README Template (AWS Security Monitoring Project)

Project Overview

This project demonstrates an **AWS-based Security Monitoring and Alerting System**. The system collects CloudTrail logs, analyzes them with Athena SQL, generates real-time alerts with EventBridge and SNS, and visualizes suspicious activities through a custom dashboard.

The solution is built entirely on **AWS native services**, without external SIEM tools.

Architecture

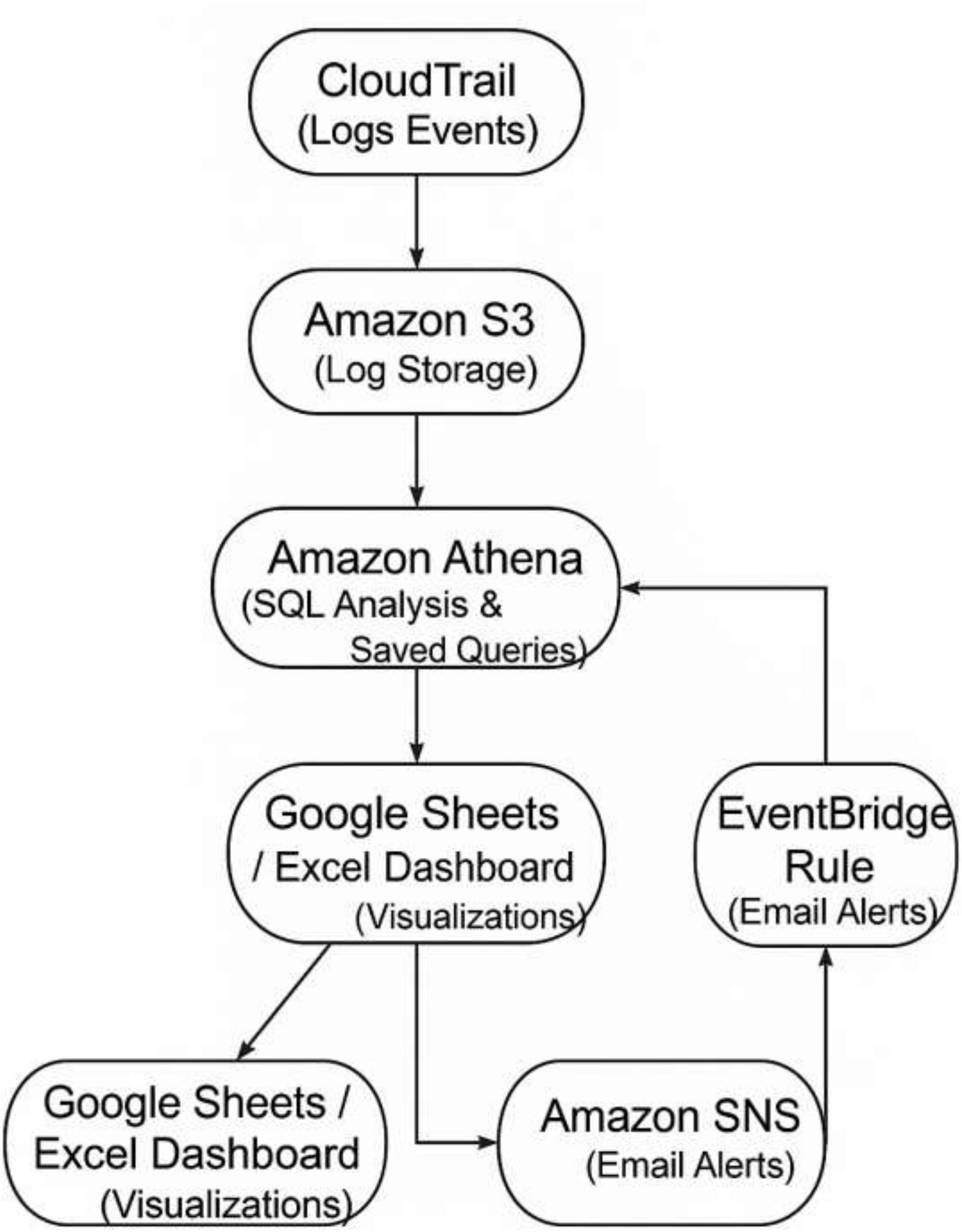
Features

- **Log Collection**
    - AWS CloudTrail logs stored in Amazon S3.
- **Analysis**
    - SQL queries on CloudTrail logs via Athena.
    - Partitioned by region/year/month/day for cost-efficient queries.
- **Detections Implemented**

