**AWS Macie: Everything You Need To Know**

With the increasing number of security breaches affecting large and small enterprises, having a well-rounded security platform is more important than ever. Protecting sensitive data like **Personal Identifiable Information** (PII) is a high priority. You’ll feel motivated to automate findings as the amount of data stored in the AWS Cloud rises, so you don’t waste time manually classifying data and allocating rights.

**Amazon Macie** can help you become more conscious of your data and the level of protection you have. We’ll look at what Amazon Macie is, how to set it up in the [AWS Management Console](https://k21academy.com/amazon-web-services/aws-management-console-walkthrough/), and more in this blog post.

**In this blog, you will learn:**

* [**What is Amazon Macie?**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#1)
* [**How does Macie work?**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#2)
* [**Macie benefits**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#3)
* [**Macie use cases**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#4)
* [**Macie set up**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#5)
* [**Macie pricing**](https://k21academy.com/amazon-web-services/aws-certified-security-specialty/aws-macie-everything-you-need-to-know/#6)

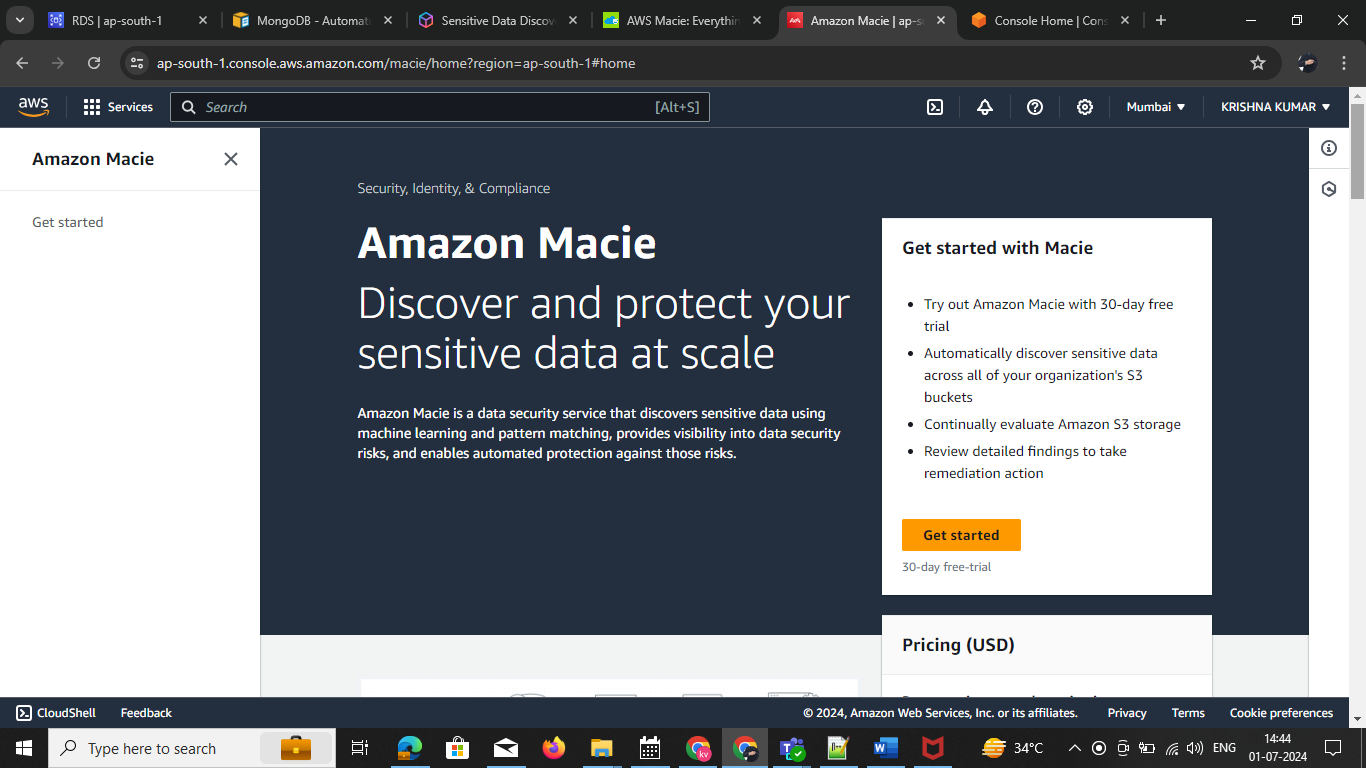
## What is Amazon Macie?

**Amazon Macie** is a security service that uses machine learning to locate, categorize, and protect sensitive data in the Amazon Web Services (AWS) cloud. It currently supports only **Amazon Simple Storage Service** (Amazon S3), while other AWS data stores are being developed.

In your S3 buckets, Macie can distinguish any personally identifiable information (PII) or protected health information (PHI). Macie also keeps an eye on the security and access management of the S3 buckets. All of this can help you comply with requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Privacy Regulation (GDPR), as well as retain the [AWS Cloud security](https://k21academy.com/amazon-web-services/aws-security-services/) you require.

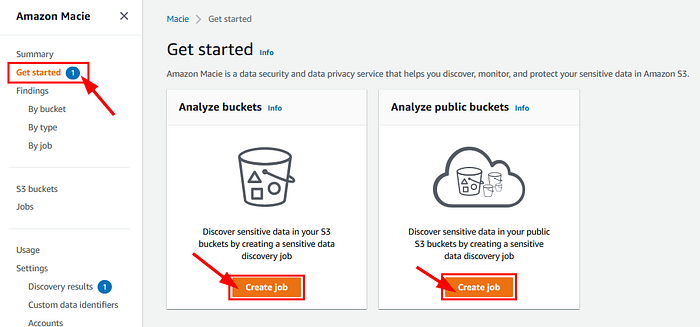
**In general, Macie helps you answer these questions about your data:**

* What methods can I use to classify data in real-time?
* What is its location?
* How do I create remediation workflows for my security and compliance requirements?
* In my S3 buckets, what data do I have?
* What personally identifiable information (PII) or protected health information (PHI) could be made public?
* Data is exchanged and kept in two ways: publicly and privately.

