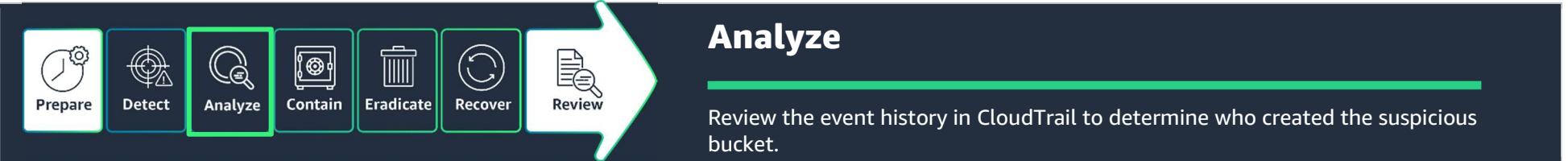


AWS Security Incident Response - Ransomware Job Aid

AWS Security Incident Response - Ransomware Job Aid					
Step	Content	Visual			
Step 1:	<p>Let's navigate to our S3 buckets and see if we can find the suspicious bucket.</p> <p>From the AWS Management Console:</p> <ol style="list-style-type: none">1. In the field search field enter S3.2. Under Services, choose S3.	<p>Detect</p> <p>Use the S3 Console to identify the suspicious bucket.</p> 			



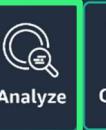
Steps	Content	Visual												
Step 2:	<p>The Amazon S3 page displays.</p> <p>Scroll down to the Buckets section, and locate the bucket, <code>we-stole-ur-data-*</code>. This confirms the bucket exists and we should investigate further.</p> <p>Next, we will use AWS CloudTrail to determine who created the suspicious bucket.</p>	<table border="1"> <thead> <tr> <th>Name</th> <th>AWS Region</th> <th>Access</th> <th>Created</th> </tr> </thead> <tbody> <tr> <td>tdir-bucketlogs9c0dca97-yk54xw4ppht8</td> <td>US East (N. Virginia) us-east-1</td> <td>not public</td> <td>June</td> </tr> <tr> <td>we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740</td> <td>US East (N. Virginia) us-east-1</td> <td>Bucket and objects not public</td> <td>June</td> </tr> </tbody> </table>	Name	AWS Region	Access	Created	tdir-bucketlogs9c0dca97-yk54xw4ppht8	US East (N. Virginia) us-east-1	not public	June	we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	US East (N. Virginia) us-east-1	Bucket and objects not public	June
Name	AWS Region	Access	Created											
tdir-bucketlogs9c0dca97-yk54xw4ppht8	US East (N. Virginia) us-east-1	not public	June											
we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	US East (N. Virginia) us-east-1	Bucket and objects not public	June											



Steps	Content	Visual
Step 1:	<p>Let's navigate to CloudTrail to determine who created the suspicious bucket.</p> <p>From the AWS Management Console:</p> <ol style="list-style-type: none"> 1. In the search field, enter CloudTrail. 2. Under Services, choose CloudTrail. 	
Step 2:	<p>The CloudTrail dashboard displays. To view the Event history in CloudTrail, choose Event history.</p>	



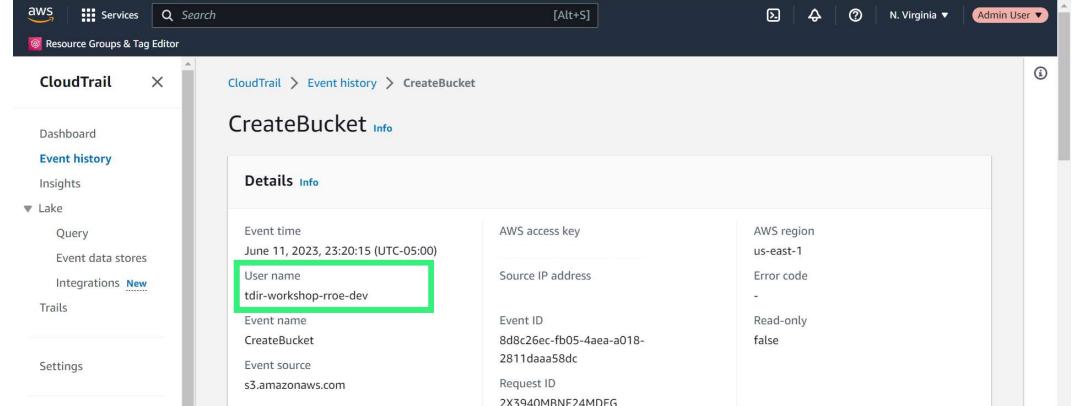
Steps	Content	Visual																																
Step 3:	<p>The Event history page displays. Under Lookup attributes, go to the first drop-down menu and choose Event name.</p> <p>Then, in the second field, enter CreateBucket.</p>	<p>Event history (9) Info</p> <table border="1"> <thead> <tr> <th>Event name</th> <th>Event time</th> <th>User name</th> <th>Event source</th> </tr> </thead> <tbody> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:20:15 (UTC-0...)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:09:28 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:59 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:52 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:36 (UTC-0...)</td> <td>TDIR-SimBuckets02-wLK0...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>Event source</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Read-only</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Event name	Event time	User name	Event source	CreateBucket	June 11, 2023, 23:20:15 (UTC-0...)	tdir-workshop-rroe-dev	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:09:28 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:59 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:52 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:36 (UTC-0...)	TDIR-SimBuckets02-wLK0...	s3.amazonaws.com	Event source				Read-only			
Event name	Event time	User name	Event source																															
CreateBucket	June 11, 2023, 23:20:15 (UTC-0...)	tdir-workshop-rroe-dev	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:09:28 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:59 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:52 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:36 (UTC-0...)	TDIR-SimBuckets02-wLK0...	s3.amazonaws.com																															
Event source																																		
Read-only																																		
Step 4:	<p>Notice a CreateBucket event appears. Let's determine if this event was where the we-stole-ur-data bucket was created. Choose CreateBucket.</p>	<p>Event history (9) Info</p> <table border="1"> <thead> <tr> <th>Event name</th> <th>Event time</th> <th>User name</th> <th>Event source</th> </tr> </thead> <tbody> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:20:15 (UTC-0...)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:09:28 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:59 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:52 (UTC-0...)</td> <td>TDIR-SimBuckets01-QMDIL...</td> <td>s3.amazonaws.com</td> </tr> <tr> <td>CreateBucket</td> <td>June 11, 2023, 23:08:36 (UTC-0...)</td> <td>TDIR-SimBuckets02-wLK0...</td> <td>s3.amazonaws.com</td> </tr> </tbody> </table>	Event name	Event time	User name	Event source	CreateBucket	June 11, 2023, 23:20:15 (UTC-0...)	tdir-workshop-rroe-dev	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:09:28 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:59 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:52 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com	CreateBucket	June 11, 2023, 23:08:36 (UTC-0...)	TDIR-SimBuckets02-wLK0...	s3.amazonaws.com								
Event name	Event time	User name	Event source																															
CreateBucket	June 11, 2023, 23:20:15 (UTC-0...)	tdir-workshop-rroe-dev	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:09:28 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:59 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:52 (UTC-0...)	TDIR-SimBuckets01-QMDIL...	s3.amazonaws.com																															
CreateBucket	June 11, 2023, 23:08:36 (UTC-0...)	TDIR-SimBuckets02-wLK0...	s3.amazonaws.com																															

 Prepare		 Detect	 Analyze	 Contain	 Eradicate	 Recover	 Review
Steps	Content						
Step 5:	<p>The CreateBucket Event history page displays. In the Details section, notice the username tdir-workshop-rroe-dev.</p>						
Step 6:	<p>Scroll down to the Event records section, and notice the CreateBucket parameter matches the suspicious bucket.</p> <p>This confirms that the tdir-workshop-rroe-dev was the user who created the new bucket.</p> <p>We identified the suspicious bucket and determined who created it. Next, we will find out what events the user performed and who created the bucket.</p>						

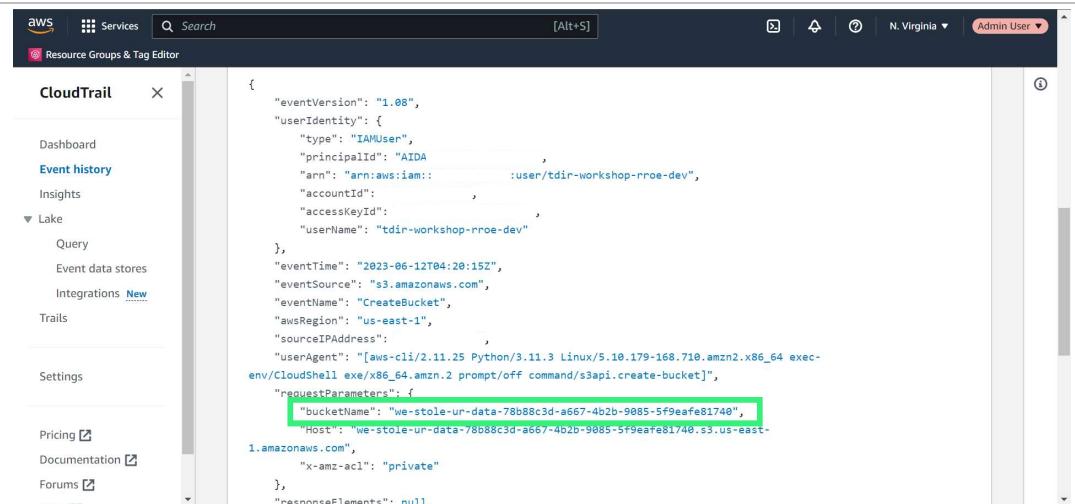
Analyze

Review the event history in CloudTrail to determine who created the suspicious bucket.

Visual



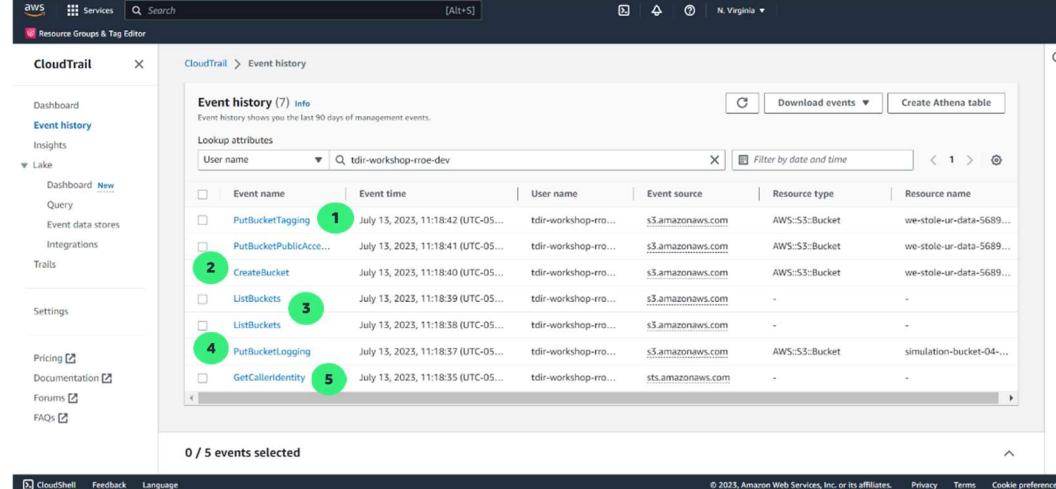
The screenshot shows the AWS CloudTrail Event history for a CreateBucket event. The 'Details' section is highlighted, showing the User name field which contains 'tdir-workshop-rroe-dev'. Other fields visible include Event time (June 11, 2023, 23:20:15 (UTC-05:00)), AWS access key, Source IP address, Event ID, Event source, Request ID, and AWS region (us-east-1). The 'Resources referenced (1)' section is also visible at the bottom.

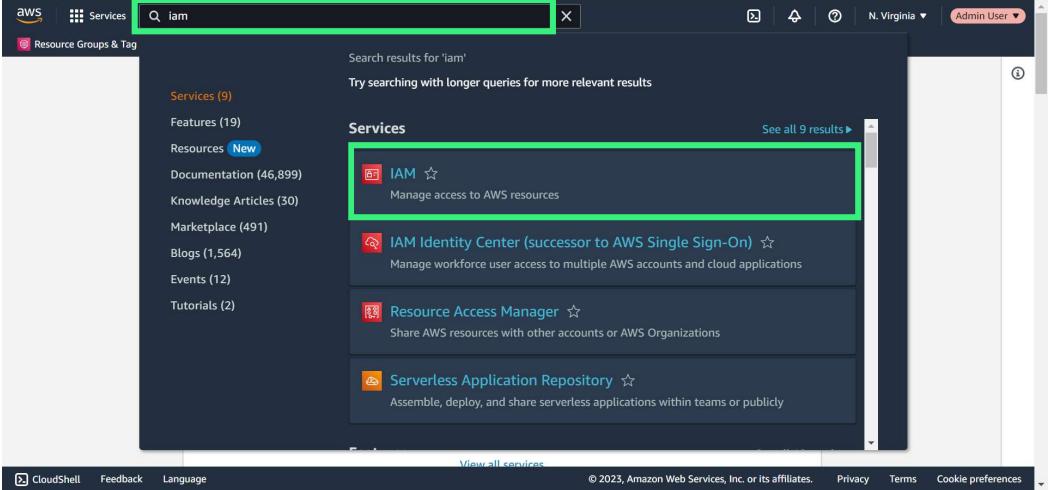


The screenshot shows the AWS CloudTrail Event history for a CreateBucket event, displaying the raw JSON event record. The 'bucketName' parameter is highlighted, showing its value as 'we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740'. Other parameters shown in the JSON include eventVersion, type, principalId, arn, accountID, accessKeyId, sourceIPAddress, userAgent, eventTime, eventSource, eventName, awsRegion, requestParameters, host, and responseElements.



