

CyTech Aquila - Cloud Security Posture Management (CSPM) Module

Cloud Security Posture Management (CSPM)

Overview:

CSPM helps secure your cloud infrastructure by discovering and evaluating cloud services (e.g., storage, compute, IAM) against CIS benchmarks to identify and remediate configuration risks that may affect data confidentiality, integrity, and availability.

Key Features:

- **Cloud Provider Support:** Compatible with **AWS**, **GCP**, and **Microsoft Azure**.
- **Evaluation Frequency:** Resources are evaluated every **24 hours** using **read-only credentials**.
- **Findings & Dashboards:**
 - High-level insights in the **Cloud Security Posture dashboard**.
 - Detailed findings available on the **Findings page**.

Pre-requisites

1. Access to CyTech - Aquila

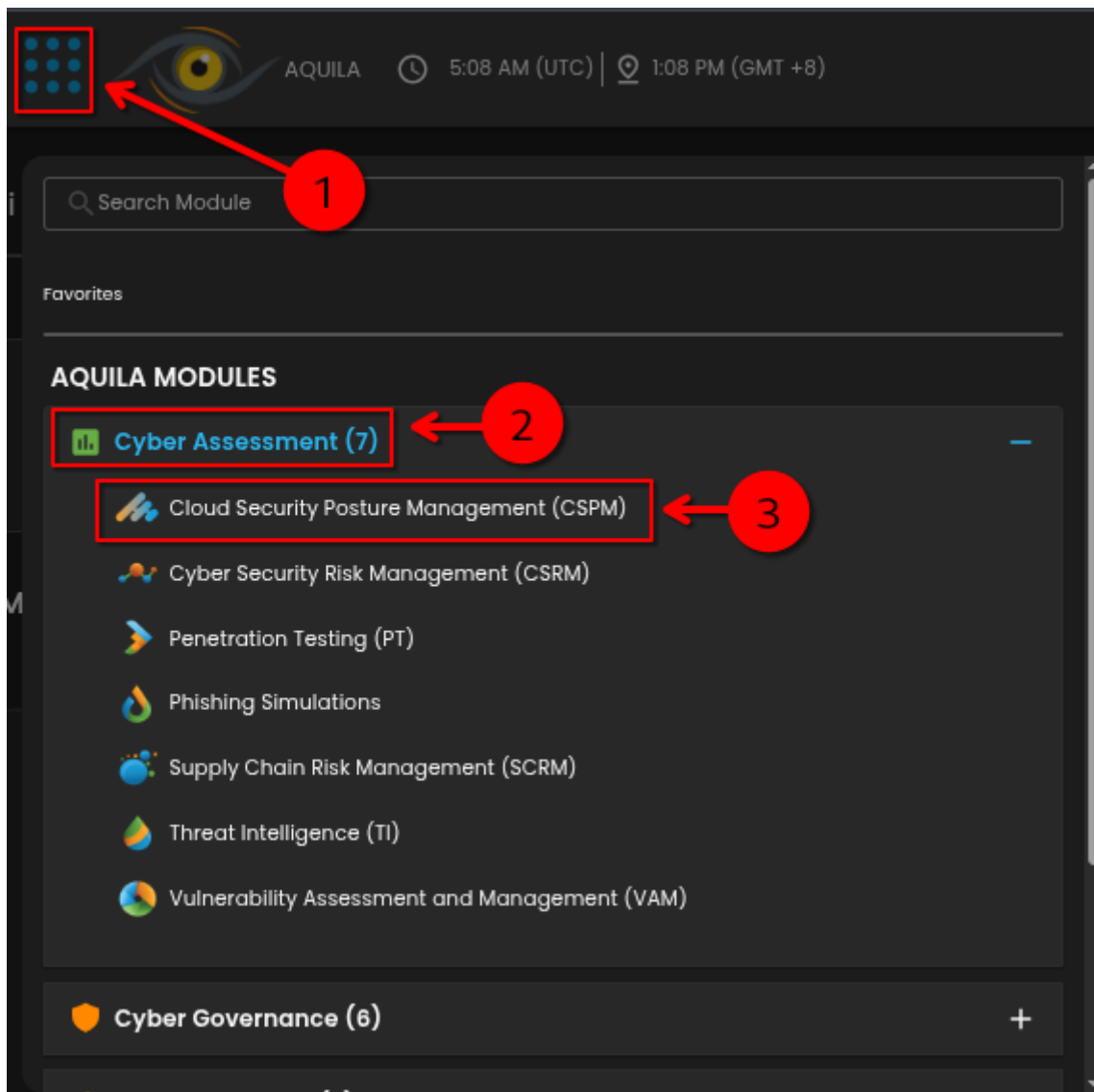
- Only users assigned the "**Owner**" or "**Admin**" role can access the Log Collector installation resources within the platform.

