ROYAL CYBER

SECURACLOUD

55 Shuman Blvd, Suite 275,
Naperville, IL 60563 USA.
Tel: +1.630.355.6292 | Email: info@royalcyber.com
https://www.royalcyber.com

Overview

Securacloud is a comprehensive Cloud Security and Compliance Platform that empowers businesses to achieve and maintain compliance while securing their cloud journey with confidence.

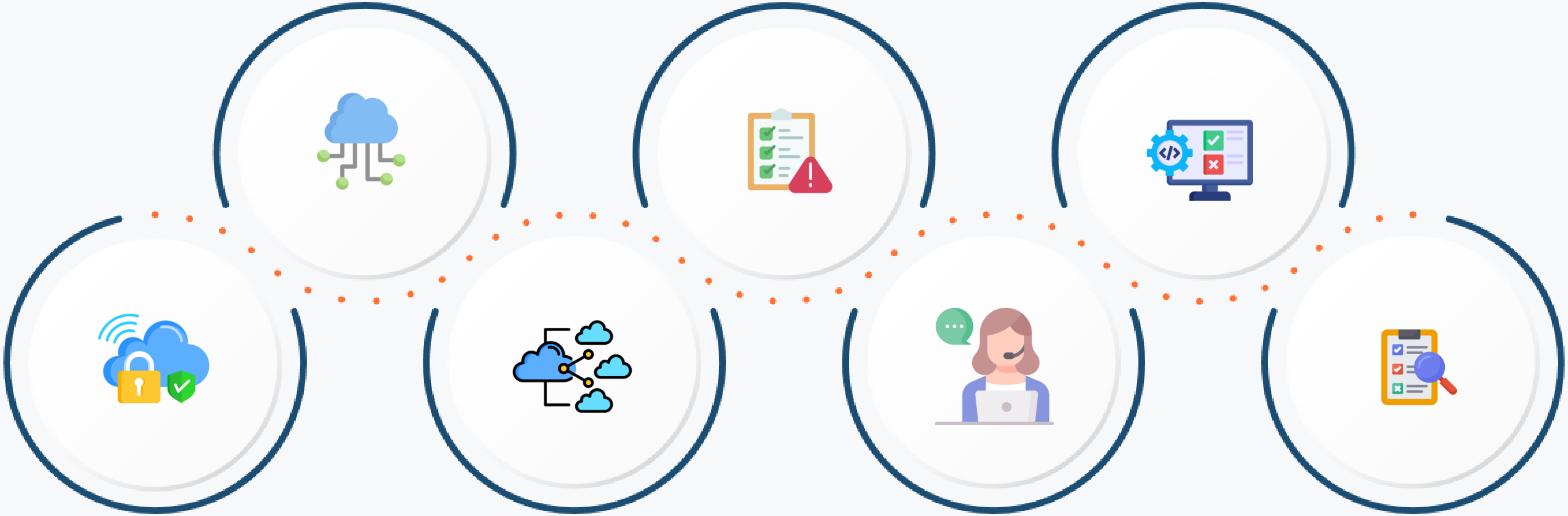
Securacloud is presently engaged with clients in the MENA and North American regions.

Copyright © 2023 Royal Cyber All rights reserved.

Securacloud Solution

ROYAL CYBER

Our comprehensive solution encompasses vital components:



Cloud Security Posture Management (CSPM) Tool

Cloud Asset Inventory

Multi-Cloud Compliance

Vulnerability and Risk Management

Managed Security Services

Penetration Testing

GAP Assessment

Copyright © 2023 Royal Cyber All rights reserved.

Industry Standards

PCI Security Standards Council

CIS Center for Internet Security

HIPAA COMPLIANT

GDPR

SOC 2 SERVICE ORGANIZATION

Information Security Management 27001 Certified

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Copyright © 2024 Royal Cyber All rights reserved.

Securacloud Tool

A Cloud Security & Compliance management tool

Copyright © 2024 Royal Cyber All rights reserved.

Risk Management

Compliance

Inventory

AI Assistant

Governance

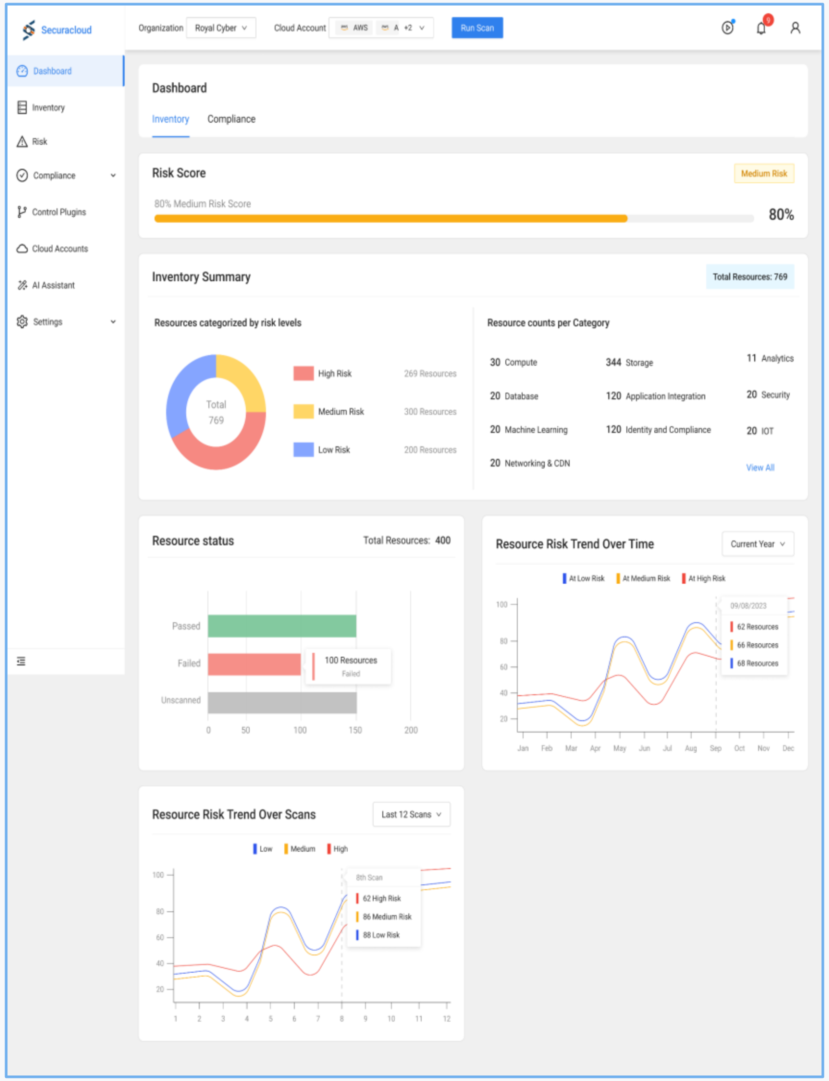
Protect your cloud-based infrastructure, Applications & cloud data using **Securacloud**