Steps	Content	Visual
Step 1:	<p>Now that we've identified the user as tdir-workshop-rroe-dev, let's use CloudTrail to investigate any other events performed by this user.</p> <p>From the Event history page in CloudTrail, in the first Lookup attributes field, choose User name. In the second field, enter the tdir-workshop-rroe-dev user that we identified earlier and press enter.</p>	<p>Visual</p>

CloudTrail Security Workflows																																												
Step	Content	Visual																																										
		<h2>Analyze</h2> <p>Use CloudTrail to investigate the events performed by the user who created the suspicious bucket.</p>  <table border="1"> <thead> <tr> <th>Event name</th> <th>Event time</th> <th>User name</th> <th>Event source</th> <th>Resource type</th> <th>Resource name</th> </tr> </thead> <tbody> <tr> <td>PutBucketTagging</td> <td>July 13, 2023, 11:18:42 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> <td>AWS::S3::Bucket</td> <td>we-stole-ur-data-5689...</td> </tr> <tr> <td>CreateBucket</td> <td>July 13, 2023, 11:18:41 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> <td>AWS::S3::Bucket</td> <td>we-stole-ur-data-5689...</td> </tr> <tr> <td>ListBuckets</td> <td>July 13, 2023, 11:18:39 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> <td>-</td> <td>-</td> </tr> <tr> <td>PutBucketLogging</td> <td>July 13, 2023, 11:18:38 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> <td>-</td> <td>-</td> </tr> <tr> <td>GetCallerIdentity</td> <td>July 13, 2023, 11:18:37 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>s3.amazonaws.com</td> <td>AWS::S3::Bucket</td> <td>simulation-bucket-04...</td> </tr> <tr> <td></td> <td>July 13, 2023, 11:18:35 (UTC-05:00)</td> <td>tdir-workshop-rroe-dev</td> <td>sts.amazonaws.com</td> <td>-</td> <td>-</td> </tr> </tbody> </table>	Event name	Event time	User name	Event source	Resource type	Resource name	PutBucketTagging	July 13, 2023, 11:18:42 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	we-stole-ur-data-5689...	CreateBucket	July 13, 2023, 11:18:41 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	we-stole-ur-data-5689...	ListBuckets	July 13, 2023, 11:18:39 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	-	-	PutBucketLogging	July 13, 2023, 11:18:38 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	-	-	GetCallerIdentity	July 13, 2023, 11:18:37 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	simulation-bucket-04...		July 13, 2023, 11:18:35 (UTC-05:00)	tdir-workshop-rroe-dev	sts.amazonaws.com	-	-
Event name	Event time	User name	Event source	Resource type	Resource name																																							
PutBucketTagging	July 13, 2023, 11:18:42 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	we-stole-ur-data-5689...																																							
CreateBucket	July 13, 2023, 11:18:41 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	we-stole-ur-data-5689...																																							
ListBuckets	July 13, 2023, 11:18:39 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	-	-																																							
PutBucketLogging	July 13, 2023, 11:18:38 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	-	-																																							
GetCallerIdentity	July 13, 2023, 11:18:37 (UTC-05:00)	tdir-workshop-rroe-dev	s3.amazonaws.com	AWS::S3::Bucket	simulation-bucket-04...																																							
	July 13, 2023, 11:18:35 (UTC-05:00)	tdir-workshop-rroe-dev	sts.amazonaws.com	-	-																																							
Step 2:	<p>The results of the query show activity related to the suspicious bucket. There is no additional activity to address.</p> <p>In the eventname column we see the following actions were taken:</p> <ol style="list-style-type: none"> PutBucketTagging: This creates a tag set for an S3 bucket. CreateBucket: This API creates buckets in the AWS account and was the API used to create the suspicious bucket named <code>we-stole-ur-data-*</code> ListBuckets: This API lists buckets in the AWS account. PutBucketLogging: This API changes the logging status of an S3 bucket. GetCallerIdentity: This API provides information to the caller about the credentials that are currently in use. It is similar to the <code>whoami</code> command found on most Unix-like operating systems. <p>Next, let's contain the situation by preventing the user (<code>tdir-workshop-rroe-dev</code>) from signing in to the console and deactivating their access key.</p>																																											

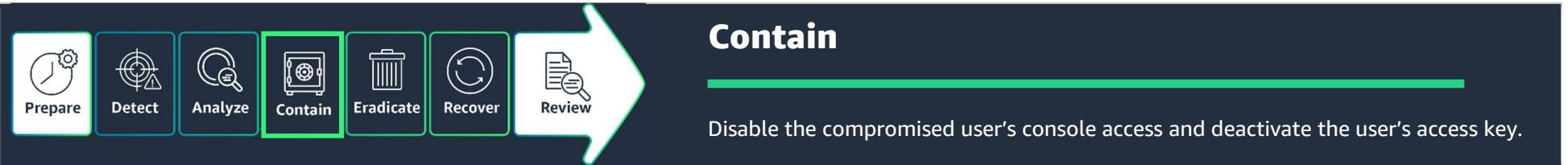
Contain						
	Prepare	Detect	Analyze	Contain	Eradicate	Recover
Disable the compromised user's console access and deactivate the user's access key.						
Steps	Content					Visual
Step 1:	<p>To disable the credentials for the compromised user, navigate to the IAM console:</p> <ol style="list-style-type: none"> 1. In the search field, enter IAM. 2. Under Services, choose IAM. 					 <p>The screenshot shows the AWS Services Catalog search results for 'iam'. The search bar at the top contains 'iam'. On the left, there's a sidebar with links like 'Services (9)', 'Features (19)', 'Resources (New)', etc. The main area lists services under 'Services': 'IAM' (highlighted with a green box), 'IAM Identity Center (successor to AWS Single Sign-On)', 'Resource Access Manager', and 'Serverless Application Repository'. Each service has a small icon and a brief description below it.</p>

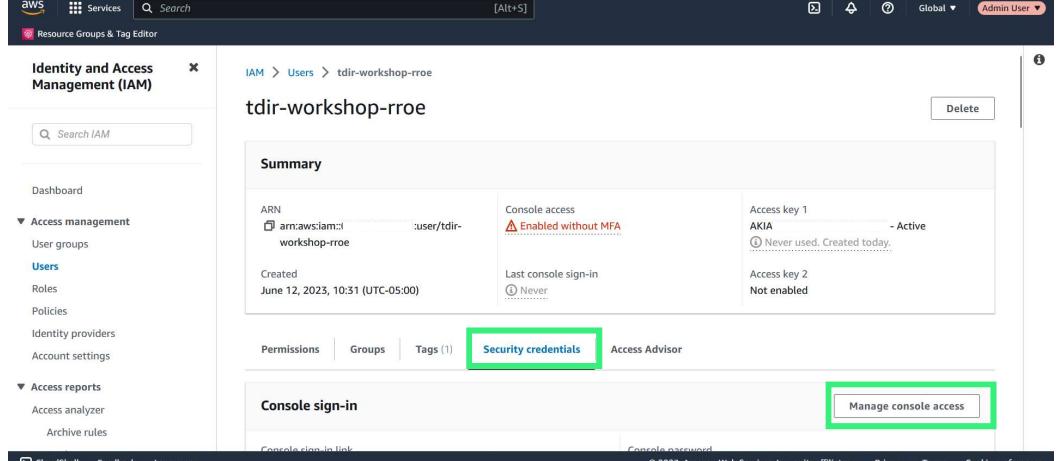
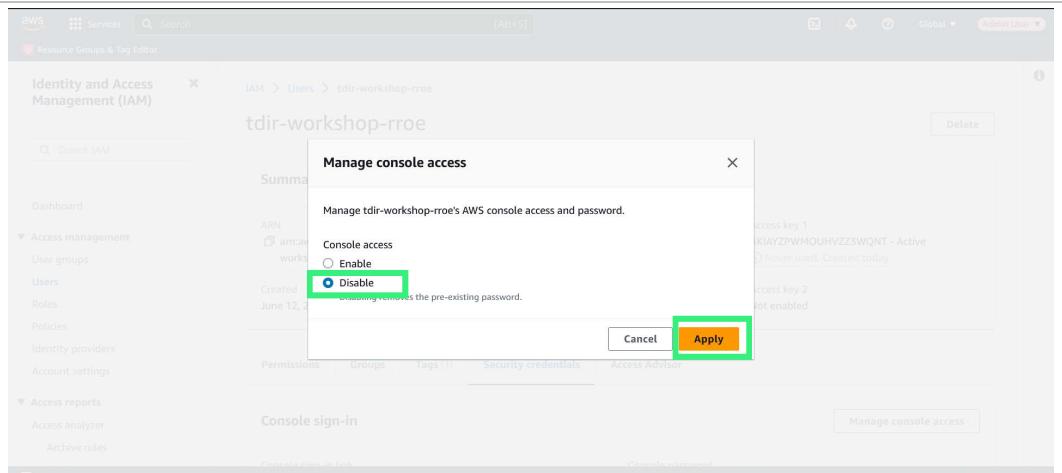


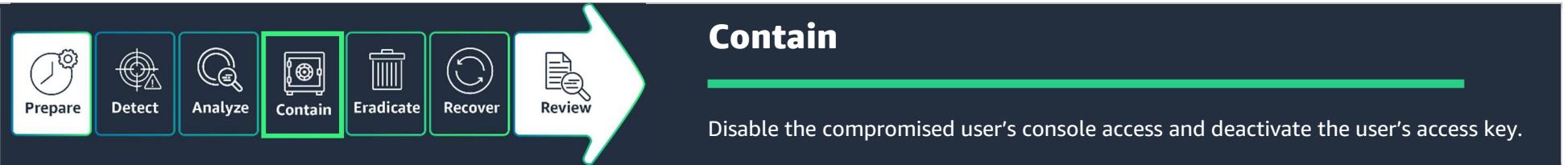
Contain

Disable the compromised user's console access and deactivate the user's access key.

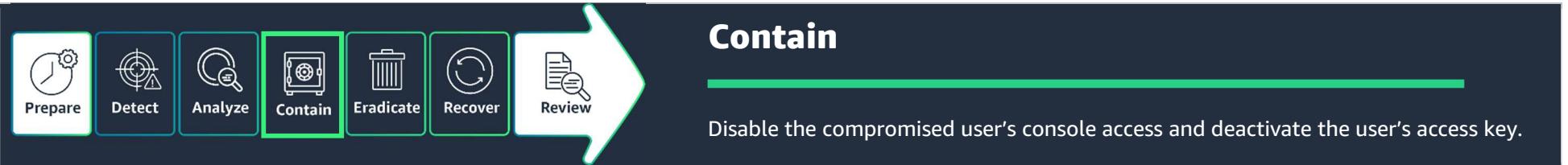
Steps	Content	Visual																																																
Step 2:	<p>The IAM dashboard displays.</p> <p>To disable the user tdir-workshop-rroe-dev under Access management, choose Users.</p>	<p>IAM dashboard</p> <p>Security recommendations</p> <p>IAM resources</p> <table border="1"> <thead> <tr> <th>User groups</th> <th>Users</th> <th>Roles</th> <th>Policies</th> <th>Identity providers</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>30</td> <td>19</td> <td>4</td> <td>0</td> </tr> </tbody> </table> <p>What's new</p> <ul style="list-style-type: none"> Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 6 months ago AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 7 months ago 	User groups	Users	Roles	Policies	Identity providers	0	30	19	4	0																																						
User groups	Users	Roles	Policies	Identity providers																																														
0	30	19	4	0																																														
Step 3:	<p>A list of users displays on the screen. Choose tdir-workshop-rroe-dev.</p>	<p>Users (7) info</p> <p>An IAM user is an identity with long term credentials that is used to interact with AWS in an account.</p> <table border="1"> <thead> <tr> <th>User name</th> <th>Groups</th> <th>Last activity</th> <th>MFA</th> <th>Password age</th> <th>Active key age</th> </tr> </thead> <tbody> <tr> <td>tdir-workshop-amansa-dev</td> <td>None</td> <td>Never</td> <td>None</td> <td>None</td> <td>41 days ago</td> </tr> <tr> <td>tdir-workshop-jstiles-dev</td> <td>None</td> <td>Never</td> <td>None</td> <td>35 days ago</td> <td>44 minutes ago</td> </tr> <tr> <td>tdir-workshop-nwolf</td> <td>admin</td> <td>3 days ago</td> <td>None</td> <td>None</td> <td>-</td> </tr> <tr> <td>tdir-workshop-roe</td> <td>None</td> <td>Never</td> <td>None</td> <td>36 days ago</td> <td>36 days ago</td> </tr> <tr> <td>tdir-workshop-rroe-dev</td> <td>None</td> <td>Never</td> <td>None</td> <td>None</td> <td>-</td> </tr> <tr> <td>tdir-workshop-sysdev</td> <td>None</td> <td>Never</td> <td>None</td> <td>None</td> <td>-</td> </tr> <tr> <td>testuser</td> <td>None</td> <td>Never</td> <td>None</td> <td>None</td> <td>-</td> </tr> </tbody> </table>	User name	Groups	Last activity	MFA	Password age	Active key age	tdir-workshop-amansa-dev	None	Never	None	None	41 days ago	tdir-workshop-jstiles-dev	None	Never	None	35 days ago	44 minutes ago	tdir-workshop-nwolf	admin	3 days ago	None	None	-	tdir-workshop-roe	None	Never	None	36 days ago	36 days ago	tdir-workshop-rroe-dev	None	Never	None	None	-	tdir-workshop-sysdev	None	Never	None	None	-	testuser	None	Never	None	None	-
User name	Groups	Last activity	MFA	Password age	Active key age																																													
tdir-workshop-amansa-dev	None	Never	None	None	41 days ago																																													
tdir-workshop-jstiles-dev	None	Never	None	35 days ago	44 minutes ago																																													
tdir-workshop-nwolf	admin	3 days ago	None	None	-																																													
tdir-workshop-roe	None	Never	None	36 days ago	36 days ago																																													
tdir-workshop-rroe-dev	None	Never	None	None	-																																													
tdir-workshop-sysdev	None	Never	None	None	-																																													
testuser	None	Never	None	None	-																																													



