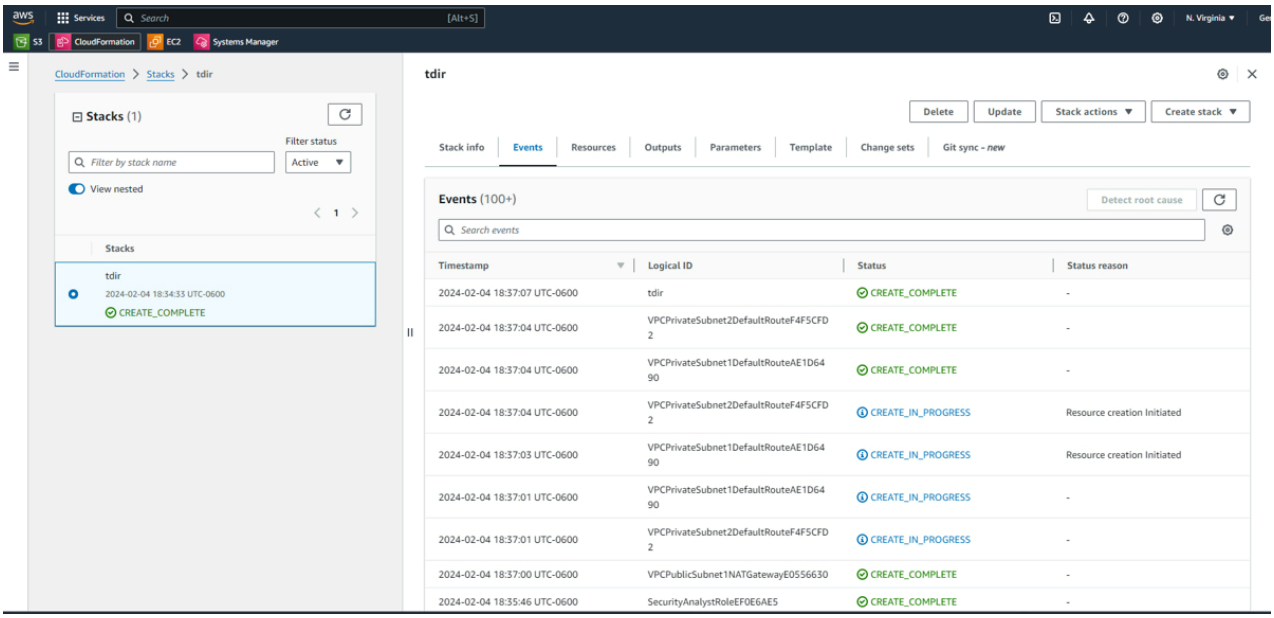
Cloud IR Walkthrough: AWS Workshop Unauthorized IAM

The following is a walkthrough through one of the posted AWS CIRT workshops that allow a CloudFormation template to build AWS resources in a personal account to go through a specific CIRT scenario. The link below provides the scenario of Simulation and Detection of Ransomware of unauthorized IAM Credential use and using AWS Athena to build queries for detection.

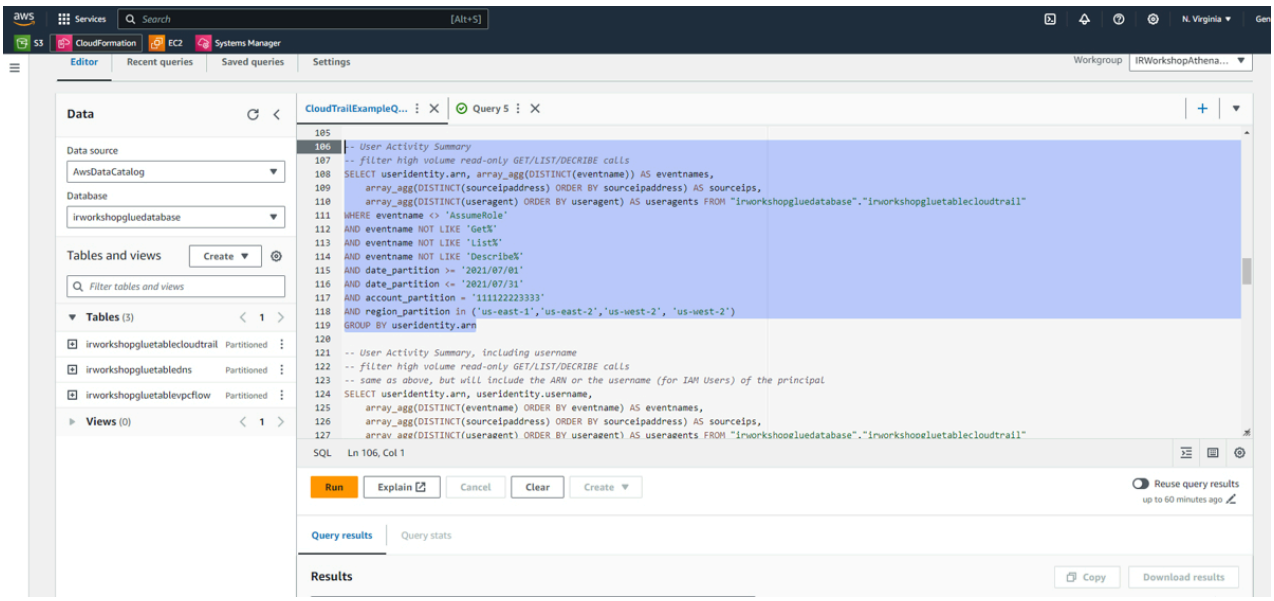
Workshop Studio

Follow the steps required in the AWS Workshop page under the Setup using your own AWS Account and completion should look like the following with resources setup using CloudFormation.

