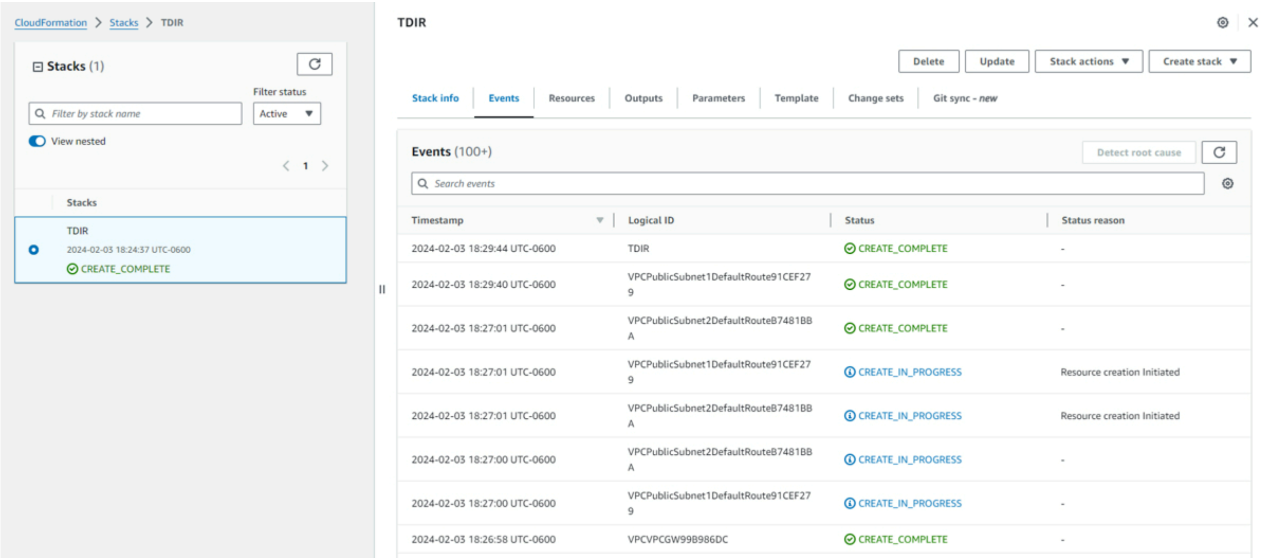
Cloud IR Walkthrough: AWS Workshop Ransomware on S3

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 in a S3 Bucket 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.

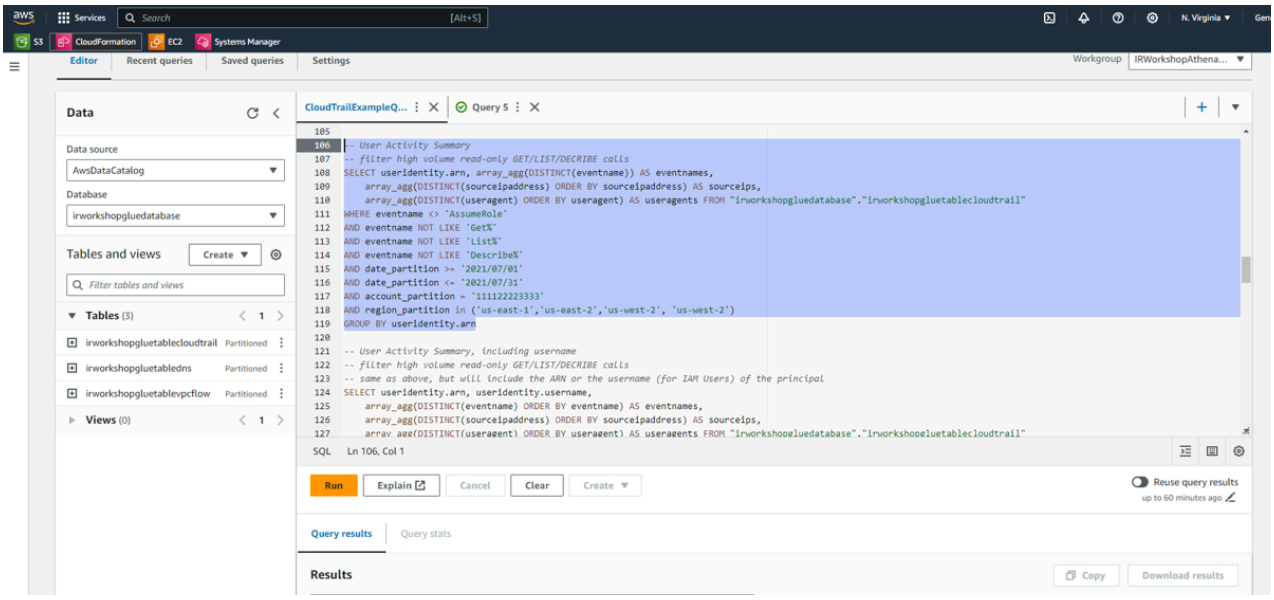


Stacks
TDIR 2024-02-03 18:24:37 UTC-0600 CREATE_COMPLETE

Timestamp	Logical ID	Status	Status reason
2024-02-03 18:29:44 UTC-0600	TDIR	CREATE_COMPLETE	-
2024-02-03 18:29:40 UTC-0600	VPCPublicSubnet1DefaultRoute91CEF279	CREATE_COMPLETE	-
2024-02-03 18:27:01 UTC-0600	VPCPublicSubnet2DefaultRouteB7481BBA	CREATE_COMPLETE	-
2024-02-03 18:27:01 UTC-0600	VPCPublicSubnet1DefaultRoute91CEF279	CREATE_IN_PROGRESS	Resource creation Initiated
2024-02-03 18:27:01 UTC-0600	VPCPublicSubnet2DefaultRouteB7481BBA	CREATE_IN_PROGRESS	Resource creation Initiated
2024-02-03 18:27:00 UTC-0600	VPCPublicSubnet2DefaultRouteB7481BBA	CREATE_IN_PROGRESS	-
2024-02-03 18:27:00 UTC-0600	VPCPublicSubnet1DefaultRoute91CEF279	CREATE_IN_PROGRESS	-
2024-02-03 18:26:58 UTC-0600	VPCVPCGW99B986DC	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".



Data source: AwsDataCatalog

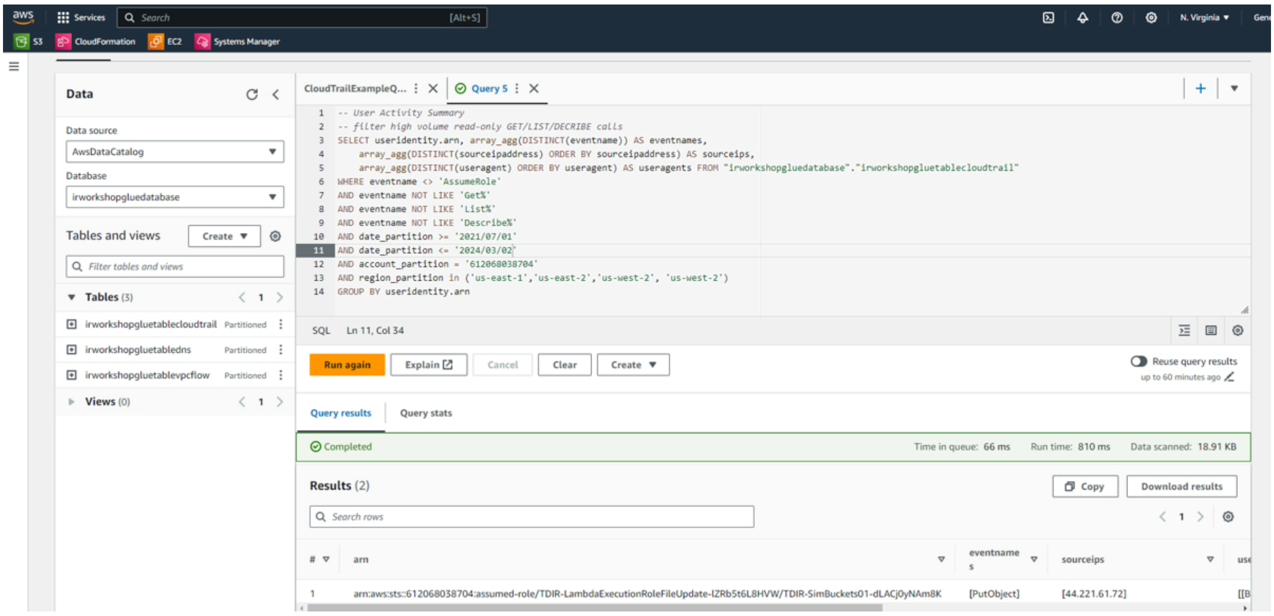
Database: irworkshopgluedatabase

Workgroup: IRWorkshopAthena...

```
-- User Activity Summary
-- filter high volume read-only GET/LIST/DECRIBE calls
SELECT useridentity.arn, array_agg(DISTINCT(eventname)) AS eventnames,
    array_agg(DISTINCT(sourceipaddress) ORDER BY sourceipaddress) AS sourceips,
    array_agg(DISTINCT(useragent) ORDER BY useragent) AS useragents FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail"
WHERE eventname <> 'AssumeRole'
AND eventname NOT LIKE 'Get%'
AND eventname NOT LIKE 'List%'
AND eventname NOT LIKE 'Describe%'
AND date_partition >= '2021/07/01'
AND date_partition <= '2021/07/31'
AND account_partition = '111122223333'
AND region_partition in ('us-east-1','us-east-2','us-west-2', 'us-west-2')
GROUP BY useridentity.arn

-- User Activity Summary, including username
-- filter high volume read-only GET/LIST/DECRIBE calls
-- same as above, but will include the ARN or the username (for IAM Users) of the principal
SELECT useridentity.arn, useridentity.username,
    array_agg(DISTINCT(eventname) ORDER BY eventname) AS eventnames,
    array_agg(DISTINCT(sourceipaddress) ORDER BY sourceipaddress) AS sourceips,
    array_agg(DISTINCT(useragent) ORDER BY useragent) AS useragents FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail"
```