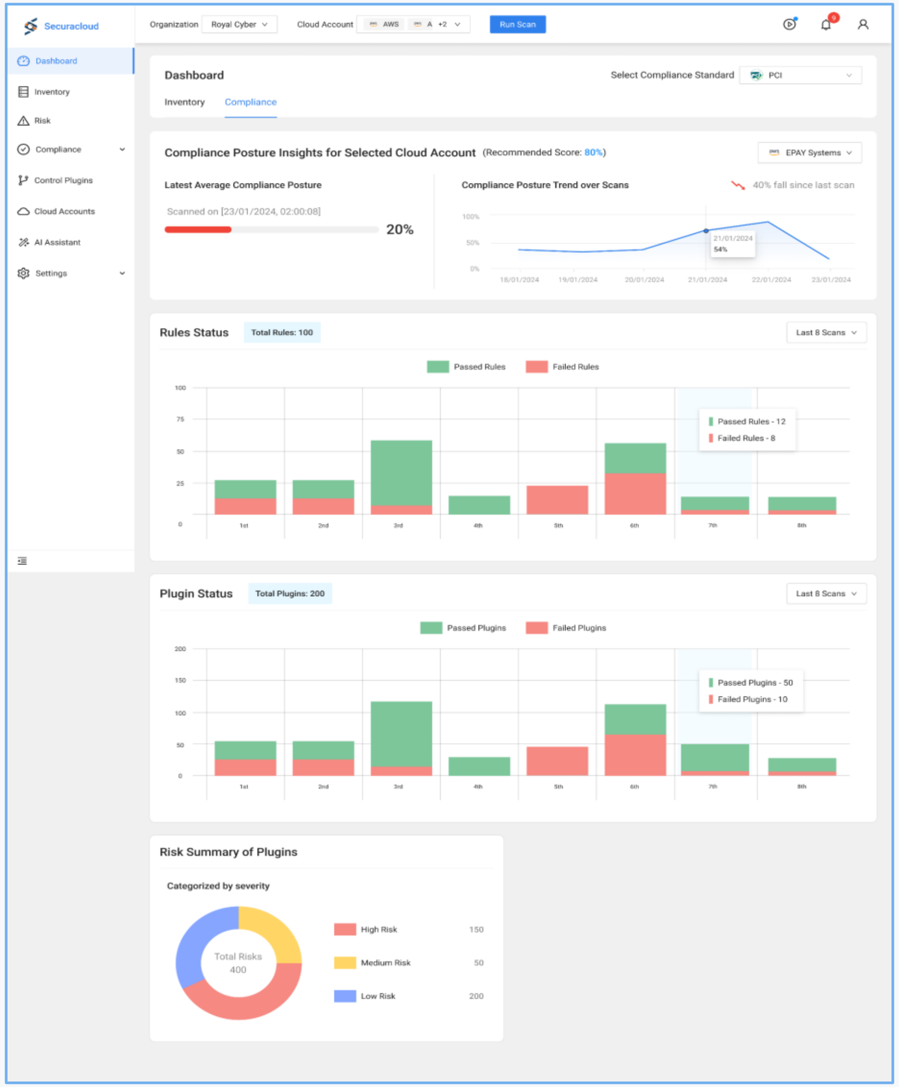
Copyright © 2024 Royal Cyber All rights reserved.

