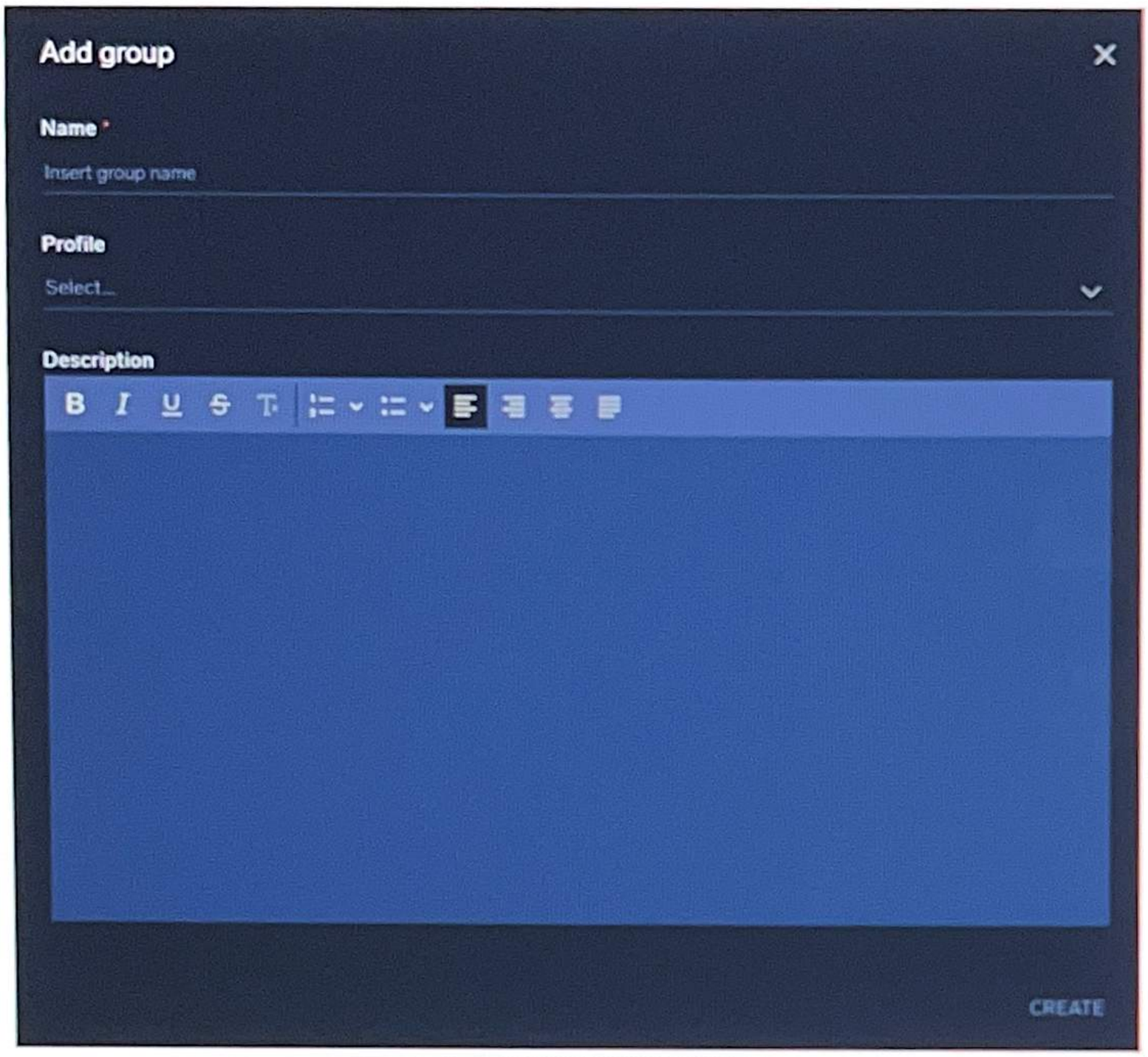


2. As with many views in Cloud SOAR, you can adjust the displayed columns in the list view by clicking the **column configuration** icon in the top right.



3. Click the "+" icon in the "Available" section on right to add any available column to the view. Likewise, click the x on the left side to remove a column from the view. Click **Apply** when finished.

4. Click the "plus" icon in the upper left to create a new group.



5. Fill in a name and user privilege Profile (created and maintained in the main Sumo Logic interface: **Administration icon > Users and Roles**) Optionally fill in a description. Click **Create** when finished.

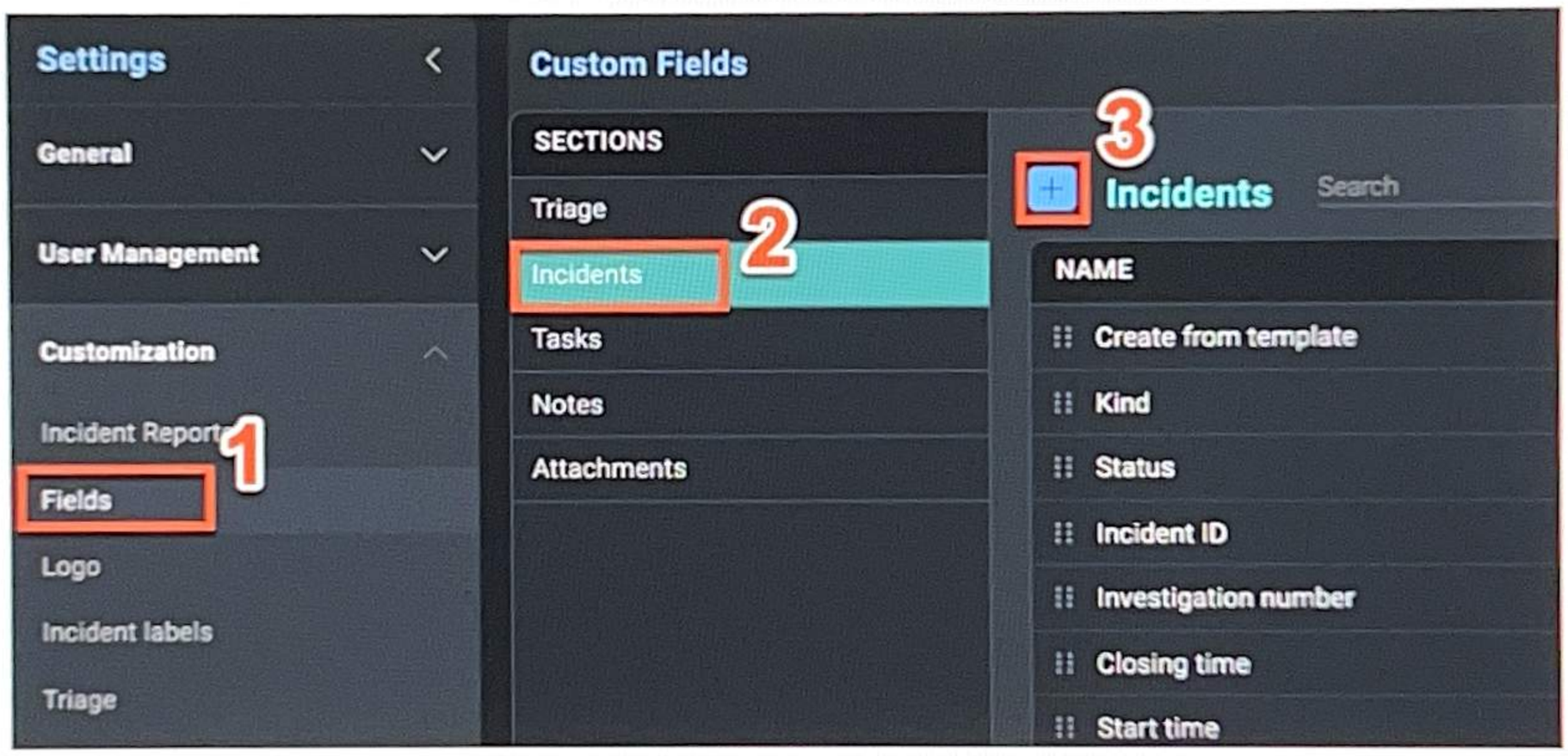
sumo logic

Lab 2: Define and Test a Custom Field

In this lab, we'll create a custom field to map data that's ingested into Cloud SOAR. We'll create a standardized naming convention for source IP addresses to help organize our Cloud SOAR instance. Then, we'll test the field to make sure it's in the system.