Steps	Content	Visual
Step 4:	The properties for the tdir-workshop-rroe-dev user display. Choose the Security credentials tab and then choose Manage console access .	
Step 5:	<p>The Manage console access window displays. Under Console access, select Disable, and then choose Apply to restrict the user access.</p> <p>We just prevented the compromised user from signing into the console. Now, we can deactivate the Access key.</p>	



Steps	Content	Visual
Step 6:	To disable the Access key, choose the Security credentials tab.	
Step 7:	Scroll down to the Access keys section. Choose the Actions drop-down menu and choose Deactivate .	



Steps	Content	Visual
Step 8:	<p>A confirmation window displays. Choose Deactivate.</p> <p>Now that we've contained the situation by disabling the user, let's check the suspicious bucket and see what we find.</p>	<p>Deactivate AKIA...</p> <p>Deactivate access key AKIA... You can't use an inactive key to make AWS API calls but you can activate it again later.</p> <p>Access key last used: None</p> <p>IAM user: tdir-workshop-rroe</p> <p>Account</p> <p>Cancel Deactivate</p>



Analyze

Use the S3 console to review objects in the suspicious bucket.

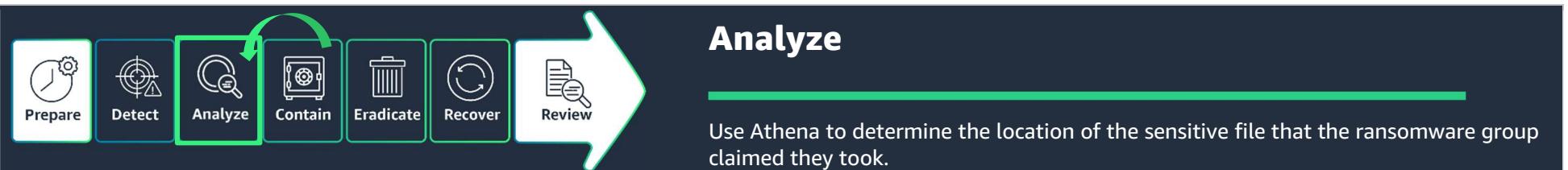
Steps	Content	Visual																
Step 1:	<p>From the Amazon S3 Buckets page, navigate to the suspicious bucket titled we-stole-ur-data-*.</p> <p>To see the objects in the bucket, choose we-stole-ur-data-*.</p>	<table border="1"> <thead> <tr> <th>Name</th> <th>AWS Region</th> <th>Access</th> <th>Last modified</th> </tr> </thead> <tbody> <tr> <td>tdir-bucketathena8bd64ef0-1bq4e5ahqik6</td> <td>US East (N. Virginia) us-east-1</td> <td>Bucket and objects not public</td> <td>June</td> </tr> <tr> <td>tdir-bucketlogs9c0dca97-yk54xw4ppht8</td> <td>US East (N. Virginia) us-east-1</td> <td>Bucket and objects not public</td> <td>June</td> </tr> <tr> <td>we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740</td> <td>US East (N. Virginia) us-east-1</td> <td>Bucket and objects not public</td> <td>June</td> </tr> </tbody> </table>	Name	AWS Region	Access	Last modified	tdir-bucketathena8bd64ef0-1bq4e5ahqik6	US East (N. Virginia) us-east-1	Bucket and objects not public	June	tdir-bucketlogs9c0dca97-yk54xw4ppht8	US East (N. Virginia) us-east-1	Bucket and objects not public	June	we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	US East (N. Virginia) us-east-1	Bucket and objects not public	June
Name	AWS Region	Access	Last modified															
tdir-bucketathena8bd64ef0-1bq4e5ahqik6	US East (N. Virginia) us-east-1	Bucket and objects not public	June															
tdir-bucketlogs9c0dca97-yk54xw4ppht8	US East (N. Virginia) us-east-1	Bucket and objects not public	June															
we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	US East (N. Virginia) us-east-1	Bucket and objects not public	June															
Step 2:	<p>The objects in the bucket displays on the Objects tab.</p> <p>Choose the file name all_your_data_are_belong_to_us.txt.</p>	<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Last modified</th> <th>Size</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>all_your_data_are_belong_to_us.txt</td> <td>txt</td> <td>June 11, 2023, 23:20:19 (UTC-05:00)</td> <td>336.0 B</td> <td>Standard</td> </tr> </tbody> </table>	Name	Type	Last modified	Size	Storage class	all_your_data_are_belong_to_us.txt	txt	June 11, 2023, 23:20:19 (UTC-05:00)	336.0 B	Standard						
Name	Type	Last modified	Size	Storage class														
all_your_data_are_belong_to_us.txt	txt	June 11, 2023, 23:20:19 (UTC-05:00)	336.0 B	Standard														



Analyze

Use the S3 console to review objects in the suspicious bucket.

Steps	Content	Visual
Step 3:	<p>To examine the contents of the file, from the download menu, choose all_your_data_are_belong_to_us.txt.</p> <p>Note: We will download this file for training purposes; in a real-world scenario, we would want to do this in a secure environment or isolated Amazon Elastic Compute (Cloud Amazon EC2) instance.</p>	
Step 4:	<p>Once the file downloads, open the all_your_data_are_belong_to_us.txt file in Notepad.</p> <p>The file reveals that the ransomware group has taken customer data in the form of a sensitive file named credit-card-data.csv. Write down the name of this file for future reference.</p> <p>Note: While we're investigating, be aware that any information a threat actor provides may be incorrect or be an attempt to evade defenses.</p> <p>Next, we will use Amazon Athena to locate the credit-card-data.csv file.</p>	<p>We have deleted all your files and have taken your customer data including the CREDIT-CARD-DATA.CSV file containing the credit card numbers of EVERY SINGLE ONE of your 10 customers.</p> <p>Pay us 100 BILLION DOLLARS in bitcoin within 48 hours and we will return the file and promise not to leak it onto the dark web.</p> <p>BTC Wallet address: <></p>

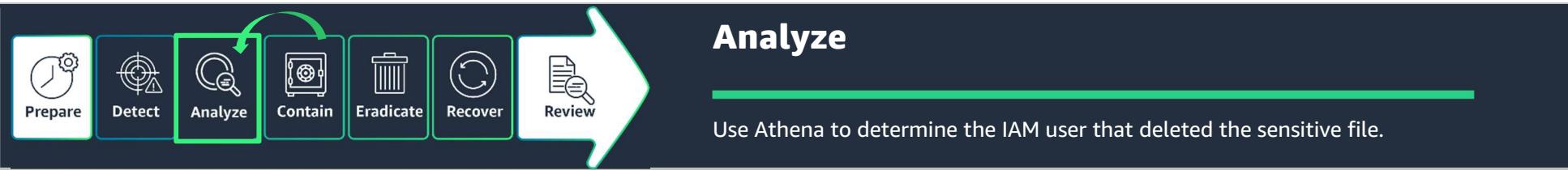


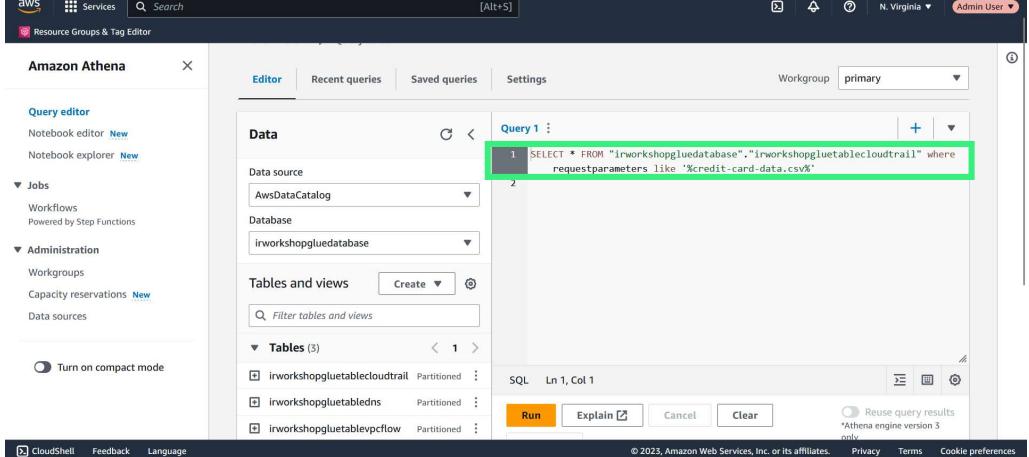
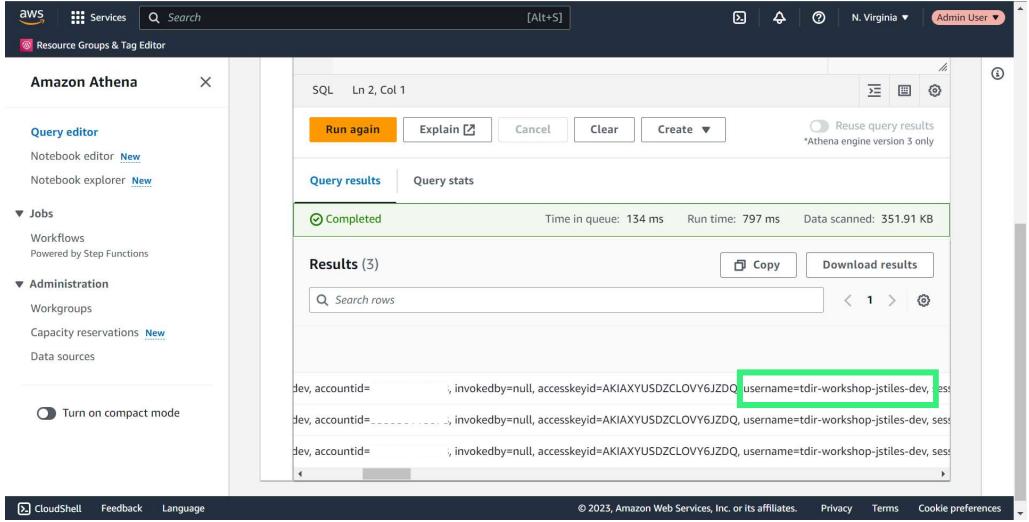
Steps	Content	Visual
Step 1:	<p>Use Athena to query AWS CloudTrail, to determine the location of the sensitive file.</p> <p>From the AWS Management Console:</p> <ol style="list-style-type: none"> 1. In the search field, enter Athena. 2. Under Services, choose Athena. 	<p>The screenshot shows the AWS Management Console search results for 'athena'. The search bar at the top contains 'athena'. Below the search bar, there is a 'Services' section with a card for 'Athena' highlighted with a green box. The 'Athena' card includes the subtext 'Serverless interactive analytics service'. To the right of the search results, there is a sidebar with various links like Documentation, Knowledge Articles, Marketplace, Blogs, Events, and Tutorials. At the bottom of the screen, there is a footer with links for CloudShell, Feedback, Language, and other AWS services.</p>
Step 2:	<p>Based on the results of the query, we see that the API calls in the eventname column are GetObject, HeadObject, and DeleteObject.</p> <p>This tells us that the object metadata and the object itself were obtained (HeadObject and GetObject) and that the object was deleted (DeleteObject).</p>	<p>The screenshot shows the Amazon Athena Query Editor. On the left, there is a sidebar with options for Query editor, Notebook editor, Notebook explorer, Jobs, Workflows, Administration, and Data sources. The main area is titled 'Amazon Athena' and shows a SQL query: 'SQL Ln 2, Col 1'. Below the query, there are tabs for 'Query results' and 'Query stats'. The 'Query results' tab is selected, showing a table with 3 completed rows. The columns are: ventime, eventsource, eventname, awsregion, sourceipaddress, and useragent. The 'eventname' column for the three rows is highlighted with a green box. The first row has 'HeadObject', the second 'GetObject', and the third 'DeleteObject'. The table also includes buttons for Run again, Explain, Cancel, Clear, Create, Copy, and Download results.</p>

