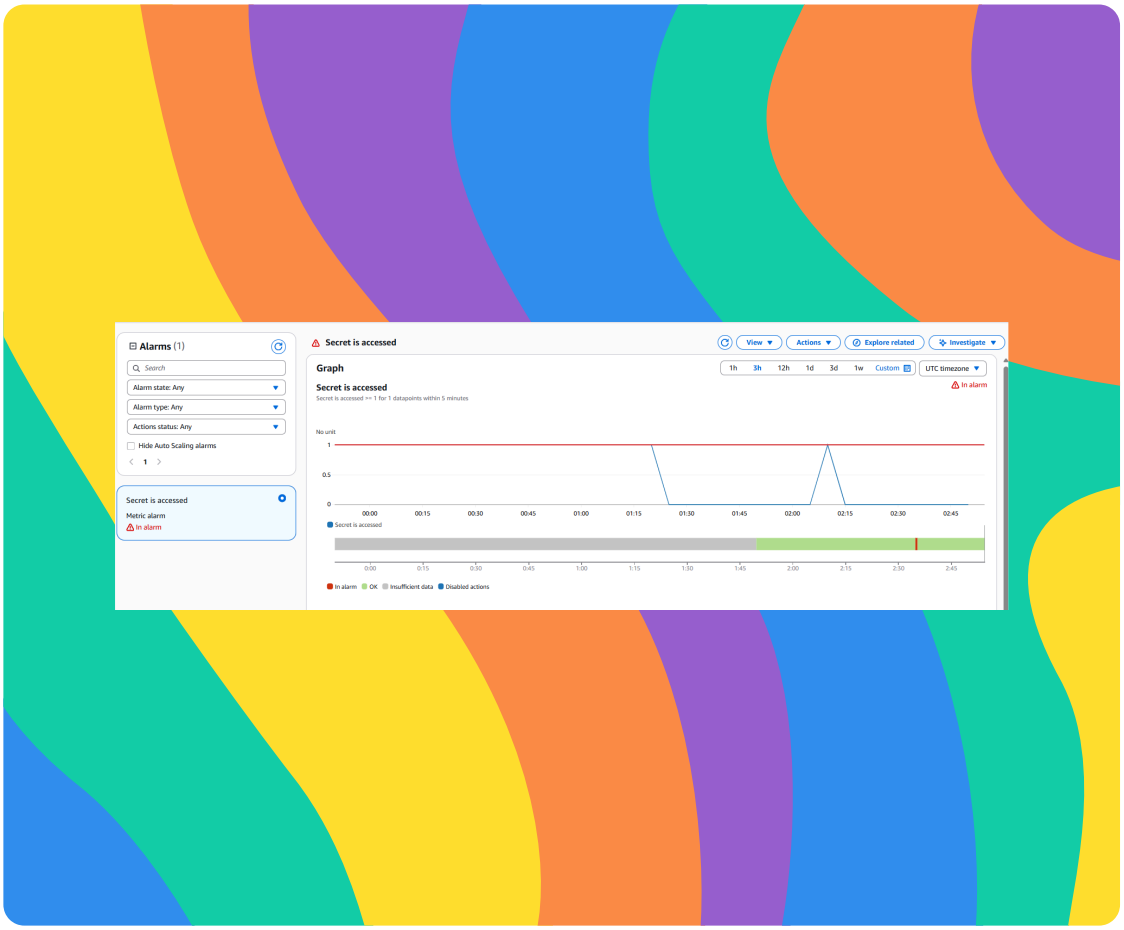
nextwork.org

Build a Security Monitoring System

WA awswani



Introducing Today's Project!

I'm doing this project to learn, how to setup a security detection system using multiple aws services. From CloudTrail, Cloudwatch, SNS, for we can actively receive notifications when users from our org is accessing sensitive information.

Tools and concepts

The services I used included CloudTrail, SNS, and CloudWatch, along with Secrets Manager, IAM roles, and S3 buckets. Key concepts I learned through this project were the differences and complementary roles of CloudWatch and CloudTrail, particularly how the trails and logs worked together. Ultimately, these played a role in enabling the SNS notification to trigger when the secrets were accessed.