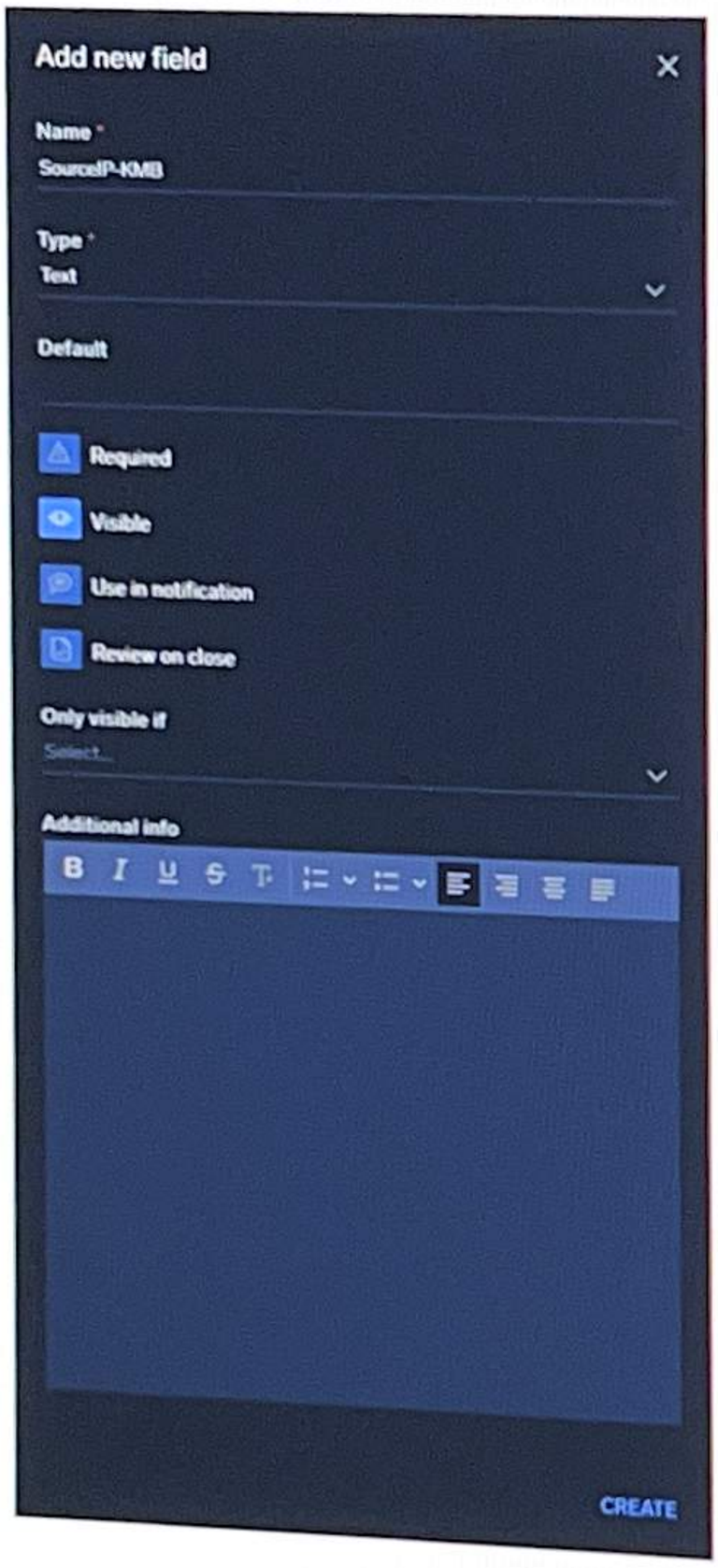
Define a Custom Field

1. In the upper right, click on the **Configuration (cog)** icon, then select **Fields** (under **Cloud SOAR Configurations**)
2. In the Custom Fields menu, select **Incidents**.
3. Click the **Plus Icon** to create a new field.



4. For **Name**, use **SourceIP-###,** replacing ### with your initials or training number. For example, if Riya Singh's account is training+admin321, she'd type SourceIP-RS or SourceIP-321.
5. For **Type**, select **Text**.
6. Leave **Visible** selected, and leave the other options unselected.

7. Click **Create**.

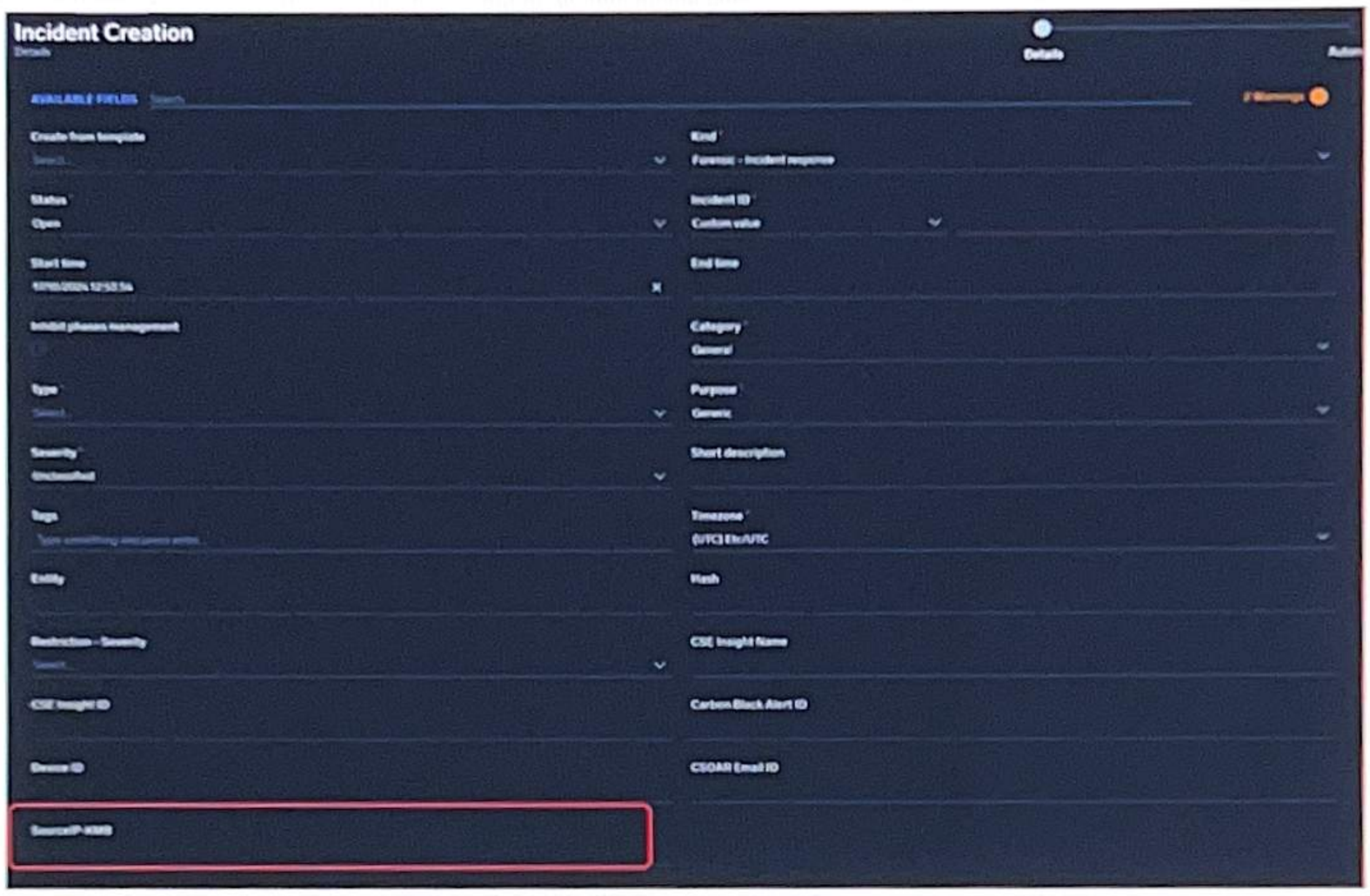


View Your Custom Field

To test the new field, we'll create a new Incident manually.

1. In the top navigation bar, click **Incidents**.
2. Click the **plus icon** to create a new incident.

3. Scroll to the bottom of the Available Fields section. You should see your field.

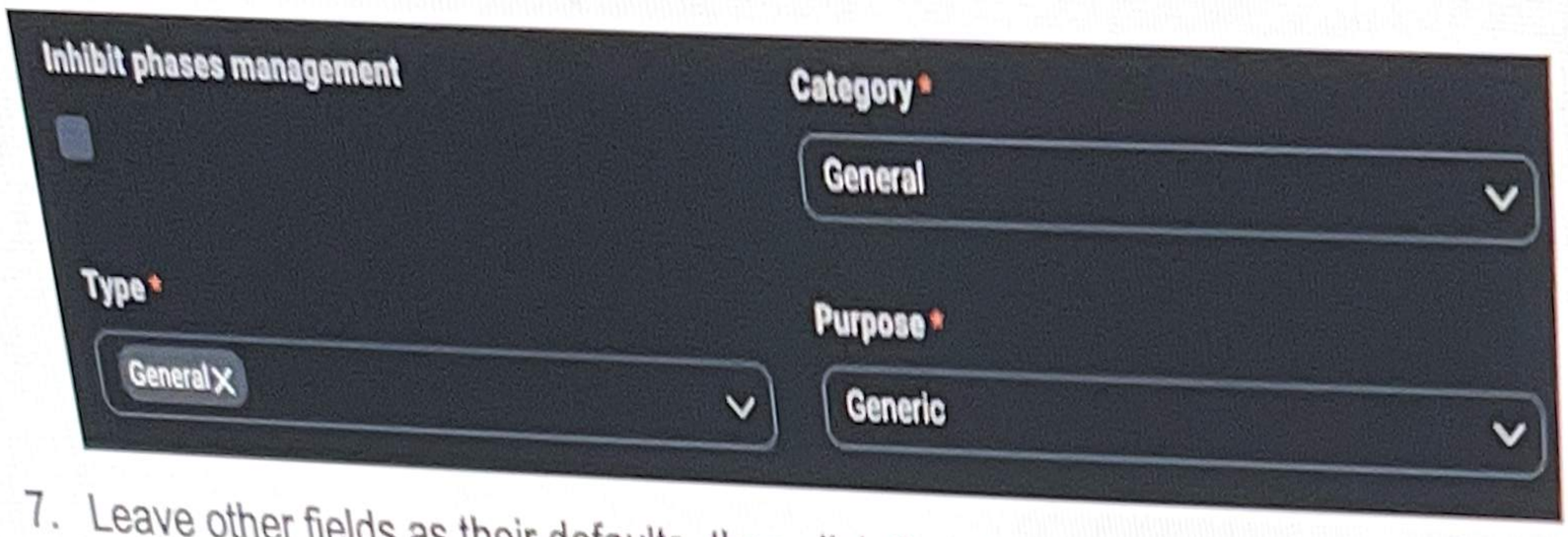


Note: Your field may appear in either the left or right column. It may be near the bottom or several rows up, depending on how many of your classmates are completing this lab at the same time as you.

