CyTech AQUILA - Cloud Security Posture Management (CSPM) Module

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**.

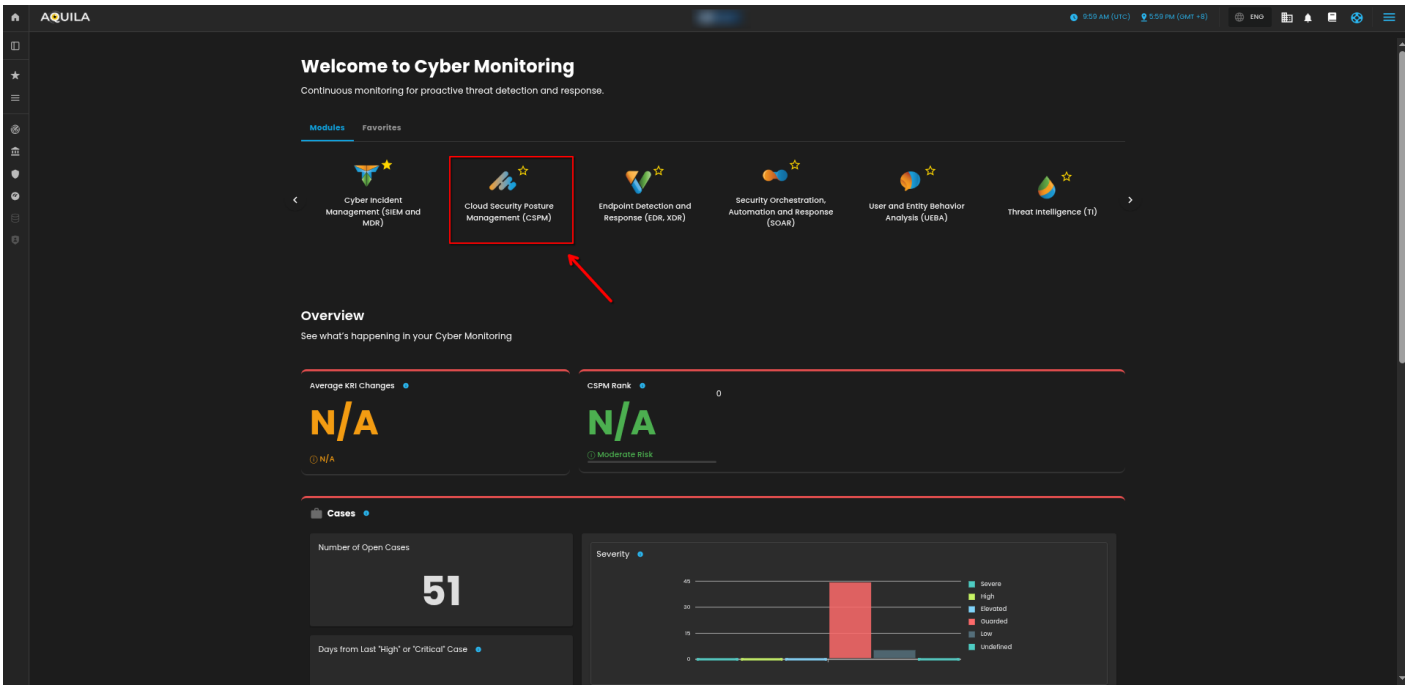
Pre-requisites

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

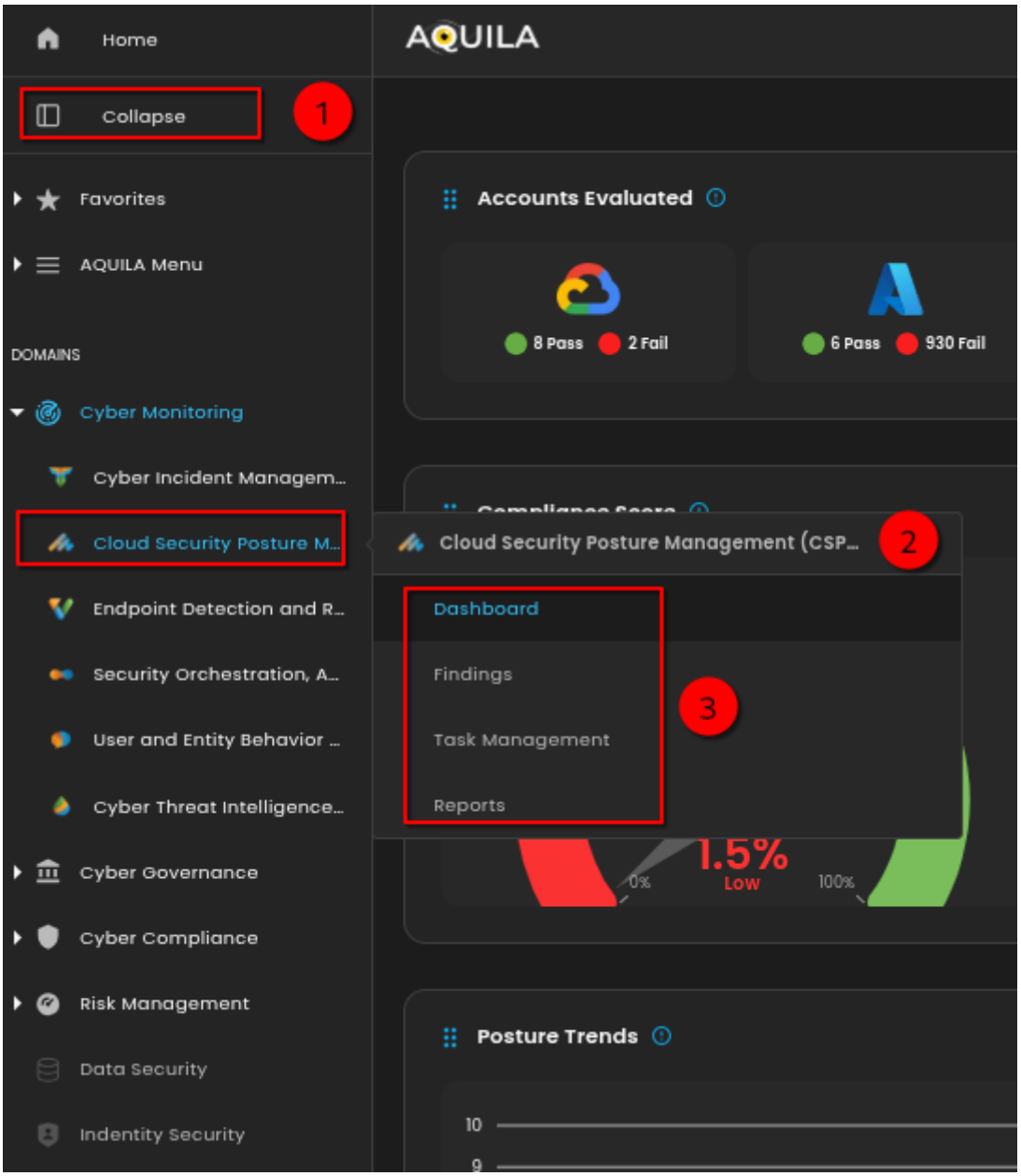