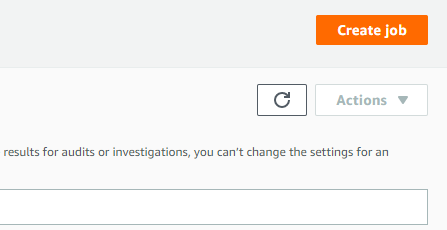
** STEP1:** Goto AWS Macie -🡪 click get start

**2** Before enabling the “**Job”**we need to have data for analysis which need to be stored the data in S3. Store some data in S3 by creating a bucket and upload objects and needed permissions according to your consideration.

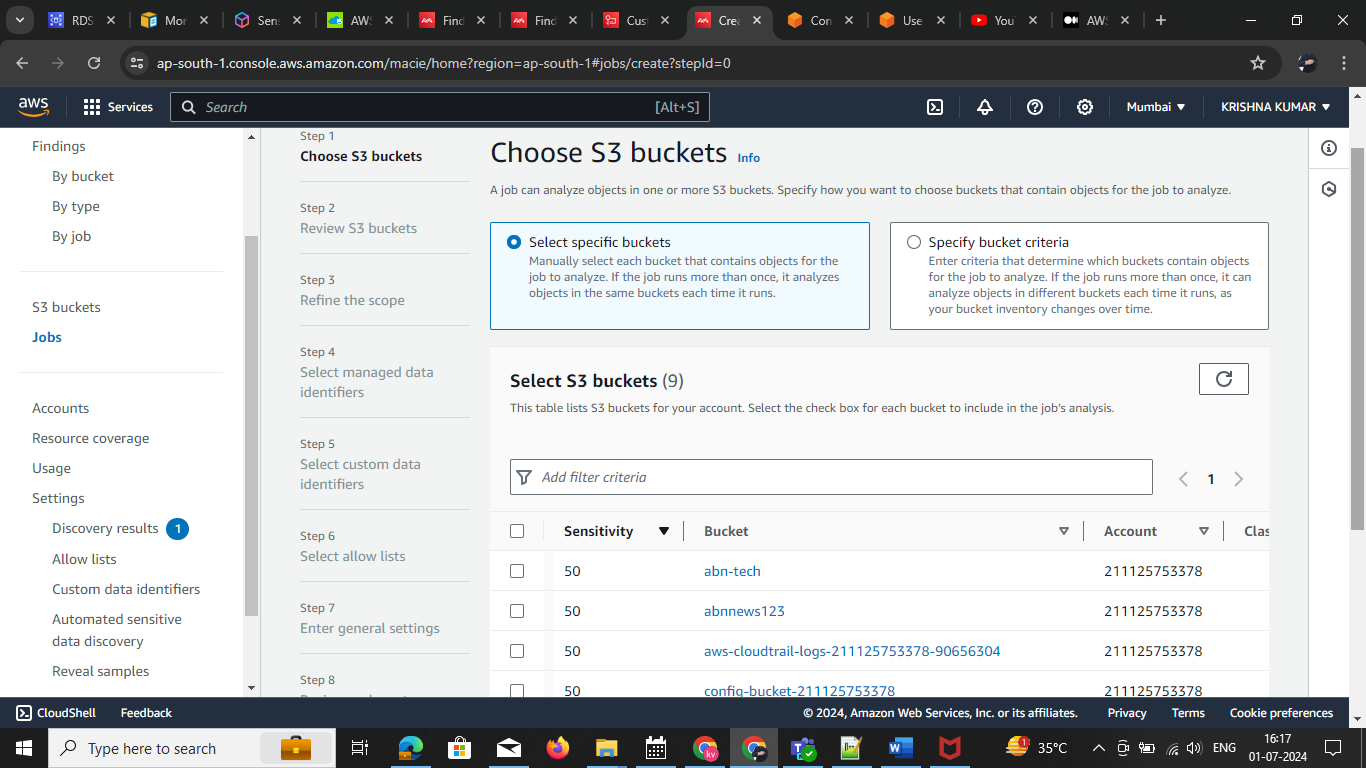
**3** And then just click on **“Get started”** in the menu and select which **“Job”** you want to start.