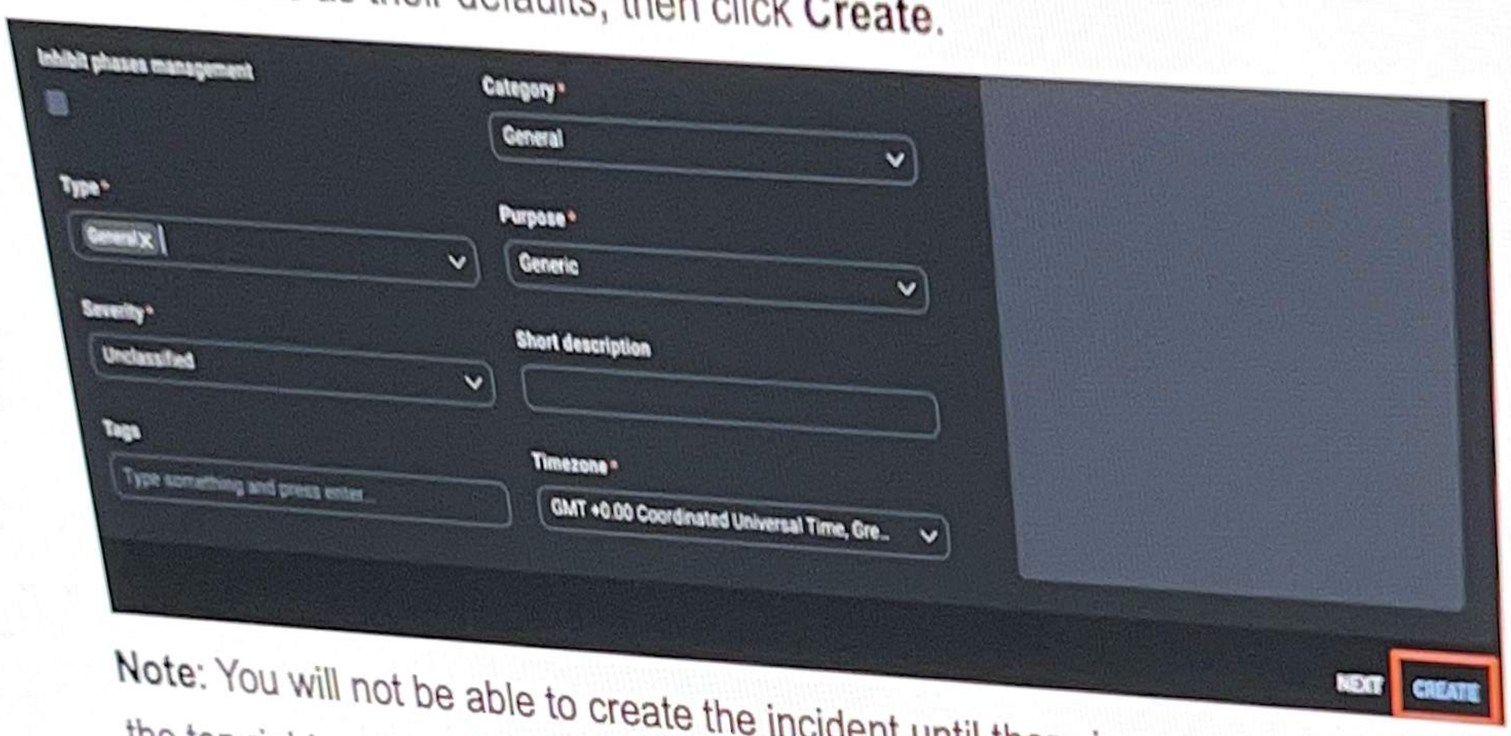
4. Type **1.1.1.1** in your field. This will link your field with a malicious IP address, that we'll use in a later lab.

5. For **Incident ID**, use your unique identifier. For example, if Riya Singh were using training+admin321 as her account, she would use “RS 321”.

6. Select **Generic** for the **Purpose**, **General** for the **Type**, and **General** for the **Category**.



7. Leave other fields as their defaults, then click **Create**.



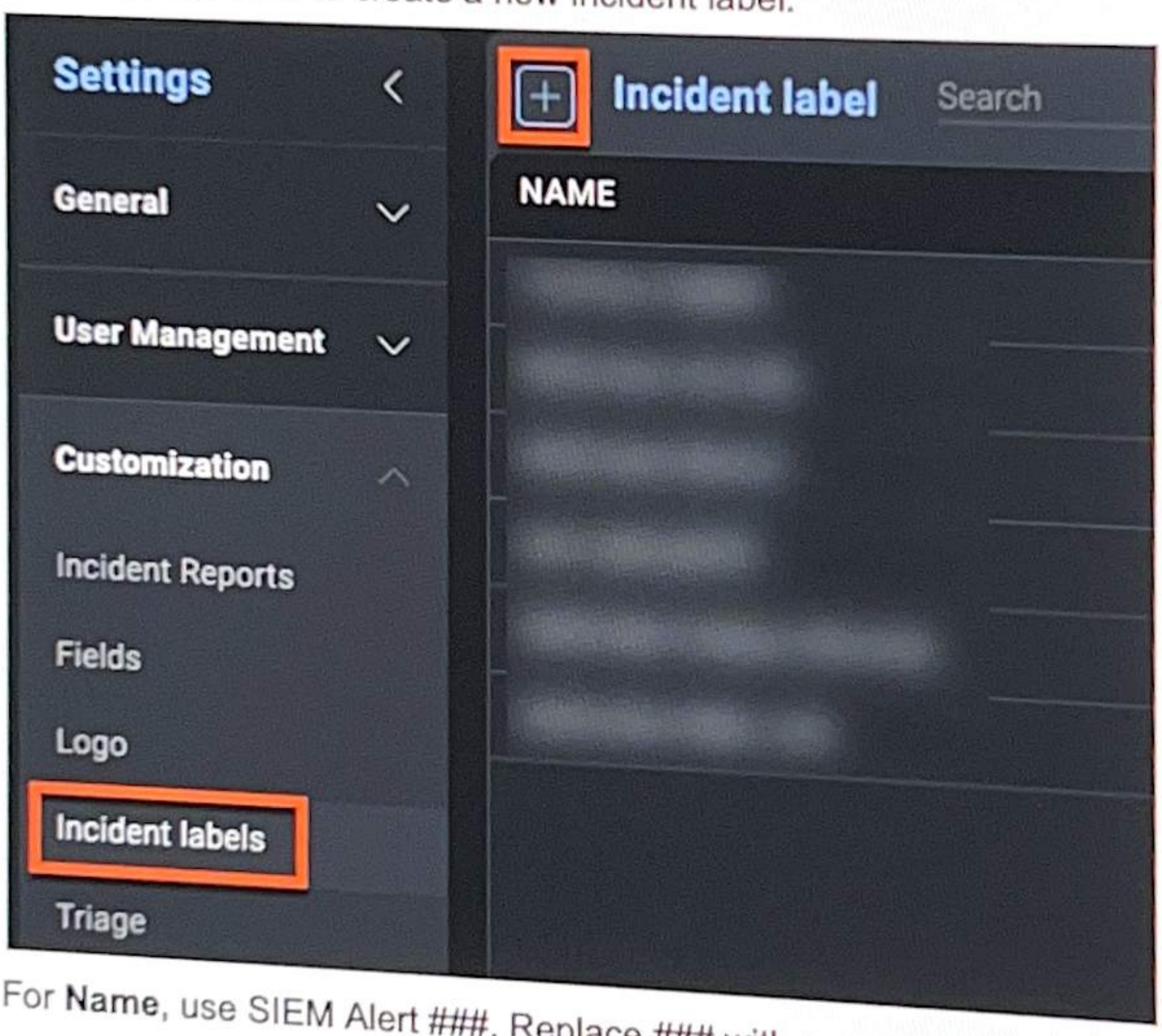
Note: You will not be able to create the incident until there is a green **No Issue Found** in the top right corner. If you see the orange **Warning** icon, hover over it to learn what fields are missing or invalid.

sumo logic

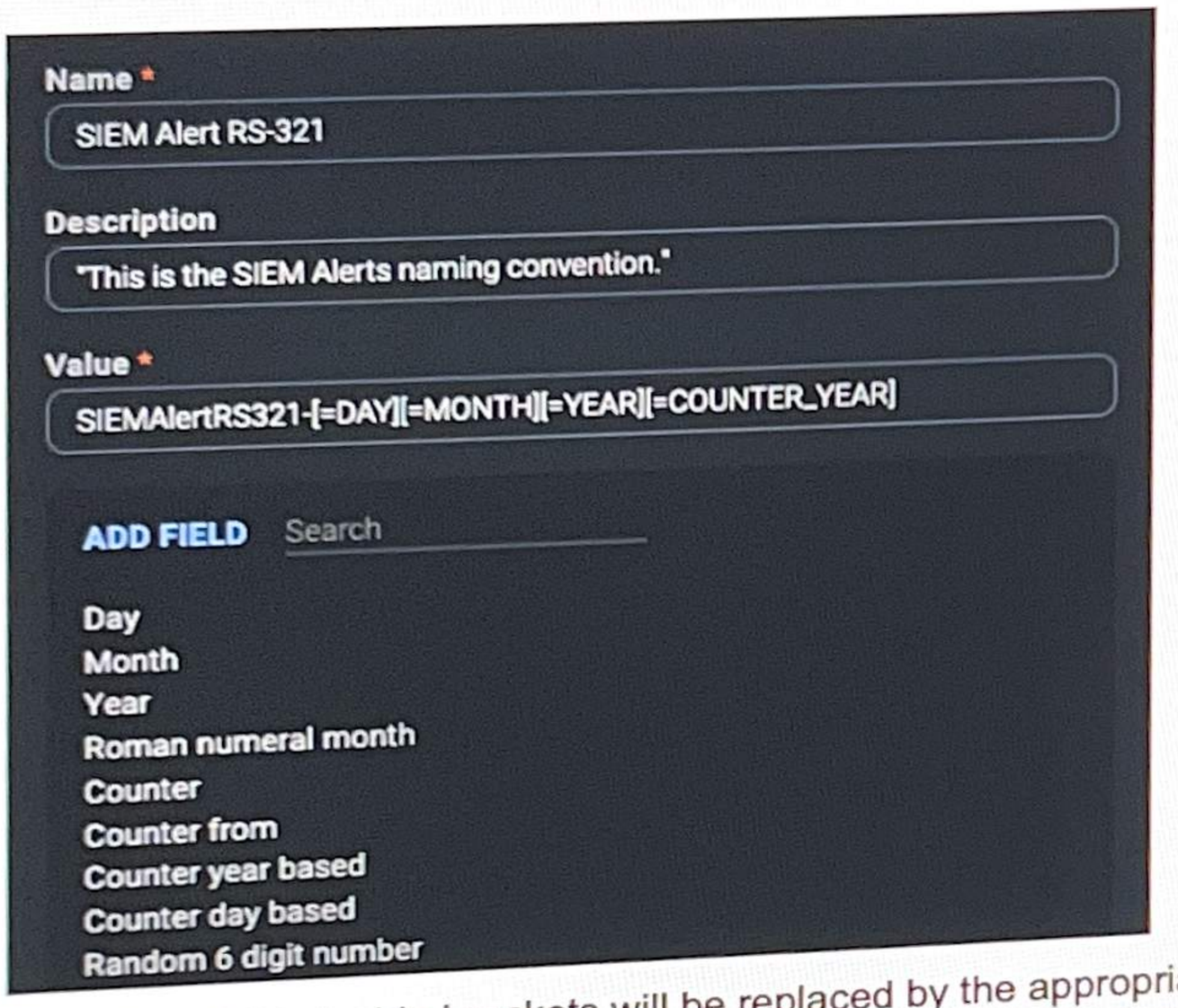
Lab 3: Customize Incident Labels

In this lab, we'll create a custom incident label. This new label will make it easier to sort and respond to incidents.