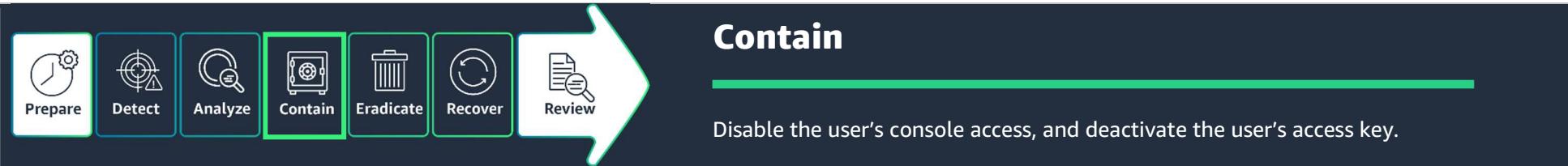
Analyze

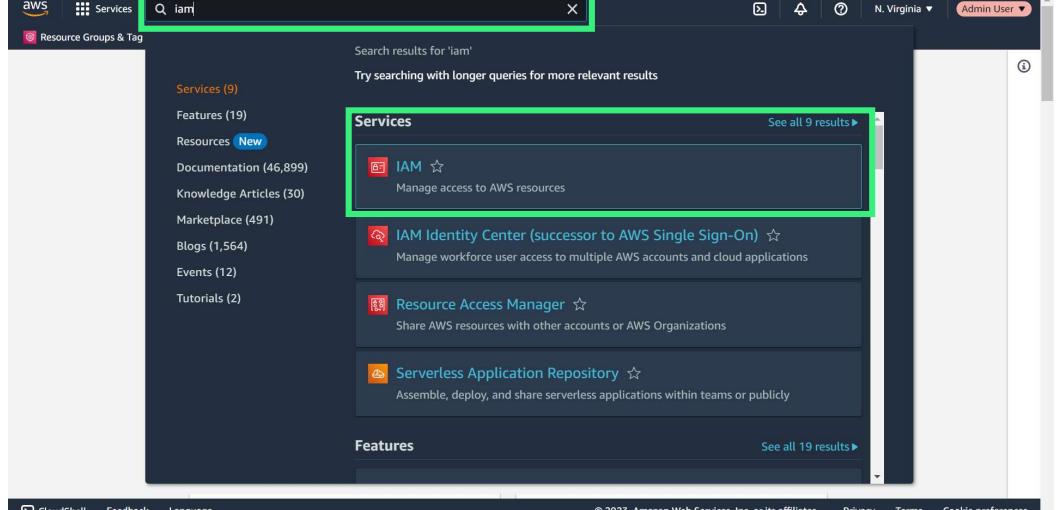
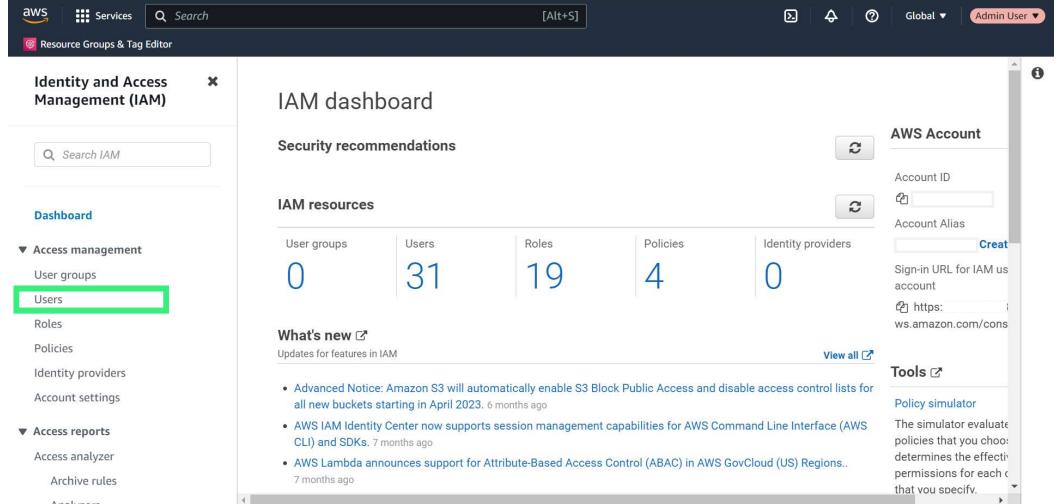
Use Athena to determine the location of the sensitive file that the ransomware group claimed they took.

Steps	Content								
Step 3:	<p>Scroll horizontally to the requestparameters column to see exactly which object the API calls were made for.</p> <p>This information confirms that the credit-card-data.csv object was taken and deleted, and that the S3 bucket from which it was taken was simulation-bucket-03-8lonc4g9dwxzrbim with a prefix/folder location of backup/customers/payment_information/.</p> <p>Because the CSV file was deleted, we will need to determine the name of the IAM user that retrieved and deleted the CSV object.</p>								
	<p>Visual</p> <table border="1"> <thead> <tr> <th>Results (3)</th> <th></th> </tr> </thead> <tbody> <tr> <td>ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")</td> <td>null</td> </tr> <tr> <td>ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")</td> <td>null</td> </tr> <tr> <td>ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")</td> <td>null</td> </tr> </tbody> </table>	Results (3)		ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null	ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null	ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null
Results (3)									
ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null								
ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null								
ksw574uhdlr.s3.us-east-1.amazonaws.com", "key": "backup/customers/payment_information/credit-card-data.csv")	null								

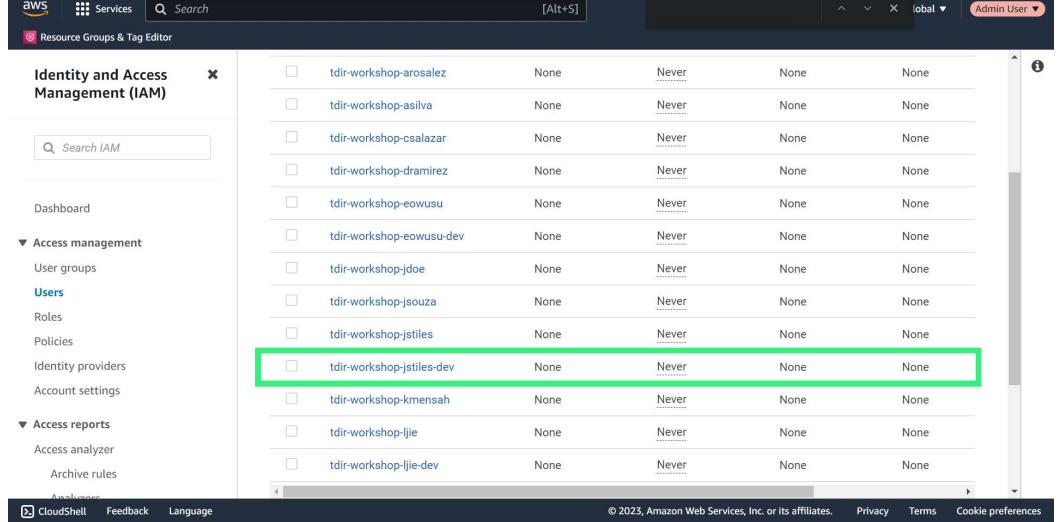
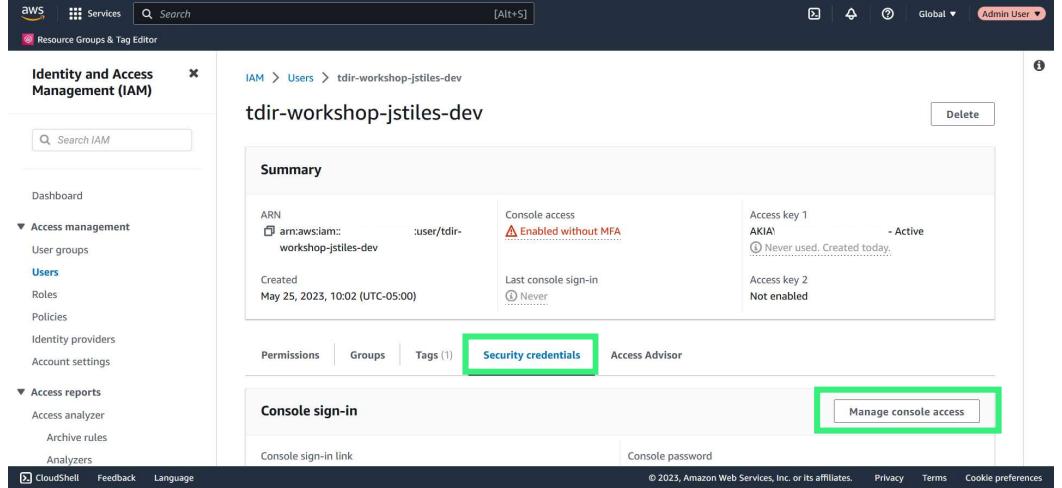


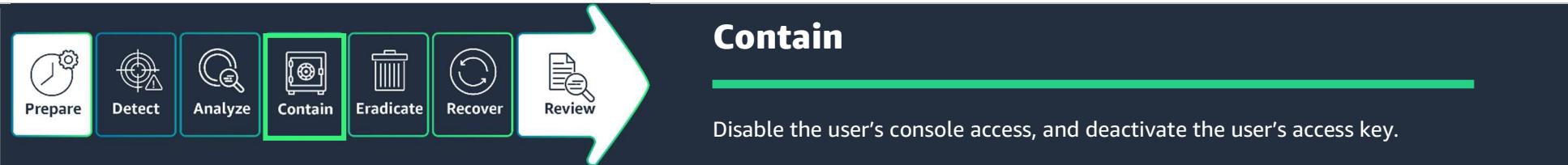
Steps	Content	Visual												
Step 1:	<p>Now that we've confirmed that the file was deleted, we can use this query to see what IAM user performed the action.</p>	 <pre>1 SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where requestparameters like '%credit-card-data.csv%'</pre>												
Step 2:	<p>Scroll to the useridentity column to see that the username parameter is tdir-workshop-jstiles-dev. This is the name of the IAM user that was used to retrieve and delete the credit-card-data.csv object.</p> <p>Because this tdir-workshop-jstiles-dev user was involved in the new activity, let's prevent the compromised user from signing in to the console by disabling their access and deactivating their access key.</p>	 <p>SQL Ln 2, Col 1</p> <p>Run again Explain Cancel Clear Create</p> <p>Completed Time in queue: 134 ms Run time: 797 ms Data scanned: 351.91 KB</p> <p>Results (3)</p> <table border="1"> <thead> <tr> <th>Search rows</th> <th>Copy</th> <th>Download results</th> </tr> </thead> <tbody> <tr> <td>dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses</td> <td></td> <td></td> </tr> <tr> <td>dev, accountid=-----, invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses</td> <td></td> <td></td> </tr> <tr> <td>dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses</td> <td></td> <td></td> </tr> </tbody> </table>	Search rows	Copy	Download results	dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses			dev, accountid=-----, invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses			dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses		
Search rows	Copy	Download results												
dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses														
dev, accountid=-----, invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses														
dev, accountid= , invokedby=null, accesskeyid=AKIAJAXYUSDZCLOVY6JZDQ, username=tdir-workshop-jstiles-dev, ses														



Steps	Content	Visual
Step 1:	To navigate to the IAM console: <ol style="list-style-type: none"> In the search field, enter IAM. Under Services, choose IAM. 	
Step 2:	The IAM dashboard displays. To disable the user tdir-workshop-jstile-dev under Access management, choose Users .	



Steps	Content	Visual
Step 3:	A list of users displays on the screen. Choose tdir-workshop-jstiles-dev .	
Step 4:	The properties for the tdir-workshop-jstiles-dev user display. Choose the Security credentials tab, and then choose Manage console access .	