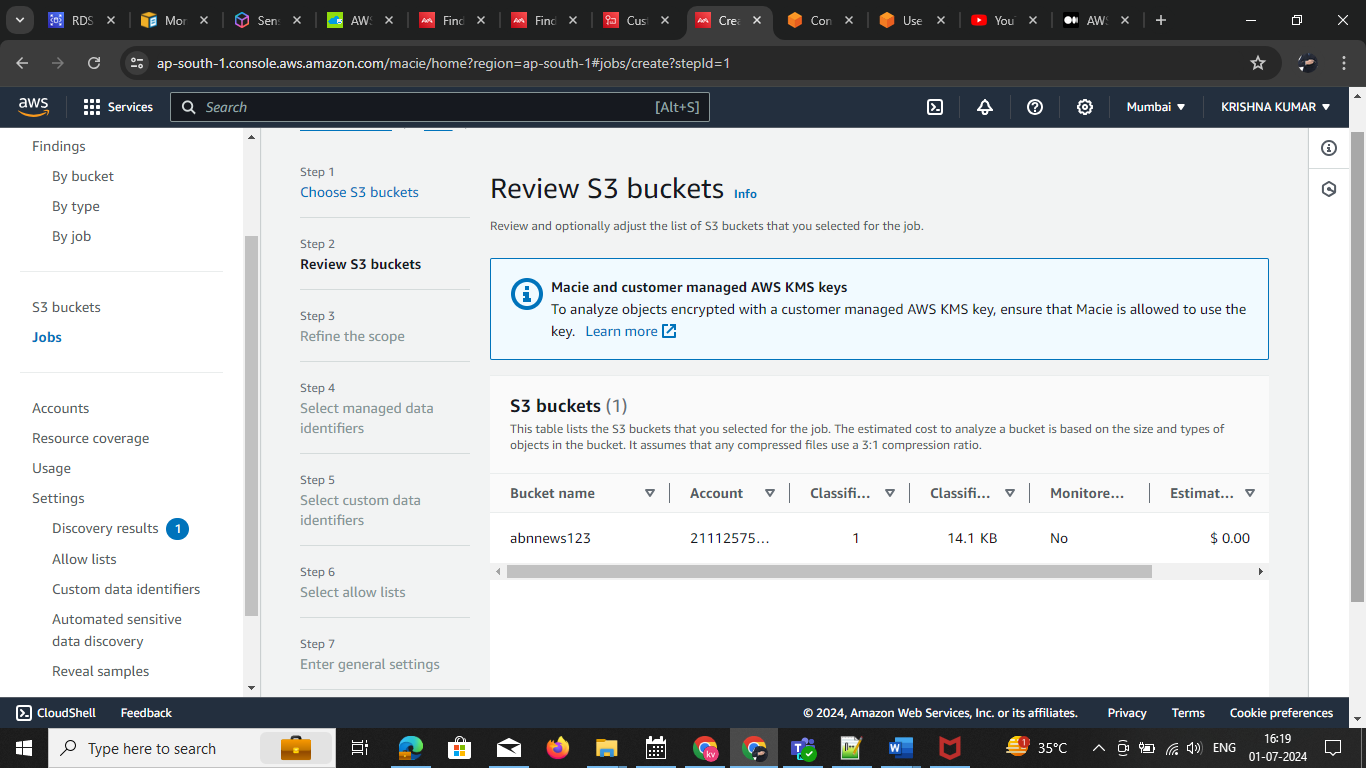
**5.**Just click on **“Create job”**



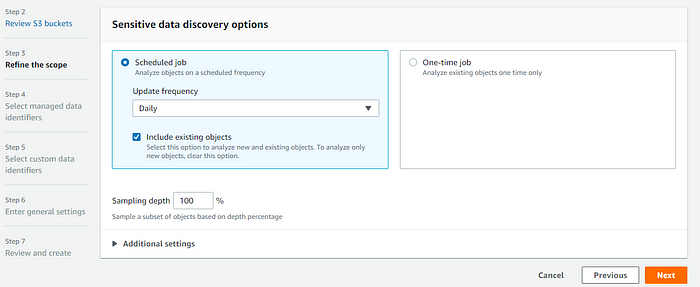
Click on the criteria you desire “select specific buckets” or “select specific bucket criteria”. And choose the buckets you want to monitor manually by clicking the check box. Click next.

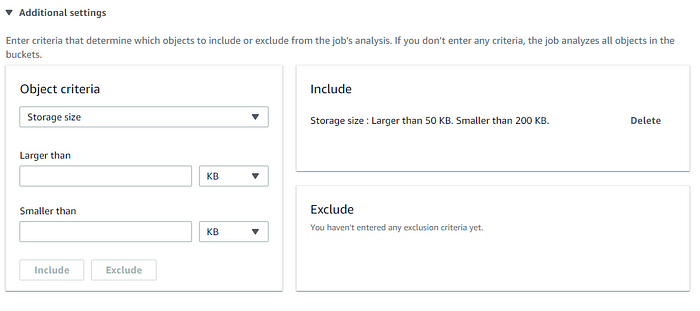


**6.**Review the buckets to make sure the needed buckets are added. Click “**Next”**

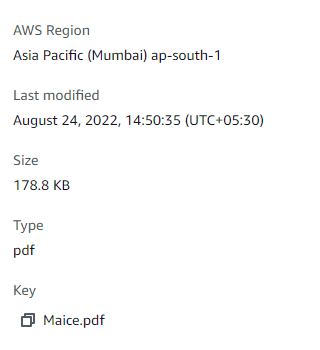


**7.** Choose the scheduled job or one-time job as per your requirement. Here i am selecting a one-time job. In additional settings, We have included or excluded different options. Here I am selecting the storage size and specifying between 50 KB to 200 KB. 8:We have different options here in object criteria and select according to your requirement. Click Next. In my case select one job