> **To navigate to CSPM Module please follow the instructions below:**

Step 1: Log in to CyTech - AQUILA. *click here* --> **AQUILACYBER.ai**
Step 2: Click on Cyber Monitoring.

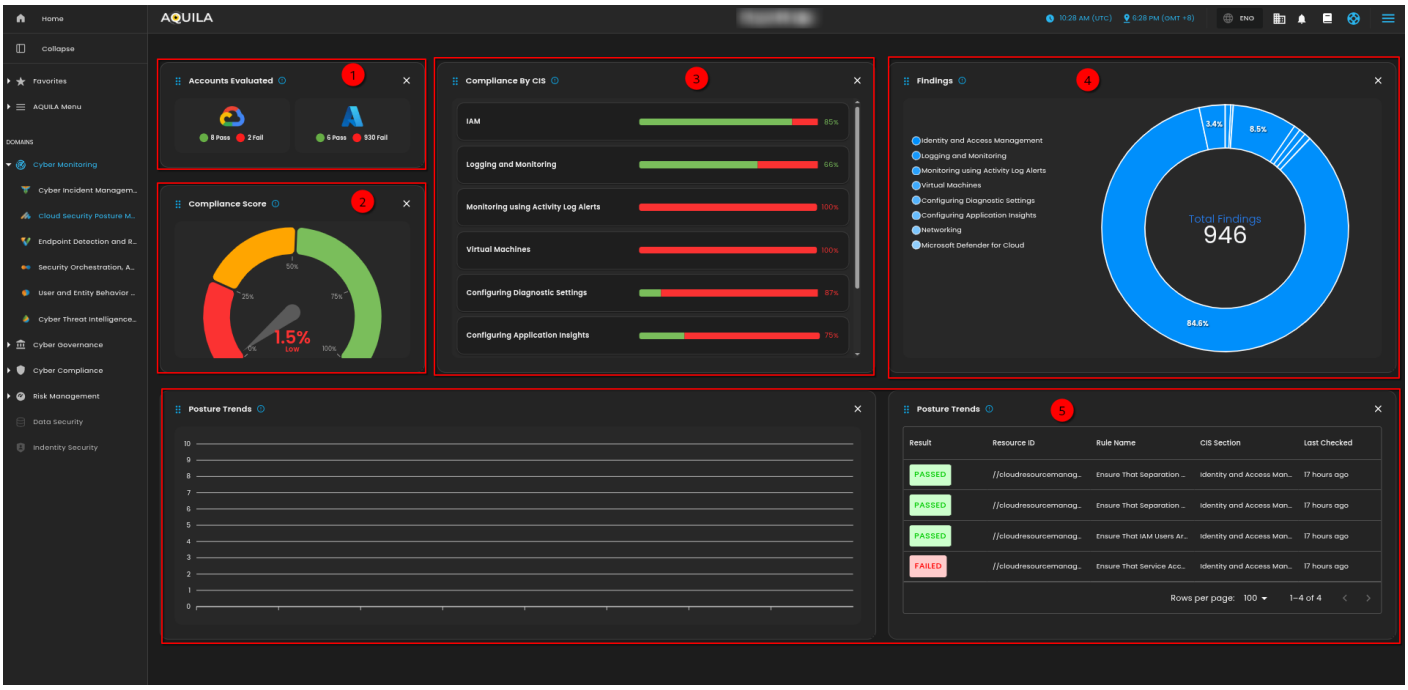
Step 3: Choose Cloud Security Posture Management (CSPM).