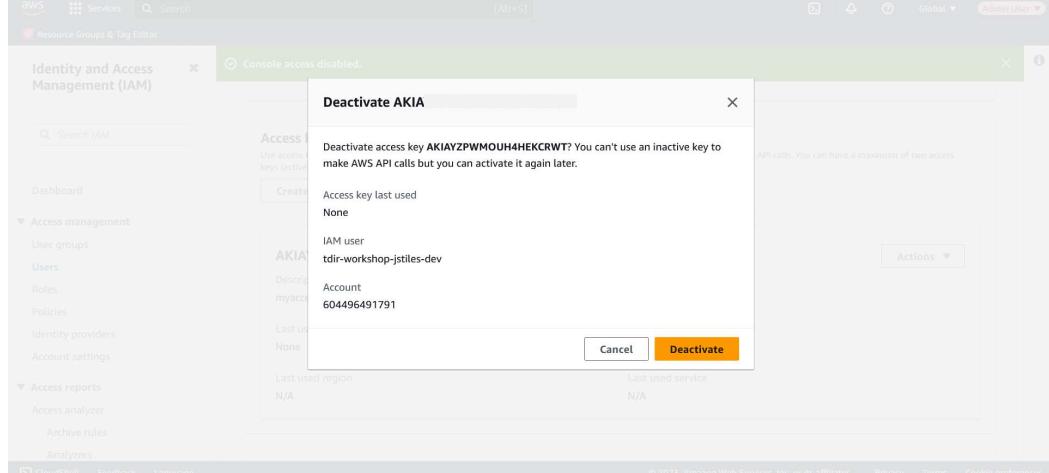


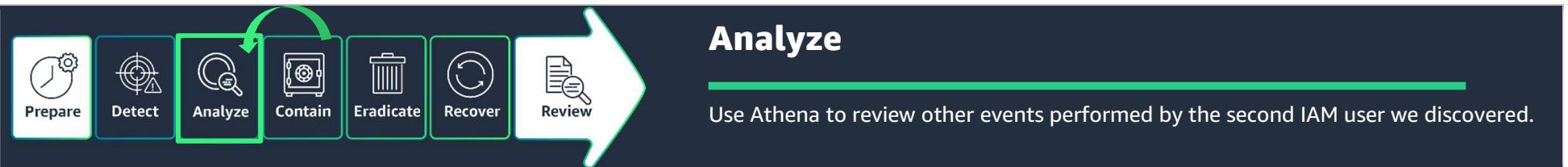
Steps	Content	Visual
Step 5:	<p>The Manage console access window displays. For console access, select Disable, and then choose Apply to restrict the user's access.</p> <p>We just prevented the compromised user from signing in to the console.</p>	
	<p>The message, "Console access disabled," displays.</p>	

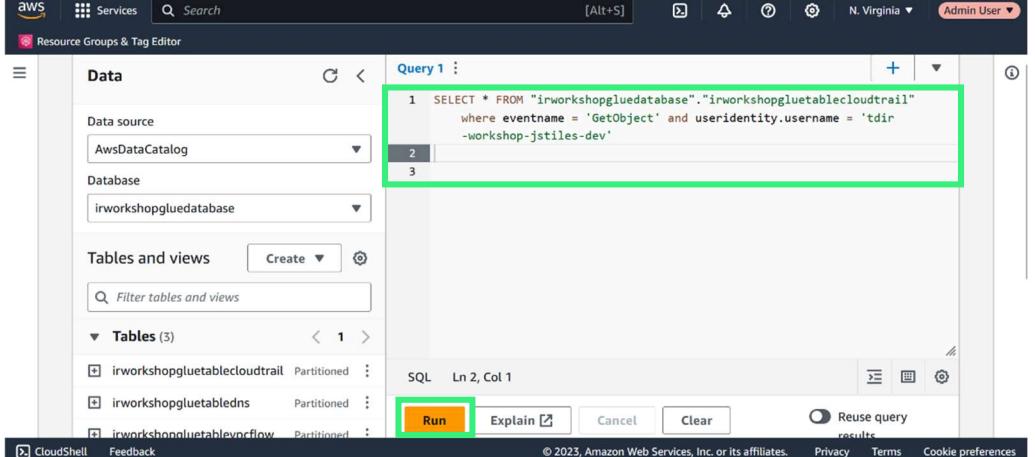
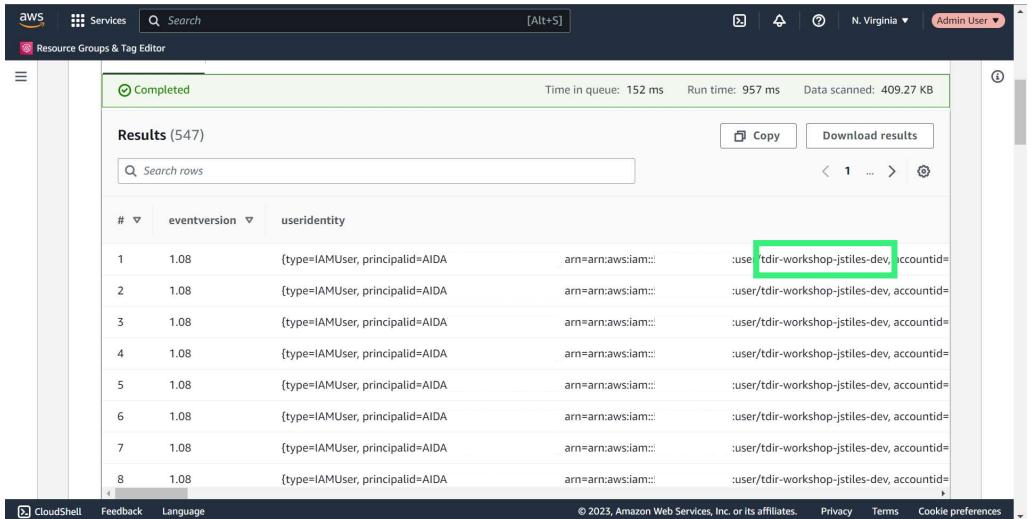


Steps	Content	Visual
Step 6:	To deactivate the access key. Choose the Security credentials tab.	
Step 7:	Scroll down to the Access keys section. Choose the Actions drop-down menu, and then choose Deactivate .	



Steps	Content	Visual
Step 8:	<p>A confirmation pop-up displays. Choose Deactivate.</p> <p>Now that we've contained the situation by restricting permissions of the user, let's check the new S3 bucket and see what we find.</p>	



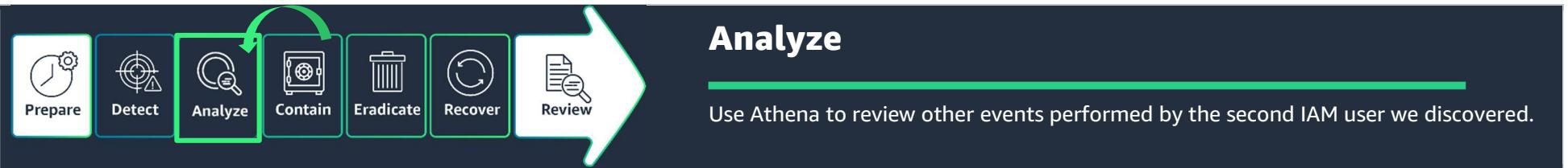
Steps	Content	Visual																																													
Step 1:	To determine if tdir-workshop-jstiles-dev took any other objects, navigate to Athena. On the Editor tab, for Query 1, enter this query and then choose Run.	 <p>The screenshot shows the AWS Athena Query Editor. The 'Data' pane on the left displays the 'Data source' as 'AwsDataCatalog' and the 'Database' as 'irworkshopgluedatabase'. Under 'Tables and views', there are three tables listed: 'irworkshopgluetablecloudtrail', 'irworkshopgluetabledns', and 'irworkshopgluetablevflow'. The 'Query 1' editor pane on the right contains the following SQL query:</p> <pre>1 SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'GetObject' and useridentity.username = 'tdir -workshop-jstiles-dev'</pre> <p>The 'Run' button at the bottom of the editor is highlighted with a green box. The status bar at the bottom indicates 'CloudShell Feedback'.</p>																																													
Step 2:	The query that we searched for, GetObject, shows a large number of results. This indicates the GetObject API was called, and the user (tdir-workshop-jstiles-dev) downloaded other objects.	 <p>The screenshot shows the AWS Athena Results page. The top bar indicates the query completed successfully with a green bar. The results table has columns: '#', 'eventversion', 'useridentity', 'arn=arn:aws:iam::', and 'user=tdir-workshop-jstiles-dev, accountid=' followed by a redacted account ID. The results table lists 547 rows, each corresponding to a GetObject event from the IAMUser principal AIDA. The status bar at the bottom indicates 'CloudShell Feedback Language'.</p> <table border="1"> <thead> <tr> <th>#</th><th>eventversion</th><th>useridentity</th><th>arn=arn:aws:iam::</th><th>user=tdir-workshop-jstiles-dev, accountid=</th></tr> </thead> <tbody> <tr><td>1</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>2</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>3</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>4</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>5</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>6</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>7</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> <tr><td>8</td><td>1.08</td><td>{type=IAMUser, principalId=AIDA}</td><td>arn=arn:aws:iam::</td><td>:user=tdir-workshop-jstiles-dev, accountid=</td></tr> </tbody> </table>	#	eventversion	useridentity	arn=arn:aws:iam::	user=tdir-workshop-jstiles-dev, accountid=	1	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	2	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	3	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	4	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	5	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	6	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	7	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=	8	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=
#	eventversion	useridentity	arn=arn:aws:iam::	user=tdir-workshop-jstiles-dev, accountid=																																											
1	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
2	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
3	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
4	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
5	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
6	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
7	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											
8	1.08	{type=IAMUser, principalId=AIDA}	arn=arn:aws:iam::	:user=tdir-workshop-jstiles-dev, accountid=																																											



Analyze

Use Athena to review other events performed by the second IAM user we discovered.

Steps	Content	Visual																																																																														
Step 3:	<p>Let's see what other activities the compromised IAM user tdir-workshop-jstiles-dev conducted.</p> <p>In Athena, on the Editor tab, enter this query and then choose Run.</p> <p>Use the same query in the previous step removing the where clause specifying the GetObject API. The query results will include all the username tdir-workshop-jstiles-dev activities.</p>	<pre> SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.username = 'tdir-workshop-jstiles-dev' and eventname != 'DeleteObject' and eventname != 'GetObject' </pre>																																																																														
Step 4:	<p>The query returns a large number of results. Reviewing the results shows that the DeleteObject and the GetObject API calls were used multiple times.</p> <p>This proves that the IAM user tdir-workshop-jstiles-dev was used to retrieve and delete numerous objects.</p>	<table border="1"> <thead> <tr> <th>time</th> <th>eventsource</th> <th>eventname</th> <th>awsregion</th> <th>sourceipaddress</th> <th>useragent</th> </tr> </thead> <tbody> <tr><td>16-12T04:19:44Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:43Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:44Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:45Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:46Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:46Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:46Z</td><td>s3.amazonaws.com</td><td>GetObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:51Z</td><td>s3.amazonaws.com</td><td>DeleteObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:51Z</td><td>s3.amazonaws.com</td><td>DeleteObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:51Z</td><td>s3.amazonaws.com</td><td>DeleteObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:51Z</td><td>s3.amazonaws.com</td><td>DeleteObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> <tr><td>16-12T04:19:52Z</td><td>s3.amazonaws.com</td><td>DeleteObject</td><td>us-east-1</td><td>[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]</td><td></td></tr> </tbody> </table>	time	eventsource	eventname	awsregion	sourceipaddress	useragent	16-12T04:19:44Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:43Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:44Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:45Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]		16-12T04:19:52Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]	
time	eventsource	eventname	awsregion	sourceipaddress	useragent																																																																											
16-12T04:19:44Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:43Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:44Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:45Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:46Z	s3.amazonaws.com	GetObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:51Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												
16-12T04:19:52Z	s3.amazonaws.com	DeleteObject	us-east-1	[aws-cli/2.11.25 Python/3.11.3 Linux/5.10.179-1]																																																																												



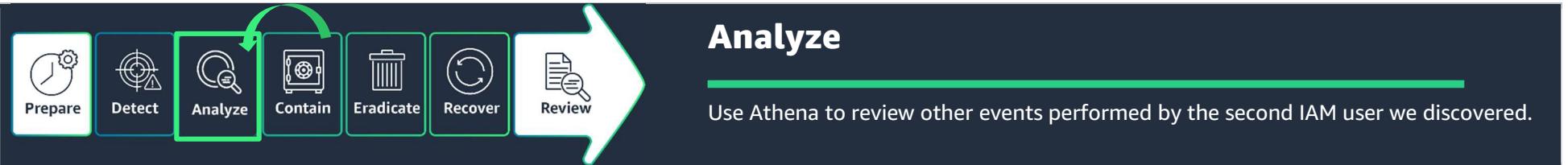
Steps	Content	Visual
Step 5:	<p>We can reduce the number of results by eliminating these two API calls from our query. In Athena, on the Editor tab, enter SELECT, * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.username = 'tdir-workshop-jstile-dev' and eventname != 'DeleteObject' and eventname != 'GetObject' and then choose Run again.</p> <p>Note: We used the != operator for this query. We are reducing the number of results to not include delete object and get object by using !=.</p>	<pre>1 SELECT * FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where useridentity.username = 'tdir-workshop-jstile-dev' and eventname != 'DeleteObject' and eventname != 'GetObject'</pre>



Analyze

Use Athena to review other events performed by the second IAM user we discovered.

