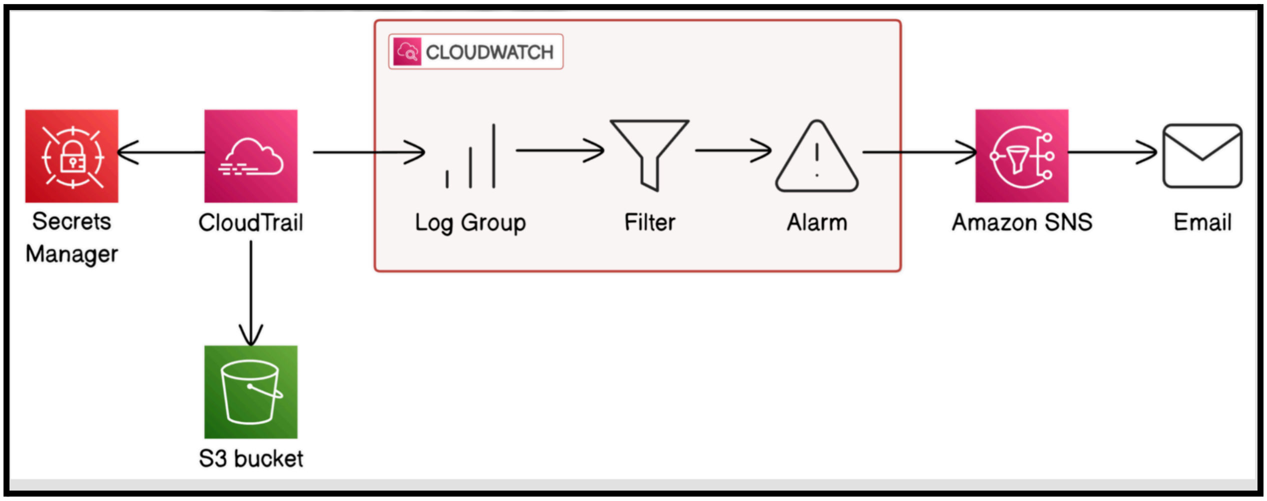
🛡️ Build a Security Monitoring System on AWS

By Evans Yeboah



🚀 Project Overview

In this project, I demonstrate how to set up a security monitoring system on AWS. My goal was to learn how to:

- Create secrets using AWS Secrets Manager
- Enable AWS CloudTrail to record logs
- Configure CloudWatch Alarms and SNS to monitor activity across the system

🧰 Tools & Concepts

Services used:

- AWS Secrets Manager
- AWS CloudTrail
- Amazon CloudWatch
- Amazon SNS

Key concepts learned:

- Secret encryption and retrieval
- CloudTrail event analysis
- CloudWatch metric filters and alarms
- SNS topic creation and notification setup

