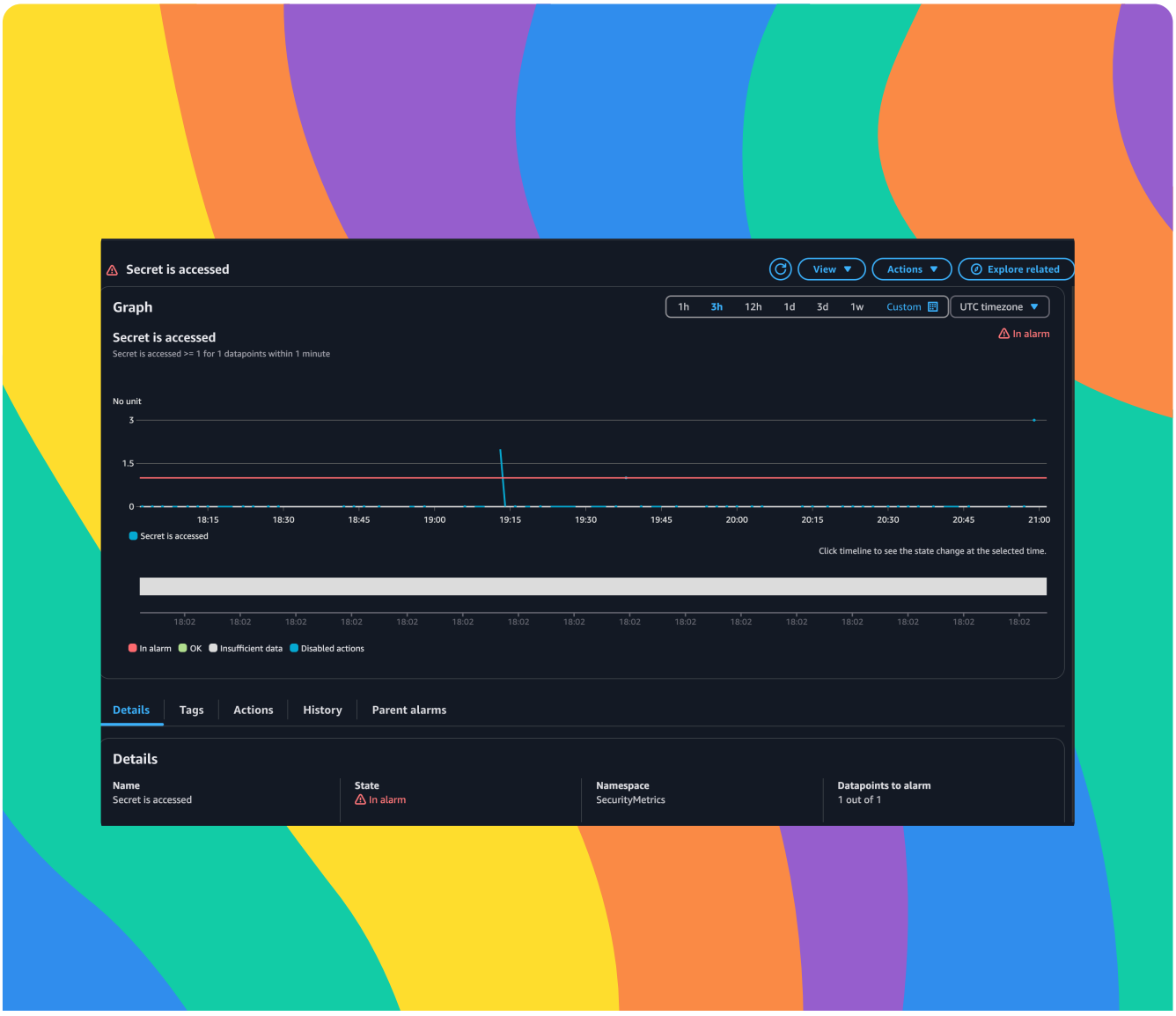
nextwork.org

Build a Security Monitoring System

TA

tahirgroot@gmail.com

https://medium.com/@tahirbalarabe2/how-to-moni...