Steps	Content	Visual																																																																								
Step 6:	<p>This query provides us with 21 results—much more manageable. These results provide more detail about the scope of the unauthorized activity.</p> <p>Based on the data in the eventname column, the following additional activities were performed (don't forget we already filtered out DeleteObject and GetObject from the query results).</p> <p>The last seven API calls are interesting, and we will look further into these.</p>	<p>Visual representation of the AWS CloudTrail event log data. The table shows 21 rows of event details, including eventtime, eventsource, eventname, awsregion, and sourceipaddress.</p> <table border="1"> <thead> <tr> <th></th> <th>eventtime</th> <th>eventsource</th> <th>eventname</th> <th>awsregion</th> <th>sourceipaddress</th> </tr> </thead> <tbody> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:01Z</td><td>iam.amazonaws.com</td><td>AttachUserPolicy</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:02Z</td><td>iam.amazonaws.com</td><td>CreateAccessKey</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:18Z</td><td>sts.amazonaws.com</td><td>GetCallerIdentity</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:20Z</td><td>iam.amazonaws.com</td><td>DeleteAccessKey</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:21Z</td><td>iam.amazonaws.com</td><td>DetachUserPolicy</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:20:22Z</td><td>iam.amazonaws.com</td><td>DeleteUser</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:19:14Z</td><td>sts.amazonaws.com</td><td>GetCallerIdentity</td><td>us-east-1</td><td>...</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:19:16Z</td><td>s3.amazonaws.com</td><td>ListBuckets</td><td>us-east-1</td><td>[...]</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:19:17Z</td><td>s3.amazonaws.com</td><td>ListBuckets</td><td>us-east-1</td><td>[...]</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:19:18Z</td><td>s3.amazonaws.com</td><td>ListBuckets</td><td>us-east-1</td><td>[...]</td></tr> <tr><td>p-jstiles-dev, sessioncontext=null)</td><td>2023-06-12T04:19:19Z</td><td>s3.amazonaws.com</td><td>ListObjects</td><td>us-east-1</td><td>[...]</td></tr> </tbody> </table>		eventtime	eventsource	eventname	awsregion	sourceipaddress	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:01Z	iam.amazonaws.com	AttachUserPolicy	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:02Z	iam.amazonaws.com	CreateAccessKey	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:18Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:20Z	iam.amazonaws.com	DeleteAccessKey	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:21Z	iam.amazonaws.com	DetachUserPolicy	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:22Z	iam.amazonaws.com	DeleteUser	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:14Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	...	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:16Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:17Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:18Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]	p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:19Z	s3.amazonaws.com	ListObjects	us-east-1	[...]
	eventtime	eventsource	eventname	awsregion	sourceipaddress																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:01Z	iam.amazonaws.com	AttachUserPolicy	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:02Z	iam.amazonaws.com	CreateAccessKey	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:18Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:20Z	iam.amazonaws.com	DeleteAccessKey	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:21Z	iam.amazonaws.com	DetachUserPolicy	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:20:22Z	iam.amazonaws.com	DeleteUser	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:14Z	sts.amazonaws.com	GetCallerIdentity	us-east-1	...																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:16Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:17Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:18Z	s3.amazonaws.com	ListBuckets	us-east-1	[...]																																																																					
p-jstiles-dev, sessioncontext=null)	2023-06-12T04:19:19Z	s3.amazonaws.com	ListObjects	us-east-1	[...]																																																																					



Steps	Content	Visual																																																												
Step 7:	<p>Let's analyze the last seven API calls and focus on the time they occurred.</p> <p>Note: The dates and times displayed in your account will be different. Use these only as an example.</p> <ol style="list-style-type: none"> DeleteUser: The tdir-workshop-rroe-dev user was deleted. DetachUserPolicy: The AdministratorAccess policy was detached from the tdir-workshop-rroe-dev IAM user. DeleteAccessKey: An access key for tdir-workshop-rroe-dev was deleted. GetCallerIdentity: The GetCallerIdentity API was called by the tdir-workshop-jstiles-dev IAM user. CreateAccessKey: An access key was created for tdir-workshop-rroe-dev. AttachUserPolicy: The AdministratorAccess policy was attached to tdir-workshop-rroe-dev. CreateUser: The user tdir-workshop-rroe-dev was created. <p>Based on the last seven API calls, the tdir-workshop-jstiles-dev created the IAM user tdir-workshop-rroe-dev. This gives them administrative privileges just before the IAM user tdir-workshop-rroe-dev was used to create the new bucket in the AWS account.</p>	<table border="1"> <thead> <tr> <th>Event name</th> <th>Event time</th> <th>User name</th> <th>Event source</th> <th>Resource type</th> </tr> </thead> <tbody> <tr> <td>1 DeleteUser</td> <td>July 25, 2023, 00:57:31 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::User</td> </tr> <tr> <td>2 DetachUserPolicy</td> <td>July 25, 2023, 00:57:29 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::User, AWS::I...</td> </tr> <tr> <td>3 DeleteAccessKey</td> <td>July 25, 2023, 00:57:27 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::AccessKey, ...</td> </tr> <tr> <td>4 GetCallerIdentity</td> <td>July 25, 2023, 00:57:24 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>sts.amazonaws.com</td> <td>-</td> </tr> <tr> <td>5 CreateAccessKey</td> <td>July 25, 2023, 00:57:01 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::AccessKey, ...</td> </tr> <tr> <td>6 AttachUserPolicy</td> <td>July 25, 2023, 00:56:59 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::User, AWS::I...</td> </tr> <tr> <td>7 CreateUser</td> <td>July 25, 2023, 00:56:57 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>iam.amazonaws.com</td> <td>AWS::IAM::User</td> </tr> <tr> <td>ListBuckets</td> <td>July 25, 2023, 00:55:40 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>s3.amazonaws.com</td> <td>-</td> </tr> <tr> <td>ListBuckets</td> <td>July 25, 2023, 00:55:39 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>s3.amazonaws.com</td> <td>-</td> </tr> <tr> <td>ListBuckets</td> <td>July 25, 2023, 00:55:37 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>s3.amazonaws.com</td> <td>-</td> </tr> <tr> <td>GetCallerIdentity</td> <td>July 25, 2023, 00:55:34 (UTC-05...)</td> <td>tdir-workshop-jstil...</td> <td>sts.amazonaws.com</td> <td>-</td> </tr> </tbody> </table> <p>0 / 5 events selected</p>	Event name	Event time	User name	Event source	Resource type	1 DeleteUser	July 25, 2023, 00:57:31 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User	2 DetachUserPolicy	July 25, 2023, 00:57:29 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User, AWS::I...	3 DeleteAccessKey	July 25, 2023, 00:57:27 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::AccessKey, ...	4 GetCallerIdentity	July 25, 2023, 00:57:24 (UTC-05...)	tdir-workshop-jstil...	sts.amazonaws.com	-	5 CreateAccessKey	July 25, 2023, 00:57:01 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::AccessKey, ...	6 AttachUserPolicy	July 25, 2023, 00:56:59 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User, AWS::I...	7 CreateUser	July 25, 2023, 00:56:57 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User	ListBuckets	July 25, 2023, 00:55:40 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-	ListBuckets	July 25, 2023, 00:55:39 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-	ListBuckets	July 25, 2023, 00:55:37 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-	GetCallerIdentity	July 25, 2023, 00:55:34 (UTC-05...)	tdir-workshop-jstil...	sts.amazonaws.com	-
Event name	Event time	User name	Event source	Resource type																																																										
1 DeleteUser	July 25, 2023, 00:57:31 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User																																																										
2 DetachUserPolicy	July 25, 2023, 00:57:29 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User, AWS::I...																																																										
3 DeleteAccessKey	July 25, 2023, 00:57:27 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::AccessKey, ...																																																										
4 GetCallerIdentity	July 25, 2023, 00:57:24 (UTC-05...)	tdir-workshop-jstil...	sts.amazonaws.com	-																																																										
5 CreateAccessKey	July 25, 2023, 00:57:01 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::AccessKey, ...																																																										
6 AttachUserPolicy	July 25, 2023, 00:56:59 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User, AWS::I...																																																										
7 CreateUser	July 25, 2023, 00:56:57 (UTC-05...)	tdir-workshop-jstil...	iam.amazonaws.com	AWS::IAM::User																																																										
ListBuckets	July 25, 2023, 00:55:40 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-																																																										
ListBuckets	July 25, 2023, 00:55:39 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-																																																										
ListBuckets	July 25, 2023, 00:55:37 (UTC-05...)	tdir-workshop-jstil...	s3.amazonaws.com	-																																																										
GetCallerIdentity	July 25, 2023, 00:55:34 (UTC-05...)	tdir-workshop-jstil...	sts.amazonaws.com	-																																																										



Steps	Content	Visual
Step 1:	<p>Now that we've narrowed the scope of the incident and identified which users were involved, let's search for other buckets that might have been deleted.</p> <p>In Athena, on the Editor tab, enter SELECT eventtime, eventname, requestparameters FROM "irworkshopgluedatabase"."irworkshopgluetablecloudtrail" where eventname = 'DeleteBucket', and then choose Run.</p>	
Step 2:	<p>There are no results for bucket deletions. Let's see now if there were objects download from an S3 bucket.</p>	

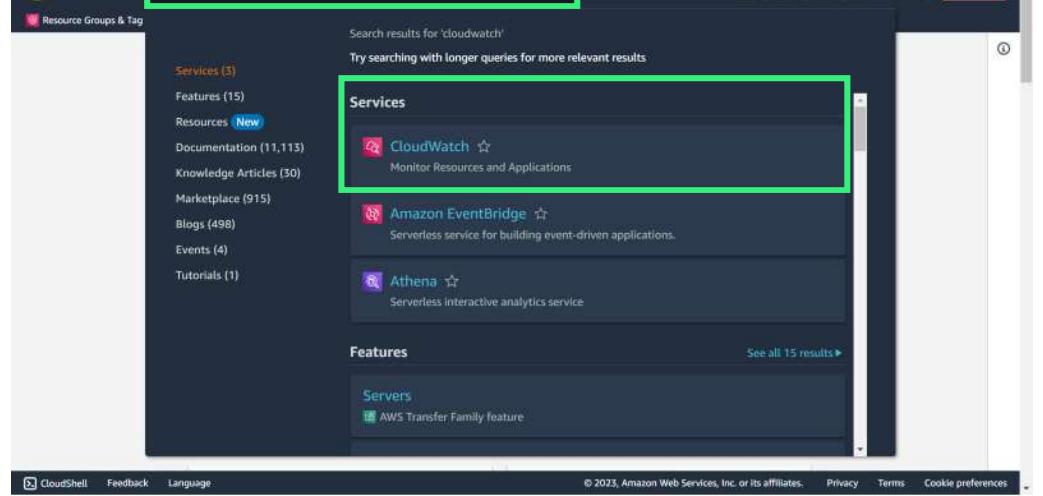


Analyze

Use Athena to review other events performed by the second IAM user we discovered.

Steps	Content	Visual
Step 3:	We can search for any objects that were download from S3 buckets by using this query in Athena.	
Step 4:	<p>The results confirm that multiple objects were retrieved from the simulation-bucket-02-* bucket.</p> <p>Next, we will search for the number the of bytes downloaded from the simulation-bucket-02-* using CloudWatch.</p>	



Steps	Content	Visual
Step 1:	<p>To access CloudWatch to search for the number of bytes downloaded from the simulation-bucket-02-* bucket:</p> <p>From the AWS Management Console:</p> <ol style="list-style-type: none"> 1. In the search field, enter CloudWatch. 2. From the Services list, choose CloudWatch. 	<p>Analyze</p> <p>Use CloudWatch to search for bytes downloaded from S3 buckets.</p> 

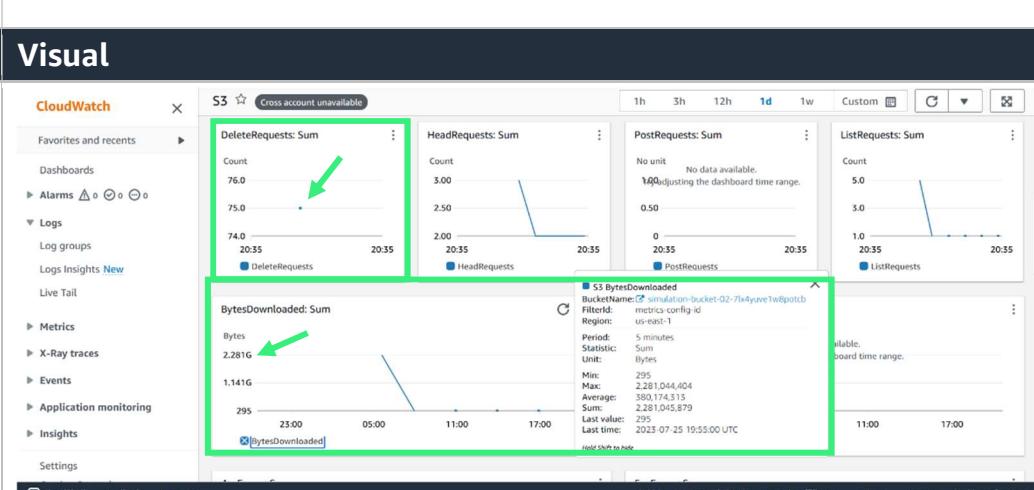


Analyze

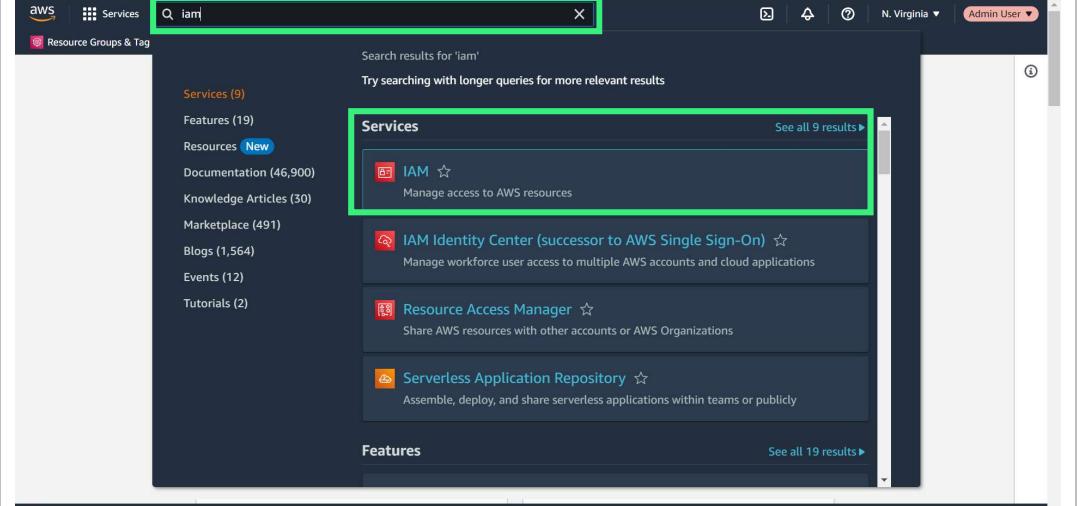
Use CloudWatch to search for bytes downloaded from S3 buckets.

