sumo logic

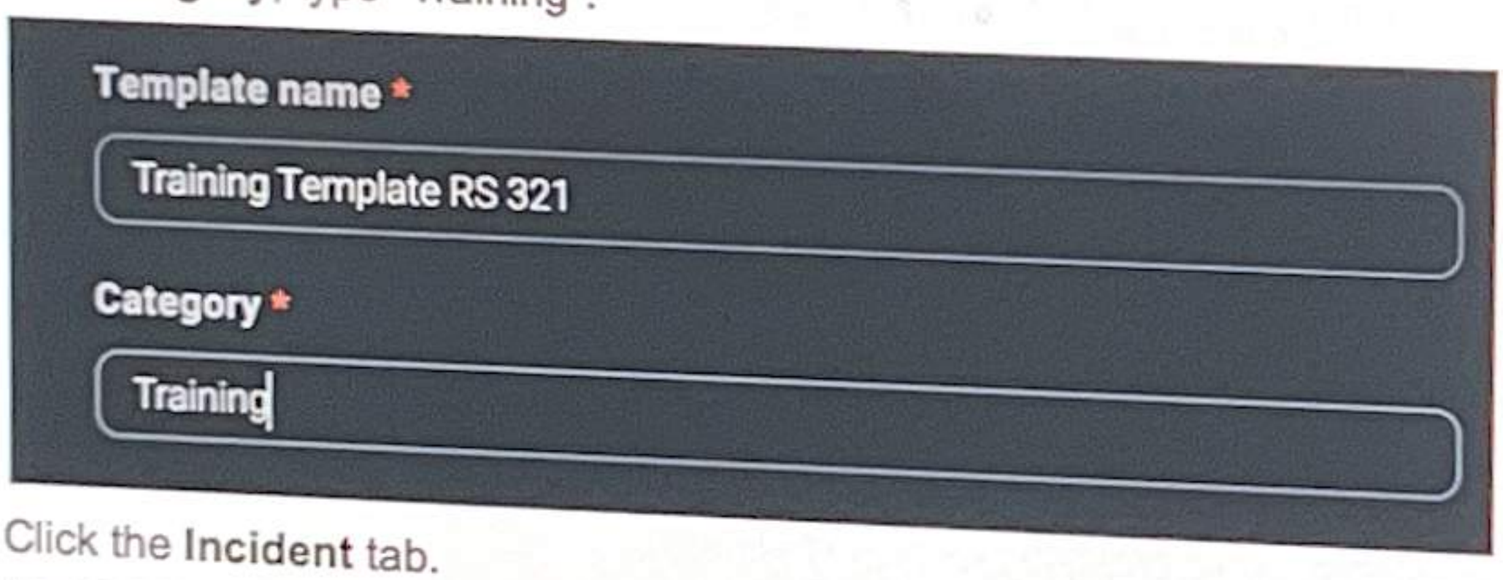
36. After testing and troubleshooting playbook details (if needed), click the "Publish" (clipboard) icon next to the edit/pencil icon to publish your playbook. (You can add a description here if you wish)