Step 4: Hover into leftmost panel to view all the CSPM sections.

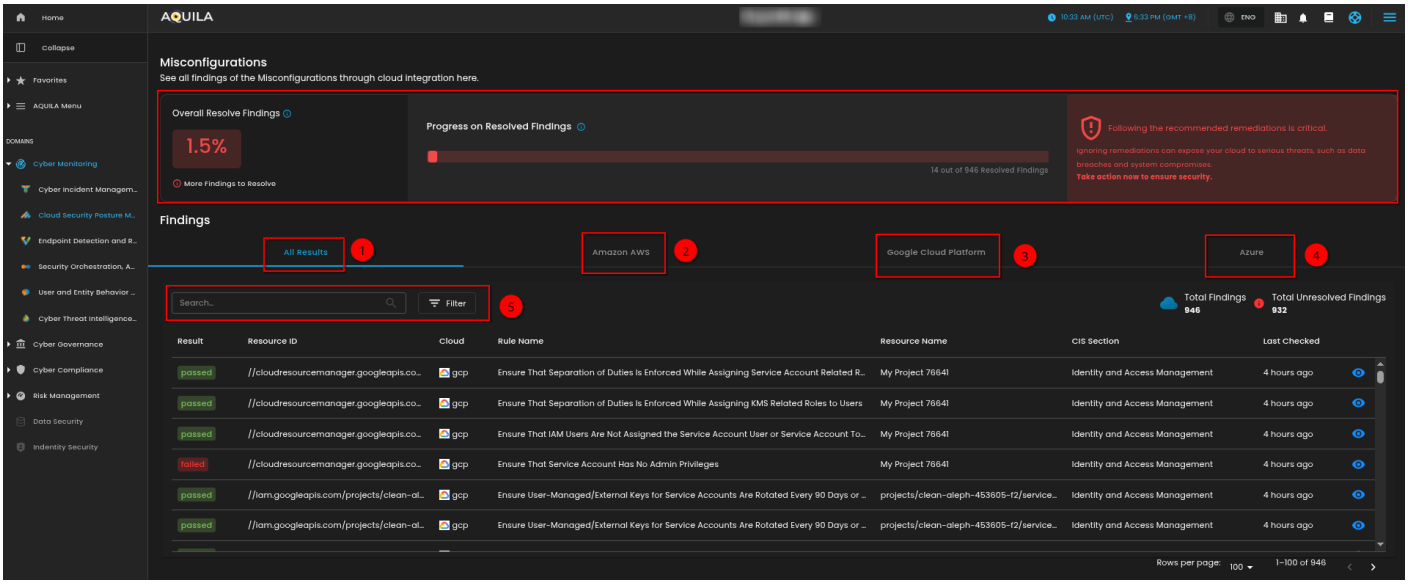


Here in the CSPM Dashboard you can view all the evaluations. Such as Account Evaluated, Compliance Score, Compliance by Center in Internet Security (CIS), Findings and Posture Trends.



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.**



Misconfigurations

This section gives an overview of all misconfiguration findings detected from cloud integrations across AWS, GCP, and Azure.

Overall Resolve Findings

Displays the percentage of resolved vs. unresolved misconfigurations. It includes a progress bar and a warning message urging users to follow remediation steps to maintain cloud security.

All Results Tab

Lists all misconfiguration findings from all cloud providers in one consolidated view.

Amazon AWS Tab

Filters the findings to only show results from Amazon Web Services (AWS).

Google Cloud Platform Tab

Shows findings that pertain exclusively to GCP (Google Cloud Platform) assets.