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



Data source: AwsDataCatalog

Database: irworkshopgluedatabase

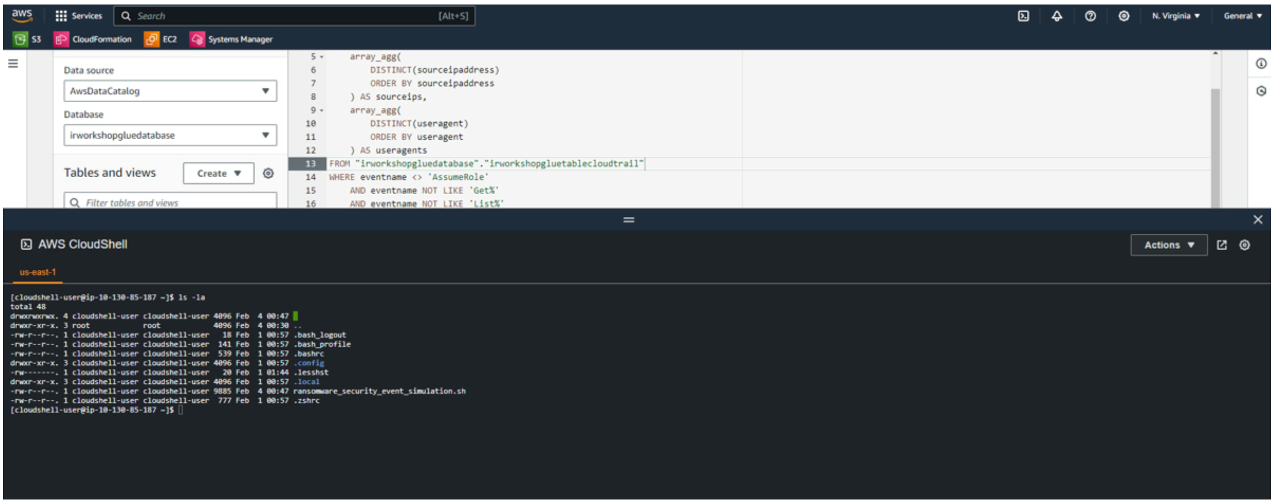
```
-- User Activity Summary
-- filter high volume read-only GET/LIST/DECRIBE calls
SELECT useridentity.arn, array_agg(DISTINCT(eventname)) AS eventnames,
    array_agg(DISTINCT(sourceipaddress) ORDER BY sourceipaddress) AS sourceips,
    array_agg(DISTINCT(useragent) ORDER BY useragent) AS useragents FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail"
WHERE eventname <> 'AssumeRole'
AND eventname NOT LIKE 'Get%'
AND eventname NOT LIKE 'List%'
AND eventname NOT LIKE 'Describe%'
AND date_partition >= '2021/07/01'
AND date_partition <= '2024/03/02'
AND account_partition = '612068038704'
AND region_partition in ('us-east-1','us-east-2','us-west-2', 'us-west-2')
GROUP BY useridentity.arn
```

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

Results (2)

#	arn	eventnames	sourceips	use
1	arn:aws:sts::612068038704:assumed-role/TDIR-LambdaExecutionRoleFileUpdate-lZRb5t6L8HVW/TDIR-SimBuckets01-dLACj0yNAm8K	[PutObject]	[44.221.61.72]	[[B

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

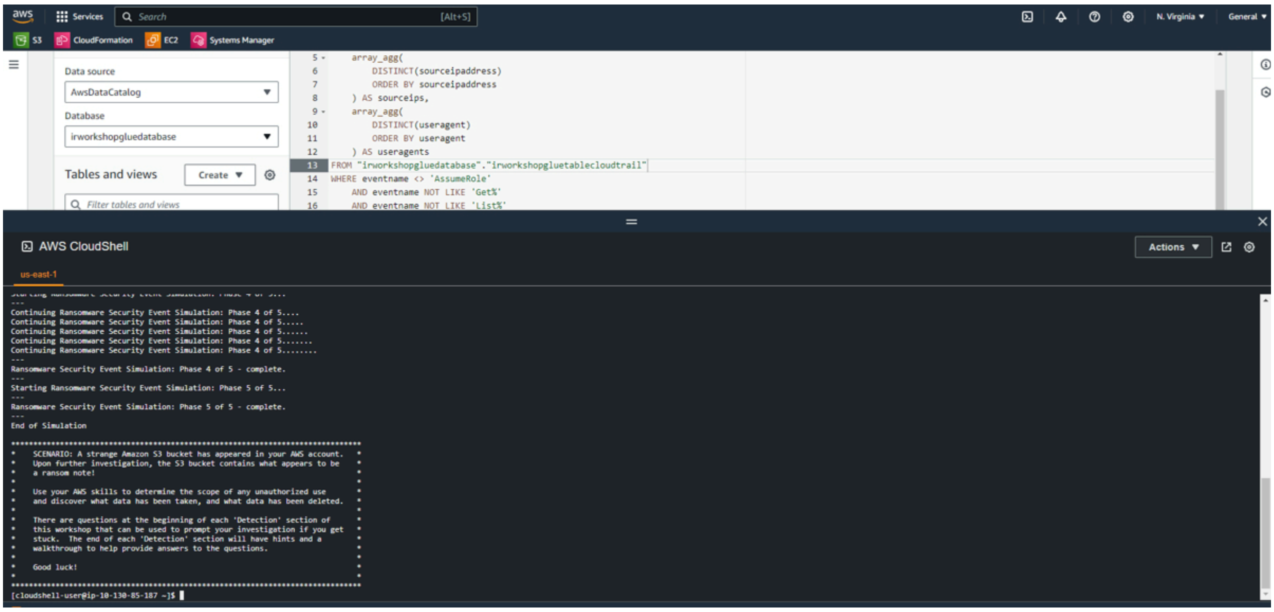


Data source: AwsDataCatalog

Database: irworkshopgluedatabase

```
    array_agg(
        DISTINCT(sourceipaddress)
        ORDER BY sourceipaddress
    ) AS sourceips,
    array_agg(
        DISTINCT(useragent)
        ORDER BY useragent
    ) AS useragents
FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail"
WHERE eventname <> 'AssumeRole'
    AND eventname NOT LIKE 'Get%'
    AND eventname NOT LIKE 'List%'
```

```
[cloudshell-user@ip-10-130-85-187 ~]$ ls -la
total 48
drwxrwxrwx. 4 cloudshell-user cloudshell-user 4096 Feb  4 00:47 .
drwxr-xr-x. 3 root            root            4096 Feb  4 00:30 ..
-rw-r--r--. 1 cloudshell-user cloudshell-user   18 Feb  1 00:57 .bash_logout
-rw-r--r--. 1 cloudshell-user cloudshell-user  141 Feb  1 00:57 .bash_profile
-rw-r--r--. 1 cloudshell-user cloudshell-user  539 Feb  1 00:57 .bashrc
drwxr-xr-x. 3 cloudshell-user cloudshell-user 4096 Feb  1 00:57 .config
-rw-------. 1 cloudshell-user cloudshell-user   20 Feb  1 01:44 .lesshst
drwxr-xr-x. 3 cloudshell-user cloudshell-user 4096 Feb  1 00:57 .local
-rw-r--r--. 1 cloudshell-user cloudshell-user 9885 Feb  4 00:47 ransomware_security_event_simulation.sh
-rw-r--r--. 1 cloudshell-user cloudshell-user  777 Feb  1 00:57 .zshrc
[cloudshell-user@ip-10-130-85-187 ~]$
```



Data source: AwsDataCatalog

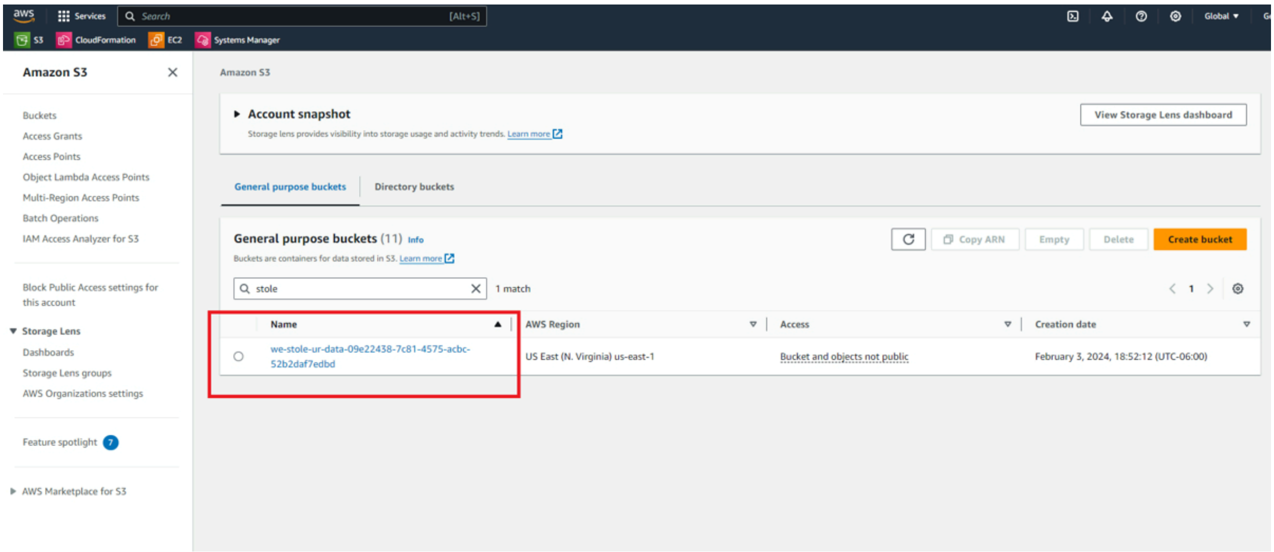
Database: irworkshopgluedatabase

```
    array_agg(
        DISTINCT(sourceipaddress)
        ORDER BY sourceipaddress
    ) AS sourceips,
    array_agg(
        DISTINCT(useragent)
        ORDER BY useragent
    ) AS useragents
FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail"
WHERE eventname <> 'AssumeRole'
    AND eventname NOT LIKE 'Get%'
    AND eventname NOT LIKE 'List%'
```

```
Starting Ransomware Security Event Simulation: Phase 4 of 5...
---
Continuing Ransomware Security Event Simulation: Phase 4 of 5....
Continuing Ransomware Security Event Simulation: Phase 4 of 5.....
Continuing Ransomware Security Event Simulation: Phase 4 of 5......
Continuing Ransomware Security Event Simulation: Phase 4 of 5.......
Continuing Ransomware Security Event Simulation: Phase 4 of 5........
---
Ransomware Security Event Simulation: Phase 4 of 5 - complete.
---
Starting Ransomware Security Event Simulation: Phase 5 of 5...
---
Ransomware Security Event Simulation: Phase 5 of 5 - complete.
---
End of Simulation

*************************************************************************
*   SCENARIO: A strange Amazon S3 bucket has appeared in your AWS account.  *
*   Upon further investigation, the S3 bucket contains what appears to be  *
*   a ransom note!                                                         *
*                                                                          *
*   Use your AWS skills to determine the scope of any unauthorized use     *
*   and discover what data has been taken, and what data has been deleted. *
*                                                                          *
*   There are questions at the beginning of each 'Detection' section of    *
*   this workshop that can be used to prompt your investigation if you get *
*   stuck.  The end of each 'Detection' section will have hints and a      *
*   walkthrough to help provide answers to the questions.                  *
*                                                                          *
*   Good luck!                                                             *
*                                                                          *
*************************************************************************
[cloudshell-user@ip-10-130-85-187 ~]$
```