1. In the top right, click **Configuration (cog)**, then **Incident Labels** (under **Cloud SOAR Configuration**).
2. Click the **Plus Icon** to create a new incident label.



3. For **Name**, use SIEM Alert ###. Replace ### with your initials or unique identifier. For example, if Riya Singh were using the training+admin321 account, then she would type SIEM Alert RS or SIEM Alert 321.
4. Optionally, you can include a short **Description**. For now, type "This is the SIEM Alerts naming convention."
5. For **Value**, write SIEMAlert####-. Replace ###- with your initials or unique identifier.
6. Double click **Day**, **Month**, **Year**, and **Counter year based** in the **Add Field** area. This will add [=DAY][=MONTH][=YEAR][=COUNTER_YEAR] to the end of your Value.



Note: The fields inside brackets will be replaced by the appropriate variable when this Incident label is used. For example, if the Incident is created in October, the [=MONTH] field will be replaced by 10.

7. Click **Save**.

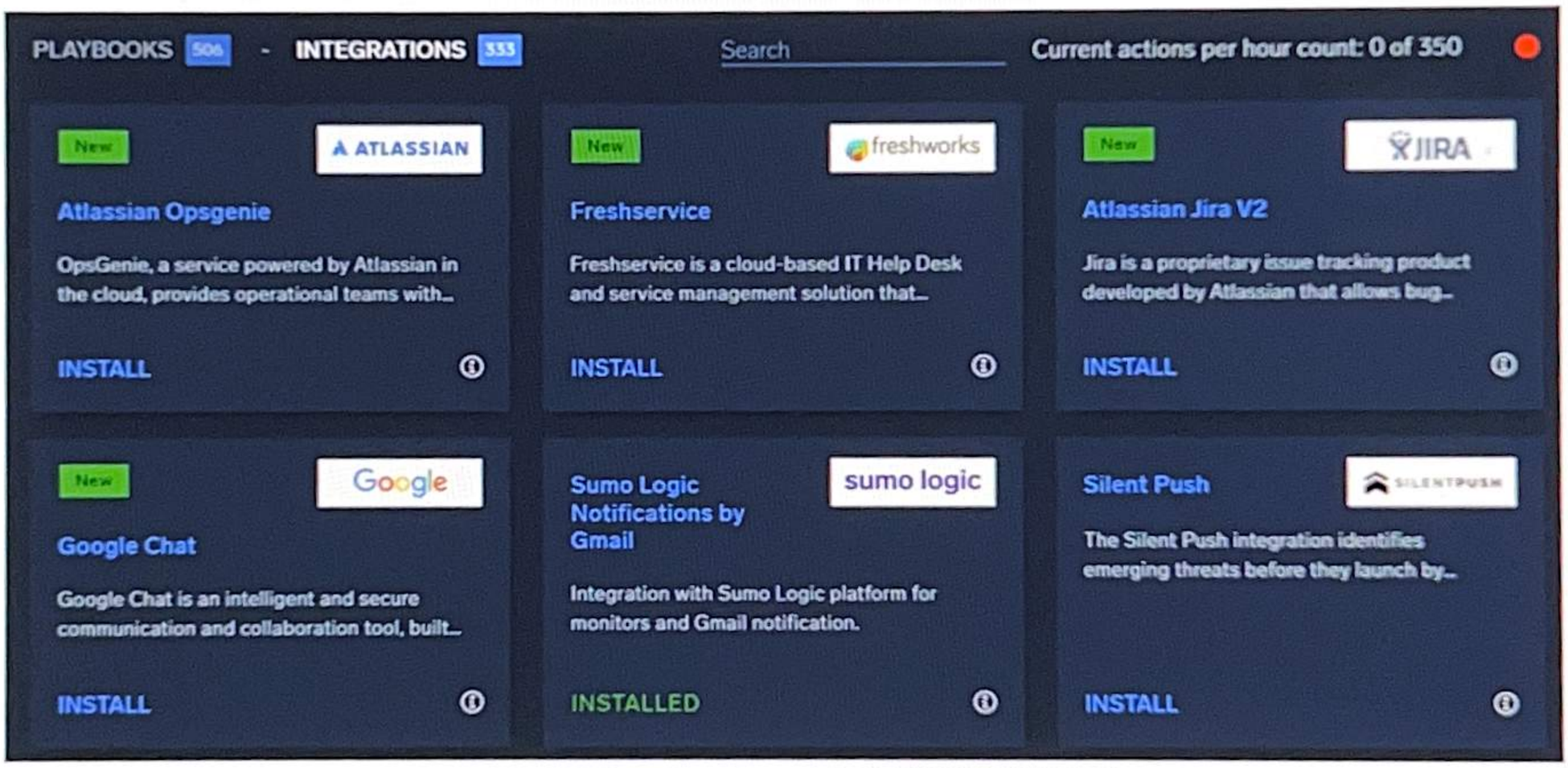
Congratulations!

Now you can use this incident label the next time you manually create an incident. You can also use it when creating or configuring automation rules that create incidents.

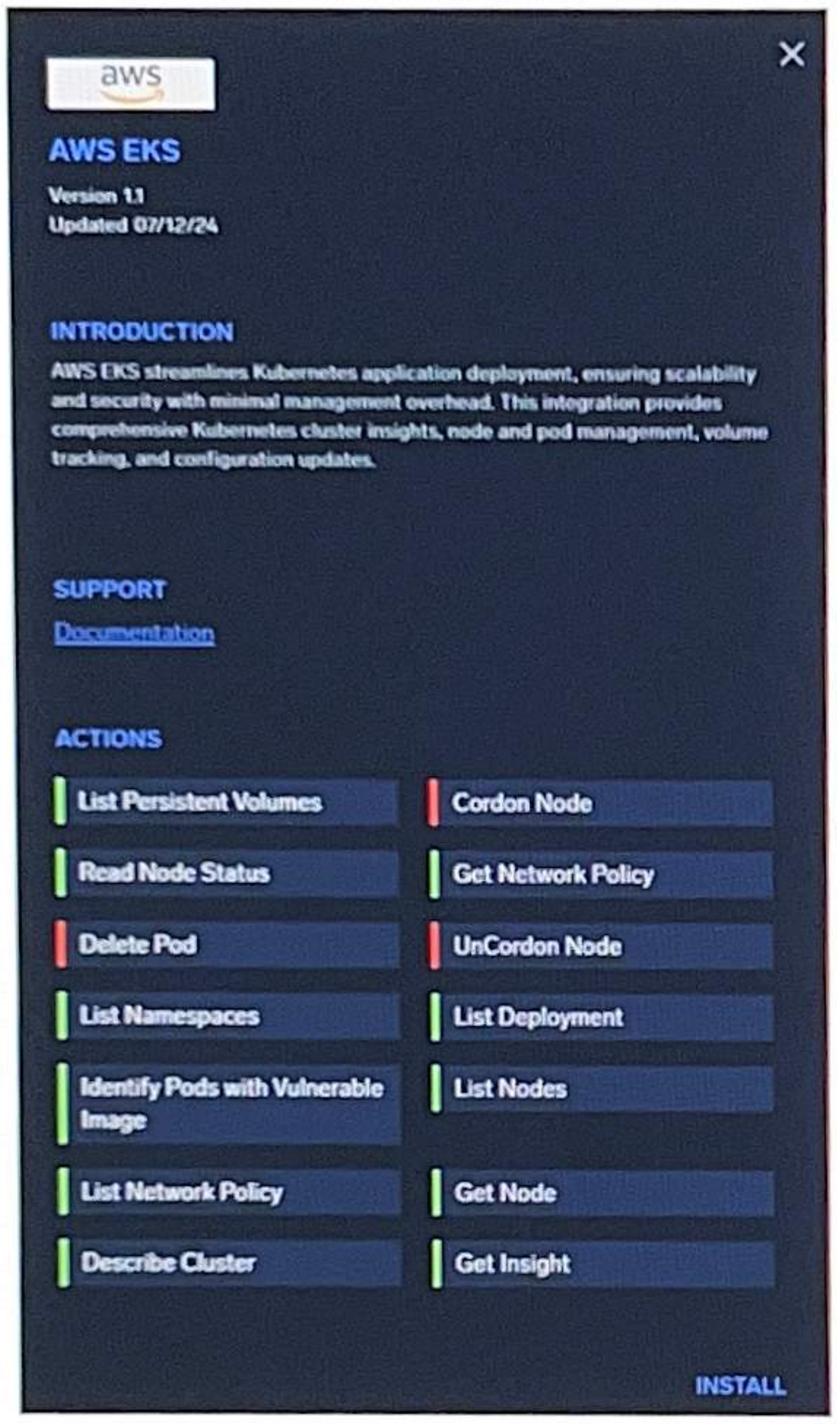
Lab 4: Import and Configure a new Integration

Many key functional elements in Cloud SOAR are done through "integrations" – separate modules that support other Sumo Logic (or third-party vendor) functionality. Cloud SOAR has over 300 out-of-the-box integrations available for install and use.