Azure Tab

Filters results to display only Azure-related misconfiguration findings.

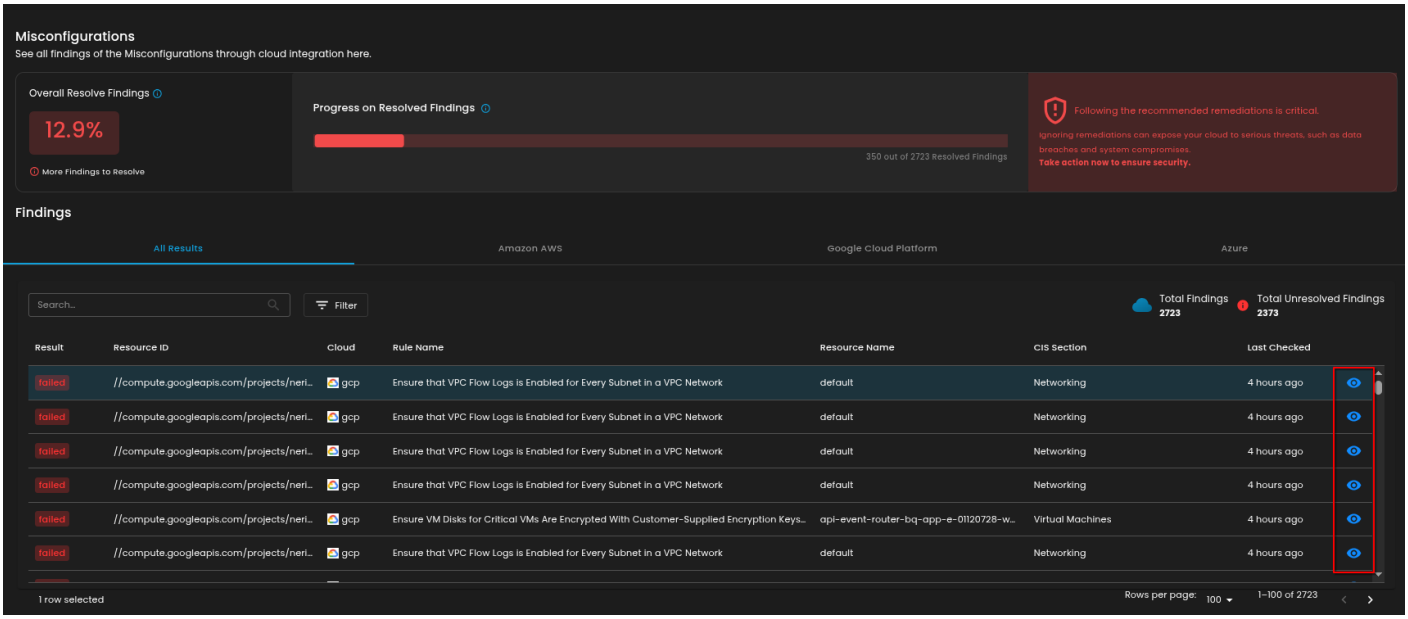
Search & Filter Function

- **Search Bar**: Quickly locate specific misconfiguration results by keyword.
- **Filter Button**: Apply advanced filters (e.g., cloud type, severity, category) to narrow down the displayed results.

