

# 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.

The screenshot displays the AWS CloudFormation console for a stack named 'tdir'. The 'Events' tab is selected, showing a list of 100+ events. The stack is in a 'CREATE\_COMPLETE' state. The events table lists the following resources and their creation status:

Timestamp	Logical ID	Status	Status reason
2024-02-04 18:37:07 UTC-0600	tdir	CREATE_COMPLETE	-
2024-02-04 18:37:04 UTC-0600	VPCPrivateSubnet2DefaultRouteF4F5CFD2	CREATE_COMPLETE	-
2024-02-04 18:37:04 UTC-0600	VPCPrivateSubnet1DefaultRouteAE1D6490	CREATE_COMPLETE	-
2024-02-04 18:37:04 UTC-0600	VPCPrivateSubnet2DefaultRouteF4F5CFD2	CREATE_IN_PROGRESS	Resource creation Initiated
2024-02-04 18:37:03 UTC-0600	VPCPrivateSubnet1DefaultRouteAE1D6490	CREATE_IN_PROGRESS	Resource creation Initiated
2024-02-04 18:37:01 UTC-0600	VPCPrivateSubnet1DefaultRouteAE1D6490	CREATE_IN_PROGRESS	-
2024-02-04 18:37:01 UTC-0600	VPCPrivateSubnet2DefaultRouteF4F5CFD2	CREATE_IN_PROGRESS	-
2024-02-04 18:37:00 UTC-0600	VPCPublicSubnet1NATGatewayE0556630	CREATE_COMPLETE	-
2024-02-04 18:35:46 UTC-0600	SecurityAnalystRoleEFOE6AE5	CREATE_COMPLETE	-

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".

The screenshot shows the AWS Athena console interface. On the left, the 'Data' pane shows the 'AwsDataCatalog' data source and the 'inworkshopgluedatabase' database. The 'Tables and views' section lists several tables including 'inworkshopgluetablecloudtrail'. The main pane displays a SQL query titled 'CloudTrailExampleQ...' with the following content:

```

105
106 -- User Activity Summary
107 -- filter high volume read-only GET/LIST/DESCRIBE calls
108 SELECT useridentity.arn, array_agg(DISTINCT(eventname)) AS eventnames,
109        array_agg(DISTINCT(sourceipaddress) ORDER BY sourceipaddress) AS sourceips,
110        array_agg(DISTINCT(useragent) ORDER BY useragent) AS useragents FROM "inworkshopgluedatabase"."inworkshopgluetablecloudtrail"
111 WHERE eventname <> 'AssumeRole'
112 AND eventname NOT LIKE 'Get%'
113 AND eventname NOT LIKE 'List%'
114 AND eventname NOT LIKE 'Describe%'
115 AND date_partition >= '2021/07/01'
116 AND date_partition <= '2021/07/31'
117 AND account_partition = '111122223333'
118 AND region_partition IN ('us-east-1','us-east-2','us-west-2','us-west-2')
119 GROUP BY useridentity.arn
120
121 -- User Activity Summary, including username
122 -- filter high volume read-only GET/LIST/DESCRIBE calls
123 -- same as above, but will include the ARN or the username (for IAM Users) of the principal
124 SELECT useridentity.arn, useridentity.username,
125        array_agg(DISTINCT(eventname) ORDER BY eventname) AS eventnames,
126        array_agg(DISTINCT(sourceipaddress) ORDER BY sourceipaddress) AS sourceips,
127        array_agg(DISTINCT(useragent) ORDER BY useragent) AS useragents FROM "inworkshopgluedatabase"."inworkshopgluetablecloudtrail"

```

Below the query editor, there are buttons for 'Run', 'Explain', 'Cancel', 'Clear', and 'Create'. The 'Query results' tab is selected, showing 'Query stats'.