To navigate to CSPM Module please follow the instructions below:

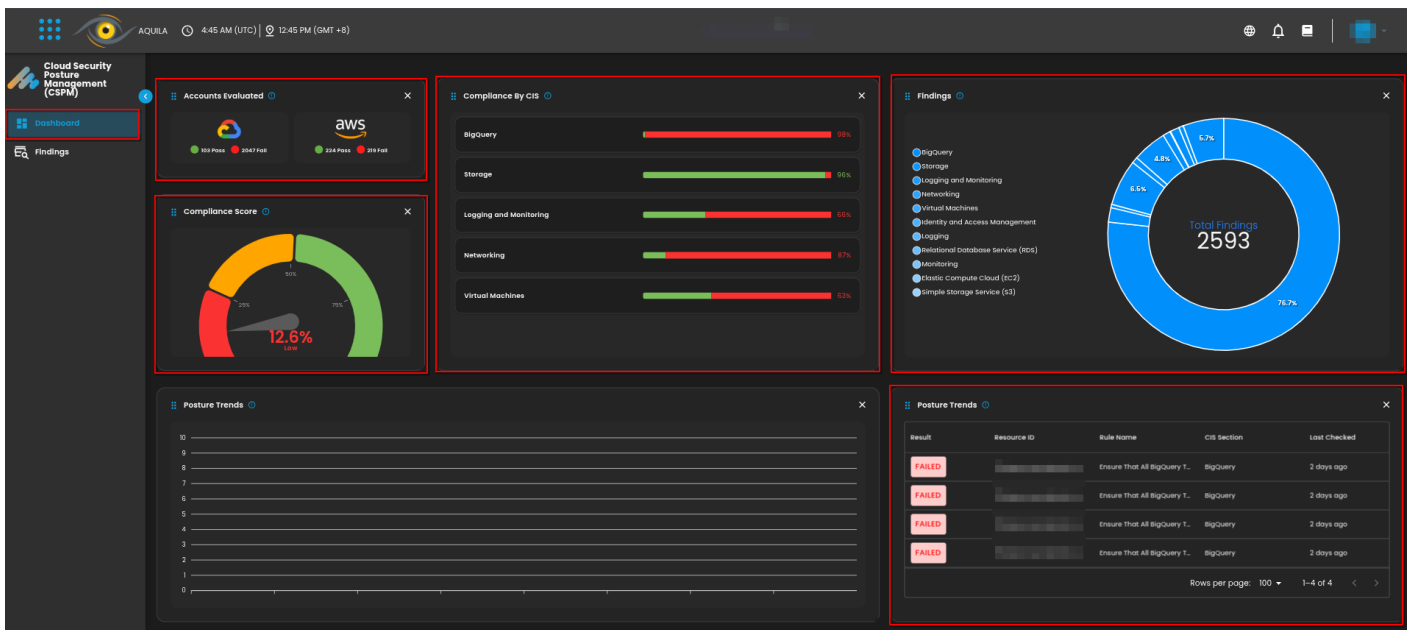
Step1: Log in to CyTech - Aquila. Click here: cytechint.io . Click the icon  to display the Aquila Modules.

Step2: Click on Cyber Assessment.

Step3: Choose Cloud Security Posture Management (CSPM).



Here in the CSPM Dashboard you can view all the evaluations. Such as Account Evaluated, Compliance Score, Compliance by Center in Internet Security (CIS), Findings and Posture Trends.



1. Account Evaluated:

- This refers to the specific cloud accounts that have been assessed for security compliance. An "account" in this context typically represents a collection of cloud resources under a single administrative domain within a cloud service provider (e.g., an AWS account, an Azure subscription). Evaluating an account involves checking its resources and configurations against security benchmarks.

2. Compliance Score:

- The compliance score is a metric that indicates how well a cloud account or resource adheres to predefined security benchmarks, such as those set by the Center for Internet Security (CIS). It is usually expressed as a percentage, with a higher score indicating better compliance. This score helps organizations quickly assess their security posture and identify areas needing improvement.