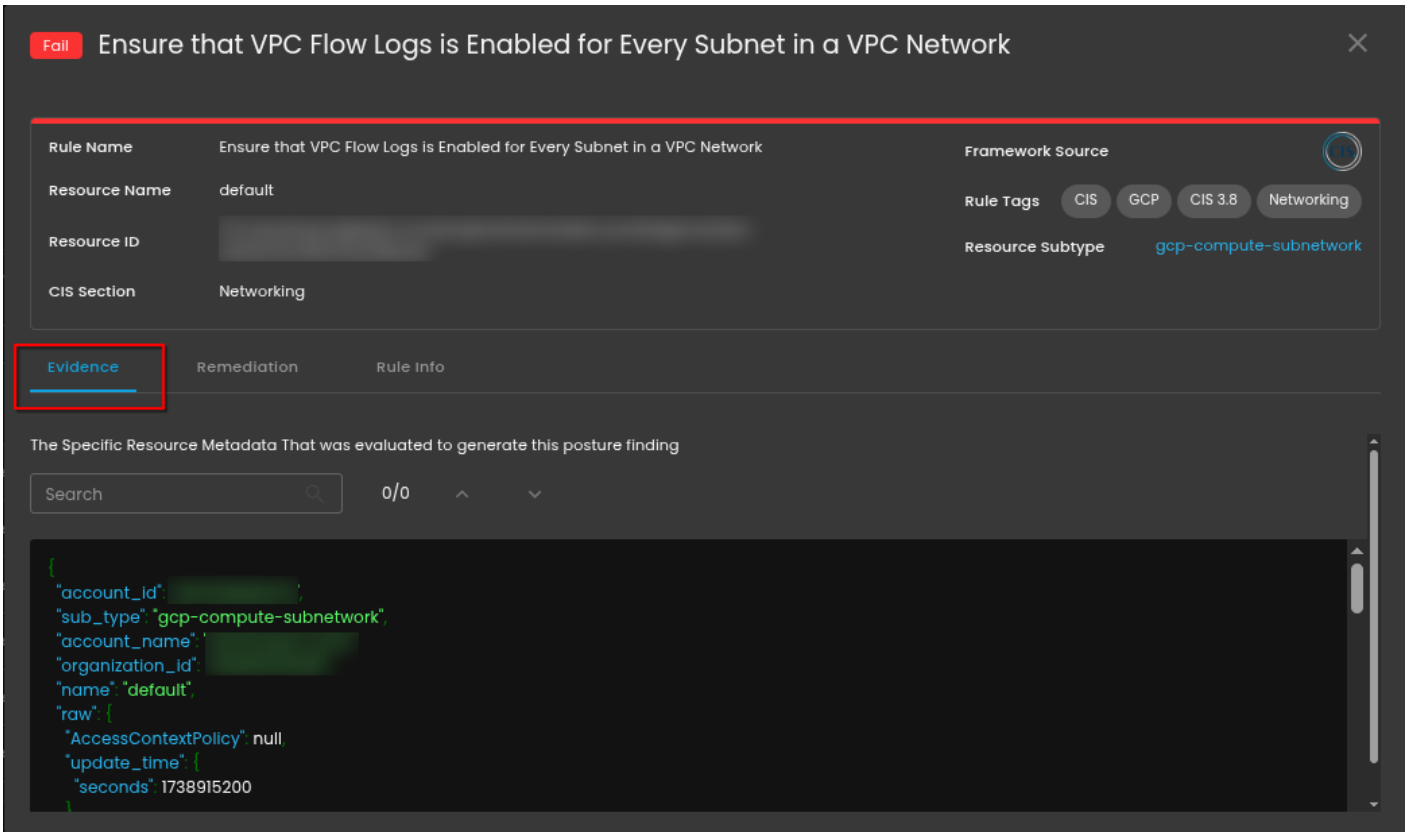
---

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.

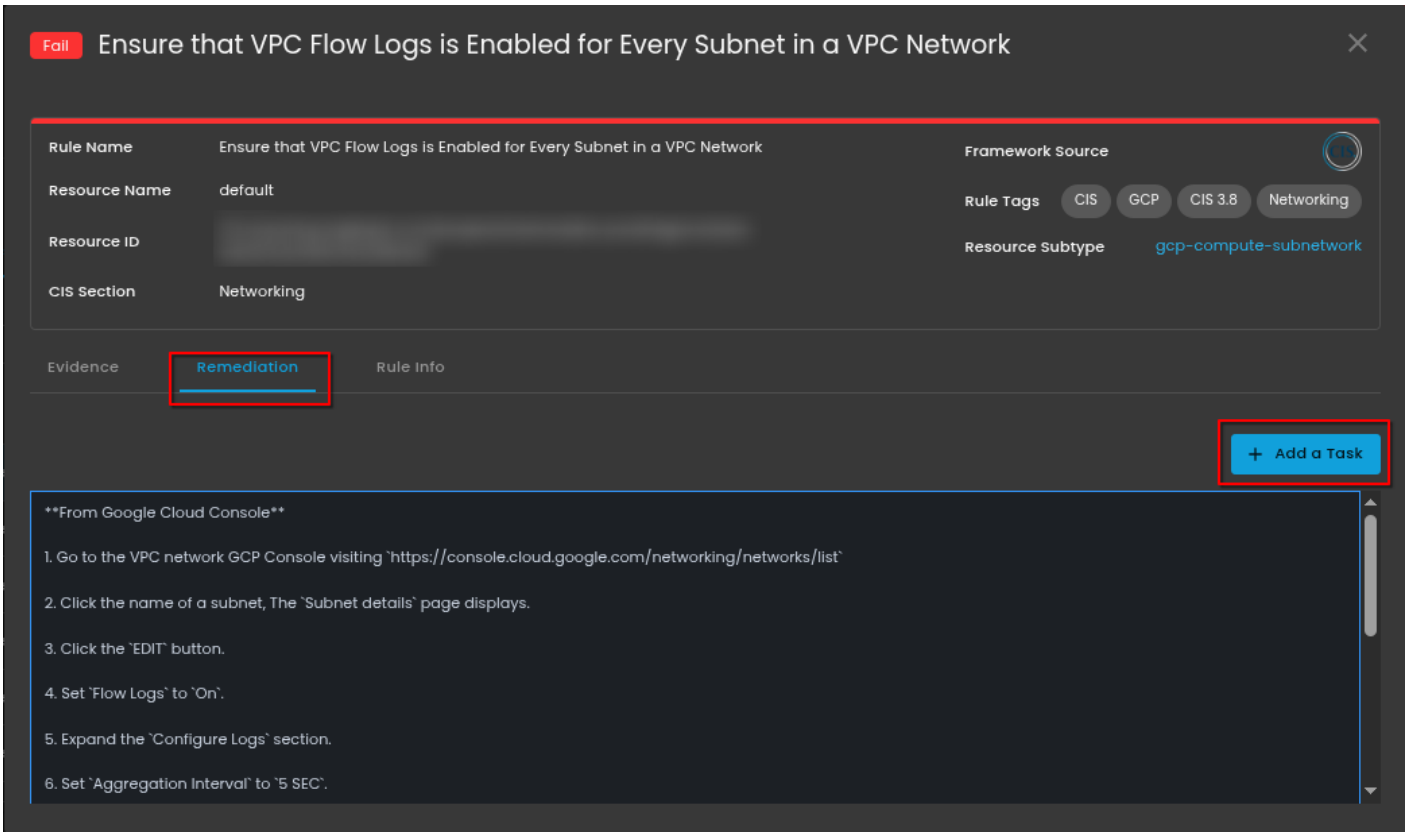
By clicking each of the misconfigurations , it will show you all the details such as Evidence, Remediation and Rule Info.



