



CyberArk Audit to Amazon Security Lake Adapter

CYBERARK AUDIT TO AMAZON SECURITY LAKE ADAPTER INTEGRATION

Name of Company

Website

Name of Product

Version

Date

CyberArk

<https://www.cyberark.com>

CyberArk Audit to Amazon
Security Lake Adapter

2.0

March 2023

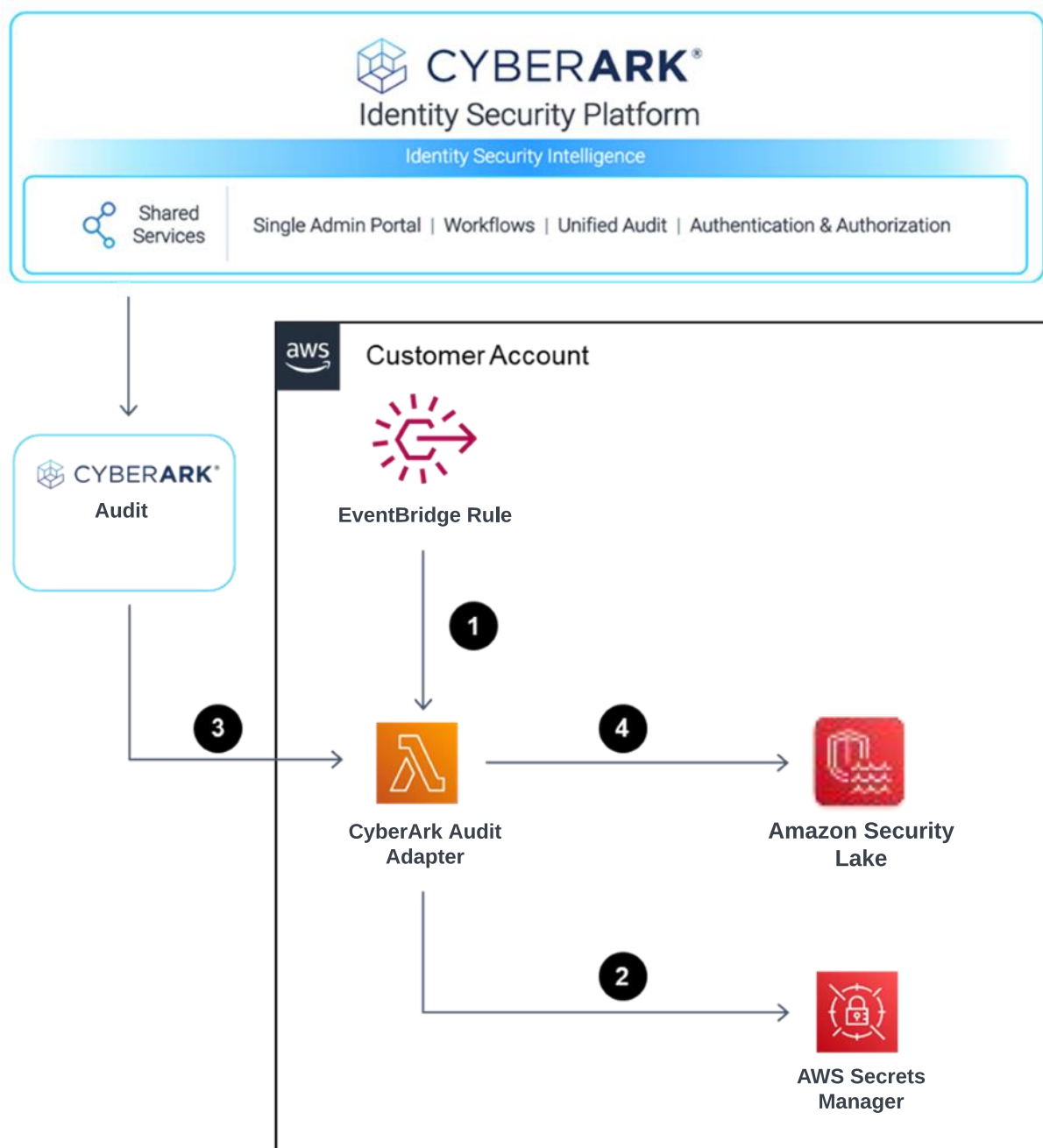
SOLUTION OVERVIEW

Organizations using CyberArk Identity Security products can streamline management of audit and security events for their IT environment compliance. CyberArk Audit transforms event information into Open Cybersecurity Schema Framework (OCSF) for consumption through Amazon Security Lake, which allows customers to build a security data lake from integrated cloud and on-premises data sources, as well as from their private applications. With support for the OCSF standard, Security Lake reduces the complexity and costs for customers to make their security solutions data accessible to address a variety of security use cases such as threat detection, investigation, and incident response.

