

elp

dent_Lab_Guide_-_Cloud_SOAR_Administr...

e 26 of 32



Q Search

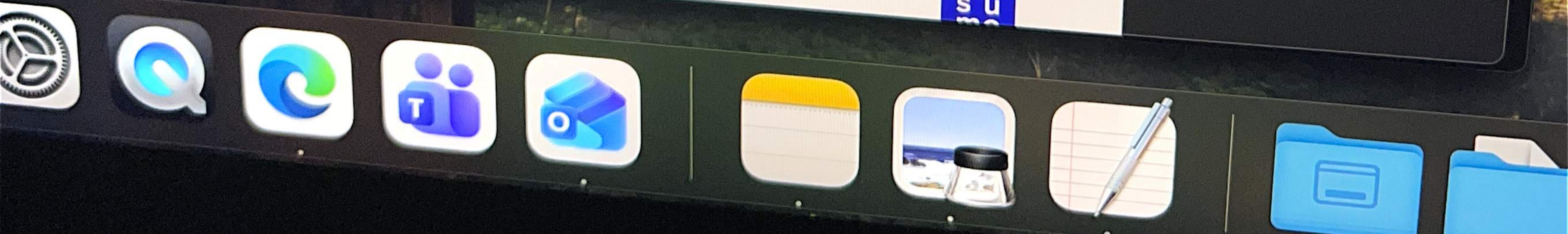
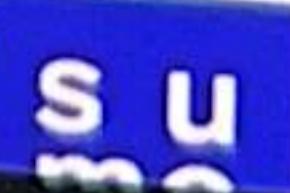


sumo logic

36. After testing and troubleshooting playbook details (if needed), click the "Publish" (clipboard) icon next to the edit/pencil icon to publish your playbook. (You can add a description here if you wish)

©2024 Sumo Logic, All Rights Reserved.