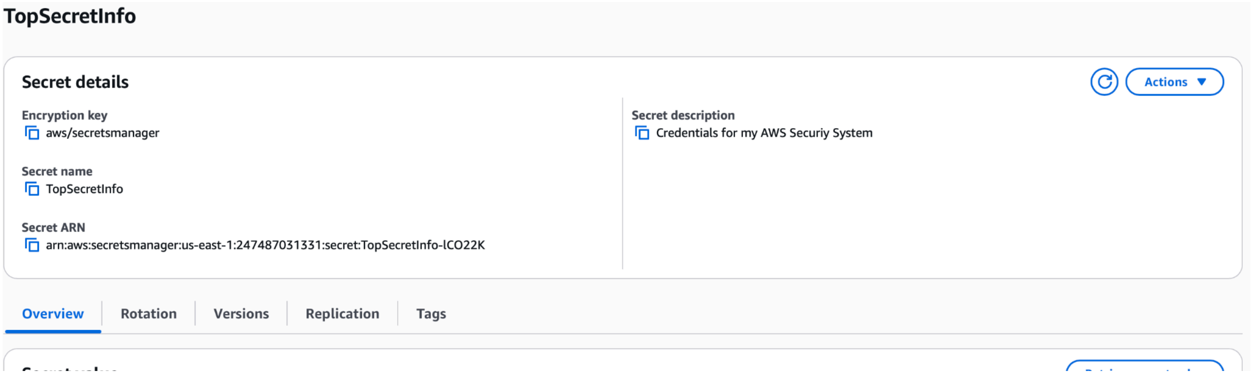
🧠 Project Reflection

This project took approximately two hours. The most challenging part was configuring the SNS notification. It was also the most rewarding—security is a top priority for me, and this project helped reinforce that.

🔐 Create a Secret

AWS Secrets Manager helps protect sensitive information like passwords, API keys, and credentials. Instead of storing credentials in code or sharing them via email, Secrets Manager keeps them secure.

For this project, I created a secret called **TopSecretInfo** containing credentials for my AWS security system.



TopSecretInfo

Secret details

Encryption key
aws/secretsmanager

Secret name
TopSecretInfo

Secret ARN
arn:aws:secretsmanager:us-east-1:247487031331:secret:TopSecretInfo-lCO22K

Secret description
Credentials for my AWS Securiy System

📜 Set Up CloudTrail

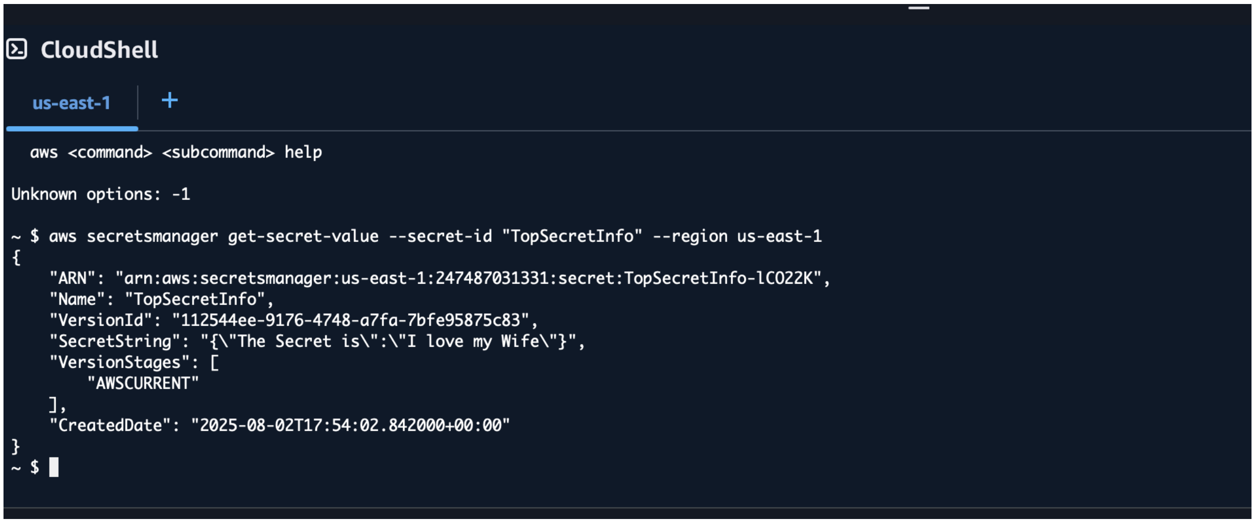
AWS CloudTrail records activity across an AWS account. It documents who did what, when, and from where.