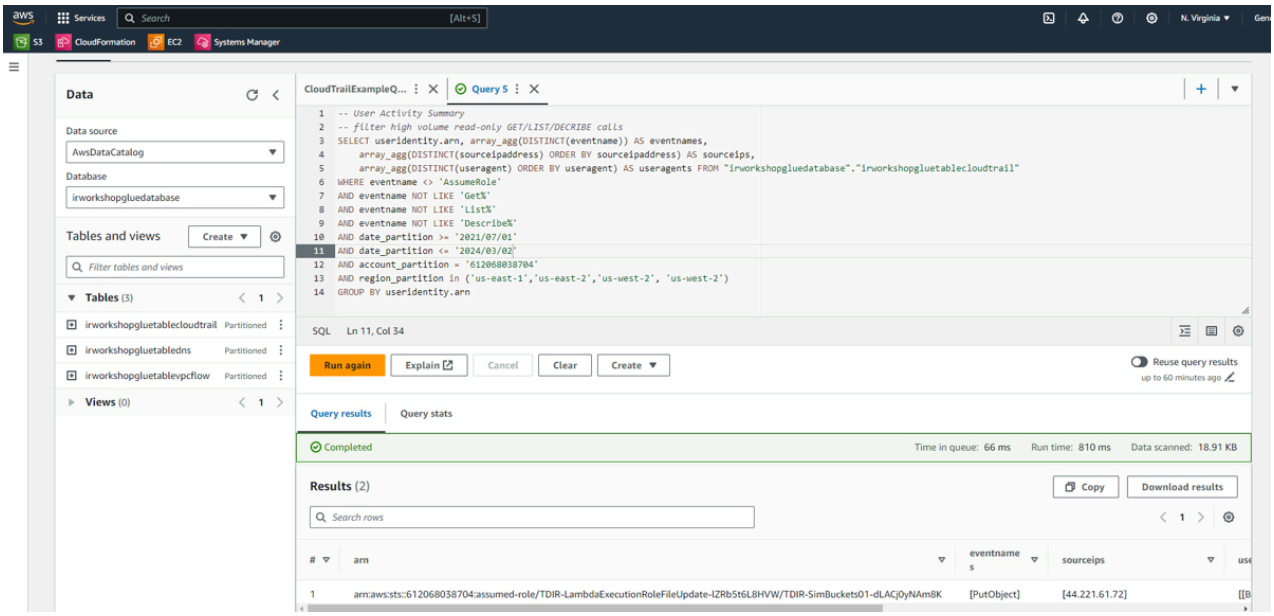


Use some of the saved queries to review the logs in the S3 buckets for the AWS account setup specifically the CloudTrail Logs using one of the queries as such with the date and AWS account ID.

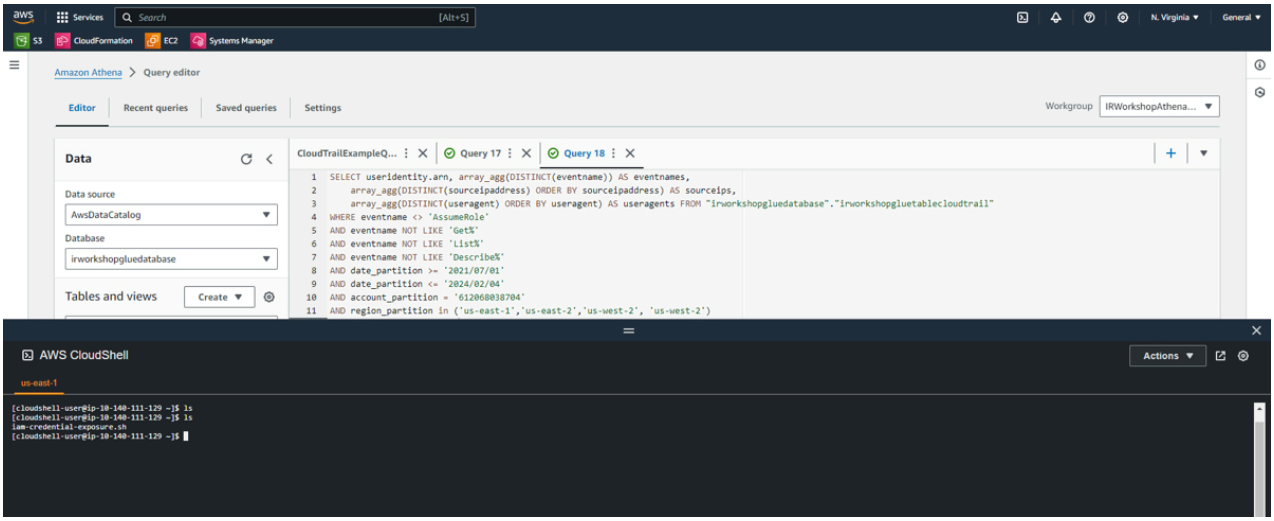
Workgroup for the AWS walkthrough should be "IRWorkshopAthenaWorkGroup".

