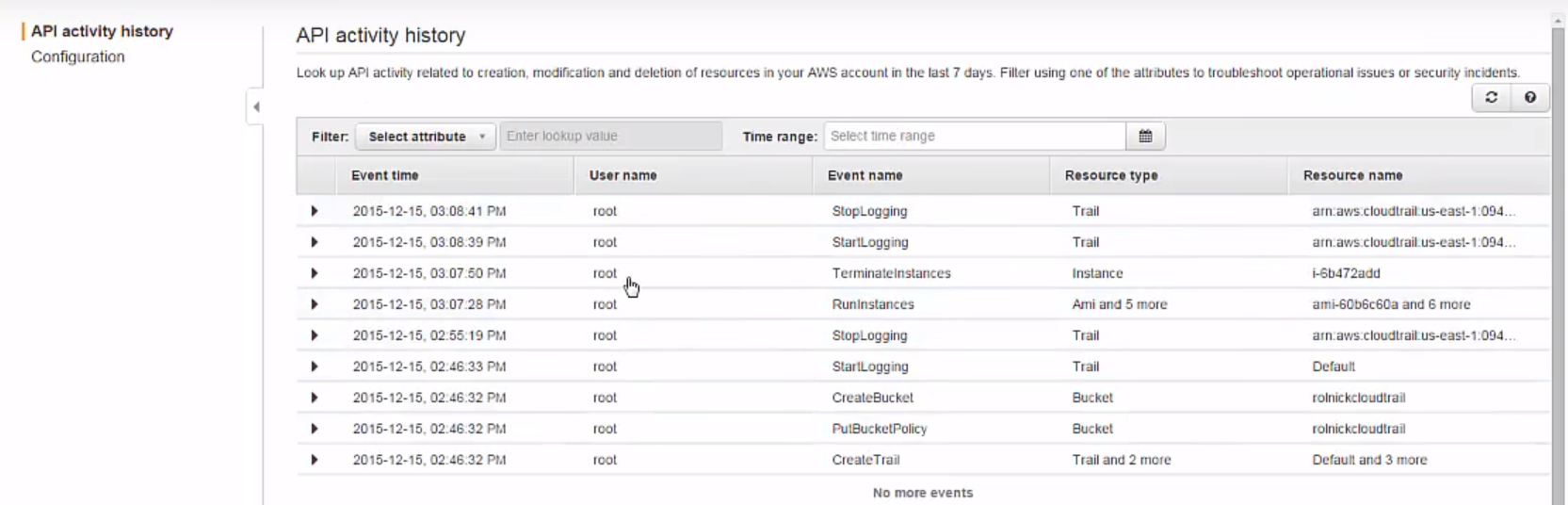
**Cloud Trail** is a service that enables you to do:

1. compliance to either: a.) internal standards or

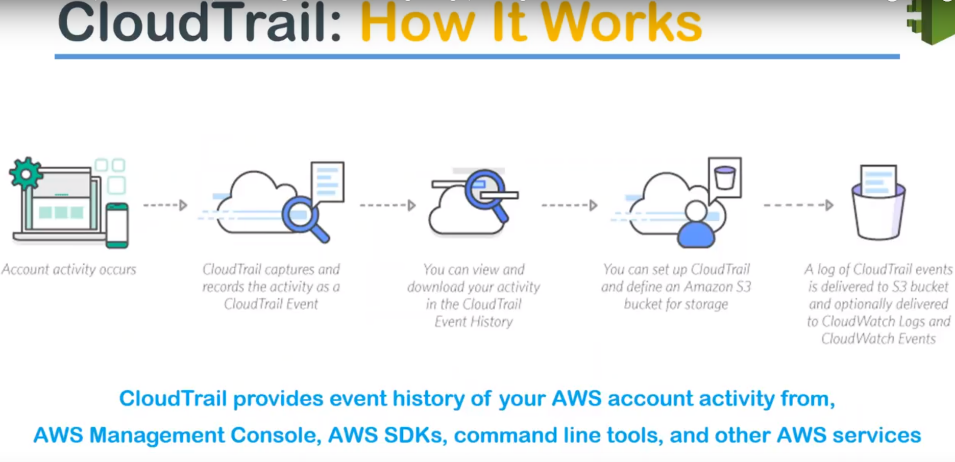
b.) third-party regulatory authority standards

1. helps you to comply with the governance policies set by your organization
2. helps you to achieve an operational auditing

or even in risk auditing.