CloudTrail event types include:

- **Management events:** Admin actions like creating EC2 instances or accessing secrets
- **Data events:** High-volume actions like uploading to S3 or invoking Lambda
- **Insights events:** Detect unusual patterns, such as mass IAM user creation
- **Network activity events:** Track changes to VPCs or subnet traffic

Read vs. Write API activity:

- *Read:* Listing S3 buckets, describing EC2 instances, viewing secret metadata
- *Write:* Creating, deleting, modifying resources, or retrieving secret values



```
  aws <command> <subcommand> help

Unknown options: -1

~ $ aws secretsmanager get-secret-value --secret-id "TopSecretInfo" --region us-east-1
{
    "ARN": "arn:aws:secretsmanager:us-east-1:247487031331:secret:TopSecretInfo-lCO22K",
    "Name": "TopSecretInfo",
    "VersionId": "112544ee-9176-4748-a7fa-7bfe95875c83",
    "SecretString": "{\"The Secret is\":\"I love my Wife\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2025-08-02T17:54:02.842000+00:00"
}
~ $
```

✅ Verifying CloudTrail

I retrieved the secret in two ways:

1. Through the AWS Console
2. Using CloudShell with the command:

aws secretsmanager get-secret-value --secret-id "TopSecretInfo" --region us-east-1

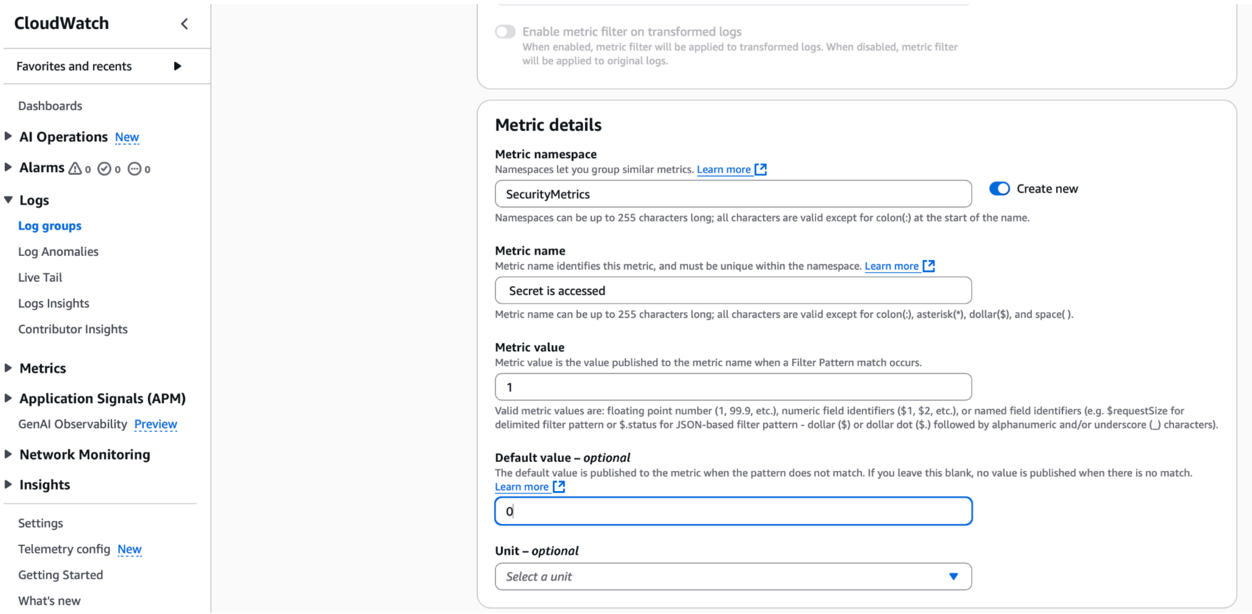
I analyzed CloudTrail logs to confirm:

- **Event source:** `secretsmanager.amazonaws.com`
- **Event name:** `GetSecretValue`
- **User name:** IAM identity that accessed the secret
- **Resource type:** Secrets Manager

📊 CloudWatch Metrics

Amazon CloudWatch Logs aggregates logs from AWS services for visibility and analysis. Once logs are in CloudWatch, you can:

- Create alerts based on patterns (e.g., secret access)
- Visualize trends
- Trigger automated responses