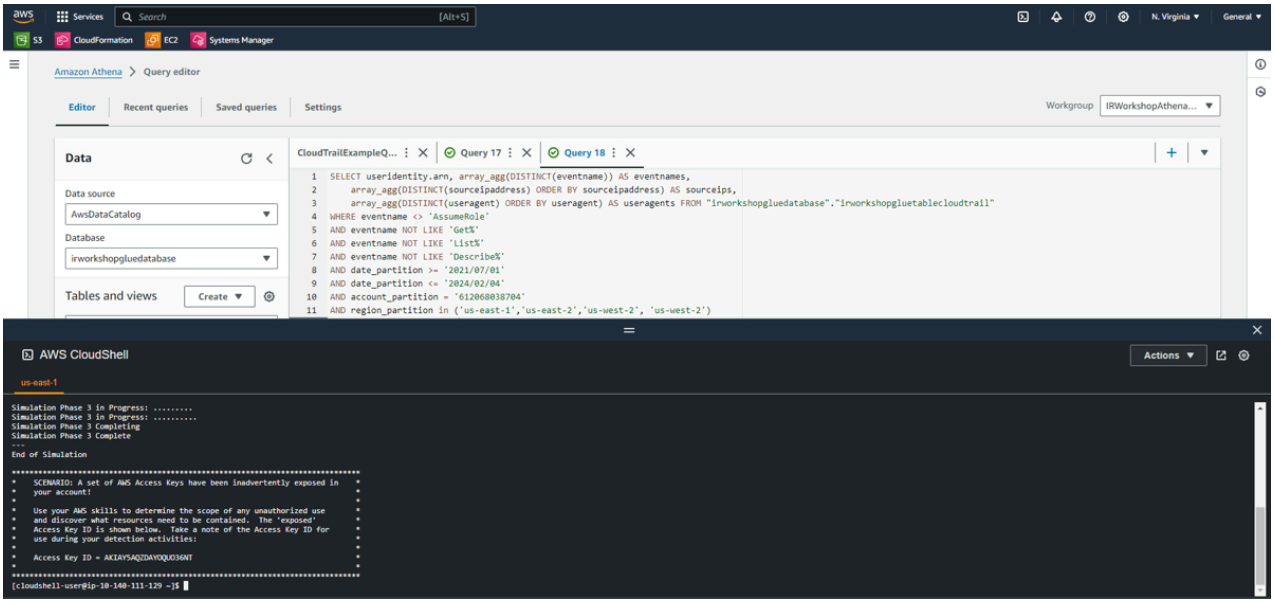


Modify the CloudTrail query to query the AWS account between the given dates for the IR workshop.



Afterwards, follow the steps in the AWS IR Workshop to simulate Ransomeware events with the upload of a bash script into AWS CloudShell.