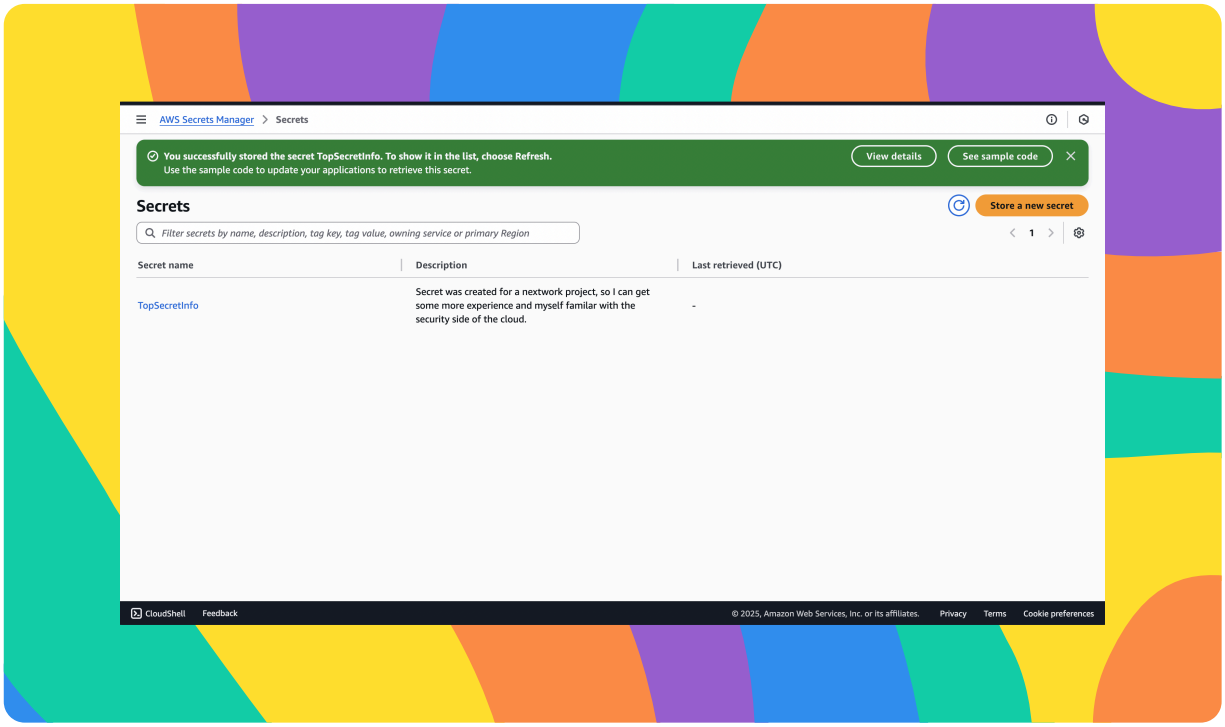
Project reflection

This project took me approximately 2 hours or so, but it was an overall great experience for me. The most challenging part was not getting distracted by the abundance of features available throughout the project. It was a rewarding experience to do this project, and it is amazing to add to my portfolio.

Create a Secret

It's aws security service for storing secrets and any sensitive information.

The secret, I created was about I love cloud and I can't wait to make it and hot dogs are good.



Set Up CloudTrail

CloudTrail is a monitoring service, that we used to record activity within our aws account. So we are able to investigate later and look into the logs.

CloudTrail events include types like management events,data event, insights, and network activity events. But, we chose management events due to it being the default cost effectivie, and do it being for free compared to us choosing data event.

