Securing our digital future, together.

Ref: Redbelly Cloud Security Architecture Review

Project Background

Redbelly is approaching a major release milestone which will see golden image templates for cloud nodes made available to the Redbelly community. Prior to this go live Redbelly have sought to assess the security posture of both the Amazon Web Services and Google Cloud Platform cloud nodes.

In response to this requirement Tesserent was engaged with the objectives of assessing the cloud nodes to identify risk exposures, understand the current security posture and in turn to provide recommendations and treatments to improve the security of each node.

Engagement Overview

Tesserent conducted a thorough security review of the cloud nodes with evidence collected through a variety of mechanisms including technical assessment tools, document review and technical workshops. Both GCP and AWS environment were assessed for their alignment to CIS (Centre for Internet Security) standards. Through these activities a comprehensive view of the current configuration was established. In addition to the CIS benchmarking a series of other findings were elicited from the evidence collection activity, the break down was as follows:

- 1 High Risk
- 3 Medium Risks
- 7 Low

After the presentation of the assessment report, Redbelly initiated remedial activities, addressing the identified high-risk issues, and providing evidence of resolution back to Tesserent. Medium risks unrelated to the configuration of the golden images will be remediated in accordance with Redbelly's risk management practices.

Conclusion

While opportunities for improvement were identified during the assessment, post-remediation, there were no significant residual risks that would warrant concern regarding the integrity of the golden images.

Redbelly have demonstrated a commitment to understanding and improving their security posture of both their internal operating environment as well as the ICT services that they provide to their community.

Tesserent Limited ABN 13 605 672 928
Phone (03) 9880 5555 • Email info@tesserent.com
Level 5, 990 Whitehorse Rd Box Hill VIC 3128 Australia • tesserent.com

Redbelly Network
Security Architecture Review
Findings Report

Version **0.1** – 7th February 24
Commercial in Confidence
Tesserent Limited
www.tesserent.com
ACN 605 672 928

Document Control Responsibilities

This is a Controlled Document. If the Version Number on the front cover is not in Orange, you have an Uncontrolled Copy. Contact the Document Controller to ensure you have the latest version.
For additional information, contact one of the following parties:

Role	Responsibility	Assigned to	Position
Document Owner	Overall responsibility for the accuracy of the document. Nominating Reviewers and Distribution.	Jack Morris	Partner
Document Author	Prepare the document to the Document Owner's specification.	Len Carriage	Cyber Architect
Reviewed By	Document accuracy in relation to customer technical and commercial requirements	Jack Morris	Partner
Document Controller	Version Control and Distribution to nominated document holders.	Matt Richards	Project Manager
Address	Level 7, 10 Hobart Place, Canberra City, ACT 2601 Phone +61 2 61983391		
Confidentiality	This document is classified. It shall not be disclosed in whole or part, except for the sole purpose of evaluation, without the prior written permission of Tesserent Limited. Its contents must not be divulged to third parties.		

Version Control

This table must be completed for versions 1.0 and greater. Versions lower than 1.0 are draft versions prior to first release of the document. Versions ending in a letter (e.g. 1.1a) are draft revisions.

Version Number	Date Issued	Reason for Update
0.1	30 January 2024	Initial draft

COPYRIGHT NOTICE

Commercial in Confidence

By receiving and reviewing this document, you agree that its contents are and remain the property and confidential information of Tesserent, and that you will:

1. maintain its confidentiality and of all other confidential information provided to you by a member of Tesserent; and

2. only use and copy that information to the extent required to complete your obligations with Tesserent.

Tesserent may have relied on the information provided by you in preparing this document for your consideration. If this information is not correct, is incomplete, or is amended, Tesserent may need (and reserves its right) to amend this document.

Tesserent has exercised care to avoid errors in the information contained in this document but does not warrant that the information is error or omission free. Tesserent accept no responsibility whatsoever for any loss or damage of any kind arising out of the use of all or any part of the information contained herein.

TABLE OF CONTENTS

1. Introduction **5**
2. Engagement Approach **6**
3. Key Recommendations **6**
4. Key Issues and Risks **7**
4.1. Findings Summary findings: **7**
5. Risks and Findings **8**
5.1.1. R01 Lack of architecture or as built documentation 8
5.1.2. R02 Heap buffer overflow vulnerability 9
5.2. CIS Compliance **10**
5.2.1. Compliance Overview 10
5.2.2. Security Score Breakdown 10
5.2.3. CIS Controls Breakdown 11
5.2.4. CIS Compliance / GCP CIS 2.0.0 11
5.2.4.1. GCP CIS Section 1 Identity and Access Management 11
5.2.4.2. GCP CIS Controls Section 2 Logging and Monitoring 13
5.2.4.3. GCP CIS Controls Section 3 Networking 15
5.2.4.4. GCP CIS Controls Section 4 Virtual Machines 17
5.2.4.5. GCP CIS Controls Section 5 Storage 19
5.2.4.6. GCP CIS Controls Section 6 Cloud SQL Database Services 19
5.2.4.7. GCP CIS Controls Section 7 BiqQuery 21
5.2.5. Compliance / AWS CIS 2.0.0 21
5.2.5.1. AWS CIS Controls Section 1 Identity and Access Management 22
5.2.5.2. AWS CIS Controls Section 2 Storage 23
5.2.5.3. AWS CIS Controls Section 3 Logging 24
5.2.5.4. AWS CIS Controls Section 4 Monitoring 25
5.2.5.5. AWS CIS Controls Section 5 Networking 28

1. Introduction

Redbelly Network is a layer 1 blockchain technology that has developed a solution for Compliant Asset Tokenisation. As part of an upcoming major release Redbelly have approached Tesserent to assess the golden images for their GCP and AWS nodes to ensure they are built securely and in alignment with industry best practices.

Tesserent have conducted the assessment using a combination of evidence types including interviews with system experts as well as directly off the cloud platforms using Tesserent's preferred Cloud Security Posture Management solution.

Tesserent have provided the test results of the infrastructure nodes against the CIS Benchmarks from the Centre for Internet Security (CIS), which are a set of globally recognised and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defenses. Developed with a global community of security experts, the guidelines help organisations proactively safeguard against emerging risks. Companies implement the CIS Benchmark guidelines to limit configuration-based security vulnerabilities in their digital assets.

The report provides a holistic view of the environment which will provide Redbelly with a comprehensive understanding of the security posture of the cloud platforms they are operating.

Purpose and Acceptance

This Findings Report document outlines the key requirements and deliverables of Redbelly and Tesserent.
The signing of this document represents its acceptance.
I have reviewed this document and accept all technical and commercial aspects of the document.

Tesserent	Redbelly.
Proposed By: …… (Authorised Signature) Name: _____ Title: _____ Date _____	Accepted By: …… (Authorised Signature) Name: _____ Title: _____ Date _____

2. Engagement Approach

In collaboration with Redbelly stakeholders, Tesserent conducted a cloud security architecture review using two data gathering activities: an assessment using the Orca cloud security posture management (CPSM) platform and a technical discovery workshop. The purpose of these activities was to understand the current architecture and extant security posture within Redbelly tenancy (including security controls and their configuration), current capability gaps and any existing in-flight security projects or other relevant activities that can be combined with industry best practice to develop a robust overall security architecture review to enable Redbelly to move forward.

The results of these data gathering activities were compiled and assessed by the Tesserent team to support the development of rationalised risk assessments that incorporate our understanding of your requirements and specific use cases. On the basis of these risk assessments, a range of recommendations were made in the form of technical remediations, which are included in this document.

3. Key Recommendations

During Tesserent's assessment it was clear Redbelly have employed good security practices as a rule however, there still remain areas where Redbelly could realise significant improvements to the organisation's security posture by considering the adoption of the following recommendations:

Vulnerability and Patch Management Strategy
Through Tesserent's Cloud Security Posture Management Solution a number of instances of vulnerable software versions being used were identified. This indicates that patch management within the environments could be improved to reduces the risk of compromise from vulnerable software.
By developing a strategy for vulnerability management and an accompanying patch management strategy followed by respective processes and technologies Redbelly would greatly reduce its operating risk
Effort: High
Risk Reduction: High

Identity and Access Management Review
System entities and users in both environments were identified as having excessive privileges and insecure account practices including the use of default accounts. Identity represents a key attack vector used by threat actors and as such it is important to ensure good identity hygiene is practiced including implementing least privilege, separation of duties and Privilege Access Management solutions.
Tesserent Recommends conducting an access review across the environment and removing excessive privilege where identified. Ultimately, Redbelly should consider developing a centralised identity strategy to simplify the identity landscape and minimise risks across cloud platforms.
Effort: Medium
Risk Reduction: High

Governance Frameworks
Through discussions with Redbelly Tesserent identified an opportunity to improve the governance structures that support the operations and change to RedBelly's ICT environments. Effective governance ensures that appropriate documentation is created, and processes are followed that ensure systems are designed and implemented in a secure and consistent manner. Additionally, governance is a critical control that enables recovery after disruptions including disaster scenarios.
Tesserent recommends reviewing the current governance frameworks to ensure that both Architecture and Security are critical design considerations before moving services into production.
Effort: Medium

Risk Reduction: High

4. Key Issues and Risks

Leveraging artefacts uncovered during the workshop process Tesserent has created a key risk register, and utilises a risk analysis table based on the principle that a risk has two primary dimensions:

RISK LIKELYHOOD	RISK IMPACT				
	Very Low	Low	Moderate	High	Critical
Certain					
High					
Moderate					
Low					
Not Likely					
Undetermined					

4.1. Findings Summary findings:

The below summary details key findings and failed compliances identified through the assessment that Redbelly should seek to address as a priority.

Finding ID	Category	Finding	Priority	Recommendation
R01	Enterprise	Lack of architecture or as built documentation	Medium	• Tesserent recommends that Redbelly develop the security documentation for the platforms and associated systems • Tesserent recommends reviewing and as necessary implementing or adapting architecture design authority processes as well as security risk management practices
R02	GCP	Heap buffer overflow	High	• Tesserent recommends that Redbelly upgrade to version or above 8.4 or above or patch the local version to the latest version. • Tesserent recommends a review of the vulnerability management and patch management processes currently used to ensure they are scanning all cloud services and that reasonable SLAs

				within risk tolerance for Redbelly are in place.
Logging and Monitoring 2.2	GCP	Ensure that sinks are configured for all log entries (Manual)	Medium	Configure Cloud Audit Log Policy for 'GCP - averer-production and redbelly-testnet' to log all entries
Identity and Access Management 1.5	AWS	'Ensure MFA is enabled for the 'root' user account	Medium	Enable MFA for root accounts
2.2.1 Elastic Compute 2	AWS	Ensure EBS Volume Encryption is Enabled in all Regions	Low	Enable EBS Volume Encryption across all regions
4.1 Virtual Machines	GCP	Ensure that instances are not configured to use the default service account	Low	Assess the required privilege for each instance and apply a least privilege model
4.2 Virtual Machines	GCP	Ensure that instances are not configured to use the default service account with full access to all Cloud APIs	Low	Ensure full API access is not accessible for all instances unless otherwise required.
4.3 Virtual Machines	GCP	Ensure 'Block Project-Wide SSH Keys' Is Enabled for VM Instances	Low	Enable 'Block Project-Wide SSH Keys'
4.4 Virtual Machines	GCP	Ensure oslogin is enabled for a Project	Low	Enable oslogin for Projects
4.7 Virtual Machines	GCP	Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)		Encrypt using CSEK wherever possible.
4.9 Virtual Machines	GCP	Ensure that Compute instances do not have public IP addresses	Low	Remove compute instance access to public IPs

5. Risks and Findings

5.1.1. R01 Lack of architecture or as built documentation

During the workshops conducted with Redbelly it was identified that there is no documentation detailing the design and as built information for both either the GCP or AWS. Design documentation is important reference information for mitigating outages or disruptions to systems that may be caused by changes or as a result of disaster scenarios.
Additionally, design documentation is used as supporting evidence for security risk management practices.

Likelihood: Moderate
Impact: High
Risk: Moderate

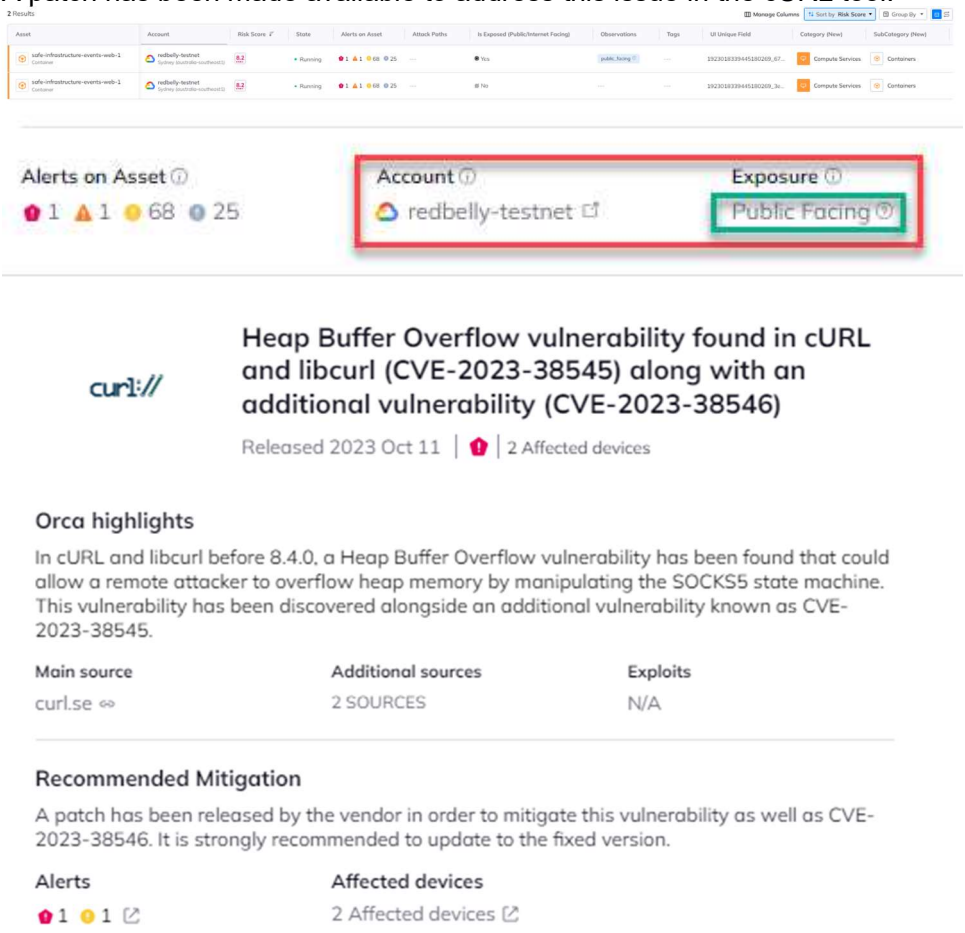
Recommendation:

- Tesserent recommends that Redbelly develop the security documentation for the platforms and associated systems

- Tesserent recommends reviewing and as necessary implementing or adapting architecture design authority processes as well as security risk management practices

5.1.2. R02 Heap buffer overflow vulnerability

Two devices were identified with a known vulnerability on the device exposing the assets to Heap buffer overflow attack. The CVE has been assessed as having a CVSS base score of 9.8. The vulnerability allows an attacker to pass a malformed host name that exceeds the byte limit onto the target buffer which in turn can lead to remote execution.
A patch has been made available to address this issue in the cURL tool.



NOTE: Of the two devices one is publicly facing to the Internet and therefore is deemed high risk and high priority.

Likelihood: Moderate
Impact: Critical
Risk: High

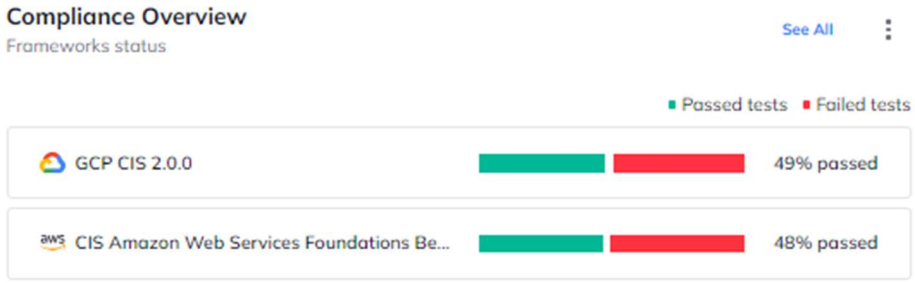
Recommendation:

- Tesserent recommends that Redbelly upgrade to version or above 8.4 or above or patch the local version to the latest version.
- Tesserent recommends a review of the vulnerability management and patch management processes currently used to ensure they are scanning all cloud services and that reasonable SLAs within risk tolerance for Redbelly are in place.

5.2. CIS Compliance

5.2.1. Compliance Overview

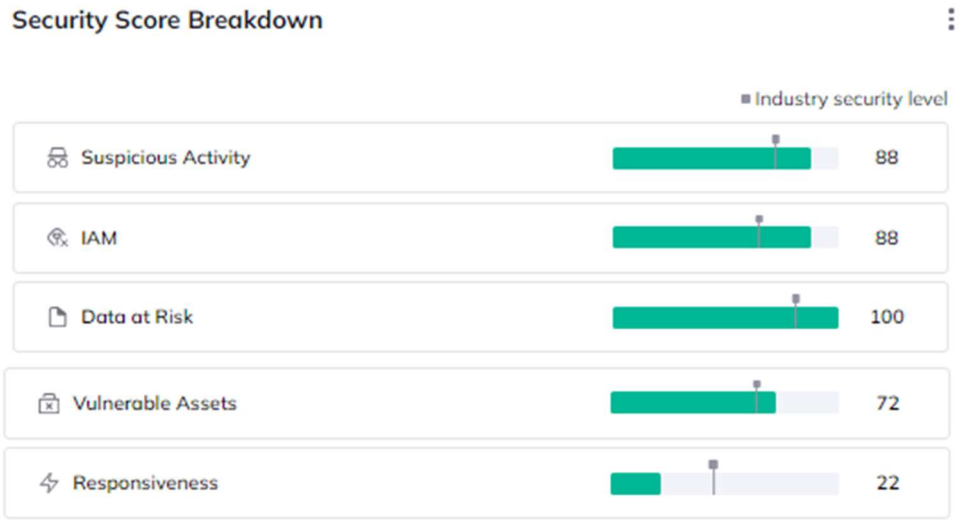
The CIS (Centre for Internet Security) score for both platforms is provided below, and unfortunately, both platforms have scored below 50%. Essentially, this indicates that more than 50% of the systems, devices, and configuration items require urgent attention and corrective action to improve their security posture. Fixing these configuration errors is crucial for enhancing overall security.



CIS compliance is the act of meeting cybersecurity standards from the Centre for Internet Security CIS compliance means establishing baseline configurations to protect systems and data from cyberattacks and other forms of IT risk and are considered Best Practice.

5.2.2. Security Score Breakdown

As shown in the Security Score Breakdown, compared to other similar industries, Redbelly Network scores well for all of them except Responsiveness, however, this is merely the CSPM tool advising that no alerts have been actioned since scanning took place which is to be expected. As such, the Responsiveness score can be discounted in this context.



5.2.3. CIS Controls Breakdown

The following sections summarise the CIS controls that both passed and failed the CIS benchmarks for the relevant platform. You will also note that many of these failed CIS controls are also reflected in the System Alerts because there is a significant risk that the misconfigured security controls could be exploited.

The items which were assessed have been marked with either Green, for pass, Red, for fail or action required, and Beige for items which will require manual inspection.

5.2.4. CIS Compliance / GCP CIS 2.0.0

Legend

Requires Manual inspection	Passed Tests	Failed Tests

5.2.4.1. GCP CIS Section 1 Identity and Access Management

Section score: 33%

Control ID	Priority	Description
1.1	Low	***Ensure that corporate login credentials are used***
1.2	High	***Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)***
1.3	High	***Ensure that Security Key Enforcement is enabled for all admin accounts (Manual)***
1.4	Low	***Ensure that there are only GCP-managed service account keys for each service account*** **Comments:** User managed service accounts should not have user-managed keys. User-managed keys can be easily leaked by common development malpractices like checking keys into the source code or leaving them in the Downloads directory, or accidentally leaving them on support blogs/channels. It is recommended to prevent user-managed service account keys. Applies to: firebase-deployer@averer-production.iam.gserviceaccount.com firebase-deployer@redbelly-testnet.iam.gserviceaccount.com grafana-cloud@redbelly-testnet.iam.gserviceaccount.com orac-scan@averer-production.iam.gserviceaccount.com orca-scan@redbelly-testnet.iam.gserviceaccount.com
1.5	Low	***Ensure that Service Account has no Admin privileges*** **Comments**: The GCP IAM Service Account named 106230767677-compute@developer.gserviceaccount.com has been assigned with role roles/editor that grants admin privileges. This poses a risk as the holder of these roles can perform critical actions such as deleting, updating, and changing settings without user intervention. Also applies to: firebase-adminsdk-vr7ul@averer-production.iam.gserviceaccount.com

		firebase-adminsdk-bgx09@redbelly-testnet.iam.gserviceaccount.com github-action@redbelly-testnet.iam.gserviceaccount.com github-action@averer-production.iam.gserviceaccount.com firebase-deployer@averer-production.iam.gserviceaccount.com firebase-deployer@redbelly-testnet.iam.gserviceaccount.com 77236197852-compute@developer.gserviceaccount.com
1.6	Low	***Ensure that IAM users are not assigned the Service Account User or Service Account Token Creator roles at project level*** **Comments**: Granting the 'iam.serviceAccountUser' or 'iam.serviceAserviceAccountTokenCreatorccountUser' roles to a user for a project gives the user access to all service accounts in the project, including service accounts that may be created in the future. This can result in elevation of privileges by using service accounts and corresponding Compute Engine instances. In order to implement least privileges best practices, IAM users should not be assigned the Service Account User or Service Account Token Creator roles at the project level. Applies to: chun.ko@redbelly.network
1.7	Low	***Ensure user-managed/external keys for service accounts are rotated every 90 days or less***
1.8	Low	***Ensure that Separation of duties is enforced while assigning service account related roles to users*** **Comments**: Service Account admin Role allows the user/identity to create, delete, and manage service accounts. Service Account User Role allows the user/identity to assign service accounts to Apps/Compute Instances. No user should have Service Account Admin and Service Account User roles assigned at the same time to avoid security or privacy incidents and errors. Applies to: chun.ko@redbelly.network GCP User
1.9	Medium	***Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible***
1.10	Low	***Ensure KMS encryption keys are rotated within a period of 90 days***
1.11	Low	***Ensure that Separation of duties is enforced while assigning KMS related roles to users***
1.12	Low	***Ensure API keys only exist for active services*** **Comments**: PI keys are used for authentication, they are simple encrypted strings that identify an application without any principal. Project 'redbelly-testnet' is using API keys - Browser key (auto created by Firebase). API keys are insecure because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to not use API keys in order to avoid these security risks Applies to: GCP - averer-production and redbelly-testnet accounts
1.13	Low	***Ensure API keys are restricted to use by only specified Hosts and Apps*** **Comments**:

		API keys are used for authentication, they are simple encrypted strings that identify an application without any principal. The API key 'Browser key (auto created by Firebase)' does not have any application restrictions. In order to reduce attack vectors, API-Keys can be restricted only to trusted hosts, HTTP referrers or applications. Applies to: GCP API Key
1.14	Low	***Ensure API keys are restricted to only APIs that application needs access*** **Comments**: API keys are used for authentication, they are simple encrypted strings that identify an application without any principal. API key 'Browser key (auto created by Firebase)' is not restricted only to required APIs. In order to reduce attack surfaces by providing least privileges, API-Keys can be restricted to use (call) only APIs required by an application Applies to: GCP API Key
1.15	Low	***Ensure API keys are rotated every 90 days***
1.16	Low	***Ensure Essential Contacts is Configured for Organization*** **Comments**: Many Google Cloud services, such as Cloud Billing, send out notifications to share important information with Google Cloud users. By default, these notifications are sent to members with certain Identity and Access Management (IAM) roles. With Essential Contacts, you can customize who receives notifications by providing your own list of contacts. It was detected that the project 'redbelly-testnet' has no essential contacts configured or is missing one of the following categories: 'LEGAL', 'SECURITY', 'SUSPENSION', 'TECHNICAL', 'TECHNICAL_INCIDENTS'. Applies to: GCP - averer-production and redbelly-testnet accounts
1.17	medium	***Ensure that Dataproc cluster is encrypted using customer-managed encryption key***
1.18	high	***Ensure secrets are not stored in cloud functions environment variables by using secret manager (Manual)***

5.2.4.2. **GCP** CIS Controls Section 2 Logging and Monitoring

Section score: 19%

Control ID	Priority	Description
2.1	Low	***Ensure that Cloud Audit Logging is configured properly (Manual)***
2.2	Medium	***Ensure that sinks are configured for all log entries (Manual)*** **Comments**: GCP Cloud Audit Log is a service that provides two audit logs for each project, folder and organisation. The two audit logs covered are Admin Activity and Data Access. It was detected that the policy (N/A) is not configured properly for Cloud Audit Log types. Applies to: GCP - averer-production and redbelly-testnet accounts
2.3	Low	***Ensure that retention policies on log buckets are configured using Bucket Lock***
2.4	Low	***Ensure log metric filter and alerts exist for project ownership assignments/changes*** **Comments**:

		In order to prevent unnecessary project ownership assignments to users/service-accounts and further misuses of projects and resources, all roles/Owner assignments should be monitored using a custom metric filter. Applies to: GCP - averer-production and redbelly-testnet accounts
2.5	Low	***Ensure that the log metric filter and alerts exist for Audit Configuration changes*** **Comments**: Configuring the metric filter and alerts for audit configuration changes ensures the recommended state of audit configuration is maintained so that all activities in the project are audit-able at any point in time. Applies to: GCP - averer-production and redbelly-testnet accounts
2.6	Low	***Ensure that the log metric filter and alerts exist for Custom Role changes*** **Comments**: It is recommended that a metric filter and alarm be established for changes to Identity and Access Management (IAM) role creation, deletion and updating activities. Applies to: GCP - averer-production and redbelly-testnet accounts
2.7	Low	***Ensure that the log metric filter and alerts exist for VPC Network Firewall rule changes*** **Comments**: Monitoring for Create or Update Firewall rule events gives insight to network access changes and may reduce the time it takes to detect suspicious activity. Applies to: GCP - averer-production and redbelly-testnet accounts
2.8	Low	***Ensure that the log metric filter and alerts exist for VPC network route changes*** **Comments**: is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path. Applies to: GCP - averer-production and redbelly-testnet accounts
2.9	Low	***Ensure that the log metric filter and alerts exist for VPC network changes*** **Comments**: It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes. Monitoring changes to a VPC will help ensure VPC traffic flow is not getting impacted. Applies to: GCP - averer-production and redbelly-testnet accounts
2.10	Low	***Ensure that the log metric filter and alerts exist for Cloud Storage IAM permission changes*** **Comments**: is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes. Monitoring changes to cloud storage bucket permissions may reduce the time needed to detect and correct permissions on sensitive cloud storage buckets and objects inside the bucket. Applies to: GCP - averer-production and redbelly-testnet accounts

2.11	Low	***Ensure that the log metric filter and alerts exist for SQL instance configuration changes*** **Comments**: It is recommended that a metric filter and alarm be established for SQL instance configuration changes. Monitoring changes to SQL instance configuration changes may reduce the time needed to detect and correct misconfigurations done on the SQL server. Applies to: GCP - averer-production and redbelly-testnet accounts
2.12	Low	***Ensure that Cloud DNS logging is enabled for all VPC networks*** **Comments**: We have found that idp-db-vpc VPC doesn't have a DNS policy with cloud logging enabled. Cloud DNS logging records the queries from the name servers within your VPC to Stackdriver. Logged queries can come from Compute Engine VMs, GKE containers, or other GCP resources provisioned within the VPC. Monitoring of Cloud DNS logs provides visibility to DNS names requested by the clients within the VPC. These logs can be monitored for anomalous domain names, evaluated against threat intelligence, etc. Applies to: rbn-vpc-testnet-europe-west9-1-fc2f3e25 rbn-vpc-testnet-asia-southeast1-0-cd259a4b default rbn-vpc-testnet-europe-west9-1-f3fd4d72 rbn-vpc-testnet-asia-southeast1-0-cd5c8bb1 idp-db-vpc rbn-vpc-testnet-asia-southeast1-0-9a128e46 rbn-vpc-testnet-europe-west9-1-db317765 rbn-vpc-testnet-europe-west9-1-f683d401 rbn-vpc-testnet-us-west1-5-4a67ba9b rbn-vpc-testnet-australia-southeast2-8-c312f22b rbn-vpc-testnet-asia-southeast1-0-89ecc918 rbn-vpc-testnet-asia-southeast1-0-637d1648 rbn-vpc-testnet-australia-southeast1-4-a16a6822 rbn-vpc-testnet-europe-west9-1-7b44a962 rbn-vpc-testnet-europe-west9-1-a91d653f rbn-vpc-testnet-asia-southeast1-0-0ca05eb1
2.13	Low	***Ensure Cloud Asset Inventory Is Enabled***
2.14	Low	***Ensure 'Access Transparency' is 'Enabled' (Manual)***
2.15	Low	***Ensure 'Access Approval' is 'Enabled'***
2.16	Low	***Ensure Logging is enabled for HTTP(S) Load Balancer (Manual)***

5.2.4.3. GCP CIS Controls Section 3 Networking

Section score: 40%

Control ID	Priority	Description
3.1	Low	***Ensure that the default network does not exist in a project*** **Comments**: The default network has a preconfigured network configuration and automatically generates insecure firewall rules. These automatically

		created firewall rules do not get audit logged and cannot be configured to enable firewall rule logging. Furthermore, the default network is an auto mode network, which means that its subnets use the same predefined range of IP addresses, and as a result, it's not possible to use Cloud VPN or VPC Network Peering with the default network. Applies to: GPC Virtual Private Cloud
3.2	Low	***Ensure legacy networks do not exist for a project***
3.3	Low	***Ensure that DNSSEC is enabled for Cloud DNS*** **Comments**: Domain Name System Security Extensions (DNSSEC) in Cloud DNS enables domain owners to take easy steps to protect their domains against DNS hijacking and man-in-the-middle and other attacks and should be enabled. Applies to: GCP DNS Managed Zone
3.4	Low	***Ensure that RSASHA1 is not used for the key-signing key in Cloud DNS DNSSEC***
3.5	Low	***Ensure that RSASHA1 is not used for the zone-signing key in Cloud DNS DNSSEC***
3.6	Low	***Ensure that SSH access is restricted from the internet*** **Comments**: Firewall rules are defined at the VPC network level and are specific to the network in which they are defined. The rules themselves cannot be shared among networks. Firewall rules only support IPv4 traffic. When specifying a source for an ingress rule or a destination for an egress rule by address, only an IPv4 address or IPv4 block in CIDR notation can be used. Generic (0.0.0.0/0) incoming traffic from the internet to VPC or VM instance using SSH on Port 22 can be avoided. Applies to: GCP VPC Firewall Rule
3.7	Low	***Ensure that RDP access is restricted from the Internet*** **Comments**: GCP Firewall Rules are specific to a VPC Network. Each rule either allows or denies traffic when its conditions are met. Its conditions allow users to specify the type of traffic, such as ports and protocols, and the source or destination of the traffic, including IP addresses, subnets, and instances. Applies to: GCP VPC Firewall Rule
3.8	Low	***Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network*** **Comments**: Flow Logs is a feature that enables users to capture information about the IP traffic going to and from network interfaces in the organization's VPC Subnets. Once a flow log is created, the user can view and retrieve its data in Stackdriver Logging. It is recommended that Flow Logs be enabled for every business critical VPC subnet. Applies to: default rbn-subnet-testnet-asia-southeast1-0-cd259a4b idp-db-subnet rbn-subnet-testnet-europe-west9-1-f3fd4d72 rbn-subnet-testnet-europe-west9-1-f683d401

		rbn-subnet-testnet-asia-southeast1-0-9a128e46 rbn-subnet-testnet-asia-southeast1-0-89ecc918 rbn-subnet-testnet-europe-west9-1-db317765 rbn-subnet-testnet-asia-southeast1-0-cd5c8bb1 rbn-subnet-testnet-asia-southeast1-0-0ca05eb1 rbn-subnet-testnet-europe-west9-1-a91d653f rbn-subnet-testnet-australia-southeast2-8-c312f22b rbn-subnet-testnet-us-west1-5-4a67ba9b rbn-subnet-testnet-australia-southeast1-4-a16a6822 rbn-subnet-testnet-europe-west9-1-fc2f3e25 rbn-subnet-testnet-asia-southeast1-0-637d1648 rbn-subnet-testnet-europe-west9-1-7b44a962
3.9	Low	***Ensure no HTTPS or SSL proxy load balancers permit SSL policies with weak cipher suites***
3.10	Medium	***Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)***

5.2.4.4. GCP CIS Controls Section 4 Virtual Machines

Section score: 33%

Control ID	Priority	Description
4.1	Low	***Ensure that instances are not configured to use the default service account*** **Comments**: It is recommended to configure your instance to not use the default Compute Engine service account because it has the Editor role on the project. Applies to: rhs-db-connector
4.2	Low	***Ensure that instances are not configured to use the default service account with full access to all Cloud APIs*** **Comments**: We have found a Vm instance with full access to all Cloud APIs that is using the default service account. To support principle of least privileges and prevent potential privilege escalation it is recommended that instances are not assigned to default service account Compute Engine default service account with Scope Allow full access to all Cloud APIs. Applies to: rhs-db-connector

4.3	Low	***Ensure 'Block Project-Wide SSH Keys' Is Enabled for VM Instances*** **Comments**: Project-wide SSH keys are stored in Compute/Project-meta-data. Project wide SSH keys can be used to login into all the instances within project. Using project-wide SSH keys eases the SSH key management but if compromised, poses the security risk which can impact all the instances within project. It is recommended to use Instance specific SSH keys which can limit the attack surface if the SSH keys are compromised. Applies to: multisig-server bn-vm-testnet-us-west1-5-4a67ba9b rbn-vm-testnet-australia-southeast2-8-c312f22b rbn-vm-testnet-asia-southeast1-0-0ca05eb1 bn-vm-testnet-australia-southeast1-4-a16a6822 rbn-vm-testnet-europe-west9-1-a91d653f rhs-db-connector
4.4	Low	***Ensure oslogin is enabled for a Project*** **Comments**: Enabling osLogin ensures that SSH keys used to connect to instances are mapped with IAM users. Revoking access to IAM user will revoke all the SSH keys associated with that particular user. It facilitates centralized and automated SSH key pair management which is useful in handling cases like response to compromised SSH key pairs and/or revocation of external/third-party/Vendor users. Applies to: rhs-db-connector
4.5	Low	***Ensure 'Enable connecting to serial ports' is not enabled for VM Instance***
4.6	Low	***Ensure that IP forwarding is not enabled on Instances***
4.7	Low	***Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)*** **Comments**: Customer-Supplied Encryption Keys (CSEK) are a feature in Google Cloud Storage and Google Compute Engine. If you supply your own encryption keys, Google uses your key to protect the Google-generated keys used to encrypt and decrypt your data. By default, Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for you without any additional actions on your part. However, if you wanted to control and manage this encryption yourself, you can provide your own encryption keys. At least business critical VMs should have VM disks encrypted with CSEK. Applies to: multisig-server bn-vm-testnet-us-west1-5-4a67ba9b rbn-vm-testnet-australia-southeast2-8-c312f22b rbn-vm-testnet-asia-southeast1-0-0ca05eb1 bn-vm-testnet-australia-southeast1-4-a16a6822 rbn-vm-testnet-europe-west9-1-a91d653f rhs-db-connector

4.8	Low	***Ensure Compute instances are launched with Shielded VM enabled***
4.9	Low	***Ensure that Compute instances do not have public IP addresses*** **Comments**: To reduce your attack surface, Vm instances should not have public IP addresses. Instead, instances should be configured behind load balancers, to minimize the instance's exposure to the internet. Applies to: multisig-server bn-vm-testnet-us-west1-5-4a67ba9b rbn-vm-testnet-australia-southeast2-8-c312f22b rbn-vm-testnet-asia-southeast1-0-0ca05eb1 bn-vm-testnet-australia-southeast1-4-a16a6822 rbn-vm-testnet-europe-west9-1-a91d653f rhs-db-connector
4.10	Medium	***Ensure that App Engine applications enforce HTTPS connections (Manual)***
4.11	Low	***Ensure that Compute instances have Confidential Computing enabled***
4.12	Low	***Ensure the latest operating system updates are installed on your virtual machines in all projects (Manual)***

5.2.4.5. GCP CIS Controls Section 5 Storage

Section score: 100%

Control ID	Priority	Description
5.1	Low	***Ensure that Cloud Storage bucket is not anonymously or publicly accessible***
5.2	Low	***Ensure that Cloud Storage buckets have uniform bucket-level access enabled***

5.2.4.6. **GCP** CIS Controls Section 6 Cloud SQL Database Services

Section score: 57%

Sub-Section MySQL Database 57%

Control ID	Priority	Description
6.1.1	Medium	***Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges (Manual)***
6.1.2	Low	***Ensure 'skip_show_database' database flag for Cloud SQL Mysql instance is set to 'on'***
6.1.3	Low	***Ensure that the 'local_infile' database flag for a Cloud SQL Mysql instance is set to 'off'***
6.4	Low	***Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL*** **Comments**: SQL database connections if successfully trapped (MITM); can reveal sensitive data like credentials, database queries, query outputs etc. It is

		recommended to enforce all incoming connections to SQL database instance to use SSL. This applies to rhs-db and idp-db
6.5	Low	***Ensure that Cloud SQL Database instances do not implicitly whitelist all public IP addresses***
6.6	Low	***Ensure that Cloud SQL database instances do not have public IPs***
6.7	Low	***Ensure that Cloud SQL database instances are configured with automated backups*** **Comments**: Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with that instance. Automated backups need to be set for any instance that contains data that should be protected from loss or damage. This applies to rhs-db and idp-db

Sub-Section – PostgreSQL 33%

Control ID	Priority	Description
6.2.1	Low	***Ensure 'log_error_verbosity' database flag for Cloud SQL PostgreSQL instance is set to 'DEFAULT' or stricter***
6.2.2	Low	***Ensure that the 'log_connections' database flag for Cloud SQL PostgreSQL instance is set to 'on'*** **Comment**: PostgreSQL does not log attempted connections by default. Enabling the 'log_connections' setting will create log entries for each attempted connection as well as successful completion of client authentication which can be useful in troubleshooting issues and to determine any unusual connection attempts to the server. This applies to rhs-db and idp-db
6.2.3	Low	***Ensure that the 'log_disconnections' database flag for Cloud SQL PostgreSQL instance is set to 'on'*** **Comment**: PostgreSQL does not log session details such as duration and session end by default. Enabling the log_disconnections setting will create log entries at the end of each session which can be useful in troubleshooting issues and determine any unusual activity across a time period. The log_disconnections and log_connections work hand in hand and generally, the pair would be enabled/disabled together. This applies to rhs-db and idp-db
6.2.4	Medium	***Ensure 'log_statement' database flag for Cloud SQL PostgreSQL instance is set appropriately (Manual)***
6.2.5	Medium	***Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning' (Manual)***
6.2.6	Low	***Ensure 'log_min_error_statement' database flag for Cloud SQL PostgreSQL instance is set to 'Error'*** **Comment**: The log_min_error_statement flag defines the minimum message severity level that is considered as an error statement. Messages for error statements are logged with the SQL statement. ERROR is considered the best practice setting. This applies to ldp-db and rhs-db SQL instances

6.2.7	Low	***Ensure that the 'log_min_duration_statement' database flag for Cloud SQL PostgreSQL instance is set to '-1' (disabled)***
6.2.8	Low	***Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging*** **Comment**: Open source pgaudit extension enables you to manage and access logs in a central location. By enabling cloudsql.enable_pgaudit flag and installing the extension you enable database auditing in your PostgreSQL through pgAudit. This extension provides detailed session and object logging to comply with government, financial, & ISO standards and provides auditing capabilities to mitigate threats by monitoring security events on the instance. It was detected that both Sql Instances idp-db pgaudit and rhs-db pgaudi the flag is disabled.
6.2.9	Low	***Ensure Instance IP assignment is set to private***

Sub-Section SQL Server 86%

Control ID	Priority	Description
6.3.1	Low	***Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'***
6.3.2	Low	***Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'***
6.3.3	Medium	***Ensure 'user Connections' Database Flag for Cloud Sql Server Instance Is Set to a Non-limiting Value (Manual)***
6.3.4	Low	***Ensure 'user options' database flag for Cloud SQL Server instance is not configured***
6.3.5	Low	***Ensure 'remote access' database flag for Cloud SQL Server instance is set to 'off'***
6.3.6	Low	***Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'***
6.3.7	Low	***Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'***

5.2.4.7. GCP CIS Controls Section 7 BiqQuery

Section score: 100%

Control ID	Priority	Description
7.1	Low	***Ensure that BigQuery datasets are not anonymously or publicly accessible***
7.2	Low	***Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)***
7.3	Low	***Ensure that a Default Customer-managed encryption key (CMEK) is specified for all BigQuery Data Sets***

5.2.5. Compliance / AWS CIS 2.0.0

Legend

Requires Manual inspection	Passed Tests	Failed Tests

5.2.5.1. AWS CIS Controls Section 1 Identity and Access Management

Section score: 50%

Control ID	Priority	Description
1.1	Medium	***Maintain current contact details (Manual)***
1.2	Medium	***Ensure security contact information is registered (Manual)***
1.3	Medium	***Ensure security questions are registered in the AWS account (Manual)***
1.4	Low	***Ensure no 'root' user account access key exists***
1.5	Medium	***Ensure MFA is enabled for the 'root' user account*** **Comment**: AWS IAM User named <root_account> does not have MFA enabled. The root user account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs into an AWS website, they will be prompted for their username and password as well as for an authentication code from their AWS MFA device.
1.6	Medium	***Ensure hardware MFA is enabled for the 'root' user account (Manual)***
1.7	Medium	***Eliminate use of the 'root' user for administrative and daily tasks***
1.8	Low	***Ensure IAM password policy requires minimum length of 14 or greater*** **Comment**: The password policy PasswordPolicy, associated with the Account named 135561891954, does not enforce a proper minimum length. A password without a minimum length of 14 characters is weaker and much easier to crack, increasing the risk of unauthorized access.
1.9	Low	**Ensure IAM password policy prevents password reuse**
1.10	Medium	**Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password**
1.11	Medium	**Do not setup access keys during initial user setup for all IAM users that have a console password**
1.12	Low	**Ensure credentials unused for 45 days or greater are disabled**
1.13	Low	**Ensure there is only one active access key available for any single IAM user**
1.14	Low	**Ensure access keys are rotated every 90 days or less**
1.15	Low	***Ensure IAM Users Receive Permissions Only Through Groups***
1.16	Low	***Ensure IAM policies that allow full administrative privileges are not attached*** **Comment**: IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended and considered a standard security advice to grant least privilege -that is, granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks, instead of allowing full administrative privileges.

1.17	Low	***Ensure a support role has been created to manage incidents with AWS Support*** **Comment**: AWS provides a support centre that can be used for incident notification and response, as well as technical support and customer services. Create an IAM Role to allow authorized users to manage incidents with AWS Support.
1.18	Low	**Ensure IAM instance roles are used for AWS resource access from instances**
1.19	Low	**Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed**
1.20	Low	***Ensure that IAM Access analyser is enabled for all regions*** **Comment**: Enable IAM Access analyser for IAM policies about all resources. IAM Access Analyzer is a technology introduced at AWS reinvent 2019. After the Analyzer is enabled in IAM, scan results are displayed on the console showing the accessible resources. Scans show resources that other accounts and federated users can access, such as KMS keys and IAM roles. So, the results allow you to determine if an unintended user is allowed, making it easier for administrators to monitor least privileges access.
1.21	Medium	***Ensure IAM users are managed centrally via identity federation or AWS Organizations for multi-account environments (Manual)***
1.22	Medium	***Ensure access to AWSCloudShellFullAccess is restricted (Manual)***

5.2.5.2. AWS CIS Controls Section 2 Storage

Section score: 56%
Sub-Section - Simple Storage Service (S3)
Section Score 25%

Control ID	Priority	Description
2.1.1	Medium	***Ensure S3 Bucket Policy is set to deny HTTP requests*** **Comment**: The AWS S3 Bucket named rbn-testnet-artefacts does not enforce HTTPS. If a bucket's policy doesn't explicitly deny non-HTTPS connections, it puts the bucket in the risk of eavesdropping and man-in-the-middle attacks. This bucket was created 2 months ago, 2023, December 13.
2.1.2	Low	***Ensure MFA Delete is enabled on S3 buckets*** **Comment**: Using MFA-protected S3 buckets will enable an extra layer of protection to ensure that the S3 objects (files) cannot be accidentally or intentionally deleted by the AWS users that have access to the buckets.
2.1.3	Medium	***Ensure all data in Amazon S3 has been discovered, classified and secured when required (Manual)***
2.1.4	Low	***Ensure that S3 Buckets are configured with 'Block public access (bucket settings)'***

Sub-Section – Elastic Cloud Compute (EC2)
Section Score 0%

Control ID	Priority	Description
2.2.1	Low	***Ensure EBS Volume Encryption is Enabled in all Regions*** **Comment**: Elastic Compute Cloud (EC2) supports account-level encryption for Elastic Block Store (EBS) service, which uses Key Management Service (KMS) keys. Disabled encryption requires you to build, secure and maintain your own key management infrastructure. You can encrypt volumes and snapshots manually only at creation time - it is impossible to encrypt an existing unencrypted volume or snapshot. While enabled by default, new EBS volumes and snapshot copies are encrypted at rest, which provides an additional layer of data protection.

Sub-Section – Relational Database Services (RDS)
Section Score 100%

Control ID	Priority	Description
2.3.1	Low	***Ensure that encryption-at-rest is enabled for RDS Instances***
2.3.2	Low	***Ensure Auto Minor Version Upgrade feature is Enabled for RDS Instances***
2.3.3	Low	***Ensure that public access is not given to RDS Instance***

Sub-Section – Elastic File system (EFS)
Section Score 100%

Control ID	Priority	Description
2.4.1	Low	***Ensure that encryption is enabled for EFS file systems***

5.2.5.3. AWS CIS Controls Section 3 Logging

Section score: 55%

Control ID	Priority	Description
3.1	Low	***Ensure CloudTrail is enabled in all regions*** **Comment**: AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. Visibility into your AWS account activity is a key aspect of security and operational best practices. Enabling logging with CloudTrail allows you to identify what actions were performed in your account, by who, and on which assets - enabling quicker discovery and response to anomalous activity or events in your account. We identified that for the CloudAccount there isn't CloudTrail which enabled logging in all regions, Management Events, and logging all types of events (read and write).
3.2	Low	***Ensure CloudTrail log file validation is enabled***
3.3	Medium	***Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible***
3.4	Low	***Ensure CloudTrail trails are integrated with CloudWatch Logs***
3.5	Low	***Ensure AWS Config is enabled in all regions*** **Comment**: AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended to enable AWS Config to be enabled in all regions.

3.6	Low	***Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket***
3.7	Low	***Ensure CloudTrail logs are encrypted at rest using KMS CMKs***
3.8	Low	***Ensure rotation for customer created symmetric CMKs is enabled***
3.9	Low	***Ensure VPC flow logging is enabled in all VPCs*** Comment: The following VPCs are non-compliant vpc-0dd445d46d8400906 vpc-094dc1901b4f71429 vpc-03afbba7b52611fb1 vpc-0da38fc4c97dd9983 vpc-0c05137877e19a096 vpc-05d1ae1547052a3d5 vpc-034ee81184872109d vpc-01a1b1f1bd46b4b2f vpc-0a12cecdd57bfeef0 vpc-0b91fda8cf0106d5d vpc-099d1313c521dc790 vpc-00b881e5262005025 vpc-0244b95a2b5190308 vpc-077acc7dc3eb888bd vpc-06eb0ce68557059b5 rbn-vpc-testnet-us-west-2-3-d89ee32a vpc-0c67a1d59ad0d9a58 vpc-0c6af76c71efb9a60
3.10	Low	***Ensure that Object-level logging for write events is enabled for S3 bucket*** **Comment**: S3 object-level API operations such as GetObject, DeleteObject, and PutObject are called data events. By default, CloudTrail trails don't log data events and so it is recommended to enable Object-level logging for S3 buckets.
3.11	Low	***Ensure that Object-level logging for read events is enabled for S3 bucket*** **Comment**: S3 object-level API operations such as GetObject, DeleteObject, and PutObject are called data events. By default, CloudTrail trails don't log data events and so it is recommended to enable Object-level logging for S3 buckets.

5.2.5.4. AWS CIS Controls Section 4 Monitoring

Section score: 6%

Control ID	Priority	Description
4.1	Low	***Ensure IAM policy changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.
4.2	Low	***Ensure management console sign-in without MFA is monitored***

		Comment: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring for single-factor console logins will increase visibility into accounts that are not protected by MFA.
4.3	Low	***Ensure usage of 'root' account is monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring for root account logins will provide visibility into the use of a fully privileged account and an opportunity to reduce the use of it.
4.4	Low	***Ensure IAM policy changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact.
4.5	Low	***Ensure CloudTrail configuration changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account.
4.6	Low	***Ensure AWS Management Console authentication failures are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation.
4.7	Low	***Ensure disabling or scheduled deletion of customer created CMKs is monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Data encrypted with disabled or deleted keys will no longer be accessible.
4.8	Low	***Ensure S3 bucket policy changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch and establishing corresponding metric filters and alarms. No such filter or alarm was detected for changes to S3 bucket policies. Monitoring changes to S3 bucket policies will make it easier to detect and rectify permissive policies.
4.9	Low	***Ensure AWS Config configuration changes are monitored*** Comment: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring changes to AWS Config configuration will help ensure sustained visibility of configuration items within the AWS account.
4.10	Low	***Ensure security group changes are monitored*** Comment: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing

		corresponding metric filters and alarms. Security Groups are a stateful packet filter that controls ingress and egress traffic within a VPC. Monitoring changes to security group will help ensure that resources and services are not unintentionally exposed.
4.11	Low	***Ensure Network Access Control Lists (NACL) changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. NACLs are used as a stateless packet filter to control ingress and egress traffic for subnets within a VPC. Monitoring changes to NACLs will help ensure that AWS resources and services are not unintentionally exposed.
4.12	Low	***Ensure changes to network gateways are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Network gateways are required to send/receive traffic to a destination outside of a VPC. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path.
4.13	Low	***Ensure route table changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Routing tables are used to route network traffic between subnets and to network gateways. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.
4.14	Low	***Ensure VPC changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is possible to have more than 1 VPC within an account, in addition it is also possible to create a peer connection between 2 VPCs enabling network traffic to route between VPCs. Monitoring changes to VPC will help ensure VPC traffic flow is not getting impacted.
4.15	Low	***Ensure AWS Organizations changes are monitored*** **Comment**: Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Monitoring AWS Organizations changes can help you prevent any unwanted, accidental or intentional modifications that may lead to unauthorized access or other security breaches. This monitoring technique helps you to ensure that any unexpected changes performed within your AWS Organizations can be investigated and any unwanted changes can be rolled back.
4.16	Low	***Ensure AWS Security Hub is enabled***

5.2.5.5. AWS CIS Controls Section 5 Networking

Section score: 78%

Sub-Section – 5.1 Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports 100%

Control ID	Priority	Description
5.1.1	Low	***Ensure no Network ACLs allow ingress from 0.0.0.0/0 to SSH port (22)***
5.1.2	Low	***Ensure no Network ACLs allow ingress from 0.0.0.0/0 to Remote Desktop port (3389)***

Sub-Section - 5.2 Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports 50%

Control ID	Priority	Description
5.2.1	Low	***Ensure no security groups allow ingress from::/0 to SSH port (22)*** The following Security Groups allow ingress from, 0.0.0.0/0 sg-0e9aa68dd6a9a1073 sg-08c829d93a760fc83 sg-0c97471f37cccb628 sg-025cb7d37cb56ef65 sg-04020844d50bffe6d sg-0b51f18e74ea82439 sg-08c139b5aa0e4c9e3 sg-061c995688788564d
5.2.2	**Low**	***Ensure no security groups allow ingress from 0.0.0.0/0 to Remote Desktop port (3389)***

Sub-Section - 5.3 Ensure no security groups allow ingress from::/0 to remote server administration ports 100%

Control ID	Priority	Description
5.3.1	Low	***Ensure no security groups allow ingress from ::/0 to SSH port (22)***
5.3.2	Low	***Ensure no security groups allow ingress from 0.0.0.0/0 to Remote Desktop port (3389)***

Control ID	Priority	Description
5.4	Low	***Ensure the default security group of every VPC restricts all traffic*** The following VPC's failed the control: vpc-03afbba7b52611fb1 vpc-0c67a1d59ad0d9a58 vpc-0a12cecdd57bfeef0 vpc-0da38fc4c97dd9983 vpc-094dc1901b4f71429 vpc-06eb0ce68557059b5

		vpc-05d1ae1547052a3d5 vpc-077acc7dc3eb888bd vpc-01a1b1f1bd46b4b2f vpc-099d1313c521dc790 vpc-0b91fda8cf0106d5d vpc-034ee81184872109d vpc-0c6af76c71efb9a60 vpc-0dd445d46d8400906 vpc-0c05137877e19a096 rbn-vpc-testnet-us-west-2-3-d89ee32a vpc-0244b95a2b5190308 vpc-00b881e5262005025
5.5	Low	***Ensure routing tables for VPC peering are "least access"***
5.6	Low	***Ensure that EC2 Metadata Service only allows IMDSv2*** The following EC2 Instances are not enforcing the use of IMDSv2, the enhanced version of the Instance Metadata Service. IMDSv2 solves a lot of security issues in the original version (IMDSv1) by using session-based authentication. If an instance is still using IMDSv1, malicious actors can use compromised applications running inside it to gain unauthorized access to the metadata service. rbnvm-testnet-us-west-2-3-8862234c rbnvm-testnet-ap-southeast-1-6-670d3a19 rbnvm-testnet-ap-southeast-2-2-06126dfa rbnvm-testnet-eu-west-3-7-b7ded656