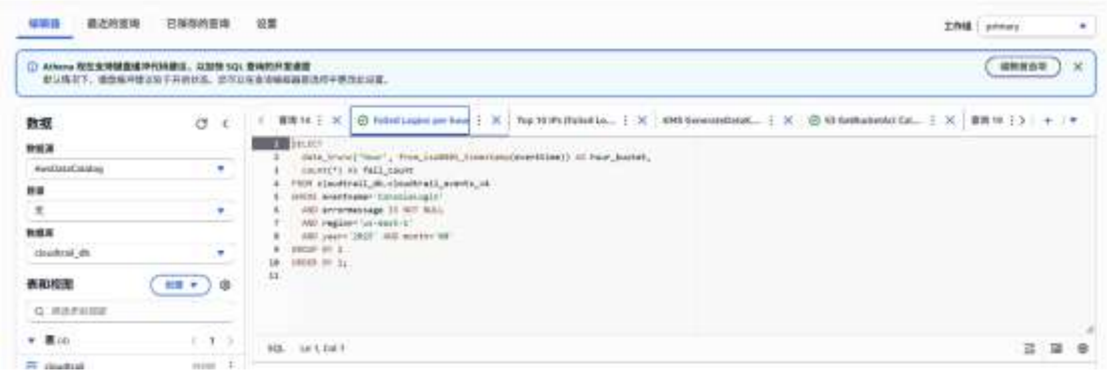
1. Failed Console Login attempts
2. Top source IPs for failed logins
3. Abnormal KMS GenerateDataKey usage
4. Excessive S3 GetBucketAcl calls

- **Alerting**
    - EventBridge rule in **us-east-1** detects login events.
    - SNS topic delivers real-time email alerts.
- **Visualization**
    - Dashboard built in Google Sheets with 4 charts:
        - Failed logins per hour
        - Top 10 source IPs
        - KMS key usage per minute
        - S3 ACL reconnaissance per hour

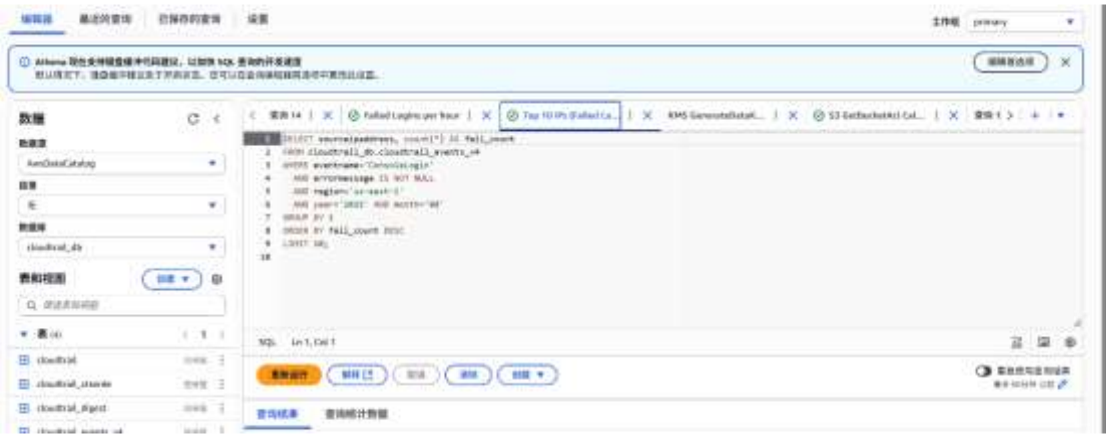
- Architecture



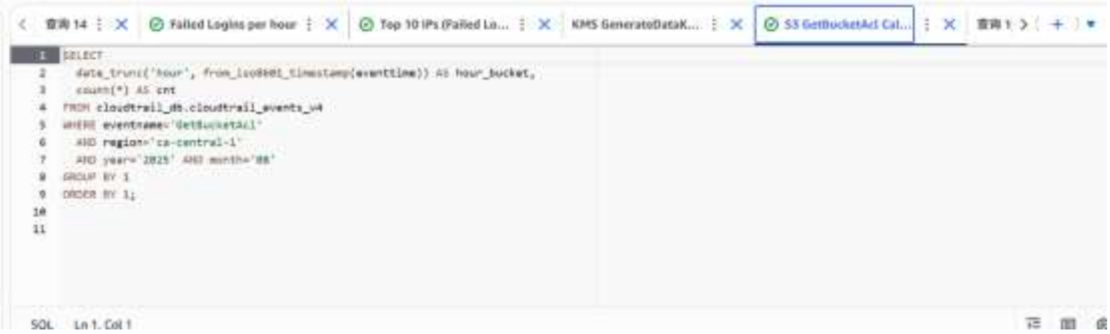
Example Queries (Athena SQL)