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

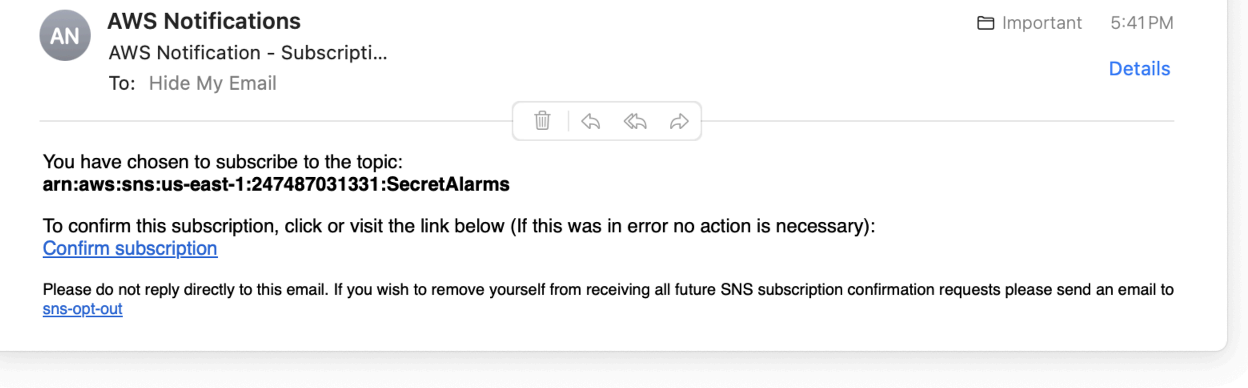
Unit – *optional*
Select a unit

I created a metric filter that increments by 1 each time the secret is accessed. The default value is set to 0 to show periods with no access.

⏰ CloudWatch Alarm & SNS

CloudWatch Alarms monitor metrics and trigger actions when thresholds are crossed. I set up an alarm to monitor secret access and created an SNS topic called **SecurityAlarms** to send email notifications.

AWS requires email confirmation for SNS subscriptions to prevent accidental opt-ins.



You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:247487031331:SecretAlarms

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

---

🛠️ Troubleshooting Notification Errors

To test the system, I:

- Verified CloudTrail captured secret access events
- Checked the SNS alarm functionality

Troubleshooting steps:

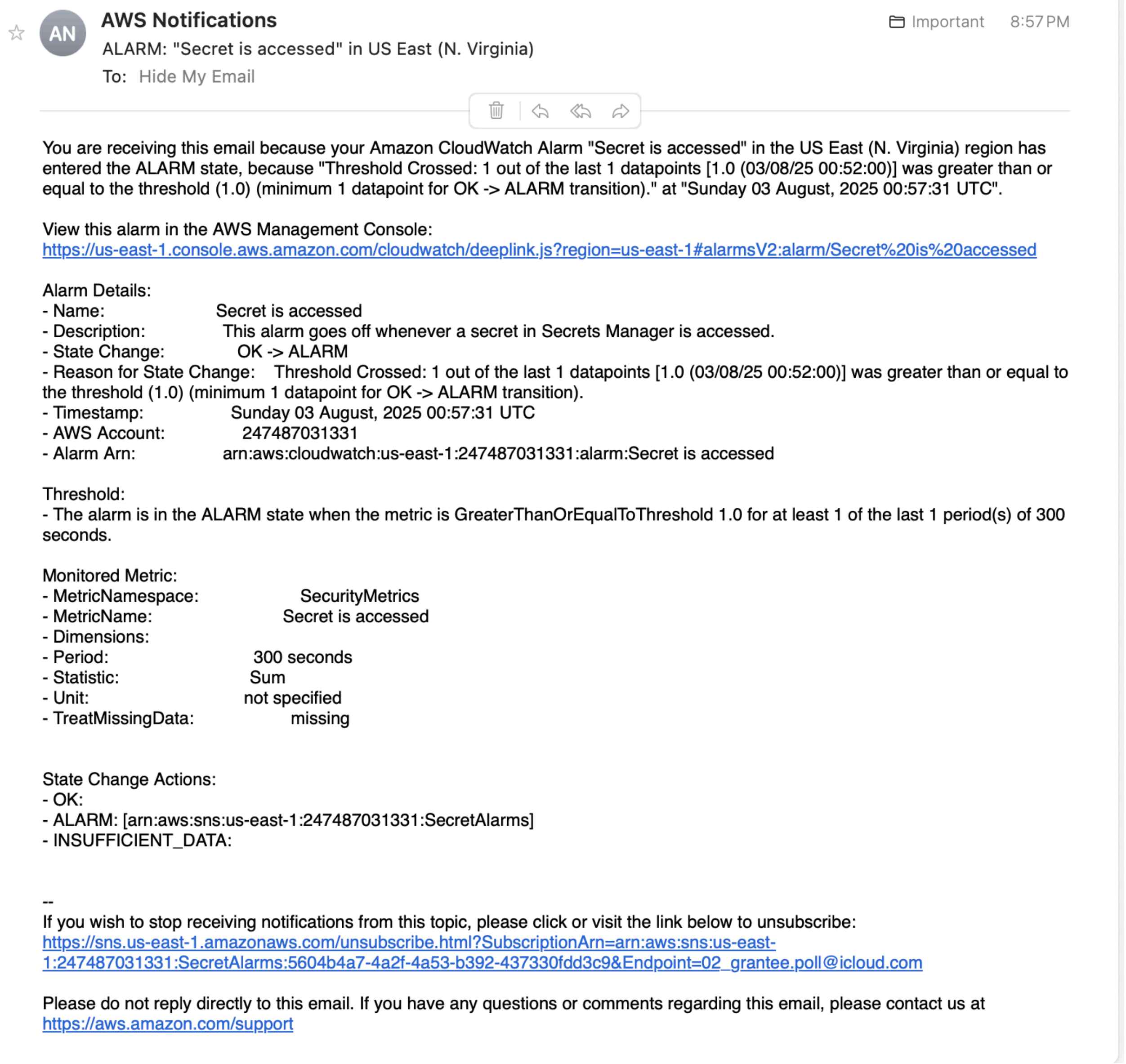
- Reviewed alarm history
- Inspected SNS topic access policy
- Verified SNS encryption settings
- Manually published test messages

The initial issue was due to using the wrong CloudWatch threshold calculation. I corrected it to use **sum** instead of **count**.

✅ Success!

I validated the system by:

- Accessing the secret
- Receiving an SNS email notification
- Confirming the CloudWatch alarm triggered correctly



AWS Notifications
ALARM: "Secret is accessed" in US East (N. Virginia)
To: Hide My Email

You are receiving this email because your Amazon CloudWatch Alarm "Secret is accessed" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (03/08/25 00:52:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Sunday 03 August, 2025 00:57:31 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Secret%20is%20accessed

Alarm Details:
- Name: Secret is accessed
- Description: This alarm goes off whenever a secret in Secrets Manager is accessed.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (03/08/25 00:52:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Sunday 03 August, 2025 00:57:31 UTC
- AWS Account: 247487031331
- Alarm Arn: arn:aws:cloudwatch:us-east-1:247487031331:alarm:Secret is accessed

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace: SecurityMetrics
- MetricName: Secret is accessed
- Dimensions:
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