Steps	Content	Visual
Step 2:	The CloudWatch service page displays. From the Overview menu, select Service dashboards .	
Step 3:	The Automatic dashboards page displays. To review the simulation-bucket-02-* S3 bucket, choose S3 .	



Steps	Content	Visual
Step 4:	<p>The Amazon S3 dashboard displays. Scroll down to the S3 DeleteRequests: Sum for the simulation- bucket-02-*. This shows 75 delete requests.</p> <p>The BytesDownloaded: Sum section shows that 2.28GB of data was downloaded from the bucket.</p> <p>Now that we've identified the scope of the incident from the amount of data downloaded, let's check on any other sensitive files.</p>	 <p>CloudWatch Metrics Dashboard for S3 bucket. The 'BytesDownloaded: Sum' metric is highlighted. Key data points from the highlighted section:</p> <ul style="list-style-type: none"> BucketName: simulation-bucket-02-7lx4yue1w8p0tcb FilterId: null Requester: null Period: 5 minutes Statistic: Sum Unit: Bytes Min: 295 Max: 2,281,044,404 Average: 380,174,515 Sum: 2,281,045,879 Last value: 295 Last time: 2023-07-25 19:55:00 UTC



Steps	Content	Visual
Step 1:	<p>To navigate to the IAM console:</p> <ol style="list-style-type: none"> 1. In the search field, enter IAM. 2. Under Services, choose IAM. 	 <p>The screenshot shows the AWS search interface. The search bar at the top contains the text "iam". Below the search bar, there are sections for "Services" and "Features". The "Services" section is expanded, showing a list of services. The "IAM" service is highlighted with a green box. Other services listed include IAM Identity Center, Resource Access Manager, and Serverless Application Repository. The "Features" section below has a "See all 19 results" link.</p>



Contain

Use the IAM console to rotate the compromised user's credentials.

- Step 2:** The IAM dashboard displays. Under Access management, choose **Users**.

IAM dashboard

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules

CloudShell Feedback Language

AWS Account

Account ID

Account Alias

Sign-in URL for IAM user account

https://ws.amazon.com/cons

Tools

Policy simulator

View all

What's new

Updates for features in IAM

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 6 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 7 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions. 7 months ago

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Step 3:** A list of users displays on the screen. Choose **tdir-workshop-jstiles-dev**.

tdir-workshop-amansa	None	Never	None	None
tdir-workshop-arosalez	None	Never	None	None
tdir-workshop-asilva	None	Never	None	None
tdir-workshop-csalazar	None	Never	None	None
tdir-workshop-dramirez	None	Never	None	None
tdir-workshop-eowusu	None	Never	None	None
tdir-workshop-eowusu-dev	None	Never	None	None
tdir-workshop-jdoe	None	Never	None	None
tdir-workshop-jsouza	None	Never	None	None
tdir-workshop-jstiles	None	Never	None	None
tdir-workshop-jstiles-dev	None	Never	None	None
tdir-workshop-kmensah	None	Never	None	None
tdir-workshop-ljje	None	Never	None	None

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Step 4: The user details page displays. Choose **Security credentials**, and then choose **Enable console access**.

This screenshot shows the AWS IAM User Details page for the user 'tdir-workshop-jstiles-dev'. The 'Security credentials' tab is highlighted with a green box. The 'Console sign-in' section contains a button labeled 'Enable console access' with a green box around it.

Step 5: The manage console access window displays. Under Set password, choose **Autogenerated password**, and then choose **Apply**.

This screenshot shows the 'Manage console access' dialog box. The 'Set password' section is highlighted with a green box, showing the 'Autogenerated password' radio button selected. The 'Apply' button at the bottom right is also highlighted with an orange box.



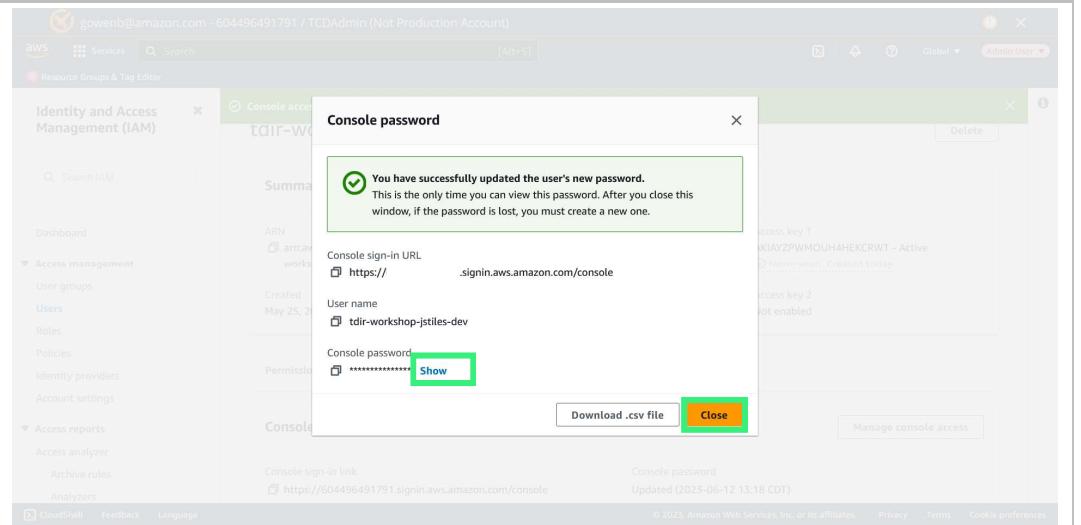
Step 6:

The console password window displays, indicating that we've successfully updated the user's new password. To view the console password, choose **Show**. Otherwise, choose **Close** to close the window.

Note: Because the tdir-workshop-jstiles-dev user had previously deleted the tdir-workshop-rroe-dev user, we don't need to take any actions on that user.

Contain

Use the IAM console to rotate the compromised user's credentials.





Steps	Content	Visual
Step 1:	<p>From the AWS Management Console:</p> <ol style="list-style-type: none"> 1. In the search field, enter S3. 2. Under the Services list, choose S3. 	<p>Visual representation of the AWS Management Console search results for 's3'. The search bar at the top contains 's3'. Below it, the 'Services' section is expanded, showing a list of services. The 'S3' service is highlighted with a green box. It is described as 'Scalable Storage in the Cloud'.</p> 



Step 2: Scroll down to the Buckets section, and choose the **we-stole-ur-data-*** bucket.

Name	AWS Region	Access	Created
tdir-bucketathena8bd64ef0-1bq4e5ahqjk6	US East (N. Virginia) us-east-1	Bucket and objects not public	June
tdir-bucketlogs9c0dca97-yk54xw4ppht8	US East (N. Virginia) us-east-1	Bucket and objects not public	June
we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	US East (N. Virginia) us-east-1	Bucket and objects not public	June

Step 3: The bucket Objects page displays. Select **all_your_data_are_belong_to_us.txt** and then choose Delete.

Name	Type	Last modified	Size	Storage class
all_your_data_are_belong_to_us.txt	txt	June 11, 2023, 23:20:19 (UTC-05:00)	336.0 B	Standard



Step 4: The Delete objects page displays. Scroll to the **Delete objects?** section. In the text field, enter **delete**, and then choose **Delete objects**.

Deleting the specified objects adds delete markers to them
If you need to undo the delete action, you can delete the delete markers. Learn more [? \[Alt+S\]](#)

Specified objects

Name	Type	Last modified	Size
all_your_data_are_belong_to_us.txt	txt	June 11, 2023, 23:20:19 (UTC-05:00)	336.0 B

Delete objects?

To confirm deletion, type **delete** in the text input field.
delete

Cancel **Delete objects**

Step 5: The Delete objects: status page displays with a status message indicating that the object has been deleted. Choose **Close**.

Successfully deleted objects
View details below.

Delete objects: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully deleted	Failed to delete
s3://we-stole-ur-data-78b88c3d-a667-4b2b-9085-5f9eafe81740	1 object, 336.0 B	0 objects

Failed to delete Configuration

Failed to delete (0)

CloudShell **Feedback** **Language** © 2023, Amazon Web Services, Inc. or its affiliates. **Privacy** **Terms** **Cookie preferences**

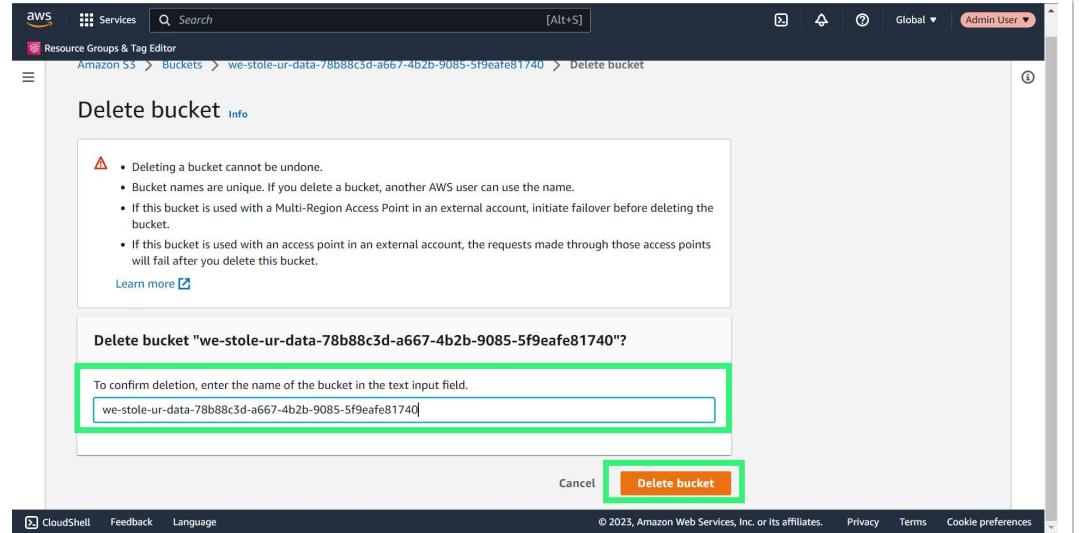


Step 6: The we-stole-ur-data-* bucket page displays. Choose **Buckets** from the navigation menu.

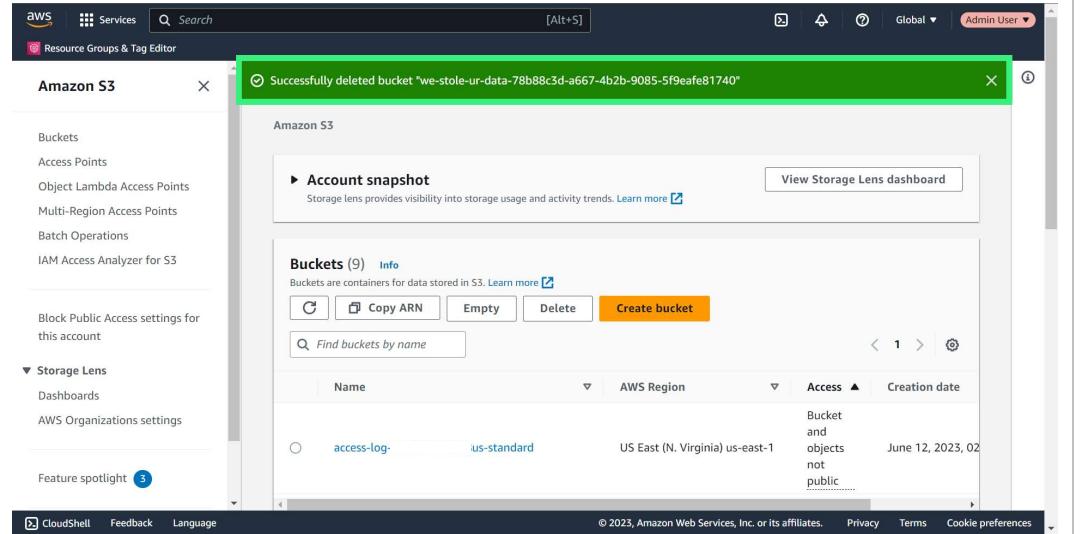
Step 7: The Buckets page displays. Choose **we-stole-ur-data-* bucket**. Then, choose **Delete**.