26



F1

80

F3

Q

F4

L

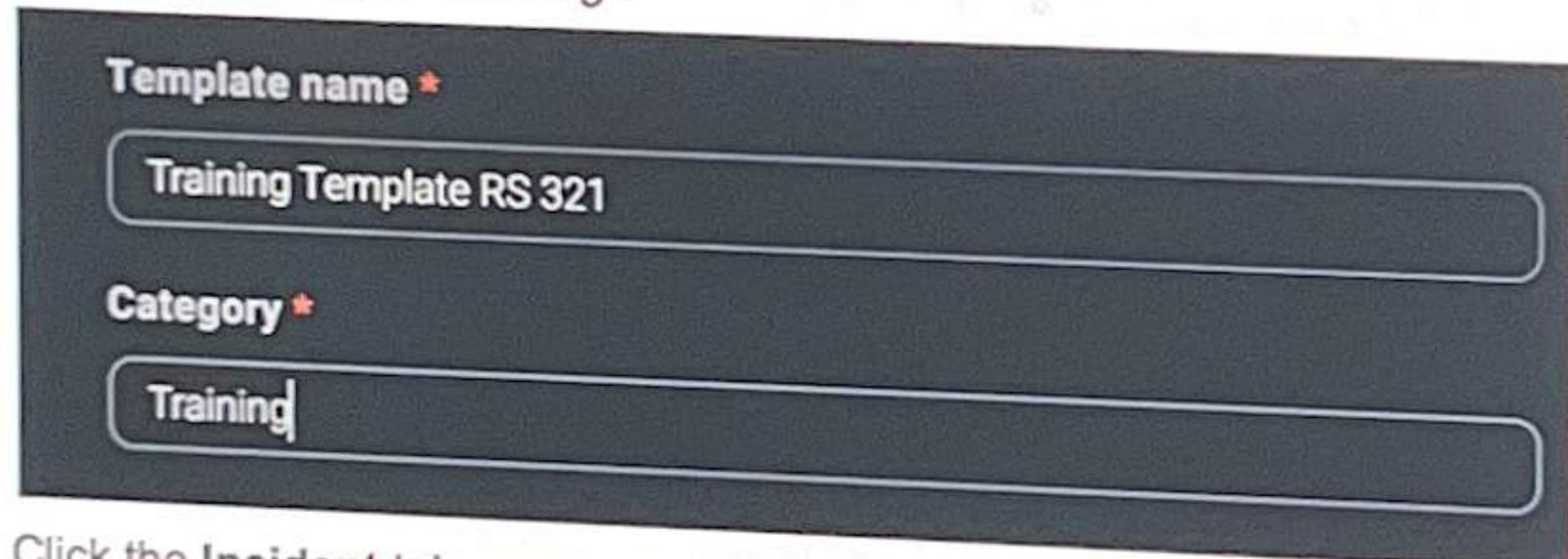
C

W

Lab 6: Create a Custom Incident Template

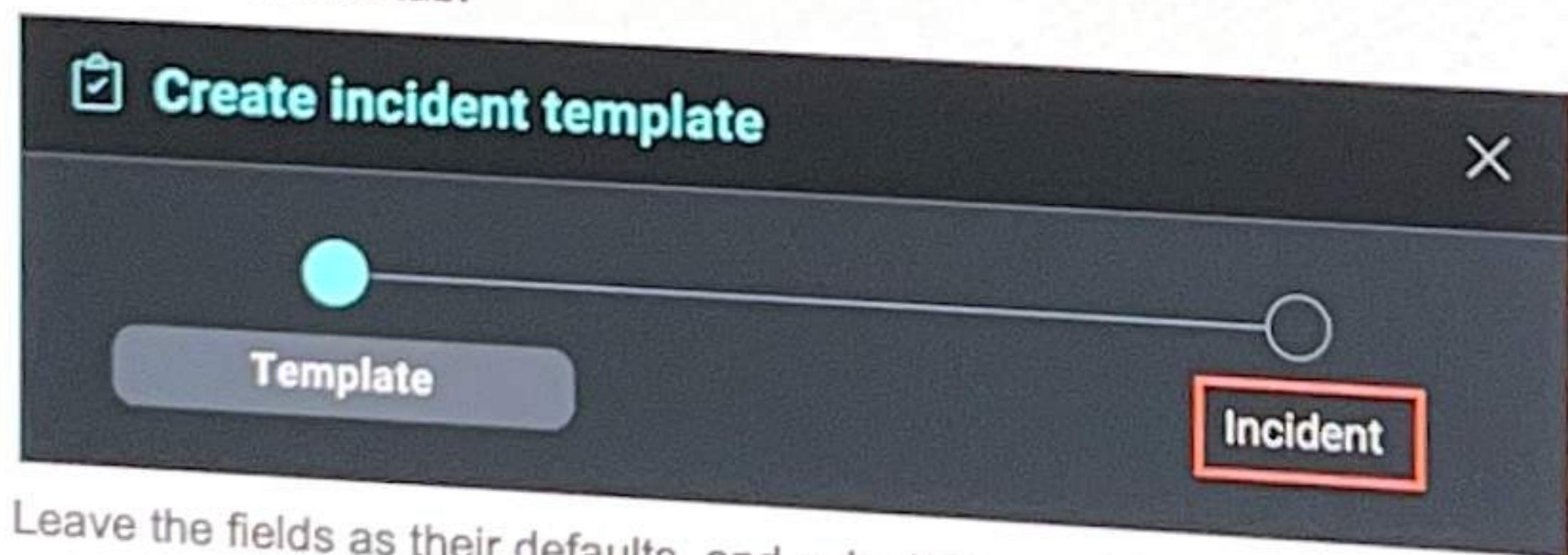
In this lab, we'll create a custom incident template. This template will automatically assign the playbook you created earlier to certain new incidents, and then automatically run it.

1. In the left navigation menu, click **Automation > Templates**.
2. Near the top, click the **plus icon** to create a new template.
3. For **Template Name**, type "Template ###". Replace ### with your initials or chosen ID number. For example, if Riya Singh were using training+admin321 as her account, she would write "Template RS".
4. For **Category**, type "Training".



The screenshot shows a dark-themed UI for creating a template. At the top, there's a field labeled "Template name *" with the value "Training Template RS 321". Below it is a field labeled "Category *" with the value "Training". Both fields have a thin white border around them.

5. Click the **Incident** tab.



6. Leave the fields as their defaults, and select **General** for **Type**.

7. Click **Apply** to create the template.

Create incident template

Template Incident

Kind*
Forensic - Incident response

Status*
Open

Category*
General

Type*
General X

Purpose*
Generic

Severity*
Unclassified

APPLY



sumo logic

8. Click the plus icon next to Playbook to add a new playbook.

The screenshot shows the 'Training Template RS 321' incident details. The 'Playbook' section is highlighted with a red box around the '+' icon. The incident details include Kind: Forensic - Incident response, Status: Open, Category: General, Purpose: Generic, Timezone: GMT +0:00 Coordinated Universal Time, Greenwich Mean Time, and Owner: Training Admin321.

9. Search for your initials or ID number and select the check mark next to the playbook you created in the previous lab.

10. Click Add.

The screenshot shows the 'Add playbook' modal window. A specific playbook named 'Training RS 321' is selected and highlighted with a red box. The modal also includes an 'Add' button at the bottom right.

©2024 Sumo Logic, All Rights Reserved.

11. Toggle the Autorun switch to Enabled (blue) position.

Playbook			
NAME	TYPE	DESCRIPTION	AUTORUN
Training RS 321	General	This playbook will enrich IP data from an...	<input checked="" type="checkbox"/>