Next, an unusual S3 Bucket with the name of "we-stole-ur-data-*" should appear now in AWS S3 with the help of the CloudFormation template. Search the new AWS S3 Bucket to look for the "CreateBucket" API Call within the CloudTrail Logs.



Storage lens provides visibility into storage usage and activity trends. Learn more

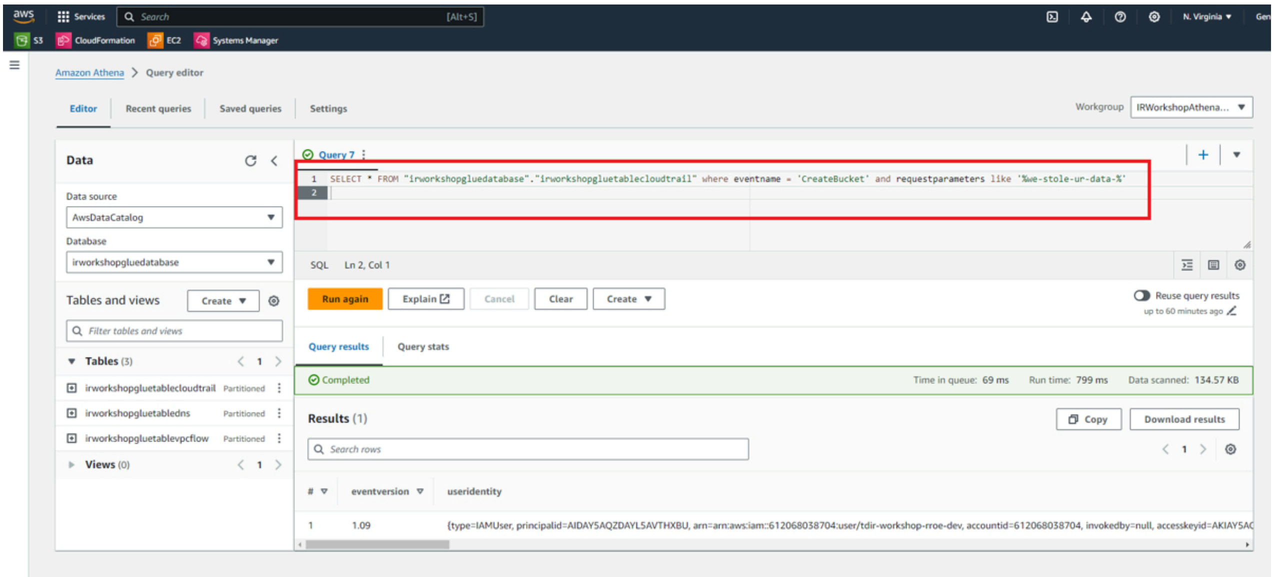
General purpose buckets (11) Info

Buckets are containers for data stored in S3. Learn more

stole — 1 match

Name	AWS Region	Access	Creation date
we-stole-ur-data-09e22438-7c81-4575-acbc-52b2daf7edbd	US East (N. Virginia) us-east-1	Bucket and objects not public	February 3, 2024, 18:52:12 (UTC-06:00)

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



Workgroup: IRWorkshopAthena...

Data source: AwsDataCatalog

Database: irworkshopgluedatabase

- irworkshopgluetablecloudtrail Partitioned
- irworkshopgluetabledns Partitioned
- irworkshopgluetablevpcflow Partitioned

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'CreateBucket' and requestparameters like '%we-stole-ur-data-%'
```

SQL Ln 2, Col 1

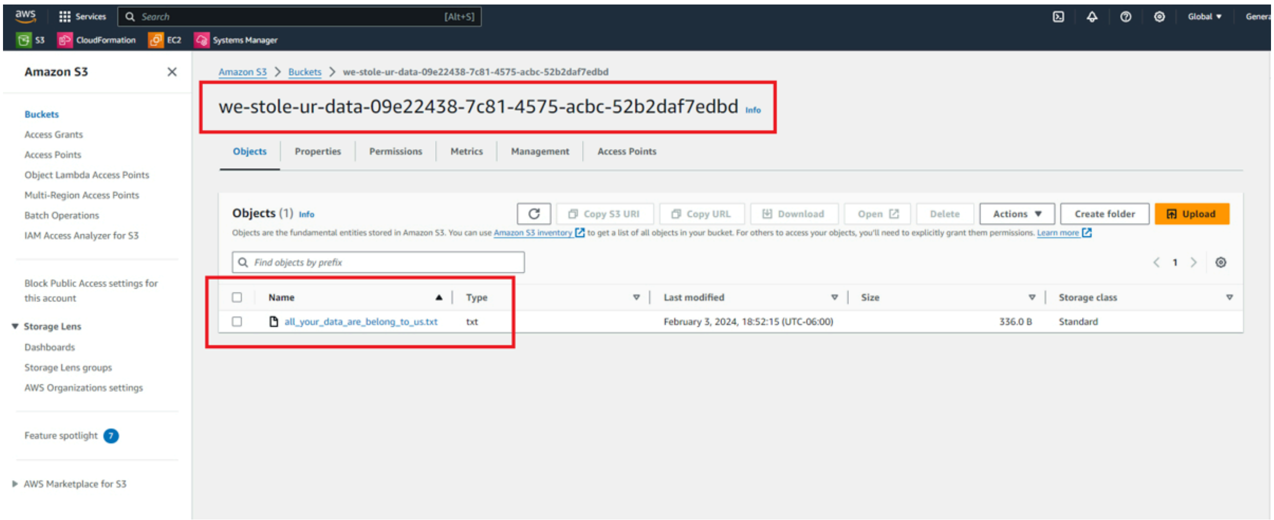
Reuse query results up to 60 minutes ago

Completed Time in queue: 69 ms Run time: 799 ms Data scanned: 134.57 KB

Results (1)

#	eventversion	useridentity
1	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYL5AVTHXBU, arn=arn:aws:iam::612068038704:user/tdir-workshop-rroe-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5AC

Next, check the AWS S3 Bucket for objects and realize that there is a "all_your_data_are_belong_to_us.txt" file in the new malicious AWS S3 Bucket. After investigating it is realized that the "PutObject" API call was not recorded due to either no Server access logging or data events recorded in the CloudTrail configuration.



Amazon S3 > Buckets > we-stole-ur-data-09e22438-7c81-4575-acbc-52b2daf7edbd

we-stole-ur-data-09e22438-7c81-4575-acbc-52b2daf7edbd

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
all_your_data_are_belong_to_us.txt	txt	February 3, 2024, 18:52:15 (UTC-06:00)	336.0 B	Standard

"all_your_data_are_belong_to_us.txt" Text file:

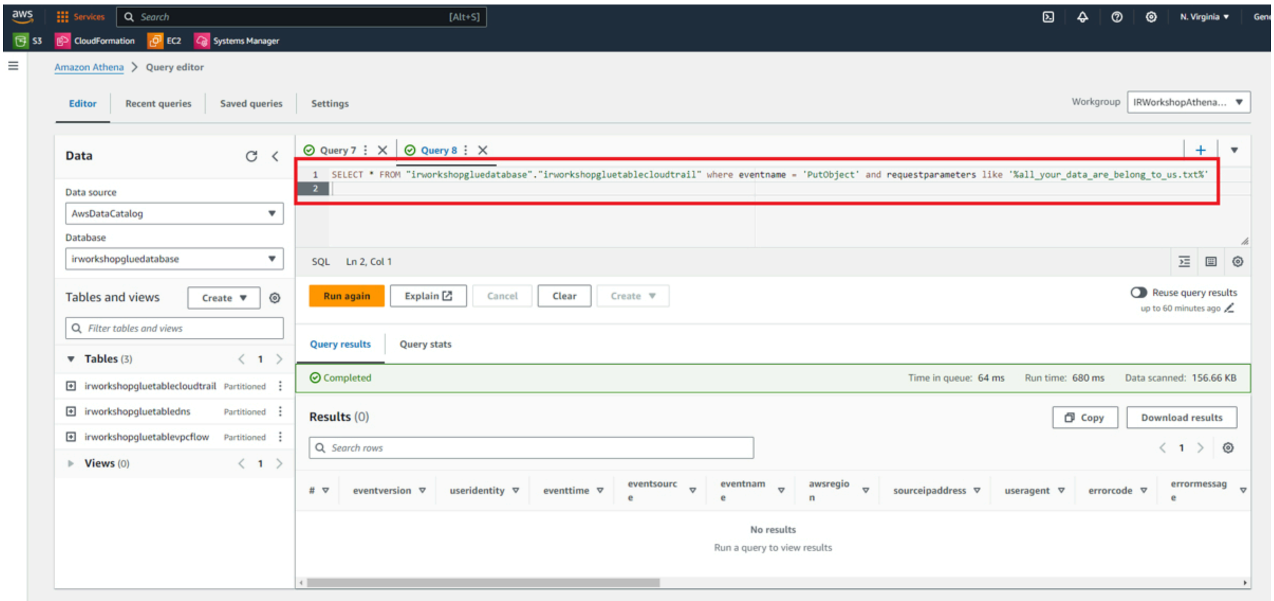
~~~
```
We have deleted all your files and have taken your customer data includin

Pay us 100 BILLION DOLLARS in bitcoin within 48 hours and we will return


BTC Wallet address: <>
```
~~~

Search for PutObject API call in CloudTrail:

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



Amazon Athena > Query editor

Workgroup: IRWorkshopAthena...

Data source: AwsDataCatalog

Database: irworkshopgluedatabase

Tables (3): irworkshopgluetablecloudtrail, irworkshopgluetabledns, irworkshopgluetablevpcflow

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'PutObject' and requestparameters like '%all_your_data_are_belong_to_us.txt%'
```