sumo logic

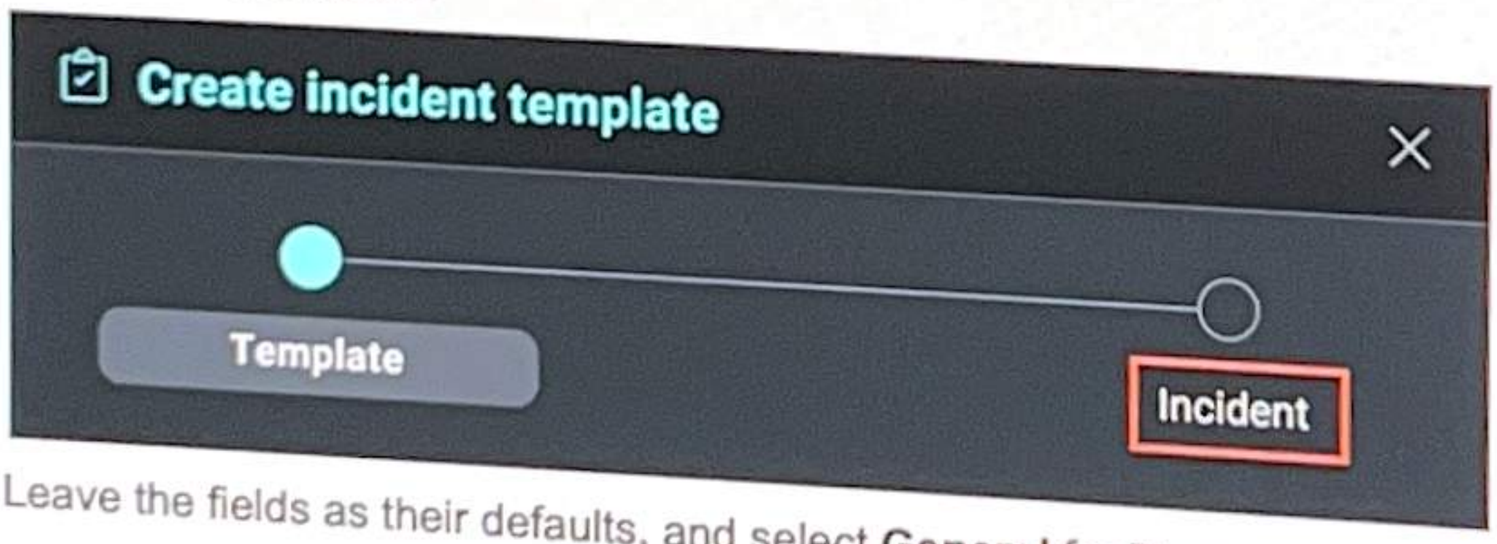
## Lab 6: Create a Custom Incident Template

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".

