Amazon CloudTrail

CYBERARK ISI EVENT WRITER –
- AWS CLOUDTRAIL INTEGRATION

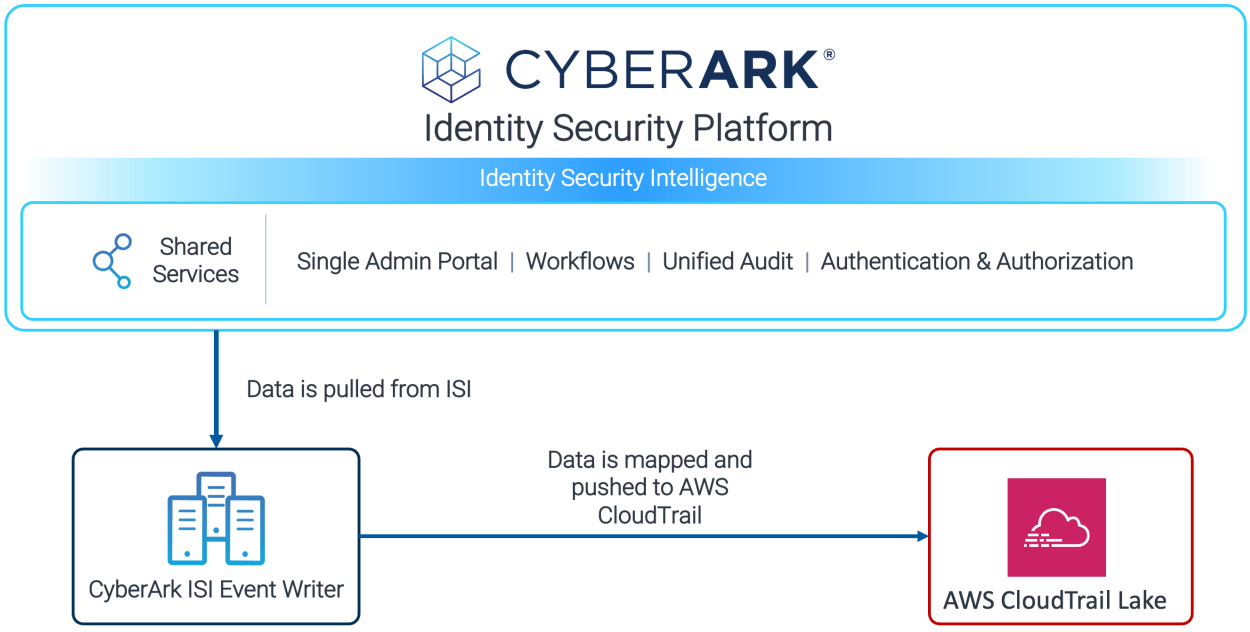
August 2022

1 CYBERARK ISI EVENT WRITER - INTEGRATION OVERVIEW

CyberArk Identity Security Intelligence, analyzes data collected from various sources and identifies patterns to detect threats and high-risk activities, combined with AWS CloudTrail Lake, which empowers organizations with an aggregate and immutable storage of events recorded by CloudTrail.

CloudTrail Lake simplifies activity log analysis by integrating collection, storage, optimization, and query in the same source. By consolidating these features into one environment, CloudTrail Lake eliminates the need for separate data processing pipelines that span across teams and products.

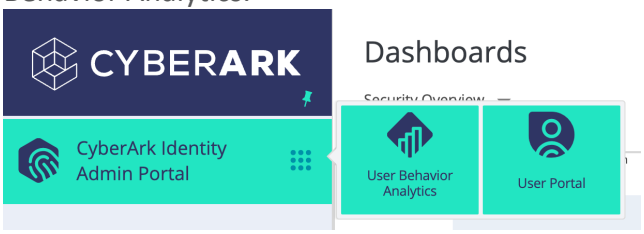
You can now use CloudTrail Lake to ingest activity logs from any source in your hybrid environments, making CloudTrail Lake the single source of immutable user and API activity logs for auditing and security investigations across hybrid environments. You can store, access, analyze, troubleshoot, and take action on this data without maintaining multiple log aggregators and reporting tools.