TA
tahirgroot@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

In this project, I will demonstrate how to setup a monitoring system in AWS using CloudTrail, CloudWatch and SNS! I am doing this project to learn how security and monitoring services in AWS work, plus have a working system that acutally sends emails too.

Tools and concepts

Services I used were CloudTrail, Cloud Watch and SNS I also used Secrets manager IAM (roles) and S3 buckets. Key concepts I learnt include secret storing, CloudWatch vs Cloud Trail, what are notifications and different kinds of end points, how to create a Coud watch filter and alarm

Project reflection

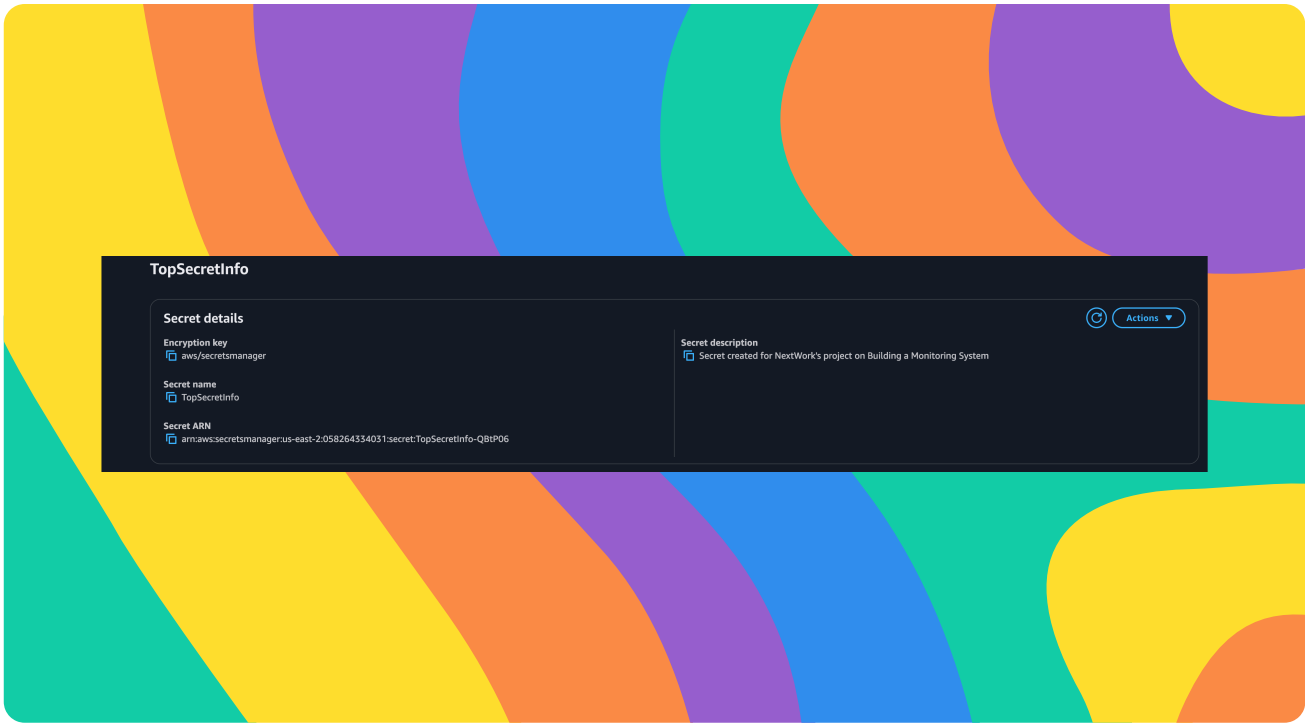
This project took me approximately 3 hours The most challenging part was troubleshooting why the email wasnt delivering in our first test. It would be frustrating when an error is happening but they are no error logs or error messages. It was most rewarding to compare Cloud Trail, SNS Notification and Alarms.

TA
tahirgroot@gmail.com
NextWork Student

Create a Secret

Secrets Manager is AWS' security service for storing secrets. i.e. database credentials, account ids, api keys...anything that is sensitive information that would cause damage/trouble if it got leaked and shouldn't be lying around in code.