Completed — Time in queue: 64 ms Run time: 680 ms Data scanned: 156.66 KB

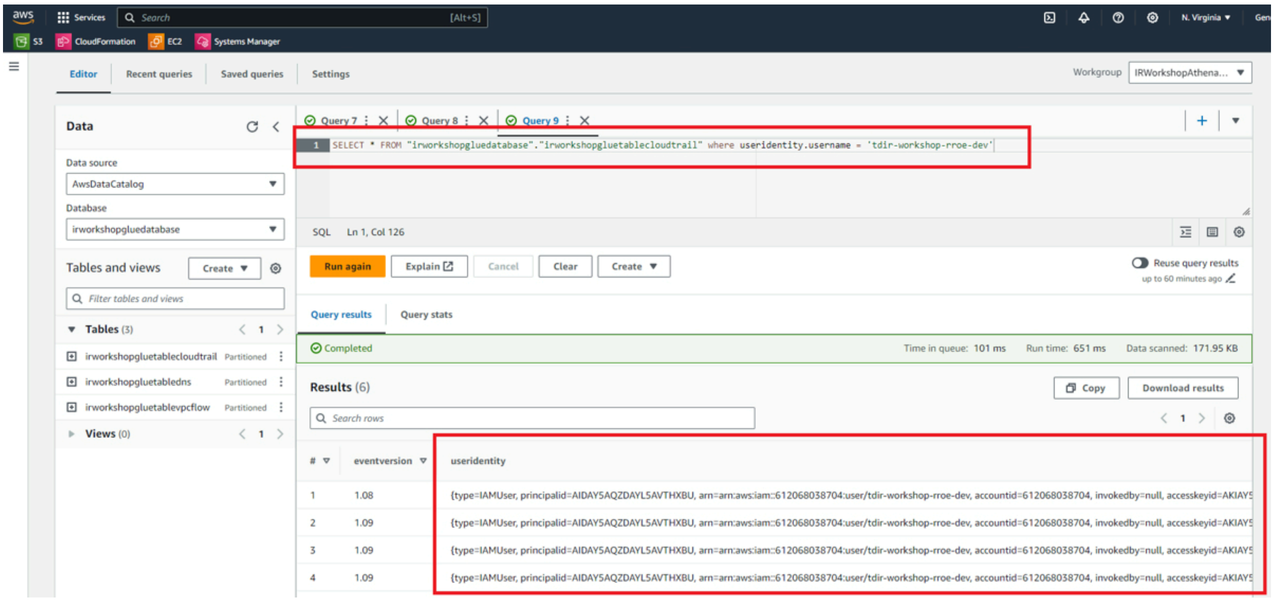
Results (0)

No results

Run a query to view results

Next, Investigate the user "tdir-workshop-rroe-dev" that initiated the "CreateBucket" API call and review the actions performed by the IAM user inside the associated AWS account.

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



Data source: AwsDataCatalog

Database: irworkshopgluedatabase

Tables (3): irworkshopgluetablecloudtrail, irworkshopgluetabledns, irworkshopgluetablevpcflow

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.username = 'tdir-workshop-rroe-dev'
```

SQL Ln 1, Col 126

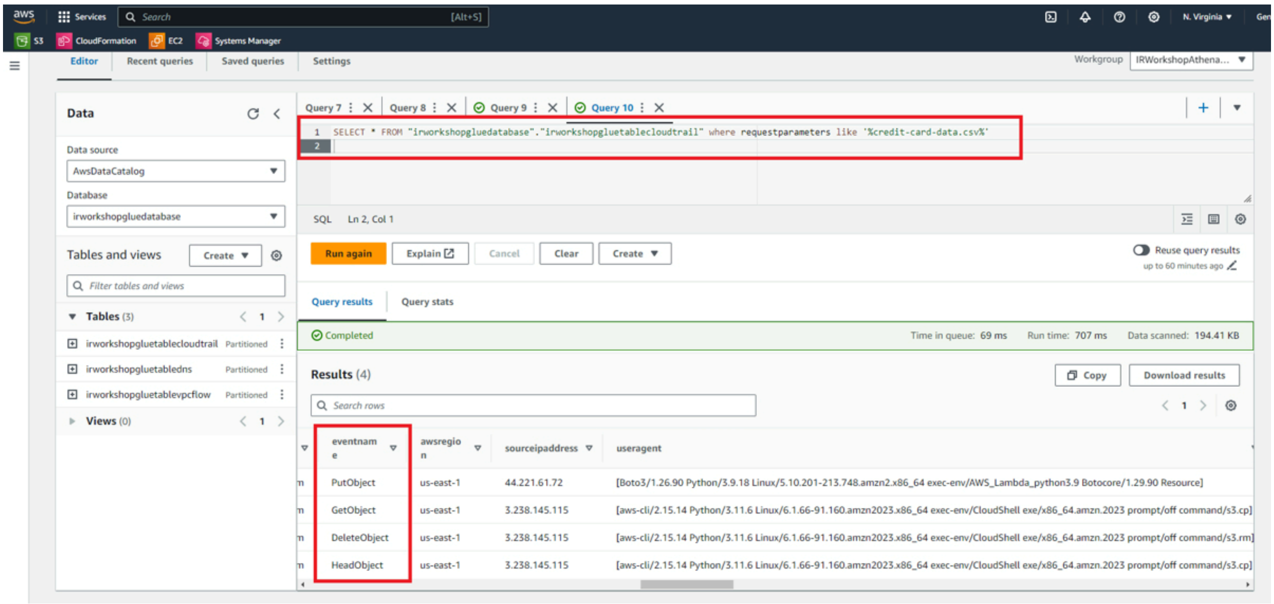
Completed Time in queue: 101 ms Run time: 651 ms Data scanned: 171.95 KB

Results (6)

#	eventversion	useridentity
1	1.08	{type=IAMUser, principalid=AIDAY5AQZDAYL5AVTHXBU, arn=arn:aws:iam::612068038704:user/tdir-workshop-rroe-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
2	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYL5AVTHXBU, arn=arn:aws:iam::612068038704:user/tdir-workshop-rroe-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
3	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYL5AVTHXBU, arn=arn:aws:iam::612068038704:user/tdir-workshop-rroe-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
4	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYL5AVTHXBU, arn=arn:aws:iam::612068038704:user/tdir-workshop-rroe-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5

Create a query to look for the "credit-card-data.csv" taken by the Ransomware attacks and invesigate their actions accordingly using CloudTrail and notice that successful "GetObject", "HeadObject" and "DeleteObject" API calls made.

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



Data source: AwsDataCatalog

Database: irworkshopgluedatabase

Tables (3): irworkshopgluetablecloudtrail, irworkshopgluetabledns, irworkshopgluetablevpcflow

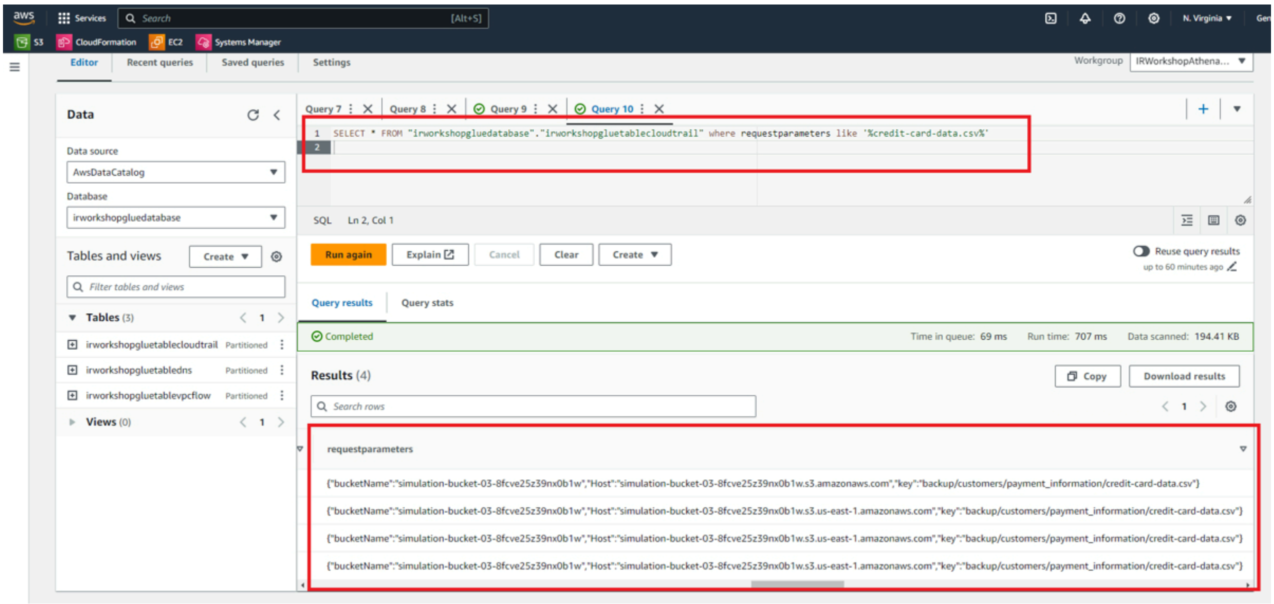
```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where requestparameters like '%credit-card-data.csv%'
```

SQL Ln 2, Col 1

Completed Time in queue: 69 ms Run time: 707 ms Data scanned: 194.41 KB

Results (4)

eventname	awsregion	sourceipaddress	useragent
PutObject	us-east-1	44.221.61.72	[Boto3/1.26.90 Python/3.9.18 Linux/5.10.201-213.748.amzn2.x86_64 exec-env/AWS_Lambda_python3.9 Botocore/1.29.90 Resource]
GetObject	us-east-1	3.238.145.115	[aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CloudShell exe/x86_64.amzn.2023 prompt/off command/s3.cp]
DeleteObject	us-east-1	3.238.145.115	[aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CloudShell exe/x86_64.amzn.2023 prompt/off command/s3.rm]
HeadObject	us-east-1	3.238.145.115	[aws-cli/2.15.14 Python/3.11.6 Linux/6.1.66-91.160.amzn2023.x86_64 exec-env/CloudShell exe/x86_64.amzn.2023 prompt/off command/s3.cp]



Data source: AwsDataCatalog

Database: irworkshopgluedatabase

Tables and views

Tables (3)

- irworkshopgluetablecloudtrail Partitioned
- irworkshopgluetabledns Partitioned
- irworkshopgluetablevpcflow Partitioned

Views (0)

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where requestparameters like '%credit-card-data.csv%'
```