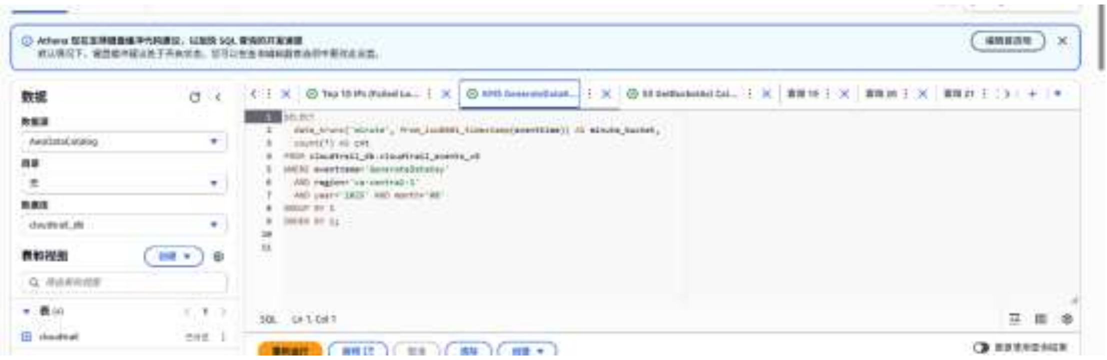
```sql
SELECT
  date_trunc('hour', from_iso8601_timestamp(eventtime)) AS hour_bucket,
  COUNT(*) AS fail_count
FROM cloudtrail_db.cloudtrail_events_v4
WHERE eventname='ConsoleLogin'
  AND errormessage IS NOT NULL
  AND region='us-east-1'
  AND year='2025' AND month='08'
GROUP BY 1
ORDER BY 1;
```



```sql
SELECT sourceipaddress, count(*) AS fail_count
FROM cloudtrail_db.cloudtrail_events_v4
WHERE eventname='ConsoleLogin'
  AND errormessage IS NOT NULL
  AND region='us-east-1'
  AND year='2025' AND month='08'
GROUP BY 1
ORDER BY fail_count DESC
LIMIT 10;
```



```sql
SELECT
  date_trunc('hour', from_iso8601_timestamp(eventtime)) AS hour_bucket,
  count(*) AS cnt
FROM cloudtrail_db.cloudtrail_events_v4
WHERE eventname='GetBucketAcl'
  AND region='ca-central-1'
  AND year='2025' AND month='08'
GROUP BY 1
ORDER BY 1;
```



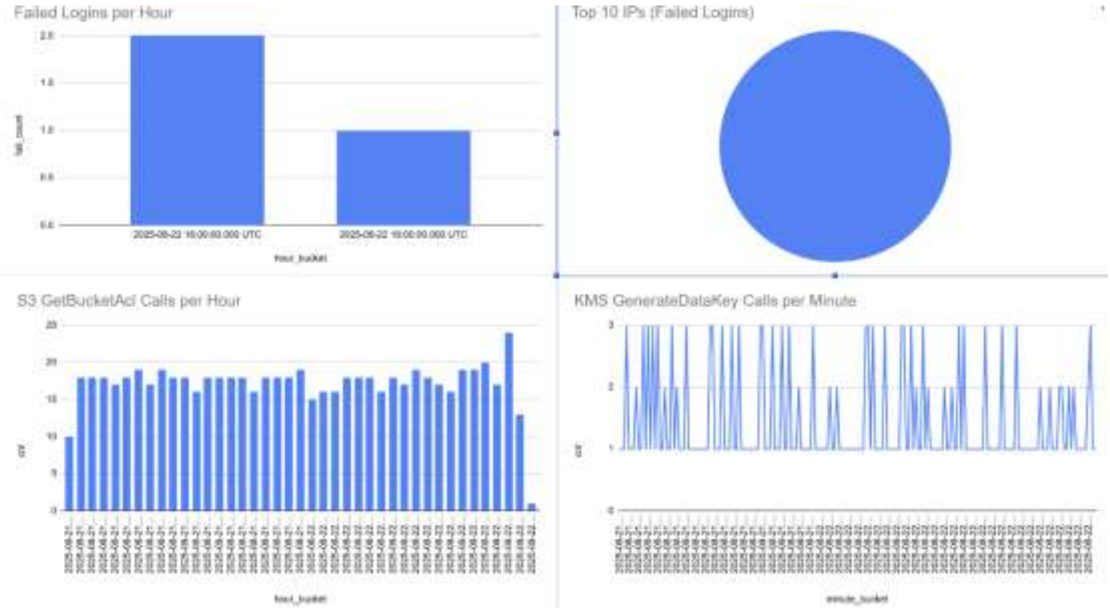
```sql
SELECT
  date_trunc('minute', from_iso8601_timestamp(eventtime)) AS minute_bucket,
  count(*) AS cnt
FROM cloudtrail_db.cloudtrail_events_v4
WHERE eventname='GenerateDataKey'
  AND region='ca-central-1'
  AND year='2025' AND month='08'
GROUP BY 1
ORDER BY 1;
```