Working together to mitigate advanced attacks, CyberArk Identity Security Platform and Amazon Security Lake position organizations to rapidly collect, detect, alert, and send findings to subscribers for further analytics.

CyberArk Audit Adapter, a Lambda function, collects security event information from CyberArk Identity Security Platform and provides the data to Amazon Security Lake in OCSF format. The deployed solution contains a Lambda function which is activated based on an EventBridge rule. This rule is invoked every five minutes to query the audit service which collects information from CyberArk Identity Security Platform as shown in the flow below:

1. Invoke AWS EventBridge rule every five minutes
2. Request CyberArk Audit Subscription Credential from AWS Secrets Manager
3. Query CyberArk Audit for new audits
4. Transform CyberArk Audits to OCSF format
5. Store transformed audits in Amazon Security Lake



Amazon Security Lake is a data lake for security logs built in the customer's account. It is designed to optimize the cost of storing and querying massive security log sources, while maintaining good query performance and compatibility.

CyberArk Audit is an adapter provided through the AWS CDK application and deployed in an Amazon Security Lake-empowered account. Once the adapter stack is deployed, the function — which is triggered by an event rule — is permitted to read secrets and write to the Amazon Security Lake S3 bucket in OCSF standard. This contains all the relevant fields with audit events.

INSTALLATION & INTEGRATION CONFIGURATION

Please follow the next sections to subscribe, install and configure the integration.

PREREQUISITES

- Python 3.8
- [AWS CDK](#)
- [Poetry](#) Python dependency manager
- Docker

CREATE NEW SUBSCRIPTION FOR CYBERARK AUDIT

1. Login to your CyberArk SaaS web console
2. Copy your session token
 - a. Open your browsers dev tools
 - b. Navigate to Application storage tab
 - c. Locate the cookies for the CyberArk SaaS site
 - d. Copy the value of the cookie named "idToken-<random UUID>"
3. Open Postman or another REST client
4. Create a new POST HTTP request
5. Endpoint URL:
`https://<your_subdomain>.cyberark.cloud/api/audit/audits/subscribers`
6. Optional request body:
`{"friendlyName": "<name for the new subscription>"}`
7. Paste the value of the session token into the authorization header.
The header should look like this:
`Authorization: "Bearer <Session token>"`
8. Send the request, the response contains authentication credentials and endpoint information for querying audits.
9. Copy the response

STORE SUBSCRIPTION CREDENTIALS IN AWS SECRETS MANAGER

1. Login to AWS Console at <https://console.aws.amazon.com>
2. Navigate to AWS Secrets Manager service
3. Click on the "Store a new secret" button
4. For secret type choose "Other type of secret"
5. For Key/value pairs, click on the Plaintext tab
6. Paste the response value of the audit subscription request from the previous section
7. Choose an encryption key that's appropriate for you, or keep the default key
8. Click on Next
9. For the secret name, choose a name that matches your naming convention
10. Click on Next
11. There is no need for rotation, click on Next
12. Confirm the settings and store the credentials by clicking on the Store button
13. Copy the secret name that was created

REGISTER AMAZON SECURITY LAKE CUSTOM SOURCE

Follow Amazon Security Lake documentation and register a new custom source.
Register a source for the following event classes:

- `ENTITY_AUDIT`

Copy the S3 prefix that Amazon Security Lake creates for the event classes.

SET UP CYBERARK AMAZON SECURITY LAKE ADAPTER

Initialize Environment

1. Open a new terminal window and navigate to the unzipped project folder
2. Run the following command to create a python virtual environment and install dependencies:
`poetry install`

Update Context Parameters

3. Open the file `cdk.json` in a text editor
4. Locate the parameter `audits-subscription-secret-name` and replace the value placeholder with the path to the Audit subscription credentials that you stored in AWS Secrets Manager
5. Locate the parameter `event-class-to-s3-prefixes-mapping`, update the S3 prefix for each event type according to the S3 prefix returned by Amazon Security Lake.
6. **[Optional]** Using a KMS key to encrypt S3 objects – Locate the parameter `s3-kms-key-arn`, update the value with the ARN of the KMS key that will be used to encrypt S3 objects. Leave empty if you wish to use S3 SSE.