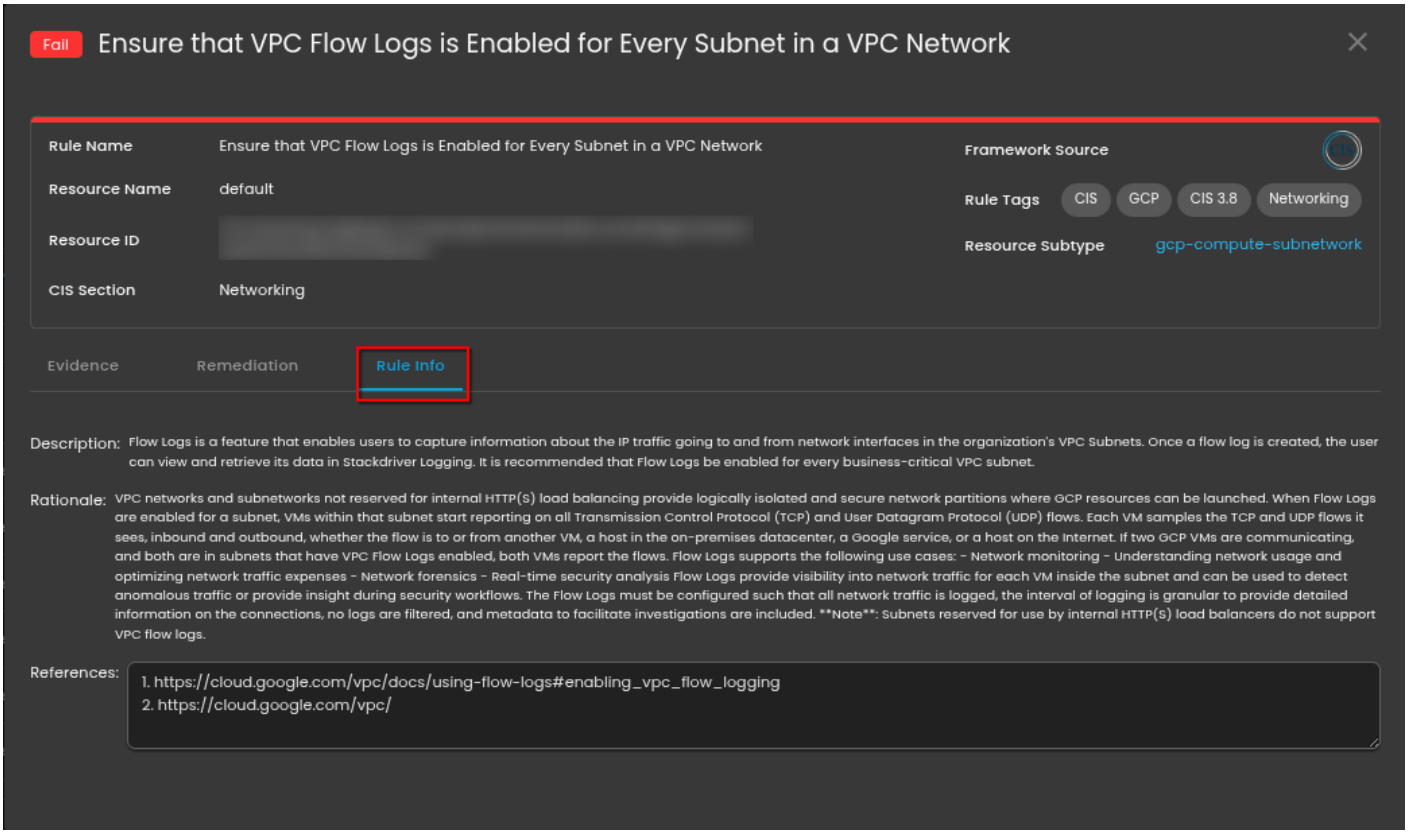
In the evidence tab, it will give you the details of information that supports the misconfiguration.