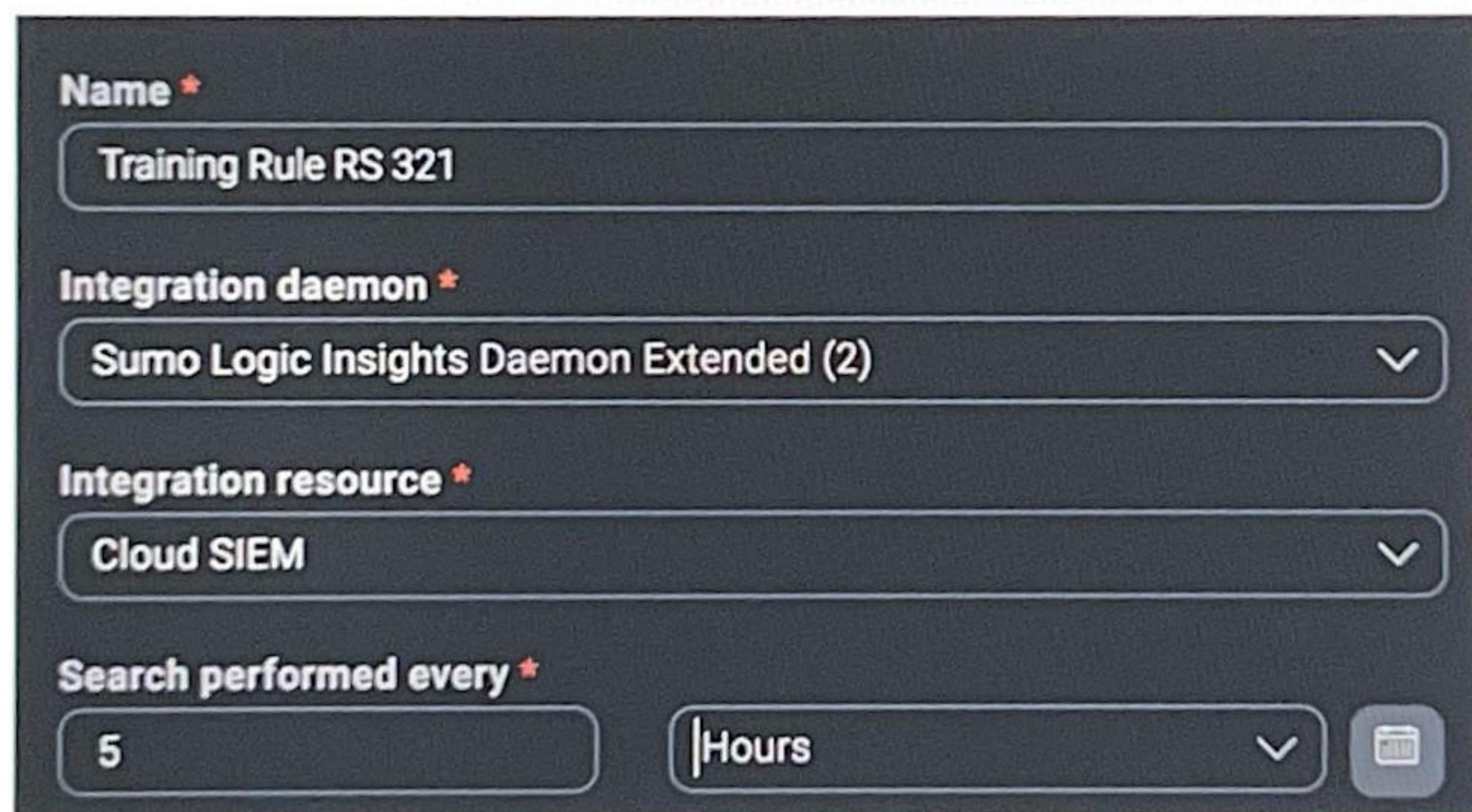
Congratulations!

You just created a custom incident template with a custom playbook.

Lab 7: Create a Custom Automation Rule

In this lab, we'll create a custom automation rule. This rule will pull information from Cloud SIEM every five hours.

1. In the left navigation menu, click **Automation > Rules**.
2. Near the top, click the **plus icon** to create a new rule.
3. For **Name**, type "Training Rule ###". Replace ### with your initials and/or chosen ID number. For example, if Riya Singh were using training+admin321 as her account, she could use "Training Rule RS 321".
4. For **Integration daemon**, select **Sumo Logic Insights Daemon Extended (2)**.
5. For **Integration resource**, select **Cloud SIEM**.
6. For **Search performed every**, type **5** then select **hours**.



The screenshot shows a dark-themed UI for creating a new automation rule. The fields are as follows:

- Name ***: Training Rule RS 321
- Integration daemon ***: Sumo Logic Insights Daemon Extended (2)
- Integration resource ***: Cloud SIEM
- Search performed every ***: 5 Hours

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

Post-lab cleanup

1. In the left nav menu, **Automation > Rules**.
2. Find your rule and click it.
3. Make sure the rule is **disabled**. The enabled switch should be black, not blue.



sumo logic

The screenshot shows the configuration page for a training rule named 'Training Rule RS 321'. At the top, there is an 'Enable' button with a red border. To the right of the enable button is the 'sumo logic' logo. Below the header, there is a section titled 'Details' containing the following configuration options:

- Daemon name: Sumo Logic Insights Daemon Extended (2)
- Integration resource: Cloud SIEM
- Search performed every: 5 Hours
- Created artifacts: []
- Process from: Last Item First Item

As a best practice, you can enable and test new rules, but then disable them, since they can disrupt your environment. Continue testing your rules until correct behavior is seen.

Congratulations!

You now have a custom automation rule that you can add to your SOAR environment.