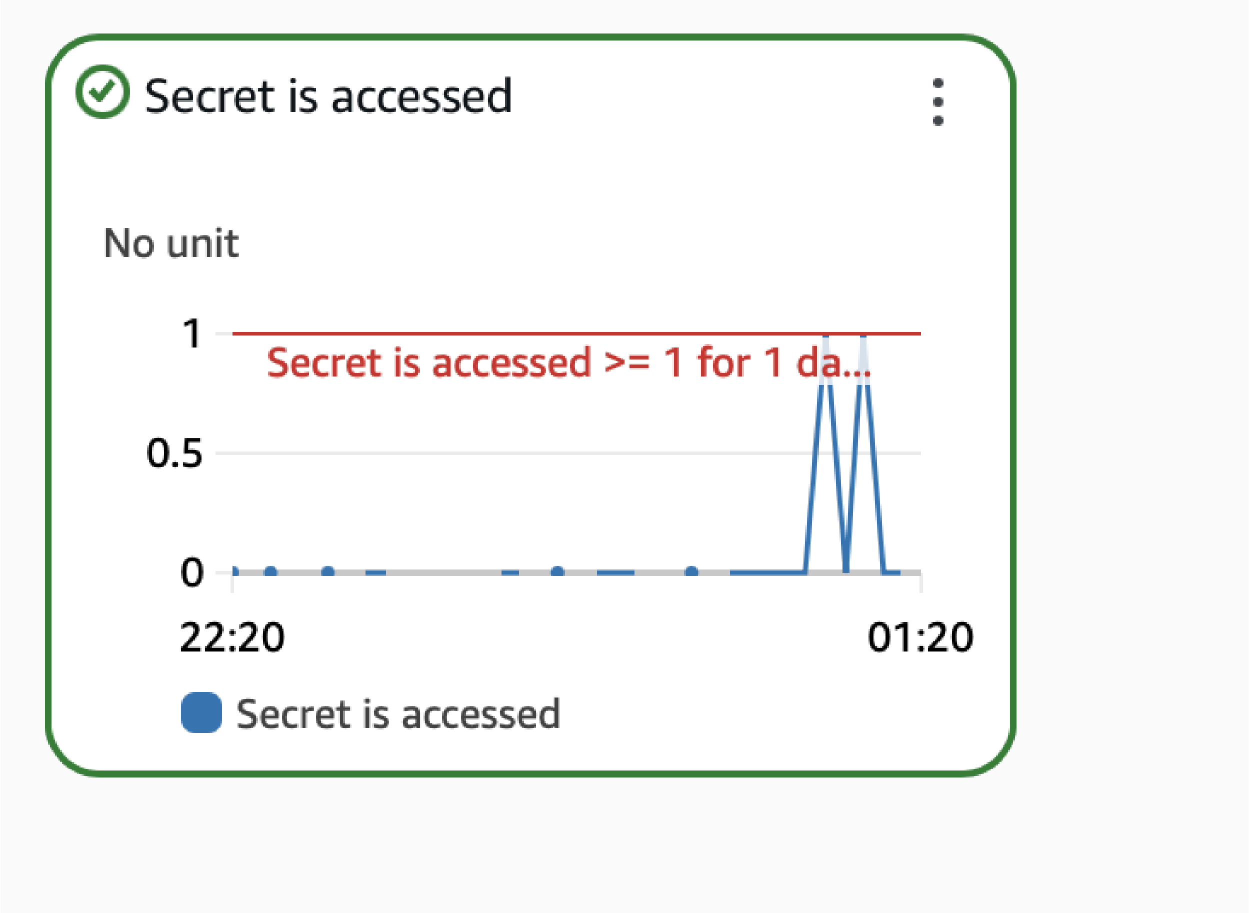
State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:247487031331:SecretAlarms]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:247487031331:SecretAlarms:5604b4a7-4a2f-4a53-b392-437330fdd3c9&Endpoint=02_grantee.poll@icloud.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

🔁 Comparing CloudTrail & CloudWatch Notifications

As a project extension, I enabled CloudTrail SNS notifications to receive real-time alerts for specific logging activities. My inbox was flooded with emails, which showed how active and responsive the system was.


Secret is accessed
No unit
Secret is accessed >= 1 for 1 da...
22:20
01:20
🟦 Secret is accessed