To set up for my project, I created a secret called TopSecretInfo in Secrets Manager. This secret contains that contains a hot take from me... I mentioned that i need 3 coffees a day to function



TA
tahirgroot@gmail.com
NextWork Student

Set Up CloudTrail

CloudTrail is a monitoring service it is used to track events and activities in my AWS account. These logs are very helpful for security(i.e detecting suspicious activity), compliance (i.e. proving that you 're following the rules or something). and troubleshooting(i.e identifying what happened/changed if something breaks).

CloudTrail events include types like management data, insights and network activity events. In this project, I set up my trail in track management event because accessing a secret falls into that category. It is not a data event (which capures high voulme actions perfomed on resoruces) becuase all management events are free to track(and AWS lets us track security operations like this for free)!

Read vs Write Activity

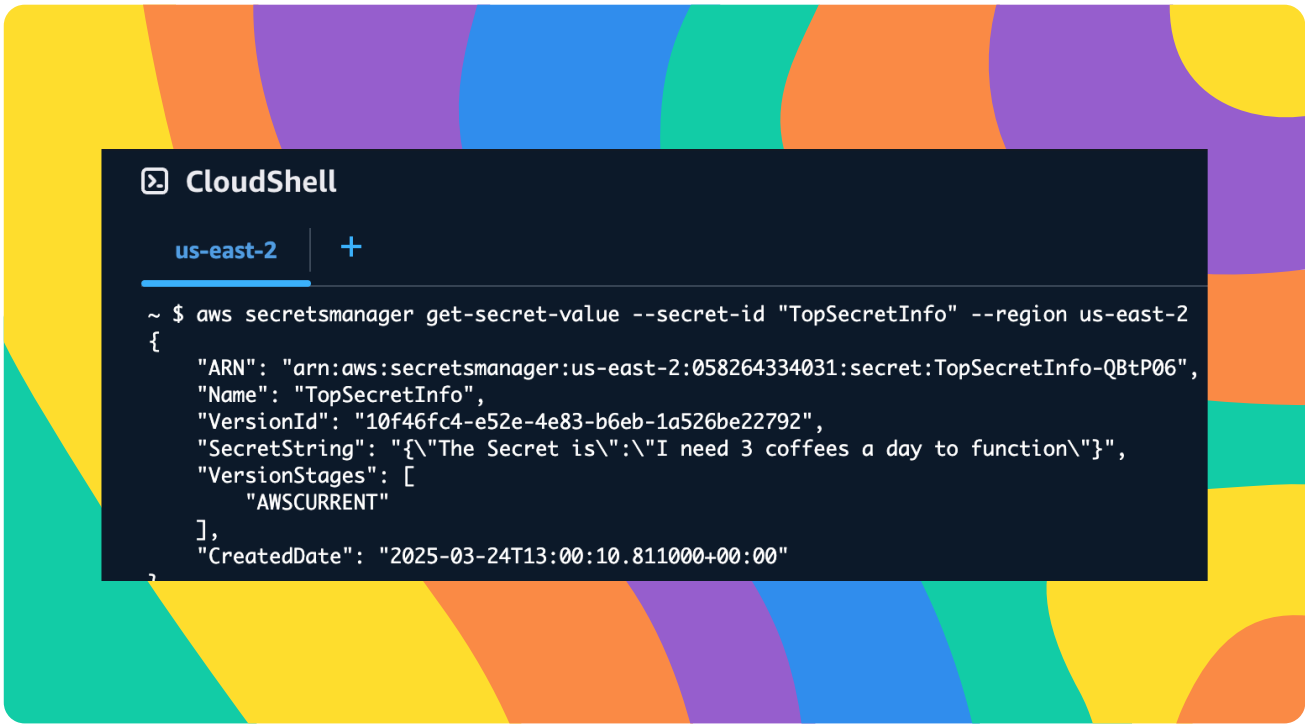
Read Api activity involves accessing, reading, opening a resource. Write API activity involves creating, deleting, updating a resource. For this project, i ticked both to learn both types of activites, but I really only need the write activites (accessing a secret is considered a write activity becuase of its importance)

TA
tahirgroot@gmail.com
NextWork Student

Verifying CloudTrail

I retrieved the secret in two ways: First through the secrets Manager console, where i could easily select a 'Retrieve secrets value' button. Second way is using the AWS CLI i.e running a get-secret-value in cloudshell.