If we go here, we can see all different API calls happened …Who is Done what???



what happens is, when we setup **Cloud Trail** in our a/c is:

* it starts monitoring all the API activity that is happening in your account either from your console or your AWS CLI or even your SDKs.
* All this activity is logged into your s3 bucket and
* from there you can process it using a cloud watch events or any third party log management systems.

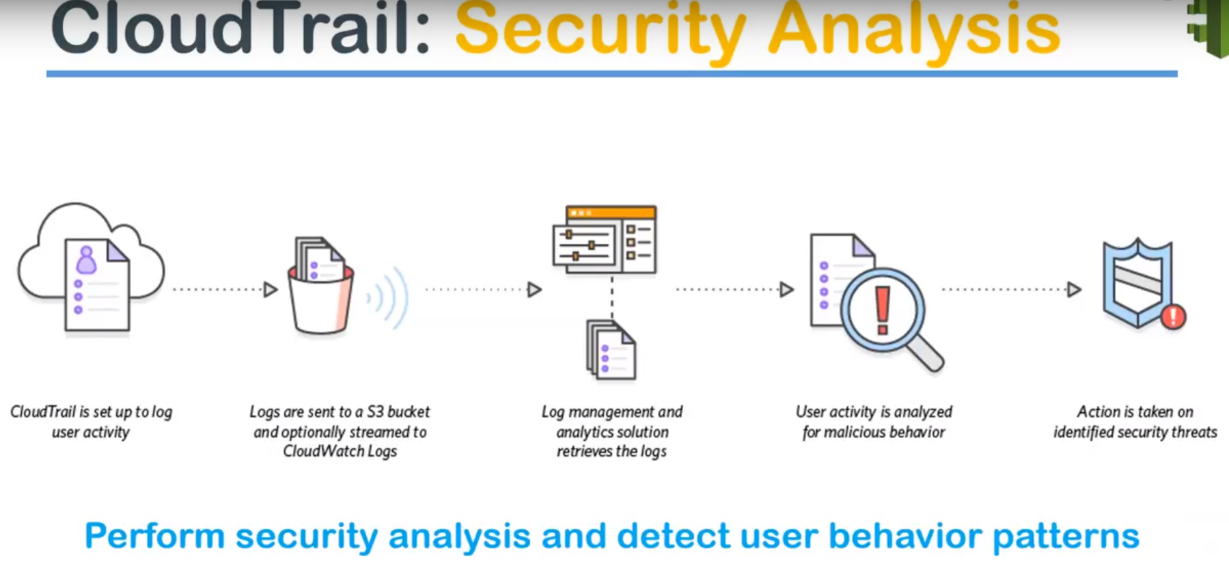
**Let us see common use cases** is a compliance aid

where audit agency or a third party security authority is looking for a certain amount of a log information then you can go to your S3 Bucket, where the encrypted logs are stored and then you decrypt them and retrieve the logs and provide your auditor…with all that information.

and the logs are reviewed for any unauthorized access and the compliance activity is successfully completed.

