# Integrating Cyera DSPM Platform with Google Security Command Center

\*Enhancing Cloud Security with Automated Threat Detection and Response\*

## Introduction

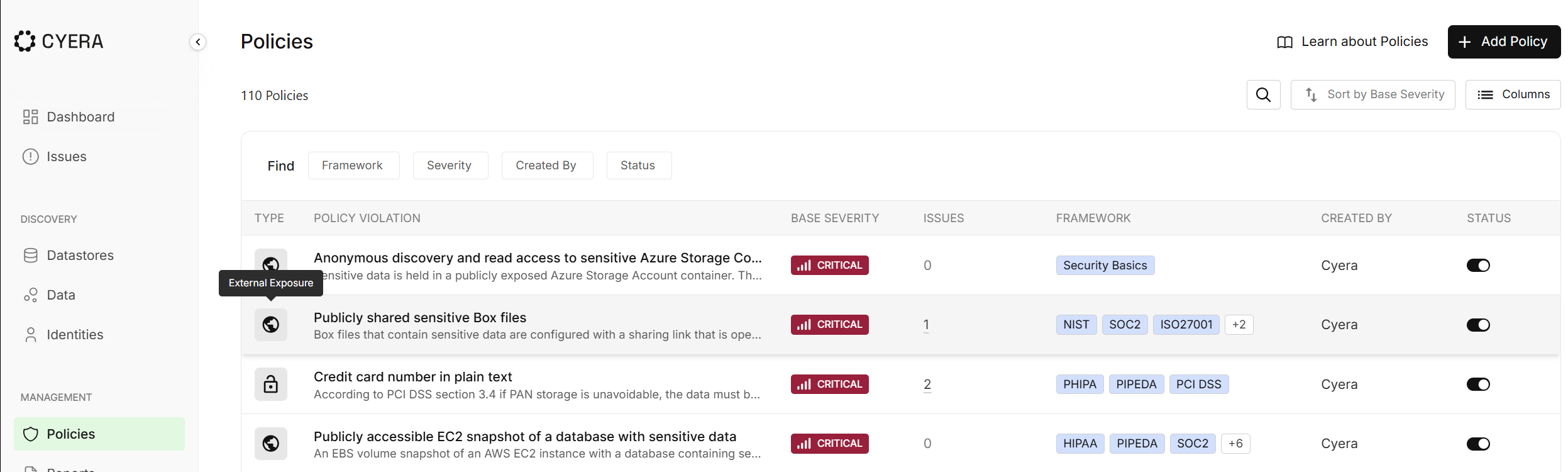
In today’s cloud-native environment, data security is paramount. Organizations must identify, classify, and protect sensitive data across multiple cloud platforms while ensuring compliance with regulations. Cyera’s Data Security Posture Management (DSPM) platform helps businesses gain real-time insights into their data security posture.  
  
Integrating Cyera with Google Security Command Center (SCC) enables organizations to increase visibility into their data security landscape across multiple cloud services and datastores. Cyera DSPM platform can deliver findings to the Google Security Command Center (SCC) which reflects organization’s compliance to extensive range of Cyera’s policies.

Policies are used to identify potential data security vulnerabilities, unauthorized access to the organization's sensitive data, breaches and violations of data security laws and regulations such as PCI DSS, GDPR, HIPAA. LGPD, and PIPEDA, to name a few.

Examples of policies include:

* Credentials in plain text
* Credit card number in plain text
* Google Drive Files containing sensitive data are shared publicly
* Google Drive Files containing sensitive data are shared across the organization
* Google Drive Files containing sensitive data are shared with an external organization that is not explicitly allowed
* Publicly shared sensitive data on Google Drive
* Sensitive data is accessible to anonymous users
* Unencrypted sensitive data in Azure SQL database
* Publicly shared sensitive Microsoft 365 files
* Anonymous discovery and read access to sensitive Azure Storage Container files
* Sensitive data is accessible to stale or external users

A policy consists of some details such as its name, description, severity and frameworks it applies to, and a collection of conditions. When Cyera detects data that meets all of a policy’s conditions, the policy is triggered and an issue for that data is created and displayed in the Cyera platform.



This blog post outlines the end-to-end integration process, proposed architecture, and deployment instructions.

## 📌 Proposed Architecture

The integration leverages Google Cloud Functions, Pub/Sub, and Cloud Scheduler to periodically pull security findings from Cyera and forward them to Google Security Command Center (SCC). Below is an overview of the architecture:

1. Cloud Scheduler triggers a Cloud Function every minute via Pub/Sub.

2. The Cloud Function fetches security findings from Cyera API.

3. Findings are processed and formatted to align with SCC’s schema.

4. Findings are ingested into Google SCC, enabling threat correlation and automated security analysis.

High level architecture diagram of the proposed solution is shown below. This example covers Cyera delivering findings related to AWS datastores, such as Amazon S3 and RDS. However, since Cyera has capability to assess data posture across multiple environments and platforms (AWS, Azure and on premises) this solution applies to other platforms as well.

A diagram of a computer security system

AI-generated content may be incorrect.

## 📖 Deployment Instructions

Below are the detailed steps to set up and deploy the integration.