Deploy to AWS Account

7. Open a new terminal and navigate to the project folder
8. Activate the python virtual environment by running:
`poetry shell`
9. Make sure you are logged in to your AWS account and that your AWS CLI configured with the correct profile and credentials.
10. Deploy the CDK project to your account by running:
`cdk deploy`
11. Follow the prompts from the CDK CLI

Once deployed the adapter lambda will be triggered every 5 minutes, query CyberArk SaaS for new audits, transform them to OCSF format, deliver the events to the correct S3 path according to the event class.

TROUBLESHOOTING

The adapter lambda function writes log events to Amazon CloudWatch. If you encounter issues while running the adapter or find that audit events are not delivered to Amazon Security Lake, check the Amazon CloudWatch log for errors and refer to the following table for possible solutions.

Error	Solution
Failed to read CyberArk's Audit service subscription data	There is an issue with the Audit's service subscription data stored in AWS Secrets Manager. Try to create a new subscription using CyberArk Audit Service and store the subscription data again in AWS Secrets Manager.
Failed to get audits page, response code [401]	There is an issue with the Audit's service subscription data stored in AWS Secrets Manager. Try to create a new subscription using CyberArk Audit Service and store the subscription data again in AWS Secrets Manager.
Failed to transform audit, OCSF schema validation error. Audit type [<AuditType>]	There is a error when trying to convert audits of type <AuditType> to OCSF schema events. Please contact CyberArk support.
Failed to write security events to S3	Check lambda functions permissions and Amazon Security Lake S3 bucket policy. Make sure the lambda function is allowed to write object to the S3 bucket and bucket policy does not deny the lambda function from writing objects.
Lambda function execution timed out	Edit the function configuration and increase the max timeout

OCSF TO CYBERARK AUDIT ATTRIBUTE MAPPING

The following tables describe the mapping between OCSF objects attributes and CyberArk audit attributes.

OCSF Entity Audit Attribute	CyberArk Audit Attribute	CyberArk to OCSF Value mapping
activity_name	actionType	• Create – Created • Trust added – Created • Download – Read • Edit – Updated • Suspend – Updated • Active – Updated • Delete - Deleted
activity_id	actionType	• Create – 1 • Trust added – 1 • Download – 2 • Edit – 3 • Suspend – 3 • Active – 3 • Delete - 4

time	Timestamp	
message	message	
severity	auditType	
severity_id	auditType	Info – 1 Informational
status	action	
type_uid	actionType	- Create – 300401 - Trust added – 300401 - Download – 300402 - Edit – 300403 - Suspend – 300403 - Active – 300403 - Delete - 300404
type_name	actionType	- Create – Created - Trust added – Created - Download – Read - Edit – Updated - Suspend – Updated - Active – Updated - Delete - Deleted

OCSF Managed Entity Attribute	CyberArk Audit Attribute
name	auditCode Possible values: - DPA Policy - DPA Connector - DPA Connector Script - DPA Connector Pool - SSH CA Public Key - Certificate - Certificate Script - Trust - AWS Account - Azure Subscription - Windows Domain
data	customData

OCSF Product Attribute

CyberArk Audit Attribute

uid	applicationCode
name	serviceName
feature	component

MAINTENANCE & SCHEMA UPDATES

Newer versions of the adapter may be released with support for new audit types, bug fixes, and OCSF schema updates.

The versions will be released to the CyberArk marketplace.

To update to the newer version, take the following steps:

12. Download the newer adapter version from CyberArk marketplace
13. Extract the downloaded archive to a folder
14. Copy the cdk.json file from the older version to the extracted folder
15. Redeploy the adapter to your AWS account

Additional steps may be included in the version release notes.

CONTACT INFO

Business Contact	Name	CyberArk Business Development
	Email	Business_Development@cyberark.com
Technical Contact	Name	Business Development Technical Team
	Email	BizDevTech@cyberark.com

SUPPORT

Contact	Email	support@cyberark.com
	Support Portal	https://cyberark-customers.force.com/s/login/
Phone	Americas	+1-617-663-0300
	Americas and Canada Toll Free	+1-844-537-7700
	Europe, Middle East & Africa	+44-203-7287074
	Asia Pacific & Japan	+65-6460-4254
	Israel	+972-3-9180011
	Australia	+61-1800-290865