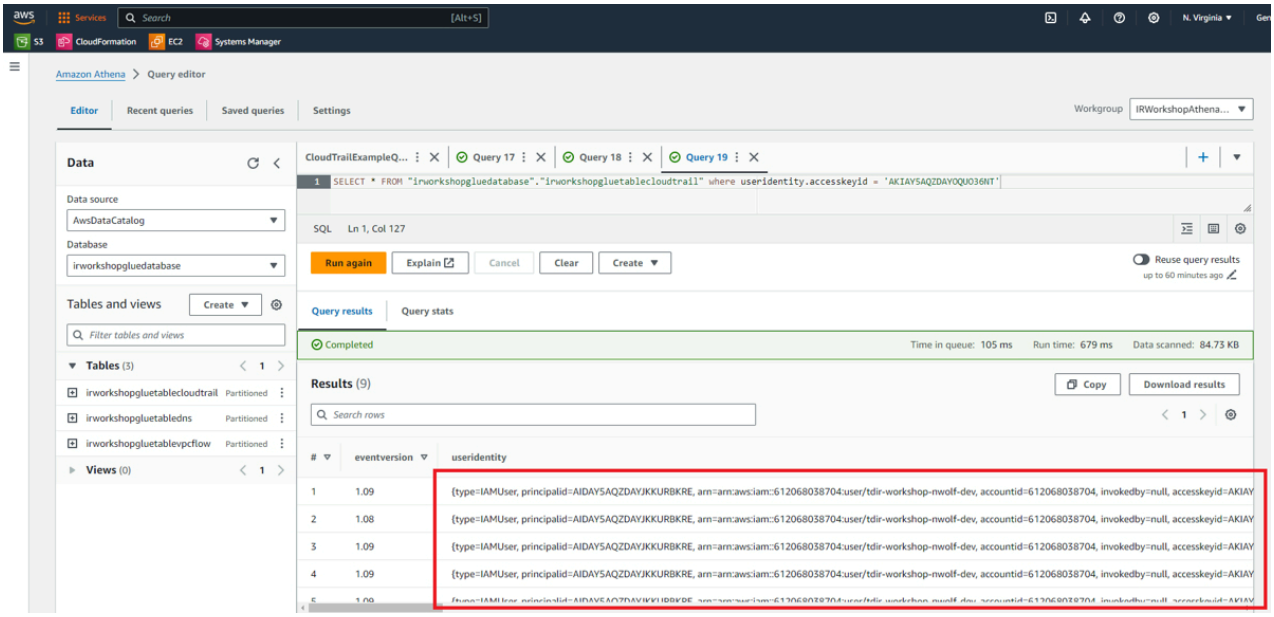


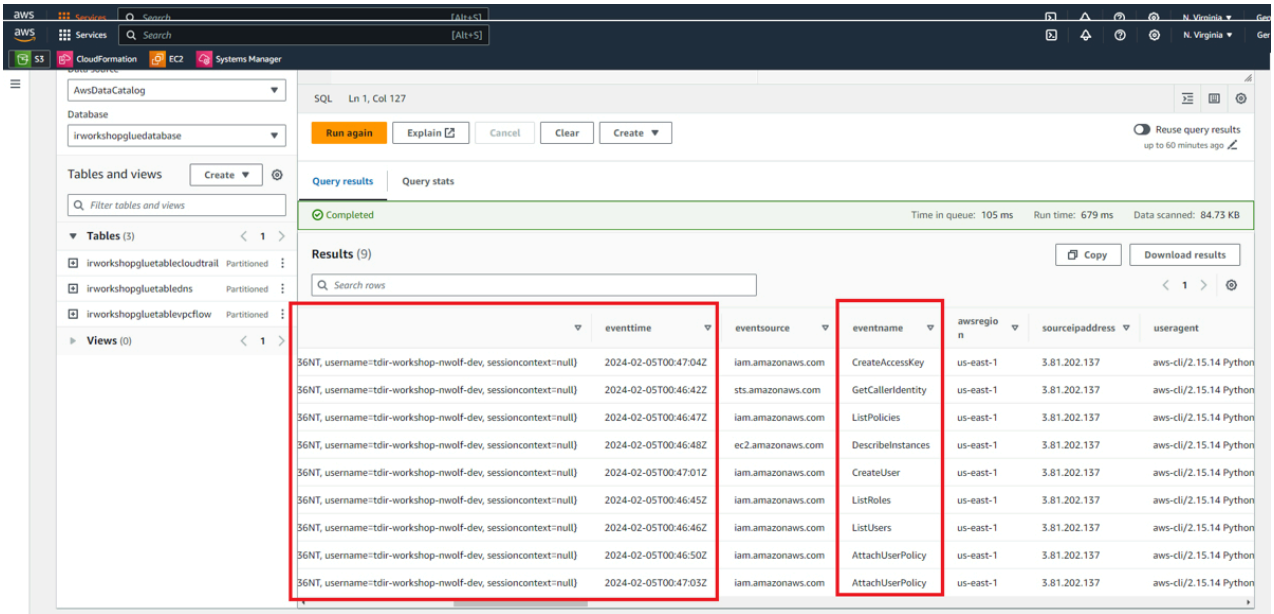


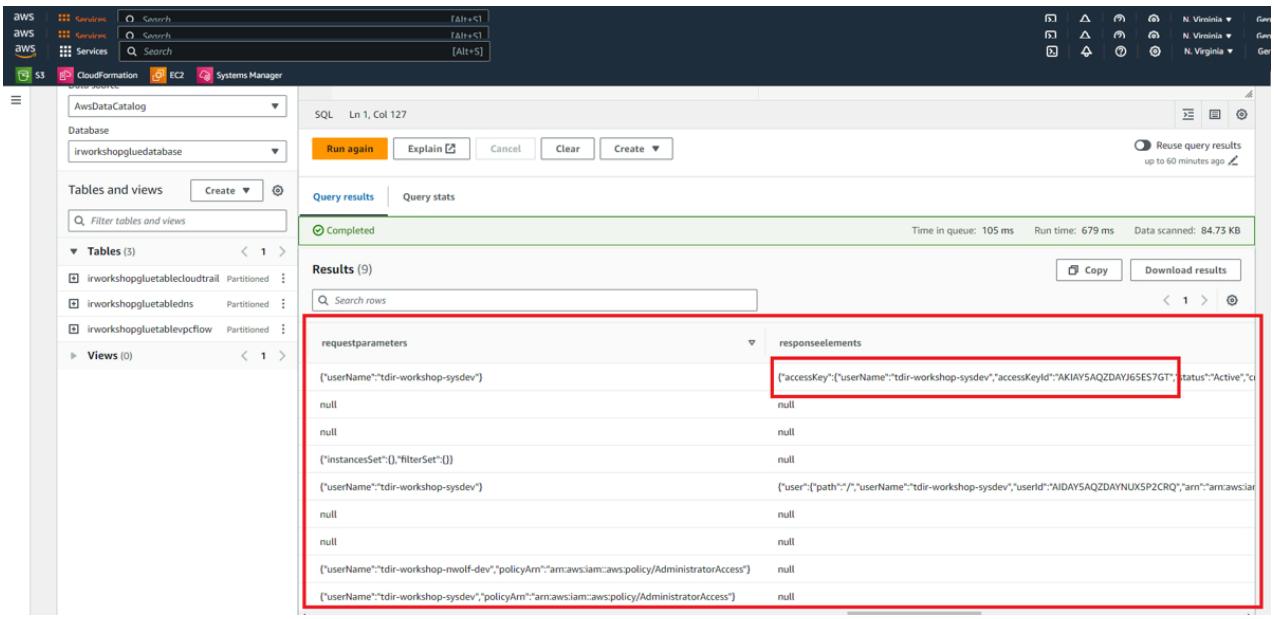
First, the AWS Workshop Unauthorized IAM will begin with an investigation of the IAM user Access Key posted above using AWS Athena queries on AWS CloudTrail API Calls.