Visibility

Governance

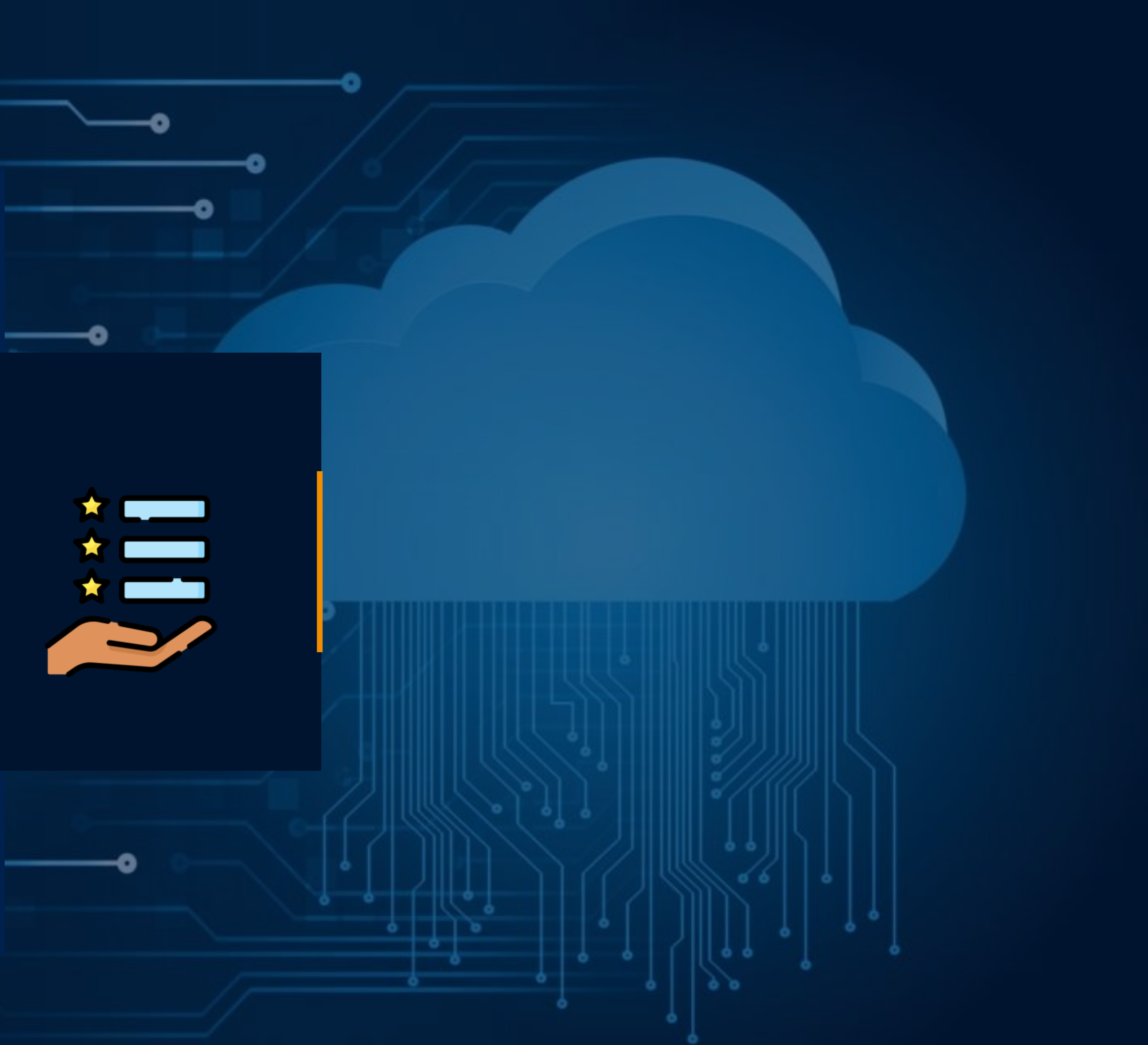
Compliance





Copyright © 2024 Royal Cyber All rights reserved.

Features



Copyright © 2024 Royal Cyber All rights reserved.

Agentless Infrastructure Scanning:
Conduct thorough assessments of cloud environments without the need for intrusive agents, ensuring seamless integration and minimal disruption.

Centralized Cloud Security Dashboard:
Gain real-time visibility into security postures and compliance statuses across all cloud assets through a centralized, user-friendly interface.

Custom Compliance Builder:
Tailor compliance frameworks to suit specific organizational requirements, enabling precise adherence to industry standards and regulations.

Identity-based Multi-Account Integration:
Effortlessly integrate multiple accounts while ensuring granular control over access permissions and user identities.

Multi-Cloud Support:
Seamlessly manage security across various cloud platforms, providing a unified approach to safeguarding diverse infrastructures.

Copyright © 2024 Royal Cyber All rights reserved.

Remediation Guidelines:
Access best-practice-based insights and detailed instructions tailored to rectify identified vulnerabilities.

800+ Plugins/Controls:
Leverage an extensive library of pre-built plugins and controls to customize security assessments and address a wide range of potential threats.

AI-Based Search:
Harness the power of artificial intelligence to efficiently navigate through vast datasets and pinpoint critical security issues with unparalleled accuracy.

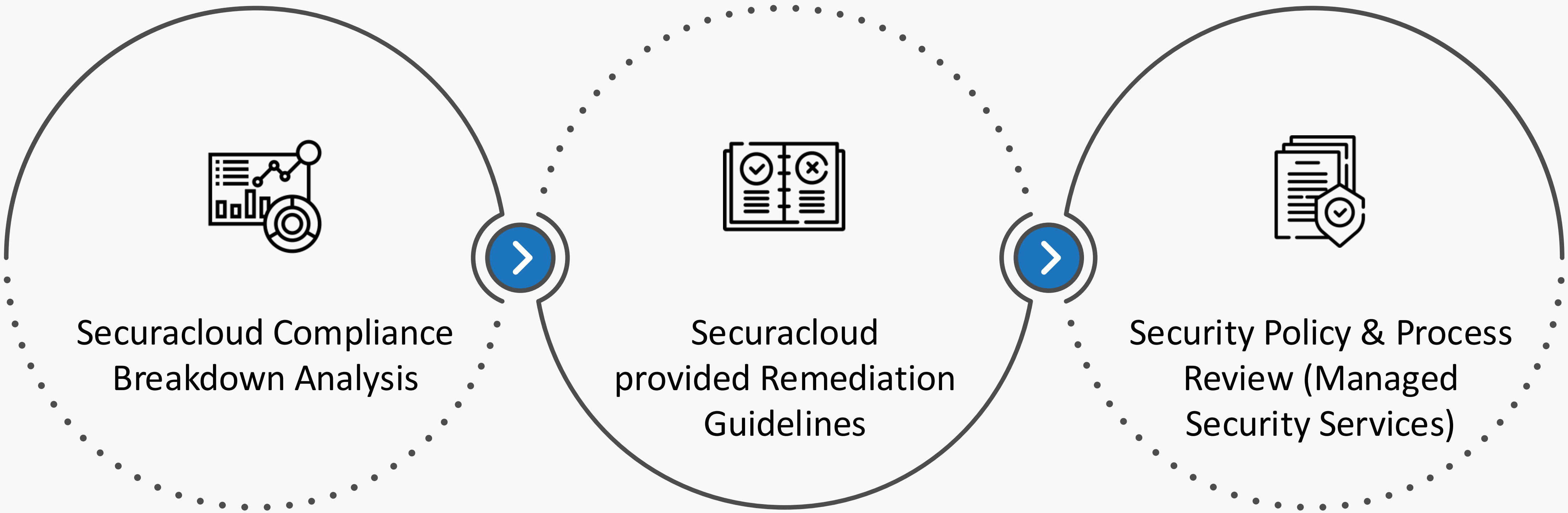
Cloud Asset Inventory:

Maintain an up-to-date inventory of cloud assets, facilitating comprehensive risk assessment and ensuring holistic security coverage.