That is one-way people use **Cloud Trail.**

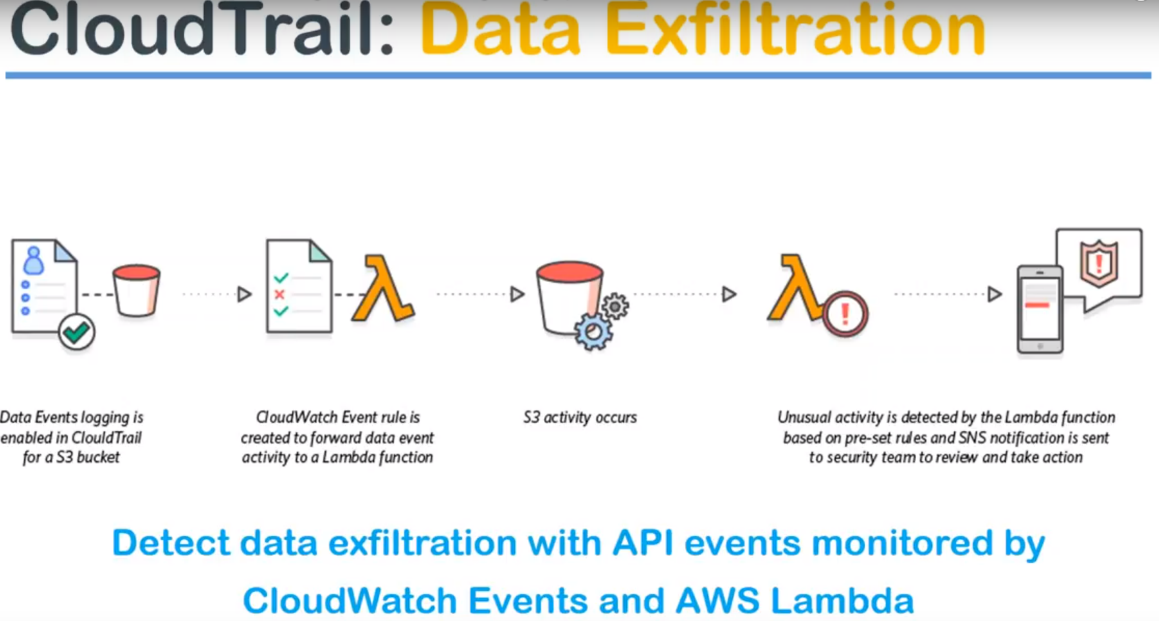
**Other use case** is for **security analysis:**

****

For example: Let’s say… you have all the logs stored in your s3 bucket and you want to find any malicious user activity or any unauthorized activity happening.

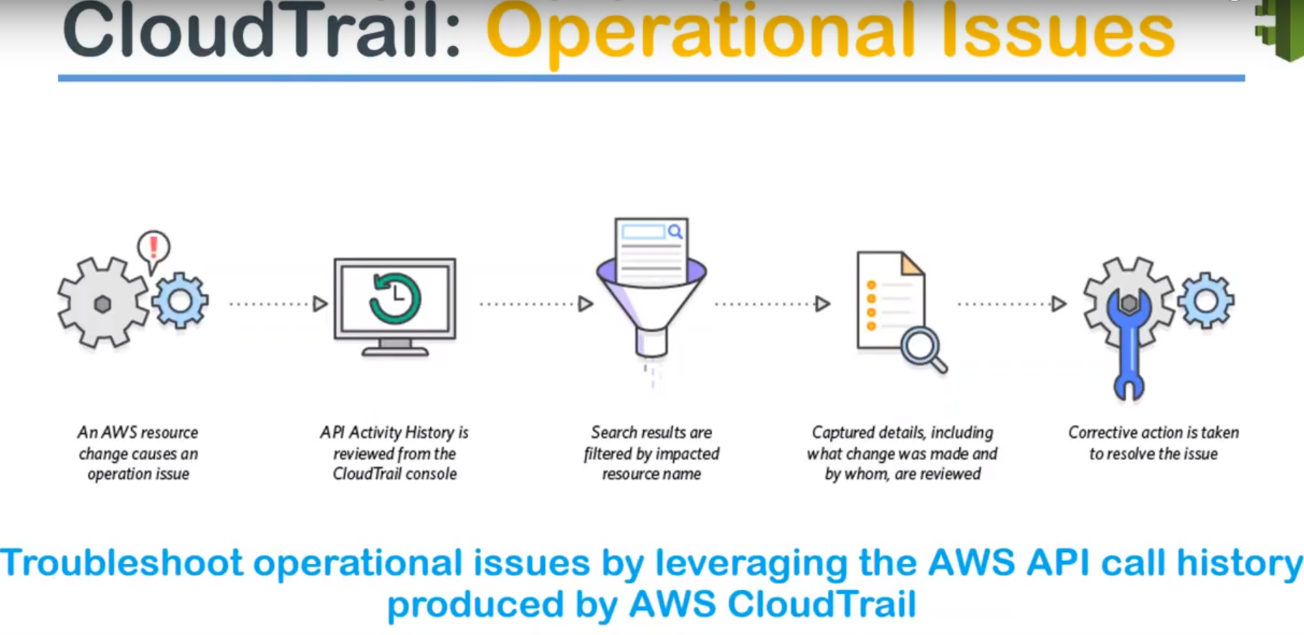
So you can feed all the logs from your s3 bucket and then send it to a third party log management system and then find out any anomalous behavior and create an event or a threat analysis from that point onwards.