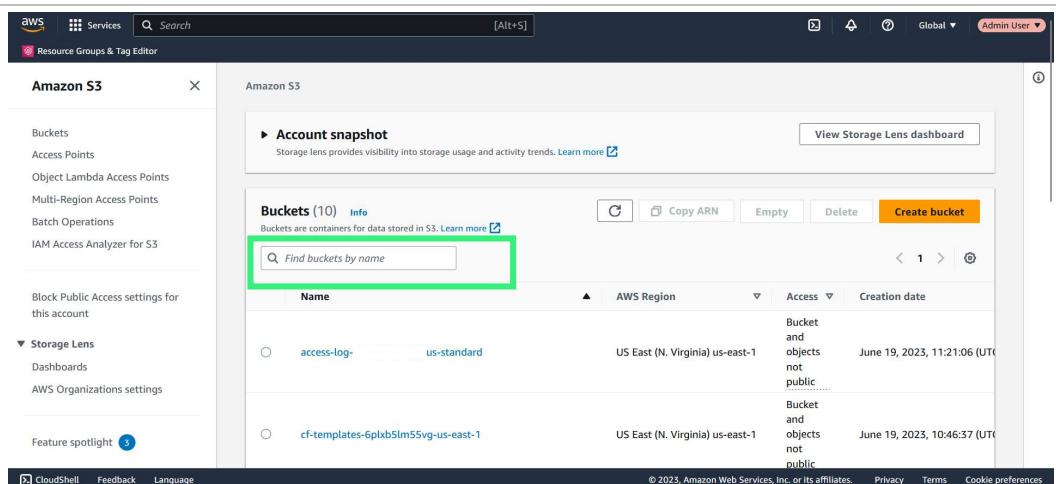
Step 8: The Delete bucket page displays. In the last field on the page, enter **we-stole-ur-data-*** and then choose **Delete bucket**.



Step 9: The Buckets page displays with a status message indicating that the bucket was successfully deleted.



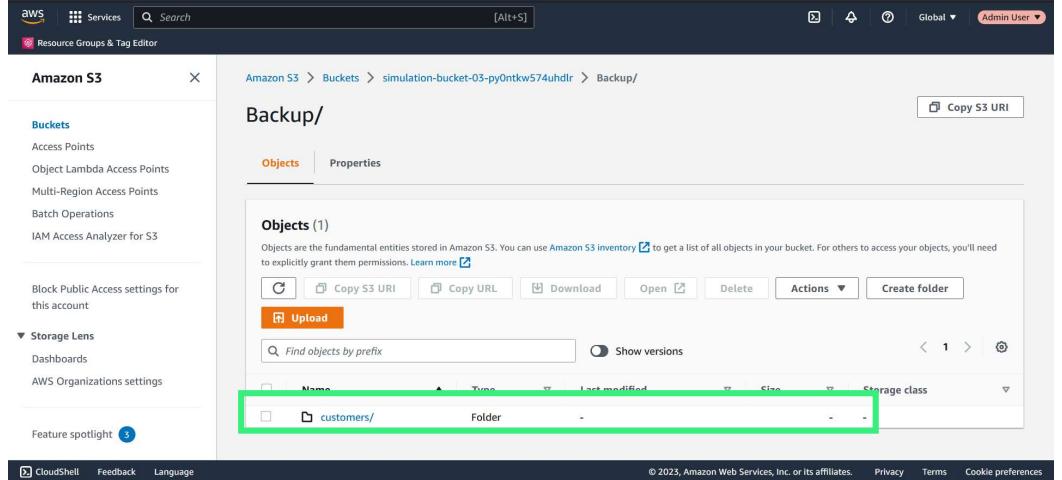
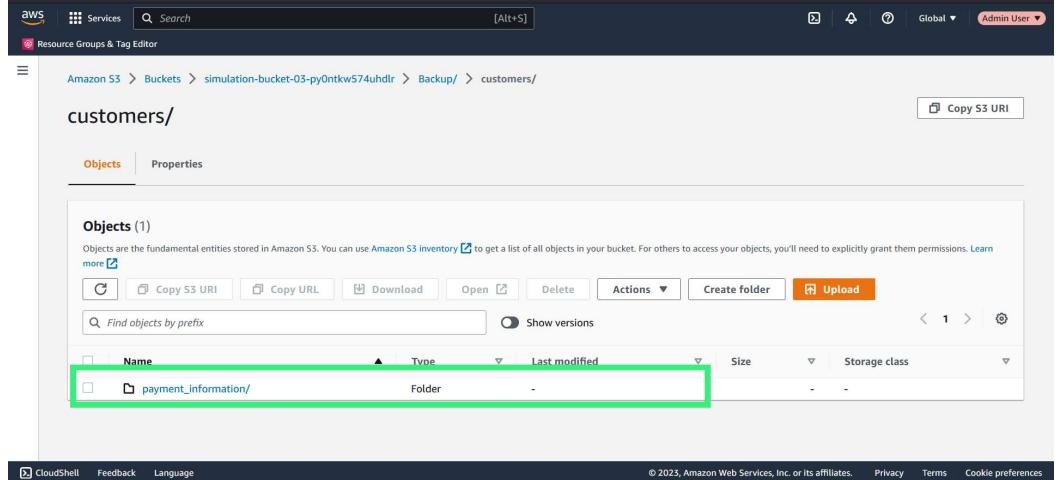


Steps	Content	Visual
Step 1:	<p>Earlier, we confirmed that the credit-card-data.csv object was taken and deleted from the S3 bucket simulation-bucket-03-8lonc4g9dwxzrbim located in the backup/customers/payment_information/ folder.</p> <p>Let's restore this file. From the AWS Management Console:</p> <ol style="list-style-type: none"> 1. In the search field, enter S3. 2. Under Services, choose S3. 	
Step 2:	<p>The S3 Buckets page displays. In the Find buckets by name text field, enter simulation-bucket-03-8lonc4g9dwxzrbim.</p>	



Steps	Content	Visual
Step 3:	In the Buckets section, choose simulation-bucket-03-8lonc4g9dwxzrbim .	
Step 4:	On the Objects tab, choose Backup/ .	



Steps	Content	Visual
Step 5:	In the Backup/ folder, choose customers/ .	
Step 6:	In the customers/ folder, choose payment_information/ .	



Recover

Use the Amazon S3 console to restore files to a previous version.

Steps	Content	Visual																																				
Step 7:	The payment information folder displays. Because the threat actors deleted the credit-card-data.csv file, this folder no longer shows that object. To see previous versions of objects in this folder, select Show versions .																																					
Step 8:	Select credit-card-data.csv with Delete marker type, and then choose Delete . Note: A delete marker in Amazon S3 is a placeholder (or marker) for a versioned object that was named in a simple delete request.	<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Version ID</th> <th>Last modified</th> <th>Size</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>credit-card-data.csv</td> <td>Delete marker</td> <td>Vq6vtHySLmUW5VlXD_hmesk8wjWWHI_</td> <td>June 14, 2023, 13:32:43 (UTC-05:00)</td> <td>0 B</td> <td>-</td> </tr> <tr> <td>credit-card-data.csv</td> <td>CSV</td> <td>N1Z7GMU-6-MOe=VAhu+mtMCAdwIMs5k</td> <td>June 14, 2023, 13:31:10 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>CSV</td> <td>QcV87GVJY0vEErAOGHwHc_JXZo6sN7y</td> <td>June 14, 2023, 13:30:37 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>CSV</td> <td>2xut1vgumfuVabmJ1kZqYWRsbmF5kWkv</td> <td>June 14, 2023, 13:30:08 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>CSV</td> <td>kjPfG_4kYBaegWv7tFd9WipG6Bnqc</td> <td>June 14, 2023, 13:28:56 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> </tbody> </table>	Name	Type	Version ID	Last modified	Size	Storage class	credit-card-data.csv	Delete marker	Vq6vtHySLmUW5VlXD_hmesk8wjWWHI_	June 14, 2023, 13:32:43 (UTC-05:00)	0 B	-	credit-card-data.csv	CSV	N1Z7GMU-6-MOe=VAhu+mtMCAdwIMs5k	June 14, 2023, 13:31:10 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	CSV	QcV87GVJY0vEErAOGHwHc_JXZo6sN7y	June 14, 2023, 13:30:37 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	CSV	2xut1vgumfuVabmJ1kZqYWRsbmF5kWkv	June 14, 2023, 13:30:08 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	CSV	kjPfG_4kYBaegWv7tFd9WipG6Bnqc	June 14, 2023, 13:28:56 (UTC-05:00)	26.0 B	Standard
Name	Type	Version ID	Last modified	Size	Storage class																																	
credit-card-data.csv	Delete marker	Vq6vtHySLmUW5VlXD_hmesk8wjWWHI_	June 14, 2023, 13:32:43 (UTC-05:00)	0 B	-																																	
credit-card-data.csv	CSV	N1Z7GMU-6-MOe=VAhu+mtMCAdwIMs5k	June 14, 2023, 13:31:10 (UTC-05:00)	26.0 B	Standard																																	
credit-card-data.csv	CSV	QcV87GVJY0vEErAOGHwHc_JXZo6sN7y	June 14, 2023, 13:30:37 (UTC-05:00)	26.0 B	Standard																																	
credit-card-data.csv	CSV	2xut1vgumfuVabmJ1kZqYWRsbmF5kWkv	June 14, 2023, 13:30:08 (UTC-05:00)	26.0 B	Standard																																	
credit-card-data.csv	CSV	kjPfG_4kYBaegWv7tFd9WipG6Bnqc	June 14, 2023, 13:28:56 (UTC-05:00)	26.0 B	Standard																																	



Steps	Content	Visual
Step 9:	The delete objects page displays. Scroll down to the Permanently delete objects? section. Enter permanently delete , and then choose Delete objects .	
Step 10:	The Delete objects: status page displays with a status message indicating that objects have been deleted. Choose Close .	



Recover

Use the Amazon S3 console to restore files to a previous version.

Steps	Content	Visual																														
Step 11:	<p>Now, in the Objects section of the payment information screen, select Show versions.</p>	<p>The screenshot shows the AWS S3 console with the path 'payment_information/'. The left sidebar has 'Buckets' and 'Storage Lens' sections. The main area shows one object, 'credit-card-data.csv'. Below the object list is a 'Actions' dropdown and a 'Create folder' button. A green box highlights the 'Show versions' button in the top right of the object list area.</p>																														
Step 12:	<p>You can now review the files in the folders.</p> <p>The payment_information folder now shows the credit-card-data.csv object, confirming that it has been successfully restored.</p>	<p>The screenshot shows the AWS S3 console with the path 'payment_information/'. The left sidebar has 'Buckets' and 'Storage Lens' sections. The main area shows four versions of the 'credit-card-data.csv' object. Each version has a unique version ID and timestamp. A green box highlights the entire list of objects in the table.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Version ID</th> <th>Last modified</th> <th>Size</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>credit-card-data.csv</td> <td>csv</td> <td>h13765WzfVM96zVAhu.mtWCAYlxMqSk</td> <td>June 14, 2023, 13:31:10 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>csv</td> <td>QcV87GVJY0vEEEAOGHwHc_JXZo6sN7y</td> <td>June 14, 2023, 13:30:37 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>csv</td> <td>2xut1vgumfuVAbmJ1kZqYWRsbmF5KWk</td> <td>June 14, 2023, 13:30:08 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> <tr> <td>credit-card-data.csv</td> <td>csv</td> <td>kjPffG_4kY8iaeWv7tFd9vWipG6Bnqc</td> <td>June 14, 2023, 13:28:56 (UTC-05:00)</td> <td>26.0 B</td> <td>Standard</td> </tr> </tbody> </table>	Name	Type	Version ID	Last modified	Size	Storage class	credit-card-data.csv	csv	h13765WzfVM96zVAhu.mtWCAYlxMqSk	June 14, 2023, 13:31:10 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	csv	QcV87GVJY0vEEEAOGHwHc_JXZo6sN7y	June 14, 2023, 13:30:37 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	csv	2xut1vgumfuVAbmJ1kZqYWRsbmF5KWk	June 14, 2023, 13:30:08 (UTC-05:00)	26.0 B	Standard	credit-card-data.csv	csv	kjPffG_4kY8iaeWv7tFd9vWipG6Bnqc	June 14, 2023, 13:28:56 (UTC-05:00)	26.0 B	Standard
Name	Type	Version ID	Last modified	Size	Storage class																											
credit-card-data.csv	csv	h13765WzfVM96zVAhu.mtWCAYlxMqSk	June 14, 2023, 13:31:10 (UTC-05:00)	26.0 B	Standard																											
credit-card-data.csv	csv	QcV87GVJY0vEEEAOGHwHc_JXZo6sN7y	June 14, 2023, 13:30:37 (UTC-05:00)	26.0 B	Standard																											
credit-card-data.csv	csv	2xut1vgumfuVAbmJ1kZqYWRsbmF5KWk	June 14, 2023, 13:30:08 (UTC-05:00)	26.0 B	Standard																											
credit-card-data.csv	csv	kjPffG_4kY8iaeWv7tFd9vWipG6Bnqc	June 14, 2023, 13:28:56 (UTC-05:00)	26.0 B	Standard																											