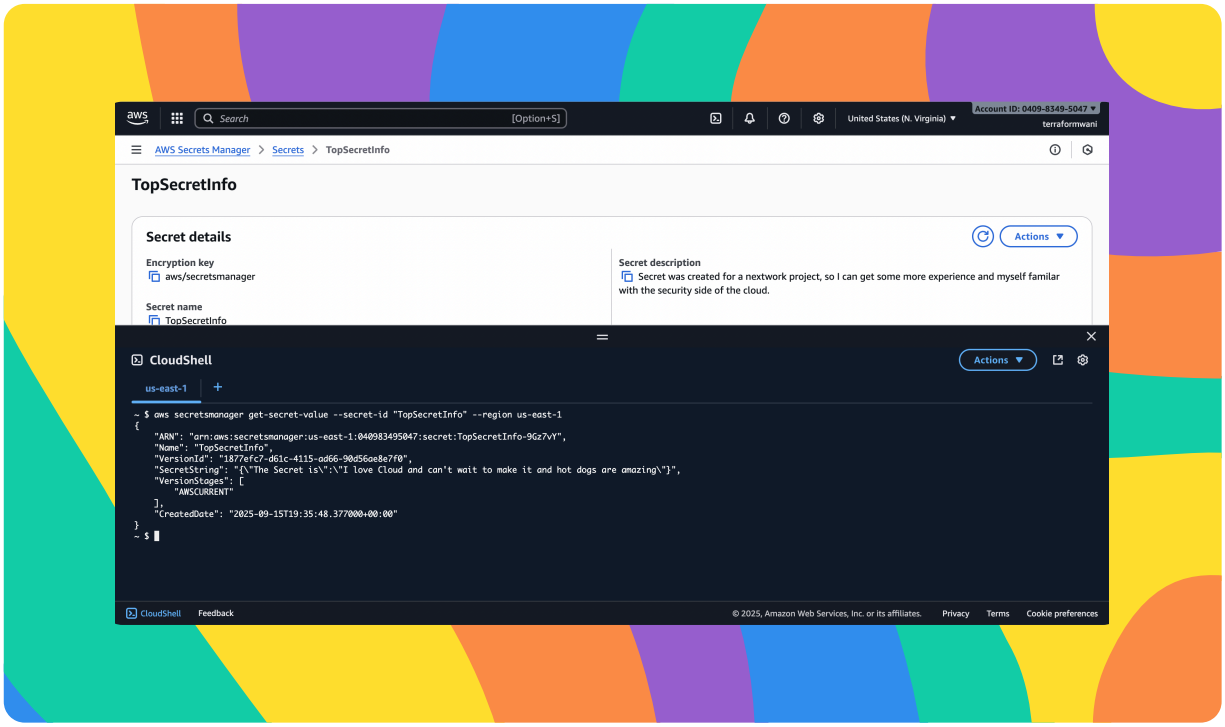
Read vs Write Activity

Read api gives us the ability to look at the reading and opening the resouce. While write invovles creating, deleting, and updating a resource.

Verifying CloudTrail

retrieve key via secrets manager, and aws cli

It showed everything prior to us making the value but yes it recorded everything and that was pretty cool and even showed when the secret value was retrieved.