To analyze my CloudTrail events, i.e see the event where we get our secret's value, I visited the event history in cloud trail . I found that there was a GetSecretValue event tracked regardless of whether we did it over the CLI or over the console. This tells us that CloudTrail can definitely see and track when i open our secrets Manager key.



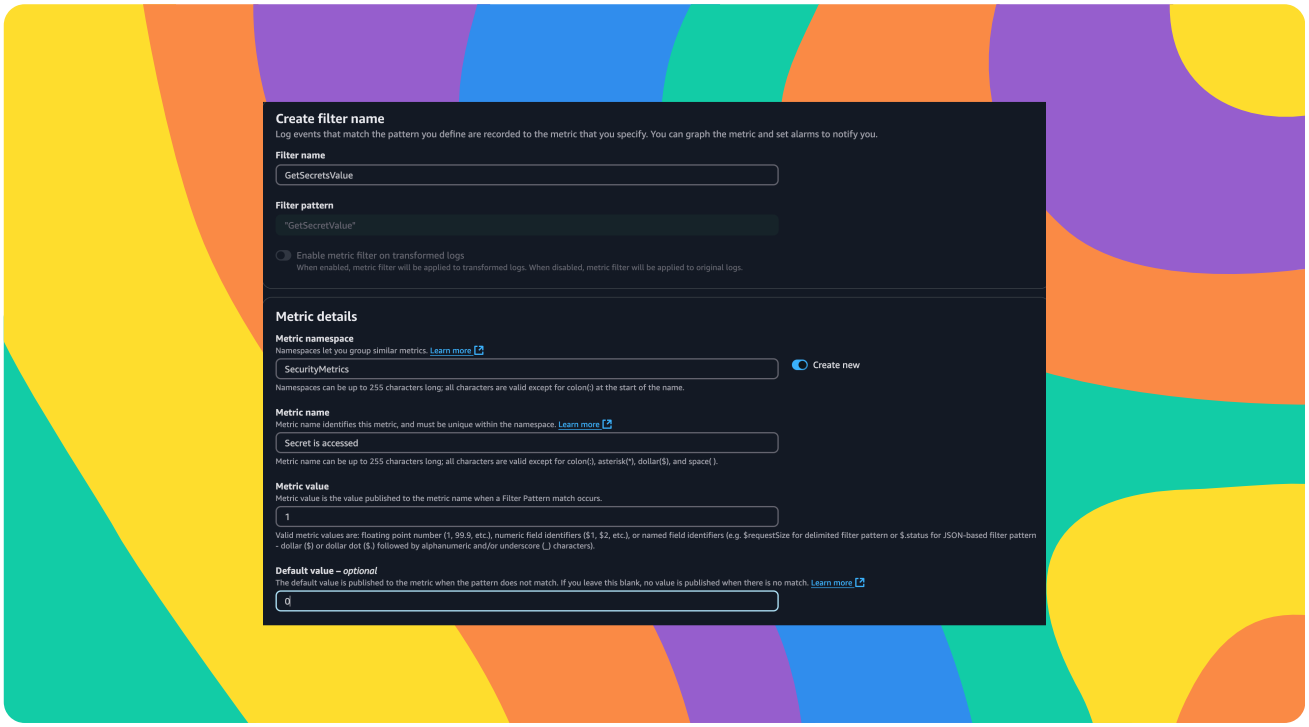
TA
tahirgroot@gmail.com
NextWork Student

CloudWatch Metrics

CloudWatch Logs is a monitioring service that brings together logs from other AWS services (including Cloudtrail) to help me analyze and create alarms for . Its important for monitoring because i get to create insights and get alerted based on events that happen in my account.

CloudTrail's Event History is useful for quickly reading (management) events that happened in the last 90 days. while CloudWatch Logs are better for combining and analyzing logs from different sources, accesssing logs for longer than 90 days, and advanced filtering.

A CloudWatch metric is a specific way that i can count or track events that are in a log group. When setting up a metric, the metric value represents how we increment or 'count' an event when it passes our filters (in our case, i want to increment metric value by 1 whenever my secret is accessed) Default value is used when the event that i am tracking does not occur.