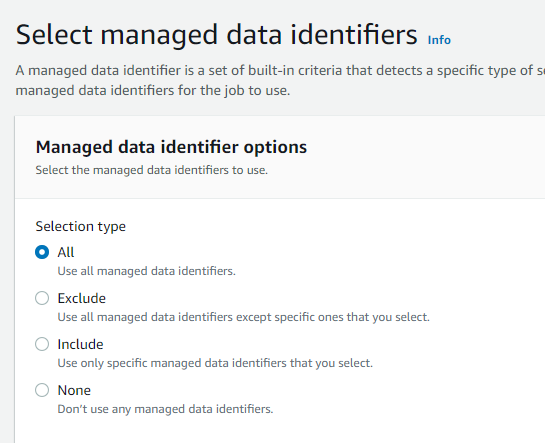




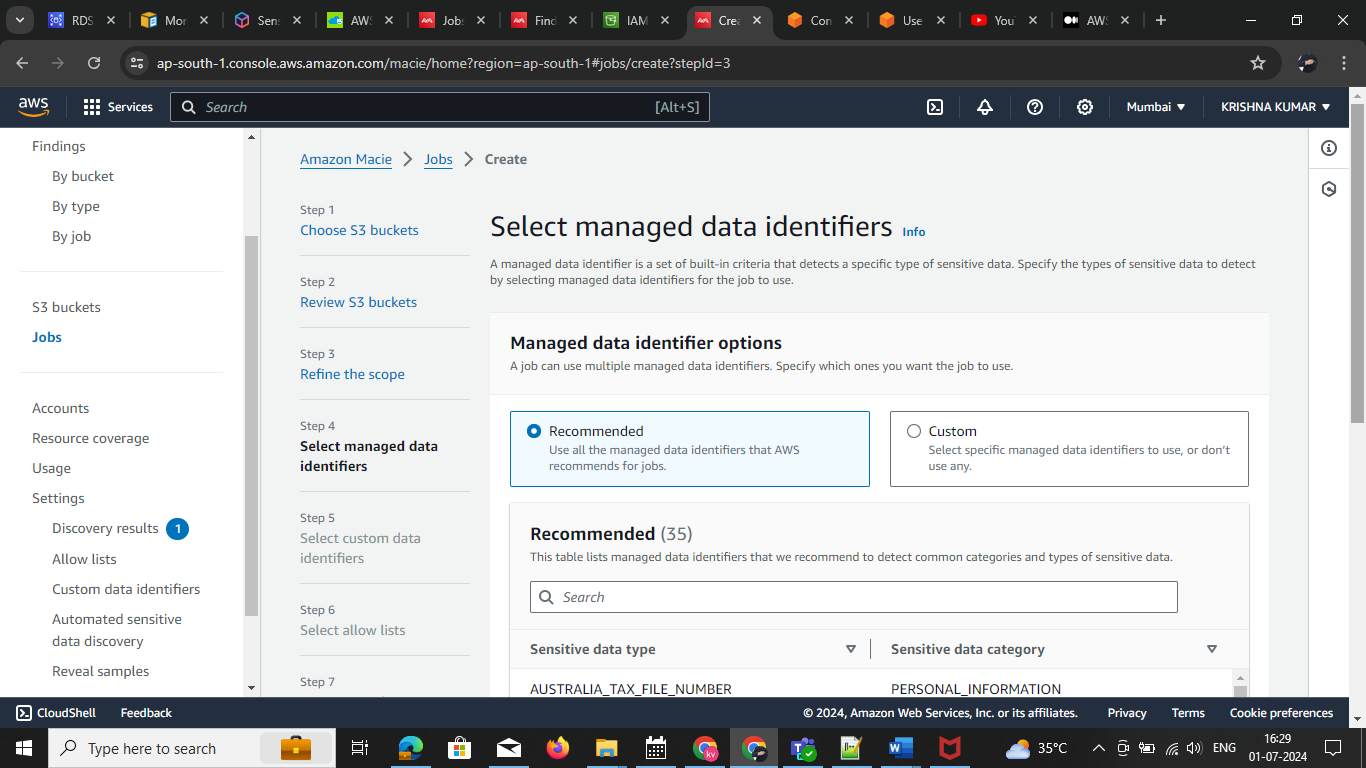
For reference, I am adding the screenshot of the size of the file i uploaded in S3 bucket.



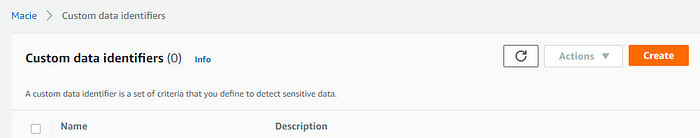
**9.**Select manage data identifiers. Click next. In my case select inclu



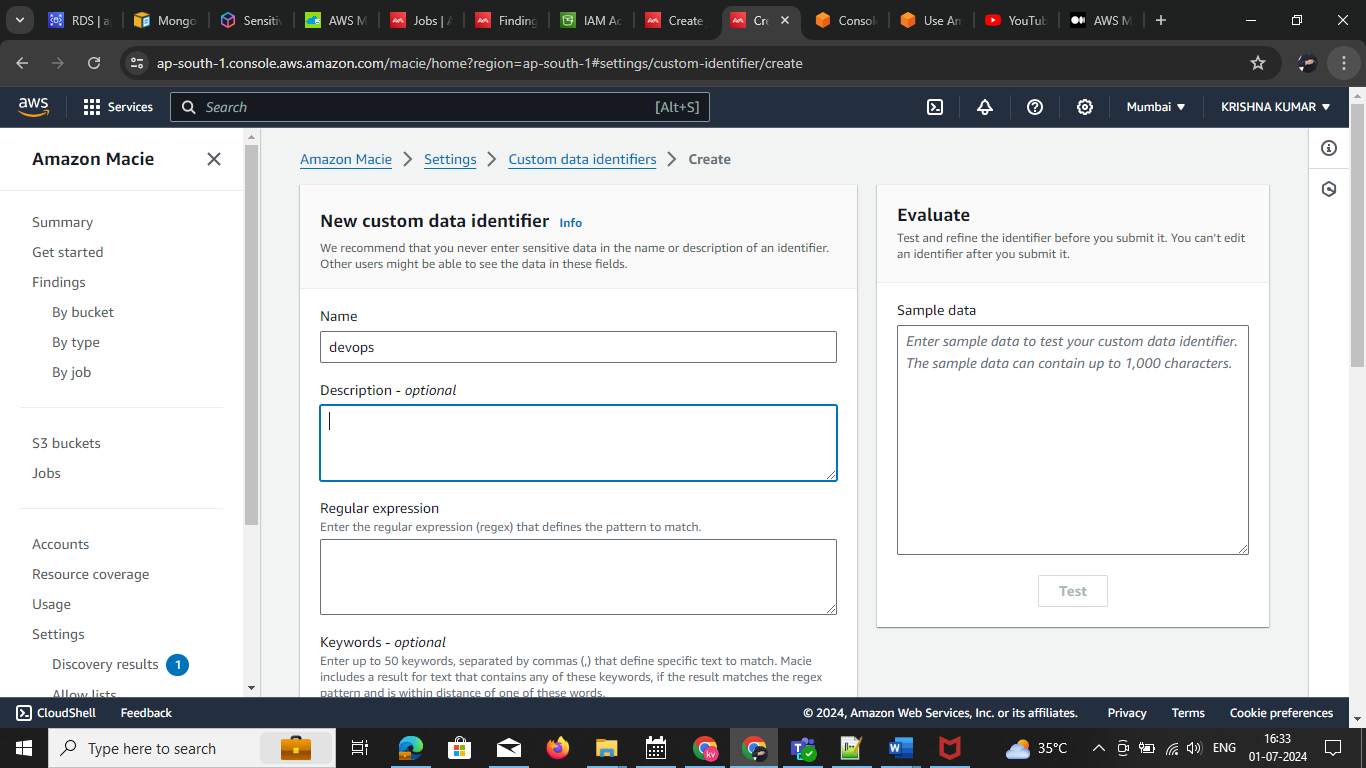
**10.**To create custom identifiers for better scanning we need to click on manage custom identifiers. Select the any one based on req