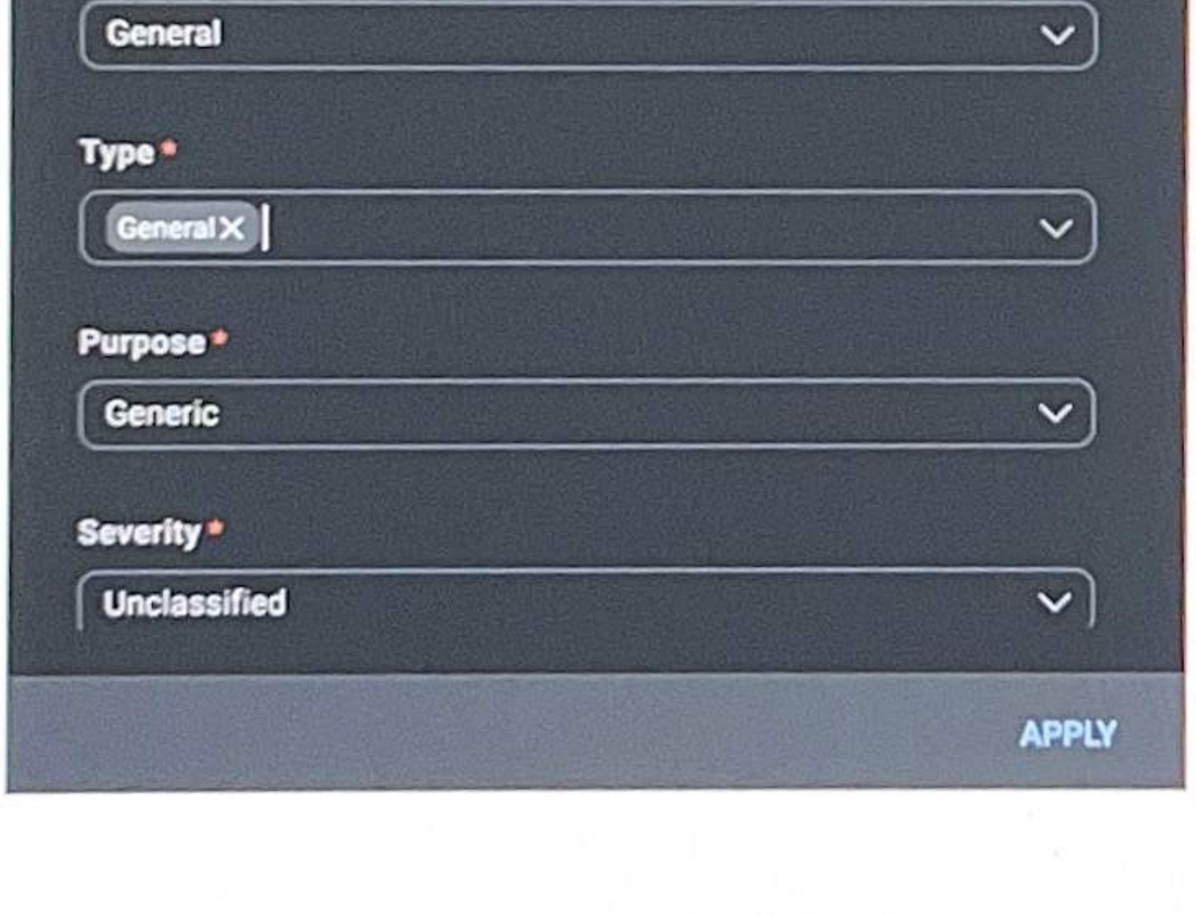



5. Click the **Incident** tab.



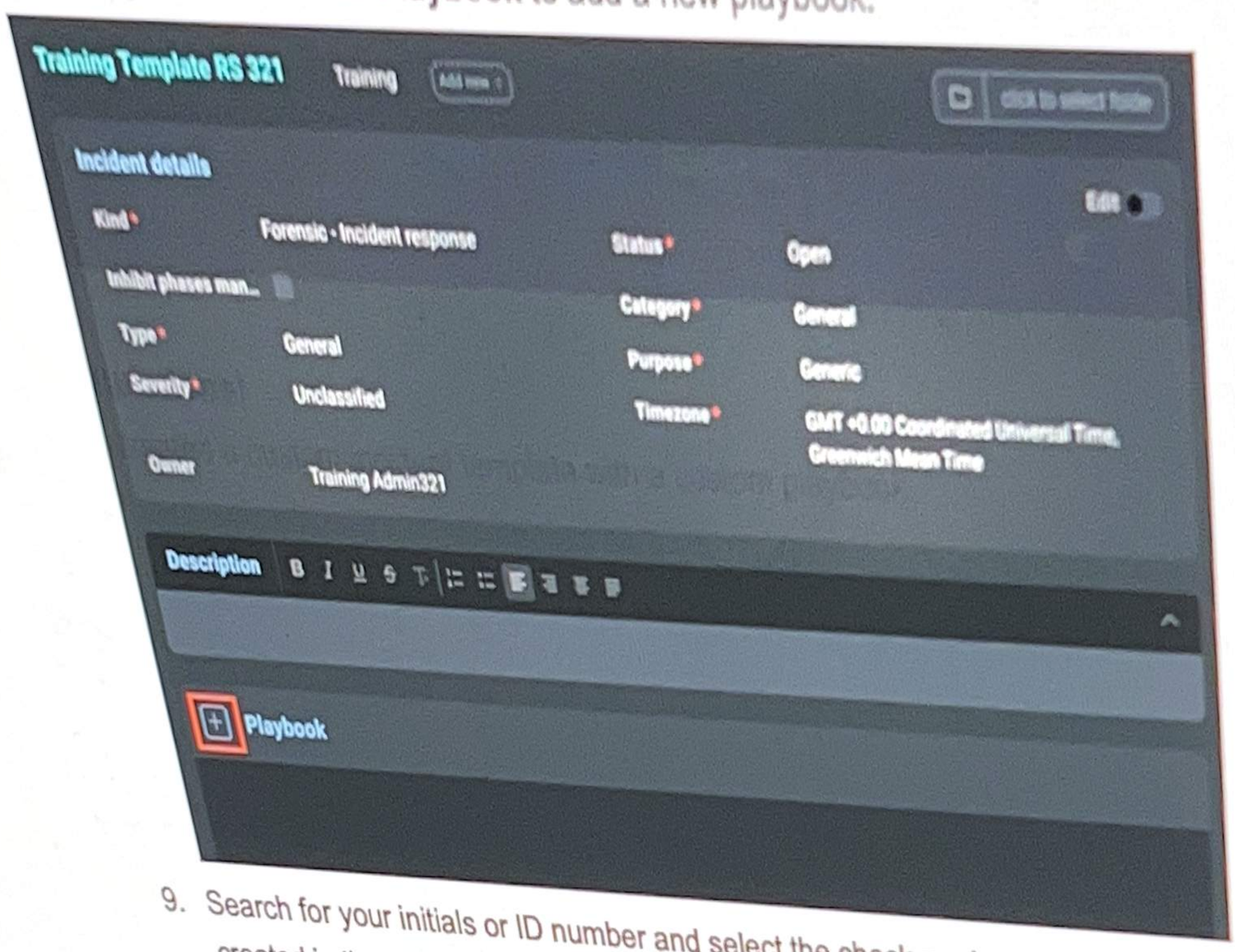

6. Leave the fields as their defaults, and select **General** for **Type**.