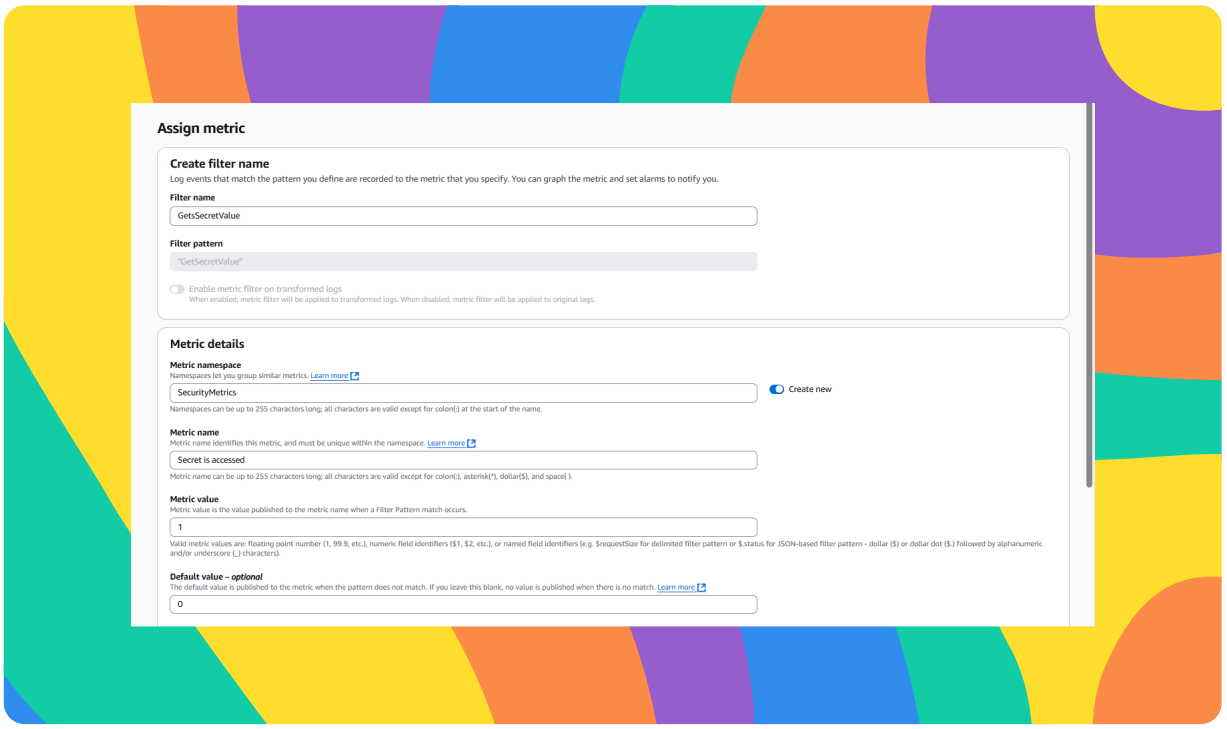


CloudWatch Metrics

CloudWatch Logs is important for monitoring because it gives a more in depht on insights, and alerted on events that happen in our account.

CloudTrail's Event History is useful for 90 day of tracking events. While, Cloudwatch gives more insights and alerts on events taking place.

A CloudWatch metric is a specific way we can 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 by 1 when a secret is accessed. The default value is used when the event we are tracking does not occur.

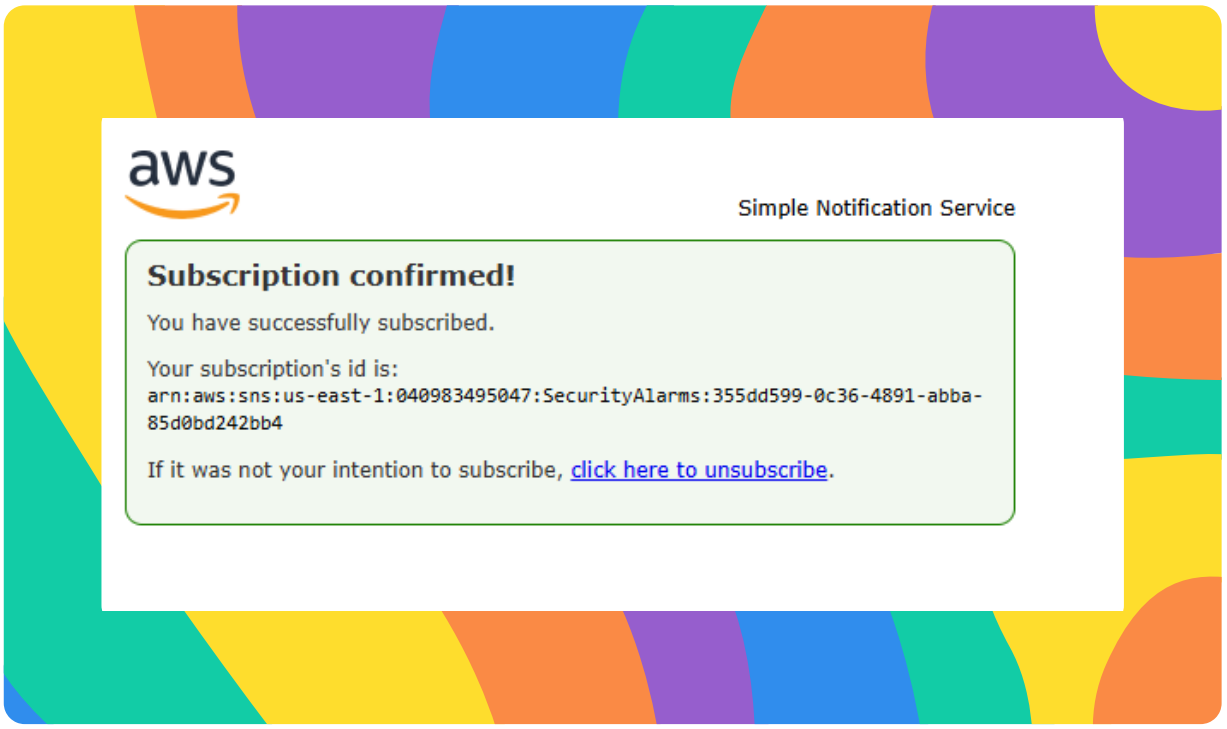

Assign metric
Create filter name
Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.
Filter name
GetsSecretValue
Filter pattern
"GetSecretValue"
Enable metric filter on transformed logs
When enabled, metric filter 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

CloudWatch Alarm

A CloudWatch alarm is a feature and an alert system in CloudWatch that is designed to "go off" and indicate when certain conditions have been met. In the events 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 a newsletter that emails, phone numbers, functions, and apps can subscribe to get notified when SNS has a new update to share. My SNS topic is set up to send an email when the secrets get accessed.