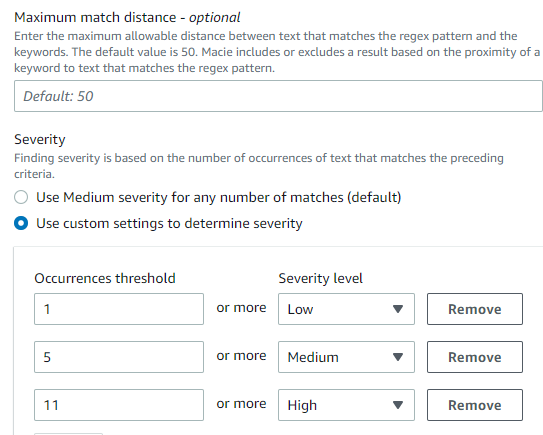


**11.**It will redirect to these pages. And click on create. Here we are customizing it in regex expressions by entering [0–9] expression any data present in the object. And customizing severity based on the number you prefer. Click on create.

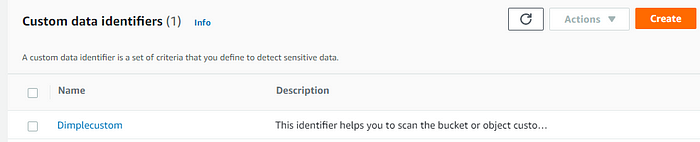


Note : if you need to create the custom data go to this process

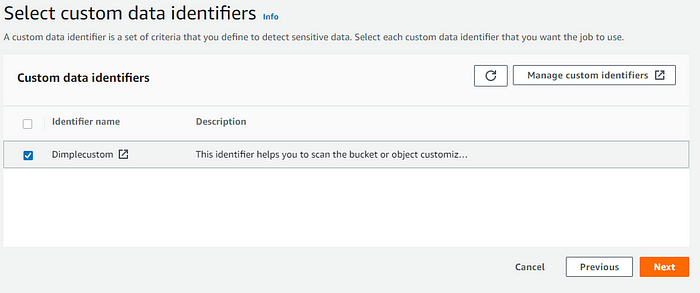




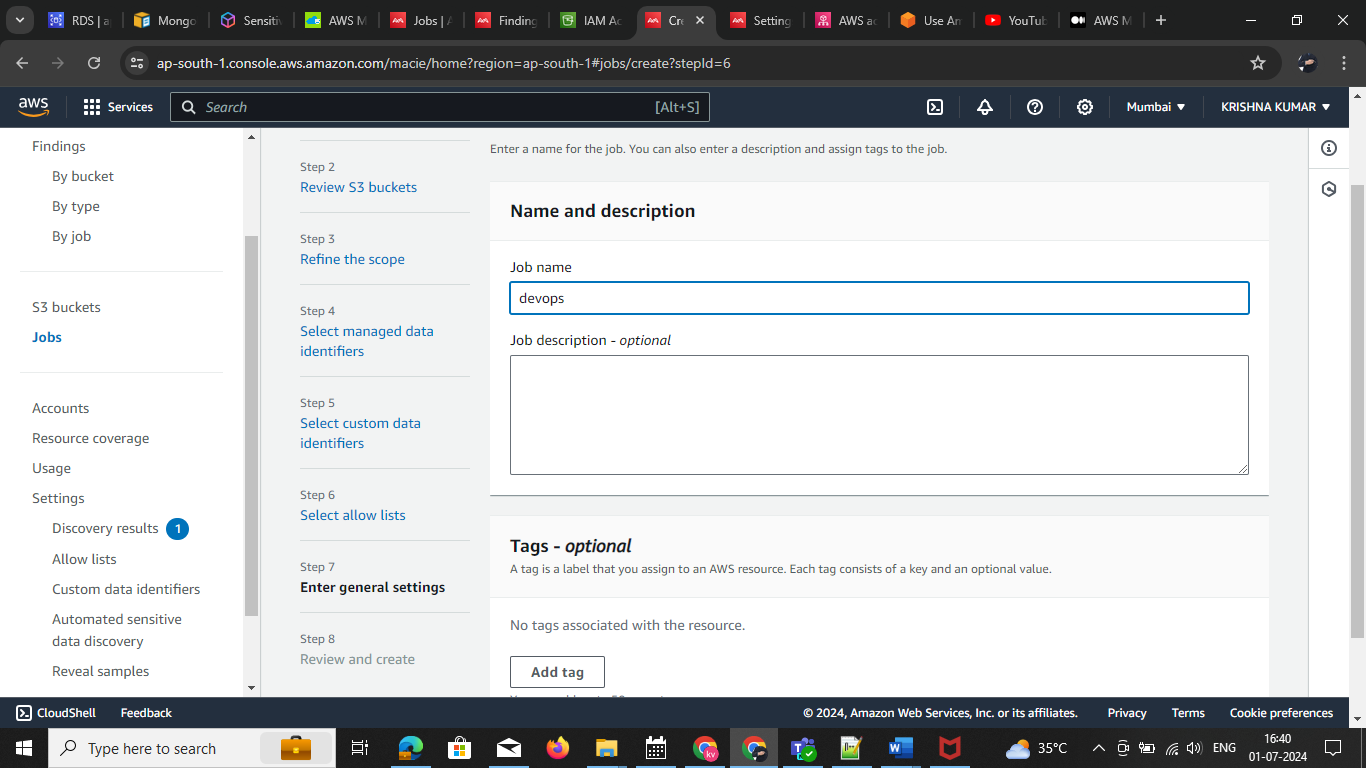
We can find the Custom data identifiers. We created before.