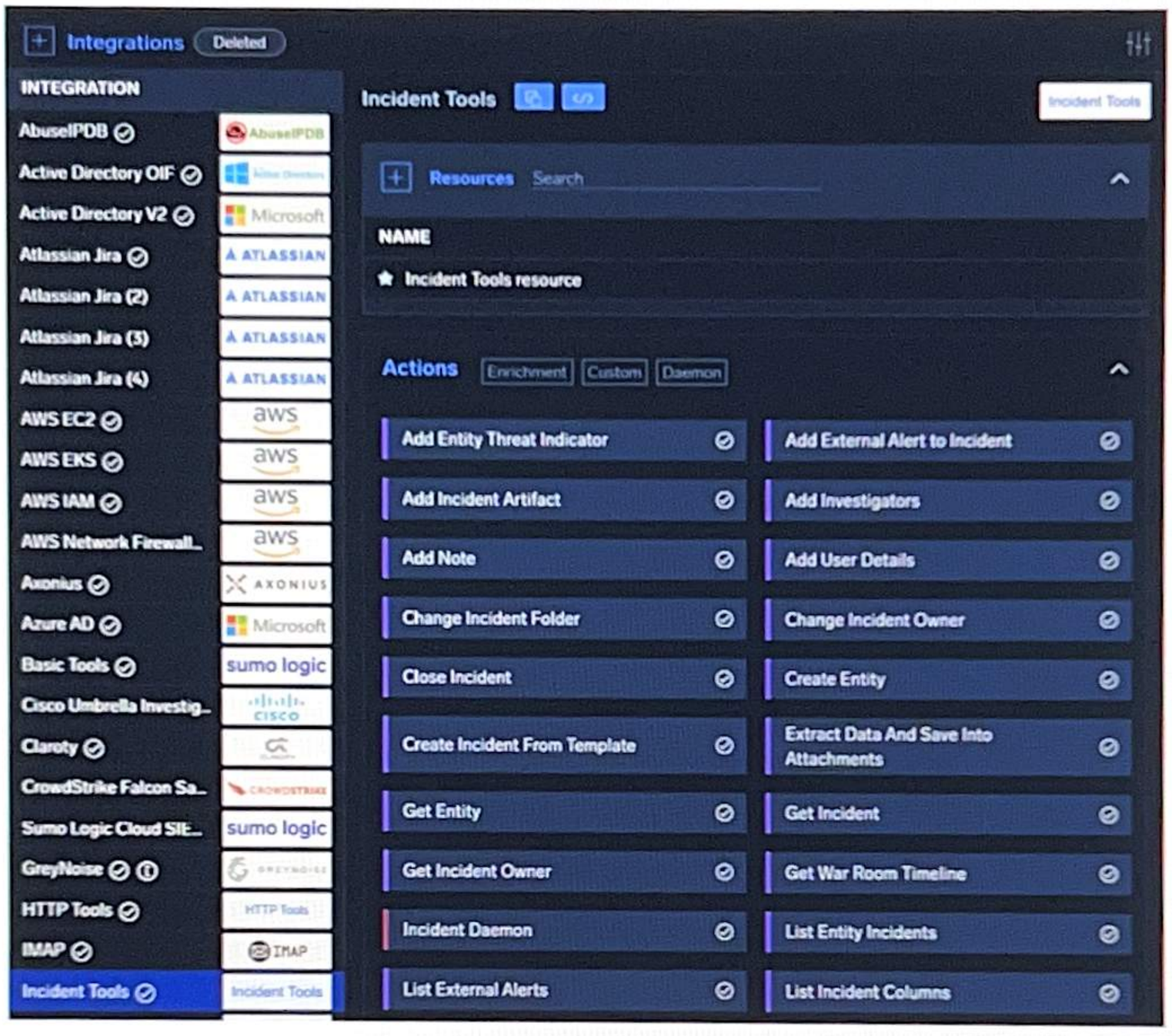
1. In the left nav menu, select **Automation > App Central**.
2. Click on the **Integrations** tab from the top tab row.
3. The **App Central** integrations page shows a long list of installed and available integrations to augment Cloud SOAR functionality with both Sumo Logic and third-party vendor functionality.



4. Choose a sample integration from the list and click on it. A popup window will appear showing the details about the integration, including version, description, and a list of actions that are supported in automations.



5. In the left menu, click **Integrations**. In this view, you can see the integrations that have already been installed and configured in the system. Locate an integration called **Incident Tools** in the list and click on it.
6. The view on the right will show the integration details, including available actions. Many integrations after install will require appropriate configuration using "resources".

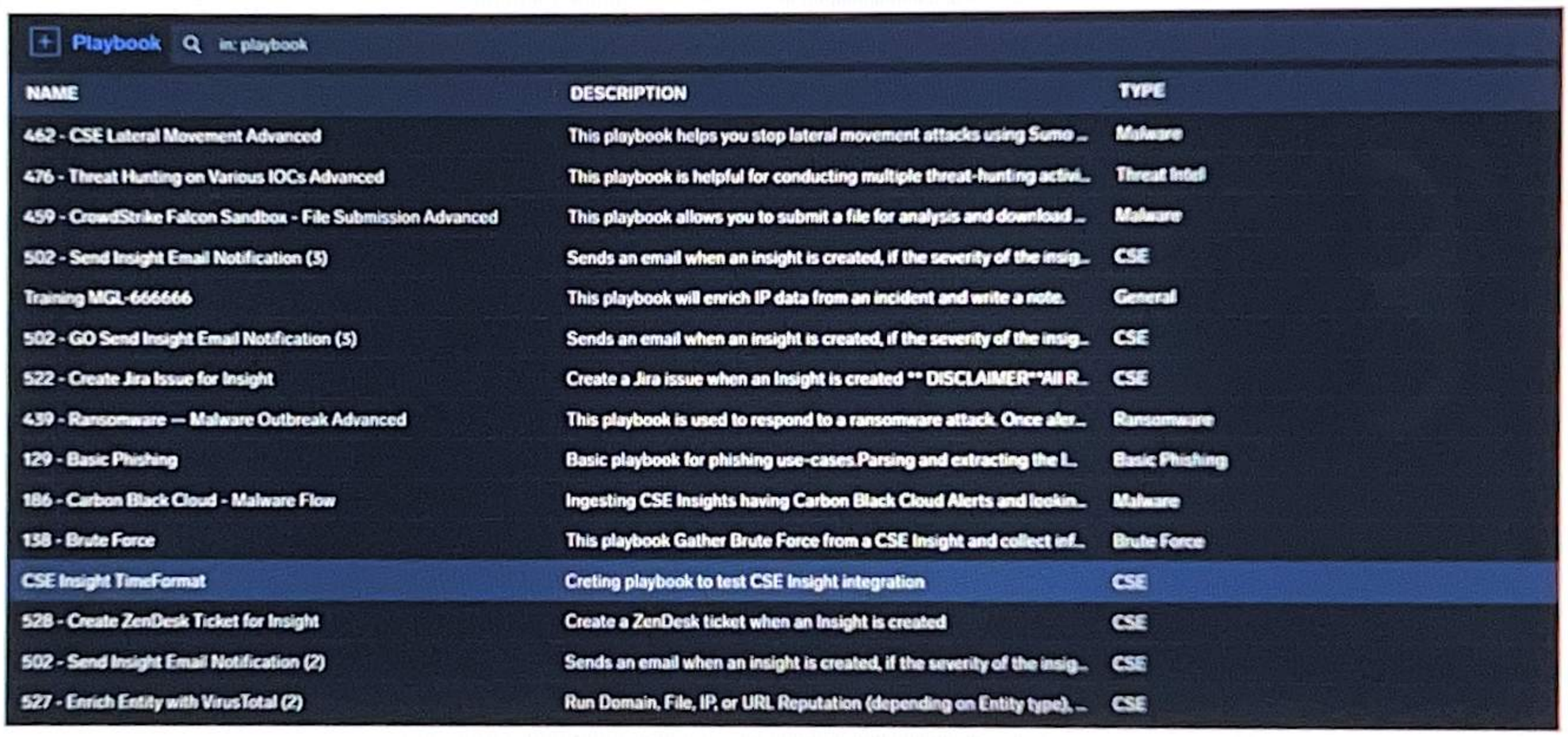


7. Move the mouse cursor over the existing resource called "Incident Tools resource", then click the "Edit" (pencil) icon.
8. When you create a resource or configure an existing one, you will need to enter the appropriate connection information such as the API web URL (for either Sumo Logic or a third-party service) and associated API keys. Many Sumo Logic integrations will require you to create an Access ID and Access Key through the Sumo Logic UI to use in configuring integrations. Some third party integrations may require you to visit their website and sign up for an account in order to obtain the appropriate URL and/or credentials for their API.
9. Click the **Test** button after you have configured the resource to test the connection info. You will see a popup that indicates whether the test was successful (may take a few seconds to execute depending on the integration).