AWS requires email confirmation because it will not automatically start sending emails to addresses that we have subscribed to. This helps prevent unwanted subscriptions for users who are receiving these emails.


aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:us-east-1:040983495047:SecurityAlarms:355dd599-0c36-4891-abba-85d0bd242bb4
If it was not your intention to subscribe, click here to unsubscribe.

Troubleshooting Notification Errors

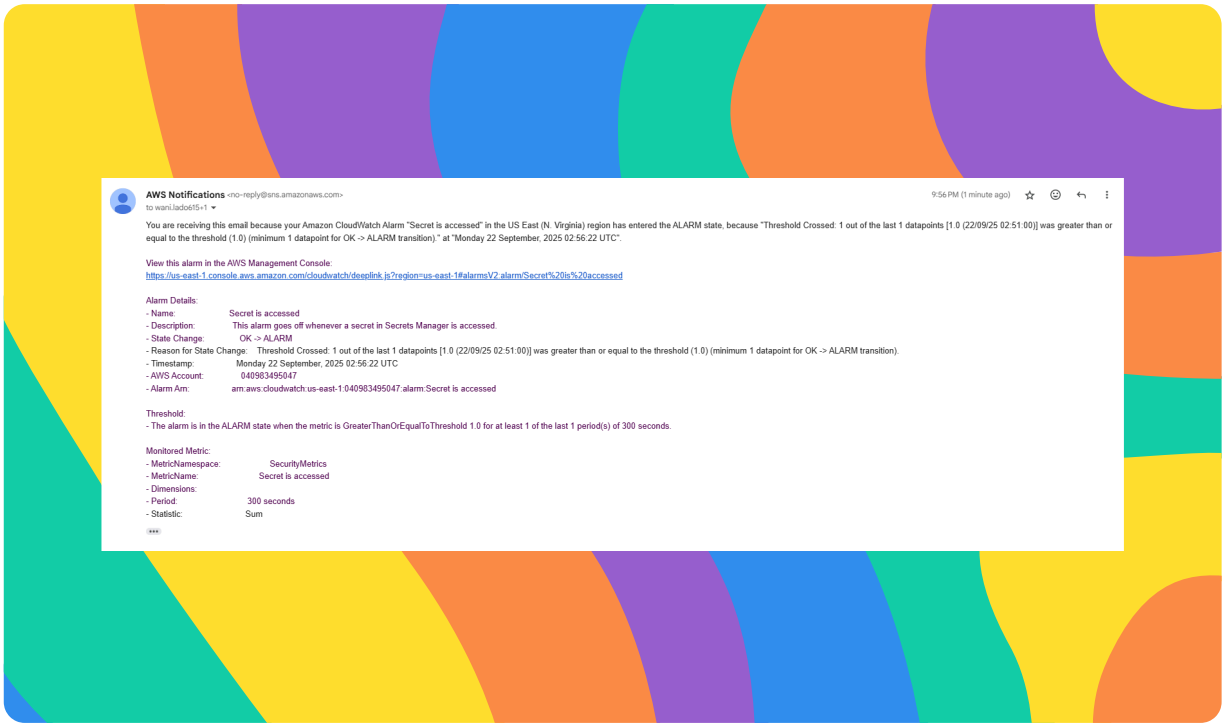
To test my monitoring system, I opened and accessed the secret again. The results were, I didn't receive any notifications in my email.

When troubleshooting the notification issues, I investigated every part of the monitoring system, from whether CloudTrail is picking up on events from when accessing events or sending logs to CloudWatch. Also, verified if the filter accidentally rejects the correct events, whether the alarm gets triggered, and sends an email.

I initially didn't receive an email before because CloudWatch was configured to use the wrong threshold. Instead of calculating the "average" number of times a secret was accessed in the time period. The key solution was actually the "SUM"

Success!

To validate that the 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 1-2 minutes after the event occurred, and my CloudWatch was also in an alarm state.



The place to learn & showcase your skills

Check out nextwork.org for more projects