### 1️. Prerequisites

Before deployment, ensure:

* ✅ You have access to Google Cloud Console.
* ✅ A Google Cloud project is set up.
* ✅ Google Cloud SDK (`gcloud CLI`) is installed.
* ✅ Cyera Tenant is deployed and issues are generated in Cyera tenant
* ✅ Cyera API credentials are available. For detailed instructions on generating Cyera CLIENT\_ID and CLIENT\_SECRET consult Cyera documentation.

### 2️. Enable Required APIs

Run the following command to enable necessary Google Cloud APIs:

```sh  
gcloud services enable cloudfunctions.googleapis.com \  
 secretmanager.googleapis.com \  
 securitycenter.googleapis.com \  
 cloudresourcemanager.googleapis.com \  
 cloudscheduler.googleapis.com \  
 pubsub.googleapis.com  
```

### 3️. Store Cyera API Credentials Securely

Use Google Secret Manager to store sensitive credentials:

```sh  
gcloud secrets create CLIENT\_ID --replication-policy="automatic"  
gcloud secrets create CLIENT\_SECRET --replication-policy="automatic"

### 4️. Set Up Pub/Sub for Triggering the Function

Create a Pub/Sub topic:

```sh  
gcloud pubsub topics create cyera-trigger  
```

### 5️. Grant the Cloud Function service account required permissions on the Organization and Project level

1. Grant access to secrets in Secret Manager

gcloud secrets add-iam-policy-binding CLIENT\_ID \

--member="serviceAccount:<YOUR\_SERVICE\_ACCOUNT>" \

--role="roles/secretmanager.secretAccessor"

gcloud secrets add-iam-policy-binding CLIENT\_SECRET \

--member="serviceAccount:<YOUR\_SERVICE\_ACCOUNT>" \

--role="roles/secretmanager.secretAccessor"

1. Grant SCC Admin role on project level

gcloud secrets add-iam-policy-binding <PROJECT\_ID> \

--member="serviceAccount:<YOUR\_SERVICE\_ACCOUNT>" \

--role="roles/secretmanager.admin"

1. Grant SCC Admin role on Organization level

gcloud secrets add-iam-policy-binding <ORGANIZATION\_ID> \

--member="serviceAccount:<YOUR\_SERVICE\_ACCOUNT>" \

--role="roles/secretmanager.admin"

1. Grant Organization Viewer role

gcloud secrets add-iam-policy-binding <ORGANIZATION\_ID> \

--member="serviceAccount:<YOUR\_SERVICE\_ACCOUNT>" \

--role="roles/ resourcemanager.organizationViewer"

Replace <YOUR\_SERVICE\_ACCOUNT> with your actual **service account email**.

Replace <PROJECT\_ID> with the ID of the project where cloud function will be deployed

Replace <ORGANIZATION\_ID> with ID of your organization

### 6. Set up Cloud Scheduler to invoke the function every 10 minutes

The scheduler may be adjusted to invoke function at any interval using CRON expressions

gcloud scheduler jobs create pubsub cyera-scheduler-job \

--schedule="\*/10 \* \* \* \*" \

--time-zone="UTC" \

--topic=cyera-trigger \

--message-body="Triggering cyera-to-scc function" \

--location=us-central1

### 7. Deploy the Cloud Function

Create a `[requirements.txt](https://github.com/cyeragit/Google-SCC-Integration/blob/main/requirements.txt)` file with the necessary Python dependencies:

```txt  
requests

google-cloud-securitycenter

google-cloud-secret-manager

google-cloud-resource-manager

google-auth

google-auth-oauthlib

google-auth-httplib2

google-api-core

protobuf

```

Deploy the function with the following command. Ensure that the Cloud Function file is called [**main.py**](https://github.com/cyeragit/Google-SCC-Integration/blob/main/main.py)**.**

gcloud functions deploy cyera-to-scc \

--runtime python310 \

--trigger-topic cyera-trigger \

--entry-point cloud\_function\_entry \

--memory 512MB \

--region us-central1 \

--timeout 60s \

--service-account <YOUR\_SERVICE\_ACCOUNT>

Ensure that **Cloud Function Service Account** has the required Pub/Sub permissions:

### 8. Verify Deployment

Once deployed:

* ✅ Check logs in Google Cloud Console under Cloud Functions.
* ✅ Verify Pub/Sub messages are triggering the function.
* ✅ Check if findings appear in Google SCC under Security Findings.

If the deployment is successful, the new Source named “Cyera Issues” is added to the Security Command Center Sources section

A screenshot of a computer

AI-generated content may be incorrect.

Following the Cyera Issues link opens the findings in SCC that were generated based on the Cyera issues:

A screenshot of a computer

AI-generated content may be incorrect.

Opening individual findings reveals the following properties:

* Description
* State
* Severity
* Event time
* Create time
* Category

A screenshot of a computer

AI-generated content may be incorrect.

Displaying the Source Properties shows

* Cyera datastore name
* Cyera datastore provider
* Cyera datastore sensitivity
* Cyera datastore type

A screenshot of a computer

AI-generated content may be incorrect.

## 📢 Conclusion

By integrating Cyera DSPM with Google SCC, security teams can:  
✔ Automate threat detection by ingesting security findings into SCC.  
✔ Enhance visibility into data security risks across cloud environments.  
✔ Improve incident response with real-time security alerts and correlation.  
  
This integration ensures proactive security posture management while simplifying compliance monitoring.  
  
🚀 Secure your cloud with Cyera + Google SCC today! 🚀