Author: Nelson Woghiren

Summary

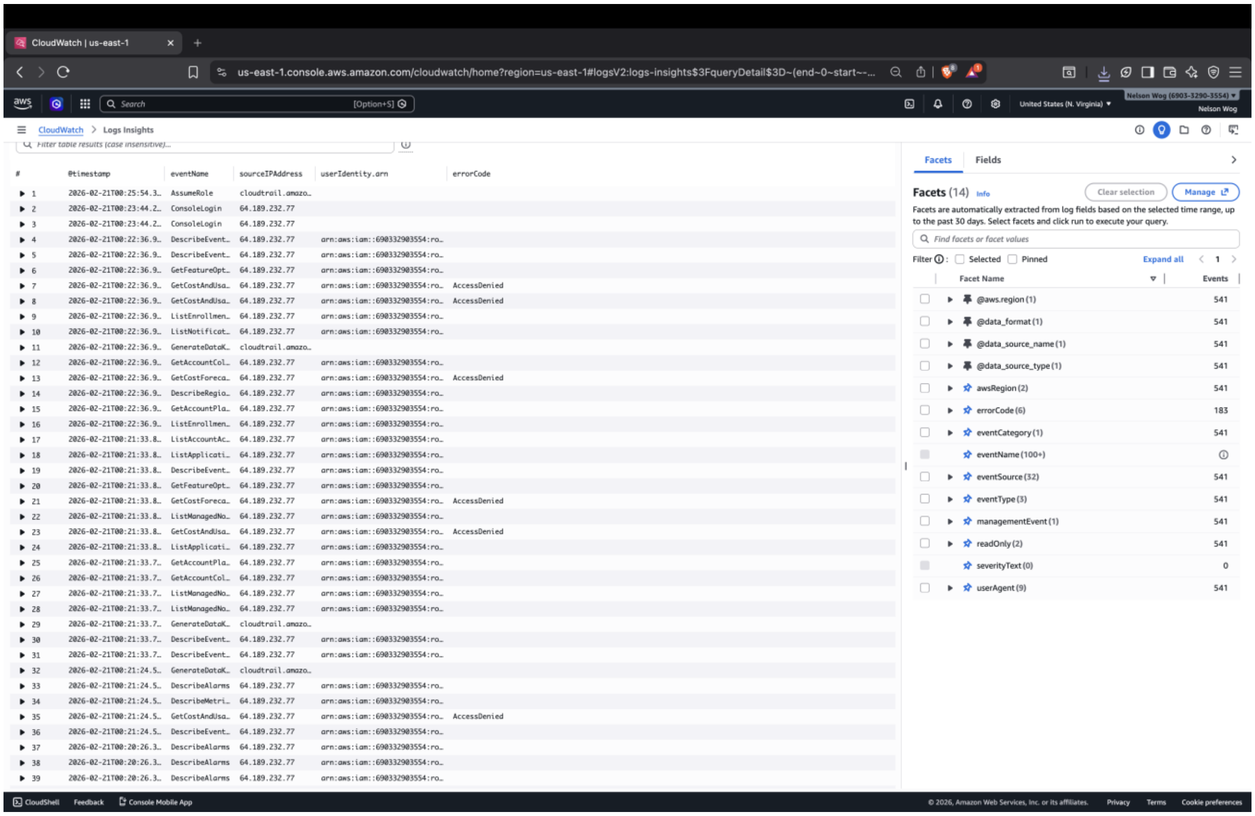
- EC2 Instance: t3.micro (terminated for cost savings)
- S3 Bucket: nelson-blue-team-lab-2026
- CloudTrail: Enabled, encryption with KMS, log file validation on
- CloudWatch Logs: Connected to CloudTrail trail for real time monitoring

  - IAM User
  - Nelson-admin (minimal privileges, no root usage)
  - Test- User (created for simulation, deleted)

- Threat: Unauthorized access attempt to S3 bucket
- Simulation:
  - Logged in as test-user
  - Attempted to list bucket contents – ACCESSDENIED triggered
- Detection:
  - Logged into nelson-admin/root account
  - CloudWatch Logs insights query used:

```
 Fields @timestamp,  eventName,  sourceIPAddress,
userIdentity.arn, errorCode
```

```
|   sort @timestamp desc
|   limit   50
```