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

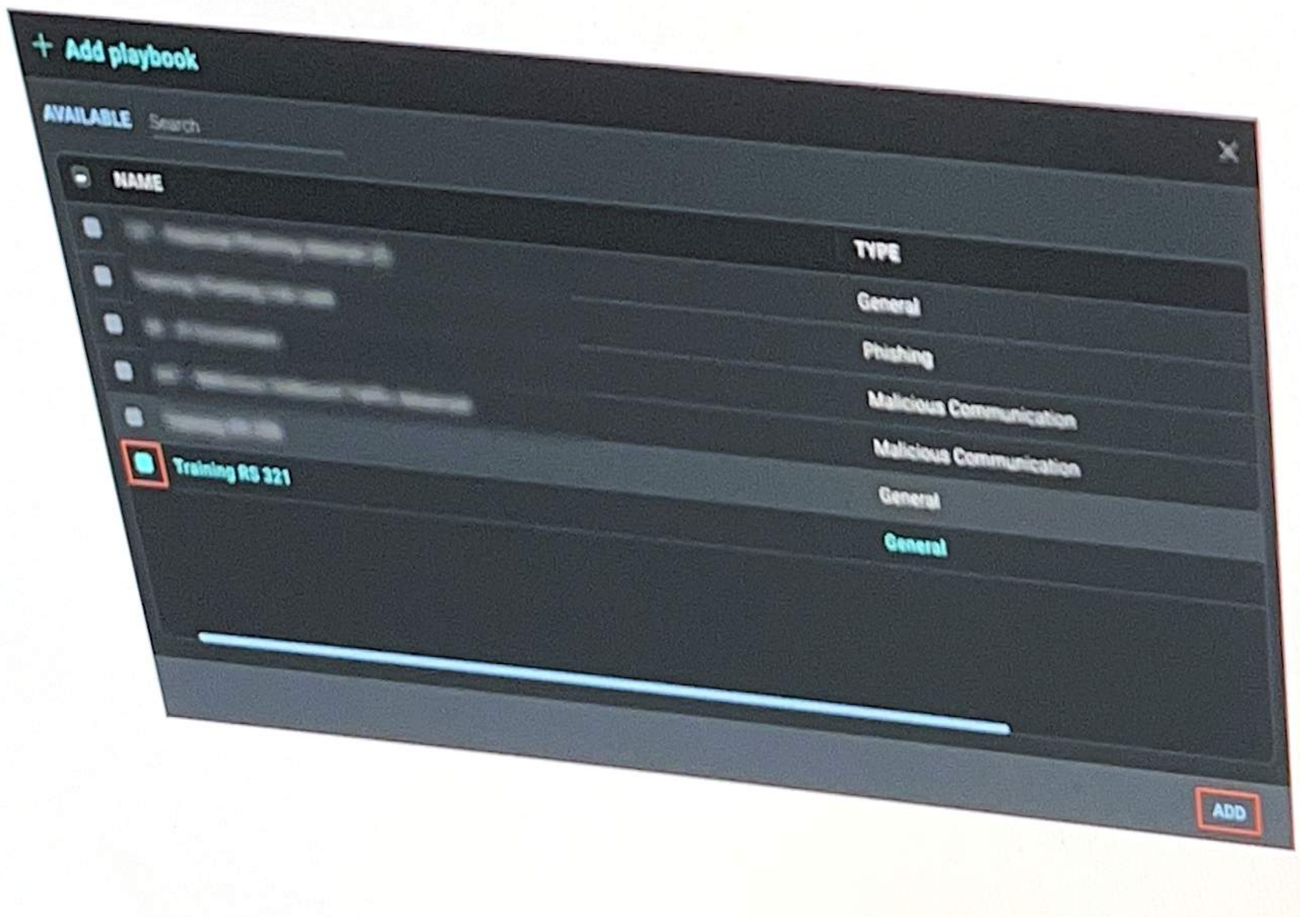


sumo logic

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




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**.