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

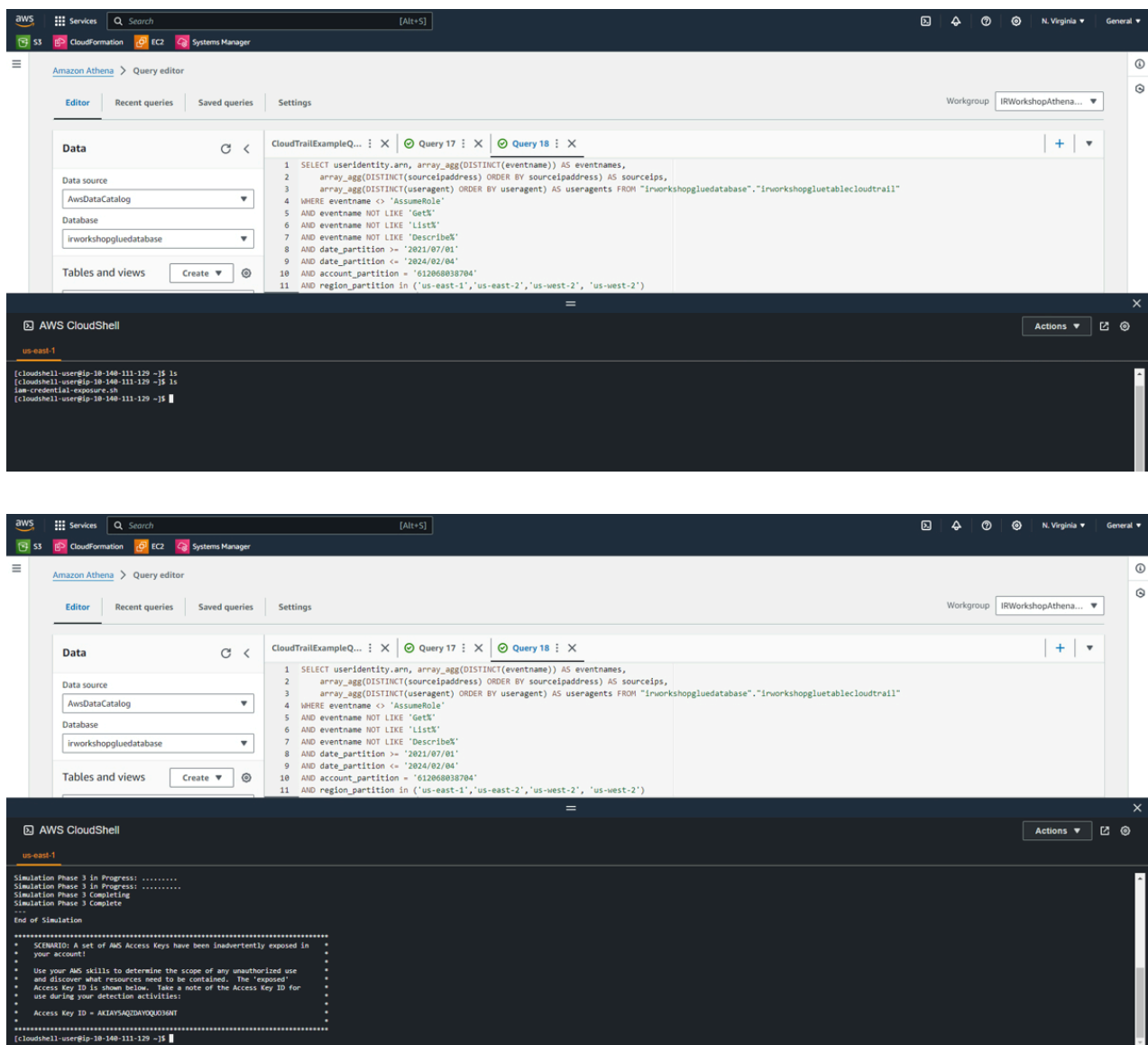
The screenshot shows the AWS Athena console interface after the query has been executed. The 'Query results' tab is selected, showing 'Query stats' and 'Results (2)'. The query is highlighted in blue. The results table shows the following data:

#	arn	eventname	sourceips	useragents
1	arn:aws:sts:612068038704:assumed-role/TDIR-LambdaExecutionRoleFileUpdate-IZRb5t6L8HVW/TDIR-SimBuckets01-dLAcJyNAmBK	[PutObject]	[44.221.61.72]	[B...

Below the results table, there are buttons for 'Copy' and 'Download results'. The 'Query stats' section shows the following information:

- Completed
- Time in queue: 66 ms
- Run time: 810 ms
- Data scanned: 18.91 KB

Afterwards, follow the steps in the AWS IR Workshop to simulate Ransomware 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 source: AwsDataCatalog Database: inworkshopgluedatabase

Tables and views: Filter tables and views

Tables (3): inworkshopgluetablecloudtrail, inworkshopgluetabledns, inworkshopgluetablevpcflow

Views (0)

SQL: `SELECT * FROM "inworkshopgluedatabase"."inworkshopgluetablecloudtrail" where userIdentity.accessKeyId = 'AKIAJ5AQZDAYOQ036NT'`

Run again Explain Cancel Clear Create

Query results Query stats

Completed Time in queue: 105 ms Run time: 679 ms Data scanned: 84.73 KB

Results (9)