The following AWS Athena query is meant to gather all CloudTrail events concerning the Unauthorized IAM user.

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" wh
```


Amazon Athena > Query editor
Editor
Recent queries
Saved queries
Settings
Workgroup
IRWorkshopAthena...
Data
Data source
AwsDataCatalog
Database
irworkshopgluedatabase
Tables and views
Create
Filter tables and views
Tables (3)
irworkshopgluetablecloudtrail Partitioned
irworkshopgluetableedns Partitioned
irworkshopgluetablevpcflow Partitioned
Views (0)
CloudTrailExampleQ...
Query 17
Query 18
Query 19
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.accesskeyid = 'AKIAY5AQZDAYOQUO36NT'
SQL Ln 1, Col 127
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Query results
Query stats
Completed
Time in queue: 105 ms
Run time: 679 ms
Data scanned: 84.73 KB
Results (9)
Copy
Download results
Search rows
eventversion useridentity
1 1.09 {type=IAMUser, principalid=AIDAY5AQZDAYJKKURBKRE, arn=arn:aws:iam::612068038704:user/tdir-workshop-nwolf-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
2 1.08 {type=IAMUser, principalid=AIDAY5AQZDAYJKKURBKRE, arn=arn:aws:iam::612068038704:user/tdir-workshop-nwolf-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
3 1.09 {type=IAMUser, principalid=AIDAY5AQZDAYJKKURBKRE, arn=arn:aws:iam::612068038704:user/tdir-workshop-nwolf-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