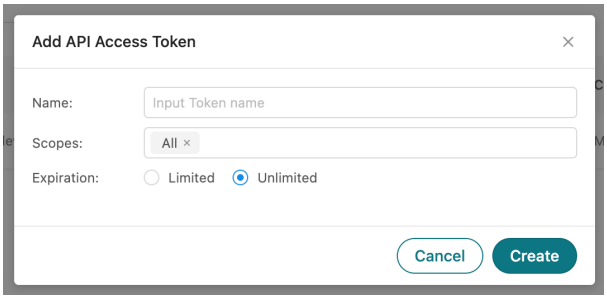
2 CREATE API TOKEN FOR CYBERARK IDENTITY

The integration requires to have an API token to be defined in CyberArk Identity.

- Sign into the CyberArk Identity Admin Portal and use the portal switcher to select User Behavior Analytics.



- Select Settings > API.
- Click New to create a new API token.



- Enter the following information and then click Create:

Field	Description
Name	Enter a name for the API token.
Scopes	Select **All** from the drop-down menu.
Expiration	Select **Unlimited** to reuse the same token. If you select Limited, the token expires, and the integration will not be able to pull the events after the indicated date is reached.

- Copy the API token you just created and then click **Done**.
  The API token is required the first time you run the integration.

3 ENABLE CYBERARK INTEGRATION VIA CLOUDTRAIL CONSOLE

Please follow the instructions defined in this link:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

to enable CyberArk Integration and create a channel. The channel ARN will be used to complete the integration.

4 CREATE A NEW IAM USER AND GRANT PERMISSION

The integration needs to have an IAM user to perform the operation of sending events to AWS CloudTrail. This user must have permissions to call the PutAuditEvents API. Apply a policy with the following permissions to the IAM user. This policy statement allows access to this user to call PutAuditEvents API for the Channel you have created via the CloudTrail Console in step 3.

This is a sample of what an IAM policy granting the necessary permissions to the IAM user might look like:

```
{
  "Effect": "Allow",
  "Action": "cloudtrail-data:PutAuditEvents",
  "Resource": "<Channel ARN>"
}
```

5 DOWNLOAD CYBERARK ISI EVENT WRITER

The CyberArk ISI Event Writer is available from CyberArk Marketplace. Download the zip file and unzip it for execution.

6 RUN THE CYBERARK ISI EVENT WRITER.

Below, find the instructions to run the CyberArk ISI Event Writer as a docker container standalone as an example, but it could also be adjusted to the infrastructure present in your environment.

Make sure to also understand the use of AWS IAM Roles Anywhere for workloads running outside of AWS (see https://docs.aws.amazon.com/rolesanywhere/latest/userguide/introduction.html)

- Locate the cyberark_isi_event_writer folder on your system and make sure there isn't a isi-event writer already located there.

  Command to delete the syslog-writer:

  > docker rm isi-event-writer

  Command to delete the syslog writer image:

  > docker rmi isi-event-writer:latest

- Load the docker image from the tar file.

  > docker load < isi-event-writer.tar.gz

- Run the following command with the IAM user you created in step 4:

  > docker run --name isi-event-writer -it --env AWS_ACCESS_KEY_ID=XXXXXXXXX --env AWS_SECRET_ACCESS_KEY=YYYYYYY --env AWS_DEFAULT_REGION=ZZZZ --net=host -v $HOME/Downloads/data:/home/cyberark-isi-event-writer/data isi-event-writer

  Make sure to provide the values for AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY, and AWS_DEFAULT_REGION

  Note: As best business practice, please follow the guidelines to avoid exposing keys and secrets as parameters. Please read about Summon here: https://cyberark.github.io/summon/

  And use a solution like the one described here: Summon Inject Secrets

- At the prompts, enter the following information (this is only required the first time you run the syslog writer):

Prompt	Description
Enter Tenant URL:	Type the Identity URL: https://<your tenant name>/admin To obtain your tenant name for the URL, login to the CyberArk Identity Admin Portal, Settings, and Tenant URLs and pick the original Tenant URL (the one you cannot remove or delete)
Enter API bearer token:	Paste the API token you copied earlier from the User Behavior Analytics Portal as described in section 2
Enable AWS CloudTrail Integration (yes/no):	Specify Yes to enable the integration with AWS CloudTrail
AWS Region [us-east-1]:	Enter the AWS Region to use for the integration with AWS CloudTrail
AWS Recipient Account ID:	Enter the AWS Recipient ID to use for the integration with AWS CloudTrail
Ingestion Channel ARN:	Enter the AWS Ingestion Channel ARN. A channel that allows a partner or source application to send events to an event data store in CloudTrail.

The CyberArk ISI Event Writer server should now be up and running.

Once, the integration is running and events data is being pushed to CloudTrail, you can use the following documentation to query the information:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/query-lake-examples.html