

Integrating AWS Cloudtrail with XDR Dashboard

https://campus.barracuda.com/doc/96767287/

The steps below outline integration between AWS CloudTrail and XDR Monitoring. AWS CloudTrail service helps monitor governances, compliance, and operational and risk auditing of AWS accounts. Customers who are looking to monitor their AWS environment should follow the implementation instructions listed below to enable XDR to monitor their AWS environment in real time.

To integrate AWS Cloudtrail

- If your Trail isn't set up, follow this link to set up a trail within cloudtrail: <u>https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trailusing-the-console-first-time.htm</u>
- 2. Ensure the trail is logging to a S3 Bucket. If you edit the trail, you can see the name of the bucket it's writing log files to. Take note of the S3 Bucket Name:

rail name nter a display name for your trail.			
skoutcloudtrail			
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.			
- 128 characters. Only letters, numbers, per			
Enable for all accounts in my orga oreview accounts in your organization, ope torage location Info	nization en AWS Organizations. See all accounts 🔀		
Enable for all accounts in my orga o review accounts in your organization, ope torage location Info Create new S3 bucket Create a bucket to store logs for the	nization en AWS Organizations. See all accounts [2] Use existing S3 bucket choose an existing bucket to store logs for this trail.		
Enable for all accounts in my orga o review accounts in your organization, ope torage location Info Create new S3 bucket Create a bucket to store logs for the rail log bucket name nter a new S3 bucket name and folder (pre	nization en AWS Organizations. See all accounts Use existing S3 bucket Choose an existing bucket to store logs for this trail.		

Replace with the name of the S3 Bucket that your CloudTrail is writing logs to Afterwards hit save and then take note of the URL of the SQS Queue

```
{
```

3.

"Version": "2012-10-17", "Id": "__default_policy_ID",



"Statement": [
{	
"Sid": "owner_statement",	,
"Effect": "Allow",	
"Principal": "*",	
"Action": "SQS:*",	
"Resource": " <sqs-queue-arm< th=""><th>N>",</th></sqs-queue-arm<>	N>",
"Condition": {	
"ArnLike": {	
"aws:SourceArn": '	<pre>"" arn:aws:s3:*:*:<bucket-name"< pre=""></bucket-name"<></pre>
}	
}	
}	
1	
}	
olastic integration logs	
elastic-integration-logs	
Name	Тире
Delastic-integration-logs	Standard
Encryption	URL
•	https://sqs.us-east-1.amazonaws.com/398991929182/elastic- interpreting lange
	integration-logs
▶ More	

4. Navigate to the S3 Bucket that your cloudtrail is writing logs to.

Click **Properties** > Scroll down to **Event Notifications** and click **Create event notification**. Type a name for the event name.

In **Event Types**, select everything to monitor all Cloudtrail updates.

For the **Destination**, enter the SQS queue you made.

Barracuda XDR



De	stination
	Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more
Des	stination
	Run a Lambda function script based on S3 events.
С	SNS topic Send notifications to email, SMS, or an HTTP endpoint.
0	SQS queue Send notifications to an SQS queue to be read by a server.
Spe	ecify SQS queue
С	Choose from your SQS queues
0	Enter SQS queue ARN
SQ	S queue
a	rn:aws:sqs:us-east-1:422354213072:ess-test

- For XDR to receive AWS SQS messages, an access key id and secret access key will need to be generated. A user permissioned in IAM with a role only allowed to read access from SQS queues:
 - $\circ\,$ Setting up a new user in IAM

- <u>https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-s</u> <u>etting-up.html</u>

 SQS IAM permissioning JSON's (Only need the SQS Send Message permission, first example)

-<u>https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-b</u> asic-examples-of-sqs-policies.html

- 6. Once completed, provide XDR the following information -
 - Queue Url: <u>https://sqs.us-east-1.amazonaws.com/123/test-queue</u>
 - Access key id
 - Secret Access Key



Figures

- 1. 1.png
- 2. 2.png
- 3. 3.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.