Dashboard

The dashboard consists of four visualizations:

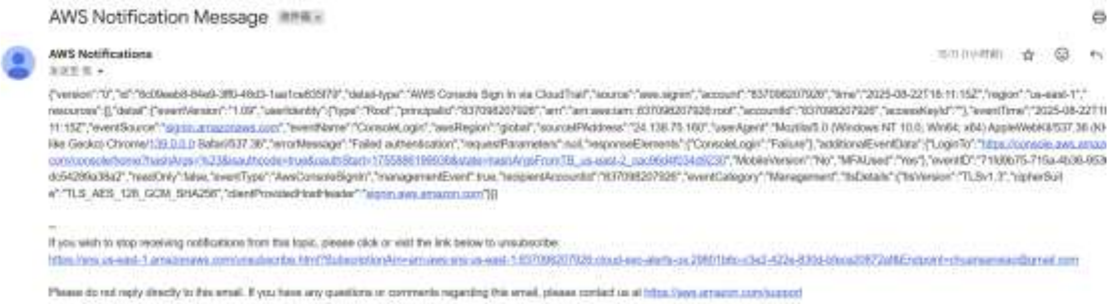
1. **Failed Logins per Hour**

2. **Top 10 Source IPs**
3. **KMS GenerateDataKey Calls per Minute**
4. **S3 GetBucketAcl Calls per Hour**



Alerts

- EventBridge rule forwards login events to SNS.
- Example: Email received for failed ConsoleLogin attempt.



AWS Notification Message

AWS Notifications

{"version":"0","id":"8c06eeb8-84e9-3ff0-48d3-1aa1ca835f79","detail-type":"AWS Console Sign In via CloudTrail","source":"aws.signin","account":"837098207926","time":"2025-08-22T18:11:15Z","region":"us-east-1","resources":[],"detail":{"eventVersion":"1.09","userIdentity":{"type":"Root","principalId":"837098207926","arn":"arn:aws:iam::837098207926:root","accountId":"837098207926","accessKeyId":""},"eventTime":"2025-08-22T18:11:15Z","eventSource":"signin.amazonaws.com","eventName":"ConsoleLogin","awsRegion":"global","sourceIPAddress":"24.138.75.160","userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36","errorMessage":"Failed authentication","requestParameters":null,"responseElements":{"ConsoleLogin":"Failure"},"additionalEventData":{"LoginTo":"https://console.aws.amazon.com/console/home?hashArgs=%23&isauthcode=true&oauthStart=1755886199606&state=hashArgsFromTB_us-east-2_[illegible]","MobileVersion":"No","MFAUsed":"Yes"},"eventID":"71d0b75-715a-4b36-953[illegible]dc54289a38a2","readOnly":false,"eventType":"AwsConsoleSignIn","managementEvent":true,"recipientAccountId":"837098207926","eventCategory":"Management","tlsDetails":{"tlsVersion":"TLSv1.3","cipherSuite":"TLS_AES_128_GCM_SHA256","clientProvidedHostHeader":"signin.aws.amazon.com"}}}

--

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-1:837098207926:cloud-sec-alerts-[illegible]&Endpoint=[illegible]@gmail.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

Deliverables

- queries/ → SQL scripts for Athena.
- dashboard.png → Visualization screenshot.
- alert_email.png → Example SNS alert.
- architecture.png → System architecture diagram.

Resume Highlight

Built an AWS security monitoring PoC using CloudTrail, Athena, EventBridge, and SNS. Delivered real-time alerts for suspicious login activity and a dashboard visualizing login trends, KMS usage, and S3 reconnaissance attempts.