SQL Ln 2, Col 1

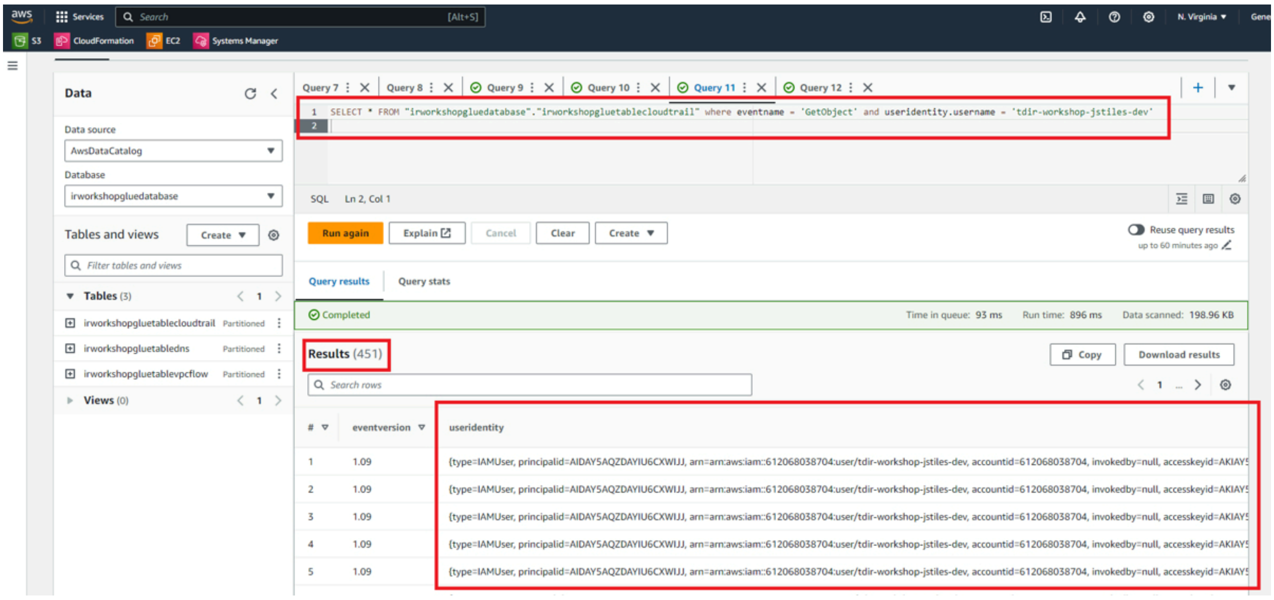
Completed Time in queue: 69 ms Run time: 707 ms Data scanned: 194.41 KB

Results (4)

```
requestparameters
{"bucketName":"simulation-bucket-03-8fcve25z39nx0b1w","Host":"simulation-bucket-03-8fcve25z39nx0b1w.s3.amazonaws.com","key":"backup/customers/payment_information/credit-card-data.csv"}
{"bucketName":"simulation-bucket-03-8fcve25z39nx0b1w","Host":"simulation-bucket-03-8fcve25z39nx0b1w.s3.us-east-1.amazonaws.com","key":"backup/customers/payment_information/credit-card-data.csv"}
{"bucketName":"simulation-bucket-03-8fcve25z39nx0b1w","Host":"simulation-bucket-03-8fcve25z39nx0b1w.s3.us-east-1.amazonaws.com","key":"backup/customers/payment_information/credit-card-data.csv"}
{"bucketName":"simulation-bucket-03-8fcve25z39nx0b1w","Host":"simulation-bucket-03-8fcve25z39nx0b1w.s3.us-east-1.amazonaws.com","key":"backup/customers/payment_information/credit-card-data.csv"}
```

While investigating, AWS IAM user "tdir-workshop-jstiles-dev" appears as a new IAM user to investigate that manipulated "credit-card-data.csv". Create a new query that searches new AWS IAM user "tdir-workshop-jstiles-dev" that details what other API calls were made.

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



Data source: AwsDataCatalog

Database: irworkshopgluedatabase

Tables and views

Tables (3)

- irworkshopgluetablecloudtrail Partitioned
- irworkshopgluetabledns Partitioned
- irworkshopgluetablevpcflow Partitioned

Views (0)

```
SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'GetObject' and useridentity.username = 'tdir-workshop-jstiles-dev'
```

SQL Ln 2, Col 1

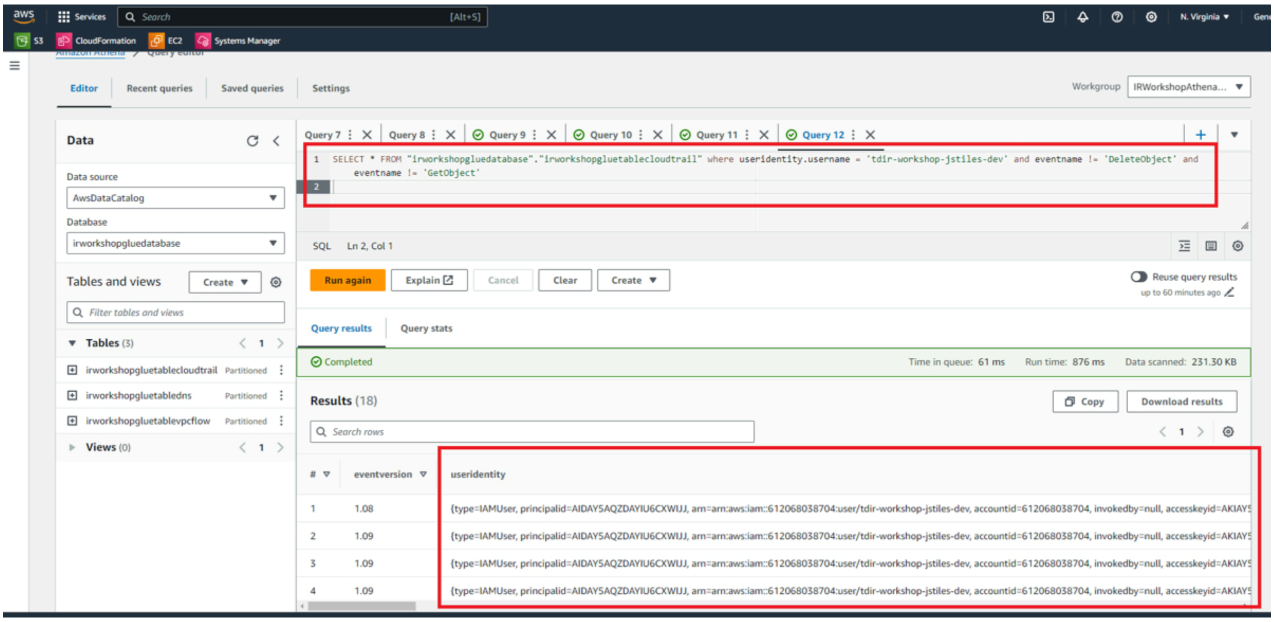
Completed Time in queue: 93 ms Run time: 896 ms Data scanned: 198.96 KB

Results (451)

```
#   eventversion   useridentity
1   1.09           {type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
2   1.09           {type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
3   1.09           {type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
4   1.09           {type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
5   1.09           {type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY
```

Notice that there are 451 CloudTrial API calls made by IAM user "tdir-workshop-jstiles-dev" in the above query mostly attributed to "GetObject" and "DeleteObject" API calls in CloudTrail. Create another AWS Athena query that excludes "GetObject" and "DeleteObject" in order to get additional information on the actions performed by the attacker IAM user "tdir-workshop-jstiles-dev".

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

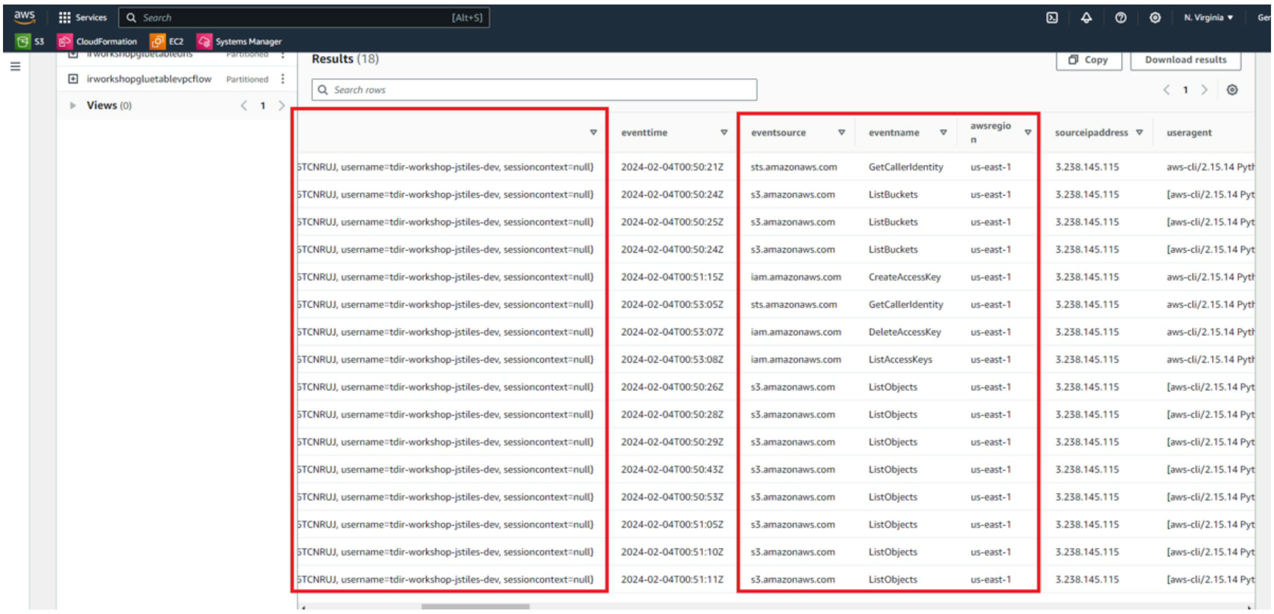


```
1  SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.username = 'tdir-workshop-jstiles-dev' and eventname != 'DeleteObject' and
     eventname != 'GetObject'
2
```