Role-based Access Security:
Implement robust access controls based on roles and responsibilities, bolstering security measures and mitigating risks of unauthorized access.

Copyright © 2024 Royal Cyber All rights reserved.

GAP Assessment



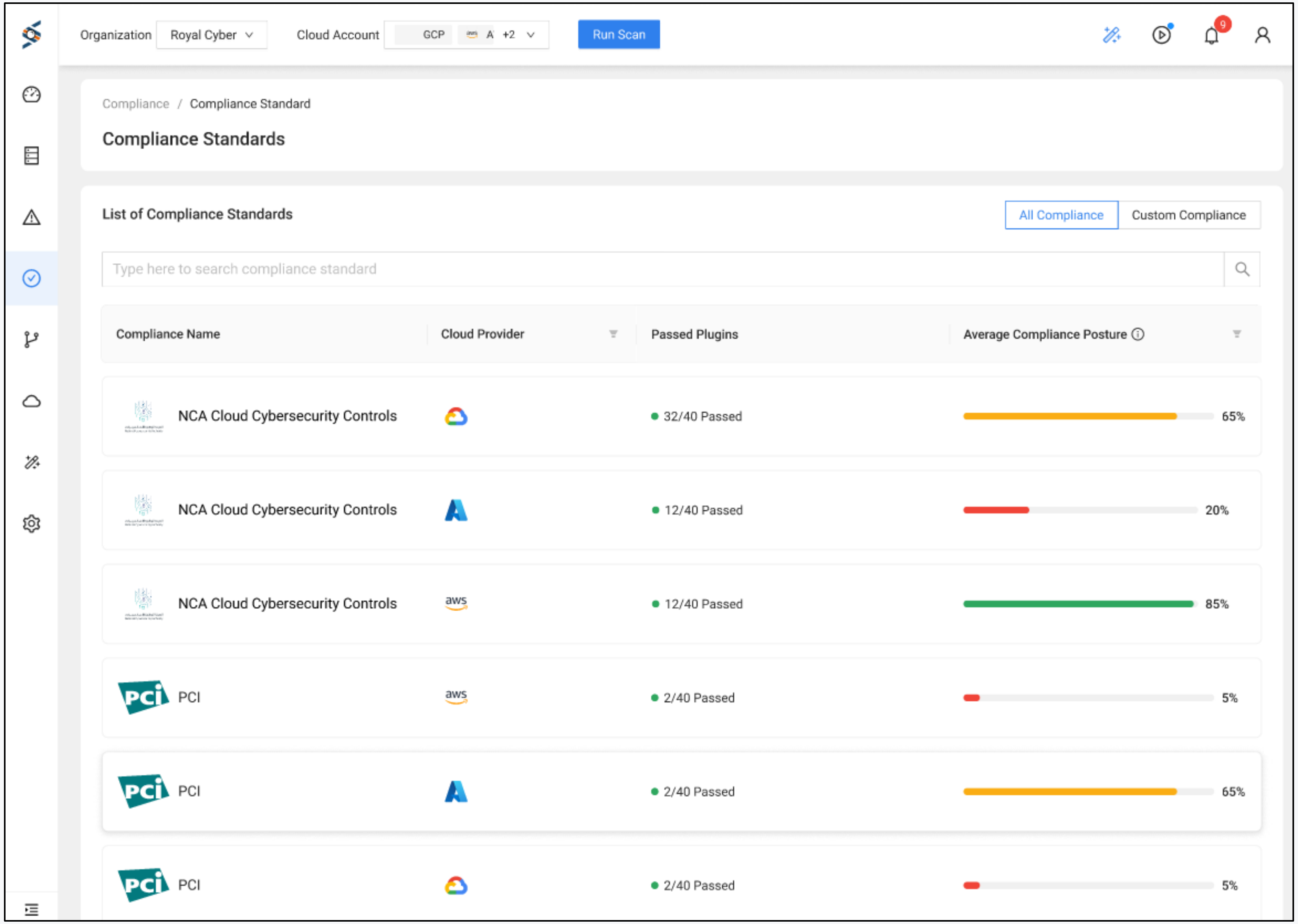
Securacloud Compliance Breakdown Analysis

Securacloud provided Remediation Guidelines

Security Policy & Process Review (Managed Security Services)

Copyright © 2024 Royal Cyber All rights reserved.