4 1.09 {type=IAMUser, principalid=AIDAY5AQZDAYJKKURBKRE, arn=arn:aws:iam::612068038704:user/tdir-workshop-nwolf-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY

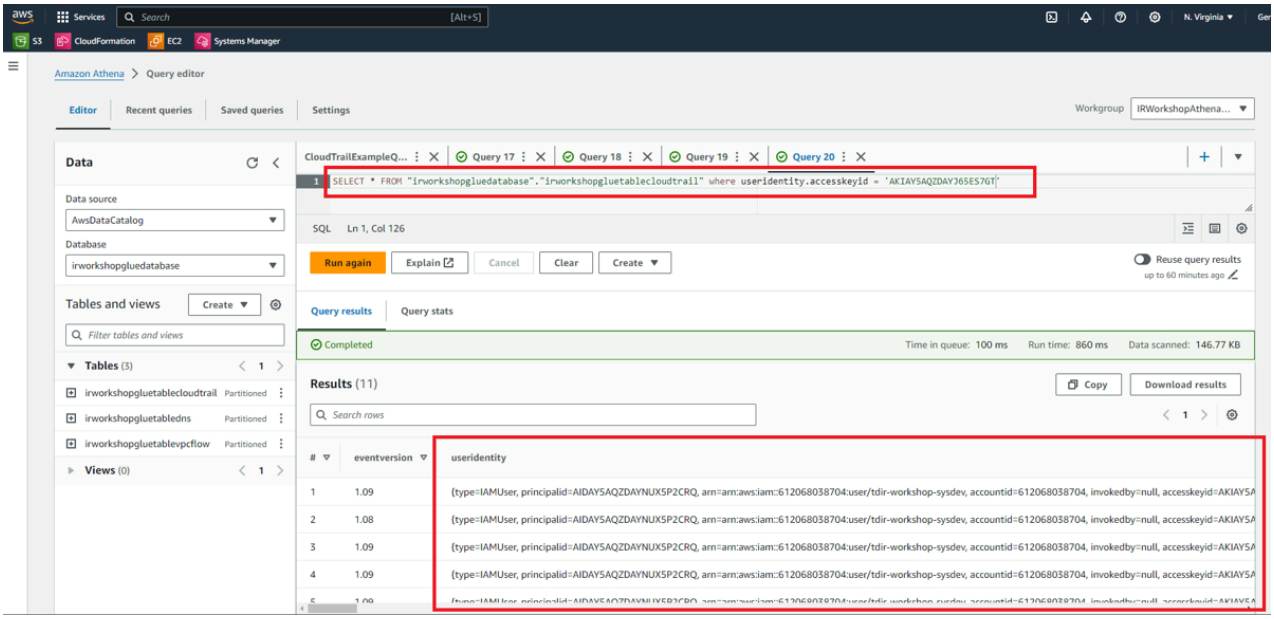

eventtime eventsource eventname awsregion sourceipaddress useragent
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:47:04Z iam.amazonaws.com CreateAccessKey us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:42Z sts.amazonaws.com GetCallerIdentity us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:47Z iam.amazonaws.com ListPolicies us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:48Z ec2.amazonaws.com DescribeInstances us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:47:01Z iam.amazonaws.com CreateUser us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:45Z iam.amazonaws.com ListRoles us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:46Z iam.amazonaws.com ListUsers us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:46:50Z iam.amazonaws.com AttachUserPolicy us-east-1 3.81.202.137 aws-cli/2.15.14 Python
36NT, username=tdir-workshop-nwolf-dev, sessioncontext=null} 2024-02-05T00:47:03Z iam.amazonaws.com AttachUserPolicy us-east-1 3.81.202.137 aws-cli/2.15.14 Python

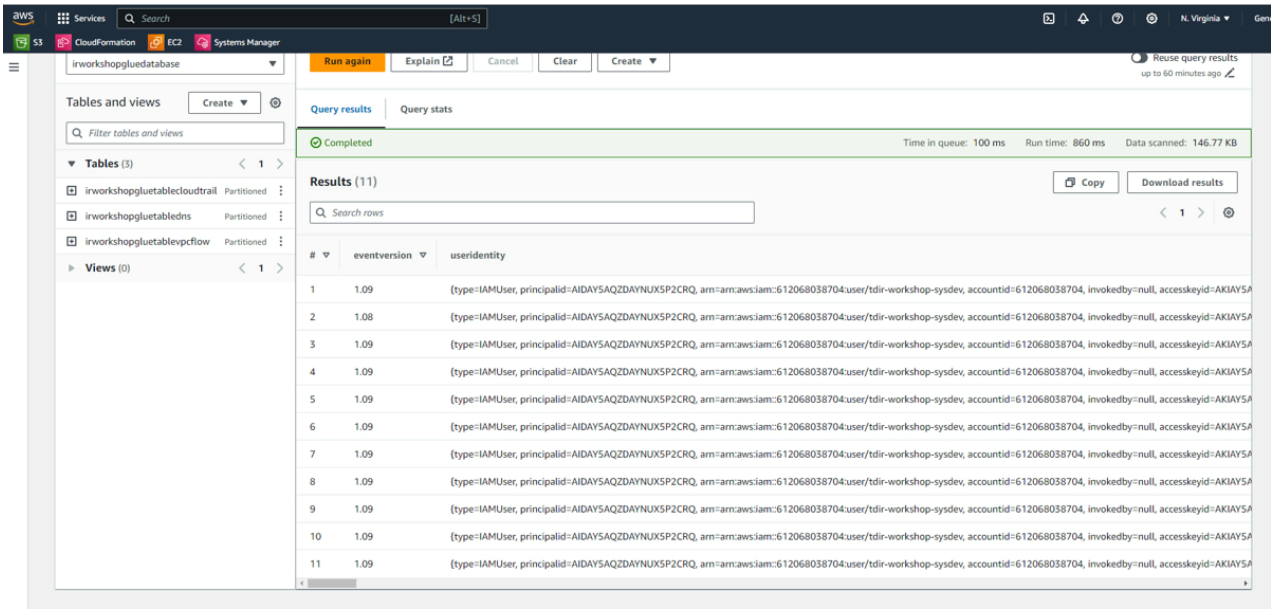

requestparameters responseelements
{"userName":"tdir-workshop-sysdev"} {"accessKey":{"userName":"tdir-workshop-sysdev","accessKeyId":"AKIAY5AQZDAYJ65ES7GT","status":"Active",
null null
null null