Lab 5: Create a Custom Playbook

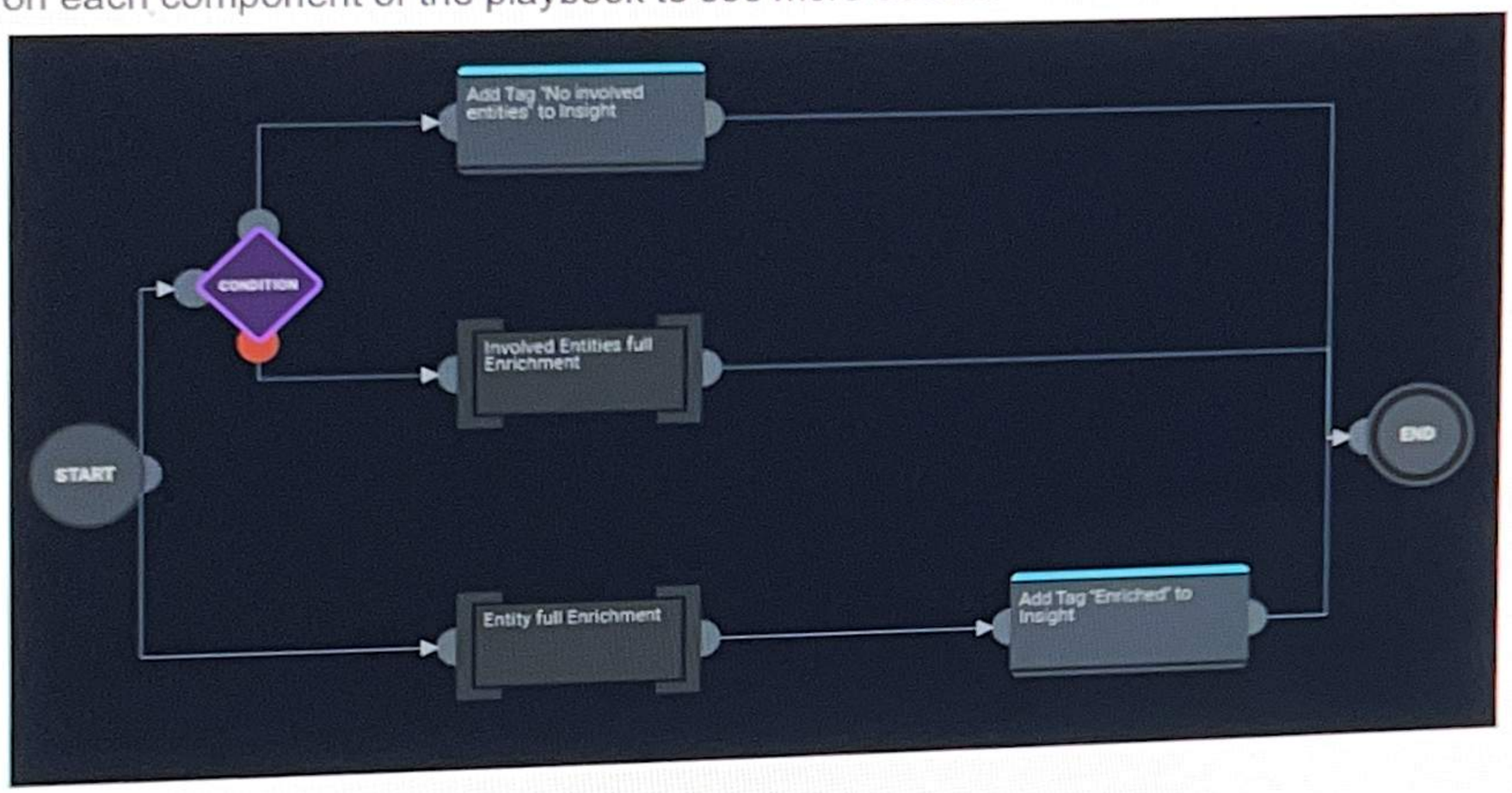
The Cloud SOAR allows us to create automations that will run when triggered by an incident. These automations are powered through "playbooks" – predefined actions run in an automated workflow to respond to an incident. Let's create a playbook for use when a Cloud SIEM insight is recorded.

1. Click on **Automation > Playbooks** in the left nav menu. The following screen will show the list of available playbooks.



2. Click any of the available playbooks. The sidebar will open on the right, showing the individual action components for that playbook. Playbooks can have any number of actions as well as branching conditions to manage different branches of actions. Click

on each component of the playbook to see more details.



3. Now let's create a new playbook of our own. Click the **'+' sign** next to "Playbook" in the top menu.

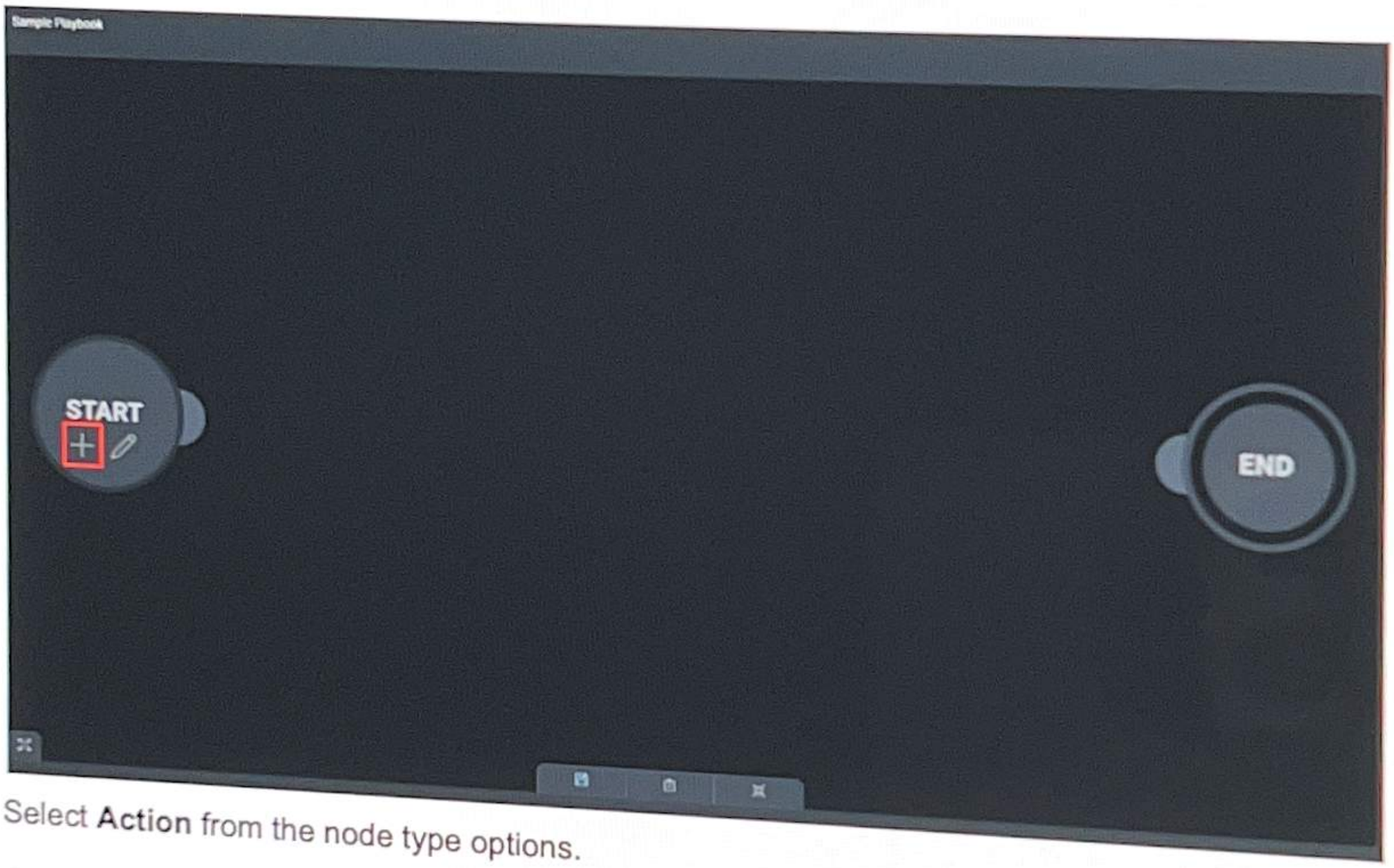
4. Enter a sample name "Training Playbook XXX" with XXX replaced by your initials or 3-digit ID. Optionally, you can enter a description. Select "Cloud SIEM" as the **Type** for the playbook.

5. Click **Create** when finished.

6. On the following screen, you'll see the starting template for your new playbook, with Start and End nodes. Switch to Edit mode by clicking the **Edit (pencil)** button in the bottom toolbar.

7. Before we start adding actions to our playbook, we'll want to set up the initial configuration of the playbook so we get the proper inputs from the Cloud SIEM Insight. Mouse over the Start node, and click on the **Edit** (pencil) icon.
8. In the **Edit Node** popup, select "Insight" from the playbook input parameters dropdown. Choosing "Insight" will automatically populate the popup view with a number of input parameters that will be added to the playbook from the corresponding Insight.
9. Click **Update** to save and close the input parameters.

10. We're now ready to start adding actions to the playbook. Click the **'+' icon** below the Start node to add an action.