sumo logic

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


**Congratulations!**

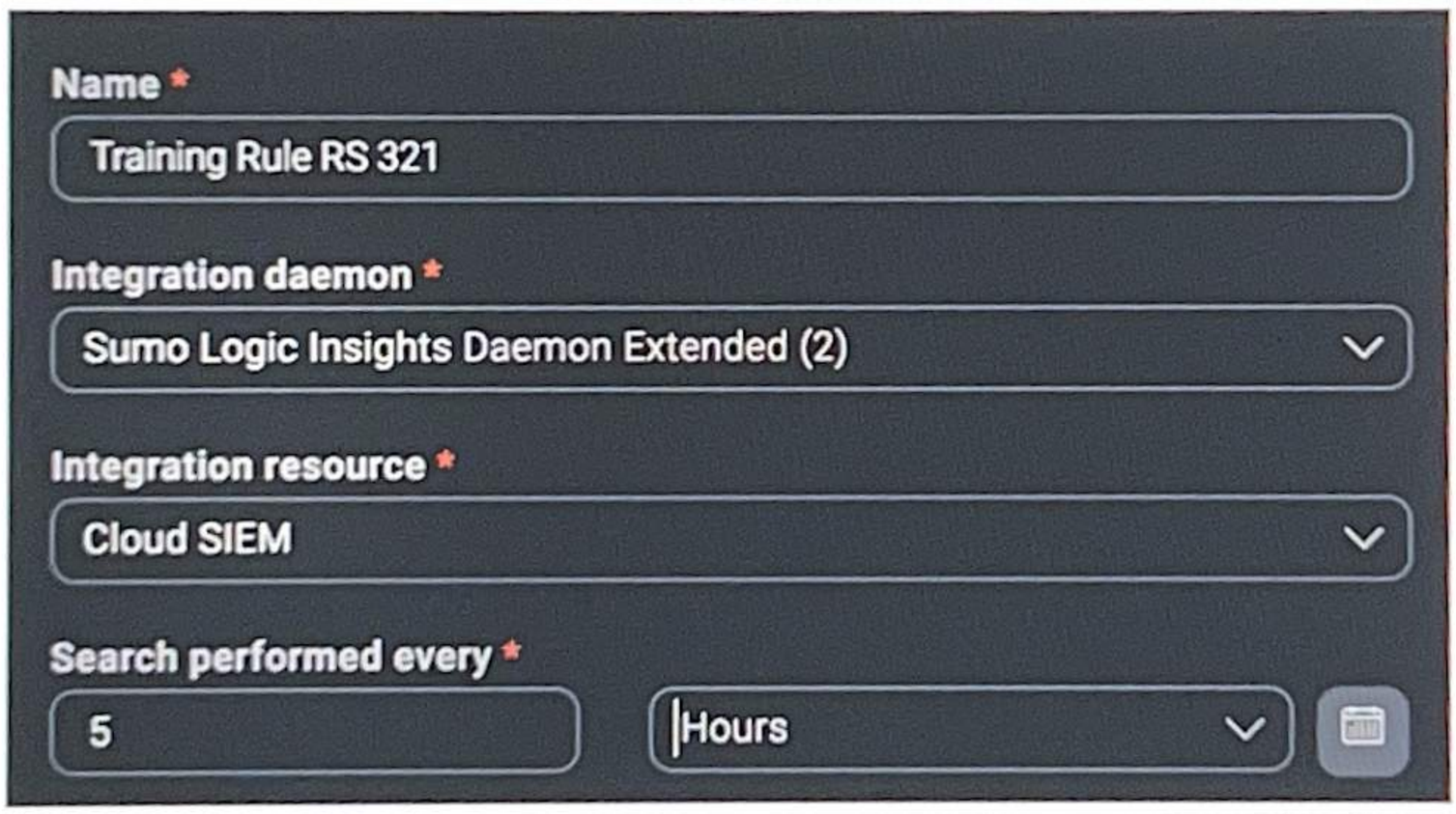
You just created a custom incident template with a custom playbook.