Compliance



Organization Royal Cyber

Cloud Account GCP aws A +2

Compliance / Compliance Standard

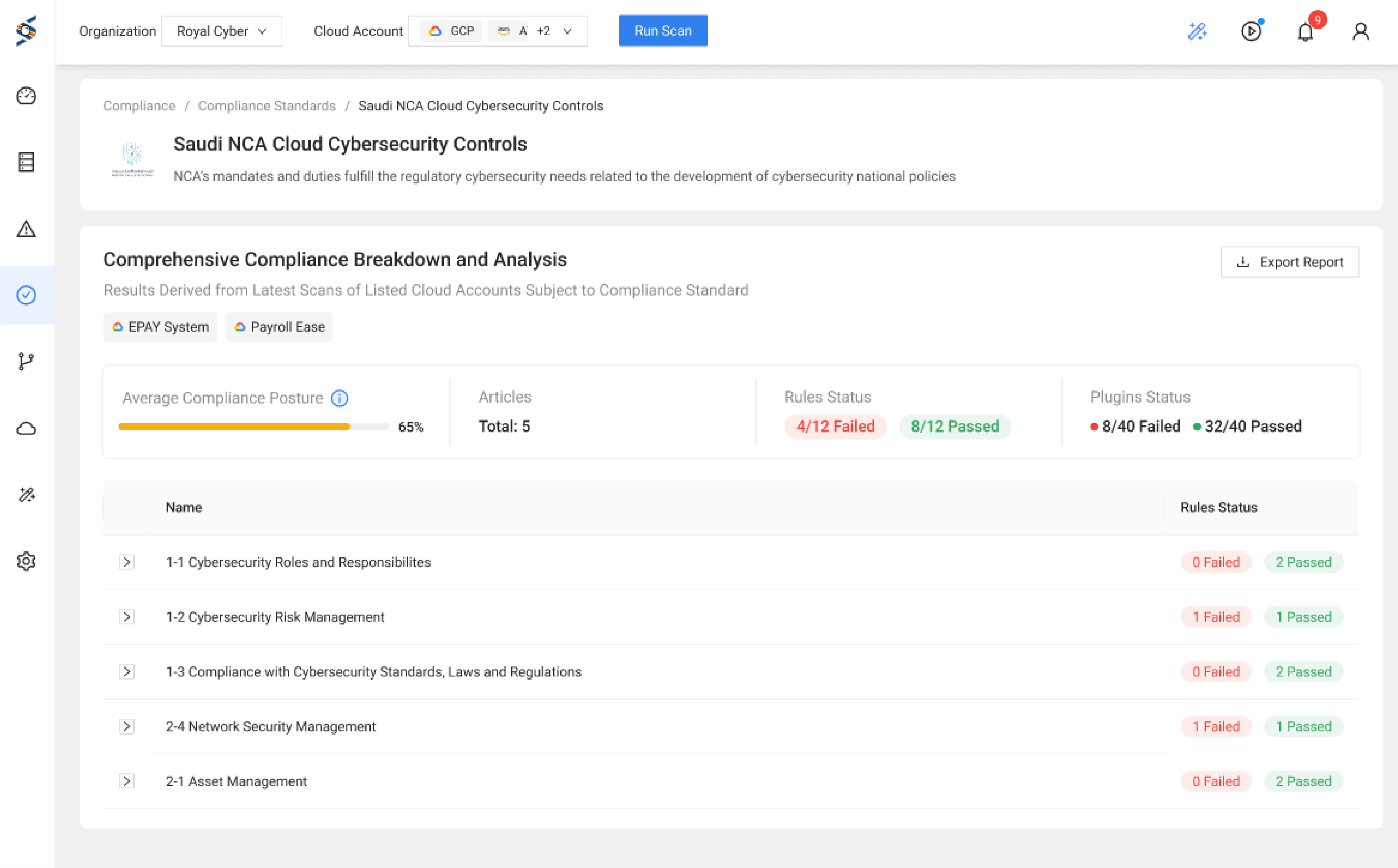
Compliance Standards

List of Compliance Standards

Compliance Name	Cloud Provider	Passed Plugins	Average Compliance Posture
NCA Cloud Cybersecurity Controls		32/40 Passed	65%
NCA Cloud Cybersecurity Controls		12/40 Passed	20%
NCA Cloud Cybersecurity Controls	aws	12/40 Passed	85%
PCI	aws	2/40 Passed	5%
PCI		2/40 Passed	65%
PCI		2/40 Passed	5%

Copyright © 2024 Royal Cyber All rights reserved.

Breakdown Analysis



Organization Royal Cyber

Cloud Account GCP A +2

Compliance / Compliance Standards / Saudi NCA Cloud Cybersecurity Controls

Saudi NCA Cloud Cybersecurity Controls

NCA's mandates and duties fulfill the regulatory cybersecurity needs related to the development of cybersecurity national policies

Comprehensive Compliance Breakdown and Analysis

Results Derived from Latest Scans of Listed Cloud Accounts Subject to Compliance Standard