{"instancesSet":{},"filterSet":{}} null
{"userName":"tdir-workshop-sysdev"} {"user":{"path":"/","userName":"tdir-workshop-sysdev","userId":"AIDAY5AQZDAYNUX5P2CRQ","arn":"arn:aws:
null null
null null
{"userName":"tdir-workshop-nwolf-dev","policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"} null
{"userName":"tdir-workshop-sysdev","policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"} null

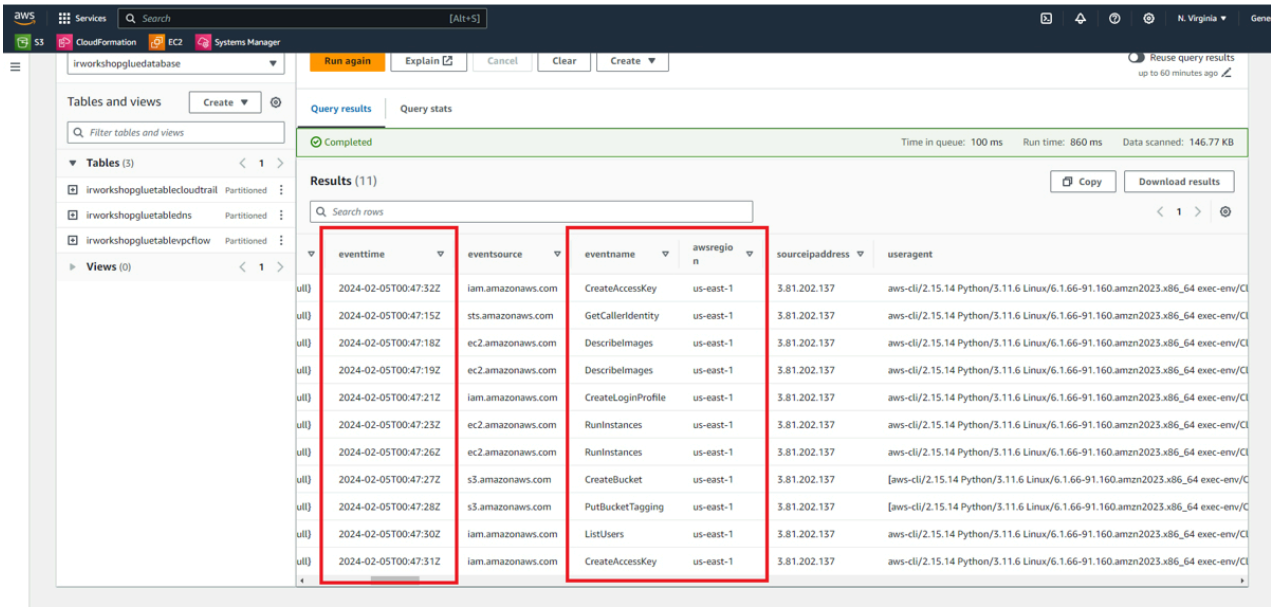
Notice in the AWS CloudTrail results that the useridentity associated with Unauthorized IAM user is "tdir-workshop-nwolf-dev" when using the AWS Athena search queries. Furthermore, looking at the additional AWS CloudTrail API calls you are able to see that a "CreateAccessKey" was used by the "tdir-workshop-nwolf-dev" IAM user to create a new AWS Access Key for AWS IAM user "tdir-workshop-sysdev" within the AWS account that needs furter investigation. Additionally, the Unauthorized IAM user "tdir-workshop-nwolf-dev" used the "CreateUser" CloudTrail API call to create the "tdir-workshop-sysdev" earlier than the "CreateAccessKey" CloudTrail API call to achieve some persistence with an additional AWS IAM user account.

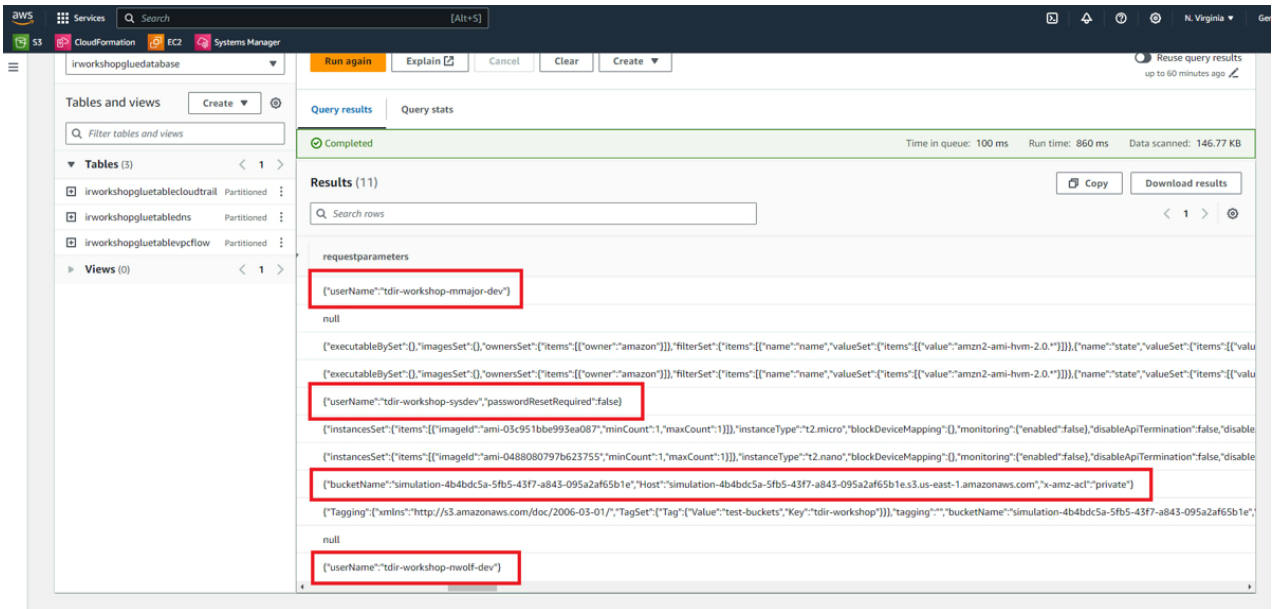
Copy the newly created AWS IAM user Access Key and run the previous AWS Athena query to review the CloudTrail API calls by the unathorized AWS IAM user.

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" wh
```