sumo logic

## 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.

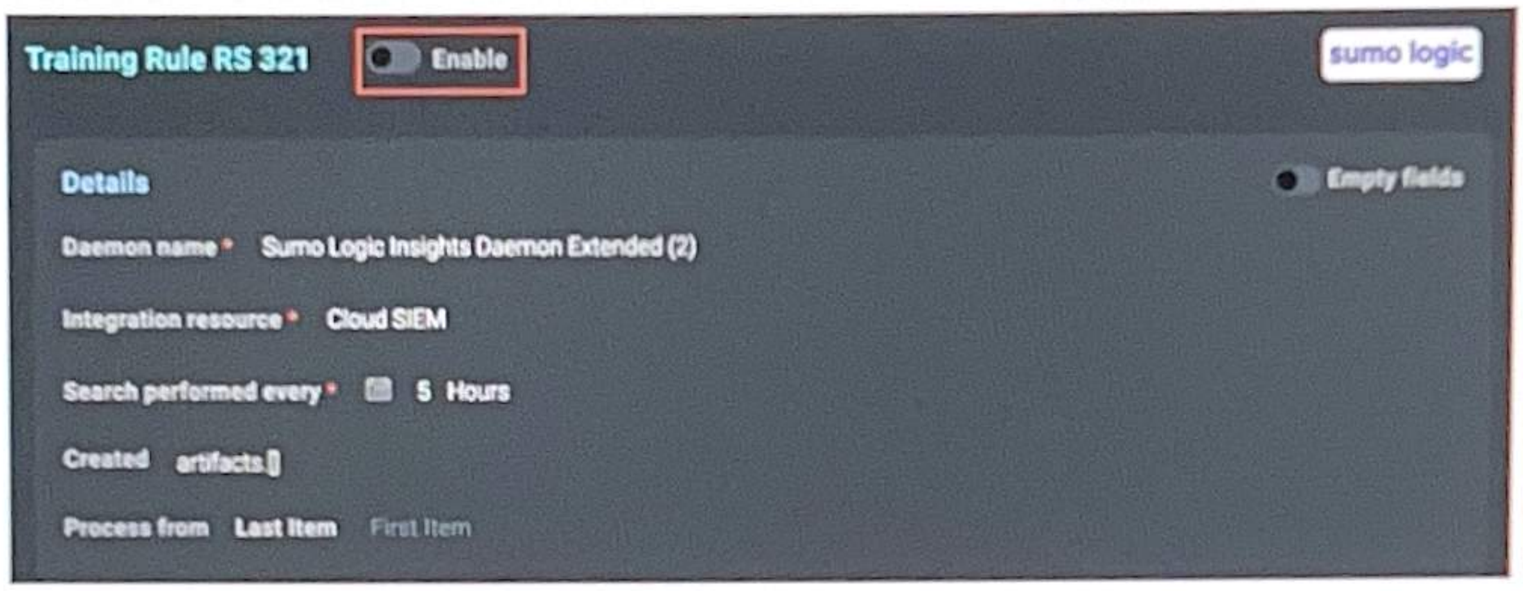
1. In the left navigation menu, click **Automation > Rules**.
2. Near the top, click the **plus icon** to create a new rule.
3. For **Name**, type "Training Rule ###". Replace ### with your initials and/or chosen ID number. For example, if Riya Singh were using training+admin321 as her account, she could 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**.




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.




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.