Completed Time in queue: 61 ms Run time: 876 ms Data scanned: 231.30 KB

Results (18)

#	eventversion	useridentity
1	1.08	{type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
2	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
3	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5
4	1.09	{type=IAMUser, principalid=AIDAY5AQZDAYIU6CXWIJJ, arn=arn:aws:iam::612068038704:user/tdir-workshop-jstiles-dev, accountid=612068038704, invokedby=null, accesskeyid=AKIAY5

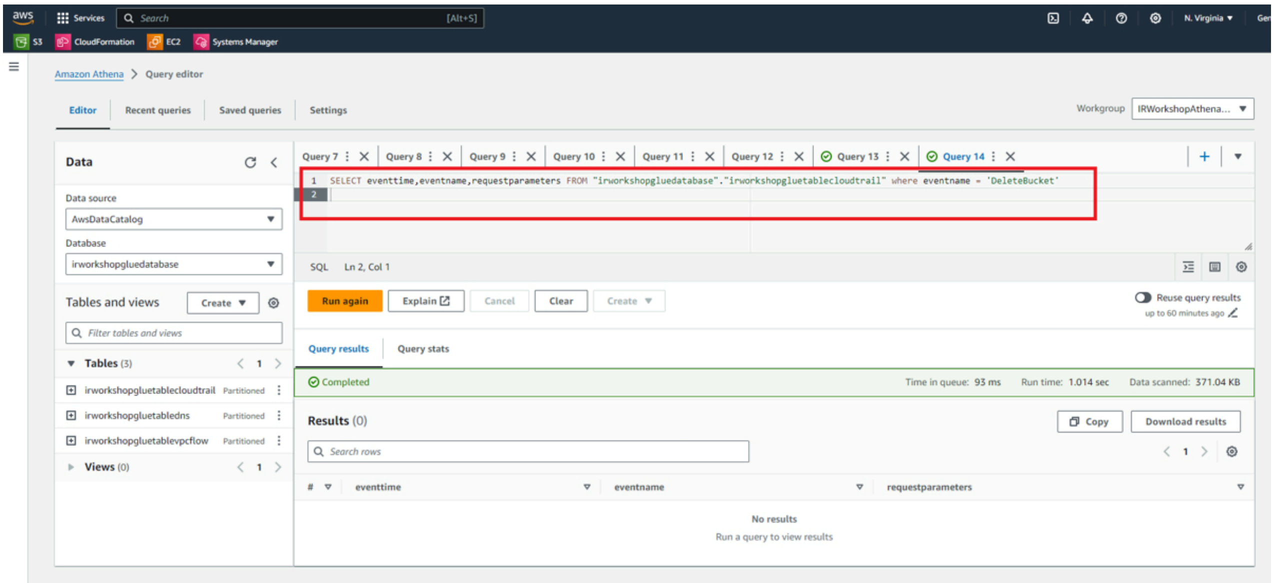


Results (18)

	eventtime	eventsource	eventname	awsregion	sourceipaddress	useragent
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:21Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	3.238.145.115	aws-cli/2.15.14 Pyth
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:24Z	s3.amazonaws.com	ListBuckets	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:25Z	s3.amazonaws.com	ListBuckets	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:24Z	s3.amazonaws.com	ListBuckets	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:51:15Z	iam.amazonaws.com	CreateAccessKey	us-east-1	3.238.145.115	aws-cli/2.15.14 Pyth
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:53:05Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	3.238.145.115	aws-cli/2.15.14 Pyth
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:53:07Z	iam.amazonaws.com	DeleteAccessKey	us-east-1	3.238.145.115	aws-cli/2.15.14 Pyth
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:53:08Z	iam.amazonaws.com	ListAccessKeys	us-east-1	3.238.145.115	aws-cli/2.15.14 Pyth
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:26Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:28Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:29Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:43Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:50:53Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:51:05Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:51:10Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt
5TCNRUJ, username=tdir-workshop-jstiles-dev, sessioncontext=null}	2024-02-04T00:51:11Z	s3.amazonaws.com	ListObjects	us-east-1	3.238.145.115	[aws-cli/2.15.14 Pyt

Additionally, search for any bucket deletions inside the AWS Account to investigate further on the actions performed by unknown or abnormal AWS IAM users.

```
SELECT eventtime,eventname,requestparameters FROM "irworkshopgluedatabase
```



```
SELECT eventtime,eventname,requestparameters FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'DeleteBucket'
```

Completed Time in queue: 93 ms Run time: 1.014 sec Data scanned: 371.04 KB

Results (0)

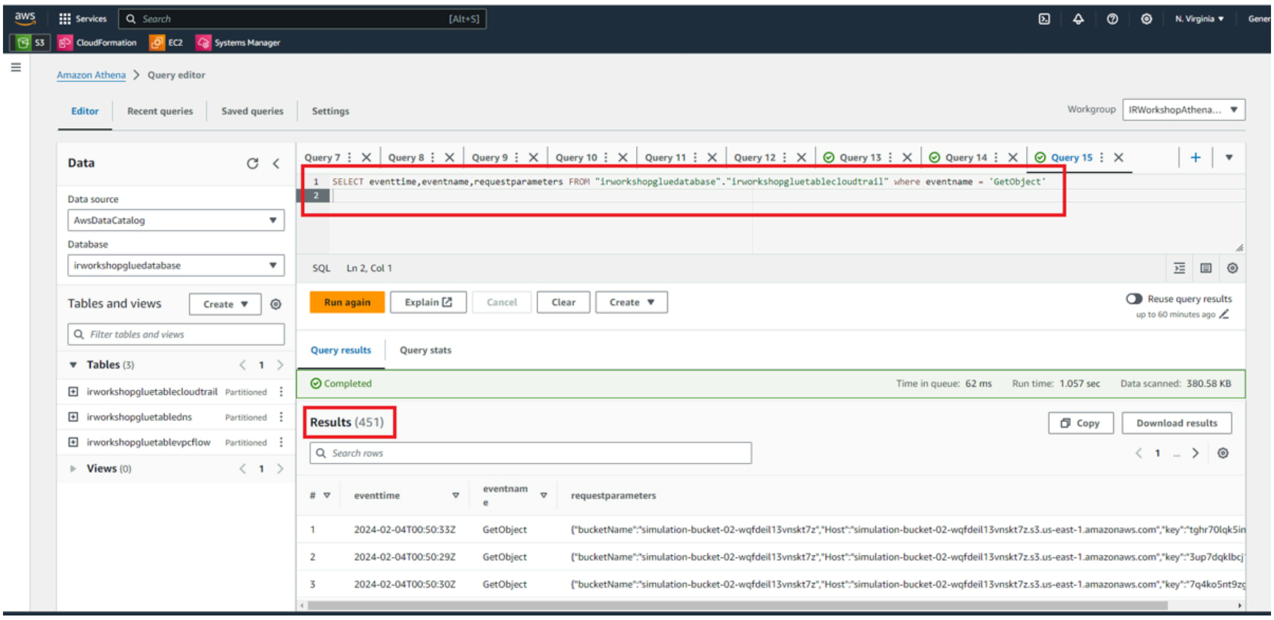
#	eventtime	eventname	requestparameters

No results

Run a query to view results

Furthermore, check to see whether objects were recieved using the "GetObject" API call within the AWS account. Notice in the results the "simulation-bucket-02-*" returned a lot of results for downloaded objects.

```
SELECT eventtime,eventname,requestparameters FROM "irworkshopgluedatabase
```



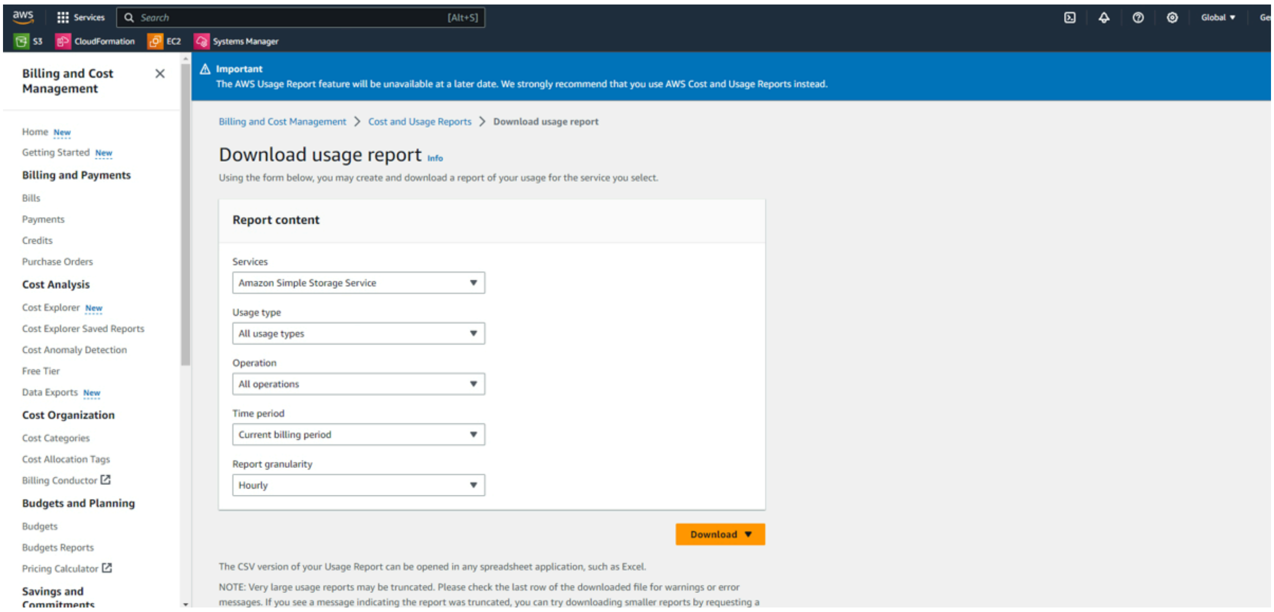
```
SELECT eventtime,eventname,requestparameters FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'GetObject'
```