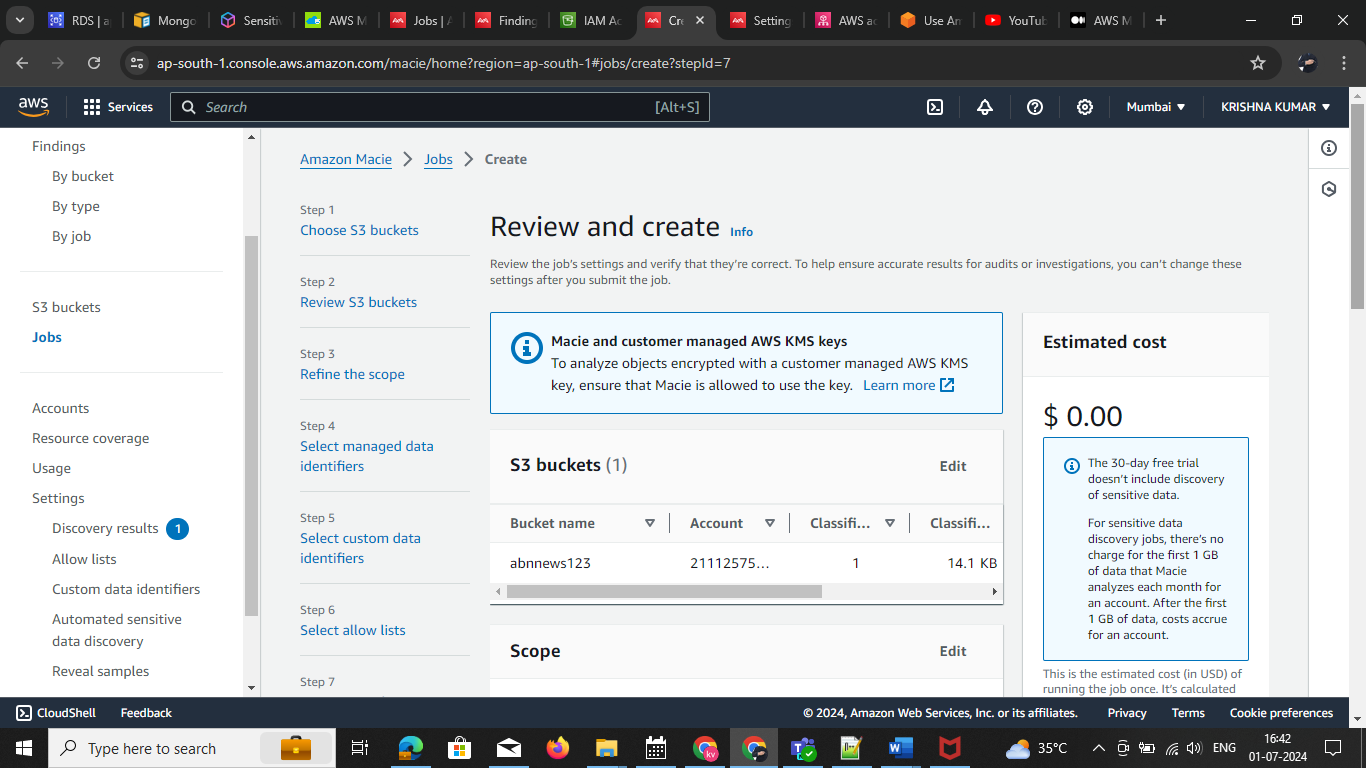
**12.**Select the job we created for custom identifiers. Click next.