#	eventversion	userIdentity
1	1.09	(type=IAMUser, principalId=AIDAYSQZDAYJKKURBKRE, arn=arn:aws:iam:612068038704:user/tdir-workshop-nwolf-dev, accountId=612068038704, invokedBy=null, accessKeyId=AKIAJ5AQZDAYOQ036NT)
2	1.08	(type=IAMUser, principalId=AIDAYSQZDAYJKKURBKRE, arn=arn:aws:iam:612068038704:user/tdir-workshop-nwolf-dev, accountId=612068038704, invokedBy=null, accessKeyId=AKIAJ5AQZDAYOQ036NT)
3	1.09	(type=IAMUser, principalId=AIDAYSQZDAYJKKURBKRE, arn=arn:aws:iam:612068038704:user/tdir-workshop-nwolf-dev, accountId=612068038704, invokedBy=null, accessKeyId=AKIAJ5AQZDAYOQ036NT)
4	1.09	(type=IAMUser, principalId=AIDAYSQZDAYJKKURBKRE, arn=arn:aws:iam:612068038704:user/tdir-workshop-nwolf-dev, accountId=612068038704, invokedBy=null, accessKeyId=AKIAJ5AQZDAYOQ036NT)

SQL: `SELECT * FROM "inworkshopgluedatabase"."inworkshopgluetablecloudtrail" where userIdentity.accessKeyId = 'AKIAJ5AQZDAYOQ036NT'`

Run again Explain Cancel Clear Create

Query results Query stats

Completed Time in queue: 105 ms Run time: 679 ms Data scanned: 84.73 KB

Results (9)

#	eventtime	eventsources	eventname	awsregion	sourceaddress	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

SQL: `SELECT * FROM "inworkshopgluedatabase"."inworkshopgluetablecloudtrail" where userIdentity.accessKeyId = 'AKIAJ5AQZDAYOQ036NT'`

Run again Explain Cancel Clear Create

Query results Query stats

Completed Time in queue: 105 ms Run time: 679 ms Data scanned: 84.73 KB

Results (9)

requestparameters	responseelements
({"userName":"tdir-workshop-sysdev"}	({"accessKey":{"userName":"tdir-workshop-sysdev","accessKeyId":"AKIAJ5AQZDAYJ65E7GT","status":"Active","c"}
null	null
({"instancesSet":[],"filterSet":[]}	null
({"userName":"tdir-workshop-sysdev"}	({"user":{"path":"/","userName":"tdir-workshop-sysdev","userId":"AIDAYSQZDAYNUXSP2CRQ","arn":"arn:aws:iam:612068038704:user/tdir-workshop-sysdev"}}
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 further 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 unauthorized AWS IAM user.

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

The screenshot shows the Amazon Athena Query Editor interface. The query being executed is:

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.accesskeyid = 'AKIAV5AQZDAY76SE576T'
```

The query has completed successfully. The results show 11 rows. The first four rows are highlighted with a red box, showing the 'eventversion' and 'useridentity' columns. The 'useridentity' column contains the following values:

- (type=IAMUser, principal=AKIAV5AQZDAY76SE576T, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAV5AQZDAY76SE576T)
- (type=IAMUser, principal=AKIAV5AQZDAY76SE576T, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAV5AQZDAY76SE576T)
- (type=IAMUser, principal=AKIAV5AQZDAY76SE576T, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAV5AQZDAY76SE576T)
- (type=IAMUser, principal=AKIAV5AQZDAY76SE576T, arn=arn:aws:iam::612068038704:user/tdir-workshop-sysdev, accountid=612068038704, invokedby=null, accesskeyid=AKIAV5AQZDAY76SE576T)



The screenshot shows the AWS Systems Manager console. The top navigation bar includes 'AWS', 'Services', 'Search', and the user's name 'N. Virginia'. The left sidebar shows the 'Systems Manager' service selected. The main content area displays the 'Run' button in orange, with other buttons like 'Explain', 'Cancel', 'Clear', and 'Create'. Below the 'Run' button, the 'Query results' section shows a list of results for the 'irworkshopgluedatabase' instance. The results are displayed in a table with columns for 'requestParameters', 'tags', and 'tags'. The 'requestParameters' column contains a JSON object with 'userName' and 'passwordResetRequired' fields. The 'tags' column contains a list of tags, including 'Name', 'Environment', and 'Project'. The 'tags' column also includes a 'requestParameters' field with a JSON object containing 'userName' and 'passwordResetRequired' fields. The 'tags' column also includes a 'requestParameters' field with a JSON object containing 'userName' and 'passwordResetRequired' fields.