Completed Time in queue: 62 ms Run time: 1.057 sec Data scanned: 380.58 KB

Results (451)

#	eventtime	eventname	requestparameters
1	2024-02-04T00:50:33Z	GetObject	{"bucketName":"simulation-bucket-02-wqfdeil13vnskt7z","Host":"simulation-bucket-02-wqfdeil13vnskt7z.s3.us-east-1.amazonaws.com","key":"tghr70lqk5in
2	2024-02-04T00:50:29Z	GetObject	{"bucketName":"simulation-bucket-02-wqfdeil13vnskt7z","Host":"simulation-bucket-02-wqfdeil13vnskt7z.s3.us-east-1.amazonaws.com","key":"3up7dqklbcj
3	2024-02-04T00:50:30Z	GetObject	{"bucketName":"simulation-bucket-02-wqfdeil13vnskt7z","Host":"simulation-bucket-02-wqfdeil13vnskt7z.s3.us-east-1.amazonaws.com","key":"7q4ko5nt9zg

Given the previous AWS Athena S3 activity results point to a lot of downloaded objects from S3 Buckets the next best course of action would be use the AWS Management Console and check the Cost & Usage Report concerning S3. From the Cost & Usage reports section under Billing download a Usage report AWS S3 that details in a CSV Report data exfiltration and deletion.



Important
The AWS Usage Report feature will be unavailable at a later date. We strongly recommend that you use AWS Cost and Usage Reports instead.

Billing and Cost Management > Cost and Usage Reports > Download usage report

Download usage report Info

Using the form below, you may create and download a report of your usage for the service you select.

Report content

Services: Amazon Simple Storage Service

Usage type: All usage types

Operation: All operations

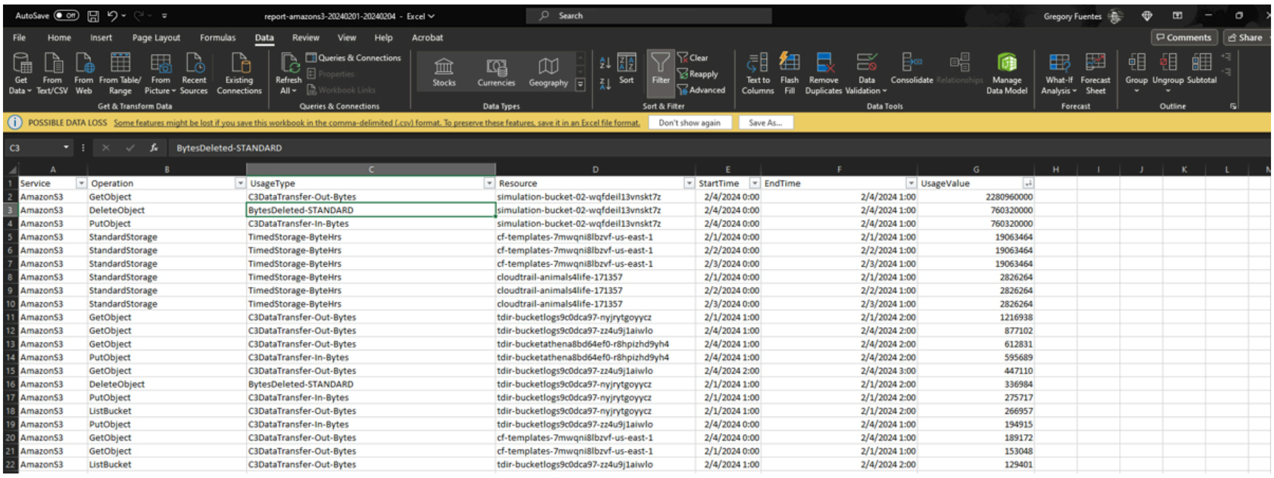
Time period: Current billing period

Report granularity: Hourly

Download ▼

The CSV version of your Usage Report can be opened in any spreadsheet application, such as Excel.

NOTE: Very large usage reports may be truncated. Please check the last row of the downloaded file for warnings or error messages. If you see a message indicating the report was truncated, you can try downloading smaller reports by requesting a

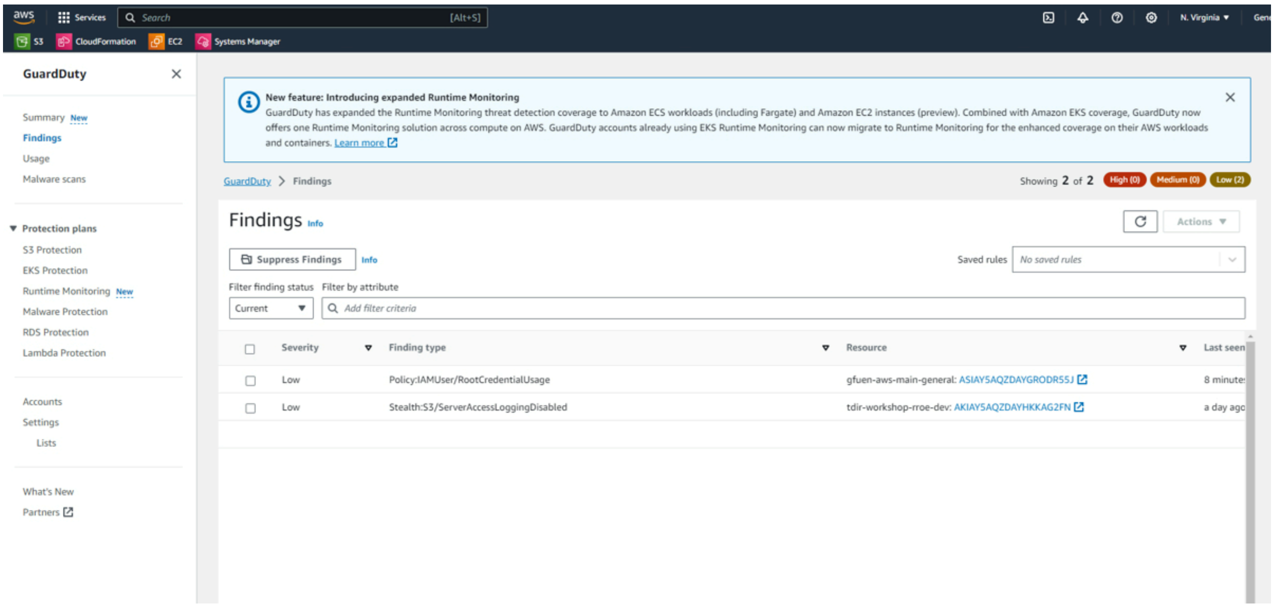


POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. Don't show again Save As...

C3 BytesDeleted-STANDARD

	A	B	C	D	E	F	G
1	Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
2	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	simulation-bucket-02-wqfdeil13vnskt7z	2/4/2024 0:00	2/4/2024 1:00	2280960000
3	AmazonS3	DeleteObject	BytesDeleted-STANDARD	simulation-bucket-02-wqfdeil13vnskt7z	2/4/2024 0:00	2/4/2024 1:00	760320000
4	AmazonS3	PutObject	C3DataTransfer-In-Bytes	simulation-bucket-02-wqfdeil13vnskt7z	2/4/2024 0:00	2/4/2024 1:00	760320000
5	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cf-templates-7mwqni8lbzvf-us-east-1	2/1/2024 0:00	2/1/2024 1:00	19063464
6	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cf-templates-7mwqni8lbzvf-us-east-1	2/2/2024 0:00	2/2/2024 1:00	19063464
7	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cf-templates-7mwqni8lbzvf-us-east-1	2/3/2024 0:00	2/3/2024 1:00	19063464
8	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cloudtrail-animals4life-171357	2/1/2024 0:00	2/1/2024 1:00	2826264
9	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cloudtrail-animals4life-171357	2/2/2024 0:00	2/2/2024 1:00	2826264
10	AmazonS3	StandardStorage	TimedStorage-ByteHrs	cloudtrail-animals4life-171357	2/3/2024 0:00	2/3/2024 1:00	2826264
11	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	tdir-bucketlogs9c0dca97-nyjrytgoyycz	2/1/2024 1:00	2/1/2024 2:00	1216938
12	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	tdir-bucketlogs9c0dca97-zz4u9j1aiwlo	2/4/2024 1:00	2/4/2024 2:00	877102
13	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	tdir-bucketathena8bd64ef0-r8hpizhd9yh4	2/4/2024 1:00	2/4/2024 2:00	612831
14	AmazonS3	PutObject	C3DataTransfer-In-Bytes	tdir-bucketathena8bd64ef0-r8hpizhd9yh4	2/4/2024 1:00	2/4/2024 2:00	595689
15	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	tdir-bucketlogs9c0dca97-zz4u9j1aiwlo	2/4/2024 2:00	2/4/2024 3:00	447110
16	AmazonS3	DeleteObject	BytesDeleted-STANDARD	tdir-bucketlogs9c0dca97-nyjrytgoyycz	2/1/2024 1:00	2/1/2024 2:00	336984
17	AmazonS3	PutObject	C3DataTransfer-In-Bytes	tdir-bucketlogs9c0dca97-nyjrytgoyycz	2/1/2024 1:00	2/1/2024 2:00	275717
18	AmazonS3	ListBucket	C3DataTransfer-Out-Bytes	tdir-bucketlogs9c0dca97-nyjrytgoyycz	2/1/2024 1:00	2/1/2024 2:00	266957
19	AmazonS3	PutObject	C3DataTransfer-In-Bytes	tdir-bucketlogs9c0dca97-zz4u9j1aiwlo	2/4/2024 0:00	2/4/2024 1:00	194915
20	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	cf-templates-7mwqni8lbzvf-us-east-1	2/4/2024 0:00	2/4/2024 1:00	189172
21	AmazonS3	GetObject	C3DataTransfer-Out-Bytes	cf-templates-7mwqni8lbzvf-us-east-1	2/1/2024 0:00	2/1/2024 1:00	153048
22	AmazonS3	ListBucket	C3DataTransfer-Out-Bytes	tdir-bucketlogs9c0dca97-zz4u9j1aiwlo	2/4/2024 1:00	2/4/2024 2:00	129401

Next, time to check AWS GuardDuty and the findings associated with the AWS account. Notice that there is a finding for "Stealth:S3/ServerAccessLoggingDisabled" with the IAM user "tdirworkshop-rroe-dev" involved in the offending AWS S3 event.