3. Compliance by Center for Internet Security (CIS):

- This refers to the evaluation of cloud resources against the security guidelines and best practices defined by the CIS benchmarks. These benchmarks provide a set of controls and recommendations to secure cloud environments. Compliance by CIS helps organizations ensure their configurations align with industry standards for security.

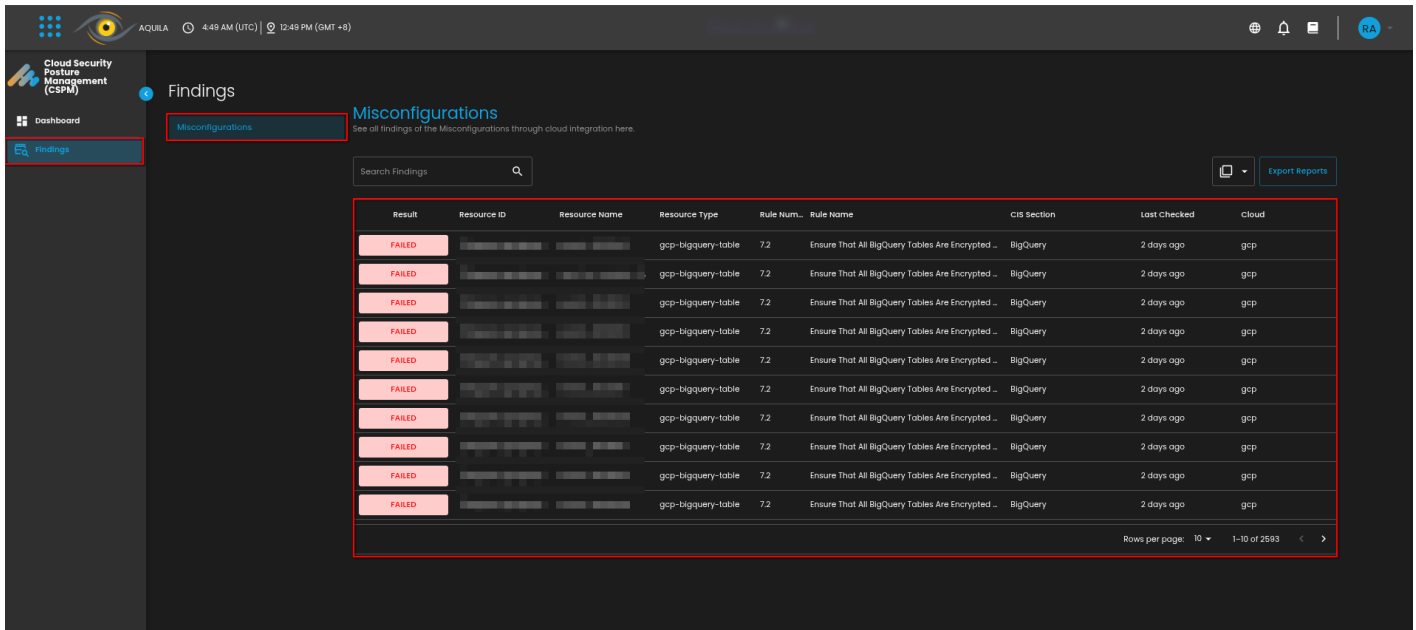
4. Findings:

- Findings are the results of the security assessments conducted by the CSPM module. They detail specific issues or misconfigurations identified during the evaluation process. Each finding typically includes information about the affected resource, the nature of the issue, its severity, and recommended remediation steps.

5. Posture Trends:

- Posture trends refer to the analysis of changes in security posture over time. This involves tracking improvements or regressions in compliance scores and findings. Understanding posture trends helps organizations identify patterns, measure the effectiveness of their security initiatives, and make informed decisions about future security strategies.

In the Findings Dashboard - it shows you all the detailed misconfigurations evaluated by our CSPM Module. Here you view the Result, Resource ID, Resource Name, Resource Type, Rule Number, Rule Name, CIS Section, Last Checked and Cloud.



Result	Resource ID	Resource Name	Resource Type	Rule Num.	Rule Name	CIS Section	Last Checked	Cloud
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp
FAILED			gcp-bigquery-table	7.2	Ensure That All BigQuery Tables Are Encrypted ..	BigQuery	2 days ago	gcp

1. **Result:**

- The result indicates the outcome of a security assessment for a specific rule or check. It typically shows whether the resource passed or failed the evaluation based on compliance with the security benchmark.