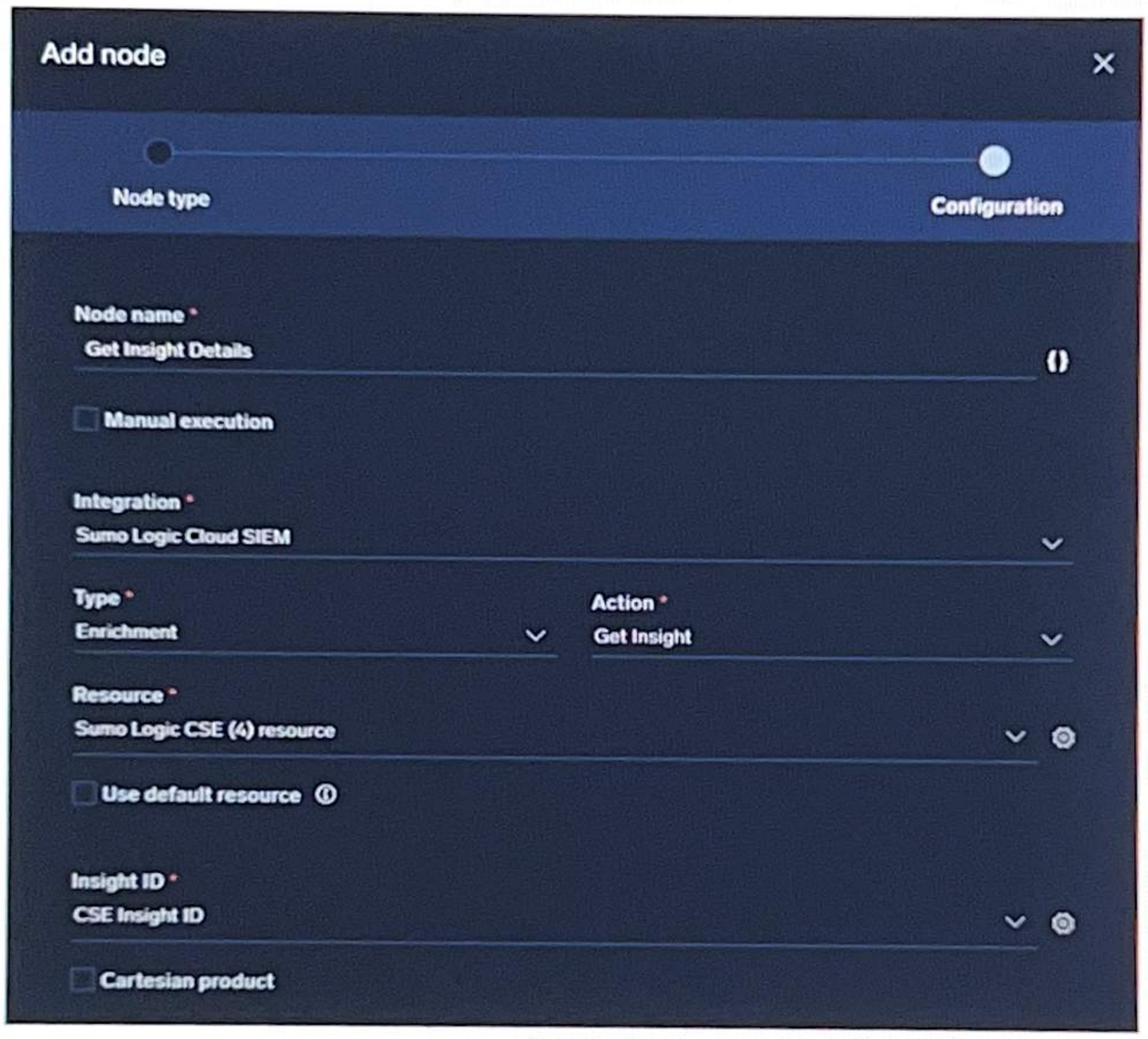


11. Select **Action** from the node type options.

When creating an action node, fill out the node configuration using the "Add Node" dialog box (pictured below). Use the following parameters to configure the node (if a field is not listed, keep the default value. Make sure you fill out the listed configuration fields in order, as some later fields will only appear in the dialog box after you've configured fields above it.)

12. Action Node Parameters:
    a. **Name**: "Get Insight Details"
    b. **Integration**: Sumo Logic Cloud SIEM
    c. **Type**: Enrichment
    d. **Action**: Get Insight
    e. **Insight ID**: CSE Insight ID

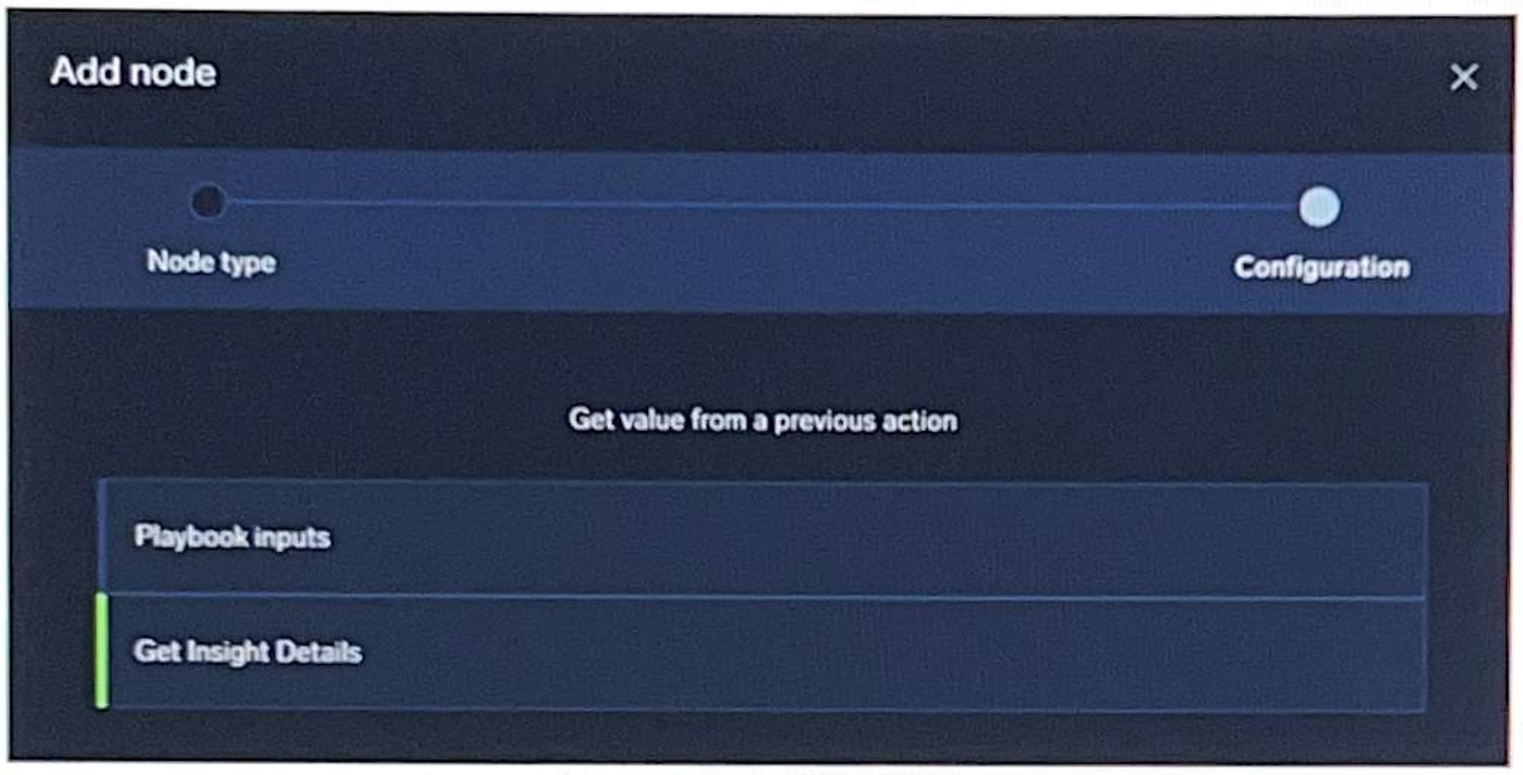
13. Leave other fields as defaults. The configuration should look like the screenshot below.



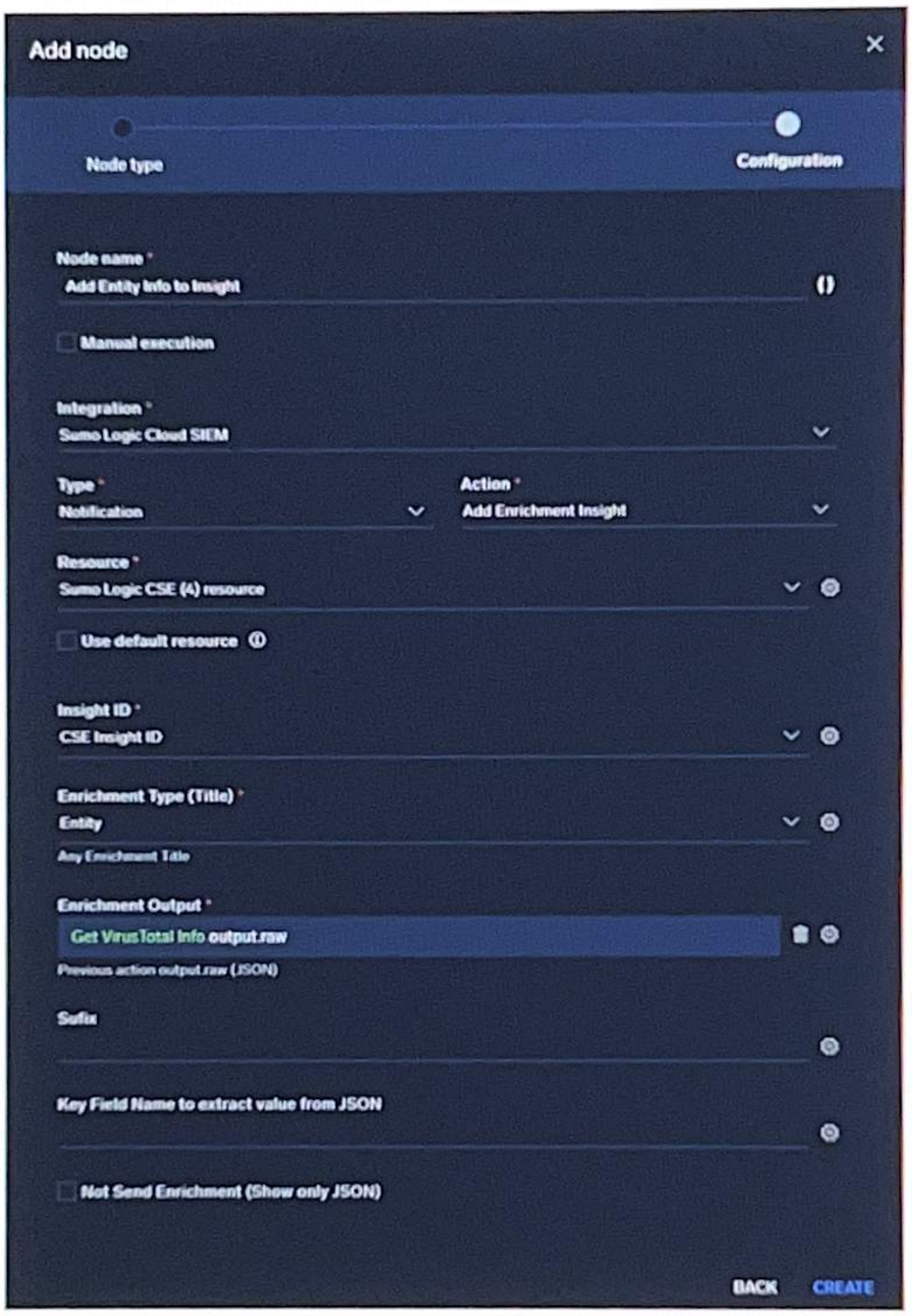
14. Click **Create** when finished.
15. Add another action to the playbook by clicking the 'plus' icon on the "Get Insight Details" node you just created. Use the parameters outlined below (keep the default if the field is not listed):
    a. **Name**: "Get VirusTotal Info"
    b. **Integration**: VirusTotal V3
    c. **Type**: Enrichment
    d. **Action**: IP Reputation
    e. **IPs**: (see below)

For many node parameters, you will have the option of selecting input/output values from other nodes earlier in the playbook sequence, allowing you to leverage other actions to generate data to use in later actions. This is done through the "cog" icon displayed on the right side of applicable node parameters.