UseCase-3: **data exfiltration.**



If you want to identify if somebody's copying some data from your s3 bucket or if you're suspicious that some event might have be happening in your data management platform…. then what you can do is:

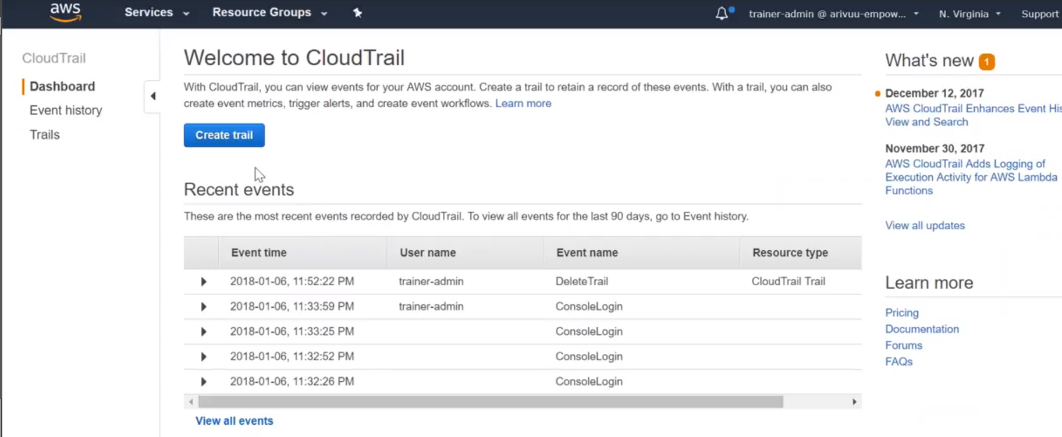
You pick up the API events from your cloud trail and then you can fit into your lambda and then the lambda can identify whether it is an authorized access or an unusual activities happening and then it can run some preventive or corrective actions depending upon the pre-set rules that has been configured.

**UseCase-4:**  operational issues ****

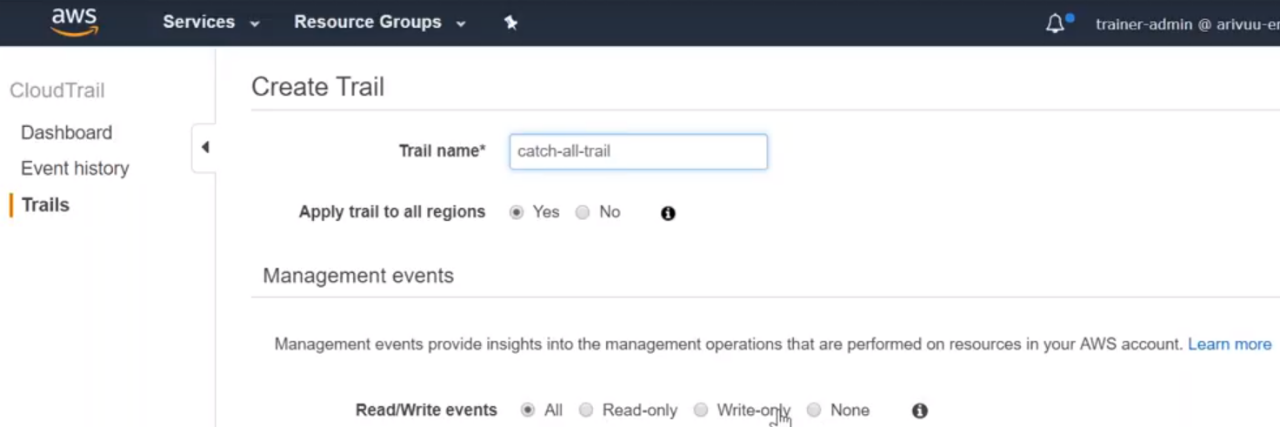
let us say there's an AWS resource changed…Let’s say somebody has modified something and you are not sure what exactly caused the issue then the best thing that you can do is :

Best thing to do is : Goto API activity history in the cloud trail events and try to find out what was the cause of the problem and then quickly resolve issues so that the outage or the service downtime… that is passed by the change is not pro-longed.