2. **Resource ID:**

- This is a unique identifier assigned to a specific cloud resource within an account. The Resource ID helps in precisely identifying and referencing the resource in security assessments and reports.

3. **Resource Name:**

- The resource name is the human-readable name assigned to a cloud resource. It helps users easily identify and manage resources within their cloud environment.

4. **Resource Type:**

- This refers to the category or kind of cloud resource being evaluated, such as a virtual machine, storage bucket, database instance, etc. Understanding the resource type is crucial for applying the correct security checks and benchmarks.

5. **Rule Number:**

- The rule number is a unique identifier for a specific security rule or check within a benchmark. It helps users quickly reference and locate the rule in documentation or reports.

6. **Rule Name:**

- The rule name provides a descriptive title for a security rule or check. It summarizes the purpose or focuses of the rule, such as "Ensure encryption is enabled for storage buckets."

7. **CIS Section:**

- CIS Sections refer to categories of security best practices defined by the Center for Internet Security (CIS) benchmarks. These sections group related security controls and guidelines that help ensure cloud resources are configured securely.

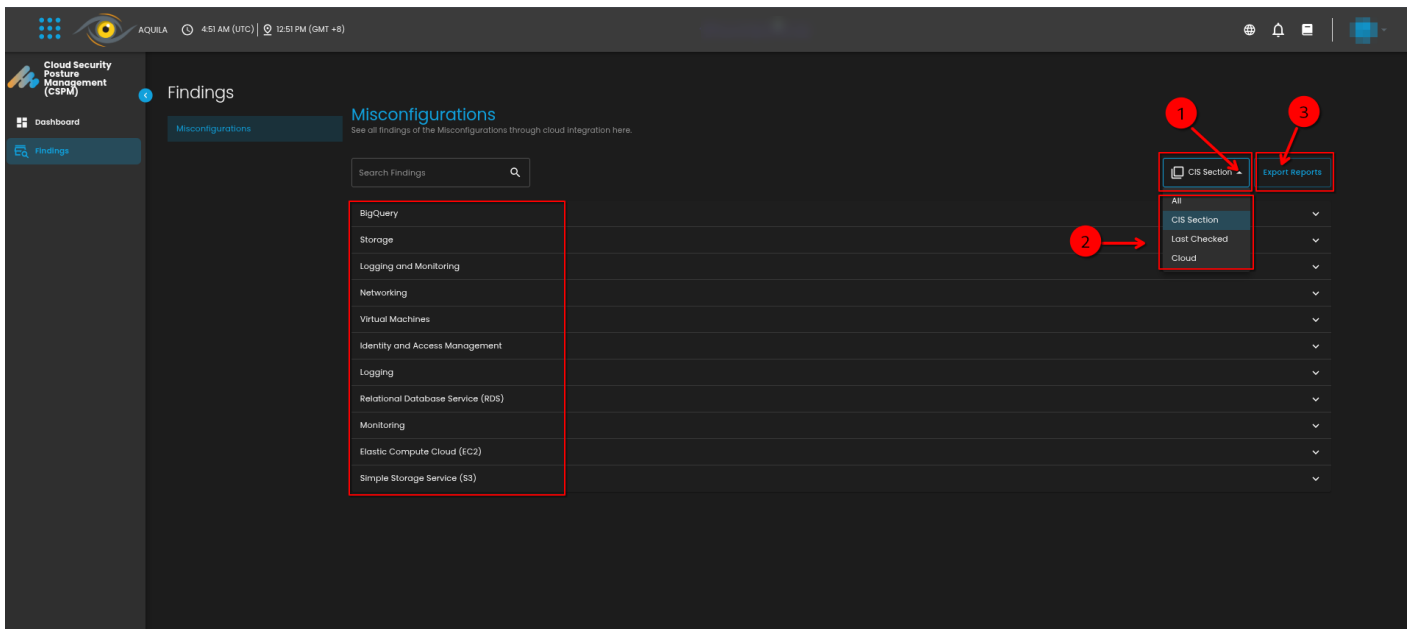
8. Last Checked:

- This indicates the most recent time when a particular resource or configuration was assessed for compliance with security benchmarks. It helps users understand how up to date the security posture information is.

9. Cloud:

- In CSPM, "Cloud" refers to the specific cloud service provider or environment being assessed. This could include platforms like AWS, Azure, or Google Cloud. The CSPM module evaluates resources within these cloud environments against security benchmarks.