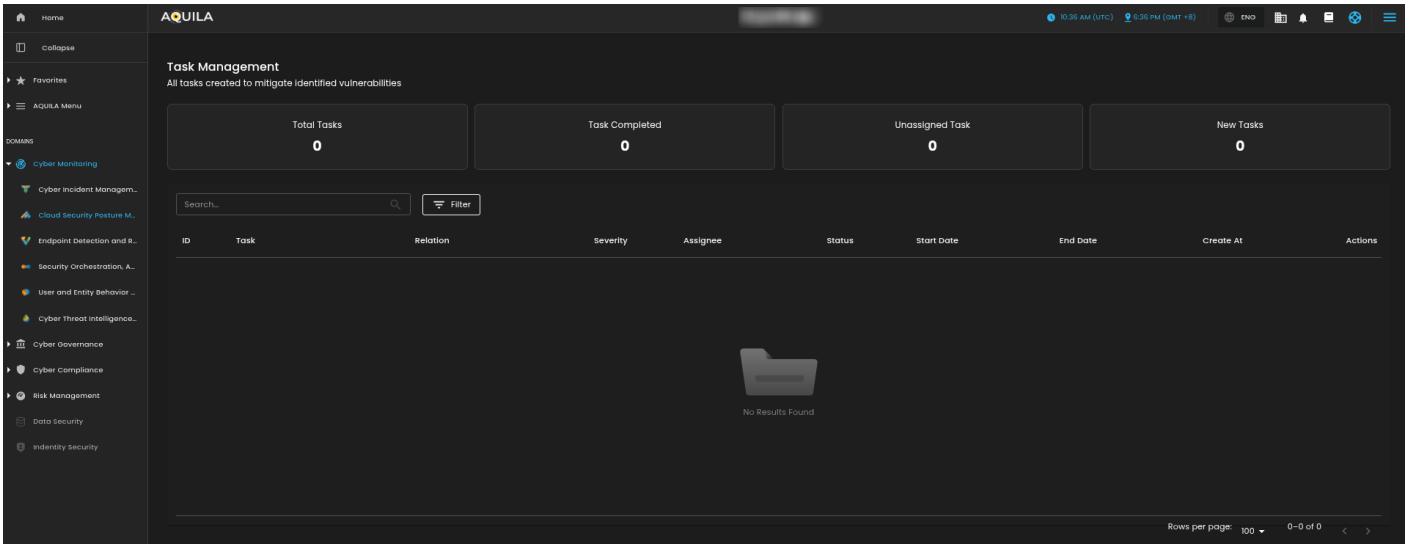
Remediation tab shows all the needed instructions to resolved the misconfigurations and you can also "Add a Task" function.



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



> **Task Management Section- Displays all tasks created to mitigate identified vulnerabilities from cloud security findings.**



Summary Cards

- **Total Tasks**: The overall number of tasks created.
- **Task Completed**: Number of tasks successfully resolved.
- **Unassigned Task**: Tasks not yet assigned to any user.
- **New Tasks**: Recently added tasks not yet started or in progress.