EPAY System

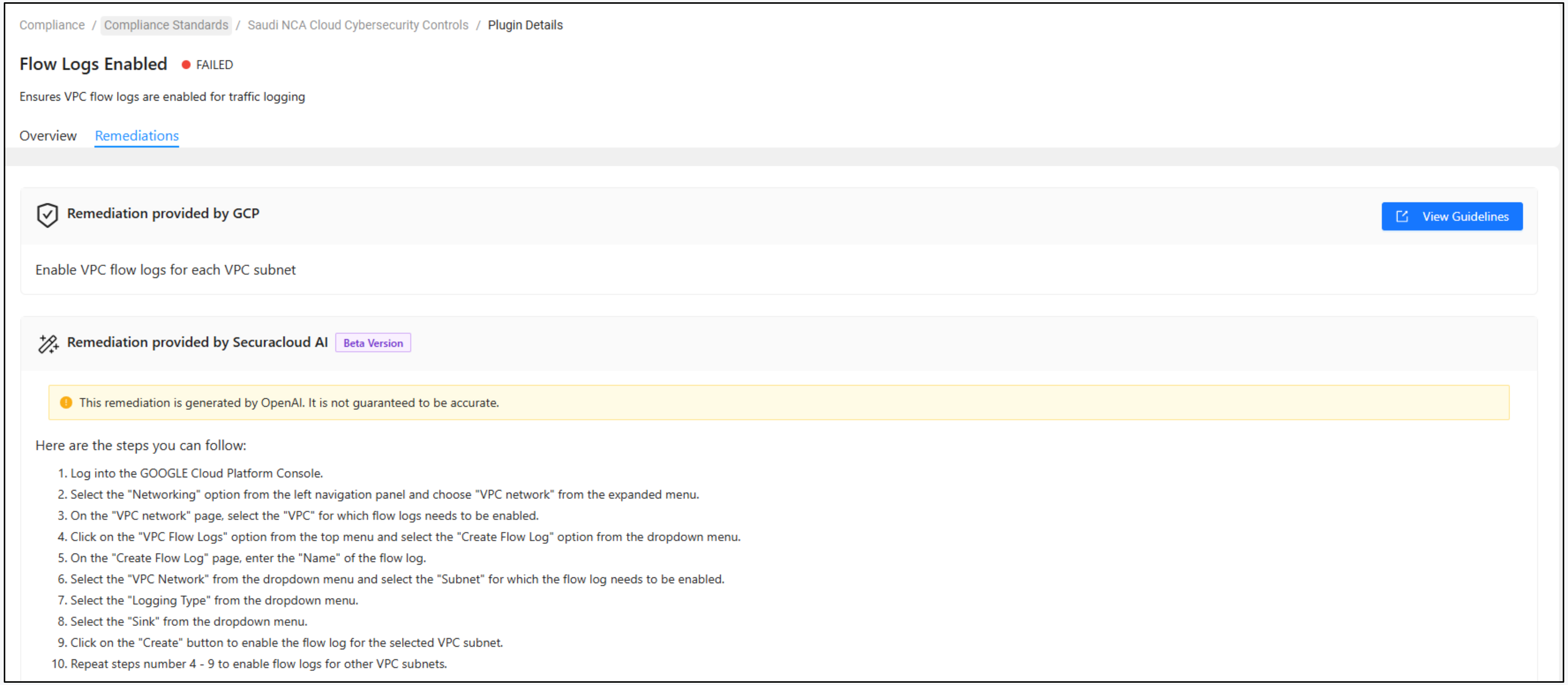
Payroll Ease

Average Compliance Posture	Articles	Rules Status	Plugins Status
65%	Total: 5	4/12 Failed 8/12 Passed	● 8/40 Failed ● 32/40 Passed

Name	Rules Status
1-1 Cybersecurity Roles and Responsibilites	0 Failed 2 Passed
1-2 Cybersecurity Risk Management	1 Failed 1 Passed
1-3 Compliance with Cybersecurity Standards, Laws and Regulations	0 Failed 2 Passed
2-4 Network Security Management	1 Failed 1 Passed
2-1 Asset Management	0 Failed 2 Passed

Copyright © 2024 Royal Cyber All rights reserved.

Remediation Guidelines


Compliance / Compliance Standards / Saudi NCA Cloud Cybersecurity Controls / Plugin Details
Overview
Remediations
View Guidelines

Flow Logs Enabled ● FAILED

Ensures VPC flow logs are enabled for traffic logging

Remediation provided by GCP

Enable VPC flow logs for each VPC subnet

Remediation provided by Securacloud AI Beta Version

This remediation is generated by OpenAI. It is not guaranteed to be accurate.

Here are the steps you can follow:

1. Log into the GOOGLE Cloud Platform Console.
2. Select the "Networking" option from the left navigation panel and choose "VPC network" from the expanded menu.
3. On the "VPC network" page, select the "VPC" for which flow logs needs to be enabled.
4. Click on the "VPC Flow Logs" option from the top menu and select the "Create Flow Log" option from the dropdown menu.
5. On the "Create Flow Log" page, enter the "Name" of the flow log.
6. Select the "VPC Network" from the dropdown menu and select the "Subnet" for which the flow log needs to be enabled.
7. Select the "Logging Type" from the dropdown menu.
8. Select the "Sink" from the dropdown menu.
9. Click on the "Create" button to enable the flow log for the selected VPC subnet.
10. Repeat steps number 4 - 9 to enable flow logs for other VPC subnets.

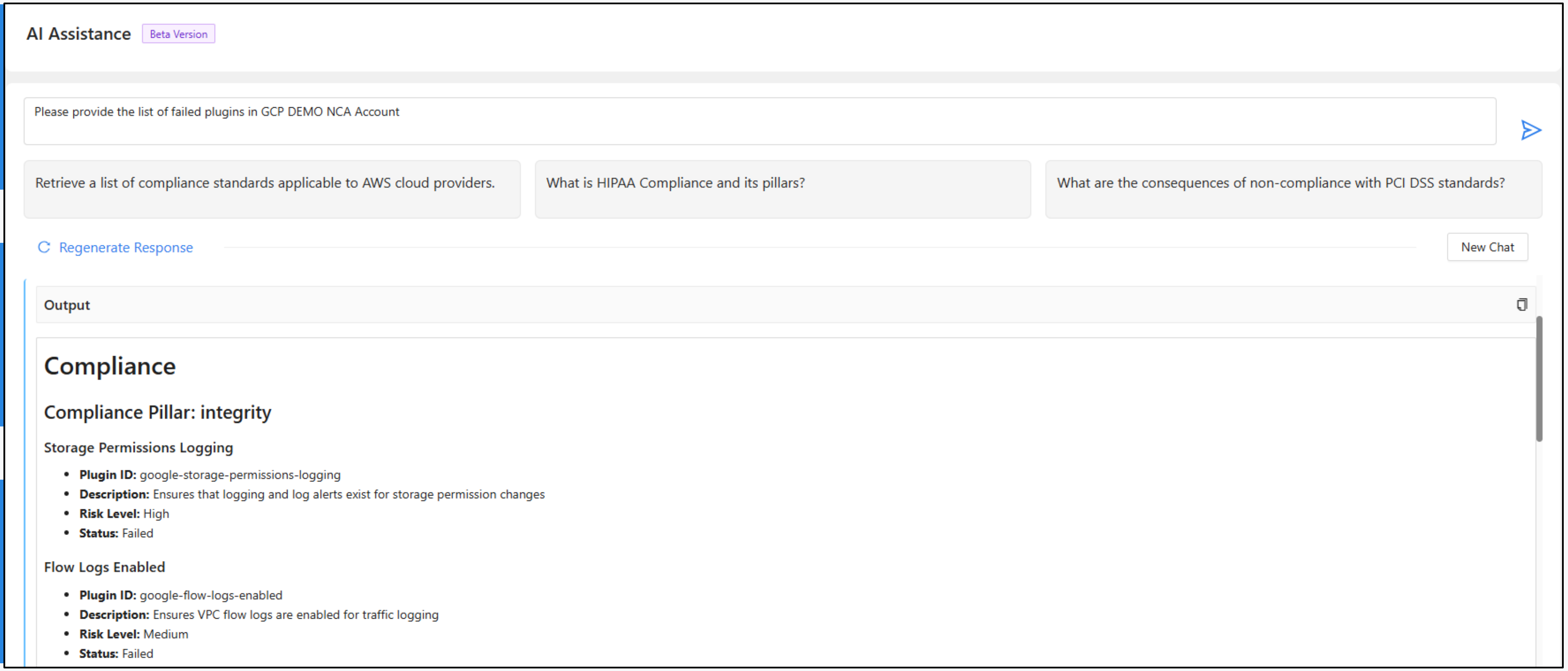
Copyright © 2024 Royal Cyber All rights reserved.