That way Cloud trail increases your operational issue troubleshooting time.

1.)

cloud trail dashboard…Create Trail

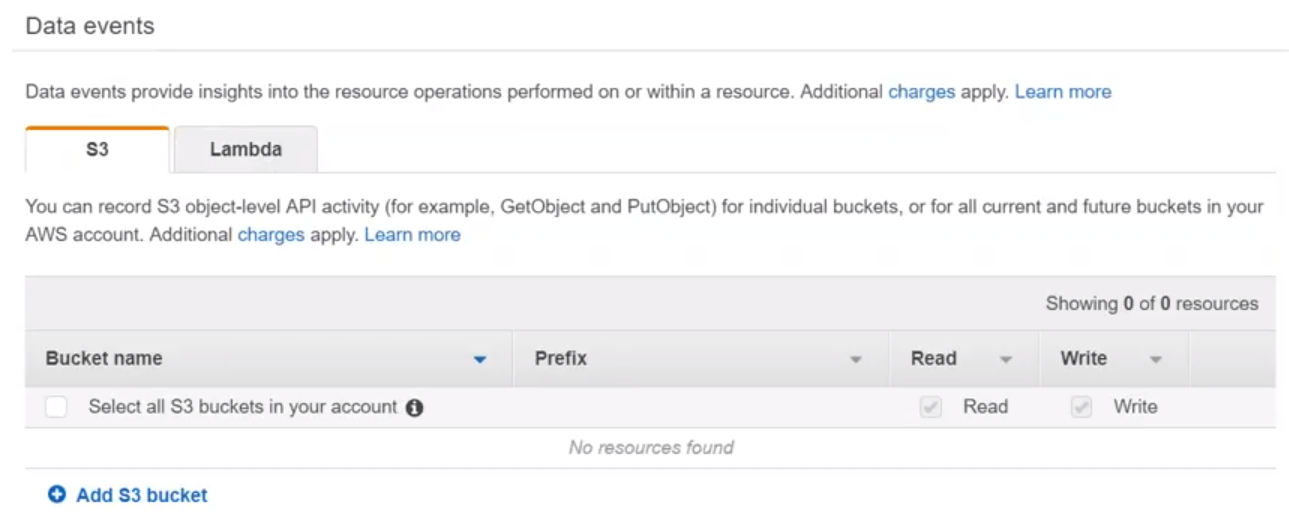
2.)

Cloudtrail name:

Apply to all regions..

Read and write events

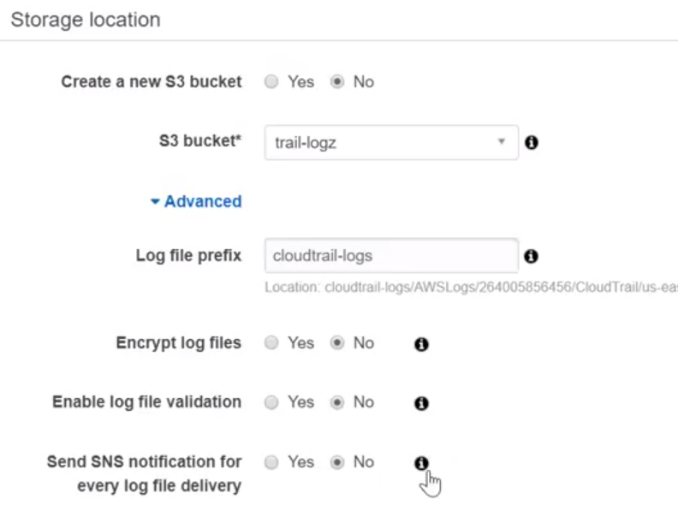
3.)



capture all/ particular events related to s3 or lambda.

let us not go to fine-grained detail at this moment and capture everything..

4.)Where to store this logs??



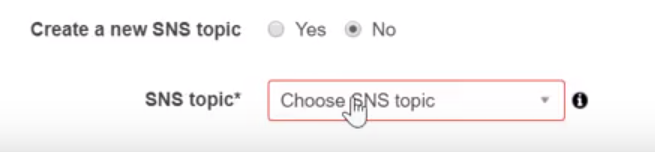
Bucketname

Prefix

Version logs?

Encrypt logs?

SNS logs



Select SNS and give topic name…