CloudWatch > Logs Insights

#	@timestamp	eventName	sourceIPAddress	userIdentity.arn	errorCode
1	2026-02-21T00:25:54.3…	AssumeRole	cloudtrail.amazo…		
2	2026-02-21T00:23:44.2…	ConsoleLogin	64.189.232.77		
3	2026-02-21T00:23:44.2…	ConsoleLogin	64.189.232.77		
4	2026-02-21T00:22:36.9…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
5	2026-02-21T00:22:36.9…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
6	2026-02-21T00:22:36.9…	GetFeatureOpt…	64.189.232.77	arn:aws:iam::690332903554:ro…	
7	2026-02-21T00:22:36.9…	GetCostAndUsa…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
8	2026-02-21T00:22:36.9…	GetCostAndUsa…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
9	2026-02-21T00:22:36.9…	ListEnrollmen…	64.189.232.77	arn:aws:iam::690332903554:ro…	
10	2026-02-21T00:22:36.9…	ListNotificat…	64.189.232.77	arn:aws:iam::690332903554:ro…	
11	2026-02-21T00:22:36.9…	GenerateDataK…	cloudtrail.amazo…		
12	2026-02-21T00:22:36.9…	GetAccountCol…	64.189.232.77	arn:aws:iam::690332903554:ro…	
13	2026-02-21T00:22:36.9…	GetCostForeca…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
14	2026-02-21T00:22:36.9…	DescribeRegio…	64.189.232.77	arn:aws:iam::690332903554:ro…	
15	2026-02-21T00:22:36.9…	GetAccountPla…	64.189.232.77	arn:aws:iam::690332903554:ro…	
16	2026-02-21T00:22:36.9…	ListEnrollmen…	64.189.232.77	arn:aws:iam::690332903554:ro…	
17	2026-02-21T00:21:33.8…	ListAccountAc…	64.189.232.77	arn:aws:iam::690332903554:ro…	
18	2026-02-21T00:21:33.8…	ListApplicati…	64.189.232.77	arn:aws:iam::690332903554:ro…	
19	2026-02-21T00:21:33.8…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
20	2026-02-21T00:21:33.8…	GetFeatureOpt…	64.189.232.77	arn:aws:iam::690332903554:ro…	
21	2026-02-21T00:21:33.8…	GetCostForeca…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
22	2026-02-21T00:21:33.8…	ListManagedNo…	64.189.232.77	arn:aws:iam::690332903554:ro…	
23	2026-02-21T00:21:33.8…	GetCostAndUsa…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
24	2026-02-21T00:21:33.8…	ListApplicati…	64.189.232.77	arn:aws:iam::690332903554:ro…	
25	2026-02-21T00:21:33.7…	GetAccountPla…	64.189.232.77	arn:aws:iam::690332903554:ro…	
26	2026-02-21T00:21:33.7…	GetAccountCol…	64.189.232.77	arn:aws:iam::690332903554:ro…	
27	2026-02-21T00:21:33.7…	ListManagedNo…	64.189.232.77	arn:aws:iam::690332903554:ro…	
28	2026-02-21T00:21:33.7…	ListManagedNo…	64.189.232.77	arn:aws:iam::690332903554:ro…	
29	2026-02-21T00:21:33.7…	GenerateDataK…	cloudtrail.amazo…		
30	2026-02-21T00:21:33.7…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
31	2026-02-21T00:21:33.7…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
32	2026-02-21T00:21:24.5…	GenerateDataK…	cloudtrail.amazo…		
33	2026-02-21T00:21:24.5…	DescribeAlarms	64.189.232.77	arn:aws:iam::690332903554:ro…	
34	2026-02-21T00:21:24.5…	DescribeMetri…	64.189.232.77	arn:aws:iam::690332903554:ro…	
35	2026-02-21T00:21:24.5…	GetCostAndUsa…	64.189.232.77	arn:aws:iam::690332903554:ro…	AccessDenied
36	2026-02-21T00:21:24.5…	DescribeEvent…	64.189.232.77	arn:aws:iam::690332903554:ro…	
37	2026-02-21T00:20:26.3…	DescribeAlarms	64.189.232.77	arn:aws:iam::690332903554:ro…	
38	2026-02-21T00:20:26.3…	DescribeAlarms	64.189.232.77	arn:aws:iam::690332903554:ro…	
39	2026-02-21T00:20:26.3…	DescribeAlarms	64.189.232.77	arn:aws:iam::690332903554:ro…	

Facets (14)

Facets are automatically extracted from log fields based on the selected time range, up to the past 30 days. Select facets and click run to execute your query.

Facet Name	Events
@aws.region (1)	541
@data_format (1)	541
@data_source_name (1)	541
@data_source_type (1)	541
awsRegion (2)	541
errorCode (6)	183
eventCategory (1)	541
eventName (100+)	
eventSource (32)	541
eventType (3)	541
managementEvent (1)	541
readOnly (2)	541
severityText (0)	0
userAgent (9)	541

CloudWatch | us-east-1
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:logs-insights$3FqueryDetail$3D~(end~0~start~-...
Search
[Option+S]
United States (N. Virginia)
Nelson Wog (6903-3290-3554)
Nelson Wog
Filter table results (case insensitive)...
Facets
Fields
Info
Clear selection
Manage
Find facets or facet values
Filter: Selected Pinned
Expand all
1
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Hardening Measures:

- S3: Block public access, default encryption with KMS
- CloudTrail: KMS encryption, log file validation
- IAM/Users:
    - Minimal privileges for Nelson-admin
    - Root not used for day-to-day actions
    - Test-user removed after simulation

Conclusion: This lab demonstrates the full blue team workflow

Deploy EC2 and S3, enable CloudTrail + CloudWatch, simulate suspicious activity, detect it via CloudTrail logs and CloudWatch Logs insights, Harden the environment, collect and save evidence.