Create filter name
Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.
Filter name
GetSecretsValue
Filter pattern
"GetSecretValue"
Enable metric filter on transformed logs
When enabled, metric filter will be applied to transformed logs. When disabled, metric filter will be applied to original logs.
Metric details
Metric namespace
Namespaces let you group similar metrics. Learn more
SecurityMetrics
Create new
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.
Metric name
Metric name identifies this metric, and must be unique within the namespace. Learn more
Secret is accessed
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).
Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.
1
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers ($1, $2, etc.), or named field identifiers (e.g. $requestSize for delimited filter pattern or $.status for JSON-based filter pattern - dollar ($) or dollar dot ($.) followed by alphanumeric and/or underscore (_) characters).
Default value – optional
The default value is published to the metric when the pattern does not match. If you leave this blank, no value is published when there is no match. Learn more
0

TA
tahirgroot@gmail.com
NextWork Student

CloudWatch Alarm

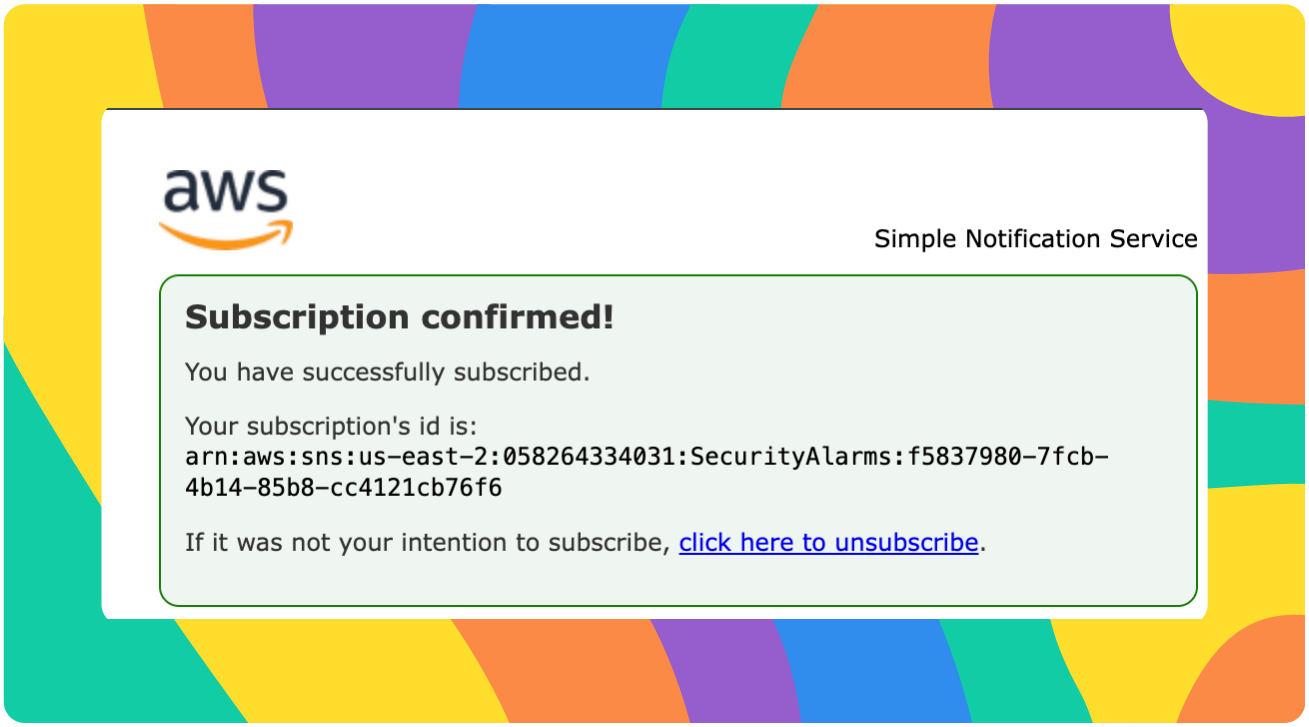
A CloudWatch alarm is a feature and alert system in Cloud Watch that's designed to go off i.e. indicate when certain conditions have been met in our log group. I set my CloudWatch alarm threshold to be about how many times the GetSecretValue event happens in a 5 minute period so the alarm will trigger when the average number of times is above 1.