Search & Filter Function

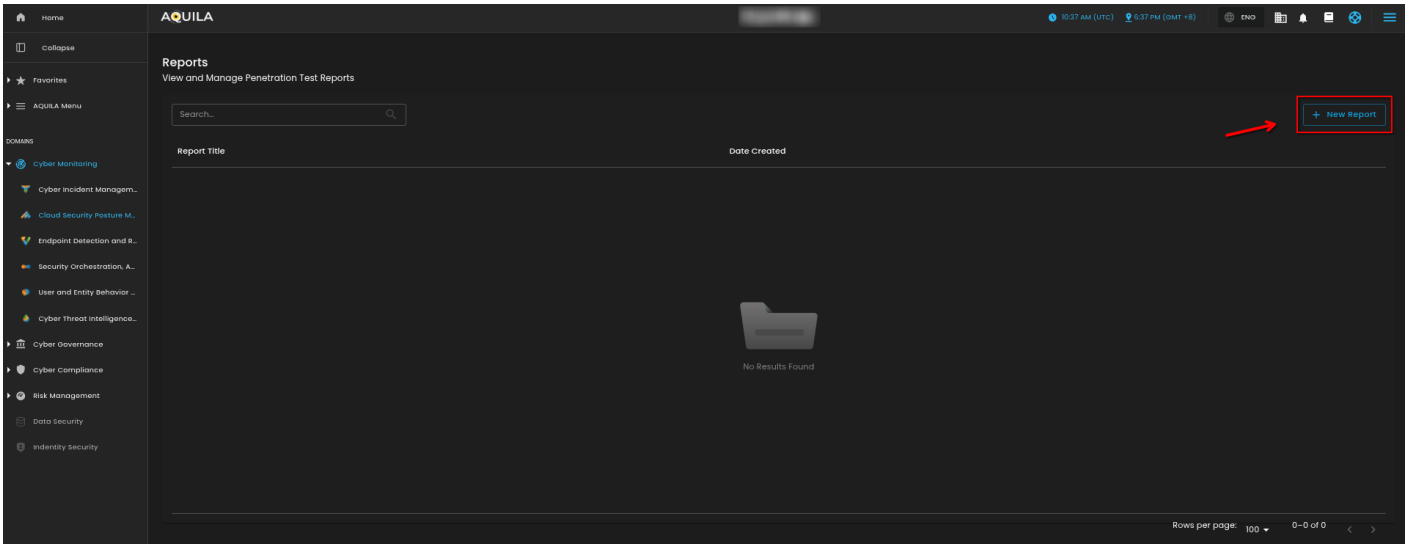
- **Search Bar**: Allows quick lookup of specific tasks by keyword.
- **Filter Button**: Opens advanced filtering options (e.g., severity, assignee, status).

Task Table

Displays task details including:

- **ID**: Unique identifier for each task
- **Task Name**
- **Relation**: Link to associated misconfiguration or finding
- **Severity**: Impact level of the issue
- **Assignee**: Person responsible for the task
- **Status**: Current progress (e.g., new, in progress, completed)
- **Start/End Date, Created At**: Timeline info for tracking progress
- **Actions**: Manage or update the task

> **Reports Section 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.

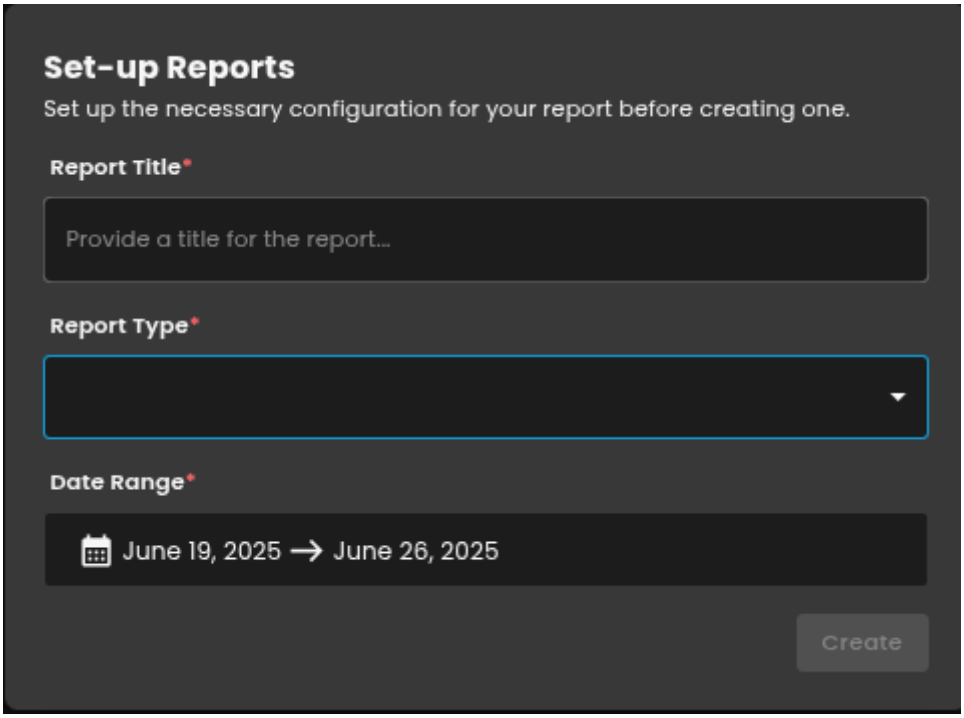
Step2: Choose desired output.

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.



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

Revision #8
Created 6 May 2025 03:58:29 by Richmond Abella
Updated 25 September 2025 02:51:50 by Richmond Abella