AI Assistance

Powered by Generative AI and SecuraCloud Datasources

Account-Specific Intelligence

Proactive Remediation



Please provide the list of failed plugins in GCP DEMO NCA Account

Retrieve a list of compliance standards applicable to AWS cloud providers.

What is HIPAA Compliance and its pillars?

What are the consequences of non-compliance with PCI DSS standards?

Compliance

Compliance Pillar: integrity

Storage Permissions Logging

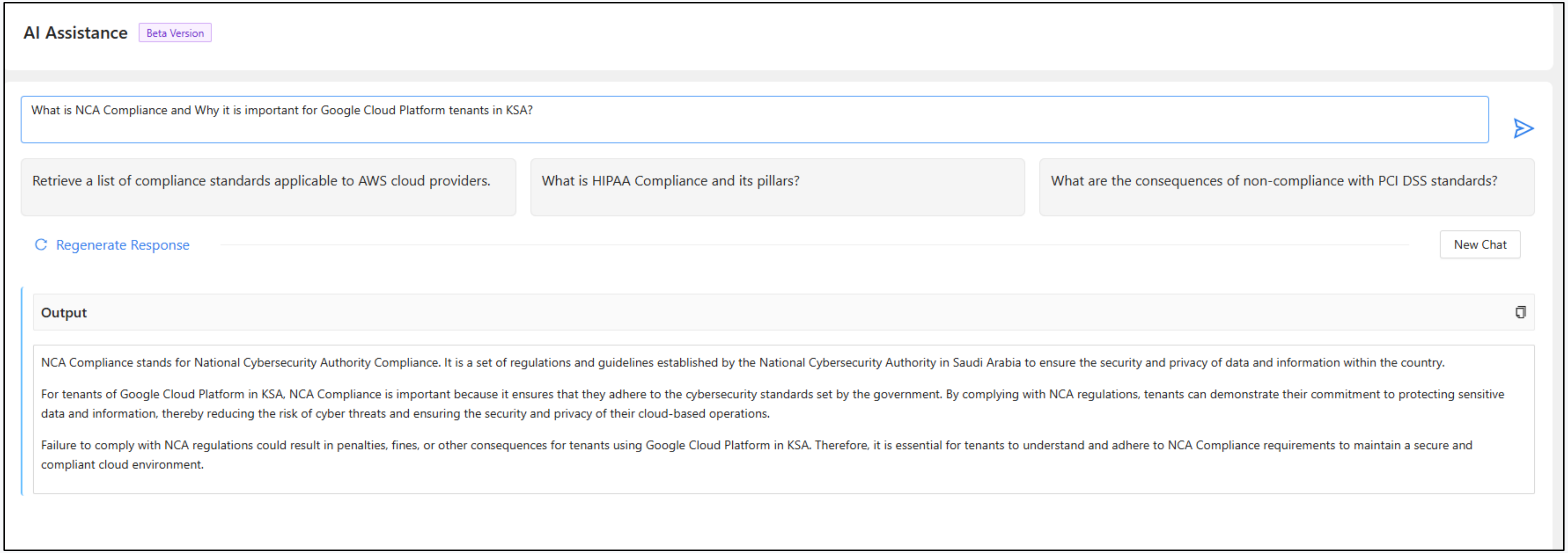
- **Plugin ID:** google-storage-permissions-logging
- **Description:** Ensures that logging and log alerts exist for storage permission changes
- **Risk Level:** High
- **Status:** Failed

Flow Logs Enabled

- **Plugin ID:** google-flow-logs-enabled
- **Description:** Ensures VPC flow logs are enabled for traffic logging
- **Risk Level:** Medium
- **Status:** Failed

Copyright © 2024 Royal Cyber All rights reserved.

AI Assistance


AI Assistance
Beta Version

What is NCA Compliance and Why it is important for Google Cloud Platform tenants in KSA?