I created an SNS topic along the way. An SNS topic is like newsletter/broadcast channel channel that emails, phone numbers, functions. Apps can subscribe to(so they get notified when SNS has a new update to share My SNS topic is set up to send us an email when our secrets gets accessed

AWS requires email confirmation because it would not automatically start emailling addresses that we subscribe to an SNS topic. This helps prevent any unwanted subscriptions for recipicients (i.e people who are receiving those email(S))

TA

tahirgroot@gmail.com
NextWork Student



Troubleshooting Notification Errors

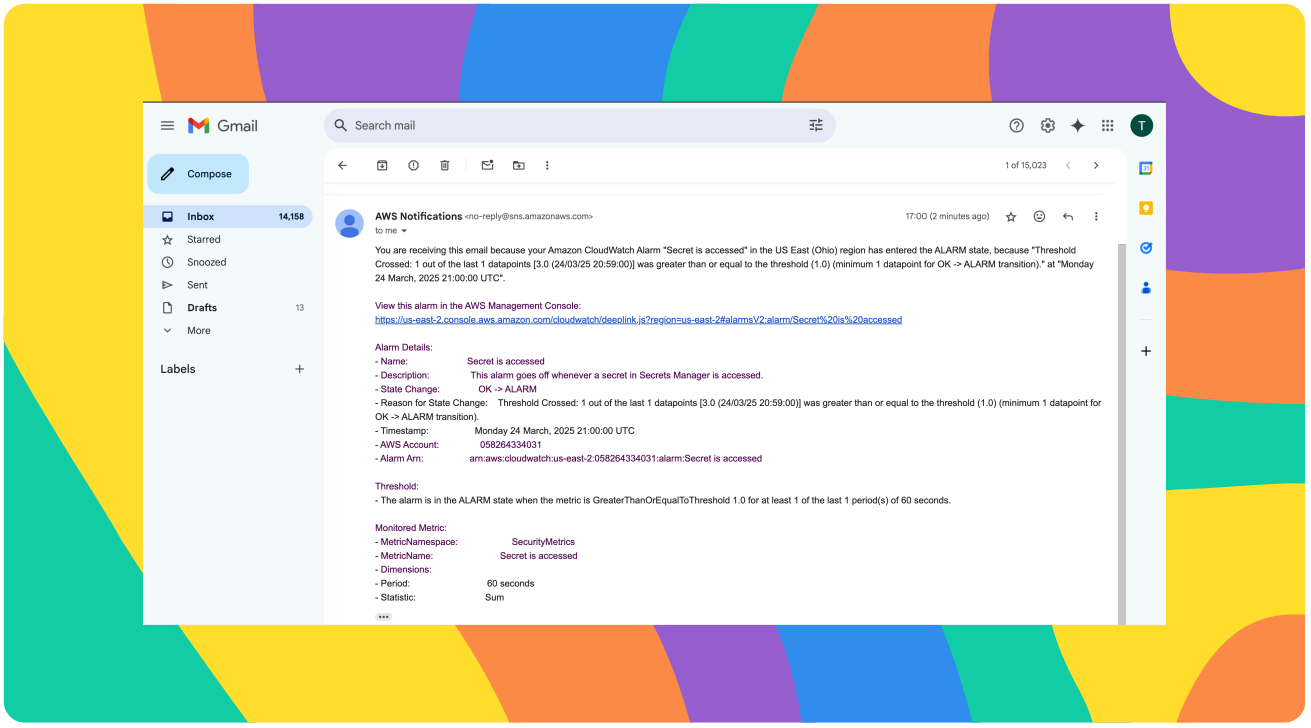
To test my monitoring system, I exposed and accessed my secret again? The results weren't succesful - I didnt get any emails/notifications about my secrets getting accessed.

When troubleshooting the modification issues, I investigated every single part of my monitoring system - wether CloudTrail is picking up on events that are happening when i access my secret, whether CloudTrail is sending logs to cloudwatch, whether the filter is accidently rejecting the correct events, whether the alarm gets triggered, whether the triggering of the alarm sends and email.