New feature: Introducing expanded Runtime Monitoring
GuardDuty has expanded the Runtime Monitoring threat detection coverage to Amazon ECS workloads (including Fargate) and Amazon EC2 instances (preview). Combined with Amazon EKS coverage, GuardDuty now offers one Runtime Monitoring solution across compute on AWS. GuardDuty accounts already using EKS Runtime Monitoring can now migrate to Runtime Monitoring for the enhanced coverage on their AWS workloads and containers. Learn more

GuardDuty > Findings

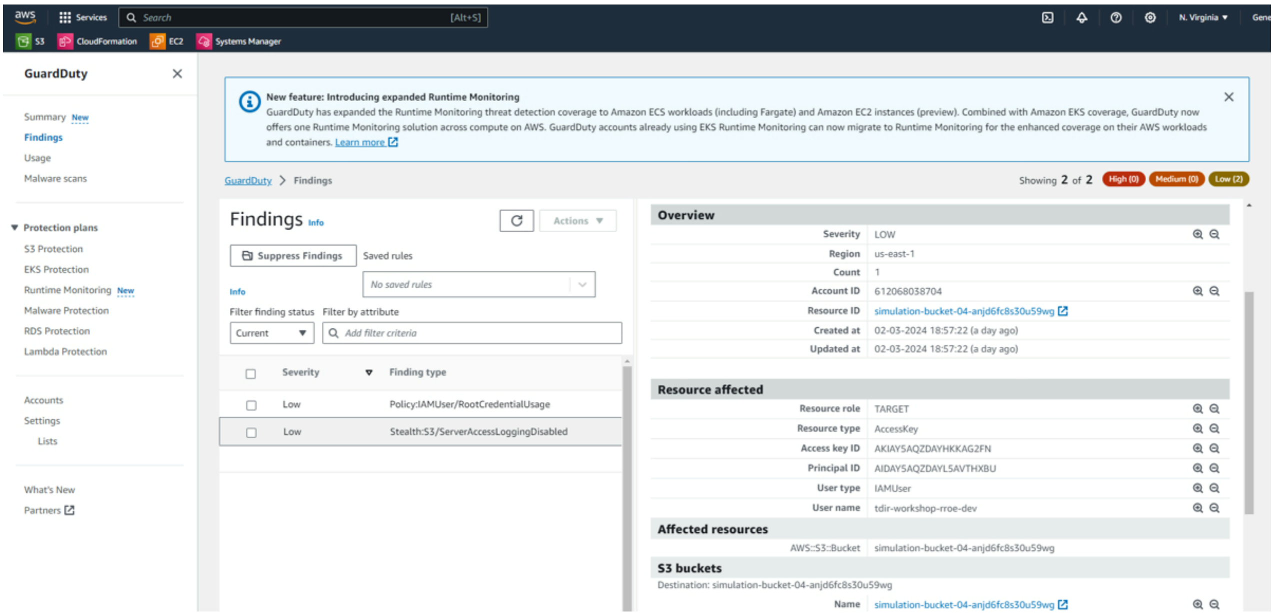
Showing 2 of 2 High (0) Medium (0) Low (2)

Findings Info

Saved rules: No saved rules

Filter finding status: Current ▾ Filter by attribute: Add filter criteria

□	Severity	Finding type	Resource	Last seen
□	Low	Policy:IAMUser/RootCredentialUsage	gfuen-aws-main-general: ASIAY5AQZDAYGRODR55J	8 minute
□	Low	Stealth:S3/ServerAccessLoggingDisabled	tdir-workshop-rroe-dev: AKIAY5AQZDAYHKKAG2FN	a day ago



New feature: Introducing expanded Runtime Monitoring
GuardDuty has expanded the Runtime Monitoring threat detection coverage to Amazon ECS workloads (including Fargate) and Amazon EC2 instances (preview). Combined with Amazon EKS coverage, GuardDuty now offers one Runtime Monitoring solution across compute on AWS. GuardDuty accounts already using EKS Runtime Monitoring can now migrate to Runtime Monitoring for the enhanced coverage on their AWS workloads and containers. Learn more

GuardDuty > Findings

Showing 2 of 2 High (0) Medium (0) Low (2)

Findings Info

Saved rules: No saved rules

Filter finding status: Current ▾ Filter by attribute: Add filter criteria

□	Severity	Finding type
□	Low	Policy:IAMUser/RootCredentialUsage
□	Low	Stealth:S3/ServerAccessLoggingDisabled

Overview

Severity	LOW
Region	us-east-1
Count	1
Account ID	612068038704
Resource ID	simulation-bucket-04-anjd6fc8s30u59wg
Created at	02-03-2024 18:57:22 (a day ago)
Updated at	02-03-2024 18:57:22 (a day ago)

Resource affected

Resource role	TARGET
Resource type	AccessKey
Access key ID	AKIAY5AQZDAYHKKAG2FN
Principal ID	AIDAY5AQZDAYL5AVTHXBU
User type	IAMUser
User name	tdir-workshop-rroe-dev

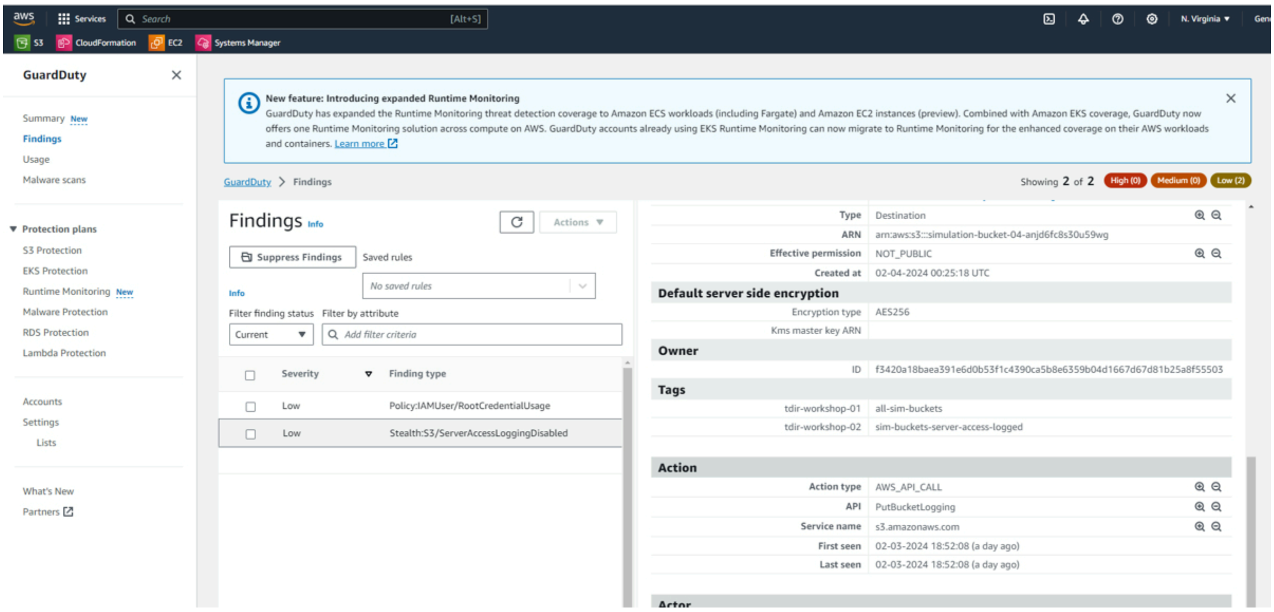
Affected resources

AWS::S3::Bucket	simulation-bucket-04-anjd6fc8s30u59wg

S3 buckets

Destination: simulation-bucket-04-anjd6fc8s30u59wg

Name	simulation-bucket-04-anjd6fc8s30u59wg



New feature: Introducing expanded Runtime Monitoring
GuardDuty has expanded the Runtime Monitoring threat detection coverage to Amazon ECS workloads (including Fargate) and Amazon EC2 instances (preview). Combined with Amazon EKS coverage, GuardDuty now offers one Runtime Monitoring solution across compute on AWS. GuardDuty accounts already using EKS Runtime Monitoring can now migrate to Runtime Monitoring for the enhanced coverage on their AWS workloads and containers. Learn more

GuardDuty > Findings

Showing 2 of 2 High (0) Medium (0) Low (2)

Findings Info

Saved rules: No saved rules

Filter finding status: Current ▾ Filter by attribute: Add filter criteria

□	Severity	Finding type
□	Low	Policy:IAMUser/RootCredentialUsage
□	Low	Stealth:S3/ServerAccessLoggingDisabled

Type	Destination
ARN	arn:aws:s3:::simulation-bucket-04-anjd6fc8s30u59wg
Effective permission	NOT_PUBLIC
Created at	02-04-2024 00:25:18 UTC

Default server side encryption

Encryption type	AES256
Kms master key ARN	

Owner

ID	f3420a18baea391e6d0b53f1c4390ca5b8e6359b04d1667d67d81b25a8f55503

Tags

tdir-workshop-01	all-sim-buckets
tdir-workshop-02	sim-buckets-server-access-logged

Action

Action type	AWS_API_CALL
API	PutBucketLogging
Service name	s3.amazonaws.com
First seen	02-03-2024 18:52:08 (a day ago)
Last seen	02-03-2024 18:52:08 (a day ago)

Actor