Retrieve a list of compliance standards applicable to AWS cloud providers.
What is HIPAA Compliance and its pillars?
What are the consequences of non-compliance with PCI DSS standards?
Regenerate Response
New Chat
Output

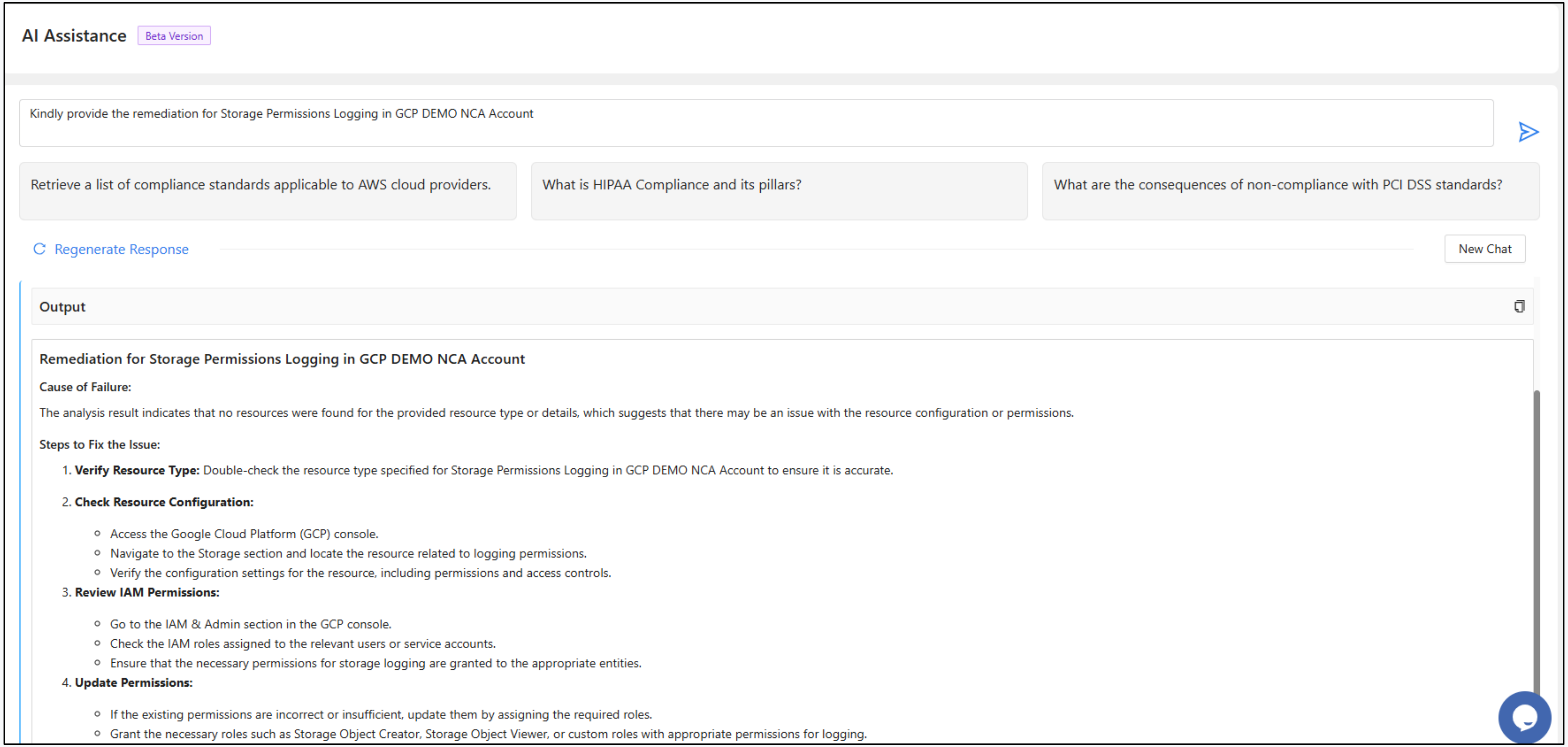
NCA Compliance stands for National Cybersecurity Authority Compliance. It is a set of regulations and guidelines established by the National Cybersecurity Authority in Saudi Arabia to ensure the security and privacy of data and information within the country.

For tenants of Google Cloud Platform in KSA, NCA Compliance is important because it ensures that they adhere to the cybersecurity standards set by the government. By complying with NCA regulations, tenants can demonstrate their commitment to protecting sensitive data and information, thereby reducing the risk of cyber threats and ensuring the security and privacy of their cloud-based operations.

Failure to comply with NCA regulations could result in penalties, fines, or other consequences for tenants using Google Cloud Platform in KSA. Therefore, it is essential for tenants to understand and adhere to NCA Compliance requirements to maintain a secure and compliant cloud environment.

Copyright © 2024 Royal Cyber All rights reserved.

Remediation Guideline using AI


AI Assistance
Beta Version

Kindly provide the remediation for Storage Permissions Logging in GCP DEMO NCA Account

Retrieve a list of compliance standards applicable to AWS cloud providers.
What is HIPAA Compliance and its pillars?
What are the consequences of non-compliance with PCI DSS standards?
Regenerate Response
New Chat
Output

Remediation for Storage Permissions Logging in GCP DEMO NCA Account

Cause of Failure:

The analysis result indicates that no resources were found for the provided resource type or details, which suggests that there may be an issue with the resource configuration or permissions.

Steps to Fix the Issue:

1. **Verify Resource Type:** Double-check the resource type specified for Storage Permissions Logging in GCP DEMO NCA Account to ensure it is accurate.
2. **Check Resource Configuration:**
   - Access the Google Cloud Platform (GCP) console.
   - Navigate to the Storage section and locate the resource related to logging permissions.
   - Verify the configuration settings for the resource, including permissions and access controls.
3. **Review IAM Permissions:**
   - Go to the IAM & Admin section in the GCP console.
   - Check the IAM roles assigned to the relevant users or service accounts.
   - Ensure that the necessary permissions for storage logging are granted to the appropriate entities.
4. **Update Permissions:**
   - If the existing permissions are incorrect or insufficient, update them by assigning the required roles.
   - Grant the necessary roles such as Storage Object Creator, Storage Object Viewer, or custom roles with appropriate permissions for logging.

Copyright © 2024 Royal Cyber All rights reserved.

THANK YOU