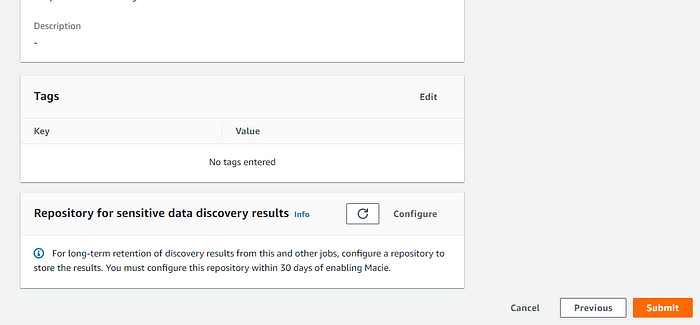


**13.**Give a job name and tags click next**.** In my JOB NAME IS DEVOPS

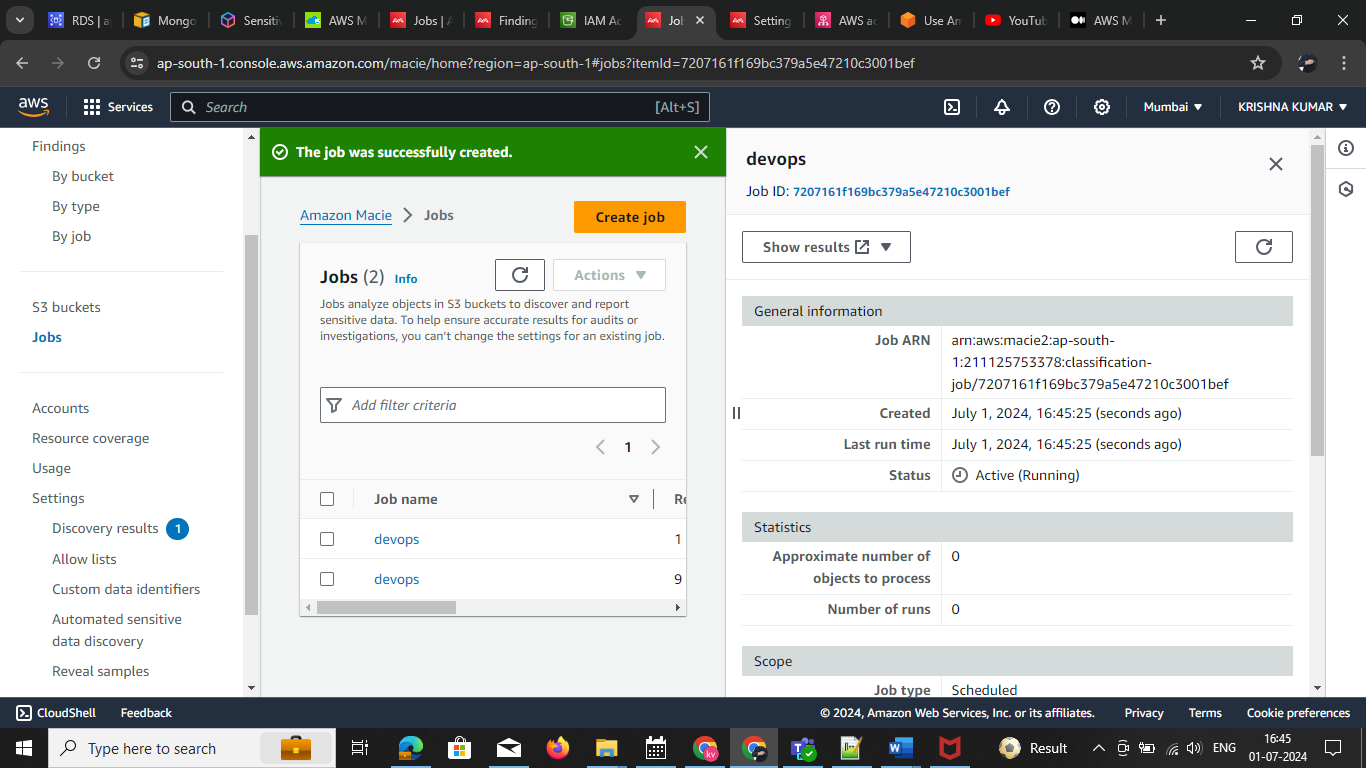


**14.**Review and create it.

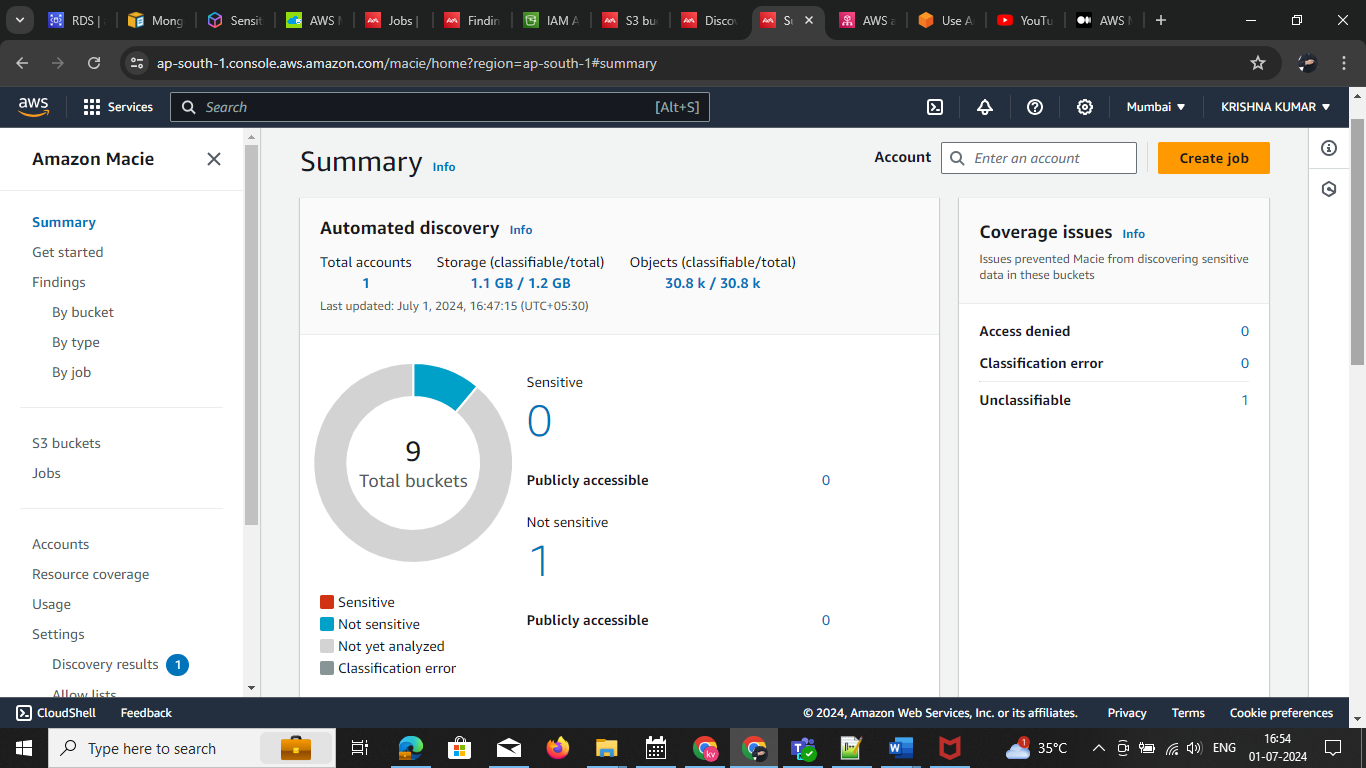


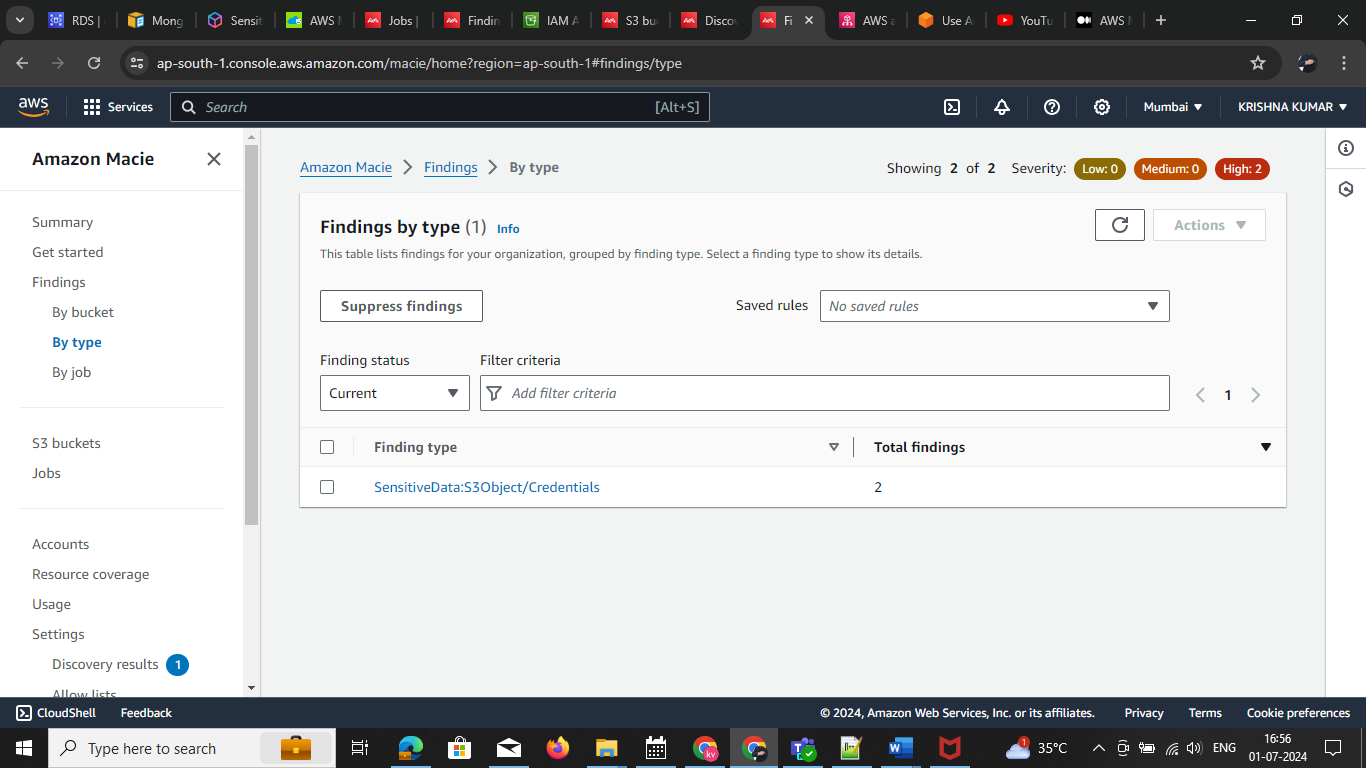
click on submit

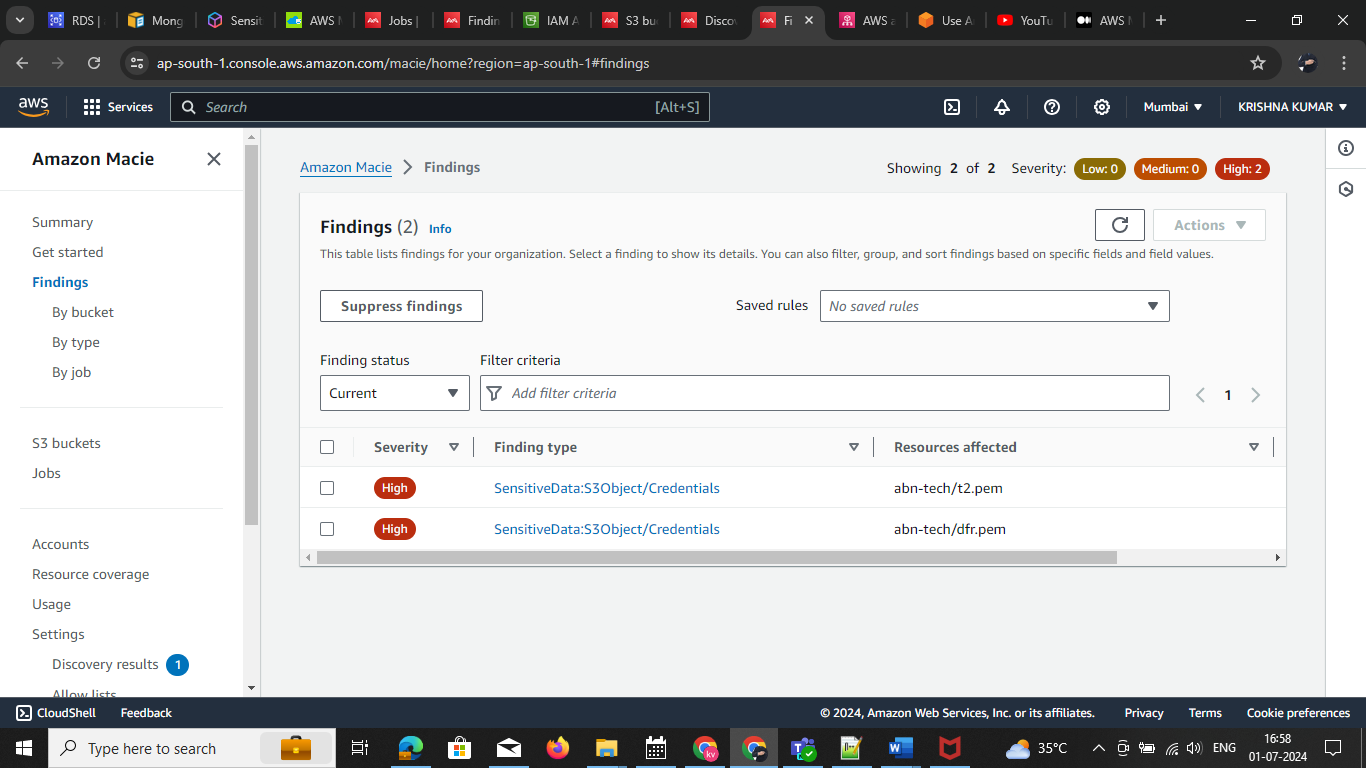
**15.**Here we find the result and the necessary details we need according to our configuration.



**Check the summary**



click on the type



Note: I my s3 bucket adding. Pem keys getting warning

Amazon Macie makes data privacy across the whole Amazon S3 environment simple, delivering insights that you may utilise to respond promptly as needed. Macie also allows you to identify sensitive data in other data repositories by temporarily transferring it to S3.