Navigate through the leftmost button as highlighted in the image.



Step1: By clicking the box icon's drop-down button, it will show options to display desired findings.

Step2: Choose desired output.

1. All:

- This typically refers to a view or filter option that allows users to see all available data or findings within the CSPM module. It provides a comprehensive overview of all security posture assessments and findings across different cloud resources and configurations.

2. CIS Section:

- CIS (Center for Internet Security) Sections refer to categories of security best practices defined by the CIS benchmarks. These sections group related security controls and guidelines that help ensure cloud resources are configured securely. In CSPM, findings are often categorized by CIS sections to help users identify which

areas of their cloud environment are least compliant with these best practices.

3. Last Checked:

- This indicates the most recent time when a particular resource or configuration was assessed for compliance with security benchmarks. It helps users understand how up to date the security posture information is and whether any recent changes might not yet be reflected in the findings.


4. Cloud:

- In CSPM, "Cloud" refers to the specific cloud service provider or environment being assessed. This could include platforms like AWS, Azure, or Google Cloud. The CSPM module evaluates resources within these cloud environments against security benchmarks to identify potential misconfigurations or vulnerabilities.


Step 3:



1. Export Reports:

- This feature allows users to generate and download reports of their security posture findings. Exporting reports can be useful for sharing with stakeholders, conducting audits, or maintaining records for compliance purposes. Reports typically include details of the findings, affected resources, and recommendations for remediation.

Navigate through each tab and click the  icon to use filter function.

Misconfigurations
See all findings of the Misconfigurations through cloud integration here.

Search Findings 

 CIS Section 

Identity and Access Management

Result	Resource ID	Resource Name	Resource Type	Rule Num...	Rule Name	CIS Section	Last Checked	Cloud
FAILED	↑ Sort by ASC	Browser key (auto cr...	gcp-apikeys-key	1.15	Ensure API Keys Are Rotated Every 90 Days	Identity and Access Manag...	11 hours ago	gcp
FAILED	↓ Sort by DESC	Browser key (auto cr...	gcp-apikeys-key	1.12	Ensure API Keys Only Exist for Active Services	Identity and Access Manag...	11 hours ago	gcp
PASSED	Filter	Browser key (auto cr...	gcp-apikeys-key	1.14	Ensure API Keys Are Restricted to Only APIs Th...	Identity and Access Manag...	11 hours ago	gcp
PASSED	Hide column	ShopperAI	gcp-cloudresource...	1.8	Ensure That Separation of Duties Is Enforced ...	Identity and Access Manag...	11 hours ago	gcp
PASSED	Manage columns	ShopperAI	gcp-cloudresource...	1.11	Ensure That Separation of Duties Is Enforced ...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//cloudsourcecema...	ShopperAI	gcp-cloudresource...	1.6	Ensure That IAM Users Are Not Assigned the S...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//cloudsourcecema...	ShopperAI	gcp-cloudresource...	1.5	Ensure That Service Account Has No Admin Pr...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//iam.googleapis.co...	projects/decisive-ro...	gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//iam.googleapis.co...	projects/decisive-ro...	gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//iam.googleapis.co...	projects/decisive-ro...	gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp

Rows per page: 10 1-10 of 65 < >

By clicking each of the misconfigurations, it will show you all the details such as Evidence, Remediation and Rule Info.

Misconfigurations

See all findings of the Misconfigurations through cloud Integration here.

CIS Section[Export Reports](#)

Identity and Access Management

Result	Resource ID	Resource Name	Resource Type	Rule Num...	Rule Name	CIS Section	Last Checked	Cloud
FAILED	//apikeys.googleapi...	Browser key (auto cr...	gcp-apikeys-key	1.15	Ensure API Keys Are Rotated Every 90 Days	Identity and Access Manag...	11 hours ago	gcp
FAILED	//apikeys.googleapi...	Browser key (auto cr...	gcp-apikeys-key	1.12	Ensure API Keys Only Exist for Active Services	Identity and Access Manag...	11 hours ago	gcp
PASSED	//apikeys.googleapi...	Browser key (auto cr...	gcp-apikeys-key	1.14	Ensure API Keys Are Restricted to Only APIs Th...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//cloudresourcem...		gcp-cloudresource...	1.8	Ensure That Separation of Duties Is Enforced ...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//cloudresourcem...		gcp-cloudresource...	1.11	Ensure That Separation of Duties Is Enforced ...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//cloudresourcem...		gcp-cloudresource...	1.6	Ensure That IAM Users Are Not Assigned the S...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//cloudresourcem...		gcp-cloudresource...	1.5	Ensure That Service Account Has No Admin Pr...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//iam.googleapis.co...		gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp
PASSED	//iam.googleapis.co...		gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp
FAILED	//iam.googleapis.co...		gcp-iam-service-a...	1.7	Ensure User-Managed/External Keys for Servi...	Identity and Access Manag...	11 hours ago	gcp

Rows per page: 10 1-10 of 65

In the evidence tab, it will give you the details of information that supports the misconfiguration.