Services
Search
[Alt+S]
S3
CloudFormation
EC2
Systems Manager
N. Virginia
irworkshopgluedatabase
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Tables and views
Create
Filter tables and views
Tables (3)
irworkshopgluetablecloudtrail Partitioned
irworkshopgluetableedns Partitioned
irworkshopgluetablevpcflow Partitioned
Views (0)
Query results
Query stats
Completed
Time in queue: 100 ms
Run time: 860 ms
Data scanned: 146.77 KB
Results (11)
Copy
Download results
Search rows
eventversion useridentity
1 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
2 1.08 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
3 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
4 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
5 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
6 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
7 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
8 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
9 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
10 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA
11 1.09 {type=IAMUser, principalid=AIDAYSAQZDAYNUX5P2CRQ, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAYSA


Services
Search
[Alt+S]
S3
CloudFormation
EC2
Systems Manager
N. Virginia
irworkshopgluedatabase
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Tables and views
Create
Filter tables and views
Tables (3)
irworkshopgluetablecloudtrail Partitioned
irworkshopgluetableedns Partitioned
irworkshopgluetablevpcflow Partitioned
Views (0)
Query results
Query stats
Completed
Time in queue: 100 ms
Run time: 860 ms
Data scanned: 146.77 KB
Results (11)
Copy
Download results
Search rows
eventtime eventsource eventname awsregion sourceipaddress useragent
2024-02-05T00:47:32Z iam.amazonaws.com CreateAccessKey us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:15Z sts.amazonaws.com GetCallerIdentity us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:18Z ec2.amazonaws.com DescribeImages us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:19Z ec2.amazonaws.com DescribeImages us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:21Z iam.amazonaws.com CreateLoginProfile us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:23Z ec2.amazonaws.com RunInstances us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:26Z ec2.amazonaws.com RunInstances us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:27Z s3.amazonaws.com CreateBucket us-east-1 3.81.202.137 [aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/C
2024-02-05T00:47:28Z s3.amazonaws.com PutBucketTagging us-east-1 3.81.202.137 [aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/C
2024-02-05T00:47:30Z iam.amazonaws.com ListUsers us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL
2024-02-05T00:47:31Z iam.amazonaws.com CreateAccessKey us-east-1 3.81.202.137 aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CL


Services
Search
[Alt+S]
S3
CloudFormation
EC2
Systems Manager
N. Virginia
irworkshopgluedatabase
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Tables and views
Create
Filter tables and views
Tables (3)
irworkshopgluetablecloudtrail Partitioned
irworkshopgluetableedns Partitioned
irworkshopgluetablevpcflow Partitioned
Views (0)
Query results
Query stats
Completed
Time in queue: 100 ms
Run time: 860 ms
Data scanned: 146.77 KB
Results (11)
Copy
Download results
Search rows
requestparameters
{"userName":"tdir-workshop-mmajor-dev"}
null
{"executableBySet":{},"imagesSet":{},"ownersSet":{"items":[{"owner":"amazon"}]},"filterSet":{"items":[{"name":"name","valueSet":{"items":[{"value":"amzn2-ami-hvm-2.0.*"}]}},{"name":"state","valueSet":{"items":[{"valu
{"executableBySet":{},"imagesSet":{},"ownersSet":{"items":[{"owner":"amazon"}]},"filterSet":{"items":[{"name":"name","valueSet":{"items":[{"value":"amzn2-ami-hvm-2.0.*"}]}},{"name":"state","valueSet":{"items":[{"valu
{"userName":"tdir-workshop-sysdev","passwordResetRequired":false}
{"instancesSet":{"items":[{"imageId":"ami-03c951bbe993ea087","minCount":1,"maxCount":1}]},"instanceType":"t2.micro","blockDeviceMapping":{},"monitoring":{"enabled":false},"disableApiTermination":false,"disable
{"instancesSet":{"items":[{"imageId":"ami-0488080797b623755","minCount":1,"maxCount":1}]},"instanceType":"t2.nano","blockDeviceMapping":{},"monitoring":{"enabled":false},"disableApiTermination":false,"disable
{"bucketName":"simulation-4b4bdc5a-5fb5-43f7-a843-095a2af65b1e","Host":"simulation-4b4bdc5a-5fb5-43f7-a843-095a2af65b1e.s3.us-east-1.amazonaws.com","x-amz-acl":"private"}
{"Tagging":{"xmlns":"http://s3.amazonaws.com/doc/2006-03-01/","TagSet":{"Tag":{"Value":"test-buckets","Key":"tdir-workshop"}}},"tagging":"","bucketName":"simulation-4b4bdc5a-5fb5-43f7-a843-095a2af65b1e",
null
{"userName":"tdir-workshop-nwolf-dev"}