16. For the **IPs** field, click the "cog" icon on the right, and display the "Get value from a previous action" dialog.



17. Select the "Get Insight Details" action. This will display a list of available inputs and outputs from the results of the previous action.
18. Find the "output.entity.ip.address" field in the list and select it.
19. Leave other fields as the defaults. Click **Create** to save the new action.
20. Add another action to the playbook by clicking the 'plus' icon on the "Get VirusTotal Info" node you just created. Use the parameters outlined below (leave as default any field not listed:
    a. **Name**: "Add Entity Info to Insight"
    b. **Integration**: Sumo Logic Cloud SIEM
    c. **Type**: Notification
    d. **Action**: Add Enrichment Insight
    e. **Insight ID**: CSE Insight ID
    f. **Enrichment Type (Title)**: Entity
    g. **Enrichment Output**: "cog" icon > Get VirusTotal Info > output.raw



21. Click **Create** to save the action.

Playbooks also allow "condition" nodes that can switch execution branches depending on the true/false results of a given expression. Let's add a condition node to our playbook that will differentiate the execution branch depending on the severity of the insight.

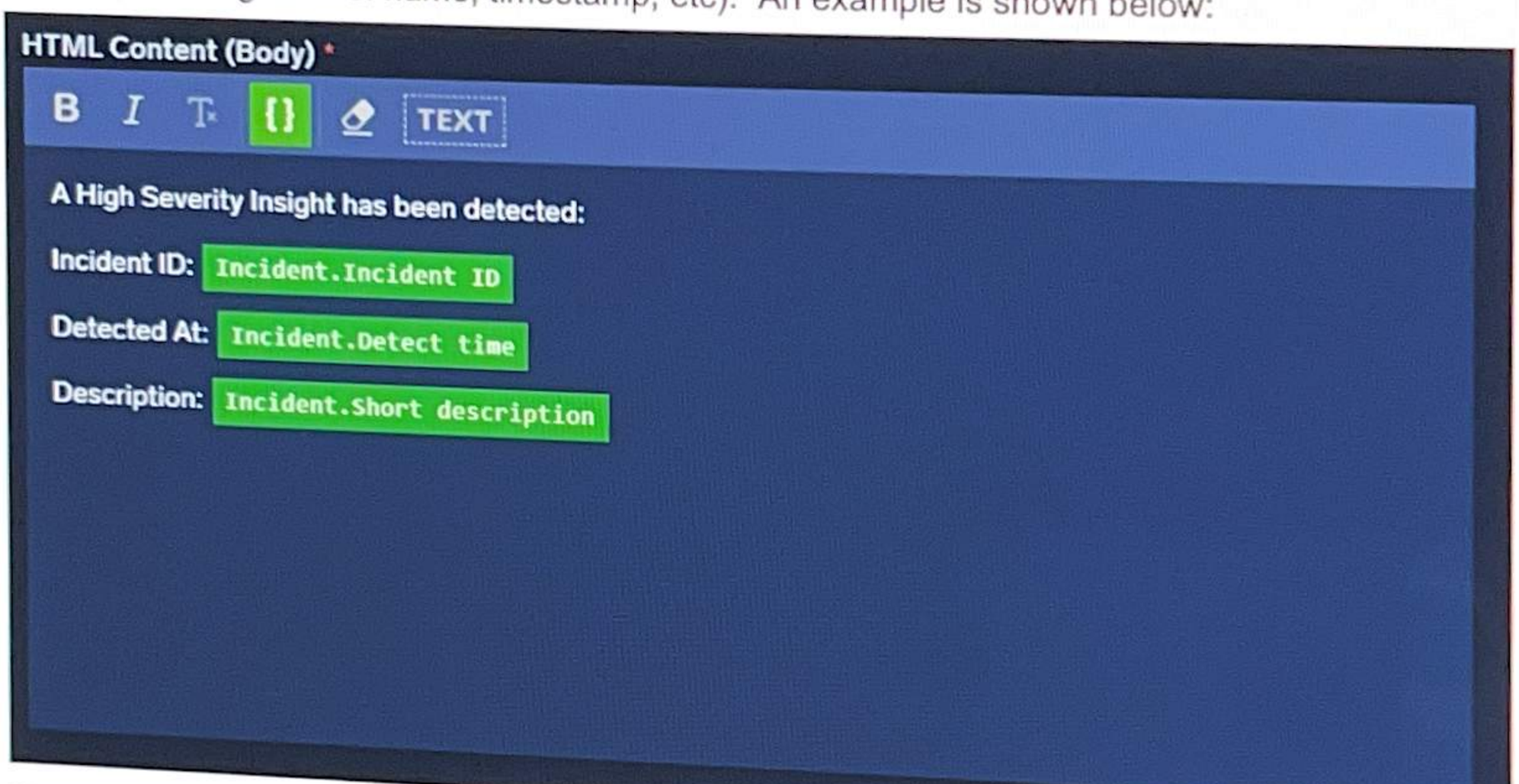
22. Click the 'plus' icon under our last action (the blue "Add Entity Info to Insight" action). Choose a **Condition** node.
23. Click the pencil icon to edit the new Condition node.
24. For the top "select a value", select the "output.severity" option from the "Get Insight Details" action. Make sure "==" is selected in the middle row.

25. For the bottom "select a value" field, add a manual value: "High".
26. Click **Create** to save the Condition node.
27. Click the 'plus' icon under the Condition node to create a new node. Select "Action" for this new node. Use the parameters below (keep defaults for anything not listed):
    a. **Name**: "Send Notification Email"
    b. **Integration**: Basic Tools
    c. **Type**: Notification
    d. **Action**: Send Email
    e. **Recipients**: enter an email address (real or fake) (NOTE: you will need to press Enter after typing the email address to parse and submit it)
    f. **Subject**: "High Severity Insight detected"
    g. **HTML Content (Body)**: (see below)

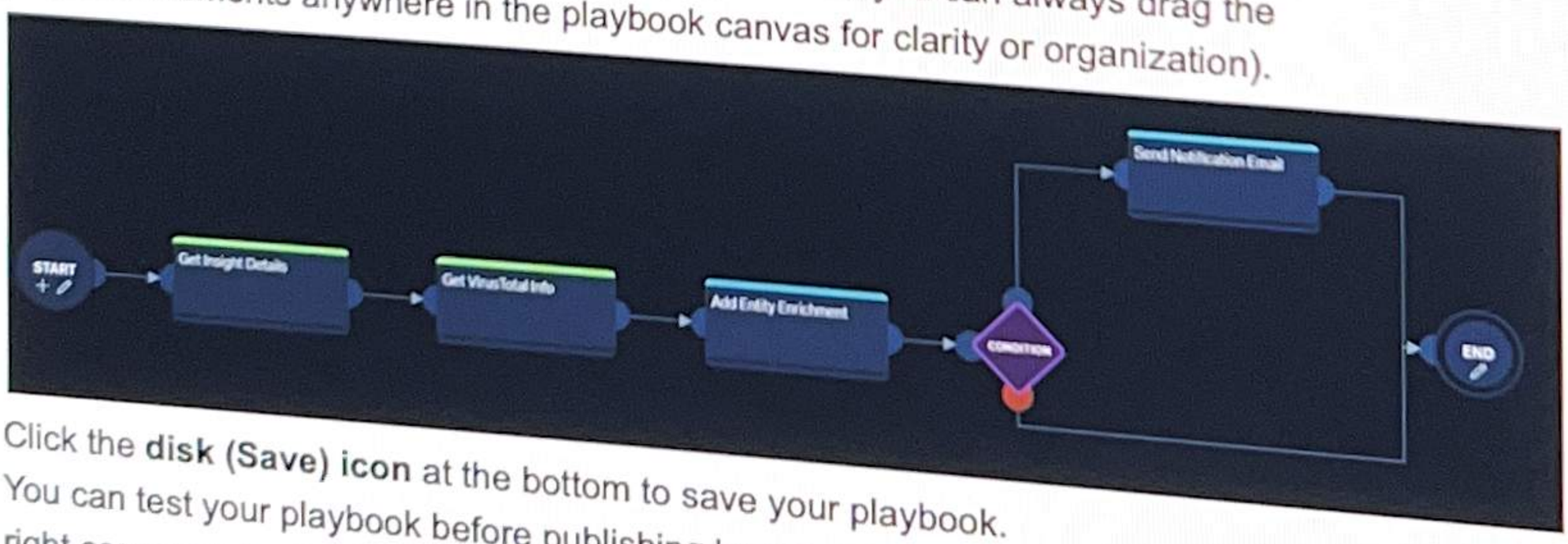
When composing content for an email notification, you have the option of using input parameters from earlier in the playbook in addition to your desired custom text.

28. Click on the "{ }" icon to add a parameter field to your **HTML Content (Body)** text.
29. Click on the red parameter box that appears and select a source for the desired input parameter (for instance: "Insight.Severity" or "Get Insight Details.output.name"). The parameter box will turn green once you have selected a valid source parameter. You can add custom text before or after the source parameter.
30. Add one or more source parameters and accompanying custom text to outline what you want the email to say (for instance, explain that a high severity insight has been detected

with the following details: name, timestamp, etc). An example is shown below:



31. Click **Create** when finished with this action.
32. When you've created your final node(s) for your playbook, manually drag the mouse cursor from the gray connection circle on the right side of the Email Notification node to the left connection area of the "End" node. Drag and connect the "failure" end of the condition node to the End node as well.
33. Verify that the Start > End node sequence for all branches have been completed – it will look more or less like the screenshot below. (Note that you can always drag the playbook elements anywhere in the playbook canvas for clarity or organization).



34. Click the **disk (Save) icon** at the bottom to save your playbook.
35. You can test your playbook before publishing by going to the "triple dot" icon in the upper right corner and selecting "Run Test".