Fail Ensure API Keys Are Rotated Every 90 Days



Rule Name Ensure API Keys Are Rotated Every 90 Days

Framework Source

Resource Name Browser key (auto created by Firebase)

Rule CIS GCP CIS 1.15

Resource ID

Tags Identity and Access Management

CIS Section Identity and Access Management

Resource Subtype gcp-apikeys-key

Evidence

Remediation

Rule Info

root: { 2 Items

Resource: { 8 Items

"account_id":

"sub_type": "gcp-apikeys-key"

"organization_id":

"account_name":

"name": "Browser key (auto created by Firebase)"

raw: { ... } 6 Items

"id":

"type": "key-management"

"Evidence": "2023-11-01T18:43:36.764807Z"

Remediation tab shows all the needed instructions to resolved the misconfigurations.

Fail

Ensure API Keys Are Rotated Every 90 Days

✕

Rule Name

Ensure API Keys Are Rotated Every 90 Days

Framework Source

Resource Name

Browser key (auto created by Firebase)

Rule

CIS

GCP

CIS 1.15

Resource ID

[REDACTED]

Tags

Identity and Access Management

CIS Section

Identity and Access Management

Resource Subtype

[gcp-apikeys-key](#)

Evidence

Remediation

Rule Info

****From Google Cloud Console****

1. Go to 'APIs & Services \Credentials' using 'https://console.cloud.google.com/apis/credentials'

2. In the section 'API Keys', Click the 'API Key Name'. The API Key properties display on a new page.

3. Click 'REGENERATE KEY' to rotate API key.

4. Click 'Save'.

5. Repeat steps 2,3,4 for every API key that has not been rotated in the last 90 days.

****Note:**** Do not set 'HTTP referrers' to wild-cards (* or *. [TLD] or *. [TLD] / *) allowing access to any/wide HTTP referrer(s)
Do not set 'IP addresses' and referrer to 'any host (0.0.0.0 or 0.0.0.0/0 or ::0)'

****From Google Cloud CLI****

There is not currently a way to regenerate and API key using gcloud commands.
To 'regenerate' a key you will need to create a new one, duplicate the restrictions from the key being rotated, and delete the old key.

6. List existing keys.

...

gcloud services api-keys list

...

7. Note the 'UID' and restrictions of the key to regenerate.

8. Run this command to create a new API key. <key_name> is the display name of the new key.

...

gcloud alpha services api-keys create --display-name=<key_name>

...

Note the 'UID' of the newly created key

9. Run the update command to add required restrictions.

Rule info tab shows the full details such as Description, Rationale, and References.

Fail

Ensure API Keys Are Rotated Every 90 Days

Rule Name

Ensure API Keys Are Rotated Every 90 Days

Resource Name

Browser key (auto created by Firebase)

Resource ID

CIS Section

Identity and Access Management

Framework Source

Rule

CIS

GCP

CIS 1.15

Tags

Identity and Access Management

Resource Subtype

gcp-apikeys-key

Evidence

Remediation

Rule Info

Description:

API Keys should only be used for services in cases where other authentication methods are unavailable. If they are in use it is recommended to rotate API keys every 90 days.

Rationale:

Security risks involved in using API-Keys are listed below: - API keys are simple encrypted strings - API keys do not identify the user or the application making the API request - API keys are typically accessible to clients, making it easy to discover and steal an API key. Because of these potential risks, Google recommends using the standard authentication flow instead of API keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API. Once a key is stolen, it has no expiration, meaning it may be used indefinitely unless the project owner revokes or regenerates the key. Rotating API keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used. API keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.

References:

1. <https://developers.google.com/maps/api-security-best-practices#regenerate-apikey>

2. <https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys>

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #6

Created 6 May 2025 03:58:29 by Richmond Abella

Updated 28 May 2025 09:04:23 by Richmond Abella