I initially didn't receive an email before because Cloud watch was configured to use the wrong threshold - instead of caculating the average number of times a secret was accessed in a time period, it should have been the SUM !

Success!

To validate that our monitoring system can successfully detect and alert when my secret is accessed, I checked my secret's value one more time. I received an email within 1-2 minutes of the event! Our Alarm in cloud watch is also in alarm state.

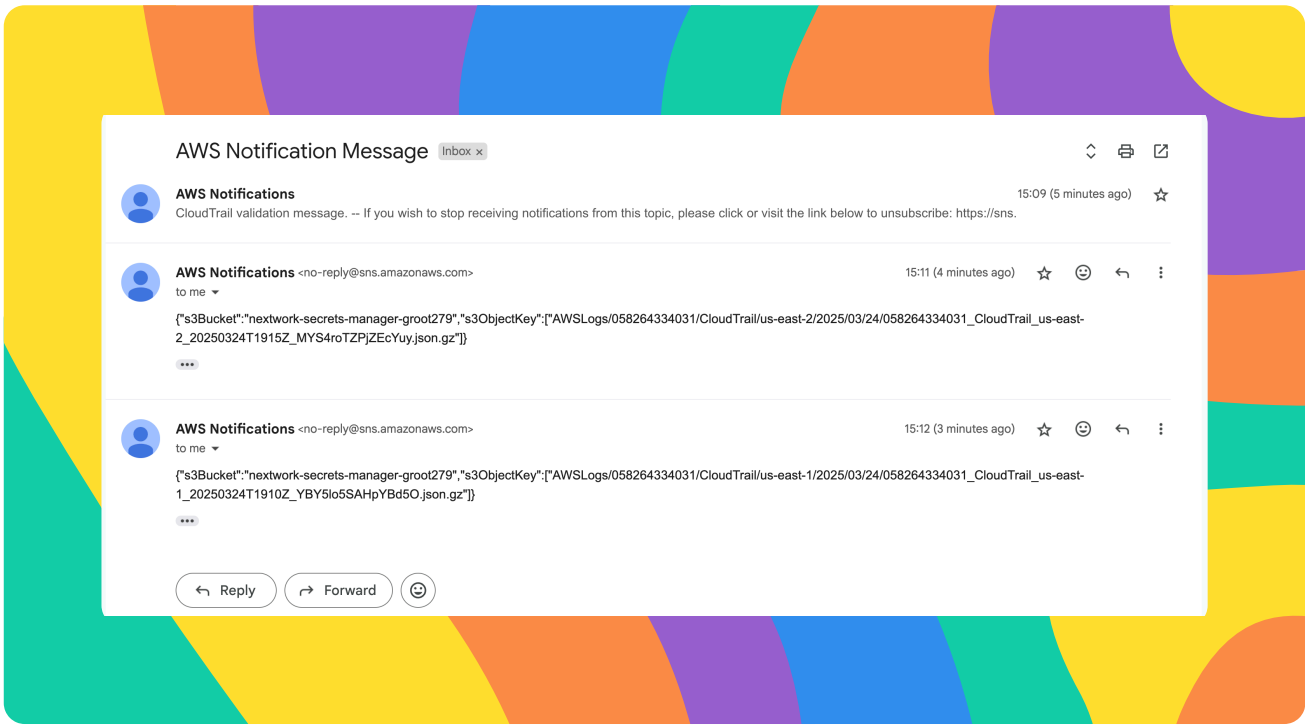


TA
tahirgroot@gmail.com
NextWork Student

Comparing CloudWatch with CloudTrail Notifications

In a project extension, i enabled SNS notification Delivery in CloudTrail because this lets us evaluate CloudTrail vs Cloudwatch for notifying us about events like ou secrets getting access

After enabling CloudTrail SNS notifications, my inbox was very quickly filled with new emails from SNS (as it was notified by cloudtrail) In terms of the usefulness of these emails, I thought that we re receiving lots(its a litlle overwhelming) and the logs themseleves) and the logs themselves dont show what happened in terms of management events that occured. We only see that new logs have been stored in our buckets.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects